Kamal Lodaya (Ed.)

LNCS 7750

Logic and Its Applications

5th Indian Conference, ICLA 2013
Chennai, India, January 2013
Proceedings

Springer

Lecture Notes in Computer Science 7750

FoLLI Publications on Logic, Language and Information

Subline of Lectures Notes in Computer Science

Kamal Lodaya (Ed.)

Logic and Its Applications

5th Indian Conference, ICLA 2013
Chennai, India, January 10-12, 2013
Proceedings

Springer

Volume Editor

Kamal Lodaya
The Institute of Mathematical Sciences
CIT Campus
Chennai 600113, India
E-mail: kamal@imsc.res.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-36038-1 e-ISBN 978-3-642-36039-8
DOI 10.1007/978-3-642-36039-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012955140

CR Subject Classification (1998): F.4.1, F.3.1, I.2.3-4, F.4.3, F.1.1-2, G.2.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at ICLA2013: 5th Indian Conference on Logic and its Applications (ICLA), held at the Institute of Mathematical Sciences, Chennai, during January 10–12, 2013.

The ICLA series is a biennial conference organized by the Association for Logic in India. It aims to bring together researchers from a wide variety of fields in which formal logic plays a significant role: mathematicians, philosophers, computer scientists, and logicians. ICLA also welcomes papers on the history of logic.

The papers in the volume span a wide range of themes. We have contributions to decision theory, communication theory and set theory, to proof theory and modeling systems. We thank the authors who submitted to the conference for their contributions, and those whose papers appear here for their work in preparing the final versions.

Like the previous conferences (IIT-Bombay, 2005 and 2007; Jadavpur University, Kolkata, 2007; IMSc, 2009; and Delhi University, 2011), at the fifth conference, too, we were fortunate to have a number of highly eminent researchers giving plenary talks. It gives me great pleasure to thank Mirna Džamonja, Joseph Halpern, Agi Kurucz, Martin Otto, Mark Reynolds, Adriane Rini, and Gabriel Sandu for agreeing to give invited talks and for contributing to this volume. In spite of our approaching him very late, Max Cresswell was gracious and kindly agreed to give an invited talk.

I would like to thank the Program Committee (PC): for their cooperation in finding many external reviewers, who put in a great deal of hard work along with the PC members in generating at least three review reports for each paper. I express my gratitude to all PC members for making discussing and selecting the papers an easy job, and thank all the reviewers for their invaluable help. We used the EasyChair system which, streamlined the whole process.

The conference was held at the Institute of Mathematical Sciences (IMSc), Chennai. I thank IMSc and the administration for immediately agreeing to take on the responsibility, and the Organizing Committee members (Sujata Ghosh, R. Ramanujam, S.P. Suresh) and the IMSc volunteers for taking on the work load. Ramanujam helped both with the programmatic and with the organizational work, he deserves a special thank you.

I thank the Editorial Board of Springer for agreeing to publish this volume in their LNCS series.

November 2012 Kamal Lodaya

Organization

Organizing Committee

Sujata Ghosh	Indian Statistical Institute, Chennai, India
Kamal Lodaya	The Institute of Mathematical Sciences, Chennai, India
R. Ramanujam (Chair)	The Institute of Mathematical Sciences, Chennai, India
S.P. Suresh	Chennai Mathematical Institute, India

The Organizing Committee thank all the volunteers who helped out, including A. Baskar, Soma Dutta, Anup Mathew, Ramchandra Phawade, A.V. Sreejith.

Programme Committee

Mihir Chakraborty	ISI Kolkata/Jadavpur University, India
Roy T. Cook	University of Minnesota, Minneapolis, USA
Rajeev Gore	Australian National University, Canberra, AU
Kamal Lodaya (Chair)	The Institute of Mathematical Sciences, India
David C. Makinson	London School of Economics, UK
Johann Makowsky	Technion, Haifa, Israel
Angelo Montanari	University of Udine, Italy
Ranjan Mukhopadhyay	Viswa Bharati, Santiniketan, India
Vineet Padmanabhan	University of Hyderabad, India
R. Ramanujam	The Institute of Mathematical Sciences, India
Esko Turunen	Tampere University of Technology, Finland
Rineke Verbrugge	University of Groningen, The Netherlands

Additional Reviewers

The Programme Committee would like to thank the reviewers listed below.

Baskar Anguraj
Alexandru Baltag
Mohua Banerjee
Can Baskent
Achim Blumensath
Davide Bresolin
Jeremy Dawson
Catalin Dima
Agostino Dovier
Deepak Garg
Giangiacomo Gerla
Sujata Ghosh
Marie-Hélène Gorisse
Dimitar Guelev
James Hales
Joseph Halpern

Bernhard Heinemann
Wesley Holliday
Zhe Hou
Giorgi Japaridze
Jouni Järvinen
Bakhadyr Khoussainov
Churn-Jung Liau
Pabitra Mitra
Yoram Moses
Sara Negri
André Nies
Nicola Olivetti
Eric Pacuit
Mimmo Parente
Dirk Pattinson
Alessandro Provetti
Arun Pujari
Dilip Raghavan
N. Raja
Bryan Renne
Adriane Rini
David Ripley
François Schwarzentruber
Jayanta Sen
Sunil Easaw Simon
John Slaney
S.P. Suresh
Jakub Szymanik
Wolfgang Thomas
Jimmy Thomson
Hans Van Ditmarsch
Jan von Plato
Peter B.M. Vranas
Yanjing Wang

Table of Contents

Invited Papers

Contributed Papers

Constructive Decision Theory*

(Extended Abstract)

Lawrence E. Blume[1], David A. Easley[1], and Joseph Y. Halpern[2]

[1] Economics Department
Cornell University
Ithaca, NY 14853, USA
[2] Computer Science Department
Cornell University
Ithaca, NY 14853, USA

Most models of decisionmaking under uncertainty describe a decision environment with a set of states and a set of outcomes. Objects of choice are *acts*, functions from states to outcomes. The decision maker (DM) holds a preference relation on the set of all such functions. Representation theorems characterize those preference relations with utility functions on acts that separate (more or less) tastes on outcomes from beliefs on states. The canonical example is Savage's [11] characterization of those preference relations that have a subjective expected utility (SEU) representation: Acts are ranked by the expectation of a utility payoff on their outcomes with respect to a probability distribution on states. *Choquet expected utility* [12] maintains the separation between tastes and beliefs, but does not require that beliefs be represented by an additive measure. Tversky and Kahneman's [13] *cumulative prospect theory* relaxes the taste-belief separation by assessing gains and losses with different belief measures; Wakker and Tversky [15] discuss generalizations of SEU from this point of view. Modern attempts to represent *ambiguity* in choice theory relax both the meaning of likelihood and the separation of tastes and beliefs that characterize SEU. All of these generalizations of SEU, however, maintain the state-outcome-act description of objects of choice and, moreover, take this description of choice problems as being given prior to the consideration of any preference notion.

We, on the other hand, follow Ellsberg [4] in locating the source of ambiguity in the description of the problem. For Savage [11, p. 9], the *world* is 'the object about which the person is concerned' and a *state* of the world is 'a description of the world, leaving no relevant aspect undescribed.' But what are the 'relevant' descriptors of the world? Choices do not come equipped with states. Instead they are typically objects described by their manner of realization, such as 'buy 100 shares of IBM' or 'leave the money in the bank,' 'attack Iraq,' or 'continue to

---

* Work supported in part by NSF under grants CTC-0208535, ITR-0325453, and IIS-0534064, by ONR under grants N00014-00-1-03-41 and N00014-01-10-511, and by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the ONR under grant N00014-01-1-0795. A preliminary version of this paper entitled "Redoing the foundations of decision theory" appeared in the *Proceedings of Tenth International Conference on Principles of Knowledge Representation and Reasoning*, 2006.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 1–4, 2013.

negotiate.' In Savage's account [11, sec. 2.3] it is clear that the DM 'constructs the states' in contemplating the decision problem. In fact, his discussion of the rotten egg foreshadows this process. Subsequently, traditional decision theory has come to assume that states are given as part of the description of the decision problem. We suppose instead that states are constructed by the DM in the course of deliberating about questions such as 'How is choice A different from choice B?' and 'In what circumstances will choice A turn out better than choice B?'. These same considerations apply (although here Savage may disagree) to outcomes. This point has been forcefully made by Weibull [16].

There are numerous papers in the literature that raise issues with the state-space approach of Savage or that derive a subjective state space. Machina [10] surveys the standard approach and illustrates many difficulties with the theory and with its uses. These difficulties include the ubiquitous ambiguity over whether the theory is meant to be descriptive or normative, whether states are exogenous or constructed by the DM, whether states are external to the DM, and whether they are measurable or not. Kreps [9] and Dekel, Lipman, and Rustichhini [3] use a menu choice model to deal with unforeseen contingencies—an inability of the DM to list all possible states of the world. They derive a subjective state space that represents possible preference orders over elements of the menu chosen by the DM. Ghirardato [5] takes an alternative approach to unforeseen contingencies and models acts as correspondences from a state space to outcomes. Gilboa and Schmeidler [6] and Karnhi [7] raise objections to the state space that are similar to ours and develop decision theories without a state space. Both papers derive subjective probabilities directly on outcomes. Ahn [1] also develops a theory without a state space; in his theory, the DM chooses over sets of lotteries over consequences. Ahn and Ergin [2] allow for the possibility that there may be different descriptions of a particular event, and use this possibility to capture framing. For them, a 'description' is a partition of the state space. They provide an axiomatic foundation for decision making in this framework, built on Tversky and Koehler's [14] notion of *support theory.*

Our approach differs significantly from these mentioned above. The inspiration for our approach is the observation that objects of choice in an uncertain world have some structure to them. Individuals choose among some simple actions: 'buy 100 shares of IBM' or 'attack Iraq'. But they also perform various tests on the world and make choices contingent upon the outcome of these tests: 'If the stock broker recommends buying IBM, then buy 100 shares of IBM; otherwise buy 100 shares of Google.' These tests are written in a fixed language (which we assume is part of the description of the decision problem, just as Savage assumed that states were part of the description of the decision problem). The language is how the DM describes the world. We formalize this viewpoint by taking the objects of choice to be (syntactic) programs in a programming language.

The programming language is very simple—we use it just to illustrate our ideas. Critically, it includes tests (in the context of **if** ... **then** ... **else** statements). These tests involve syntactic descriptions of the events in the world, and allow us to distinguish events from (syntactic) descriptions of events.

In particular, there can be two different descriptions that, intuitively, describe the same event from the point of view of the modeler but may describe different events from the point of view of the decision maker. Among other things, this enables us to capture framing effects in our framework, without requiring states as Ahn and Ergin [2] do, and provides a way of dealing with resource-bounded reasoners.

In general, we do not include outcomes as part of the description of the decision problem; both states and outcomes are part of the DM's (subjective) representation of the problem. We assume that the DM has a weak preference relation on the objects of choice; we do not require the preference relation to be complete. The set of acts for a decision problem is potentially huge, and may contain acts that will never be considered by the DM. While we believe that empirical validity requires considering partial orders, there are also theoretical reasons for considering partial orders. Our representation theorems for partial orders require a set of probabilities and utility functions (where often one of the sets can be taken to be a singleton). Schmeidler [12, p. 572] observes that using a set of probability distributions can be taken as a measure of a DM's lack of confidence in her likelihood assessments. Similarly, a set of utilities can be interpreted as a lack of confidence in her taste assessments (perhaps because she has not had time to think them through carefully).

In the full paper, we describe the syntactic programs that we take as our objects of choice, discuss several interpretations of the model, and show how syntactic programs can be interpreted as Savage acts. We then provide a number of postulates on preference, and prove a representation theorem (essentially, a sound and complete axiomatization). The key postulate is an analogue of Krantz et al.'s [8] *cancellation axiom*. We also discuss how our framework can model boundedly rational reasoning.

References

1. Ahn, D.: Ambiguity without a state space. Review of Economic Studies (2007) (forthcoming)
2. Ahn, D., Ergin, H.: Framing contingencies (2007) (unpublished manuscript)
3. Dekel, E., Lipman, B., Rustichini, A.: Representing preferences with a unique subjective state space. Econometrica 69, 891–934 (2001)
4. Ellsberg, D.: Risk, Ambiguity and Decision. Garland Publishing, Inc., New York (2001)
5. Ghirardato, P.: Coping with ignorance: unforeseen contingencies and non-additive uncertainty. Economic Theory 17, 247–276 (2001)
6. Gilboa, I., Schmeidler, D.: Subjective distributions. Theory and Decision 56, 345–357 (2004)
7. Karni, E.: Subjective expected utility theory without states of the world. Journal of Mathematical Economics 42, 325–342 (2006)
8. Krantz, D.H., Luce, R.D., Suppes, P., Tversky, A.: Foundations of Measurement, vol 1: Additive and Polynomial Representations. Academic Press, New York (1971)
9. Kreps, D.: Static choice and unforeseen contingencies. In: Dasgupta, P., Gale, D., Hart, O. (eds.) Economic Analysis of Markets and Games: Essays in Honor of Frank Hahn. MIT Press, Cambridge (1992)

10. Machina, M.: States of the world and state of decision theory. In: Meyer, D. (ed.) The Economics of Risk. W. E. Upjohn Institute (2006)
11. Savage, L.J.: Foundations of Statistics. Wiley, New York (1954)
12. Schmeidler, D.: Subjective probability and expected utility without additivity. Econometrica 57, 571–587 (1989)
13. Tversky, A., Kahneman, D.: Advances in prospect theory: cumulative representation of uncertainty. Journal of Risk and Uncertainty 5, 297–323 (1992)
14. Tversky, A., Koehler, D.J.: Support theory: A nonextensional representation of subjective probability. Psychological Review 101(4), 547–567 (1994)
15. Wakker, P., Tversky, A.: An axiomatization of cumulative prospect theory. Journal of Risk and Uncertainty 7(7), 147–176 (1993)
16. Weibull, J.: Testing game theory. In: Huck, S. (ed.) Advances in Understanding Strategic Behavior: Game Theory, Experiments and Bounded Rationality. Essays in Honor of Werner Güth, pp. 85–104. Palgrave MacMillan (2004)

Bisimulation and Coverings for Graphs and Hypergraphs

Martin Otto

Department of Mathematics
Technische Universität Darmstadt

Abstract. We survey notions of bisimulation and of bisimilar coverings both in the world of graph-like structures (Kripke structures, transition systems) and in the world of hypergraph-like general relational structures. The provision of finite analogues for full infinite tree-like unfoldings, in particular, raises interesting combinatorial challenges and is the key to a number of interesting model-theoretic applications.

1 Introduction

Bisimulation provides the fundamental back&forth methodology to capture dynamic notions of behavioural equivalence in terms structural similarity. On one hand, bisimulation stands in the tradition of model-theoretic comparison games and may be viewed as a specialisation and adaptation of the classical Ehrenfeucht–Fraïssé method to a specifically modal context in the analysis of transition systems and graph-like structures, cf. [10]. On the other hand, bisimulation captures the quintessential notion of game equivalence, and can be seen as a general framework for the wider family of back&forth games that pertain to various other types of structures with their specific notions of observable configurations (game positions) and accessibility (transitions/moves) [21]. With respect to such generalisations, a very natural and seemingly basic, yet also very powerful, generalisation step takes us

- from graph-like structures (vertices linked by edges) to hypergraphs (subsets linked by their overlaps/intersections);
- from ordinary bisimulation to hypergraph or guarded bisimulation;
- from modal logics to guarded logics.

This generalisation, and the interesting parallels as well as the combinatorial and model-theoretic challenges it entails are at the heart of this presentation.

Both for graphs and for hypergraphs, bisimulation equivalence supports a natural process of tree unfolding [8,10,12]:

- ordinary tree unfoldings of transition systems or graphs into tree structures of finite edge-labelled paths from a designated root vertex;
- tree-like hypergraph unfoldings of hypergraphs (or relational structures) into acyclic hypergraphs (or relational structures).

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 5–16, 2013.

These unfoldings are linked to the original structures not just by some bisimulation, but they provide bisimilar *coverings*,[1] which project homomorphically to the original structure and allow for lifts of all available links to related loci in the covering structure. In other words, the bisimulation that links the covering to the base structure is induced by the homomorphic projection of the cover: the homomorphism condition guarantees the *forth*-property for the bisimulation relationship, while the *back*-property corresponds to the lifting requirement. The resulting unfoldings are acyclic in the ordinary sense of graph theory (no cycles, not even undirected ones) or of hypergraph theory (α-acyclic, the strongest notion of hypergraph acyclicity).

The mere existence of acyclic bisimilar unfoldings has strong model-theoretic and algorithmic consequences for related logics – in fact for any logic whose semantics is preserved in the process of unfolding. The *tree model property* [8] for modal logics and the *generalised tree model property* [11] of guarded logics account for various decidability and complexity results for modal and guarded logics; they stand behind the applicability of tree automata to their algorithmic model theory; they support model-theoretic characterisations of modal and guarded fragments of first-order and second-order logics; and, even though the unfoldings themselves are typically infinite, they also point us in the right direction for understanding certain approaches to the *finite model property* and the combinatorial challenges posed by the finite model theory of modal and guarded logics [10,19,26,23,11,13].

2 Bisimulations and Coverings

A the combinatorial level, we speak of graphs and hypergraphs. A hypergraph is a structure of the format $\mathcal{A} = (A, S)$ with vertex set A and set of hyperedges $S \subseteq \mathcal{P}(A)$; the case of graphs is the special case in which all hyperedges have cardinality $\leqslant 2$ (so these are undirected, but not necessarily loop-free, graphs). The graphs and hypergraphs of interest arise as combinatorial abstractions of relational structures:

- transition systems or Kripke structures (relational structures of width $\leqslant 2$) as graph-like structures, in which vertices and edges carry labels (edge- and vertex-coloured graphs) and edges may be directed; the graph abstraction is the underlying undirected link pattern between vertices, including loops.
- relational structures $\mathcal{A} = (A, (R^{\mathcal{A}}))$ with relations R of arbitrary, fixed arities; the hypergraph abstraction is the hypergraph of guarded subsets, which has, for each tuple $\mathbf{a} = (a_1, \ldots, a_r) \in R^{\mathcal{A}}$, the set of its components $[\mathbf{a}] := \{a_1, \ldots, a_r\}$ as one of its hyperedges, and in addition, every singleton set. It is often convenient to close the set of hyperedges under downward inclusion.

---

[1] I prefer this classical term to the more idiosyncratic terminology of 'bounded morphisms' in the modal logic tradition [8].

We define bisimulations and coverings for graphs and hypergraphs. They naturally arise in the study of relational structures, in which case the homomorphism needs to respect relational content: colour of vertices and colours and direction of edges in the case of graph-like structures;[2] and the full isomorphism type of the induced substructures on hyperedges in the general case. We leave this to the imagination of the reader and just note that coverings of the underlying graph or hypergraph structures of relational structures can always be lifted to proper coverings of those relational structures in a canonical manner. For graph-like structures one may also wish to disentangle multiple edges (edges between the same vertices that are of different colours). The traditional modal variant of bisimulation equivalence for transition systems of Kripke structures is, moreover, directional; and for this, one would formulate the back&forth requirements, in a setting of directed graph-like structures, as a lifting condition for forward extensions only.

Definition 2.1. [graph covering] A *covering* of a graph $\mathcal{A} = (A, E)$ by a graph $\hat{\mathcal{A}} = (\hat{A}, \hat{E})$ is a homomorphism $\pi \colon \hat{\mathcal{A}} \longrightarrow \mathcal{A}$ such that, for every $\hat{a} \in \hat{A}$ and edge $e = (a, a') \in E$ incident at $a = \pi(\hat{a})$, there is some edge $\hat{e} \in \hat{E}$ with $\pi(\hat{e}) = e$ (we regard $\hat{e}$ as a lifting of e to $\hat{a}$). The covering is *faithful* if it preserves incidence degrees in the sense that there always is a unique lifting of e to $\hat{a}$.

Definition 2.2. [hypergraph covering] A *covering* of a hypergraph $\mathcal{A} = (A, S)$ by a hypergraph $\hat{\mathcal{A}} = (\hat{A}, \hat{S})$ is a map (hypergraph homomorphism) $\pi \colon \hat{\mathcal{A}} \longrightarrow \mathcal{A}$ such that the restrictions $\pi \restriction \hat{s}$ of π to the hyperedges $\hat{s} \in \hat{S}$ are bijections onto hyperedges $\pi(\hat{s}) = s \in S$, and such that, for every $\hat{s} \in \hat{S}$ above $s = \pi(\hat{s})$ and every $s' \in S$, there is some hyperedge $\hat{s}' \in \hat{S}$ with $\pi(\hat{s}') = s'$ and $\pi \restriction (\hat{s} \cap \hat{s}') = s \cap s'$.

Note that the *back*-condition in hypergraph coverings says that the overlap between s and s' can be lifted to any $\hat{s}$ above s.

The following notions of acyclicity are the natural ones; for hypergraphs we concentrate on the strongest of the common notions of acyclicity, also known as α-acyclity [6,5]. The formulation below, in terms of conformality and chordality, is one of several equivalent ones [5]: in particular, it is equivalent to the existence of a tree decomposition whose bags are the hyperedges.

It is convenient to associate with a hypergraph $\mathcal{A} = (A, S)$ an induced graph $G(\mathcal{A})$ on the same vertex set A in which distinct vertices a and a' are linked by an edge if they are elements of the same hyperedge $s \in S$, i.e., $G(\mathcal{A})$ is a superposition of cliques replacing the hyperedges of $\mathcal{A}$.

Definition 2.3. [acyclicity] A graph is *acyclic* if it does not have any cycles; a hypergraph $\mathcal{A} = (A, S)$ is *acyclic* if it is both

(i) *conformal:* each clique in $G(\mathcal{A})$ is contained in a single hyperedge, and
(ii) *chordal:* every cycle in $G(\mathcal{A})$ of length greater than 3 has a chord, i.e., $G(\mathcal{A})$ has no induced subgraphs isomorphic to the k-cycle for $k > 3$.

---

[2] Note that a loop in a transition system is bisimilar to, and may be covered by, a non-trivial cycle or an infinite chain; in this sense, the graph case is not quite the immediate specialisation of the hypergraph case.

Every graph $\mathcal{A} = (A, E)$ possesses natural coverings by acyclic graphs $\mathcal{A}^*_a$, whose nodes are the paths from some designated root vertex a; these coverings can be made faithful by restriction to non-degenerate edge-labelled paths, i.e., to edge-labelled paths that do not reverse onto themselves. It is immediate that all acyclic coverings of a graph that is itself not acyclic must be infinite.

It is not hard to see that, similarly, every hypergraph $\mathcal{A} = (A, S)$ admits coverings by acyclic hypergraphs. Such coverings can be based on acyclic graph unfoldings of the associated intersection graph $I(\mathcal{A}) = (S, \Delta)$ where $\Delta = \{(s, s') \colon s \neq s', s \cap s' \neq \emptyset\}$. Again, acyclic coverings of a hypergraph that is itself not acyclic must be infinite.

We note that non-trivial coverings of hypergraphs can in general not preserve incidence degrees, i.e., they are usually branched coverings and there is no immediate analogy to faithful coverings, which are generally available only for graphs.

2.1 Model-Theoretic Applications

The availability of (maybe necessarily infinite) acyclic unfoldings, implies special model properties for logics whose semantics in invariant under corresponding notions of bisimulation. Many facets of model-theoretic and algorithmic well-behavedness of modal and guarded logics can be attributed more or less directly to their characteristic invariances under bisimulation equivalence. We here concentrate on special model properties and issues of expressive completeness. For background on the logics involved, modal logics (including many variants and extensions of basic modal logic ML, e.g., in the spirit of epistemic or temporal logics) and guarded logics like the guarded fragment of first-order logic GF, we refer the reader to textbook sources and surveys [8,10] and the original papers [2,11,14,12].

Theorem 2.1. *All bisimulation-invariant logics of graph-like structures, and in particular basic modal logic* ML *and the modal* μ*-calculus* L_μ*, have the* tree model property: *every satisfiable formula is satisfiable in a tree-like model.*

All guarded bisimulation-invariant logics of relational structures, and in particular the guarded fragment GF *and its fixpoint extension* μGF*, have the* generalised tree model property: *every satisfiable formula is satisfiable in a model whose hypergraph of guarded subsets is acyclic.*

Suitable tree-like models and their analysis, and the theory of tree automata that can be employed for model checking purposes, account also for characterisation theorems that characterise L_μ and μGF as expressively complete for bisimulation-invariant properties that can be expressed in monadic second-order logic and guarded second-order logic respectively. For the following see the fundamental paper by Janin and Walukiewicz [17] and, for a reduction to [17] that extends the result to the hypergraph setting and guarded logics, [12].

Theorem 2.2. *A monadic second-order definable property of pointed transition systems is expressible in the modal μ-calculus if, and only if, it is invariant under modal bisimulation equivalence.*

A guarded second-order definable property of relational structures is expressible in guarded fixpoint logic if, and only if, it is invariant under guarded bisimulation equivalence.

The classical variants of these characterisations for the bisimulation-invariant fragments of first-order logic can be proved classically, by means of compactness arguments and saturated models. These results are due to van Benthem [28] and Andréka, van Benthem and Németi [2], respectively.

Theorem 2.3. *A first-order definable property of pointed transition systems is expressible in basic modal logic* ML *if, and only if, it is invariant under modal bisimulation equivalence.*

A first-order definable property of relational structures is expressible in the guarded fragment GF *if, and only if, it is invariant under guarded bisimulation equivalence.*

Returning to special model properties, it is interesting that basic modal logic ML, many of its first-order variants (and even the modal μ-calculus, but only as long as only forward modalities are considered), and also the guarded fragment (but not guarded fixpoint logic) have the *finite model property*, see textbook sources [8,10] for ML, and [11] for GF. Finite tree models for formulae of ML can be obtained by pruning from tree-unfoldings of arbitrary models; finite models for formulae of GF can be obtained as natural combinatorial completions (w.r.t. extension properties for partial isomorphisms based on Herwig's Theorem [15]) from truncations of (tree-unfoldings of) arbitrary models according to [11].

3 Acyclicity versus Finiteness

As outlined above, acyclic coverings of finite structures are necessarily infinite if the given finite structure is not itself acyclic – both in the world of graphs and of hypergraphs. However, graphs and hypergraphs admit finite coverings that are acyclic as far as size-bounded induced sub-configurations in the covering structure are concerned.

Definition 3.1. [N-acyclicity] For $N \in \mathbb{N}$, a graph or hypergraph $\mathcal{A}$ is N*-acyclic* if every induced subtructure of $\mathcal{A}$ of size up to N is acyclic.

The (induced) sub-hypergraph $\mathcal{A} \restriction B$ of $\mathcal{A} = (A, S)$, for some $B \subseteq A$, is the hypergraph structure obtained by restricting both the vertex set and each individual hyperedge to B: $\mathcal{A} \restriction B = (B, S \restriction B)$ where $S \restriction B = \{s \cap B \colon s \in S\}$.

A graph is N-acyclic if its *girth* is greater than N. Also note that an N-acyclic graph for $N \geqslant 2\ell + 1$ is ℓ*-locally acyclic* in the sense that the induced subgraph on the ℓ-neighbourhood of any vertex is acyclic. This does not hold for

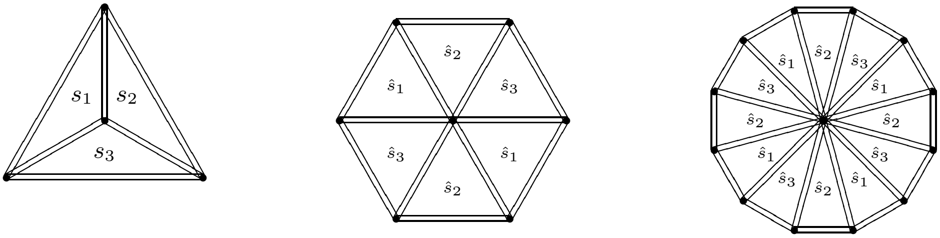


Fig. 1. Local unfoldings of a sub-divided triangle, 2-fold and 4-fold

hypergraphs: consider the hypergraph formed by the subdivision of a triangle with central vertex into the three triangles formed by the central vertex together with one edge each, of the outer triangle; it is clear that any non-trivial covering of this simple hypergraph will have a vertex above the central one whose 1-neighbourhood contains a chordless cycle of some length $3k$ or is infinite.

The discrepancy between locality in the associated graph $G(\mathcal{A})$ and locality in the intersection graph $I(\mathcal{A})$ is a characteristic feature of hypergraphs that account for their much more challenging combinatorics w.r.t. degrees of acyclicity in finite covers.

3.1 Cayley Groups and Finite Graph Coverings

N-acyclic graph covers can easily be obtained as direct products with highly regular, generic N-acyclic graphs that arise as Cayley graphs of suitable groups. Cayely graphs are a well-known source for regular graphs of large girth [1,7].

If G is a finite group generated by the finite set of non-trivial involutive group elements $\{e\colon e \in E\} \subseteq \{g \in G\colon g^2 = 1 \neq g\} \subseteq G$, then the *Cayley graph* of G w.r.t. this generator set E is the undirected loop-free E-edge-coloured graph formed by the group elements with an edge of colour $e \in E$ precisely between all pairs of group elements of the form $(g, g \cdot e)$.

Conversely, let $\mathcal{A} = (A, (R_e)_{e \in E})$ be any finite E-edge-coloured undirected graph in which each R_e is a partial matching. We here call such graphs E-graphs; if we add an e-coloured loop at every vertex not incident with an e-coloured edge, then we obtain a *complete E-graph* with the property that every vertex is incident with precisely one edge (or loop) of colour e, for every $e \in E$.

A finite complete E-graph $\mathcal{A} = (A, (R_e))$ induces a finite Cayley group that arises as a subgroup $\mathrm{sym}(\mathcal{A}) \subseteq \mathrm{Sym}(A)$ of the symmetric group $\mathrm{Sym}(A)$ on the set A. For this, each edge colour $e \in E$ is associated with a generator $e \in \mathrm{sym}(\mathcal{A})$ according to

$$\begin{aligned} e\colon A &\longrightarrow A \\ a &\longmapsto a' \quad \text{ if } (a, a') \in R_e, \end{aligned}$$

which is a non-trivial involution provided $\mathcal{A}$ has at least one e-coloured edge that is not a loop.

It is not hard to see that the girth of the Cayley graph of this group sym($\mathcal{A}$) w.r.t. the generators $e \in E$ is at least $4k+2$ if $\mathcal{A}$ is chosen to be (the completion of) the full E-coloured tree of depth k.

To obtain an N-acyclic finite covering of an arbitrary finite graph $\mathcal{A} = (A, E)$, let G be a Cayley group of girth greater than N with involutive generators $e \in E$ (the edge set of $\mathcal{A}$, where we now think of each undirected edge, or loop, as the *set* of incident vertices, so that $e^{-1} = e$). We obtain a faithful N-acyclic covering by the natural direct product of $\mathcal{A}$ and (the Cayley graph of) G:

$$\begin{aligned} &\mathcal{A} \otimes G := \big(A \times G, E \otimes G\big) \\ &\text{where } \; E \otimes G = \big\{((a,g),(a', g \cdot e)) \colon \{a, a'\} = e \in E\big\}. \end{aligned}$$

This direct product provides a covering with the natural projection onto the first factor as the covering homomorphism. For details of the following we refer the reader to [18,23]. Several specialisations to special classes of graph-like structures are discussed in [9].

Proposition 3.1. *For every $N \in \mathbb{N}$, every finite graph-like structure $\mathcal{A}$ admits faithful coverings by finite N-acyclic structures.*

Cayley groups of much more than just large girth in the above sense are constructed in [23]. An iteration of amalgamation steps that produce more and more highly acyclic E-graphs and passages from these E-graphs $\mathcal{A}$ to induced Cayley groups sym($\mathcal{A}$) produces Cayley groups without *coset cycles* of length up to N (rather than just no generator cycles of length up to N, see Definition 3.2 below).

In a Cayley group with generator set E, and for subsets $\alpha \subseteq E$, we write $G[\alpha] \subseteq G$ for the subgroup generated by $\alpha \subseteq E$, and, for a group element $g \in G$, $gG[\alpha] = \{g \cdot h \colon h \in G[\alpha]\}$ for its coset w.r.t. this subgroup. In terms of the Cayley graph, $gG[\alpha]$ consists of those vertices that are reachable from g on α-coloured paths.

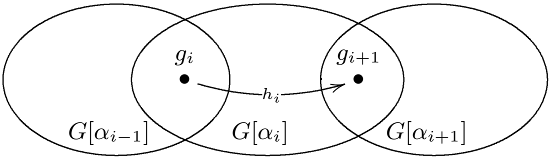


Fig. 2. Coset cycles: local view

Definition 3.2. [coset cycles] Let G be a Cayley group with involutive generators $e \in E$. A *coset cycle* of length n in G consists of a tuple $(g_i)_{i \in \mathbb{Z}_n}$ in G and a tuple of subsets $(\alpha_i)_{i \in \mathbb{Z}_n}$ of E (cyclically indexed in $\mathbb{Z}_n$) such that for all i:
(i) $h_i := g_i^{-1} \cdot g_{i+1} \in G[\alpha_i]$;
(ii) $g_i G[\alpha_i \cap \alpha_{i-1}] \cap g_{i+1} G[\alpha_i \cap \alpha_{i+1}] = \emptyset$.

G is called *N-acyclic* if it does not have any coset cycles of length up to N.

Proposition 3.2. *For every $N \in \mathbb{N}$ and every finite set E there are finite N-acyclic Cayley groups with involutive generator set E.*

For the proof see [23], where such Cayley groups are used as auxiliary ingredients in the construction of N-acyclic hypergraph covers as we shall discuss in the next section.

3.2 Finite Hypergraph Coverings

An intricate iterative construction in [23], which involves finite truncated pieces of just locally finite N-acyclic coverings and their completion through gluing operations that do not create new short cycles, yields the following. In that construction, reduced products with N-acyclic Cayley groups (as discussed further below, see Lemma 3.1) are used as part of the completion steps needed to repair deficiencies along the boundaries where necessary extensions got cut off in the truncation.

Proposition 3.3. *For every $N \in \mathbb{N}$, every finite hypergraph (or relational structure) admits coverings by finite N-acyclic hypergraphs (relational structures whose hypergraph of guarded subsets is N-acyclic).*

The role of the N-acyclic Cayley graphs from Proposition 3.2 in this construction lies in the following preservation property in reduced products – which is quite unlike the role of Cayley groups of large girth towards the construction of N-acyclic graph covers.

Let $\mathcal{A} = (A, S)$ be a hypergraph and $\sigma \colon E \to \mathcal{P}(A)$ a finite family of regions $\sigma(e)$ to be used as glueing sites in A. If G is a Cayley group with involutive generators $e \in E$, we define the *reduced product* of $\mathcal{A}$ with G (over σ) to be the hypergraph $\mathcal{A} \otimes_\sigma G = (\hat{A}, \hat{S})$, as follows.

The vertex set $\hat{A}$ of $\mathcal{A} \otimes_\sigma G$ is obtained from the direct product $A \times G$ by identifications w.r.t. the equivalence relation $\approx$ induced by

$$(a, g) \approx (a', g \cdot e) \quad \text{if} \quad a = a' \in \sigma(e).$$

The set of hyperedges $\hat{S}$ of $\mathcal{A} \otimes_\sigma G$ consists simply of those subsets that are represented by subsets of the form $s \times \{g\}$ in the direct product, for $s \in S$. The natural projection π onto the first factor is well defined and turns $\pi \colon \hat{A} \longrightarrow \mathcal{A}$ into a hypergraph cover. This construction and the following lemma are part of the rather involved route to N-acyclic hypergraph coverings in [23] that support Proposition 3.3.

Lemma 3.1. *If $\mathcal{A} = (A, S)$ is an N-acyclic hypergraph and if the finite set E parametrises glueing sites $\sigma(e) \subseteq A$ that are guarded by hyperedges of $\mathcal{A}$ in the sense that $\sigma(e) \subseteq s$ for some $s \in S$, then the reduced product $\mathcal{A} \otimes_\sigma G$ with any N-acyclic Cayley group G with involutive generator set E is again N-acyclic.*

A much more transparent construction of finite hypergraph coverings, which also achieves feasible size bounds, is obtained in [3], where the following weaker degrees of acyclicity are explored.

Definition 3.3. [weak N-acyclicity] Let $N \in \mathbb{N}$ and consider two hypergraphs $\hat{\mathcal{A}} = (\hat{A}, \hat{S})$ and $\mathcal{A} = (A, S)$ in a hypergraph covering $\pi \colon \hat{\mathcal{A}} \longrightarrow \mathcal{A}$. This covering is *weakly N-acyclic* if every induced sub-hypergraph of $\hat{\mathcal{A}}$ of size up to N can be augmented by extra hyperedges which project onto singletons or subsets of hyperedges of $\mathcal{A}$ so as to become acyclic: for $\hat{A}_0 \subseteq \hat{A}$ with $|\hat{A}_0| \leqslant N$ there is some $\hat{S}' \subseteq \{\hat{s}' \subseteq \hat{A}_0 \colon \pi(\hat{s}') \subseteq s \in S \text{ or } |\pi(\hat{s}')| = 1\}$ such that $(\hat{A}_0, \hat{S} \restriction \hat{A}_0 \cup \hat{S}')$ is acyclic.

The width $w(\mathcal{A})$ of a hypergraph $\mathcal{A} = (A, S)$ is defined to be the maximal size of hyperedges in S. The following core result from [3] was inspired by previous constructions in [25] as well as earlier and cruder approximations in [20]. Essentially, N-acyclic coverings are realised in [3] by finite quotients of suitable term structures that are designed to satisfy exactly the *back*-requirements imposed by the overlap pattern of the desired hypergraph.

Proposition 3.4. *For every $N \in \mathbb{N}$, every finite hypergraph $\mathcal{A}$ admits weakly N-acyclic coverings by finite hypergraphs whose size can be bounded polynomially in $|\mathcal{A}|$ for fixed N and width of $\mathcal{A}$.*

In fact, for fixed width, the construction in [3] also produces coverings by conformal hypergraphs of size polynomial in the given hypergraph, thus improving on a simpler but less succinct construction in [16].

3.3 Model-Theoretic Applications

The following strengthenings of the finite model property for the guarded fragment GF are almost immediate as corollaries to Propositions 3.3 and 3.4, respectively. Details as well as interesting ramifications are presented in [23,3].

In the following, a class of structures defined in terms of finitely many *forbidden finite substructures* is specified by a finite set of finite structures, and consists of all structures in which the specified structures do not occur as induced substructures, up to isomorphism. A class of structures defined in terms of *forbidden homomorphisms* from finitely many finite structures is similarly defined.

Corollary 3.1. GF *has the finite model property in restriction to any class of relational structures that is defined in terms of finitely many forbidden finite cyclic substructures.*

Corollary 3.2. GF *has the finite model property in restriction to any class of relational structures that is defined in terms of forbidden homomorphisms from finitely many finite structures.*

Among the many other consequences of the core construction of weakly N-acyclic coverings in [3] are improved bounds on the sizes of small finite models for sentences of the guarded fragment GF and its generalisation to the clique guarded fragment, and a further application that shows that finite relational structures admit polynomial time canonisation w.r.t. guarded bisimulation equivalence.

The primary model-theoretic goal in [23], on the other hand, is the analogue of the expressive completeness result in Theorem 2.3 for the guarded fragment, in the sense of finite model theory. Just as for basic modal logic ML, the assertion of expressive completeness in restriction to finite model theory does not follow (in any meaningful direct way, that is) from the classical fact, and its proof must follow very different, more constructive lines.

The finite N-acyclic coverings of [23] can be saturated w.r.t. branching behaviour so as to produce finite structures for which guarded bisimulation equivalence to sufficiently high finite depth entails first-order equivalence up to some given quantifier rank. See [23,22] for details and the general context. This yields the following.

Theorem 3.1. *A first-order definable property of finite (!) relational structures is expressible in* GF *if, and only if, it is invariant among finite structures (!) under guarded bisimulation equivalence.*

4 Outlook

Among the latest developments in the directions outlined above are the following.

Restricted back&forth homomorphism equivalences: Back&forth equivalences that combine modal or guarded bisimulation (of graph-like or hypergraph-like relational structures, respectively) with local homomorphisms (of bounded size) under the name of *unary negation bisimulation* [27] and *guarded negation bisimulation* [4], have been investigated as the underlying semantic invariances of yet more expressive well-behaved fragments of first-order logic:

Unary and guarded negation fragments: The *unary negation fragment* UN and *guarded negation fragment* GN of first-order logic are based on unconstrained (or just size-constrained) positive existential quantification and the limitation of negation to formulae that have just a single free variable (unary negation) or an explicitly guarded tuple of free variables (guarded negation). These fragments essentially extend modal logic and the guarded fragment, respectively, and display very similar model-theoretic and algorithmic properties, see [27] and [4]. Technically, the generalisation of good model-theoretic features, and especially of the finite model property, involves reductions to Corollary 3.2 above. An analogue of Theorem 3.1 has recently been outlined in [22].

Improved hypergraph constructions: New, as yet unpublished constructions based on groupoids and their analogue of Cayley graphs allow for far more generic and direct constructions of suitably acyclic hypergraps and hypergraph coverings by means of reduced products [24].

References

1. Alon, N.: Tools from higher algebra. In: Graham, R., Grötschel, M., Lovász (eds.) Handbook of Combinatorics, vol. II, pp. 1749–1783. North-Holland (1995)
2. Andréka, H., van Benthem, J., Németi, I.: Modal languages and bounded fragments of predicate logic. Journal of Philosophical Logic 27, 217–274 (1998)
3. Bárány, V., Gottlob, G., Otto, M.: Querying the guarded fragment. Logical Methods in Computer Science (submitted, 2012)
4. Bárány, V., ten Cate, B., Segoufin, L.: Guarded Negation. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011, Part II. LNCS, vol. 6756, pp. 356–367. Springer, Heidelberg (2011)
5. Beeri, C., Fagin, R., Maier, D., Yannakakis, M.: On the desirability of acyclic database schemes. Journal of the ACM 30, 497–513 (1983)
6. Berge, C.: Graphs and Hypergraphs. North-Holland (1973)
7. Biggs, N.: Cubic graphs with large girth. In: Blum, G., et al. (eds.) Annals of the New York Academy of Sciences, vol. 555, pp. 56–62 (1989)
8. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge University Press (2001)
9. Dawar, A., Otto, M.: Modal characterisation theorems over special classes of frames. Annals of Pure and Applied Logic 161, 1–42 (2009)
10. Goranko, V., Otto, M.: Model theory of modal logic. In: Blackburn, P., van Benthem, J., Wolter, F. (eds.) Handbook of Modal Logic, pp. 249–329. Elsevier (2007)
11. Grädel, E.: On the restraining power of guards. Journal of Symbolic Logic 64, 1719–1742 (1999)
12. Grädel, E., Hirsch, C., Otto, M.: Back and forth between guarded and modal logics. ACM Transactions on Computational Logics 3, 418–463 (2002)
13. Grädel, E., Otto, M.: The freedoms of (guarded) bisimulation (in preparation, 2012)
14. Grädel, E., Walukiewicz, I.: Guarded fixed point logic. In: Proc. LICS 1999, pp. 45–54 (1999)
15. Herwig, B.: Extending partial isomorphisms on finite structures. Combinatorica 15, 365–371 (1995)
16. Hodkinson, I., Otto, M.: Finite conformal hypergraph covers and Gaifman cliques in finite structures. Bulletin of Symbolic Logic 9, 387–405 (2003)
17. Janin, D., Walukiewicz, I.: On the Expressive Completeness of the Propositional μ-Calculus with Respect to Monadic Second-order Logic. In: Sassone, V., Montanari, U. (eds.) CONCUR 1996. LNCS, vol. 1119, pp. 263–277. Springer, Heidelberg (1996)
18. Otto, M.: Modal and guarded characterisation theorems over finite transition systems. Annals of Pure and Applied Logic 130, 173–205 (2004)
19. Otto, M.: Bisimulation invariance and finite models. In: Colloquium Logicum 2002. Lecture Notes in Logic, pp. 276–298. ASL (2006)
20. Otto, M.: Avoiding incidental homomorphisms into guarded covers. Technical report no. 2600, TU Darmstadt (2009)
21. Otto, M.: Model theoretic methods for fragments of FO and special classes of (finite) structures. In: Steinhorn, C., Esparza, J., Michaux, C. (eds.) Finite and Algorithmic Model Theory. LMS Lecture Notes, vol. 379, pp. 271–341. CUP (2011)
22. Otto, M.: Expressive completeness through logically tractable models. Annals of Pure and Applied Logic (under revision, 2012)

23. Otto, M.: Highly acyclic groups, hypergraph covers and the guarded fragment. Journal of the ACM 59(1) (2012)
24. Otto, M.: On groupoids and hypergraphs (unpublished draft, 2012)
25. Rosati, R.: On the decidability and finite controllability of query processing in databases with incomplete information. In: Proc. PODS 2006, pp. 356–365 (2006)
26. Rosen, E.: Modal logic over finite structures. Journal of Logic, Language and Information 6, 427–439 (1997)
27. ten Cate, B., Segoufin, L.: Unary negation. In: Proceedings of STACS, pp. 344–355 (2011)
28. van Benthem, J.: Modal Logic and Classical Logic, Bibliopolis, Napoli (1983)

Forcing Axioms, Finite Conditions and Some More

Mirna Džamonja[⋆]

School of Mathematics, University of East Anglia, Norwich NR4 7TJ,
United Kingdom
`h020@uea.ac.uk`

Abstract. We survey some classical and some recent results in the theory of forcing axioms, aiming to present recent breakthroughs and interest the reader in further developing the theory. The article is written for an audience of logicians and mathematicians not necessarily familiar with set theory.

Keywords: forcing, proper, semiproper, iteration, support.

1 Introduction

We shall work within the axioms of the Zermelo-Fraenkel set theory with Choice (ZFC). These axioms were introduced basically starting from 1908 and improving to a final version in the 1920s as an attempt to axiomatize the foundations of mathematics. There have been other such attempts at about the same time and later, but it is fair to say that for the purposes of much of modern mathematics the axioms of ZFC represent the accepted foundation (see [13] for a detailed discussion of foundational issues in set theory). Gödel's Incompleteness theorems [16] prove that for any consistent theory T which implies the Peano Axioms and whose axioms are presentable as a recursively enumerable set of sentences, so for any reasonable theory one would say, there is a sentence φ in the language of T such that T does not prove or disprove φ. In some sense the discussion of which axioms to use is made less interesting by these theorems, which can be interpreted as saying that a perfect choice of axioms does not exists. We therefore do like the most, we concentrate on the axioms that correctly model most of mathematics, and for the rest, we try to understand the limits and how we can improve them. For us ZFC is a basis for a foundation which in some circumstances can be extended to a larger set of axioms which provide an insight into various parts of mathematics. In here we concentrate on the forcing axioms (and their negations).

2 The Discovery of Forcing

The proof of Gödels' Incompleteness theorems is not constructive and in particular it does not construct an independent sentence φ, it only proves its existence.

[⋆] Mirna Džamonja thanks EPSRC for support through their grant number EP/I00498.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 17–26, 2013.

It is therefore quite amazing that for the theory of ZFC such a sentence φ turned out to be the following simple statement formulated by Cantor as early as 1878 [8] (as an implicite conjecture only at that point):

Continuum Hypothesis (CH): For every infinite subset A of the reals $\mathbb{R}$, either there is a bijection between A and $\mathbb{R}$ or there is a bijection between A and $\mathbb{N}$.

This statement tormented Cantor, who could not prove it or disprove it. With a good reason, since it was finally proved by Cohen in [9] that if ZFC is consistent then so is ZFC with the negation of CH. Since Gödel [17] had proved that if ZFC is consistent then so is ZFC along with CH, it follows that CH is independent of ZFC. To obtain his proof Cohen introduced the technique of forcing. It is a technique to extend a universe $\mathbf{V}$ of set theory to another one, $\mathbf{V}[G]$, so that $\mathbf{V}[G]$:

- has the same ordinals
- (most often) has the same cardinals and
- satisfies a desired formula ϕ.

One way to think of this technique is to imagine that we are actually working within some large ambient model of ZFC and seeing only a small submodel which we call $\mathbf{V}$. This submodel may even be assumed to be countable. Being so small, $\mathbf{V}$ has a rather particular opinion of the reality, for example it esteems that every infinite cardinal $\aleph_\alpha$ is some ordinal $\beta(\aleph_\alpha)$ among the ordinals β that actually belong to $\mathbf{V}$ (we denote this by $\aleph_\alpha^{\mathbf{V}}$). For Cohen's proof we may also assume that $\mathbf{V}$ satisfies CH- since if it does not we have already violated CH. What we aim to do is to extend $\mathbf{V}$ to a larger model which will contain $\aleph_2^{\mathbf{V}}$ many reals from our ambient universe, while $\mathbf{V}[G]$ and $\mathbf{V}$ will actually agree on their opinion of what is $\aleph_1$ and $\aleph_2$ (they will have the same cardinals). Then in $\mathbf{V}[G]$ we can choose any set A of only $\aleph_1^{\mathbf{V}}$ reals to demonstrate that A is not bijective with either $\mathbb{N}$ or $\mathbb{R}$, hence CH fails. This construction rests upon a combinatorial method which adds these new reals while preserving the cardinals. We may imagine this as a sort of inductive construction, but one in which the desired object is not added using a linearly ordered set of approximations but rather a partially ordered set. For example, thinking of a real as a function from ω to 2 (as there is a bijection between $\mathbb{R}$ and $\mathcal{P}(\omega)$), we may add a real by considering the partial order of finite partial functions from ω to 2 in their increasing order, some coherent subset of which will be glued together to give us a total function from ω to 2. The coherent subset is our G, the generic filter. The fact that such a subset can be chosen is one of the main ingredients of the method. The actual proof of the negation of CH requires us to work with functions from $\omega_2 \times \omega$ to 2, but the idea is the same.

Partial orders considered in the theory of forcing have the property of having the smallest element and are often called *forcing notions*. Elements of a forcing notion are usually called *conditions*. As we are looking for coherent subsets of a forcing notion, an important point is to consider for given two conditions if they are coherent, which means that they have a common extension. We say that conditions having such an extension are *compatible*, otherwise they are *incompatible*. A set of conditions is called *an antichain* if it consists of pairwise incompatible conditions.[1] The moral opposite of an antichain is a *filter*, which is a set in which every two conditions are compatible, moreover with a common extension in the filter itself. We also assume that filters are closed under weakenings of the conditions within the filter. The generic then is a very special kind of filter.

We digress to say that many authors consider forcing notions as partial orders which have the largest element and in which smaller elements give more information than the larger ones. The intuition may be that at the beginning we have a misty view of what our generic object is going to be, and that with every stronger condition we clear the myst and restrict the vision to a smaller relevant part, leading in the end to a single object which is the generic. The former approach was used by Cohen who discovered forcing, the latter was used by Solovay who quickly took over from Cohen to become a leading figure of set theory for many years. The two approaches are obviously equivalent, here we shall use the former one.

Cohen's discovery led to a large number of independence results, leading to many mathematical and philosophical developments. We shall concentrate on the mathematical ones. In particular we shall discuss the notion of a forcing axiom and the related concept of iterations of forcing. We shall often discuss the situation of relative consistency of a statement φ, that is to say the situation that if ZFC is consistent then so is the conjunction of ZFC and our statement φ. We shorten this description by saying "φ is consistent", and leave it to the reader to remember that this in fact only relates to relative consistency.

3 Iterated Forcing and Martin's Axiom

We have described in §2 that CH is independent of ZFC, but it turns out that so are various other statements coming from a large number of fields of mathematics. For example, the statement that every ccc[2] Boolean algebra of size less than the continuum supports a measure and that CH fails, is consistent with ZFC. Call this statement $\mathcal{BA}$. To prove this we need more than just a single step forcing extension described in the introduction and used for the failure of CH. The reader may imagine trying to prove this statement by going through some list of "small" ccc Boolean algebras and generically adding a measure to each of them. So we need to iterate the method described in the introduction. Only, this is not completely trivial as it can be shown that if we proceed naively, taking one generic after another and unions at the limit, already after ω many steps we shall no longer have a model of ZFC. Another issue which is more subtle is that even if we manage to preserve ZFC, it is easy to destroy the cardinals, in the sense that our final model will have learned that what $\mathbf{V}$ in its restricted opinion had considered to be cardinals, in fact are just bare small ordinals. For example, it might have learned that the ω_1 of $\mathbf{V}$ is countable, so the final theorem will not

---

[1] Note that the notion of an antichain here differs from that one in the theory of order, where the conditions in an antichain are simply required to be pairwise incomparable.

[2] This means that every family of pairwise disjoint elements in the algebra is countable.

be about ω_1. A forcing which does not put us in this situation is said to *preserve cardinals*. An example of such a forcing is the so called *ccc* forcing, where the word ccc is used to denote the fact that every antichain is countable.

The way out of these difficulties is the iterated forcing. We shall not describe it in detail, but we may imagine it as a huge forcing notion consisting of sequences of elements where each coordinate corresponds to a name for an element of a forcing notion, not in $\mathbf{V}$ but in some extension of it intermediate between $\mathbf{V}$ and $\mathbf{V}[G]$. Every sequence in this object has a set of nontrivial coordinates, which is to say places in where it is not equal to the trivial smallest element of the corresponding forcing notion. This set is called the *support* of a condition. A major advance in the theory was the following theorem:

Theorem 3.1 *(Martin and Solovay) An iteration with finite supports of ccc forcing is ccc.*

The history of this theorem is that Solovay and Tennebaum in [31] proved the consistency of the Souslin Hypothesis (i.e. there are no Souslin lines, meaning that the reals are characterised by being a complete order dense set with no first or last element in which every family of pairwise disjoint sets is countable) using the technique of iterating a certain forcing. Their original result was an iteration of the specific forcing destroying Souslin lines. However, Martin realised that their technique could be extended to prove Theorem 3.1 and introduced the Martin's Axiom (see below), which appears in Section 6 of [31] and the paper [22] by Martin and Solovay. The point is that iterated forcing is quite a complex technique and there is no reason to expect that a mathematician not working in set theory but interested in the possible independence of some concrete statement in mathematics should be learning the technique of iterated forcing, or of course that a set theorist will be able to work in any given part of mathematics to answer the question- although many examples of both the former and the latter are known in the literature. However, this is exactly where the forcing axioms come in, and the first one was discovered thanks to Theorem 3.1. It is *Martin's Axiom*:

Martin's Axiom (MA): For every ccc forcing notion $\mathbb{P}$ and every family $\mathcal{F}$ of $< \mathfrak{c}$ many dense sets in $\mathbb{P}$, there is a filter in $\mathbb{P}$ which intersects all elements of $\mathcal{F}$.

A *dense set* in a forcing notion is a subset such that every condition in the forcing notion has an extension in the dense set. Intersecting dense sets is what corresponds to genericity, because in fact the definition of a *generic* filter (over $\mathbf{V}$) is that it intersects every dense set which is in $\mathbf{V}$. Martin's Axiom actually follows from CH, as can be proved by induction, but the point is that it is also consistent with the negation of CH, in fact with CH being as large as we wish. This has had far reaching consequences. The point is that formulating this axiom separates the two parts of the technique of forcing: the logical one and the combinatorial one, to the extent that the "end user" of this axiom does not need to know anything about logic, it suffices to concentrate on the combinatorics involved. This in fact is often not too difficult and a careful reader of this article could easily now go away and prove for himself the consistency of the statement $\mathcal{BA}$ above, simply using MA + ¬ CH. This is why MA has had a large success in the mathematical community and a large number of independence results were obtained using it. Many of these developments are documented in Fremlin's book [19], and new developments come up regularly.

4 Beyond ccc

Many nice forcing notions are not ccc. An example is *Sacks forcing* which adds a real of a minimal Turing degree [27]. In fact, some very natural statements in mathematics are known to be independent of set theory but it is also known that these independence results cannot be shown using MA. An example is the following: say that a subset A of the reals is $\aleph_1$-dense if for every $a < b$ in A there are $\aleph_1$-many reals in the intersection $A \cap (a, b)$. Baumgartner proved in [4] that it is consistent that every two such sets are order isomorphic and CH fails. Yet, Abraham and Shelah [3] proved that this statement does not follow from MA+¬ CH. Baumgartner's proof uses PFA, the proper forcing axiom. Properness is a more general notion than that of ccc and is expressed in a less combinatorial way. It was invented by Shelah in the 1980s (see [30] for the majority of references relating to proper forcing in this section), in a response to a growing need of the set theorists to have an iterable notion of forcing which preserves cardinals (or at least $\aleph_1$) and is not necessarily ccc.

The history of this development is that Laver showed in [21] the consistency of the Borel conjecture, which postulated that all sets of reals which have strong measure zero are countable. Laver showed that this is the case in a model obtained by adding $\aleph_2$ many Laver reals to a model of GCH, using countable supports in the iteration. It is exactly this notion of a countable support that is used in the proper forcing axiom. Namely,

Theorem 4.1 *(Shelah) An iteration with countable supports of proper forcing is proper.*

Shelah also showed that Theorem 4.1 is not true when countable supports are replaced by the finite ones. It should be noted that Laver's forcing also inspired the notion of Property A, introduced by Baumgartner [5], which is a notion implied by ccc and implying properness, and which is iterable using countable support. Proper forcing is a more general notion and hence more useful. Shelah's iteration theorem is a step in Baumgartner's proof [5] that from the assumption of the consistency of the existence of one supercompact cardinal, one can prove the consistency of a forcing axiom he formulated, the proper forcing axiom PFA. PFA is the statement

Proper Forcing Axiom (PFA): For every proper forcing notion $\mathbb{P}$ and every family $\mathcal{F}$ of $\aleph_1$ many dense sets in $\mathbb{P}$, there is a filter in $\mathbb{P}$ which intersects all elements of $\mathcal{F}$.

A careful reader may wonder why in the formulation of Martin's Axiom we have the possibility to use $< \mathfrak{c}$ many dense sets and in the PFA we can only use $\aleph_1$

many. In fact, the two boil down to same, since Veličković and Todorčević proved in [34] and [7] that PFA implies $\mathfrak{c} = \aleph_2$. Proper forcing has many applications, in the set theory of the reals, combinatorial properties of ω_1 and topology, algebra and analysis. Many of these developments can be found in Shelah's monumental book mentioned above [30] and Baumgartner's article [6]. Let us give a definition of properness for those readers who would like to see the details. It is a somewhat complicated definition, involving the use of elementary models - which exactly was behind the revolution that it has created, as it was a totally new way of looking at forcing.

Let χ be a regular cardinal, which means that $\mathcal{H}(\chi)$[3] models all the (finitely) many instances of the axioms of set theory that will be used in our argument and that it contains all objects we need[4].

Definition 4.2 *Let* $\mathbb{P}$ *be a forcing notion and suppose that* N *is a countable elementary submodel of* $\mathcal{H}(\chi)$ *such that* $\mathbb{P} \in N$. *We say that* $q \in \mathbb{P}$ *is an* $(N, \mathbb{P})$-generic *condition if for every dense subset* $\mathcal{D}$ *of* $\mathbb{P}$ *with* $\mathcal{D} \in N$, *we have that* $\mathcal{D} \cap N$ *is dense above* q.

$\mathbb{P}$ *is said to be* proper *if for every* N *and* p *as above with* $p \in N$, *there is* $q \geq p$ *which is* $(N, \mathbb{P})$*-generic.*

The interested reader should plan to spend a few happy hours reading either [30] or [5], where excellent introductions are given. Good questions to test the understanding of the topic is to prove that every ccc forcing is proper and that proper forcing preserves ω_1.

5 Away from Properness

Proper forcing preserves ω_1 and the stationary subsets of it, but it is not the only forcing with these preservation properties. For example, the Prikry forcing changing the cofinality of a measurable cardinal to ω preserves stationary subsets of ω_1 and is not proper. Shelah (see [30]) defined a larger class of forcing, the semiproper forcing, which does preserve ω_1 and includes the class of proper forcing and the Prikry forcing. Then one can formulate the semiproper forcing axiom SPFA in a similar way as PFA and prove it consistent from a supercompact cardinal using a proof simillar to that of Baumgartner for PFA. With one major difference: the iteration has to be done with the so called *revised countable*

---

[3] This is the set of all sets whose transitive closure under $\in$ has size $< \chi$.

[4] The reader should recall that there are infinitely many axioms of set theory, as the Axiom of Replacement and the Axiom of Comprehension are actually infinite axioms schemes, giving one axiom for each formula of set theory. Any given argument will only use finitely many axioms and for any such finite portion ZFC* of ZFC there is a χ such that $\mathcal{H}(\chi)$ models ZFC*. The way to think of the argument to come is similar to the choice of ϵ in the continuity arguments in analysis: we know the argument works independently of the choice of ϵ, or χ in our case, and we know that the ϵ could have been chosen so that it works for the situation in question- hence the proof follows.

support. This is quite an involved concept, going way beyond the scope of this article. Foreman, Magidor and Shelah studied in [12] a similar forcing axiom, where the entries are all forcings that preserve stationary subsets of ω_1, so it is called the Martin Maximum. In fact, it turns out that SPFA and MM are the same axiom, as was proved by Shelah in [29].

The word Maximum in some sense also indicates the outlook of the subject after the invention of MM. Clearly, stronger axioms than MM could not be invented, or at least not in an obvious way, and hence research concentrated for some years on studying the weakenings of these axioms, especially weakenings of PFA. Some of the popular choices are OCA, the open colouring axiom (it has two versions, introduced respectively by Abraham, Rubin and Shelah in [1] and Todorčević in [33]), BPFA, which is the bounded PFA, introduced by Goldstern and Shelah in [18], MPR introduced by Moore in [24] and, of particular interest, PID, the P-ideal dichotomy which has the surprising feature to be consistent with the continuum hypothesis, as shown by Abraham and Todorčević in [2]. The interest of these axioms is exactly in their relative weakness, as they allow us to get the relative consistency of statements that are seemingly contradictory, such as CH and certain consequences of PID.

Another direction suggesting itself here are the forcing axioms on cardinals above ω_1. Generalised Martin Axioms were developed by Baumgartner in [5] and Shelah in [28] and their basic form is that they apply to κ^+ for some cardinal κ satisfying $\kappa = \kappa^{<\kappa}$ and to forcing satisfying some strong version of the κ^+-chain condiion (the ordinary version won't do), being $(< \kappa)$-closed[5] or some similar condition, and some condition like well-metness: every two compatible conditions have the least upper bound. The version of the κ^+-chain condition appearing in Shelah's work is called stationary κ^+-cc. The consistency of these axioms is proved by a proof similar to that of the consistency of Martin's Axiom, but using supports of size $(< \kappa)$. The situation with the generalisation of proper focing is much more complicated, and in spite of a series of papers by Rosłanowski and Shelah (see e.g. [26]) where partial solutions are found, it is fair to say that the right geneeralisation does not exist for the moment. Exciting new work by Neeman seems to be able to obtain exactly that, as we discuss in the next section.

Before leaving this section let us also discuss forcing axioms at another kind of cardinals, the successor of a singular cardinal. Work by Džamonja and Shelah in [11] gives, modulo a supercompact cardinal, the consistency of a forcing axiom at a supercompact cardinal that will be made to have cofinality ω by a certain Prikry extension. The axiom has a different form than the ones that we have seen so far, as it applies in the universe before we do the Prikry extension, rather than the final universe. It states that 2^κ is large (can be made as large as we like it), there is a normal measure $\mathcal{D}$ on κ which is obtained as an increasing union of κ^{++} filters (which allows for a very nice prediction of $\Pr(\mathcal{D})$ names for objects on κ^+) and that the Generalised Martin's Axiom holds for κ^+-stationary chain condition $(< \kappa)$-directed closed (every directed system of $< \kappa$ many conditions has a

---

[5] This means that every increasing sequence of length $< \kappa$ in the forcing has a common upper bound.

common upper bound) well-met forcing notions. Using this axiom Džamonja and Shelah obtained the consistency (modulo a supercompact cardinal) of the existence of a family of κ^{++} graphs on κ^+ for κ singular strong limit of cofinality ω, together with 2^κ being as large as we wish. Work in progress by Cummings, Džamonja, Magidor, Morgan and Shelah promises to extend this to cofinalities larger than ω as well as to $\aleph_\omega$.

6 Iterating Properness with Finite Supports- It Is Possible after All

As mentioned above, it is well known that one cannot iterate proper forcing axiom with finite supports and guarantee that the properness is preserved. Yet a recent result of Neeman in [25] shows that in some sense we can do exactly this, as he gave an alternative proof of the consistency of PFA using conditions which have finite support. Assuming some bookekepping function f coming from the Laver diamond and giving the list of all proper focings (this is the standard part of any known proof of the consistency of PFA), Neeman introduced the forcing which consists of pairs $(\mathcal{M}_p, w_p)$ where $\mathcal{M}_p$ is a finite $\in -$*increasing* sequence of elementary submodels of $\mathcal{H}(\chi)$, each either countable or of the form $\mathcal{H}(\alpha)$ for some $\alpha < \chi$, and the sequence is closed under intersections. The working part w_p is also finite and it has a support of finitely many α satisfying that at any nontrivial stage α the coordinate $w_p(\alpha)$ is forced by $\mathbb{P}_\alpha$ to be $(M_{G_\alpha}, \underset{\sim}{Q}_\alpha)$-generic for all $M \in \mathcal{M}_p$ such that $\mathbb{P}_\alpha \in M$.

Neeman's work is very revolutionary but it also builds up on some earlier developments, such as the papers by Friedman [14] and Mitchell [23] in which these authors independently obtained forcing notions to force a club to ω_2 using finite conditions and certain systems of models. This idea was also used in [10] to add a square to ω_2 , while the idea of using elementary submodels as side conditions goes back to Todorčević ([32]), with the difference that there only countable models were used. Koszmider [20] used models organised along a morass to obtain the consistency of the existence of a chain of length ω_2 in $\mathcal{P}(\omega_1)/\text{fin}$. A major ingredient in Neeman's work is also the notion of strong properness, which was used by Mitchell in [23]. Applications of Neeman's method in giving elegant proofs of several known difficult consistency results can be found in the paper [35] by Veličković and Venturi. Very new developements inspired by Neeman's work include a proof by Gitik and Magidor [15] that SPFA can be obtained by a sort of "revised finite support", and Neeman's yet unwritten work which shows how a generelisation of his method can be used to obtain a workable larger cardinal analogue of PFA.

7 Challenges

Some of the main directions of present research are indicated in the above: generalising PFA to larger cardinals and forcing axioms at the successor of a singular cardinal. There are many open questions that arise. Another direction on which we have not commented on too much and which forms a major line of research is the search for a forcing axiom on ω_1 which would be consistent with CH and give some concrete combinatorial statements, such as "measuring". Note that almost all the forcing we discussed in the context of ω_1 adds reals (which is why it is so interesting that PID is consistent with CH). There is a large theory behind this and the interested reader may start with [30], especially Chapter V.

Challenges in this field also come from applications to other fields, and without having more space to spend on the numerous applicatons of the axioms we have so far, we can just mention that applications have been found in fields as varied as the theory of Boolean algebras, topology, algebra, Banach space theory, measure theory and C*-algebras.

References

[1] Abraham, U., Rubin, M., Shelah, S.: On the consistency of some partition theorems for continuous colorings, and the structure of $\aleph_1$-dense ordered sets. Ann. Pure and Applied Logic 29(2), 123–206 (1985)

[2] Abraham, U., Todorčević, S.: Partition properties of ω_1 compatible with CH. Fund. Math. 152, 165–181 (1997)

[3] Avraham, U., Shelah, S.: Martin's Axiom does not imply that every two $\aleph_1$-dense sets of reals are isomorphic. Israel J. Math. 38(1-2), 161–176 (1981)

[4] Baumgartner, J.E.: All $\aleph_1$-dense sets of reals can be isomorphic. Fund. Math. 79(2), 101–106 (1973)

[5] Baumgartner, J.E.: Iterated forcing. In: Mathias, A.R.D. (ed.) Surveys in Set Theory. London Math. Soc. Lecture Note Ser., vol. 87, pp. 1–59. Cambridge Univ. Press, Cambridge (1983)

[6] Baumgartner, J.E.: Applications of the proper forcing axiom. In: Kunen, K., Vaughan, J.E. (eds.) Handbook of Set-theoretic Topology, pp. 913–959. North-Holland, Amsterdam (1984)

[7] Bekkali, M.: Topics in Set Theory. Springer, Heidelberg (1991)

[8] Cantor, G.: Ein Beitrag zur Mannigfaltigkeitslehre. Journal für die reine und angewandte Mathematik 187, 242–258 (1878)

[9] Cohen, P.: The independence of the continuum hypothesis. Proc. Nat. Acad. Sci. USA 50(6), 1143–1148 (1963)

[10] Dolinar, G., Džamonja, M.: Forcing Square$_{\omega_1}$ with finite conditions. Ann. of Pure and Appl. Logic 164, 49–64 (2013)

[11] Džamonja, M., Shelah, S.: Universal graphs at the successor of a singular cardinal. J. Symbol. Logic 68, 366–387 (2003)

[12] Foreman, M., Magidor, M., Shelah, S.: Martin's Maximum, saturated ideals, and nonregular ultrafilters. I. Ann. of Math. (2) 127(1), 1–47 (1988)

[13] Fraenkel, A.A., Bar-Hillel, Y., Lévy, A.: Foundations of Set Theory, 2nd revised edn. North-Holland, Amsterdam (1973)

[14] Friedman, S.D.: Forcing with finite conditions. In: Bagaria, J., Todorčević, S. (eds.) Set Theory: Centre de Recerca Matemàtica, Barcelona 2003–04. Trends in Mathematics, pp. 285–296. Birkhäuser Verlag, Basel (2006)

[15] Gitik, M., Magidor, M.: SPFA by finite conditions (preprint, 2012)

[16] Gödel, K.: Über formal unentscheidbare Säztze der Principia Mathematica und verwandter Systeme, I. Monatshefte für Mathematik und Physik 38, 173–198 (1931)

[17] Gödel, K.: The consistency of the axiom of choice and of the generalized continuum hypothesis. Proc. Nat. Acad. Sci. 24, 556–557 (1938)

[18] Goldstern, M., Shelah, S.: The bounded proper forcing axiom. J. Symbol. Logic 60, 50–73 (1995)

[19] Fremlin, D.H.: Consequences of Martin's Axiom. Cambridge tracts in Mathematics. Cambridge University Press, Cambridge (1984)

[20] Koszmider, P.: On the existence of strong chains in $\mathcal{P}(\omega_1)/\mathrm{Fin}$. J. Symbol. Logic 63(3), 1055–1062 (1998)

[21] Laver, R.: On the consistency of Borel's conjecture. Acta Math. 137, 151–169 (1976)

[22] Martin, D., Solovay, R.M.: Internal Cohen extensions. Ann. Math. Logic 2, 143–178 (1970)

[23] Mitchell, W.J.: Adding closed unbounded subsets of ω_2 with finite forcing. Notre Dame J. Formal Logic 46(3), 357–371 (2005)

[24] Moore, J.T.: Set mapping reflection. J. Math. Logic 5, 87–97 (2005)

[25] Neeman, I.: Forcing with sequences of models of two types (2011) (preprint), `http://www.math.ucla.edu/~ineeman`

[26] Rosłanowski, A., Shelah, S.: Iteration of λ-complete forcing notions not collapsing λ^+. Int. J. Math. Math. Sci. 28, 63–82 (2001)

[27] Sacks, G.E.: Forcing with perfect closed sets. In: Scott, D. (ed.) Axiomatic Set Theory. Symposia in Pure Mathematics, vol. 13, pp. 331–355. American Mathematical Society, Providence (1971)

[28] Shelah, S.: A weak generalization of MA to higher cardinals. Israel J. Math. 30(4), 297–306 (1978)

[29] Shelah, S.: Semiproper forcing axiom implies Martin Maximum but not PFA^+. J. Symbol. Logic 52(2), 360–367 (1987)

[30] Shelah, S.: Proper and improper forcing, 2nd edn. Perspectives in Mathematical Logic. Springer, Berlin (1998)

[31] Solovay, R.M., Tennenbaum, S.: Iterated Cohen extensions and Souslin's problem. Ann. of Math. 94(2), 201–245 (1971)

[32] Todorčević, S.: A note on the proper forcing axiom. In: Axiomatic Set Theory (Boulder, Colorado 1983). Contemporary Mathematics, vol. 31, pp. 209–218. Amer. Math. Soc., Providence (1984)

[33] Todorčević, S.: Partition problems in topology. American Mathematical Society, Rhode (1989)

[34] Veličković, B.: Forcing axioms and stationary sets. Adv. Math. 94(2), 256–284 (1992)

[35] Veličković, B., Venturi, G.: Proper forcing remastered (2011) (preprint), `http://arxiv.org/pdf/1110.0610.pdf`

A Note on Axiomatisations of Two-Dimensional Modal Logics

Agi Kurucz

Department of Informatics
King's College London
agi.kurucz@kcl.ac.uk

Abstract. We analyse the role of the modal axiom corresponding to the first-order formula "$\exists y\,(x = y)$" in axiomatisations of two-dimensional propositional modal logics.

One of the several possible connections between propositional multi-modal logics and classical first-order logic is to consider finite variable fragments of the latter as 'multi-dimensional' modal formalisms: First-order variable-assignment tuples are regarded as possible worlds in Kripke frames, and each first-order quantification $\exists v_i$ and $\forall v_i$ as 'coordinate-wise' modal operators $\Diamond_i$ and $\Box_i$ in these frames. This view is implicit in the algebraisation of finite variable fragments using finite dimensional cylindric algebras [6], and is made explicit in [15,12].

Here we look at axiomatisation questions for the two-dimensional case from this modal perspective. (For basic notions in modal logic and its Kripke semantics, consult e.g. [2,3].) We consider the propositional multi-modal language $\mathcal{ML}_2^\delta$ having the usual Boolean operators, unary modalities $\Diamond_0$ and $\Diamond_1$ (and their duals $\Box_0$, $\Box_1$), and a constant δ:

$$\mathcal{ML}_2^\delta: \qquad p \mid \neg\varphi \mid \varphi \vee \psi \mid \Diamond_0\varphi \mid \Diamond_1\varphi \mid \delta$$

Formulas of this language can be embedded into the two-variable fragment of first-order logic by mapping propositional variables to binary atoms $P(v_0, v_1)$ (with this fixed order of the two available variables), diamonds $\Diamond_i$ to quantification $\exists v_i$, and the 'diagonal' constant δ to the equality atom $v_0 = v_1$. Semantically, we look at first-order models as multimodal Kripke frames (fitting to the above language) of the form

$$\begin{array}{lll} \langle U \times U, \equiv_0, \equiv_1, Id\rangle, & & \text{where, for all } u_0, u_1, v_0, v_1 \in U, \\ \langle u_0, u_1\rangle \equiv_0 \langle v_0, v_1\rangle & \text{iff} & u_1 = v_1, \\ \langle u_0, u_1\rangle \equiv_1 \langle v_0, v_1\rangle & \text{iff} & u_0 = v_0, \text{ and} \\ Id = \{\langle u, u\rangle : u \in U\}. & & \end{array}$$

We call frames of this kind *square frames.* The above embedding is validity-preserving in the sense that a modal $\mathcal{ML}_2^\delta$-formula φ is valid in all square frames iff its translation $\varphi^\dagger$ is a first-order validity.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 27–33, 2013.

In the algebraic setting, the modal logic of square-frames corresponds to the equational theory of the variety RCA_2 of *2-dimensional representable cylindric algebras*. The equational theory of RCA_2 is well-known to be finitely axiomatisable [6]. By turning this equational axiomatisation to modal $\mathcal{ML}_2^\delta$-formulas, we obtain a finite axiomatisation of the modal logic of square frames [15]. In order to 'deconstruct' this axiomatisation and to try to analyse which axiom is responsible for which properties of the modal logic of square frames, below we list these axioms divided into two groups:

(i) Unimodal properties describing individual modal operators, for $i = 0, 1$:

$$\Box_i p \to p \qquad \Box_i p \to \Box_i \Box_i p \qquad \Diamond_i p \to \Box_i \Diamond_i p \tag{1}$$

These are the (Sahlqvist) axioms of the well-known modal logic **S5**, saying that each $\equiv_i$ is an equivalence relation.

(ii) Multimodal, 'dimension-connecting' properties, describing the interactions between the two diamonds, and between the diamonds and the diagonal constant:

$$\Diamond_0 \Diamond_1 p \leftrightarrow \Diamond_1 \Diamond_0 p \tag{2}$$

$$\Diamond_0 \delta \wedge \Diamond_1 \delta \tag{3}$$

$$\big(\Diamond_0(\delta \wedge p) \to \Box_0(\delta \to p)\big) \ \wedge \ \big(\Diamond_1(\delta \wedge p) \to \Box_1(\delta \to p)\big) \tag{4}$$

$$\delta \wedge \Diamond_0(\neg p \wedge \Diamond_1 p) \to \Diamond_1(\neg\delta \wedge \Diamond_0 p) \tag{5}$$

$$\delta \wedge \Diamond_1(\neg p \wedge \Diamond_0 p) \to \Diamond_0(\neg\delta \wedge \Diamond_1 p) \tag{6}$$

These axioms are also Sahlqvist formulas, with easily computable first-order correspondents: Axiom (2) says that $\equiv_0$ and $\equiv_1$ commute, (3) says that at each 'horizontal' and 'vertical' coordinate, there is at least one 'diagonal' point, while (4) says that there is at most one such. Finally, (5) is a kind of generalisation of (2) when we start from a 'diagonal' point: It says that if we start with a $\equiv_0$-step, then move on to a different point by a $\equiv_1$-step, then we can always complete the same journey by taking first a $\equiv_1$-step to a 'non-diagonal' point, followed by a $\equiv_0$-step. (And (6) says the same about starting with a $\equiv_1$-step, and then taking a $\equiv_0$ one.) Note that the axiomatisation given in [6] contains slightly complicated forms of (5) and (6). As it is shown by Venema [15], on the basis of (1), (2) and (4), the 'Henkin-axioms' are equivalent to (5) and (6).

One of the motivations in the study of so-called two-dimensional modal logics is to understand how much influence each of the (i)- and (ii)-like properties has on the resulting logics. Below we consider Kripke structures where

- the set of possible worlds is still a full Cartesian product of two sets, and the relations between the pairs of points still 'act coordinate-wise' (so at least (2), but possibly further properties in (ii) still hold),
- the accessibility relations between the pairs of points are not necessarily equivalence relations (so (i) might not hold).

Note that this direction is kind of orthogonal to the one taken by relativised cylindric algebras [6,7] and guarded fragments of first-order logic [1], where (i) is kept unchanged, while generalisations of (ii) are considered.

Let us introduce a 'product-like' construction on Kripke frames. This and similar constructions were first considered by Segerberg [13] and Shehtman [14], see also [4,9,8]. Given unimodal Kripke frames $\mathfrak{F}_0 = \langle U_0, R_0\rangle$ and $\mathfrak{F}_1 = \langle U_1, R_1\rangle$, their *δ-product* is the multimodal frame

$$\mathfrak{F}_0 \times^{\delta} \mathfrak{F}_1 = \langle U_0 \times U_1, \bar{R}_0, \bar{R}_1, Id\rangle,$$

where $U_0 \times U_1$ is the Cartesian product of sets U_0 and U_1, the binary relations $\bar{R}_0$ and $\bar{R}_1$ are defined by taking,

$$\begin{array}{lccc} \langle u_0, u_1\rangle\, \bar{R}_0 \langle v_0, v_1\rangle & \text{iff} & u_1 = v_1 \ \text{ and } \ u_0 R_0 v_0, \\ \langle u_0, u_1\rangle\, \bar{R}_1 \langle v_0, v_1\rangle & \text{iff} & u_0 = v_0 \ \text{ and } \ u_1 R_1 v_1, \end{array}$$

and

$$Id = \{\langle u, u\rangle : u \in U_0 \cap U_1\}.$$

Observe that if $\mathfrak{F} = \langle U, U \times U\rangle$ is an universal frame, then $\mathfrak{F} \times^{\delta} \mathfrak{F}$ is a square frame. Let us introduce some notation for logics of some special classes of δ-product frames:

$$\begin{aligned} \mathbf{K} \times^{\delta} \mathbf{K} &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in } \mathfrak{F}_0 \times^{\delta} \mathfrak{F}_1,\ \mathfrak{F}_i \text{ are arbitrary frames}\}, \\ \mathbf{K} \times^{sq} \mathbf{K} &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in } \mathfrak{F} \times^{\delta} \mathfrak{F},\ \mathfrak{F} \text{ is an arbitrary frame}\}, \\ \mathbf{S5} \times^{\delta} \mathbf{S5} &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in } \mathfrak{F}_0 \times^{\delta} \mathfrak{F}_1,\ \mathfrak{F}_i \text{ are equivalence frames}\}, \\ \mathbf{S5} \times^{sq} \mathbf{S5} &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in } \mathfrak{F} \times^{\delta} \mathfrak{F},\ \mathfrak{F} \text{ is an equivalence frame}\} \\ &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in } \mathfrak{F} \times^{\delta} \mathfrak{F},\ \mathfrak{F} \text{ is a universal frame}\} \\ &= \{\varphi \in \mathcal{ML}_2^{\delta} : \varphi \text{ is valid in all square frames}\}. \end{aligned}$$

Using this notation, the finite axiomatisability of RCA_2 can be reformulated as the following:

Theorem 1. [6] $\mathbf{S5} \times^{sq} \mathbf{S5}$ *is finitely axiomatised by the axioms* (1)–(6)*.*

In this note we investigate the particular role of axiom (3) in this axiomatisation. To begin with, this axiom is quite strong in the sense that it can 'force' the **S5**-properties (1) in the presence of 'two-dimensionality', as the following surprising statement shows:

Theorem 2. [10,11] *Let L be any canonical modal logic with*

$$\mathbf{K} \times^{\delta} \mathbf{K} \subseteq L \subseteq \mathbf{S5} \times^{sq} \mathbf{S5}.$$

Then $\mathbf{S5} \times^{sq} \mathbf{S5}$ *is finitely axiomatisable over L:* $\mathbf{S5} \times^{sq} \mathbf{S5}$ *is the smallest modal logic containing L and axiom* (3)*.*

In particular, as a consequence we obtain that $\mathbf{S5}\times^{sq}\mathbf{S5}$ =‘$\mathbf{S5}\times^{\delta}\mathbf{S5}$ + (3)’. Here we show that the remaining axioms indeed do axiomatise $\mathbf{S5}\times^{\delta}\mathbf{S5}$:

Theorem 3. $\mathbf{S5}\times^{\delta}\mathbf{S5}$ *is finitely axiomatised by the axioms* (1)*,* (2)*,* (4)*–*(6)*.*

On the one hand, these axioms are clearly valid in δ-products of equivalence frames. On the other hand, since (1), (2), and (4)–(6) are all Sahlqvist-formulas, the modal logic they axiomatise is determined by a first-order definable class of frames, and so it has the countable frame property. Therefore, it is enough to show the following:

Lemma 4. *Let* $\mathfrak{G} = \langle W, R_0, R_1, D\rangle$ *be a countable rooted frame, validating* (1)*,* (2)*, and* (4)*–*(6)*. Then* $\mathfrak{G}$ *is a p-morphic image of a* δ*-product* $\mathfrak{F}_0\times^{\delta}\mathfrak{F}_1$ *for some universal frames* $\mathfrak{F}_i = \langle U_i, U_i \times U_i\rangle$*,* $i = 0, 1$*.*

Proof. It is a step-by-step argument that is a generalisation of Venema's [15] proof showing that countable rooted frames validating (1)–(6) are p-morphic images of square frames.

One way of presenting such an argument is by defining a ‘p-morphism game’ $\mathcal{G}_\omega(\mathfrak{G})$ between two players $\forall$ (male) and $\exists$ (female) over $\mathfrak{G}$. In this game, $\exists$ constructs step-by-step, (special) homomorphisms from larger and larger δ-products of universal frames to $\mathfrak{G}$, and $\forall$ tries to challenge her by pointing out possible ‘defects’: reasons why her current homomorphism is not an onto p-morphism yet.

To this end, we call a triple $N = \langle U_0^N, U_1^N, f^N\rangle$ a $\mathfrak{G}$-*network*, if U_0^N, U_1^N are nonempty sets, and $f^N : U_0^N \times U_1^N \to W$ is a function such that the following hold, for all $u_i, v_i \in U_i^N$, $i = 0, 1$:

(nw1) $f^N(u_0, u_1)R_0f^N(v_0, u_1)$ and $f^N(u_0, u_1)R_1f^N(u_0, v_1)$,
(nw2) $f^N(u_0, u_1) \in D$ iff $u_0 = u_1 \in U_0^N \cap U_1^N$, and
(nw3) if there exists w in D with $f^N(u_0, u_1)R_iw$, then $u_{1-i} \in U_i^N$.

The two players build a countable sequence of $\mathfrak{G}$-networks

$$N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k \subseteq \ldots.$$

(Here $N_k \subseteq N_{k+1}$ means that $U_i^{N_k} \subseteq U_i^{N_{k+1}}$, $i = 0, 1$, and $f^{N_k} \subseteq f^{N_{k+1}}$.) In round 0, $\forall$ picks any point r in D if there is such. If not, then just any point in W. (As R_0 and R_1 are equivalence relations and $R_0 \cup R_1$ is rooted, any point in W is a root in $\mathfrak{G}$.) $\exists$ responds with the $\mathfrak{G}$-network $U_0^{N_0} = \{u_0\}$, $U_1^{N_0} = \{u_1\}$ and $f^{N_0}(u_0, u_1) = r$, with $u_0 = u_1$ if $r \in D$, and $u_0 \neq u_1$ otherwise.

In round k $(0 < k < \omega)$, some sequence $N_0 \subseteq \cdots \subseteq N_{k-1}$ of $\mathfrak{G}$-networks has already been built. $\forall$ picks

- a pair $\langle x, y\rangle \in U_0^{N_{k-1}} \times U_1^{N_{k-1}}$,
- a point $w \in W$, and
- an index $i = 0$ or $i = 1$

such that $f^{N_{k-1}}(x,y)R_i w$ holds. Let us consider $\exists$'s possible responses in the $i=0$ case. (The $i=1$ case is symmetrical.) She can respond in two ways. If there is some $u \in U_0^{N_{k-1}}$ with $f^{N_{k-1}}(u,y)=w$, then she responds with $N_k = N_{k-1}$. Otherwise, she has to respond (if she can) with some $\mathfrak{G}$-network $N_k \supseteq N_{k-1}$ such that $u^* \in U_0^{N_k}$ and $f^{N_k}(u^*,y)=w$, for some fresh point u^*.

We say that $\exists$ *has a winning strategy in* $\mathcal{G}_\omega(\mathfrak{G})$ if she can respond in each round k for $k<\omega$, no matter what moves $\forall$ take in the rounds. It is not hard to see that if $\exists$ has a winning strategy in $\mathcal{G}_\omega(\mathfrak{G})$, then $\mathfrak{G}$ is a p-morphic image of a a δ-product of universal frames: Consider a play of the game when $\forall$ eventually picks all possible pairs and corresponding R_i-connected points in $\mathfrak{G}$ (since $\mathfrak{G}$ is countable and rooted, he can do this). If $\exists$ uses her strategy, then she succeeds to construct a countable ascending chain of $\mathfrak{G}$-networks whose union gives the required p-morphism.

We show that if $\mathfrak{G}$ validates axioms (1), (2), and (4)–(6), then $\exists$ has a winning strategy in $\mathcal{G}_\omega(\mathfrak{G})$. The case of round 0 is straightforward. Suppose that we are in round $k>0$ and $\forall$ picks $\langle x,y\rangle$, w, and $i=0$ as above. We omit the case where $\exists$'s response is fully determined by the rules of the game, so we may assume that

$$f^{N_{k-1}}(u,y) \neq w, \text{ for all } u \in U_0^{N_{k-1}}. \tag{7}$$

We claim that

$$w \notin D \tag{8}$$

follows. Indeed, if $w \in D$ then $y \in U_0^{N_{k-1}} \cap U_1^{N_{k-1}}$ by (nw3), and therefore $f^{N_{k-1}}(y,y) \in D$ by (nw2). So, by axioms (1) and (4), $w = f^{N_{k-1}}(y,y)$ follows, contradicting (7).

We let $U_0^{N_k} = U_0^{N_{k-1}} \cup \{u^*\}$, for some fresh point u^*, $f^{N_k}(u^*,y)=w$, and $f^{N_k} \supseteq f^{N_{k-1}}$. We consider two cases: either there is no $w^* \in D$ with wR_1w^*, or there is such a w^*.

Case 1. There is no $w^* \in D$ with wR_1w^*.
Then we let $U_1^{N_k} = U_1^{N_{k-1}}$. Take some $u \in U_1^{N_{k-1}}$, $u \neq y$. We need to define $f^{N_k}(u^*,u)$ such that (nw1)–(nw3) hold. We have $f^{N_k}(x,u)R_1 f^{N_k}(x,y)R_0 w$ by (nw1). So by axiom (2), there exists w_u such that $f^{N_k}(x,u)R_0 w_u R_1 w$. As $w_u R_1 w$, by axiom (1) there is no $v \in D$ with $w_u R_1 v$, in particular, $w_u \notin D$. Therefore, $f^{N_k}(u^*,u) = w_u$ is a good choice.

Case 2. There exists $w^* \in D$ with wR_1w^*.
Then we let $U_1^{N_k} = U_1^{N_{k-1}} \cup \{u^*\}$. We need to define f^{N_k} on the new pairs such that (nw1)–(nw3) hold. There are several cases (see Fig. 1):

- First, let $f^{N_k}(u^*,u^*) = w^*$.
- Next, take some $u \in U_1^{N_{k-1}}$, $u \neq y$.
    - *Case* (a). There is no $v \in D$ with $f^{N_k}(x,u)R_0 v$.
      As by (nw1) we have $f^{N_k}(x,u)R_1 f^{N_k}(x,y)R_0 w$, by axiom (2) there exists w_u such that $f^{N_k}(x,u)R_0 w_u R_1 w$. As $f^{N_k}(x,u)R_0 w_u$, by axiom (1) there is no $v \in D$ with $w_u R_0 v$, and therefore $f^{N_k}(u^*,u) = w_u \notin D$ will do.

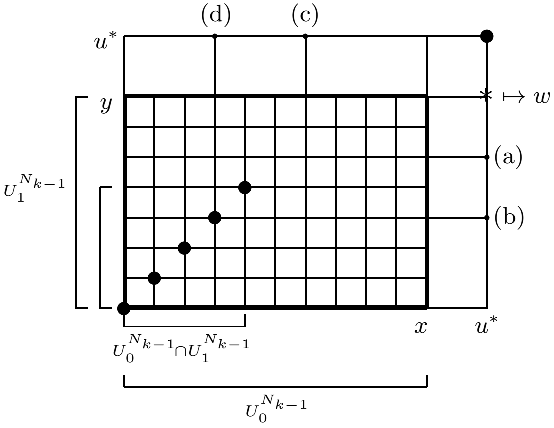


Fig. 1. The subcases in Case 2

  - *Case* (b). There is $v \in D$ with $f^{N_k}(x,u)R_0v$.
    By (nw3) and (nw2), $u \in U_0^{N_{k-1}}$ and $f^{N_k}(u,u) \in D$. By (7), we have $f^{N_k}(u,y) \neq w$. As by (nw1) we also have $f^{N_k}(u,u)R_1f^{N_k}(u,y)R_0w$, by axiom (6) there is $w_u \notin D$ with $f^{N_k}(u,u)R_0w_uR_1w$, and so $f^{N_k}(u^*,u) = w_u \notin D$ will do.
- Finally, take some $u \in U_0^{N_{k-1}}$.
  - *Case* (c). There is no $v \in D$ with $f^{N_k}(u,y)R_1v$.
    As by (nw1) we have $f^{N_k}(u,y)R_0wR_1f^{N_k}(u^*,u^*)$, by axiom (2) there is w_u such that $f^{N_k}(u,y)R_1w_uR_0f^{N_k}(u^*,u^*)$. As $f^{N_k}(u,y)R_1w_u$, by axiom (1) there is no $v \in D$ with w_uR_1v, and so $f^{N_k}(u,u^*) = w_u \notin D$ will do.
  - *Case* (d). There is $v \in D$ with $f^{N_k}(u,y)R_1v$.
    By (nw3) and (nw2), $u \in U_1^{N_{k-1}}$ and $f^{N_k}(u,u) \in D$. On the one hand, we have $f^{N_k}(u^*,u) \neq f^{N_k}(u^*,u^*)$, as $f^{N_k}(u^*,u) \notin D$ by Case (b) and (8), while $f^{N_k}(u^*,u^*) \in D$ by definition. On the other hand, by (nw1) we have $f^{N_k}(u,u)R_0f^{N_k}(u^*,u)R_1f^{N_k}(u^*,u^*)$. So by axiom (5), there is $w_u \notin D$ with $f^{N_k}(u,u)R_1w_uR_0f^{N_k}(u^*,u^*)$. Thus $f^{N_k}(u,u^*) = w_u \notin D$ will do,

completing the proof of Lemma 4.

The role of (3)-like axioms in two-dimensional logics without the individual **S5**-properties is far from clear. Unlike axioms (2) and (4)–(6), axiom (3) does not hold in $\mathbf{K} \times^{sq} \mathbf{K}$. In fact, it is not known whether, say, $\mathbf{K} \times^{sq} \mathbf{K}$ is finitely axiomatisable over $\mathbf{K} \times^{\delta} \mathbf{K}$. Also, though a general argument of [5] can be used to show that both logics are recursively enumerable, no explicit axiomatisations for them are known. Such axiomatisations should be infinite however: As it is shown by Kikot [8], neither $\mathbf{K} \times^{sq} \mathbf{K}$ nor $\mathbf{K} \times^{\delta} \mathbf{K}$ can be axiomatised using finitely many propositional variables.

References

1. Andréka, H., Németi, I., van Benthem, J.: Modal languages and bounded fragments of predicate logic. Journal of Philosophical Logic 27, 217–274 (1998)
2. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge University Press (2001)
3. Chagrov, A., Zakharyaschev, M.: Modal Logic. Oxford Logic Guides, vol. 35. Clarendon Press, Oxford (1997)
4. Gabbay, D., Kurucz, A., Wolter, F., Zakharyaschev, M.: Many-Dimensional Modal Logics: Theory and Applications. Studies in Logic and the Foundations of Mathematics, vol. 148. Elsevier (2003)
5. Gabbay, D., Shehtman, V.: Products of modal logics. Part I. Journal of the IGPL 6, 73–146 (1998)
6. Henkin, L., Monk, J.D., Tarski, A.: Cylindric Algebras, Part II. Studies in Logic and the Foundations of Mathematics, vol. 115. North-Holland (1985)
7. Henkin, L., Monk, J.D., Tarski, A., Andréka, H., Németi, I.: Cylindric Set Algebras. Lecture Notes in Mathematics, vol. 883. Springer (1981)
8. Kikot, S.: Axiomatization of modal logic squares with distinguished diagonal. Mat. Zametki 88, 238–250 (2010)
9. Kurucz, A.: Products of Modal Logics with Diagonal Constant Lacking the Finite Model Property. In: Ghilardi, S., Sebastiani, R. (eds.) FroCoS 2009. LNCS (LNAI), vol. 5749, pp. 279–286. Springer, Heidelberg (2009)
10. Kurucz, A.: On the complexity of modal axiomatisations over many-dimensional structures. In: Beklemishev, L., Goranko, V., Shehtman, V. (eds.) Advances in Modal Logic, vol. 8, pp. 256–270. College Publications (2010)
11. Kurucz, A.: Representable cylindric algebras and many-dimensional modal logics. In: Andréka, H., Ferenczi, M., Németi, I. (eds.) Cylindric-like Algebras and Algebraic Logic. Bolyai Society Mathematical Studies. Springer (to appear)
12. Marx, M., Venema, Y.: Multi-Dimensional Modal Logic. Kluwer Academic Publishers (1997)
13. Segerberg, K.: Two-dimensional modal logic. Journal of Philosophical Logic 2, 77–96 (1973)
14. Shehtman, V.: Two-dimensional modal logics. Mathematical Notices of the USSR Academy of Sciences 23, 417–424 (1978) (Translated from Russian)
15. Venema, Y.: Many-Dimensional Modal Logics. PhD thesis, Universiteit van Amsterdam (1991)

The Birth of Proof:
Modality and Deductive Reasoning[*]

Adriane Rini

Massey University, Palmerston North, New Zealand
`a.rini@massey.ac.nz`

Abstract. This paper is a part of a larger project with my New Zealand colleagues, E.D. Mares and M.J. Cresswell, both of Victoria University of Wellington. Our project is to write *A Natural History of Necessity*, investigating the ways in which philosophers' notions of necessity developed and then tracing the changes that notion undergoes throughout philosophical history. Our aim is to take an historical approach to the question 'Where does necessity comes from?' My focus in the present paper is Aristotle's invention of the simple deductive system of syllogistic logic set out in *Prior Analytics*. What I want to illustrate is the extent to which we can say that Aristotle, writing some 2400 years ago, understood logical consequence as a modal notion.

Keywords: History of logic, necessity, consequence, Aristotle, syllogistic, modality.

1 Introduction

Aristotle tells us in *Prior Analytics* A1 what a deduction (a syllogism) is[1]:

(1) A deduction is a discourse in which, certain things having been supposed, something different from the things supposed results of necessity because these things are so. (*Prior Analytics* A1, 24b18–22)[2]

Because Aristotle explicitly describes the conclusion of a valid syllogism as 'resulting of necessity', it looks, on the face of it at least, as if the necessity that he has in mind here is a modal notion. One might even say that because Aristotle uses the word 'necessity' his definition just is modal. That might be too loose a sense of modality for some, but it nonetheless seems plausible. And it is at least plausible that this sense of necessity is all that we should suppose Aristotle has in mind in (1). But is his use of the word 'necessity' in (1) really so simple? This

---

[*] This research is funded by a Marsden Grant from the Royal Society of New Zealand (2011–2013). Parts of the project also received support from the Royal Flemish Academy for Science and the Arts (2010).

[1] This definition appears also in *Topics* I.1, 100a25-27.

[2] I have used Robin Smith's translation [1] for all passages from *Prior Analytics*.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 34–49, 2013.

paper looks at how to answer the question: Can we say with any certainty what it is that Aristotle understands by 'necessity' in his definition (1)?

The following might help to make my question clearer. When Aristotle says a syllogism is valid, does he mean

(2) that from true premises you cannot have false conclusion?

– where that 'cannot' is a genuine modal. Or does he mean simply

(3) that no matter how you choose the subject and predicate terms in a syllogistic schema, you will never in fact have true premises and false conclusion?

Of course, you might say that (3) represents all there is to logical necessity, in which case you will want to say that (3) does describe a modal notion. Perhaps this was what logicians like Carnap (or the writers of many introductory logic textbooks) might have supposed. In this paper I use 'modal' in a more robust sense – that is, when I describe (2) as genuinely modal, all I mean is that (2) requires a move beyond the actual facts of the matter in a way which (3) does not. In other words, for something to count as genuinely modal we have to consider how things might have been – not just how things are. My question concerns whether Aristotle might only have the idea that in a valid schema any substitution of terms preserves truth. If that is all that he means, then the necessity he describes in (1) might not involve what I am calling genuine modality. Hence the question – can we say with any surety whether Aristotle understands 'resulting of necessity' as a modal notion?[3]

2 Some Recent Answers

Richard Sorabji [2] asks precisely this question. He is inclined to say that it is not a modal notion, but he doesn't claim to base this inclination on hard evidence.[4] My aim is to look at what evidence we have that might help to elucidate what

---

[3] The larger project of which this paper is just a small and early part looks at the history of logic to see how the nature of logical consequence has been understood by philosophers. We use this Etchemendy-style distinction as the focus for our study. Because Aristotle is the first philosopher to actually study and catalogue patterns of human reasoning, he seems to be the first we can ask such questions of. There is, to be sure, earlier evidence of counterfactual reasoning in philosophy – e.g., Zeno used *reductio* proofs; similarly, the sophists. Ancient geometry employed *reductio* proofs as well. But Aristotle gave us the *Prior Analytics*, the first treatise on logic itself, and my question is about whether Aristotle understood validity to be determined solely by form.

[4] Sorabji sometimes sounds like he thinks it is modal: "One example of an impossible compound would be the truth of the premises and the falsity of the conclusion in a valid syllogism." [3, p.223] But this example seems to me to emphasize how difficult it is to see and to articulate the distinction between (2) and (3).

it is that Aristotle himself understood about the necessity of the consequent of a (valid) syllogism. But first, consider Sorabji's approach. He points out that the word 'necessity' and its various cognate expressions are ubiquitous in Aristotle's philosophy. And Sorabji finds the wide variety of examples of necessity in Aristotle's works provide good reason for supposing that Aristotle's use of the term is *ad hoc*. If we take this view, then it looks as if the best we might be able to do is enumerate the various uses, and this is just what Sorabji does. In *Necessity, Cause, and Blame* [3], Sorabji constructs a list of necessities (pp. 222–224) which includes as many as ten senses of necessity in Aristotle's works. The necessity of the consequent is simply included as one among all the different cases. This list-making approach is not without justification – Aristotle himself does pretty much the same thing, describing various senses of necessity in *Metaphysics* V.5 and 12 – though none of Aristotle's lists are as fulsome as Sorabji's. Sorabji pays close attention to 'logical' necessity and describes what he sees as "Aristotle's habit of jumbling together logical and non-logical necessities with apparent indifference". (Sorabji, [3, 134]) He suggests that "Aristotle did not regard logical necessity as a distinct kind of necessity." (p. 133) These themes are further developed in Sorabji [3], where he emphasizes a difference between the ways that Aristotle and modern logicians treat necessity: "Modern philosophers have tended to be very parsimonious in their recognition of distinct kinds [of necessity]... In contrast with this parsimony, Aristotle recognizes a rich collection of cases. Moreover, his system of classification is refreshing to study, precisely because it does not mesh with ours." (p. 222) When he says this Sorabji has in mind philosophers such as Łukasiewicz and Quine, and the debates about the analysis of necessity that characterized much of twentieth century philosophy.

Since Aristotle does construct his own lists we can look at them to see what they suggest about the necessity which grounds Aristotle's logic. Consider Aristotle's own lists of necessities, from the 'lexicon' in *Metaphysics* V.5.

> We call the necessary (1) that without which, as a condition, a thing cannot live, e.g. breathing and food are necessary for an animal; for it is incapable of existing without these. — (2) The conditions without which good cannot be or come to be, or without which we cannot get rid or be freed of evil, e.g. drinking the medicine is necessary in order that we may be cured of disease, and sailing to Aegina is necessary in order that we may get our money. — (3) The compulsory and compulsion, i.e. that which impedes and hinders contrary to impulse and choice. For the compulsory is called necessary; that is why the necessary is painful, as Evenus says: 'For every necessary thing is ever irksome'. And compulsion is a form of necessity, as Sophocles says: 'Force makes this action a necessity'. And necessity is held to be something that cannot be persuaded – and rightly, for it is contrary to the movement which accords with choice and with reasoning. — (4) We say that that which cannot be otherwise is necessarily so. And from this sense of necessity all the others are somehow derived; for as regards the compulsory we say that it is necessary to act or to be acted on, only when

> we cannot act according to impulse because of the compelling force, – which implies that necessity is that because of which the thing cannot be otherwise; and similarly as regards the conditions of life and of good, when in the one case good, in the other life and being, are not possible without certain conditions, these are necessary, and this cause is a kind of necessity. — Again, (5) demonstration is a necessary thing, because the conclusion cannot be otherwise, if there has been demonstration in the full sense; and the causes of this necessity are the first premises, i.e. the fact that the propositions from which the deduction proceeds cannot be otherwise. [4]

On Aristotle's account all these kinds of necessities are linked. The fourth and fifth senses in particular bear on our question here. The fourth sense is primary (1015a35-6) and the fourth sense fits Aristotle's usual definition of necessity – it is 'what cannot be otherwise', or 'what is not possibly not'. The primacy of the fourth sense explains the ways in which the other senses are themselves kinds of necessities. Of course, the emphasis here is on what is common to the necessities listed in this passage. The emphasis is not on their distinctness.

The fifth sense listed in *Met* V.5 concerns 'necessity' in a special kind of syllogism – called a *demonstration* – in which both premises are themselves necessary propositions. Aristotle seems to have in mind the syllogisms described earlier in *An Pr* A8, where he explains that whenever we have a (valid) syllogism from 'premises of belonging', we also have a syllogism from premises about 'belonging of necessity'. Here is how Aristotle puts the point in *An Pr* A8:

> In the case of necessary premises, then, the situation is almost the same as with premises of belonging: that is, there either will or will not be a deduction with the terms put in the same way, both in the case of belonging and in the case of belonging or not belonging of necessity, except that they will differ in the addition of 'belonging (or not belonging) of necessity' to the terms (for the privative premise converts in the same way, and we can interpret 'being in as a whole' and 'predicated of all' in the same way).

The question is how to interpret this. Both the *Met* V.5 and *An Pr* A8 passages appear to be saying that since we have, e.g.,

(4) All B are A
All C are B
∴ All C are A (*Barbara*)

then we also have

(5) All B are A by necessity
All C are B by necessity
∴ All C are A by necessity (*Barbara LLL*)

This has suggested to some interpreters that Aristotle has a logical principle about necessitation (the K-principle) which takes us from $L(p \supset q)$ to $(Lp \supset Lq)$, and so from a valid syllogism such as Barbara (4) where there is a necessary connection between premises and conclusion, to a valid syllogism, Barbara LLL, where a *modal conclusion* follows from modal premises. If this is what Aristotle means then we need to ask how he arrives at such a principle? But that is never made entirely clear in either text. (For further discussion of this see Ebert and Nortmann [5].) Of course, the modern logician's K-principle, $L(p \supset q) \supset (Lp \supset Lq)$, is a genuinely modal principle – specifically, the antecedent must be modalized since $(p \supset q) \supset (Lp \supset Lq)$ is not a theorem of a (non-trivial) modal logic – i.e., the antecedent which represents the validity of the syllogism must be modalized. So if there is something like K at work in Aristotle's logic, then we can say that his reasoning does involve genuine modality. The difficulty is that without an account from Aristotle to show that he means in these passages the same thing that we do when we say $L(p \supset q) \supset (Lp \supset Lq)$, and without an account of how he arrives at such a principle, then we cannot be certain that his reasoning here is genuinely modal. Indeed, it is possible to give an analysis of the move from (4) to (5) which does not require genuinely modal reasoning, but which requires only modally qualified terms. Here is what I mean. If the necessity in (5) Barbara LLL is the kind of Aristotelian necessity that qualifies a term – i.e., what we represent today via *de re* modals – then (5) Barbara LLL looks like a special instance of Barbara (4). It might be that the right way to interpret (5) is as follows:

(6) Every B is a necessary-A
Every C is a necessary-B
∴ Every C is a necessary-A

Or, the right way to interpret (5) Barbara LLL might even be:

(6') Every necessary-B is a necessary-A
Every necessary-C is a necessary-B
∴ Every necessary-C is a necessary-A

Both (6) and (6') are special instances of (4) Barbara. The difference comes with the *kind* of terms which are specified. (6') has modally qualified terms uniformly substituted for non-modal terms. But that means that the reasoning involved in (6') is the same *non-modal* reasoning at work in (4). (6) is a little tricker – since in order to prove its validity we need the T-principle: $L\phi \supset \phi$ – i.e., that whatever is necessary is so. The T-principle tells us, e.g., where B is 'man', anything that is a necessary man is also a man. The upshot of this is that when the question is how to interpret Aristotle's move from (4) to (5), it appears that there are two quite different answers available. There might be a principle like K at work which is genuinely modal, or there might be a principle like T at work in Aristotle's logic, which if used as Rini [6] suggests is not strongly modal. And, at this stage there is no clear textual evidence to decide between these two.

Both Hintikka [7] and Mignucci [8] identify a line of reasoning within Aristotle's work according to which anything that is always true is necessarily true. This is known as the *principle of plenitude.* Its status in Aristotle's philosophy is controversial. (See for example Judson [9].) But it bears directly on my question in this paper because of the way in which plenitude affects the syllogistic. If anything which is always true is necessarily true, then anytime we have a true Aristotelian proposition of the form, e.g.,

(7) All B are A

then we have a true proposition of the form

(8) All B are A by necessity.

In the *Prior Analytics*, Aristotle appears to treat (7) and (8) as different propositional forms. Plenitude, however, does not. Hintikka [7] sees this as evidence of a deep confusion permeating Aristotle's modal syllogistic. Rini [10] argues that plenitude's disastrous effect on the syllogistic is better understood as evidence against plenitude, not as evidence against the syllogistic. For if (7) and (8) are not distinct propositions then we cannot capture the difference which Aristotle describes between the validity of

(9) All B are A by necessity
All C are B
∴ All C are A by necessity (*Barbara LXL*)

and the invalidity of

(10) All B are A
All C are B by necessity
∴ All C are A by necessity (*Barbara XLL*)

Without a distinction between these, quite a lot of the force of Aristotle's logical system is forfeited. While there are passages in Aristotle's works that look like good evidence that plenitude is part of his thinking, there is little textual evidence in *An Pr* that plenitude is at work in the syllogistic. Plenitude itself is clearly a notion which does involve genuine modality – it is a claim that there is nothing in the world which you could say can happen but never will happen. Its effect is to trivialize the modal syllogisms.[5] But, of course, if we do not have textual evidence that plenitude is involved in the syllogistic, then plenitude does not provide good reason to suppose that Aristotle's syllogistic requires genuine modality. And so, returning to the question proposed at the start about whether Aristotle has something like (2) or (3) in mind, whatever we say about plenitude, it just does not help with the logic of the syllogistic. Plenitude does not decide between (2) and (3).

---

[5] Rini [6] suggests that much of the modal syllogistic is trivially modal, though for different reasons.

The question of a distinction between (2) and (3) is one that arises squarely within logic, and so it seems to me that the obvious place to look for an answer is in Aristotle's syllogistic logic. I want to look at what evidence can we find in *Prior Analytics* – where Aristotle is most directly studying syllogistic logic – which indicates how Aristotle understands the necessity in (1).

3 Non-modal Reasoning in *An Pr* (the Assertoric Syllogistic)

Is there any textual evidence from *An Pr* to indicate whether Aristotle's notion of necessity in (1) goes *beyond* simple matters of fact? One way to begin is by looking at the counter-examples that Aristotle offers, to see whether – when he puts terms in place of variables – his own examples ever involve anything more than actual, real world truths and falsehoods. Aristotle's counter-examples have frequently come in for criticism – there are a variety of reasons why. Sometimes it seems Aristotle is simply too swift and not careful enough in his explanations of the counter-examples. But to be fair, Aristotle, several times, suggests the same, telling us that terms should be better chosen than the terms that he offers in the text. But perhaps the more serious criticism of his counter-examples comes from scholars who worry that they give a hint that Aristotle might be working mainly by trial and error, trying to see whether he can come up with terms to illustrate invalidity. If so, then there is a happenstance quality to the syllogistic which suggests that (3) rather than (2) better captures Aristotle's understanding of logical necessity. (Ross [11] and Łukasiewicz [12] seem to take this point further, worrying whether Aristotle's approach to logic might have involved quite a lot of trial and error.)

It helps to see just how Aristotle deals with counter-examples. Here is one example. It is the first of the counter-examples Aristotle offers. It is from *An Pr* A4, where he is explaining why a premise pair does *not* produce a syllogism:

> However, if the first extreme [A] follows all of the middle [B] and the middle [B] belongs to none of the last [C], there will not be a deduction of the extremes [C,A], for nothing necessary results in virtue of these things being so. For it is possible for the first extreme to belong to all as well as to none of the last. Consequently, neither a particular nor a universal conclusion *becomes necessary*; and, since nothing is necessary because of these, there will not be a deduction. Terms for belonging to every are animal, man, horse; for belonging to none, animal, man, stone. (*An Pr* A.4, 26a2-10) (Italics are mine.)

This passage illustrates how Aristotle explains those cases where a given premise pair does not yield a syllogism – that is, where we have no guarantee of a unique conclusion. An important point to note about his method is that he is looking for a conclusion of a specified form – any conclusion here must be a proposition linking the two terms which each occur only once in the premises. So, in the passage above, he is looking for a conclusion which links a C subject to an A predicate. (He calls these terms the *extremes*, and he calls the term which occurs twice in the premises the *middle*. The middle term drops out and does not occur in the conclusion.) So the premises we are considering are ‘All B are A’ and ‘No C is B’. And Aristotle is attempting to show that no conclusion follows which expresses a relation between C and A.

All B are A
No C is B
Some C is A / Some C is not A

Although Aristotle does not explicitly state this, it clearly suffices for him to show that neither a particular affirmative nor a particular negative can be obtained. That is, he must show that you cannot get ‘Some C is A’ (since one set of terms allows ‘No C is A’) and you cannot get ‘Some C is not A’ (since another set of terms allows ‘All C are A’). If you cannot get a particular conclusion, you cannot get a universal. When we put the terms Aristotle recommends into this schema, we get the following:

All men are animals	All men are animals
No horse is a man	No stones are men
All horses are animals	No stones are animals

Aristotle explains why these examples show that there is no syllogism from these premises. No conclusion ‘becomes necessary’ because, as his examples show, different terms give different results. One set of terms gives true premises and an affirmative ‘conclusion’. The other set of terms gives true premises and a privative ‘conclusion’. So there is no *unique* form for a conclusion relating C and A. So Aristotle says there is no syllogism.

This is the method at play right through the non-modal, *assertoric* syllogistic of *An Pr* A4-6. In an appendix (which I can make available on request), I have listed counter-examples for each set of terms that Aristotle recommends to us in the non-modal, assertoric syllogistic. Nearly all of these counter-examples involve only actual, real world truths and falsehoods. I have highlighted those cases – marking them with a ‘*’ – where it seems that something *more* than simple real world truths and falsehoods might be at play. But those cases are few, and most arise only in passages where Aristotle gives a very sweeping and complicated synopsis – i.e., they occur in passages where he does not seem to ‘sweat the details’.[6] Also, where we find such examples, Aristotle always *can* choose terms which give real life counter-examples. By far the main evidence of these counter-examples would seem to show that Aristotle’s *assertoric* syllogistic does not require modal reasoning. And so the vast majority of the examples that Aristotle offers are examples which cannot definitively decide between (2) and (3), and that leaves open the possibility that Aristotle understands the necessity

---

[6] The apparently loose and casual style of some of Aristotle’s counterexamples has led some interpreters to overlook them.

in his definition of a syllogism as indicating only that any substitution of terms in a (valid) schema which gives true premises will also give a true conclusion. It is of course possible, however, that the examples which I have starred in the appendix really are evidence of genuinely modal reasoning. But such examples seem to me too few and, as they appear in *An Pr* A5-6, far too sketchily thought out to stand as decisive evidence of genuinely modal reasoning.

Can we find any clearer evidence in the text? Aristotle intends the definition (1) to cover all (valid) syllogisms, and so in addition to the assertoric, non-modal syllogisms, it also covers what are known as the *apodeictic* syllogisms –these are syllogisms in which at least one of the premises is about necessity. (As noted above, the fifth kind of necessity in the *Metaphysics* V.5 discussion deals with the special sort of syllogism – *demonstration* – where both of the premises are themselves propositions about necessity.) Aristotle's definition (1) also covers what are known as the *problematic* syllogisms – syllogisms in which at least one of the premises is about possibility. These apodeictic and problematic syllogisms each raise different considerations and so it will help to look at each in turn. The next section looks at the apodeictic syllogisms, and what is involved in an Aristotelian premise about necessity.

4 Deductions Involving Necessary Premises in *An Pr* (the Apodeictic Syllogistic)

When we move to Aristotle's modal syllogistic we get additional textual evidence which bears on the question about how to understand the necessity in (1). Consider the following passage from the apodecitic syllogistic in *An Pr* A10:

> And moreover, it would be possible to prove by setting out terms that the conclusion is not *necessary without qualification*, but only *necessary when these things are so*. For instance, let A be animal, B man, C white, and let the premises have been taken in the same way (for it is possible for animal to belong to nothing white). Then, man will not belong to anything white either, but not of necessity: for it is possible for a man to become white, although not so long as animal belongs to nothing white. Consequently, the conclusion will be necessary when these things are so, but not necessary without qualification. (*An Pr* A.10, 30b31-40)

The schema that Aristotle is studying here is usually taken to be the following:

$$\frac{\begin{array}{l}\text{All B are by necessity A}\\ \text{All C are not A}\end{array}}{\text{All C are by necessity not B}} \quad (\textit{Camestres LXL})$$

With terms in place of variables we get:

$$\frac{\begin{array}{l}\text{All men are necessary animals}\\ \text{All white things are not animals}\end{array}}{\text{All white things are by necessity not men}}$$

Aristotle wants to explain why Camestres LXL is not a valid syllogism. His parenthetical remark is crucial to his explanation. Here, he is drawing on the fact that when we put his terms in place of variables, then we get a premise 'all white things are not animals'. But on the face of it, this is a *false* premise, since there are in fact many things that are animals but which are nonetheless white. Aristotle clearly understands this, but he reasons that we can at least *suppose* that the premises are true. And we can suppose so because 'it is possible for animal to belong to nothing white'. Today, we might explain this point by saying simply that even though the second premise is in fact false, it could have been true since it could have been the case that no animals are white. That is, it could have been true, but it is not in fact true. Aristotle reasons that we can, therefore, *suppose* that our premises are true and, when we do so, we can in fact syllogize from them. When we do, we do *not* reach a modal conclusion 'All C are by necessity not B', but we do reach a non-modal conclusion 'All C are not B'. When we suppose the premises are true then the conclusion is *necessary when these things are so* – that is to say, the conclusion follows of necessity *supposing* the premises are true. But the conclusion is not itself a modal proposition – it is not 'necessary without qualification', or as it is usually described, it is not necessary in an *absolute* sense. Aristotle is aware of the potential for confusion about the uses of 'necessity' here. There is in fact quite a lot written about his interest in distinguishing 'absolute' and 'relative' necessity.[7] Absolute necessity is the necessity that is involved in a modal proposition like the first premise, 'All men are necessary animals'. It is the necessity that describes the essentialism in Aristotle's metaphysics. Relative necessity is the necessity of the consequent – relative because the conclusion is necessary when we suppose that the given premises are true. As the passage from A10 illustrates, Aristotle does not want his reader to confuse the absolute necessity that is involved in a modal proposition, with the necessity common to all valid syllogisms whether they are modal or not.

From the point of view of this paper, the more important point about this passage is that when Aristotle tells us we have to suppose the truth of a premise such as 'All white things are not animals', he is telling us to move beyond actual, real world examples. We have, instead, to suppose that the facts were different from what they in fact are. That is the kind of thing that we often need to do in the modal syllogistic, and it is I think the first textual evidence in *An Pr* that the passage from premises to conclusion is genuinely modal. In fact, we can tell precisely where the need for such counterfactual reasoning will typically arise. Any time Aristotle's examples involve an accident term in the subject position of a universal proposition, then we might need to use counterfactual reasoning. We have to look closely in such cases to see whether supposing the premise is true is to make a supposition which takes us beyond simple actual truth.

---

[7] Patzig [13, pp.16–42] and Maier [14, vol 2, pp.242–244] both deal with it at length, but their interest is different and there seems to me little in their discussion which bears strongly on the question in the present paper. Indeed Sorabji seems to be the first to have asked it.

5 Deductions Involving Premises about Possibility in *An Pr* (the Problematic Syllogistic)

As Aristotle continues to explain the modal syllogistic, his proof methods become more sophisticated and sometimes involve what seem to be further examples of genuinely modal reasoning. In the problematic syllogistic, Aristotle considers schema involving premises about possibility. He wants to prove that there are cases where there is a syllogism even if one of the premises involves only a possibility. One of the ways he does this is to take a premise which says something is possible, and then to suppose that the possibility *really is actual*. So the proof involves a supposition that *might* be true, but *might* be false. Aristotle understands that if something is possible then it *might* be true, and that if it is possible, then supposing that it *really is* true might lead to a falsehood, but it cannot lead to an absurdity. That looks like further evidence that what he means by 'necessity' in (1) is for him a modal notion.

The idea is this. Given a premise that something is possible, assume that the possibility is realized, and then reason non-modally. Any non-modal proposition obtained in this way may then be concluded to be possible. Aristotle explains this in *An Pr* A.15: "when something false but not impossible is assumed, then what results through that assumption will also be false but not impossible" (34a25-27).[8] In fact, this is modal in a way which is beginning to approach something like a modern 'possible worlds' analysis, because of the way that it involves counterfactuals. Here is an example of what you find in the *Prior Analytics*:

> Now, with these determinations made, (11) let A belong to every B and (12) let it be possible for B to belong to every C. Then (13) it is necessary for it to be possible for A to belong to every C. (14) For let it not be possible, and (15) put B as belonging to every C (this is false although not impossible). Therefore, if (14) it is not possible for A to belong to every C[9] and (15) B belongs to every C, then (16) it will not be possible for A to belong to every B (for a deduction comes about through the third figure). But it was assumed that it is possible for A to belong to every B. Therefore, it is necessary for it to be possible for A to belong to every C (for when something false but not impossible was supposed, the result is impossible). (*An.Pr.* A15, 34a34-b2)

(11) Every B is A
(12) Every C is contingently-B
(13) Every C is possibly-A
Suppose

---

[8] We find evidence of a related discussion in *De Caelo* I.12, where Aristotle very carefully considers such contrary-to-fact propositions as 'Sitting is possible to Socrates even though he is standing'. And such examples clearly require a genuinely modal analysis.

[9] Aristotle's text suggests that he thinks that the reductio hypothesis is really a universal. In the discussion of the present passage I give the reductio hypothesis as a particular. From a modern point of view, this is not correct.

(14) Some C is not possibly-A
(15) Every C is B
Then
(16) Some B is not possibly-A

But (16) and (11) cannot both be true, so Aristotle wants to say the reductio shows we can syllogize to (13). That is, Aristotle counts Barbara XQM or (11)(12)(13) as valid.

As Aristotle explains, the proof requires *actualizing the possibility* in (12). This is captured in the move from (12) to (15). But the difficulty about this is that some choices of terms appear to generate counterexamples. For example, let A be 'horse', B be 'in the paddock' and C be 'man':

(11') Everything in the paddock is a horse
(12') Every man could be in the paddock
(13') Every man could be a horse

Even supposing the premises are true, the conclusion is false because for Aristotle no man could be a horse. The terms make it easier to see the nature of the problem. If we try actualizing the possibility in (12'), then we get 'every man is in the paddock' but if that is true, then the truth value of our initial premise (11') has to change. We cannot both suppose (12') actual and still have (11') true. In *An.Pr.* A15 Aristotle tries to explain how to *avoid* making such a mistake by telling us *not* to choose terms as I have here. Here are his own instructions:

> One must take 'belonging to every' without limiting it with respect to time, e.g., 'now' or 'at this time', but rather without qualification. For it is also by means of these sorts of premises that we produce deductions, since there will not be a deduction if the premise is taken as holding only at a moment. For perhaps nothing prevents man from belonging to everything in motion at some time (for example, if nothing else should be moving), and it is possible for moving to belong to every horse, but yet it is not possible for man to belong to any horse. Next, let the first term be animal, the middle term moving, the last term man. The premises will be in the same relationship, then, but the conclusion will be necessary, not possible (for a man is of necessity an animal). It is evident, then, that the universal should be taken as holding without qualification, and not as determined with respect to time. (*An.Pr.* A15, 34b7-18)[10]

Premise (11) is only true at a time and not true without qualification. What results is not a syllogism. Premise (11) changes its meaning – it becomes false *when* premise (12) is realized. Aristotle's instructions in *An.Pr.* A15 are a caution against choosing terms in such a way.

---

[10] Some interpreters are suspicious about the authenticity of *An.Pr.* 34b7-18. See Patterson [15, pp.167–174] and Malink [16, p. 102, n. 19].

We can give a proof that Barbara XQM – that is, (11)(12)(13) – is a valid syllogistic schema, but it is an odd sort of proof from a modern point of view because it depends upon the introduction of a semantic restriction which affects our choice of terms, and this is odd because we normally think of logic as immune to semantic restrictions. But our project is to try to explain *Aristotle's* method, not modern methods. Consider how things go if we restrict the B term so that anything which is B is necessarily-B.

(11) Every B is A
(12) Every C is possibly-B
(13) Every C is possibly-A

Start with the conclusion (13). The only way to have a false conclusion here is to produce a C *which cannot possibly be A*. In other words, for (13) to be false A must be necessary and cannot be an accident. So, A as well as B must be restricted. But A occurs as a term in premise (11), and so premise (11) will be affected too. If A must be restricted in this way then premise (11) is not really an ordinary *non-modal* premise – (11) is really a premise involving (hidden) necessity. Next consider premise (12). Aristotle's proof of (11)(12)(13) depends upon being able to realize the possibility expressed in premise (12). When we actualize 'every C is possibly-B' we get 'every C is B'. In *De Caelo* I.12, it is just such a procedure that generates the monstrous error that Judson [9] calls the insulated realization (IR) manoeuvre. But it is an error that can only occur when B is an accidental term – and such an error is blocked by our supposition at the start of the proof that anything that is B is necessarily-B, and so an accidental term B is prohibited.

I have argued that this distinction between terms about what is accidental (e.g., 'sitting', 'being in the paddock', 'moving') and what is necessary (e.g., 'man', 'animal') is crucial to understanding parts of Aristotle's logic. And this distinction between kinds of terms comes into play when we actualize (12). If B signifies something which is possible because it is a matter of mere chance or coincidence, then premise (11) only happens to be true at a given time. For example, if B is 'in the paddock' and A is 'horse', then premise (11) will be 'everything in the paddock is a horse.' (Or, following Aristotle's example, if B is 'moving' and A is 'horse', then premise (11) will be 'everything moving is a horse.') These premises hold *at a time*; they are true at a moment. But they are not true always, without respect to a time. The nature of the B term guarantees this because in these examples the B term signifies something whose possibility arises because of chance, happenstance, mere coincidence. Aristotle tells us not to choose premises like this. They get us into trouble and make a mess of syllogistic. The reason they cause trouble is that they can change too easily from true to false, and in fact they *do* change from true to false when the possibility in premise (12) is realized. If we actualize the possibility 'all men are possibly in the paddock', we get 'all men are in the paddock' and then it is not true that everything in the paddock is a horse. This makes premise (11) false when (12) is actualized. This is the IR manoeuvre and if Aristotle were to allow it then he would be making a monstrous error. But we might take his comment (*An.Pr.* A15, 34b7-18) about not choosing premises which hold only at a moment as Aristotle's attempt to avoid this error – since (11)(12)(13) is guaranteed to be valid provided the B term is restricted to terms about what is necessary.

Semantic restrictions on terms are a matter of interpretation and so invite a certain controversy. But that is not my point here. Here, my concern is with Aristotle's basic method of proof through the realization of a possibility. This method might suggest to us something like a modern possible world semantics, because very clearly his reasoning in several cases does go beyond mere matters of fact. In these proofs Aristotle is reasoning not just about what *is* the case, but about what *might* be the case even if in fact it is not. What this illustrates is Aristotle's genius at work, rising to meet the demands of a logic about possibility. He devises a new proof method – proof through realization – in order to accommodate what his new logic of possibilities requires. This proof method is unmistakably modal and indicates that by this stage in Aristotle's logical development he has something like (2) in mind.

Interpreters, however, always have to be sensitive to shifts in the text, and there is a shift in the discussion of proof through realization. As I have explained, there is clear textual evidence that Aristotle uses proof through realization. But it may be that we don't have to hang much on this sort of proof because in later parts of the modal syllogistic Aristotle seems to abandon it for other methods. He does not, however, explain why. But where he could just as well use realization, he switches, without comment, to more direct proofs in which he establishes a non-modal conclusion (from premises about necessity and contingency). He then uses a version of what modern modal logicians call the T-principle ($\phi \supset M\phi$) to argue from a non-modal conclusion to one about possibility: "And it is evident that a deduction of being possible not to belong also comes about, given that there is one of not belonging." (36a17) So, for example, after he establishes a conclusion 'A belongs to no C', he also claims 'A possibly does not belongs to no C.' Representing this in modal predicate logic, when we reach a conclusion of the form $\forall x(Cx \supset \neg Ax)$, then we also have $\forall x(Cx \supset M\neg Ax)$. This new method comes into play in *An Pr* A16, 36a7-17 (with syllogisms whose premises involve necessity and contingency), and continues through the final chapters of the modal syllogistic.) This new proof method also involves modal reasoning since it depends upon the T-principle, but it lacks the full counterfactual force of proof through realization. Still, it is clear that Aristotle does in some cases require counterfactual reasoning, and the fact that he got there at all helps to answer my initial question about whether he understood logical consequence as a modal notion.

6 Conclusion

When we look specifically at *An Pr*, at Aristotle's *logical discussions*, we can trace a growing sophistication in his treatment of necessity and we can to a certain extent 'benchmark' points of change. For a start, we saw that in the non-modal syllogistic there is too little for us to decide conclusively whether Aristotle's sense of necessity in (1) is closer to (2) or to (3). But his modal logic presents some more complicated challenges, and in his treatment of the modal cases we can see how Aristotle devises sophisticated solutions. In the syllogistic involving necessity, his proof methods shift to include counterfactual reasoning. And so they are in an important sense modal – modal in what I am calling the genuine sense described in (2). Even if we are reasoning from premises which do not in fact hold, we can suppose that they hold, and then syllogize to a conclusion which follows of necessity from that supposition. In the syllogistic about possibility, when Aristotle wants to syllogize from premises that involve contingency, he again brings in a sophisticated modal tool– proof through realization. And so we do find in the modal syllogistic evidence of the kind of genuinely modal reasoning which indicates that Aristotle does sometimes have something like (2) in mind. The sense of necessity described in (3) is not adequate to describe these sorts of counterfactual reasoning. This of course leaves open the possibility that this genuine modality might be implicit in the non-modal, assertoric cases, too. On the basis of the evidence presented here we can safely say that he got there – he got to (2), to a modal notion of logical consequence.[11]

A final unanswered question: That still does not tell us whether Aristotle understood the necessity required by his essentialist metaphysics (absolute necessity) and the necessity that binds a conclusion to the premises of a valid deduction (relative necessity) as the *same* necessity. This marks a significant point of difference between Aristotle's logic and modern logic. Today we have the individual variable, a univocal necessity operator, and the notion of scope, which together allow us to explain) the necessity involved in logical consequence and the necessity required by essentialism as the same. What we do not have is any evidence that Aristotle could understand them in terms of the same, univocal necessity operator. This is perhaps the best way of appreciating Sorabji's remarks about the lack of parsimony of Aristotle.

References

1. Smith, R.: Aristotle: Prior Analytics. Hackett Publishing Company, Indianapolis (1989)
2. Sorabji, R.: Aristotle and Oxford Philosophy. American Philosophical Quarterly 6, 127–135 (1969)
3. Sorabji, R.: Necessity, Cause, and Blame. Gerald Duckworth & Co., London (1980)
4. Barnes, J.: The Complete Works of Aristotle: The Revised Oxford Translation. Bollingen Series. Princeton University Press, Princeton (1984) [The translation of Metaphysics is by W.D. Ross]

---

[11] What we cannot tell is whether he was happy with that kind of modal reasoning. Some proofs require the notion of necessity captured by (2). But most – though not all – of the syllogistic can be explained with the less sophisticated, substitutional notion expressed by (3).

5. Ebert, T., Nortmann, U.: Aristoteles Analytica Priora Buch I. Akademie Verlag, Berlin (2007)
6. Rini, A.: Aristotle's Modal Proofs: Prior Analytics A8-22 in Predicate Logic. Springer (2011)
7. Hintikka, J.: Time and Necessity: Studies in Aristotle's Theory of Modality. Clarendon Press, Oxford (1973)
8. Mignucci, M.: On a Controversial Demonstration of Aristotle's Modal Syllogistic: An Enquiry on Prior Analytics A.15. Antenori, Padua (1972)
9. Judson, L.: Eternity and Necessity in de Caelo I.12. Oxford Studies in Ancient Philosophy, 217–255 (1983)
10. Rini, A.: When Time is of the Essence: Prior Analytics I.15 and De Caelo I.12. Logique et Analyse 183-184, 419–440 (2003)
11. Ross, W.D.: Aristotle's Prior and Posterior Analytics: A Revised Text with Introduction and Commentary. Clarendon Press, Oxford (1957) (First published in 1949. Reprinted with corrections 1957, 1965. Page references to the 1957 printing)
12. Lukasiewisc, J.: Aristotle's Syllogistic from the Standpoint of Modern Formal Logic, 2nd edn. Clarendon Press, Oxford (1957)
13. Patzig, G.: Aristotle's Theory of the Syllogism (Translated by J. Barnes). D. Reidel, Dordrecht (1968)
14. Maier, H.: Die Syllogistik des Aristoteles, 3 volumes. Tübingen (1896-1900)
15. Patterson, R.: Aristotle's Modal Logic: Essence and Entailment in the Organon. Cambridge University Press, Cambridge (1995)
16. Malink, M.: A reconstruction of Aristotle's modal syllogistic. History and Philosophy of Logic 27, 95–141 (2006)

Indiscrete Models: Model Building and Model Checking over Linear Time

Tim French, John McCabe-Dansted, and Mark Reynolds*

The University of Western Australia

Abstract. We consider the task of model building and model checking for temporal logic specifications over general linear flows of time.

We present a new notation for giving a detailed description of the compositional construction of such a model and an efficient procedure for finding it from the temporal specification.

We then also present an algorithm for checking whether a particular temporal formula holds in a general linear model.

Applications include reasoning about distributed and concurrent systems, multi-agent systems, and understanding natural language.

1 Introduction

Temporal logic is a widely used formalism for reasoning about the correctness of hardware and software systems. For many applications there are good reasons to use a logic based on some sort of dense model of time rather than the traditional discrete natural numbers model and its standard temporal logic [Pnu77]. Examples include multi-agent systems, AI, concurrency and refinement.

In contrast to the solid understanding of the reasoning tasks for discrete time temporal logics, the development of techniques for working with continuous and more general linear flows of time have been rather patchy.

General Until and Since connectives were introduced in [Kam68] for use over various linear flows. We can make a variety of different but related logics by taking this temporal language and restricting the semantics to operate on certain classes of linear flows. Other connectives have been added when there is cause and we will look at the so-called Stavi connectives [GPSS80] later in this paper.

The most natural and well-established "indiscrete" temporal logic is RTL, propositional temporal logic over real-numbers time using Kamp's Until and Since connectives. We know from [Kam68] that, as far as defining properties is concerned, this logic is as expressive as the first-order monadic logic of the real numbers order, and so RTL is at least as expressive as any other standard temporal logic which could be defined over real-numbers time.

Reasoning in RTL is fairly well understood: complete, Hilbert-style axioms systems for RTL are given in [GH90] and [Rey92]. Satisfiability and validity in RTL is decidable [BG85]. However, the decision procedure in [BG85] uses Rabin's non-elementarily complex decision procedure for the second-order monadic

---

* The work was partially supported by the Australian Research Council.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 50–68, 2013.

logic of two successors, and so is far from practical. Furthermore, deciding validity in the equally expressive first-order monadic logic of the real order is a non-elementary problem [Sto74]. More recently, there has been some more positive news as [Rey10a] showed that deciding (validity or satisfiability in) RTL is PSPACE-complete.

Reasoning in other general linear logics is less well-understood although it has been shown recently [Rey10b] that many are in PSPACE including deciding the logic USLIN of Until and Since over the class of all linear flows of time.

Satisfiability checking is not the only reasoning task. The synthesis, or model building task is a harder problem than satisfiability checking. It requires an algorithm which can output a complete description of a specific model of the input formula, whenever the input formula is satisfiable. This paper reviews the recent first synthesis result for RTL from [FMDR12a] and then builds on that.

Towards this end, we first present a new suitable notation for describing models in a concrete way. The compositional approach first presented in detail in [FMDR12a] was hinted at in [Rey01], and traces back to pioneering work in [LL66] and [BG85]. It uses a small number of distinct operations for putting together a larger model from one or more smaller ones, or copies thereof. For example, the *shuffle* construct makes a new linear structure from a dense mixture of copies of a finite number of simpler ones. A good overview of the mathematics of linear orders may be found in [Ros82].

We introduce a formal model expression language for defining a model via these inductive operations. In fact, we first give a language for making general linear structures in this way and then define a restricted sub-language (the real model expression language) capable of specifying structures with the real number flow of time. Having a formal model building language opens up the possibility for workable definitions of such tasks as synthesis and model checking for real-flowed structures. It also allows us to formalise questions of expressibility and to assess the computational complexity of these reasoning tasks.

A theorem in [FMDR12a], echoing the earlier work of [LL66], [BG85] and others states that the real model expression language is able to describe some real-flowed model of every satisfiable RTL formula. The major novel contribution of the recent work is that an EXPTIME procedure is presented for finding the real model expression of a model from any given satisfiable RTL formula. EXPTIME is best possible. The real model expression tells us exactly how to construct a specific real-flowed model of the formula. This is our RTL synthesis result.

The current paper adds results in two new directions to [FMDR12a]. We show how techniques from [Rey10b] can be used to define general linear models inside real-flowed models (in a certain sense) and give us a synthesis result for general linear time. Furthermore, this works for the more expressive Stavi language.

The other new results concern the associated model checking problems for RTL and general linear time: yet another reasoning task. Given a model expression and a formula as input, decide whether or not that formula is true at some point in the model described by the expression. We sketch a model checking procedure for U, S over general linear time and say how it can be modified for RTL.

More details of the results to do with RTL from here were published in [FMDR12a] while full details of other proofs will be found in [FMDR12b].

In section 2 we present our main logics: RTL, USLIN, the Stavi logic and monadic logic. In section 3 we introduce the compositional approach to building linear models. In section 4 we remind ourselves of useful properties of mosaics from [Rey10a] and real-time synthesis from [FMDR12a]. In section 5 we build on the RTL results for USLIN. In section 6 we tackle the associated model checking problem before we conclude in section 7.

2 The Logics

In this section we will introduce the several main logics that we will be considering: RTL, USLIN. L(U,S,U',S')/LIN and the monadic logic of order.

Fix a countable set $\mathbf{L}$ of atoms. Here, frames $(T, <)$, or flows of time, will be irreflexive linear orders. Structures $\mathbf{T} = (T, <, h)$ will have a frame $(T, <)$ and a valuation h for the atoms i.e. for each atom $p \in \mathbf{L}$, $h(p) \subseteq T$. Of particular importance will be *real* structures $\mathbf{T} = (\mathbb{R}, <, h)$ which have the real numbers flow (with their usual irreflexive linear ordering).

The language $L(U, S)$ is generated by the 2-place connectives U and S along with classical $\neg$ and $\wedge$. That is, we define the set of formulas recursively to contain the atoms and for formulas α and β we include $\neg\alpha$, $\alpha \wedge \beta$, $U(\alpha, \beta)$ and $S(\alpha, \beta)$.

Formulas are evaluated at points in structures $\mathbf{T} = (T, <, h)$. We write $\mathbf{T}, x \models \alpha$ when α is true at the point $x \in T$. This is defined recursively as follows. Suppose that we have defined the truth of formulas α and β at all points of $\mathbf{T}$. Then for all points x:

$$
\begin{array}{ll}
\mathbf{T}, x \models p & \text{iff } x \in h(p), \text{ for } p \text{ atomic;} \\
\mathbf{T}, x \models \neg\alpha & \text{iff } \mathbf{T}, x \not\models \alpha; \\
\mathbf{T}, x \models \alpha \wedge \beta & \text{iff both } \mathbf{T}, x \models \alpha \text{ and } \mathbf{T}, x \models \beta; \\
\mathbf{T}, x \models U(\alpha, \beta) & \text{iff there is } y > x \text{ in } T \text{ such that } \mathbf{T}, y \models \alpha \text{ and for all } z \in T \\
 & \quad \text{such that } x < z < y \text{ we have } \mathbf{T}, z \models \beta; \text{ and} \\
\mathbf{T}, x \models S(\alpha, \beta) & \text{iff there is } y < x \text{ in } T \text{ such that } \mathbf{T}, y \models \alpha \text{ and for all } z \in T \\
 & \quad \text{such that } y < z < x \text{ we have } \mathbf{T}, z \models \beta.
\end{array}
$$

In most of the literature on temporal logics for discrete time, the "until" connective is written in an infix manner: $\beta U \alpha$ rather than $U(\alpha, \beta)$. This corresponds to the natural language reading "I will be here until I become hungry" rather than our alternative "until I am hungry, I will be here". We choose to use the prefix notation for until (and since) because it agrees with important previous work on the language for dense time such as [Kam68], [BG85] and [GHR94] and because the infix until connective seen with discrete time is usually a slightly different connective, the non-strict until connective which we mention below.

The language is discussed more fully in [Rey03], [Rey10a] and [Rey09], for example. See those references for investigations of the "strict" versus "non-strict" connectives, infix versus postfix operators, various abbreviations, etc.

We use the following abbreviations in illustrating the logic: $F\alpha = U(\alpha, \top)$, "alpha will be true (sometime in the future)" ; $G\alpha = \neg F(\neg\alpha)$, "alpha will always hold (in the future)"; and their mirror images P and H. Particularly for dense time applications we also have: $\Gamma^{+}\alpha = U(\top, \alpha)$, "alpha will be constantly true for a while after now"; and $K^{+}\alpha = \neg\Gamma^{+}\neg\alpha$, "alpha will be true arbitrarily soon". They have mirror images Γ^{-} and K^{-}.

2.1 RTL

A formula ϕ is $\mathbb{R}$-*satisfiable* if it has a real model: i.e. . there is a real structure $\mathbf{S} = (\mathbb{R}, <, h)$ and $x \in \mathbb{R}$ such that $\mathbf{S}, x \models \phi$. A formula is $\mathbb{R}$-*valid* iff it is true at all points of all real structures. Of course, a formula is $\mathbb{R}$-valid iff its negation is not $\mathbb{R}$-satisfiable. We will refer to the logic of L(U,S) over real structures as RTL.

Let RTL-SAT be the problem of deciding whether a given formula of $L(U, S)$ is $\mathbb{R}$-satisfiable or not. The main result of [Rey10a] is:

Theorem 1. *RTL-SAT is PSPACE-complete.*

In order to help get a feel for the sorts of formulas which are valid in RTL it is worth considering a few formulas in the language. $U(\top, \bot)$ is a formula which only holds at a point with a discrete successor point so $G\neg U(\top, \bot)$ is valid in RTL. $Fp \rightarrow FFp$ is a formula which can be used as an axiom for density and is also a validity in RTL.

$(\Gamma^{+}p \wedge F\neg p) \rightarrow U(\neg p \vee K^{+}(\neg p), p)$ was used as an axiom for Dedekind completeness (in [Rey92]) and is valid. Recall that a linear order is Dedekind complete if and only if each non-empty subset which has an upper bound has a least upper bound. The formula says that if p is true constantly for a while but not forever then there is an upper bound on the interval in which it remains true. This formula is not valid in the temporal logic with until and since over the rational numbers flow of time.

One of the most interesting valid formulas of RTL is Hodkinson's axiom "Sep" (see [Rey92]). It is

$$K^{+}p \wedge \neg K^{+}(p \wedge U(p, \neg p)) \rightarrow K^{+}(K^{+}p \wedge K^{-}p).$$

This can be used in an axiomatic completeness proof to enforce the *separability* of the linear order:

Definition 1. *A linear order is separable iff it has a countable suborder which is spread densely throughout the order: i.e. between every two elements of the order lies an element of the suborder.*

The fact that the rationals are dense in them shows that the reals are separable. There are dense, Dedekind complete linear orders with end points which are not separable (eg, see [Rey92]). The negation of Sep will be satisfiable over them but not over the reals.

As we have noted in the introduction, there are complete axiom systems for RTL in [GH90] and in [Rey92]: the former using a special rule of inference and the latter just using orthodox rules.

Rabin's decision procedure for the second-order monadic logic of two successors [Rab69] is used in [BG85] to show that RTL is decidable. One of the two decision procedures in that paper just gives us a non-elementary upper bound on the complexity of RTL-SAT.

2.2 USLIN

If we use the $L(U, S)$ language over the class LIN of all linear structures, instead, then we obtain the logic which we will call USLIN. This has been axiomatised by Burgess in [Bur82] and shown to be decidable in PSPACE by Reynolds in [Rey10b].

2.3 Stavi Connectives

The question of a temporal language for general linear time is important here. We will see shortly that it is appropriate to use the expressively complete *Stavi* language [GPSS80, GHR94] with connectives $\{U, S, U', S'\}$ which we will shortly define.

First, we need to define gaps in a linear order and say where they fit into the order.

Definition 2. *A* gap γ *in a linear order* $(T, <)$ *is a set* $\gamma \subseteq T$ *such that: 1)* $\gamma \neq T$*; 2) for all* $t \in T$*, for all* $s \in \gamma$*, if* $t < s$ *then* $t \in \gamma$*; 3) for all* $t \in \gamma$ *there is* $s \in \gamma$ *such that* $t < s$*; and 4) for all* $t \in T \setminus \gamma$ *there is* $s \in T \setminus \gamma$ *such that* $s < t$*.*

If γ is a gap in $(T, <)$ and $t \in T$ then we may extend the $<$ operator by applying it to gaps as well and also write $t < \gamma$ iff $t \in \gamma$ and write $\gamma < t$ iff $t \in T \setminus \gamma$. If γ and δ are gaps in $(T, <)$ then we write $\gamma \leq \delta$ iff $\gamma \subseteq \delta$.

Stavi U': $U'(p, q)$ holds now if there is a gap in the future such that 1) q holds constantly between now and the gap, 2) q is false arbitrarily soon after the gap and 3) p is constantly true for a while after the gap. See the diagram Figure 1.

To define the semantics formally in the most direct way we need to use a subset of the linear order to define the "gap". So $(T, <, h), t \models U'(\alpha, \beta)$ iff there is a subset $\gamma \subseteq T$ such that $t \in \gamma$, for all $r < s \in T$, if $s \in \gamma$ then $r \in \gamma$; $T \setminus \gamma$ is non-empty; for all $s \in \gamma$, if $t < s$ then $(T, <, h), s \models \beta$; for all $s \notin \gamma$, there is $r \notin \gamma$ such that $t < r$ and $(T, <, h), r \not\models \beta$; and there is some $r \notin \gamma$ such that $t < r$ and for all $s \in T$, if $s \notin \gamma$ and $s < r$ then $(T, <, h), s \models \alpha$.

We also have the past, *since*, version, S' of U', i.e., with past and future swapped. Definitions and results obtained by swapping past and future are usually called *mirror images*.

Despite involving a gap, U' is in fact a first-order connective and its table is given by:

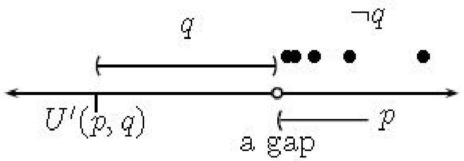


Fig. 1. A typical Stavi Until situation

$$
\begin{array}{l}
\alpha_{U'(p,q)}(t) = \\
\exists s \quad (t < s) \\
\quad \wedge \forall u(t < u < s \rightarrow \\
\qquad (\quad [\, \exists v(u < v \wedge \forall w(t < w < v \rightarrow Q(w))] \\
\qquad \quad \vee [\quad \forall v(u < v < s \rightarrow P(v)) \\
\qquad \qquad \wedge \exists v(t < v < u \wedge \neg Q(v))])) \\
\quad \wedge \exists u \; [\; t < u < s \wedge \neg Q(u)] \\
\quad \wedge \exists u \; [\; t < u < s \wedge \forall v(t < v < u \rightarrow Q(v))]
\end{array}
$$

That this is so is left as an exercise.

2.4 Monadic Logic

The first-order monadic language of order, FOMLO, is a first order language which can describe the structures we are dealing with and it is useful to translate between it and the temporal language.

The relation symbols of FOMLO are 2-ary $<$ and 1-ary, or monadic, P_0, P_1, P_2, ... each corresponding respectively to the atoms $p_0, p_1, p_2, \ldots$ of L. So atomic propositions are $x_i < x_j$ and $P_k(x_j)$ for each variable symbol x_i and each 1-ary relation symbol P_k. Formulas of the language are built up from the atoms as follows: $\neg\alpha$, $\alpha \wedge \beta$, and $\forall x_i \alpha$.

The notions of free and bound variables and sentences are as usual.

Given a temporal structure $(T, <, g)$ we can evaluate monadic formulas in it by interpreting the 1-ary predicates P_i as 1-ary relations on (i.e. subsets of) T using the valuation $g(p_i)$ to tell us where the interpretation of P_i holds as follows:

$(T, <, g), \mu \models P_i(x_j)$ iff $t_j \in g(p_i)$
$(T, <, g), \mu \models x_i < x_j$ iff $t_i < t_j$
$(T, <, g), \mu \models \neg\alpha$ iff it is not the case that $(T, <, g), \mu \models \alpha$
$(T, <, g), \mu \models \alpha_1 \wedge \alpha_2$ iff $(T, <, g), \mu \models \alpha_1$ and $(T, <, g), \mu \models \alpha_2$
$(T, <, g), \mu \models \forall x_i \alpha$ iff for every $d \in T$, $(T, <, g), \mu[x_i \mapsto d] \models \alpha$

Here μ is a (possibly partial) map from $\{x_1, x_2, \ldots\}$ to T and $\mu[x_i \mapsto d]$ is the map which is the same as μ except that x_i is mapped to d. We require that μ is defined on all the free variables of α. The truth of $(T, <, g), \mu \models \alpha$ does not depend on the value of $\mu(x_i)$ if x_i is not free in α.

Definition 3. *We say that the temporal language $L(B)$ is* expressively complete *over class K of linear orders iff for every FOMLO formula $\alpha(t)$, there is some ϕ of the temporal language such that ϕ is equivalent to α over K.*

Kamp showed in [Kam68] that $L(U, S)$ is expressively complete over $\mathbb{R}$ and over $\mathbb{N}$.

An expressive completeness result for the Stavi language over the class LIN of all linear orders was announced in [GPSS80] but detailed proofs can be found in [GHR94].

Theorem 2. *The temporal language with connectives $\{U, S, U', S'\}$ is expressively complete over the class of all linear orders.*

Thus, each formula of the first-order monadic language of order with one free time variable, has an equivalent expression in the Stavi language, a formula true at exactly the same times in any linear model. This also means that any formula of any usual temporal logic which can be defined over linear temporal structures can be easily translated into an equivalent formula in the Stavi language. See [Rey10b] for details.

Here we should also briefly mention a stronger monadic logic, the Monadic Second-oder logic, MSO, which has also played a role in this area: in this extension we can qualify over the monadic predicates.

3 Building Structures

We introduce a notation which allows the description of a temporal structure in terms of simple basic structures via a small number of ways of putting structures together to form larger ones.

The general idea is simple: using singleton structures (the flow of time is one point), we build up to more complex structures by the recursive application of four operations. They are:

- concatenation or sum of two structures, consisting of one followed by the other;
- ω repeats of some structure laid end to end towards the future;
- ω repeats laid end to end towards the past;
- and making a densely thorough *shuffle* of copies from a finite set of structures.

These operations are well-known from the study of linear orders (see, for example, [BG85]).

Model Expressions (MEs) are an abstract syntax to define models that are constructed using the follow set of primitive operators:

$$\mathcal{I} ::= \ a \in 2^{\mathbf{L}} \mid \Lambda \mid \mathcal{I} + \mathcal{J} \mid \overleftarrow{\mathcal{I}} \mid \overrightarrow{\mathcal{I}} \mid \langle \mathcal{I}_0, ..., \mathcal{I}_n \rangle$$

We refer to these operators, respectively, as *a letter*, *the empty order*, *concatenation*, *lead*, *trail*, and *shuffle*.

We relate MEs to structures via a simple relation called *correspondence* which we define inductively in a straightforward way, given the intuitions for the operators:

Definition 4. *[Correspondence] A model expression $\mathcal{I}$* corresponds *to a structure as follows:*

- *Λ is the empty sequence and corresponds to the empty structure, $(\emptyset, <, h)$ where $<$ and h are empty relations.*
- *a corresponds to any single point model $(\{x\}, <, h)$ where $<$ is the empty relation and $h(p) = x$ if and only if $p \in a$.*

The inductive cases:

- *$\mathcal{I} + \mathcal{J}$ corresponds to a structure $(T, <, h)$ if and only if T is the disjoint union of two sets U and V where $\forall u \in U$, $\forall v \in V$, $u < v$ and $\mathcal{I}$ corresponds to $(U, <^U, h^U)$ and $\mathcal{J}$ corresponds to $(V, <^V, h^V)$. ($<^U, h^U$ refers to the restriction of the relations $<$ and h to apply only to elements of U).*
- *$\overleftarrow{\mathcal{I}}$ corresponds to the structure $(T, <, h)$ if and only if T is the disjoint union of sets $\{U_i | i \in \omega\}$ where for all i, for all $u \in U_i$, for all $v \in U_{i+1}$, $v < u$, and $\mathcal{I}$ corresponds to $(U_i, <^{U_i}, h^{U_i})$.*
- *$\overrightarrow{\mathcal{I}}$ corresponds to the structure $(T, <, h)$ if and only if T is the disjoint union of sets $\{U_i | i \in \omega\}$ where for all i, for all $u \in U_i$, for all $v \in U_{i+1}$, $u < v$, and $\mathcal{I}$ corresponds to $(U_i, <^{U_i}, h^{U_i})$.*
- *$\langle \mathcal{I}_0, ..., \mathcal{I}_n \rangle$ corresponds to the structure $(T, <, h)$ if and only if T is the disjoint union of sets $\{U_i | i \in \mathbb{Q}\}$ where*
  1. *for all $i \in \mathbb{Q}$ $(U_i, <^{U_i}, h^{U_i})$ corresponds to some $\mathcal{I}_j$ for $j \leq n$,*
  2. *for every $j \leq n$, for every $a \neq b \in \mathbb{Q}$, there is some $k \in (a, b)$ where $\mathcal{I}_j$ corresponds to $(U_k, <^{U_k}, h^{U_k})$,*
  3. *for every $a < b \in \mathbb{Q}$ for all $u \in U_a$, for all $v \in U_b$, $u < v$.*

We will give an illustration of the non-trivial operations below. The *lead* operation, $\mathcal{I} = \overleftarrow{\mathcal{I}_1}$ corresponds ω submodels, each corresponding to $\mathcal{I}$, and each preceding the last, as illustrated in Figure 2.

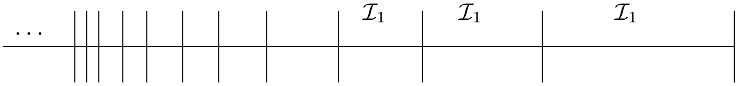


Fig. 2. The lead operation, where $\mathcal{I} = \overleftarrow{\mathcal{I}_1}$

The *trail* operator is the mirror image of the *lead* operation, whereby $\mathcal{I} = \overrightarrow{\mathcal{I}_1}$ corresponds to ω structures, each corresponding to $\mathcal{I}_1$ and each proceeding the earlier structures.

The *shuffle* operator is harder to represent with a diagram. The model expression $\mathcal{I} = \langle \mathcal{I}_1, \dots \mathcal{I}_m \rangle$ corresponds to a dense, thorough mixture of intervals corresponding to $\mathcal{I}_1, \dots, \mathcal{I}_n$, without endpoints. We define the shuffle operation using the rationals, $\mathbb{Q}$ as they are a convenient linear order with the required

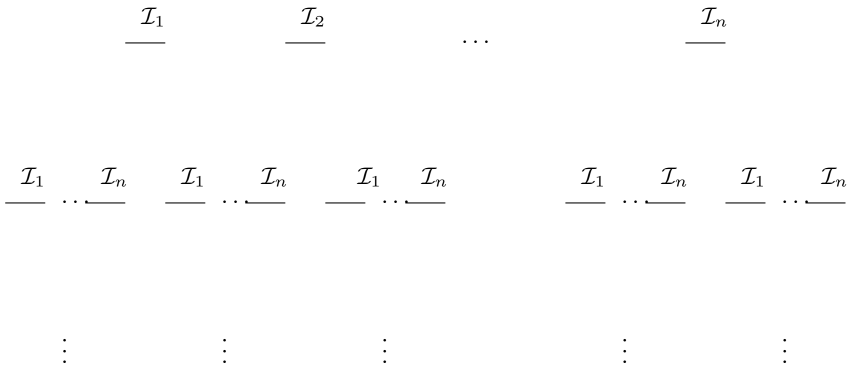


Fig. 3. The shuffle operation, where $\mathcal{I} = \langle \mathcal{I}_1, ..., \mathcal{I}_n \rangle$

properties. We will see below that and dense linear order is equivalent up to isomorphism for the purposes of the shuffle operator.

Model expressions give us a grammar whose elements correspond to general linear structures in a similar manner to the way regular expressions match words over a given alphabet. The definition of model expression correspondence is not deterministic: each particular expression corresponds to each member of an isomorphism class of structures. Furthermore, the construct for the shuffle $\langle \mathcal{I}_1, ..., \mathcal{I}_n \rangle$ does not specify how the structures corresponding to $\mathcal{I}_1, ..., \mathcal{I}_n$ are mapped to the rationals. As the mapping is dense for each i from 1 to n, the resulting structures will be isomorphic.

To start with, our particular interest in this paper are frames that are isomorphic to the real numbers. A simple argument via the Löwenheim-Skolem theorem, tells us that any formula satisfiable in a real-framed structure is also satisfiable in a countable structure. Further, our model expressions can describe such a countable model of a formula. However, for an RTL synthesis procedure we need a way of describing a real-flowed model of a given formula: one in which the underlying frame is the real numbers themselves. To address this we:

1. (non-deterministically) define a Dedekind closure of a structure; and
2. show that there is a sublanguage of model expressions that correspond to dense, separable structures without endpoints, which agree with their Dedekind closures on the interpretation of $L(U, S)$ formulas.

As every real valued structure is isomorphic to a dense, separable, Dedekind complete structure without end-points, and vice-versa (see [Rey92]) this is sufficient to justify the use of model expressions as the base artifact for synthesis and model checking results.

To define a sublanguage of separable, dense structures without endpoints, we must address the fact that some of the operators of model expressions, such as concatenation, naturally imply a discrete gap in the linear order. We build *real model expressions (RMEs)* via induction using the definitions above:

$$\mathcal{R} ::= \langle a_0, ..., a_m, \mathcal{R}_1, ..., \mathcal{R}_n \rangle \mid \mathcal{R}_0 + a + \mathcal{R}_1 \mid \overleftarrow{a + \mathcal{R}} \mid \overrightarrow{\mathcal{R} + a}$$

where $a, a_i \in 2^{\mathbf{L}}$, and $m, n \geq 0$. The letter a_0 is used as a sort of background filler to ensure that the shuffle is Dedekind complete. The abstract syntax for real model expressions is a direct sub-language for the abstract syntax for general model expressions. We note that their syntax will always define open intervals and that the base element of this recursion is a shuffle containing only points. This will define a dense, separable linear order with all the letters homogeneously distributed across the linear order.

Such a sublanguage is suggested in [BG85] where similar refinements of the [LL66] operations were applied to provide a decidability result for the monadic theory of the reals. The following lemma is suggested by that work. See [FMDR12b] for details.

Lemma 1. *Every real model expression corresponds to some structure whose frame is dense, separable and without end-points.*

It is important to note that the corresponding structures are *not* based on a real frame. In fact, any structure corresponding to a model expression $\mathcal{I}$ must be countable and therefore cannot be isomorphic to the reals. However, we will show this is sufficient for our purposes as every formula that is satisfied by a structure over the reals, is satisfied by a structure over some dense separable Dedekind complete linear order.

To address this we define a *Dedekind* closure of a structure, and show that any model corresponding to a real model expression agrees with its Dedekind closures on the interpretation of $L(U, S)$ formulae.

Definition 5. *Given a structure* $\mathbf{T} = (T, <, h)$*, we say that a gap* γ *is* curable *iff for all* $s < \gamma < t$ *there are* $u, v \in T$ *such that* $s < u < \gamma < v < t$ *and for all* $p \in \mathbf{L}$*,* $u \in h(p)$ *iff* $v \in h(p)$*.*

If every gap in $\mathbf{T}$ *is curable, a* Dedekind closure *of* $\mathbf{T}$ *is a structure* $\mathbf{T}^* = (T \cup X, <^*, h^*)$ *where:*

1. X *is a set of new points, one for each Dedekind gap of* $\mathbf{T}$*,*
2. $<^*$ *is the extension of* $<$ *such that the new point corresponding to each gap is in the right place in the order;*
3. h^* *is the extension of* h *such that for each new point* x*,* p *holds at* x *iff* p *holds at points of* T *arbitrarily closely on each side of* x*.*

Note that not every structure has a Dedekind closure. However, we have defined real model expressions in such a way that they guarantee that every Dedekind gap will be curable, and furthermore, the cure will not affect the interpretation of any formula.

Lemma 2 ([FMDR12b]). *Every structure agrees with its Dedekind closures on the interpretation of $L(U,S)$ formulae, i.e. at every point of the structure, every formula true (or false) there in the original structure, is true (or false, respectively) there in the Dedekind closure.*

Finally we must show that every real model expression corresponds to some real valued structure.

Lemma 3. *Every structure corresponding to a real model expression is dense, separable, without endpoints and agrees with it's Dedekind closure on the interpretation of $L(U,S)$ formulae.*

Proof. We can see every structure, **T**, corresponding to a real model expression has a Dedekind closure by construction. Every concatenation, lead and trail operation in a real model expression explicitly includes a single point between the two sub-expressions, so the only place a Dedekind gap may occur is in the shuffle operation. As every shuffle must include at least one single point structure, and the shuffle is dense, then there is a dense set of points in a structure corresponding to the shuffle, where each point has a consistent context. These points can be used to cure all Dedekind defects in **T** without affecting the interpretation of any $L(U,S)$ formulae. From Lemma 1 we have that **T** is dense separable and without end-points so the result follows.

It is straightforward to make the notation completely formal in the case of a finite set of atoms, and this is the case when we are considering a particular temporal formula. For example, let $[p, \neg q]$ represent a singleton structure with the obvious valuation. We might then suggest $\langle([p,q])\rangle + [p,q] + \langle([p,q],[p,\neg q])\rangle + [p,q] + \langle([p,q])\rangle$, as a model expression for $Gp \wedge U(q, \neg U(q,\neg q) \wedge \neg U(q,q))$.

Definition 6. *We say that a real-flowed structure* $(\mathbb{R}, <, h)$ *is a* compositional real structure *(or* model*) iff it is isomorphic to the Dedekind closure of a structure which corresponds to some real model expression. In that case, we say that it* realizes *the expression.*

Thus, a compositional real structure is real-flowed by definition. Note also that the real model expression tells us exactly what the model looks like (up to isomorphism).

An important result from [FMDR12a] is that an RTL formula has a real-flowed model iff it has a compositional real model. In the next section we briefly describe the proof which uses the mosaic technique for temporal logics.

Before we do so it may be worth noting that there is a similar sort of result in [BG85] where it is shown that an RTL formula has a real-flowed model iff it has a model with the valuation of each atom being a Borel set, i.e. one obtained from open sets by iterated application of complementation and countable union.

The second half of that paper [BG85] presents a series of operations corresponding to those of the real model expressions, to show the decidability of the monadic theory of the reals.

In other related work, [Thom86], it is shown how Rabin's result, that a satisfiable MSO-formula over trees is satisfied by a regular tree, generates what are essentially model expressions for orders which satisfy the formula.

The important advantages of our new result over these previous results, are that we provide an explicit notation that is adequate for representing real structures, we are able to give a finite representation in this notation for a model that supports a given satisfiable $L(U, S)$ formula, and we are able to give an efficient means for finding it.

4 Mosaics and Synthesis for *U* and *S* over the Reals

Much of the hard work for us is done by a theorem showing that deciding RTL is in PSPACE [Rey10a]. There, we decided the satisfiability of formulas by considering sets of small pieces of real structures. The idea is based on the mosaics seen in [Nem95] and applied to modal logics. Satisfiability can be decided by checking to see if there exists a finite set of mosaics sufficient to build a model of the formula.

For us, a mosaic is a small piece of a model consisting of three sets of formulas representing those true at each of two points (called the start and end of the mosaic) and those true at all points in-between (called the cover of the mosaic). There are *coherence* conditions on the mosaic which are necessary for it to be part of a model. Note that in the context of a particular formula, ϕ say, (whose satisfiability we might be investigating) we can limit our attention to a finite closure set of formulas and so make these mosaics finite in size. The set of subformulas of ϕ and their negations are a sufficient closure set and will be denoted Clϕ.

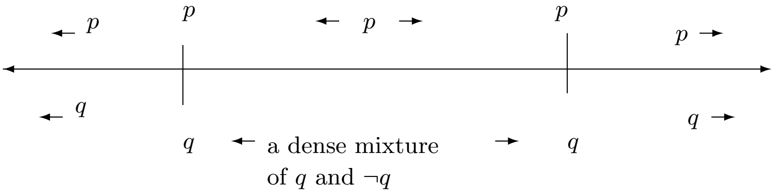


Fig. 4. Diagram representing: $\langle([p, q])\rangle + [p, q] + \langle([p, q], [p, \neg q])\rangle + [p, q] + \langle([p, q])\rangle$

The main result from [FMDR12a], built on top of the mosaic proof, is that we can use the recursively closed nature of the set (or RMS) of mosaics to describe a model in our new notation.

Theorem 3. *A formula ϕ from $L(U, S)$ is $\mathbb{R}$-satisfiable iff there is a compositional real model of ϕ. There is some c such that, in that case, a model can be described by an expression of shuffles, leads, trails and sums of length $< 2^{c|\phi|^2}$ (this bound is best possible).*

Furthermore, there is an EXPTIME procedure for finding such an expression.

Note that thanks to the expressive completeness result in [Kam68], we know that any satisfiable sentence of the first-order monadic logic of the reals also has a compositional real model. To find a description of a model from the sentence must be a hard problem as deciding validity in this logic is non-elementarily complex [Sto74]. One could use the separation technique of [GHR94] to first find an equivalent temporal formula and then use the procedure above. The translation to the temporal formula may be a time-consuming process.

Other results from [Rey10a] allow us to conclude that if we find all possible starting points (i.e. relativized mosaics in the RMS) and follow all possible ways of decomposing the mosaics (as given in the RMS) then we will eventually output a list of possible models of the formula which is in a certain sense exhaustive. Any real model of ϕ will be back-and-forth equivalent to one of the compositional models which is listed.

5 General Linear Time

In this section we leverage off the synthesis result (Theorem 3) for the reals and show how to obtain a synthesis procedure for general linear time.

To do this, we show that if a temporal formula has a general linear model then a closely related RTL formula has a real-flowed model which is closely related to a linear model of the original formula. We will show that a model expression for a general linear model of the original temporal formula can be easily extracted from the real model expression for a model of the RTL formula. Many things are left to be defined below but the idea is that the translation from the original formula into RTL is quite straightforward as is the translation between the model expressions.

In order to translate between results about general linear orders and results about the reals, we use the idea seen in [GHR94, Rey10b] of indicating a more general linear structure as a subset of a real-structure by using an extra atom to say which times belong to the substructure.

Thus we define a map $\alpha \mapsto \alpha^c$ from $L(U, S, U', S')$ to $L^c(U, S)$ (i.e. the temporal language built using U and S from a set of propositions being $L \cup \{c\}$ where c is some atom c not from L).

This map is intended to evaluate the Stavi connectives on a linear order which is the sub-order of the reals identified by the atom c. However, we will not see the map in action until lemma 4 below when we have some more machinery defined.

We could define the desired translation directly recursively but due to the desire to keep the translation in PTIME and to limit the size of the resulting formula, we work with fresh atoms only on the subformulas of the one formula we are interested in.

Suppose that we wish to translate α of $L(U, S, U', S')$. Let $cl(\alpha) = \{\beta \in L(U, S, U', S') | \beta \leq \alpha\}$ be the *closure set* of α that is the set of all subformulas of α. The size of this set will be at most the length of α.

The translation ρ will be defined only on the formulas in $cl(\alpha)$. For each formula $\beta \in cl(\alpha)$ in turn, choose a new atom $p_\beta \in L$ not used in α and not used already.

We define $\rho(\beta)$ as follows:

$$\begin{aligned}
\rho(p) &= c \wedge p \\
\rho(\neg\beta) &= c \wedge \neg(p_\beta) \\
\rho(\beta \wedge \gamma) &= c \wedge p_\beta \wedge p_\gamma \\
\rho(U(\beta, \gamma)) &= c \wedge U(c \wedge p_\beta, c \rightarrow p_\gamma) \\
\rho(S(\beta, \gamma)) &= c \wedge S(c \wedge p_\beta, c \rightarrow p_\gamma)
\end{aligned}$$

For U', it is a bit more complicated as we have to allow for *long gaps*, that is, extended intervals of constant $\neg c$.

Thus we put $\rho(U'(\beta, \gamma)) = c \wedge U(\neg c \wedge (\delta_1 \vee \delta_2), c \rightarrow p_\gamma)$ where $\delta_1 = \Gamma^+(c \rightarrow p_\beta) \wedge K^+(c \wedge \neg p_\gamma)$ and $\delta_2 = U(\neg c \wedge \delta_1, \neg c)$.

$\rho(S')$ is the mirror image.

Now just put $\alpha^c = p_\alpha \wedge \bigwedge_{\beta \in cl(\alpha)} GH(p_\beta \leftrightarrow \rho(\beta))$, where G and H are abbreviations for those connectives in $L(U, S)$.

Definition 7. *If* $(\mathbb{R}, \leq, g)$ *is a structure then* $(g(c), \leq, g|_L)$ *is the structure as follows.*

The domain is $g(c)$ *the set of points from* $\mathbb{R}$ *where the atom* c *holds in* $(\mathbb{R}, \leq, g)$.

The ordering $\leq$ *on* $g(c)$ *is just inherited from standard* $\leq$ *on* $\mathbb{R}$.

The atom p *from* L *(so not including* c*) is true (under* $g|_L$*) at* $t \in g(c)$ *iff* $t \in g(p)$.

Lemma 4. *Any* α *of* $L(U, S, U', S')$ *is satisfiable in a linear model iff* α^c *is satisfiable in the reals.*

Furthermore, if α^c *is true in* $(\mathbb{R}, \leq, g)$ *then* α *is true in* $(g(c), \leq, g|_L)$.

Proof. Say that α is satisfiable in some linear order. By Löwenheim-Skolem applied to the first-order equivalent of α there is a countable model of α. Furthermore, via a back and forth argument we can suppose that the flow of time is a subset of the rationals, and thus also of the reals.

Make a real-structure $(\mathbb{R}, \leq, g)$ to include that structure as a substructure. Make c true at the points of the substructure. Make all the normal atoms true just where they are true in the substructure.

By induction on the construction of formulas in $\mathrm{Cl}(\alpha)$ we can show, for all $x \in g(c)$, $(\mathbb{R}, \leq, g), x \models \beta^c$ iff $(g(c), \leq, g|_L), x \models \beta$.

Consideration of the length of the formulas used in our construction of α^c gives us a simple polynomial bound on its length in terms of the length of α.

Lemma 5. *The length of* α^c *is at most* $120|\alpha|$ *and* α^c *can be computed in polynomial time in the length of* α.

Given a formula ϕ of $L(U, S, U', S')$. We have defined ϕ^c. Using the RTL synthesis result we can get a real model expression $\mathcal{I}$ for a real-flowed model $(\mathbb{R}, <, g)$ of

ϕ^c. If we look at the submodel $(g(c), <, g|_L)$ where c is true then we will have a model for the original ϕ. It remains to see if we can find a general model expression for the submodel of an RME where c is true.

First, we define a translation from MEs to MEs:

Definition 8. *Say $\mathcal{I}$ is a real model expression in which the letters are $\Sigma = \wp(L \cup \{c\})$.*

Define translation τ recursively as follows:
$\tau(a) = a \setminus \{c\}$ *(if $c \in a$)*
$\tau(a) = \Lambda$ *(if $c \notin a$)*
$\tau(\mathcal{I} + \mathcal{J}) = \tau(\mathcal{I}) + \tau(\mathcal{J})$
$\tau(\overleftarrow{\mathcal{I}}) = \overleftarrow{\tau(\mathcal{I})}$
$\tau(\overrightarrow{\mathcal{I}}) = \overrightarrow{\tau(\mathcal{I})}$
$\tau(\langle \mathcal{I}_0, ..., \mathcal{I}_n \rangle) = \langle \tau(\mathcal{I}_0), ..., \tau(\mathcal{I}_n) \rangle$

Then a fairly straightforward but messy proof by induction on the construction of $\mathcal{I}$ allows us to prove the following lemma.

Lemma 6. *Suppose that $\mathcal{I}$ is a real model expression in which the letters are $\Sigma = \wp(L \cup \{c\})$.*

Suppose $(T, <, g)$ corresponds to $\mathcal{I}$.

Then $(g(c), \leq, g|_L)$ corresponds to $\tau(\mathcal{I})$.

Details of the proof are in [FMDR12b].

Thus we can now put together our synthesis result for general linear time.

Theorem 4. *There is an EXPTIME procedure which given a formula ϕ from $L(U, S, U', S')$ will decide whether ϕ is satisfiable in a linear model or not, and if so, will provide a model expression corresponding to a model of ϕ.*

Proof. Given ϕ, use the RTL synthesis algorithm (above) to try to find a model expression $\mathcal{I}$ such that there is a real-flowed model $(\mathbb{R}, <, g)$ of ϕ^c which realises $\mathcal{I}$.

RTL synthesis makes its decision in exponential time.

If there is no real-flowed model of ϕ^c then ϕ is not satisfiable in any linear order (by Lemma 4 above).

If there is a real model of ϕ^c then the algorithm finds $\mathcal{I}$ such that there is a real-flowed model $(\mathbb{R}, <, g)$ of ϕ^c which realises $\mathcal{I}$. We thus know that there is a linear model $(T, <, g)$ which corresponds to $\mathcal{I}$ and which is a model of ϕ^c. Now compute $\tau(\mathcal{I})$.

By Lemma 6 and Lemma 4 this will be a model expression for a linear model of ϕ as required.

6 Model Checking

In this section we will define a model checking procedure:

Definition 9. *We define the* model checking problem *as follows: given an ME* $\mathcal{I}$ *and formula* ϕ *of L(U,S), determine whether there exists a structure* $\mathbf{T} = (T, <, h)$ *and point* $x \in T$ *such that* $\mathbf{T}, x \vDash \phi$*.*

At a high level the model checking procedure uses the traditional approach of iteratively replacing formulas with atoms. The result of adding a formula α as an atom to an ME $\mathcal{I}$ is "add_atom$_\alpha$ $(\mathcal{I})$" which will be defined later in this section.

Definition 10. *The* model checking procedure *takes as input an ME* $\mathcal{I}$ *and formula* ϕ*. We enumerate the subformulas* $\phi_1, \ldots, \phi_n$ *of* ϕ *from shortest to longest (so* $\phi_n = \phi$*). We let* $\mathcal{I}_0 = \mathcal{I}$*, and let* $\mathcal{I}_i =$ *add_atom*$_{\phi_i}$ $(\mathcal{I}_{i-1})$ *for each* $i \in \{0, \ldots, n\}$*. We return "true" if there exists a letter* a *within* $\mathcal{I}_n$ *such that* $\phi \in a$*, and "false" otherwise.*

It is common to define the model checking problem as determining whether a formula ϕ is true at a given point. To solve this variation of the problem, with our model checking procedure, we can add a special atom t_0 and model check the formula $t_0 \rightarrow \phi$.

Since add_atom is only used on formulas where all subformulas have been replaced with atoms, we only need to consider the following forms: $p \wedge q$, $\neg p$, $U(p, q)$ and $S(p, q)$. We define add_atom$_{p \wedge q}$ $(\mathcal{I})$ as being the ME that results when each letter within $\mathcal{I}$ that contains both p and q has $p \wedge q$ added and likewise we define add_atom$_{\neg p}$ $(\mathcal{I})$ as being the ME that results when each letter within $\mathcal{I}$ that does not contain p has $\neg p$ added. We will now consider the less simple case of $U(p, q)$ and $S(p, q)$.

Given any Boolean $\dashv$ and an ME $\mathcal{K}$ we will now define a Boolean $\mathrm{pre}(\mathcal{K}, \dashv)$. Say that $\mathcal{K}$ corresponds to an interval $\mathbf{T}_\mathcal{K}$ of $\mathbf{T}$. Informally, $\dashv$ represents whether $U(p, q)$ would be true at a point added immediately after $\mathbf{T}_\mathcal{K}$, and $\mathrm{pre}(\mathcal{K}, \dashv)$ represents whether $U(p, q)$ would be true at a point added immediately prior to $\mathbf{T}_\mathcal{K}$. In the proof of correctness this will be formalised in terms of presatisfaction.

Definition 11. *We define a function "pre" from Booleans and MEs to Booleans such that: for any Boolean* $\dashv$ *and pair of MEs* $\mathcal{I}, \mathcal{J}$

1. $\mathrm{pre}(\mathcal{I} + \mathcal{J}, \dashv) = \mathrm{pre}(\mathcal{I}, \mathrm{pre}(\mathcal{J}, \dashv))$
2. $\mathrm{pre}\left(\overrightarrow{\mathcal{I}}, \dashv\right) = \mathrm{pre}(\mathcal{I}, \dashv)$
3. $\mathrm{pre}(a, \dashv) = p \in a \vee (\dashv \wedge q \in a)$
4. $\mathrm{pre}(\mathcal{J}, \dashv) = (\dashv \vee \exists l \in L(\mathcal{J}) \text{ s.t. } p \in l) \wedge \forall l \in L(\mathcal{J}), q \in l$; where $\mathcal{J}$ is of the form $\overleftarrow{\mathcal{I}}$ or $\langle \ldots \rangle$ and $L(\mathcal{J})$ is the set of letters within $\mathcal{J}$.

Note that for any $\mathcal{I}$ and $\dashv$ it is the case that $\mathrm{pre}(\mathcal{I}, \dashv) = \mathrm{pre}(\mathcal{I}, \mathrm{pre}(\mathcal{I}, \dashv))$. This may make the definition of add_atom$_{U(p,q)}$ below easier to understand.

Definition 12. *We define add_atom*$_{U(p,q)}$ $(\mathcal{I})$ *as* $t(\mathcal{I}, \bot)$*: where* t *is a function that takes an ME and a Boolean as input, and outputs an ME as follows: for any Boolean* $\dashv$ *and pair of MEs* $\mathcal{I}, \mathcal{J}$

1. $t(\mathcal{I} + \mathcal{J}, \dashv) = t(\mathcal{I}, \text{pre}(\mathcal{J}, \dashv)) + t(\mathcal{J}, \dashv)$
2. $t\left(\overleftarrow{\mathcal{I}}, \dashv\right) = \overleftarrow{t(\mathcal{I}, \text{pre}(\mathcal{I}, \dashv))} + t(\mathcal{I}, \dashv)$
3. $t\left(\overrightarrow{\mathcal{I}}, \dashv\right) = \overrightarrow{t(\mathcal{I}, \text{pre}(\mathcal{I}, \dashv))}$
4. $t(\mathcal{K}, \dashv) = \langle t(\mathcal{I}_0, \dashv'), \ldots, t(\mathcal{I}_n, \dashv')\rangle$ where $\mathcal{K} = \langle \mathcal{I}_0, \ldots, \mathcal{I}_n\rangle$
   and $\dashv' = \text{pre}(\mathcal{K}, \dashv)$
5. $t(a, \dashv) = \{\, a$ if $\neg \dashv$
   $a \cup \{U(p,q)\}$ if $\dashv$

Note that $t\left(\overleftarrow{\mathcal{I}}, \dashv\right)$ unwinds an $\mathcal{I}$ out of the $\overleftarrow{\mathcal{I}}$. This important because, in an ME such as $\overleftarrow{\{p,q\}}$ we have $U(p,q)$ true everywhere except the rightmost point and so when we add $U(p,q)$ as an atom we want to get $\overleftarrow{\{p,q,U(p,q)\}} + \{p,q\}$; not $\overleftarrow{\{p,q,U(p,q)\}}$ which has $U(p,q)$ even at the rightmost point, nor $\overleftarrow{\{p,q\}}$ which does not have $U(p,q)$ true anywhere.

As the Since operator is simply the mirror image of the Until operator, it is easy to similarly define $\text{add\_atom}_{S(p,q)}(\mathcal{I})$.

The full details of the model checking procedure will be presented in a future paper currently in preparation. Correctness is shown:

Theorem 5. *Given an ME $\mathcal{I}$ and formula ϕ, the model-checking procedure halts, and it returns* true *iff there exists a structure $\mathbf{T} = (T, < h)$ and point $x \in T$ such that $\mathcal{I}$ corresponds to $\mathbf{T}$ and $\mathbf{T}, x \models \phi$.*

A prototype implementation is already available at
`http://www.csse.uwa.edu.au/∼mark/research/Online/mechecker.html`.

The complexity is similar to that of model-checking LTL. Adding atoms has a simple recursive definition. However, each time we process an Until each $\overleftarrow{\mathcal{I}}$ is replaced with something of the form $\overleftarrow{\mathcal{I}_0} + \mathcal{I}_1$. After u Until operators have been processed this gives us something of the form $\overleftarrow{\mathcal{I}_0} + \mathcal{I}_1 + \cdots + \mathcal{I}_n$, potentially increasing the size of the ME $n+1$ times. With nested Untils (and/or Sinces) the ME can expand to size of order $|\mathcal{I}|\,\phi^{|\mathcal{I}|}$. Note though that the size of this ME is largely due to duplicated submodels. By storing and processing each unique submodel only once we get an algorithm that requires only time and space of order $\mathcal{O}\left(|\mathcal{I}||\phi|\,2^{|\phi|}\right)$. Like the commonly used model checker [HKV96] for LTL, this is linear in the length of the model and singly exponential in the length of the formula. By not storing the model generated we can produce a simple polynomial space (though inefficient) algorithm, and we can get PSPACE-completeness from a reduction from Quantified Boolean Form ulas. The basis of this reduction is to take a sequence of MEs such that $\mathcal{I}_i = \overleftarrow{\{p_i\} + \mathcal{I}_{i-1}} + \{q_i\}$, replace the i^{th} atom r_i in a prenex normal form QBF with $U(p_i, \neg q_i)$, iteratively replace the quanfiers as follows: replace $\forall r_i \psi_{i-1}$ with $U(q_i, p_i \to \psi_{i-1})$ and replace $\exists r_i \psi_{i-1}$ with $\neg\left(U\left(q_i, \neg\left(p_i \wedge \psi_{i-1}\right)\right)\right)$.

This model checking procedure can be used over the reals (when we limit ourselves to RMEs) or general linear flows. To get expressive completeness over general linear flows, we can translate the Stavi connectives using a special atom to represent "gaps" in the reals as in the previous section.

7 Conclusion

We have investigated a compositional approach to building linear temporal structures as a way of working with models on general linear flows of time. Structures are built by putting together smaller structures in a recursive way, with copies of the smaller ones occupying successive intervals of time. We have formalised the approach so that such models can be described clearly and efficiently.

We have identified a sub-language of the formal compositional model building language which can be used (in a slightly modified way) to build real-flowed structures. Any RTL formula satisfiable in the reals is satisfiable in such a compositional real-flowed model. We presented an efficient method for building a real-flowed model of any given a satisfiable formula.

Building on that result we have also given a general linear synthesis result. Given a formula of the expressive Stavi language, or its U, S sublanguage, we can decide whether it is satisfiable over linear time, and, if so, output a compositional model expression for a particular model of the formula.

In a separate result we have also introduced a model checking procedure for general linear time. The inputs are a model expression, describing a structure, and a temporal formula. The procedure decides whether that formula is true anywhere in the structure. This seems to be the first such procedure.

Future work includes model building constructions for important sub-classes of linear flows, such as dense ones, or for example just $\{\mathbb{Z}\}$. We also want to provide publicly usable implementation of our model checker.

References

[BG85] Burgess, J.P., Gurevich, Y.: The decision problem for linear temporal logic. Notre Dame J. Formal Logic 26(2), 115–128 (1985)

[Bur82] Burgess, J.P.: Axioms for tense logic I: "Since" and "Until". Notre Dame J. Formal Logic 23(2), 367–374 (1982)

[FMDR12a] French, T., McCabe-Dansted, J., Reynolds, M.: Synthesis for temporal logic over the reals. In: AiML 2012, pp. 217–238 (2012)

[FMDR12b] French, T., McCabe-Dansted, J., Reynolds, M.: Synthesis for general linear time (submitted, 2012)

[GH90] Gabbay, D.M., Hodkinson, I.M.: An axiomatisation of the temporal logic with until and since over the real numbers. Journal of Logic and Computation 1(2), 229–260 (1990)

[GHR94] Gabbay, D.M., Hodkinson, I.M., Reynolds, M.: Temporal Logic: Mathematical Foundations and Computational Aspects, vol. 1. Oxford University Press (1994)

[GPSS80] Gabbay, D.M., Pnueli, A., Shelah, S., Stavi, J.: On the temporal analysis of fairness. In: 7th ACM Symposium on Principles of Programming Languages, Las Vegas, pp. 163–173 (1980)

[HKV96] Henzinger, T.A., Kupferman, O., Vardi, M.Y.: A Space-Efficient on-the-Fly Algorithm for Real-time Model Checking. In: Sassone, V., Montanari, U. (eds.) CONCUR 1996. LNCS, vol. 1119, pp. 514–529. Springer, Heidelberg (1996)

[Kam68] Kamp, H.: Tense logic and the theory of linear order. PhD thesis, University of California, Los Angeles (1968)

[LL66] Läuchli, H., Leonard, J.: On the elementary theory of linear order. Fundamenta Mathematicae 59, 109–116 (1966)

[Nem95] Németi, I.: Decidable versions of first order logic and cylindric-relativized set algebras. In: Csirmaz, L., Gabbay, D., de Rijke, M. (eds.) Logic Colloquium 1992, pp. 171–241. CSLI Publications (1995)

[Pnu77] Pnueli, A.: The temporal logic of programs. In: Proceedings of the Eighteenth Symposium on Foundations of Computer Science, pp. 46–57. Providence, RI (1977)

[Rab69] Rabin, M.O.: Decidability of second order theories and automata on infinite trees. American Mathematical Society Transactions 141, 1–35 (1969)

[Rey92] Reynolds, M.: An axiomatization for Until and Since over the reals without the IRR rule. Studia Logica 51, 165–193 (1992)

[Rey01] Reynolds, M.: Continuous Temporal Models. In: Stumptner, M., Corbett, D., Brooks, M.J. (eds.) AI 2001. LNCS (LNAI), vol. 2256, pp. 414–425. Springer, Heidelberg (2001)

[Rey03] Reynolds, M.: The complexity of the temporal logic with "until" over general linear time. J. Comput. Syst. Sci. 66(2), 393–426 (2003)

[Rey09] Reynolds, M.: Dense time reasoning via mosaics. In: TIME 2009: Proceedings of the 2009 16th International Symposium on Temporal Representation and Reasoning, pp. 3–10. IEEE Computer Society, Washington, DC (2009)

[Rey10a] Reynolds, M.: The complexity of the temporal logic over the reals. Annals of Pure and Applied Logic 161(8), 1063–1096 (2010), doi:10.1016/j.apal.2010.01.002

[Rey10b] Reynolds, M.: The complexity of temporal logics over linear time. Journal of Studies in Logic 3, 19–50 (2010)

[Ros82] Rosenstein, J.G.: Linear Orderings. Academic Press, New York (1982)

[Sto74] Stockmeyer, L.: The complexity of decision problems in automata and logic. PhD thesis, M.I.T (1974)

[Thom86] Thomas, W.: On frontiers of regular trees. RAIRO Theoretical Informatics and Applications 20, 371–381 (1986)

Probabilistic IF Logic

Gabriel Sandu

Department of Philosophy, University of Helsinki

1 Introduction

In a seminal paper Goldfarb (1979) points out that "The connection between quantifiers and choice functions or, more precisely, between quantifier-dependence and choice functions, is at the heart of how classical logicians in the twenties viewed the nature of quantification." (Goldfarb 1979, p. 357). For a less historical but more systematic point of view, Terence Tao (2007), notices that we know how to render in first-order logic statements like:

1. For every x, there exists a y *depending on* x such that $B(x, y)$ is true

and

2. For every x, there exists a y *independent of* x such that $B(x, y)$ is true

The first one can be rendered by

$$\forall x \exists y B(x, y)$$

and the second one by

$$\exists y \forall x B(x, y).$$

(Here $B(x, y)$ is a binary relation holding of two objects x, y). Things become more complicated when four quantifiers and a ternary relation $Q(x, x', y, y')$ are involved. We can express in first-order logic statements like

3. For every x and x', there exists a y depending only on x and a y' depending on x and x' such that $Q(x, x', y, y')$ is true

and

4. For every x and x', there exists a y depending on x and x' and a y' depending only on x' such that $Q(x, x', y, y')$ is true

by

$$\forall x \exists y \forall x' \exists y' Q(x, x', y, y')$$

and

$$\forall x' \exists y' \forall x \exists y Q(x, x', y, y')$$

respectively. However, one cannot always express the statement

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 69–79, 2013.

5. For every x and x', there exists a y depending only on x and a y' depending only on x' such that $Q(x, x', y, y')$ is true.

His conclusion is that

> It seems to me that first order logic is limited by the linear (and thus totally ordered) nature of its sentences; every new variable that is introduced must be allowed to depend on all the previous variables introduced to the left of that variable. This does not fully capture all of the dependency trees of variables which one deals with in mathematics. (Tao, 2007)

2 Independence-Friendly Logic

Independence-friendly logic (IF logic), introduced in Hintikka and Sandu (1989), is intended to represent patterns of dependence and independence of quantifiers like those exemplified by 5 which go beyond those expressible in ordinary first-order logic. More exactly, the syntax of IF logic contains quantifiers of the form

$$(\exists x/W)\ (\forall x/W)$$

where W is a finite set of variables. The intended interpretation of $(\exists x/W)$ is: the existential quantifier $\exists x$ is independent of the quantifiers which bind the variables in W. The notion of independence involved here is a game-theoretical one and corresponds to the mathematical notion of uniformity. The example (5) above will be rendered in the new formalism by:

$$\forall x \forall x' (\exists y/\{x'\})(\exists y'/\{x, y\})Q(x, x', y, y').$$

Here are few examples from the mathematical literature which involve the new quantifiers.

The continuity of a function $f : \mathbb{R} \rightarrow \mathbb{R}$ is expressed by the sentence

$$\forall x \forall \epsilon \exists \delta \forall y[\mid x - y \mid < \delta \rightarrow \mid f(x) - f(y) \mid < \epsilon].$$

In this case the value of δ depends on both the value of x and the value of ϵ but is independent of the value of y.

However it turns that for certain functions f the value of δ does not depend on the value of x. In this case we say that f is *uniformly continuous*. The uniform continuity of f is captured by the IF sentence

$$\forall x \forall \epsilon (\exists \delta / x) \forall y[\mid x - y \mid < \delta \rightarrow \mid f(x) - f(y) \mid < \epsilon].$$

This sentence is (truth-) equivalent (under the interpretation to be given below) to the first-order sentence

$$\forall \epsilon \exists \delta \forall x \forall y[\mid x - y \mid < \delta \rightarrow \mid f(x) - f(y) \mid < \epsilon].$$

However, as pointed out by Tao, it is not always so that an IF-formula is equivalent to an ordinary first-order formula. Here is one example out of many (cf. Mann, Sandu, and Sevenster, 2011).

An *involution* is a function f that satisfies $f(f(x)) = x$, for all x in its domain. A finite structure has an even number of elements if and only if there is a way of pairing the elements without leaving any element out, i.e., if there exists an involution without a fixed point. Let φ_{even} be the IF sentence

$$\begin{gathered}\forall x \forall y (\exists u/\{y\})(\exists v\{x, u\}) \\ [(x = y \to u = v) \wedge (u = y \to v = x) \wedge u \neq x].\end{gathered}$$

The truth of this sentence turns out to be equivalent with that of a second-order sentence which asserts the existence of a function f such that

$$\forall x[f(f(x)) = x \wedge f(x) \neq x].$$

In other words, φ_{even} is true if and only if there is a function f which is an involution without a fixed point.

The original interpretation of IF formulas in Hintikka and Sandu (1989) and Hintikka (1996) is given by semantical games of imperfect information. An alternative, equivalent interpretation is by skolemization. Mann, Sandu and Sevenster (2011) establishes the equivalence of all interpretations. We shall adopt here the interpretation by Skolem functions.

3 Truth in IF Logic

Let φ be a formula of IF logic in a given vocabulary L and U a finite set of variables which contains the free variables of φ. We expand the vocabulary L of φ to $L^* = L \cup \{f_\psi : \psi \text{ is a subformula of } \varphi\}$. The skolemized form or skolemization of φ with variables in U is defined by the following clauses:

$Sk_U(\psi) = \psi$, for ψ an atomic subformula of φ or its negation
$Sk_U(\psi \circ \theta) = Sk_U(\psi) \circ Sk_U(\theta)$, for $\circ \in \{\vee, \wedge\}$
$Sk_U((\forall x/W)\psi) = \forall x Sk_{U \cup \{x\}}(\psi)$
$Sk_U((\exists x/W)\psi) = Subst(Sk_{U \cup \{x\}}(\psi), x, f_{\exists x}(y_1, ..., y_n))$

where $y_1, ..., y_n$enumerate all the variables in $U - W$. We notice that if $W = \varnothing$ the last clause becomes

$$Sk_U((\exists x)\psi) = Subst(Sk_{U \cup \{x\}}(\psi), x, f_{\exists x}(y_1, ..., y_n))$$

where $y_1, ..., y_n$enumerate all the variables in U. That is, we recover the notion of skolemization for the standard quantifiers. We abbreviate $Sk_\varnothing(\varphi)$ by $Sk(\varphi)$. An interpretation of $f_{\exists x}(y_1, ..., y_n)$ is called a *Skolem function.*

For an example, the Skolem form of φ_{even} is

$$\begin{gathered}\forall x \forall y \\ [(x = y \to f(x) = g(y)) \wedge (f(x) = y \to g(y) = x) \wedge f(x) \neq x].\end{gathered}$$

Let φ be an L-sentence of IF logic and $\mathbb{M}$ an L-structure. We say that φ *is true* in $\mathbb{M}$, $\mathbb{M} \models^{+} \varphi$, if and only if there exist functions $g_1, ..., g_n$ of appropriate arity in M to be the interpretations of the new function symbols $f_{x_1}, ..., f_{x_n}$in $Sk(\varphi)$ such that

$$\mathbb{M}, g_1, ..., g_n \models Sk(\varphi).$$

4 Falsity in IF Logic

In order to deal with falsity, we shall define another translation procedure, $Kr_U(\varphi)$:

$Kr_U(\psi) = \neg\psi$, for ψ an atomic subformula or its negation
$Kr_U(\psi \vee \theta) = Kr_U(\psi) \wedge Kr_U(\theta)$,
$Kr_U(\psi \wedge \theta) = Kr_U(\psi) \vee Kr_U(\theta)$
$Kr_U((\exists x/W)\psi) = \forall x Kr_{U\cup\{x\}}(\psi)$
$Kr_U((\forall x/W)\psi) = Subst(Kr_{U\cup\{x\}}(\psi), x, f_{\forall x}(y_1, ..., y_m)$

where $y_1, ..., y_m$ are all the variables in $U - W$. We call the value of interpretation of $f_{\forall x}(y_1, ..., y_m))$ a *Kreisel counter-example.*

By analogy with the truth definition, we stipulate that an IF sentence φ is false in a structure $\mathbb{M}$, $\mathbb{M} \models^{-} \varphi$ if and only if there exist functions $h_1, ..., h_m$ of appropriate arity in M to be the interpretations of the new function symbols $f_{x_1}, ..., f_{x_m}$in $Kr(\varphi)$ such that

$$\mathbb{M}, h_1, ..., h_m \models Kr(\varphi).$$

5 Expressive Power

Here we give another example of an IF sentence which is not first-order definable. It will be used later on. A set M is (Dedekind) infinite iff there is a function $h : M \to M$ which is an injection and in adition there is an element in M which is not the the image under h of any element of M. The IF sentence φ_{inf}

$$\exists w \forall x (\exists y/\{w\})(\exists z/\{w, x\})(x = z \wedge w \neq y)$$

defines the infinity of the underling domain. The Solem form of φ_{inf} is

$$\forall x(x = g(f(x)) \wedge c \neq f(x))$$

and its Kreisel form is

$$\forall w \forall y \forall z(h(w) \neq z \vee w = y).$$

It can be checked that φ_{inf} is true in a model iff the function f is an injection which range is not the entire universe. On the other side, if $\mathbb{M}$ is finite, it can be checked that we have both $\mathbb{M} \not\models^{+} \varphi_{inf}$ and $\mathbb{M} \not\models^{-} \varphi_{inf}$.

An IF formula is in *Hintikka normal form* if it is in prenex normal form, every universal quantifier is superordinate to every existential quantifier, and all of its universal quantifiers are unslashed, i.e., it has the form

$$\forall y_1 ... \forall y_m (\exists y_{m+1}/W_{m+1}) ... (\exists y_n/W_n)\varphi$$

where φ is quantifier free. In Mann, Sandu and Sevenster (2011) it is shown that every IF sentence is (truth-) equivalent with an IF sentence which is in Hintikka normal form.

6 Model-Theoretical Properties

The *Compactness Theorem* which in its standard form holds that a theory Γ is satisfiable if every finite subtheory of Γ is satisfiable holds for IF logic. The proof is straightforward: when Γ is a set of IF sentences, it is enough to consider the set $\Gamma^* = \{Sk(\varphi) : \varphi \in \Gamma\}$.

However, there is a stronger version of compactness which holds in first-order logic but not in IF logic: every first-order theory $\Gamma \cup \{\varphi\}$ has the property that $\Gamma \models \varphi$ iff there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \models \varphi$. By contrast, there is an IF theory $\Gamma \cup \{\varphi\}$ for which we have $\Gamma \models^+ \varphi$ but $\triangle \not\models^+ \varphi$for every finite $\Delta \subseteq \Gamma$. It is enough to take Γ to be the infinite set of sentences $\{\varphi_n : n \geq n\}$ where each φ_i asserts that the universe contains at least i individuals, and φ to be the sentence φ_{inf}. From this it follows that there is no sound and semantically complete proof system for IF logic.

Craig's Interpolation Theorem says that φ is a first-order sentence in the vocabulary L and ψ' is a first-order sentence inthe vocabulary L' such that $\varphi \vDash \psi$ there is a first-order interpolant θ in the vocabulary $L \cap L'$ such that $\varphi \vDash \theta$and $\theta \vDash \psi$. We can use this theorem to prove a *Separation Theorem* for IF logic. We say that two IF sentences are *contraries* if there is no model in which they are both true. One can easily prove that any two IF sentences φ and ψ which are contraries can be separated by an ordinary first-order sentence, that is, there is a first-order sentence θ such that $\varphi \vDash^+ \theta$ and $\psi \vDash^+ \neg\theta$. Other model-theoretical properties are detailed in Mann, Sandu and Sevenster (2011).

7 Strategic IF Games

7.1 Indeterminacy

Consider the IF sentence $\varphi = \forall x(\exists y/\{x\})x = y$ and a finite structure $\mathbb{M}$ which contains at least two elements. This sentence is neither true nor false in $\mathbb{M}$. The most straightforward way to establish this is by considering its Skolem and Kreisel form:

$$Sk(\varphi) = \forall x x = c$$
$$Kr(\varphi) = \forall y \neg d = y.$$

Obviously there is no expansion of $\mathbb{M}$ which satisfies $Sk(\varphi)$ and no expansion of M which satisfies $Kr(\varphi)$.

We consider the set $S_\exists$ of Skolem functions of Eloise in $\mathbb{M}$, i.e. the set of all possible values of the function symbols of $Sk(\varphi)$. In this case, $S_\exists = \mathbb{M}$. We also consider the set $S_\forall$ of all possible Kreisel counter-examples in $\mathbb{M}$: In this case $S_\forall = \mathbb{M}$. We can now formulate a two player win-lose strategic game $\Gamma(\mathbb{M}, \varphi) = (\{\exists, \forall\}, S_\exists, S_\forall, u_\exists, u_\forall)$. The two players $\exists$ and $\forall$ choose simultaneously $s \in S_\exists$ and $t \in S_\forall$, respectively. The payoff of the outcome is determined in a very simple way: if s and t satisfy the equation $c = d$ in $\mathbb{M}$, then $\exists$ wins (1 euro). If they satisfy $\neg c = d$, $\forall$ wins. Here is the complete matrix of the game for the case in which $\mathbb{M} = \{1, 2, 3\}$:

	1	2	3
1	$(1,0)$	$(0,1)$	$(0,1)$
2	$(0,1)$	$(1,0)$	$(0,1)$
3	$(0,1)$	$(0,1)$	$(1,0)$

The rows represent the strategies of Eloise and the colums the strategies of Abelard. In (m, n), $m \in \{0, 1\}$ is the payoff of Eloise, i.e. $u_\exists(m, n) = m$, and n is the payoff for Abelard for the corresponding strategies.

It is interesting to compare this game to the one associated with $\psi = \forall x(\exists y/\{x\})x \neq y$ and $M = \{1, 2, 3\}$:

	1	2	3
1	$(0,1)$	$(1,0)$	$(1,0)$
2	$(1,0)$	$(0,1)$	$(1,0)$
3	$(1,0)$	$(1,0)$	$(0,1)$

Obviously the notion of strategic IF game can be generalized to every IF sentence φ and structure $\mathbb{M}$. Given a strategic IF game $\Gamma(\mathbb{M}, \varphi) = (\{\exists, \forall\}, S_\exists, S_\forall, u_\exists, u_\forall)$, $s' \in S_\exists$ and $t' \in S_\forall$, we say that (s', t') is an equilibrium in the game $\Gamma(\mathbb{M}, \varphi)$ if the following two conditions are fulfilled:

- $u_\exists(s', t') \geq u_\exists(s, t')$ for every $s \in S_\exists$
- $u_\forall(s', t') \geq u_\forall(s', t)$ for every $t \in S_\forall$

We can check that in our earlier strategic IF games $\Gamma(\mathbb{M}, \forall x(\exists y/\{x\})x = y)$ and $\Gamma(\mathbb{M}, \forall x(\exists y/\{x\})x \neq y)$ where $\mathbb{M} = \{1, 2, 3\}$, there are no equilibria.

We overcome the indeterminacy of such IF sentences by considering mixed strategy equilibria. The procedure is due to Sevenster (2006) and was fully explored in Mann, Sandu, and Sevenster (2011).

7.2 Mixed Strategies Equilibria in IF Games

There is an equilibrium in every IF game if, instead of pure strategies, we switch to mixed strategies. Let $\Gamma(\mathbb{M}, \varphi)$ be a finite IF strategic game. A mixed strategy ν for player i in this strategic game is a probability distribution over S_i, that is, a function $\nu : S_i \to [0, 1]$ such that $\sum_{\tau \in S_i} \nu(\tau) = 1$. ν is uniform over $S'_i \subseteq S_i$ if it assigns equal probability to all strategies in S'_i and zero probability to all the strategies in $S_i - S'_i$. Obviously we can simulate a pure strategy s with a mixed strategy ν such that ν assigns s probability 1. Given a mixed strategy μ for player $\exists$ and a mixed strategy ν for player $\forall$, the expected utility for player i is given by:

$$U_i(\mu,\nu) = \sum_{s\in S_\exists} \sum_{t\in S_\forall} \mu(s)\nu(t)u_i(s,t).$$

When $s \in S_\exists$ and ν is a mixed strategy for player $\forall$, we let

$$U_i(s,\nu) = \sum_{t\in S_\forall} \nu(t)u_i(s,t).$$

Similarly if $t \in S_\forall$ and μ is a mixed strategy for player $\exists$, we let

$$U_i(\mu,t) = \sum_{s\in S_\exists} \mu(s)u_i(s,t).$$

Von Neumann's well known *Minimax Theorem* shows that every finite, constant sum, two player game has an equilibrium in mixed strategies. It is also well known that every two equilibria in such a game returns the same expected utility to the two players. Thus we can talk about *the expected utility returned to player* $\exists$ by an IF strategic game. This justifies the next definition:

Definition. Let φ be an IF sentence and $\mathbb{M}$ a finite structure. When $0 \leq r \leq 1$ we define:
$\mathbb{M} \vDash_r^{eq} \varphi$ iff the expected utility returned to player $\exists$ by the strategic game $\Gamma(\mathbb{M},\varphi)$ is r.

Recall our earlier examples $\Gamma(\mathbb{M}, \forall x(\exists y/\{x\})x = y)$ and $\Gamma(\mathbb{M}, \forall x(\exists y/\{x\})x \neq y)$ where$\mathbb{M} = \{1,2,3\}$. In both cases the uniform strategies $\mu^*(1) = \mu^*(2) = \mu^*(3) = \frac{1}{3}$ and $\nu^*(1) = \nu^*(2) = \nu^*(3) = \frac{1}{3}$ form an equilibrium. The value of the first game is $\frac{1}{3}$ and that of the second game is $\frac{2}{3}$. Thus $\mathbb{M} \vDash_{\frac{1}{3}}^{eq} \forall x(\exists y/\{x\})x = y$ and $\mathbb{M} \vDash_{\frac{2}{3}}^{eq} \forall x(\exists y/\{x\})x \neq y$. A more complex argument shows that for $\mathbb{M}$ a finite model with n elements we have $\mathbb{M} \models_{\frac{n-1}{n}}^{eq} \varphi_{inf}$. Thus when n grows to infinity the value of φ_{inf} approaches 1, as desired.

The above definition gives us the (probabilistic) value of an IF sentence φ on a given finite structure $\mathbb{M}$. It can be shown that this interpretation is a conservative extension of the earlier interpretation:

Proposition. For every IF sentence φ and finite model $\mathbb{M}$ we have: $\mathbb{M} \vDash^+ \varphi$ iff $\mathbb{M} \vDash_1^{eq} \varphi$; and $\mathbb{M} \vDash^- \varphi$ iff $\mathbb{M} \vDash_0^{eq} \varphi$.

The next proposition is often useful for checking that a pair of mixed strategies is an equilibrium.

Proposition. Let μ^*be a is a mixed strategy for player $\exists$ and $\nu^*$is a mixed strategy for player $\forall$ in the strategic IF game Γ. The pair (μ^*,ν^*) is an equilibrium in Γ if and only if the following conditions hold:

1. $U_\exists(\mu^*, \nu^*) = U_\exists(\sigma, \nu^*)$ for every $\sigma \in S_\exists$ in the support of μ^*
2. $U_\forall(\mu^*, \nu^*) = U_\forall(\mu^*, \tau)$ for every $\tau \in S_\forall$ in the support of ν^*
3. $U_\exists(\mu^*, \nu^*) \geq U_\exists(\sigma, \nu^*)$ for every $\sigma \in S_\exists$ outside the support of μ^*
4. $U_\forall(\mu^*, \nu^*) \geq U_\forall(\mu^*, \tau)$ for every $\tau \in S_\forall$ outside the support of ν^*.

It is interesting to compare the probabilistic interpretation of IF logic with other probabilistic interpretations.

8 Statistical Information: Randomizing over Individuals

Bacchus (1990) and Halpern (1990), among others, analyze statements which express empirical generalizations like "20% of the provinces of Canada are west to Saskatchewan". Such generalizations further serve to justify statements which express proportions or relative frequencies like "The probability that a random chosen flies is greater than 0.9". It has been pointed out that the second statement is about a *chance set up*: given some statistical information (that 90% of the individuals in a population have property P), then we may imagine a chance set up in which a randomly chosen individual has probability 0.9 of having property P.

To analyze this kind of statements, Halpern, following Bacchus, considers an extension of first-order logic with formulas of the form $w_x(\varphi) \geq \frac{1}{2}$ to be interpreted as "the probability that a randomly chosen x in the domain satisfies φ is greater or equal to $\frac{1}{2}$". Here $w_x(\varphi)$ is a term, in which the variable x in φ is bound by the quantifier w_x. This formulation is extended to allow arbitrary sequences of distinct variables in the subscript.

Such statements are interpreted in probability structures, that is, triples (D, I, μ) where (D, I) is a first-order structure and μ is a discrete probability function on D. That is, μ is a mapping from D to the real interval $[0, 1]$ such that $\sum_{d \in D} \mu(d) = 1$. For any $A \subseteq D$ one defines: $\mu(A) = \sum_{d \in A} \mu(d)$. Given such a probability function μ one can then define a discrete probability function μ^n on D^n by letting

$$\mu^n(d_1, ..., d_n) = \mu(d_1) \times ... \times \mu(d_n).$$

The evaluation of formulas in probability structures follows the standard lines. The clause which interests us is:

- $[w_{(x_1,...,x_n)}(\varphi)]_{M,v} = \mu^n(\{(d_1, ..., d_n) : (M, v[x_1/d_1, ..., x_n/d_n]) \models \varphi\})$

We write $M \models \varphi$ if $(M, v) \models \varphi$ for all valuations v.

Both Bacchus and Halpern consider issues of axiomatizability that will not interest me in this paper. It is worth pointing out that the term $w_{\overrightarrow{x}}(\varphi)$ which expresses statistical randomness obeys the Kolmogorov probability axioms:

Ax1 $w_{\overrightarrow{x}}(\varphi) \geq 0$
Ax2 $w_{\overrightarrow{x}}(\varphi) + w_{\overrightarrow{x}}(\neg\varphi) = 1$
Ax3 $w_{\overrightarrow{x}}(\varphi) + w_{\overrightarrow{x}}(\psi) \geq w_{\overrightarrow{x}}(\varphi \vee \psi)$
Ax4 $w_{\overrightarrow{x}}(\varphi \wedge \psi) = 0 \rightarrow w_{\overrightarrow{x}}(\varphi) + w_{\overrightarrow{x}}(\psi) = w_{\overrightarrow{x}}(\varphi \vee \psi)$

9 Degree of Belief: Randomizing over Possible Worlds

Both Bacchus (1990) and Halpern (1990) pointed out that unlike the statement "The probability that a random chosen flies is greater than 0.9" which expresses a fact about one (real) world, the statement "The probability that (the particular bird) Tweety flies is greater than 0.9" expresses a *degree of belief.* In other words, the second statement seems to implicitly assume a number of possibilities (possible worlds), in some of which Tweety flies, while in others it does not fly, and some probability distribution over these possibilities.

To analyze the second kind of statements, Halpern (1990) considers extensions of first-order languages with formulas of the form $w(Flies(Tweety)) \geq 0.9$. These are now interpreted on probability structures which have the form (D, S, π, μ), where D is a domain, S is a set of possible worlds, and for each $s \in S$, $\pi(s)$ assigns to the predicate and function symbols of the language predicates and functions of the right arity over D. μ is a discrete probability function on S. For emphais, we note that in the earlier section, the probability is taken over individuals, while in this case it is taken over possible worlds. The few clauses which interest us are:

- $(M, s, v) \vDash P(x)$ iff $v(x) \in \pi(s)(P)$
- $(M, s, v) \vDash \forall x\varphi$ iff $(M, s, v(x/d)) \vDash \varphi$ for each $d \in D$
- $[w(\varphi)]_{(M,v,s]} = \mu(\{s' \in S : (M, s, v) \models \varphi\})$

The "operator like" term $w(\varphi)$ which expresses the degree of belief in φ obeys, like his relative $w_{\overrightarrow{x}}(\varphi)$, the Kolmogorov probability axioms. When the probabilities are all 0 and 1, then the resulting probability logic reduces to ordinary logic. However, when φ is a sentence (closed formula), then for any vector $\overrightarrow{x}$ of distinct object variables we have

$$\models w_{\overrightarrow{x}}(\varphi) = 0 \vee w_{\overrightarrow{x}}(\varphi) = 1.$$

This means that a close sentence like *Flies(Tweety)* cannot take intermediate values between 0 and 1. Thus it is inconsistent in the context of the first approach to assert formulas like $0.95 \geq w_x(\varphi) \geq 0.9$. This is not any longer so in the possible world approach where $0.95 \geq w(Flies(Tweety)) \geq 0.9$ is perfectly consistent.

10 Randomizing over Strategies

We considered earlier an extension of first-order logic, IF logic, whose syntax contains sentences of the form

$$\begin{aligned}
\varphi_{MP} &= \forall x(\exists y/\{x\})x = y \\
\varphi_{IMP} &= \forall x(\exists y/\{x\})x \neq y \\
\varphi_{inf} &= \exists w\forall x(\exists y/\{w\})(\exists z/\{w, x\})(x = z \wedge w \neq y)
\end{aligned}$$

All these sentences, indetermined on finite structures, receive probabilistic values: the expected utility returned to $\exists$ by the relevant mixed strategy equilibrium. We can lift this interpretation into the syntax by extending IF languages with formulas of the form

$$NE(\varphi) = r$$

with the interpretation:

$$\mathbb{M} \vDash NE(\varphi) = r \Leftrightarrow \mathbb{M} \vDash_r^{eq} \varphi.$$

Thus, when $\mathbb{M} = \{1, ..., n\}$, we have

$$\begin{aligned} \mathbb{M} \vDash NE(\varphi_{MP}) &= {}^1/_n \\ \mathbb{M} \vDash NE(\varphi_{IMP}) &= {}^{n-1}/_n \\ \mathbb{M} \vDash NE(\varphi_{inf}) &= {}^{n-1}/_n. \end{aligned}$$

In Mann, Sandu and Sevenster (2011) it is shown that the following principles are valid

P1 $NE(\varphi \vee \psi) = max(NE(\varphi), NE(\psi))$
P2 $NE(\varphi \wedge \psi) = min(NE(\varphi), NE(\psi))$
P3 $NE(\neg\varphi) = 1 - NE(\varphi)$

Thus the probabilistic values of IF sentences obey the Kolmogorov probability axioms. Notice, however, that $NE(\varphi \vee \neg\varphi) = 1$ is not valid, but one should remember that $\neg\varphi$ is not always the contradictory of φ. For instance, when $\mathbb{M} = \{1, ..., n\}$

$$\mathbb{M} \vDash NE(\varphi_{MP}) = {}^1/_n$$

from which we get, by (P3)

$$\mathbb{M} \vDash NE(\neg\varphi_{MP}) = {}^{n-1}/_n.$$

Thus for $n > 2$

$$\mathbb{M} \vDash NE(\varphi_{MP} \vee \neg\varphi_{MP}) = {}^{n-1}/_n.$$

11 Conclusions

$w_{\overrightarrow{x}}(\varphi)$, $w(\varphi)$ and $NE(\varphi)$ obey all the Kolmogorov probability axioms. $w_{\overrightarrow{x}}(\varphi)$ expresses randomization over the individuals of a given domain, $w(\varphi)$ over possible worlds, and $NE(\varphi)$ over the verifying and falsifying strategies in a given domain. However, unlike $w_{\overrightarrow{x}}(\varphi)$ and $w(\varphi)$, $NE(\varphi)$ does not assume a prior probability distribution: the probabilistic distribution over the relevant strategies arises from the equilibrum in the underlying game.

One can reduce probability distributions over strategies to probability distributions over individuals in a domain in the sense of the following example.

Recall the Matching Pennies sentence $\varphi_{MP} = \forall x(\exists y/\{x\})x = y$ and the structure $\mathbb{M} = \{1, ..., n\}$. Recall that the value of the game is computed from the equilibrium (μ, ν) where μ and ν are the uniform probability distributions $\mu(i) = \nu(i) = 1/n$. Thus $\mathbb{M} \vDash NE(\varphi_{MP}) = 1/n$. The Skolem form of $\forall x(\exists y/\{x\})x = y$ is $\forall x(x = c)$. We replace the universal quantifier by w_x to obtain the sentence $w_x(x = c)$. Finally we form the model $(\mathbb{M}, c^M, \tau)$ where $c^M$is any arbitrary $c^M \in \{1, ..., n\}$ andτ is ν. The first clause of the last Proposition of section 7 ensures us that

$$U_\exists(c^M, \nu) = 1/n$$

It should be clear that

$$\begin{gathered} U_\exists(c^M, \nu) = \\ \nu(\{a : (M, c^M, \tau) \vDash (x = c)[a]\}) = \\ [w_x(x = c)]_{(M, c^M, \tau)}. \end{gathered}$$

References

1. Bacchus, F.: Lp, A Logic for Representing and Reasoning with Statistical Knowledge. Computational Intelligence 6, 209–231 (1990)
2. Cameron, P.J., Hodges, W.: Some combinatorics of imperfect information. Journal of Symbolic Logic 66, 673–684 (2001)
3. Halpern, J.Y.: An Analysis of First-Order Logics of Probability. Artificial Intelligence 46, 311–350 (1990)
4. Goldfarb, W.: Logic in the twenties: The nature of the quantier. Journal of Symbolic Logic 44, 351–368 (1979)
5. Hintikka, J.: Principles of Mathematics Revisited. Cambridge University Press, Cambridge (1996)
6. Hintikka, J., Sandu, G.: Informational independence as a semantic phenomenon. In: Fenstad, J.E., et al. (eds.) Logic, Methodology and Philosophy of Science, vol. 8, pp. 571–589. Elsevier, Amsterdam (1989)
7. Mann, A., Sandu, G., Sevenster, M.: Independence-Friendly Logic: A Game-theoretic Approach. Cambridge University Press (2011)
8. Sevenster, M., Sandu, G.: Equilibrium semantics of languages of imperfect information. Annals of Pure and Applied Logic 16, 618–631 (2010)
9. Sevenster, M.: Branches of Imperfect Information: Logic, Games, and Computation. PhD thesis, University of Amsterdam, Amsterdam (2006)
10. Tao, T.: Printer-friendly CSS, and nonfirstorderisability, in Terence Tao, What's new: Updates on my research and expository papers, discussion of open problems, and other maths related topics (2007)

Tableaux-Based Decision Method for Single-Agent Linear Time Synchronous Temporal Epistemic Logics with Interacting Time and Knowledge

Mai Ajspur[1] and Valentin Goranko[2]

[1] Roskilde University
`ajspur@ruc.dk`
[2] Technical University of Denmark and University of Johannesburg
`vfgo@imm.dtu.dk`

Abstract. Temporal epistemic logics are known, from results of Halpern and Vardi, to have a wide range of complexities of the satisfiability problem: from PSPACE, through non-elementary, to highly undecidable. These complexities depend on the choice of some key parameters specifying, inter alia, possible interactions between time and knowledge, such as synchrony and agents' abilities for learning and recall. In this work we develop practically implementable tableau-based decision procedures for deciding satisfiability in single-agent synchronous temporal-epistemic logics with interactions between time and knowledge. We discuss some complications that occur, even in the single-agent case, when interactions between time and knowledge are assumed and show how the method of incremental tableaux can be adapted to work in EXPSPACE, respectively 2EXPTIME, for these logics, thereby also matching the upper bounds obtained for them by Halpern and Vardi.

1 Introduction

Knowledge and time are among the most important aspects of agency. Various *temporal-epistemic logics*, proposed as logical frameworks for reasoning about these aspects of single- and multi-agent systems were actively studied in a number of publications during the 1980's, eventually summarized and uniformly presented in a comprehensive study by Halpern and Vardi [4]. In [4], the authors considered several essential characteristics of temporal-epistemic logics: *one vs. several agents*, *synchrony vs. asynchrony*, *(no) learning*, *(no) forgetting (aka, perfect recall or no recall)*, *linear vs. branching time*, and existence (or not) of a *unique initial state*. Based on these, they identified and analyzed a total of 96 temporal-epistemic logics and obtained lower bounds for the complexity of a satisfiability problem in them. In [5] matching upper bounds were claimed for all, and established for most of these logics. It turned out that most of the logics that involve more than one agents, *whose knowledge interacts with time* (e.g., who do not learn or do not forget) – are undecidable (with common knowledge), or

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 80–96, 2013.

decidable but with non-elementary time lower bound (without common knowledge). Even in the single-agent case the interaction between knowledge and time proved to be quite costly, pushing the complexities of deciding satisfiability up to EXPSPACE and 2EXPTIME. These complexity lower bounds were established in [4] and the matching upper bounds are claimed and proved for all synchronous cases in [5]. For the single-agent synchronous cases, these results follow from the non-elementary upper bounds for the multi-agent cases. However, we are not aware of *both optimal and practically implementable* decision methods developed for these logics so far (but, see further discussion on related work). By "practically implementable decision method" we mean one that would only hit the worst case complexity in 'really bad' cases – usually seldom occurring in practice – but would perform reasonably well in most of the practically occurring input instances, whereas a non-practically implementable method is one that essentially always – or, always when the answer is e.g., 'no' – would perform with the theoretically worst case complexity. For instance, the method of semantic tableau for testing tautologies in classical propositional logic is practically implementable, whereas the method using explicitly constructed truth-tables is not.

In this paper we develop such theoretically optimal and practically implementable (modulo the established complexities, of course) tableau-based procedures for deciding satisfiability in single-agent synchronous temporal-epistemic logics with interactions between time and knowledge, by building on the incremental tableau construction, described in [3] for both synchronous and asynchronous multi-agent temporal-epistemic logics with common and distributed knowledge, but with no interactions between time and knowledge (other than synchrony). The method developed there works in EXPTIME, which is the optimal complexity for the logics considered there. It was not clear whether and how that method could be adapted to produce optimal decision procedures for the cases of interacting time and knowledge, where complications arise even in the single-agent case. Here we discuss and illustrate these complications and then extend and adapt the incremental tableaux-based decision method to the single-agent case over linear time synchronous systems, for all cases of interaction between knowledge and time involving combinations of assumptions of 'no learning', 'no forgetting' and 'unique initial state', that are not easily covered by the tableau method from [3]. The basic procedure developed here works in 2EXPTIME and we describe in Section 7 how it is optimized to work in EXPSPACE, thereby also matching the EXPSPACE upper bounds obtained for these logics in [5]. For lack of space some of the technical details and proofs are omitted from this text and can be found in the technical report [1].

In order to delineate the contribution of this paper, we should put it in the context of related works. On the one hand, as discussed above, Halpern and Vardi have established in [5] theoretically optimal upper bounds (for the multi+agent cases), by means of essentially combinatorial estimates of the size of 'small' tree-like models satisfying models, but that proof is far from a practically implementable method as it requires enumerating and checking all models within the prescribed size. On the other hand, a non-optimal, yet apparently implementable tableau method for the cases of single-agent synchronous temporal-epistemic logics with no learning or with no forgetting is developed by Dixon et al in [2], where many of the concepts used here (states, pre-bubbles and bubbles, etc.) have close analogies. That method works by first transforming the input formula into a certain clausal normal form that employs a number of new atoms, used for renaming of subformulae, and then applying a tableau-like method to the resulting set. It uses double exponential space in the number of logical connectives (except negations) in the formula and does not cover the cases with unique initial state. A resolution based approach to the logics has been developed in [7], while [6] develops tableaux for first-order temporal logics, covering (under constant domain assumption) some single-agent temporal epistemic logics, too.

The tableau method developed here originates from the incremental tableaux, first developed by Pratt for PDL [8] and later by Wolper for LTL [9], and is an adaptation of the tableau for the linear time multi-agent temporal epistemic logic with no time-knowledge interaction in [3], to which we refer the reader for further references. Besides combining optimality and implementability, we believe that our tableau method is also somewhat more intuitive and more flexible and amenable to further extensions, incl. covering multi-agent logics and asynchrony.

2 Preliminaries

For lack of space, we only provide here the very basic preliminaries on the logics under consideration and on the incremental tableau method. For further details the reader is referred to [4], [5], [3].

2.1 The Single-Agent Linear Time Temporal Epistemic Logic $\mathsf{TEL}^1(\mathsf{LT})$

Syntax and Semantics. The language of $\mathsf{TEL}^1(\mathsf{LT})$ contains a set $\mathtt{AP}$ of atomic propositions, the Booleans $\neg$ ("not") and $\wedge$ ("and"), the temporal operators $\mathcal{X}$ ("next") and $\mathcal{U}$ ("until") of the logic LTL, as well as the epistemic operator $\mathbf{K}$. The formulas of $\mathsf{TEL}^1(\mathsf{LT})$ are defined as follows:

$$\varphi := p \mid \neg\varphi \mid (\varphi_1 \wedge \varphi_2) \mid \mathcal{X}\varphi \mid (\varphi_1 \,\mathcal{U} \varphi_2) \mid \mathbf{K}\varphi$$

where p ranges over $\mathtt{AP}$. All other standard Boolean and temporal connectives can be defined as usual. Formulas of the type $\mathbf{K}\varphi$ or their negations will be called *knowledge formulas* and formulas of the type $\mathcal{X}\varphi$, $\varphi_1 \,\mathcal{U}\varphi_2$ or their negations will be called *temporal formulas.* We omit parentheses when this does not result in ambiguity.

Definition 1 (Temporal-epistemic frames and models). *A* (single-agent) temporal-epistemic frame *(TEF) is a tuple* $\mathfrak{G} = (S, R, \mathcal{R})$*, where* S *is a non-empty set of* states*;* $R \subseteq S^{\mathbb{N}}$ *is a non-empty set of* runs*; and* $\mathcal{R} \subseteq (R \times \mathbb{N})^2$ *is an equivalence relation, representing the epistemic uncertainty of the agent. A* temporal-epistemic model *(TEM) is a tuple* $\mathcal{M} = (\mathfrak{F}, L)$*, where* $\mathfrak{F}$ *is a TEF and* $L : R \times \mathbb{N} \to \mathcal{P}(\mathtt{AP})$ *is a* labeling function*.*

We denote the set $R \times \mathbb{N}$ by $P(\mathfrak{S})$. An element $(r, n) \in P(\mathfrak{S})$ is called a *point*. We note that the points and not the states of a model are the elements of interest in a model, since both the epistemic relation and the labelling function are defined with respect to points and not states.

Truth and Satisfiability. Truth of formulas at a point of a TEM is defined recursively as usual, by combining the semantics for LTL and that of the standard epistemic logic:

$\mathcal{M}, (r, n) \Vdash \mathcal{X}\varphi$ iff $\mathcal{M}, (r, n + 1) \Vdash \varphi$;

$\mathcal{M}, (r, n) \Vdash \varphi\mathcal{U}\psi$ iff $\mathcal{M}, (r, i) \Vdash \psi$ for some $i \geq n$ such that $\mathcal{M}, (r, j) \Vdash \varphi$ for every $n \leq j < i$;

$\mathcal{M}, (r, n) \Vdash \mathbf{K}\varphi$ iff $\mathcal{M}, (r', n') \Vdash \varphi$ for every $((r, n), (r', n')) \in \mathcal{R}$;

A formula φ is *satisfiable* (resp., *valid*) if $\mathcal{M}, (r, n) \Vdash \varphi$ for some (resp., every) TEM M and a point (r, n) in it. Satisfiability and validity in a class of models is defined likewise.

Remark 1. Our definition of a temporal epistemic frame (and model) can obviously be extended to the multiagent case by including a relation $\mathcal{R}_a$ for all agents and extending the definition of truth and satisfiability in a model similarly. Note that in both the multi- and single agent case, our notion of temporal-epistemic model is somewhat more general than the semantical structure in [4] and [5], called an 'interpreted system'. In an interpreted system the (global) system states are tuples of local states of all agents, and runs are defined as functions from $\mathbb{N}$ to the set of global states. The epistemic relations in [4] and [5] are defined *between states, not between points*, although one could infer otherwise from the notation used there: $(r, n) \sim_a (r', n')$, but that means by definition $r(n) \sim_a r'(n')$, which again is defined to mean that the current local state of $r(n)$ and $r'(n')$ w.r.t. agent a is the same. Thus, every interpreted system as defined in [4] and [5] can obviously be redefined as a TEM in our sense, by lifting the epistemic relation from states to points. Our semantics, where runs are defined as more abstract entities, is mentioned in [4] and [5] too, and it is stated in these papers that the semantics are equivalent, but without providing arguments. This is true since every TEM $\mathcal{M}$ in our sense can be *transformed* into an equi-satisfiable interpreted system $\widehat{\mathcal{M}}$, where the local states for each agent are the respective equivalence classes of the points in $\mathcal{M}$. Then, for each run r in $\mathcal{M}$ a corresponding run r' in $\widehat{\mathcal{M}}$ is defined canonically, and the labeling from $\mathcal{M}$ is transferred canonically to $\widehat{\mathcal{M}}$. If there are no r and s in $\mathcal{M}$ for which $((r, n), (s, m)) \in \mathcal{R}_a$ for all agents, then there is a bijection between the runs in $\mathcal{M}$ and $\widehat{\mathcal{M}}$, and it is easy to show that satisfiability of formulas in $\mathcal{M}$ and $\widehat{\mathcal{M}}$ coincide. If there are such runs r and s one can do a 'trick', by adding a new starting point to each new run r' which is unique for r; these new starting points can then be labelled with $\emptyset$. Thus, the notions of satisfiability (at some point of a run in some model) in both semantics coincide.

2.2 Some Important Properties of Temporal-Epistemic Models

Definition 2 (Properties of TEF and TEM). *A TEF* $\mathfrak{S} = (S, R, \mathcal{R})$ *has the property of:*

- *Indistinguishable_Initial_States (iis), if for all runs* $r, r' \in R$*,* $((r, 0), (r', 0)) \in \mathcal{R}$*.*
- *No_Learning (nol), if whenever* $((r, n), (r', n')) \in \mathcal{R}$*, for every* $k \geq n$ *there exists a* $k' \geq n'$ *such that* $((r, k), (r', k')) \in \mathcal{R}$*.*
- *No_Forgetting (nof), if whenever* $((r, n), (r', n')) \in \mathcal{R}$*, for every* $0 \leq k \leq n$ *there exists a* $0 \leq k' \leq n'$ *such that* $((r, k), (r', k')) \in \mathcal{R}$*.*
- *Synchrony (sync), if* $((r, n), (r', n')) \in \mathcal{R}$ *implies* $n = n'$*.*

A TEM $\mathcal{M} = (\mathfrak{F}, L)$ *has the property of* $x \in \{\mathsf{nol}, \mathsf{nof}, \mathsf{sync}, \mathsf{iis}\}$ *if* $\mathfrak{F}$ *does so.*

The meaning of iis (corresponding to "unique initial state" in [4]) is clear; sync means that the agent can perceive time, i.e., has a clock; nol means that the agent does not learn over time in the sense that if it cannot distinguish two runs at any given time instance, it will not be able to do so later on. Likewise, nof means that if at a given time instance the agent can tell two different runs apart, the agent must have been able to do so at any previous time instance. We notice that if a TEF or TEM has the properties nol and iis, then it follows that it has the property nof too.

We denote the classes of all TEMs satisfying property $x \in \{\mathsf{nol}, \mathsf{nof}, \mathsf{sync}, \mathsf{iis}\}$ by TEM_x, and we further denote $\mathrm{TEM}_X = \bigcap_{x \in X} \mathrm{TEM}_x$ for $X \subseteq \{\mathsf{nol}, \mathsf{nof}, \mathsf{sync}, \mathsf{iis}\}$.

Extensions of $\mathsf{TEL}^1(\mathsf{LT})$. We denote the extension of the logic $\mathsf{TEL}^1(\mathsf{LT})$ with semantics restricted to the class TEM_X, by $\mathsf{TEL}^1(\mathsf{LT})_X$ for all $X \subseteq \{\mathsf{nol}, \mathsf{nof}, \mathsf{sync}, \mathsf{iis}\}$. Thus, validity/ satisfiability in $\mathsf{TEL}^1(\mathsf{LT})_X$ means validity/satisfiability in a model from TEM_X. In this paper we focus on the logics for synchronous models $\mathsf{TEL}^1(\mathsf{LT})_X$ (i.e. $\mathsf{sync} \in X$) and either $\mathsf{nol} \in X$ or $\mathsf{nof} \in X$. For convenience, we also denote $\mathsf{TEL}^1(\mathsf{LT}) = \mathsf{TEL}^1(\mathsf{LT})_\emptyset$ in cases where we want to emphasize that no interaction conditions are assumed.

Remark 2. The properties of sync, iis, nol and nof are all preserved when transforming a (single- or multi-agent) interpreted system into a model as in Remark 1. On the other hand, consider a (single- or multi-agent) model $\mathcal{M}$. If there are no two runs r and s in $\mathcal{M}$ such that $((r, n), (s, n)) \in \mathcal{R}_a$ for all agents a, then the transformation described in Remark 1 without the additional 'trick' preserves the properties of sync, uis, nol and nof. If there are such r and s, one can in most cases of combinations of the interaction properties perform suitable modifications that enable us to still find an equi-satisfiable interpreted system with the same interaction properties.

However, this is not the case for the single- or multiagent temporal epistemic logic with interaction properties X, where $X \in \{\ \{\mathsf{sync}, \mathsf{nol}, \mathsf{nof}\}, \{\mathsf{sync}, \mathsf{nol}, \mathsf{nof}, \mathsf{iis}\}, \{\mathsf{sync}, \mathsf{nol}, \mathsf{iis}\},\ \{\mathsf{sync}, \mathsf{nof}, \mathsf{iis}\}\ \}$. In these cases the two semantics differ, since e.g. the formula $\theta = p \wedge \neg\mathbf{K}_a p$ is satisfiable in our semantics, while it is unsatisfiable in the semantics presented in [4] and [5]. This is due to the fact that the interaction properties implies that if $\mathcal{M}, (r, n) \Vdash \theta$ for a point (r, n) in the interpreted system $\mathcal{M}$, then if $((s, n), (r, n)) \in \mathcal{R}_a$ then $((s, n'), (r, n')) \in \mathcal{R}_a$ for all n', and hence $r = s$ since R according to the definition is a *set* of runs. Thus we must have that $\mathcal{M}, (r, n) \Vdash p, \neg p$ which is a contradiction. Note, however, that the formula *is* satisfiable if e.g. the property sync is dropped.

3 Temporal Epistemic Hintikka Structures

Even though we are ultimately interested in testing formulas of $\mathsf{TEL}^1(\mathsf{LT})$ for satisfiability in a TEM, the tableau procedure we will present here tests for satisfiability in a more general kind of semantic structures, namely *temporal epistemic Hintikka structures* (TEHS). The important aspect of a Hintikka structure for a formula θ is that it contains just as much semantic information about the satisfying model of θ as it is necessary, and no more. More precisely, while a TEM provides the truth value of every formula of the language at every state, a Hintikka structure only determines the truth of formulas that are directly involved in the evaluation of the input formula θ.

Some terminology: we distinguish *conjunctive formulas*, also called $\curlywedge$*-formulas* and *disjunctive formulas*, also called $\curlyvee$-formulas, each with a respective set of components, as in the tables below:

$\curlywedge$-formula	Set of $\curlywedge$-components
$\neg\neg\varphi$	$\{\varphi\}$
$\varphi \wedge \psi$	$\{\varphi, \psi\}$
$\mathbf{K}\varphi$	$\{\mathbf{K}\varphi, \varphi\}$

$\curlyvee$-formula	Set of $\curlyvee$-components
$\neg(\varphi \wedge \psi)$	$\{\neg\varphi, \neg\psi\}$
$(\varphi \mathcal{U} \psi)$	$\{\psi, \varphi \wedge \mathcal{X}(\varphi \mathcal{U} \psi)\}$
$\neg(\varphi \mathcal{U} \psi)$	$\{\neg\psi \wedge \neg\varphi, \neg\psi \wedge \neg\mathcal{X}(\varphi \mathcal{U} \psi)\}$

It can be easily shown, that any $\curlywedge$-formula is equivalent to the conjunction of its $\curlywedge$-components, and that any $\curlyvee$-formula is equivalent to the disjunction of its $\curlyvee$-components.

Definition 3 (Fully expanded sets). *A set of formulae Δ of $\mathsf{TEL}^1(\mathsf{LT})$ is* fully expanded *if:*

1. *Δ is not* patently inconsistent, *i.e. if $\varphi \in \Delta$ then $\neg\varphi \notin \Delta$.*
2. *If $\alpha \in \Delta$ is a $\curlywedge$-formula, then all of its $\curlywedge$-components are in Δ,*
3. *If $\beta \in \Delta$ is a $\curlyvee$-formula, then at least one of its $\curlyvee$-components are in Δ,*

Definition 4 (Temporal Epistemic Hintikka Structure). *A* temporal-epistemic Hintikka structure *(TEHS) is a tuple $(\mathfrak{H}, H)$, where $\mathfrak{H} = (S, R, \mathcal{R})$ is a TEF, and H is a labeling of points in $P(\mathfrak{H})$ with sets of formulae, satisfying the following conditions, for all $(r, n) \in P(\mathfrak{H})$:*

1. *$H(r, n)$ is* fully expanded.
2. *If $\neg\mathbf{K}\varphi \in H(r, n)$ then $\neg\varphi \in H(r', n')$ for some $(r', n') \in P(\mathfrak{H})$ such that $((r, n), (r', n')) \in \mathcal{R}$.*
3. *If $((r, n), (r', n')) \in \mathcal{R}$, then $\mathbf{K}\varphi \in H(r, n)$ iff $\mathbf{K}\varphi \in H(r', n')$.*

4. *If* $\mathcal{X}\varphi \in H(r,n)$*, then* $\varphi \in H(r,n+1)$ *and if* $\neg\mathcal{X}\varphi \in H(r,n)$*, then* $\neg\varphi \in H(r,n+1)$*.*
5. *If* $\varphi\mathcal{U}\psi \in H(r,n)$*, then there exists* $i \geq n$ *such that* $\psi \in H(r,i)$ *and* $\varphi \in H(r,j)$ *holds for every* $n \leq j < i$*.*

$(\mathfrak{H}, H)$ *has the property* $x \in \{\mathsf{nol}, \mathsf{nof}, \mathsf{sync}, \mathsf{iis}\}$ *if* $\mathfrak{H}$ *has the property* x*.*

It was proved in [3] that any temporal-epistemic formula of the multi-agent linear time temporal epistemic logic with synchrony but without interaction of time and knowledge, is satisfiable in a TEM iff it is satisfiable in a TEHS. Adding any combination of the interaction conditions nol, nof or iis does not affect the truth of this claim in the 1-agent case, so we can from now on restrict attention to satisfiability in TEHS.

4 Tableaux for Synchronous $\mathsf{TEL}^1(\mathsf{LT})$ with Interaction Conditions

4.1 Overview of the Tableau Procedure for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$

The tableaux method for testing the satisfiability of an input formula θ of $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$ is used as a starting point for the procedure for $\mathsf{TEL}^1(\mathsf{LT})_X$ where $X \neq \emptyset$. To aid the presentation of the procedure for $\mathsf{TEL}^1(\mathsf{LT})_X$, we first outline the essentials of the tableau procedure for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$ developed for multi-agent case in [3]; the reader is referred to the latter for more detail.

The tableaux procedure for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$ consists of three major phases: *pretableau construction*, *prestate elimination*, and *state elimination.* It constructs a directed graph $\mathcal{T}^\theta$ (called a *tableau*) with nodes labelled by finite sets of formulas, and directed edges between nodes, representing temporal, epistemic, or label-expansion relations.

The pretableau construction phase produces the so-called the *pretableau* $\mathcal{P}^\theta$ for the input formula θ, where the nodes are of two kinds: *states* and *prestates.* States are fully expanded sets, meant to represent states of a TEHS, while prestates are finite sets of formulas and play a temporary role in the construction of $\mathcal{T}^\theta$. The pretableau phase consists of alternative constructions of epistemic and temporal successor prestates of a given state, and expanding a given prestate Γ into fully expanded sets, denoted by $\mathbf{states}(\Gamma)$, which label new or existing states.

The prestate elimination phase creates a smaller graph $\mathcal{T}_0^\theta$ out of $\mathcal{P}^\theta$, called the *initial tableau for* θ, by eliminating all the prestates from $\mathcal{P}^\theta$ and accordingly redirecting its edges.

Finally, the state elimination phase removes, in successive steps, all the states, if any, that cannot be satisfied in a TEHS, because they lack necessary successors (epistemic or temporal) or because they contain unrealized eventualities. When no more states can be removed, the elimination procedure produces a (possibly empty) subgraph $\mathcal{T}^\theta$ of $\mathcal{T}_0^\theta$, called the *final tableau for* θ. If some state Δ of $\mathcal{T}^\theta$ contains θ, the procedure declares θ satisfiable and a TEHS satisfying θ can be extracted from it; otherwise it declares θ unsatisfiable.

4.2 Complications Arising with Interacting Temporal and Epistemic Operators

In the tableau construction for the basic logic $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$, when identifying the set of formulas that must be put in the label of a temporal successor-prestate Γ for a state Δ, the procedure only has to take into account formulas that come from Δ. When the logic assumes time-knowledge interaction, e.g. nol, this is no longer the case because there will also be formulas coming from other states that are epistemically related to the immediate predecessor state Δ, that will be relevant for defining the successor (pre)state Γ. For instance, if two states are epistemically related, then they need respective successors that are epistemically related, and therefore it is necessary that these successors contain the same knowledge formulas. Likewise for the logic assuming nof: if a state (that is not in the 'first' temporal layer) is epistemically related to another state, then both states need to have predecessor-states which are also epistemically related. Therefore, the procedure has to create enough states at any temporal layer so that the states needed in the next temporal layer have respective predecessor states.

4.3 Bubbles and Bubble-Paths

Here we call any set of formulas Δ of $\mathsf{TEL}^1(\mathsf{LT})$ a *prestate.* A fully expanded prestate will be called a *state.* For any set of formulas Γ, we denote by $\mathbf{states}(\Gamma)$ the set of full expansions of Γ that are produced by the tableau- procedure for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$.

We let $K(\Delta) := \{\, \mathbf{K}\varphi \mid \mathbf{K}\varphi \in \Delta \,\}$, $\mathrm{Epi}(\Delta) := K(\Delta) \cup \{\, \neg\mathbf{K}\varphi \mid \neg\mathbf{K}\varphi \in \Delta \,\}$ and $\mathrm{Next}(\Delta) := \{\, \varphi \mid \mathcal{X}\varphi \in \Delta \,\} \cup \{\, \mathtt{neg}\varphi \mid \neg\mathcal{X}\varphi \in \Delta \,\}$, where $\mathtt{neg}\varphi = \varphi$ if the main-connective of φ is $\neg$ and $\mathtt{neg}\varphi = \neg\varphi$ otherwise. Note that in the tableaux for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$, the set $\{\neg\varphi\} \cup \mathrm{Epi}(\Delta) \setminus \{\neg\mathbf{K}\varphi\}$ is the epistemic successor prestate for the state Δ created for the diamond formula $\neg\mathbf{K}\varphi \in \Delta$, while $\mathrm{Next}(\Delta)$ is the temporal prestate created for Δ.

In order to deal with the complications discussed above, the tableau procedure presented here will act *not on single states* but on special kinds of sets of states representing possible epistemic clusters, which we will call *bubbles*, formally defined below. Any finite set of states will be called a *pre-bubble.*

Definition 5 (Bubbles). *A* bubble *B is a pre-bubble such that:*

- *for all $\Delta \in B$ and all $\neg\mathbf{K}\varphi \in \Delta$ there exists a $\Delta' \in B$ such that $\neg\varphi \in \Delta'$.*
- *B is* knowledge-consistent*, i.e. $K(\Delta) = K(\Delta')$ for all $\Delta, \Delta' \in B$.*

Definition 6 (Successor and predecessor sets). *A set of states S is a* successor-set *for a bubble B if for all $\Delta \in B$ there is a $\Delta' \in S$ s.t. $Next(\Delta) \subseteq \Delta'$. In that case, we write $B \rightarrow_{\forall\exists} S$. Respectively, S is a* predecessor-set *for B if for all $\Delta \in B$ there is a $\Delta' \in S$ s.t. $Next(\Delta') \subseteq \Delta$. In that case we write $S \rightarrow_{-1\forall\exists} B$.*

Definition 7 (Bubble-paths). *A sequence of bubbles* $\mathcal{B} = (B_i)_{0 \leq i \leq m}$ *is a called a bubble-path. It is a* successor-bubble-path*, if* $B_i \rightarrow_{\forall\exists} B_{i+1}$ *for all* $0 \leq i < m$*. It is a* predecessor-bubble-path *if* $B_i \rightarrow_{-1\forall\exists} B_{i+1}$ *for all* $0 \leq i < m$*.*

A sequence of states $\pi = (\Delta_i)_{0 \leq i \leq m}$ *is a* temporal path *if* $Next(\Delta_i) \subseteq \Delta_{i+1}$ *for all* $0 \leq i < m$*. The temporal path* $\pi = (\Delta_i)_{0 \leq i \leq m}$ follows *the bubble-path* $\mathcal{B} = (B_i)_{0 \leq i \leq m}$ *if* $\Delta_i \in B_i$ *for all* $0 \leq i \leq m$*.*

The tableau-procedure will construct bubble-paths. For logics that satisfy nol, these bubble-paths will be successor-bubble-paths, and for logics that satisfy nof, they will be predecessor-bubble-path. If the logic satisfies both nol and nof, the bubble-paths will be both successor-and predecessor-bubble-paths at the same time.

Definition 8 (Realization of eventualities). *Let* Δ *be a state in a bubble* B*. Let* $\varphi \mathcal{U} \psi$ *be an eventuality in* Δ*. Then* $\varphi \mathcal{U} \psi \in \Delta$ *is* realized on a bubble-path $\mathcal{B}$ in a tableau $\mathcal{T}$ by a temporal path π *if* B *equals the first bubble in* $\mathcal{B}$*,* Δ *equals the first state in* π*,* π *follows* $\mathcal{B}$*, and there is a subpath* π' *of* π *starting in* Δ*, where* ψ *belongs to the last state of* π'*, while* φ *belongs to all previous states in* π'*.*

We need the next technical notion in order to define satisfaction of a bubble-path in a TEM $\mathcal{M}$.

Definition 9 (State-point-assignment). *Let* $\mathcal{B} = (B_k)_{0 \leq k \leq m}$ *be a bubble-path. Let* $\mathcal{M}$ *be a TEM with a point* (r, n)*. Then a* state-point-assignment *for* $\mathcal{M}$*,* (r, n) *and* $\mathcal{B}$ *is a set*

$$A \subseteq \bigcup_{0 \leq k \leq m} \Big(B_k \times \{\, (r', n') \mid ((r', n'), (r, n + k)) \in \mathcal{R} \,\} \Big).$$

We imagine the states in the bubbles in the specified bubble-path being assigned to points of the model, so that the states in the first bubble are assigned to points epistemically related to the specified point (r, n), and states in the second bubble are assigned to points in $\mathcal{M}$ that are epistemically realted to $(r, n + 1)$, and so on.

Definition 10 (Satisfiability of a bubble-path). *Let* $\mathcal{M}$ *be a TEM*$_X$ *and* $(\bar{r}, n)$ *a point in* $P(\mathcal{M})$*. Let* $\mathcal{B} = (B_i)_{0 \leq i \leq m}$ *be a bubble-path. Then we say that* $\mathcal{M}$ satisfies $\mathcal{B}$ at $(\bar{r}, n)$ by A*, and write* $\mathcal{M}, (\bar{r}, n) \Vdash^A \mathcal{B}$*, if* A *is a states-point assignment for* $\mathcal{M}$*,* $(\bar{r}, n)$ *and* $\mathcal{B}$*, such that*

- $(\Delta, (r, n + k)) \in A$ *implies that* $\mathcal{M}, (r, n + k) \Vdash \Delta$*.*
- *if* nol $\in X$ *then for all* $0 \leq k < m$ *and all* $\Delta \in B_k$ *there is a run* r*, such that* $(\Delta, (r, n + k)) \in A$ *and* $(\Delta', (r, n + k + 1)) \in A$ *for some* $\Delta' \in B_{k+1}$ *with* $Next(\Delta) \subseteq \Delta'$*.*
- *if* nof $\in X$ *then for all* $0 < k \leq m$ *and all* $\Delta \in B_k$ *there is a run* r *such that* $(\Delta, (r, n + k)) \in A$ *and* $(\Delta', (r, n + k - 1)) \in A$ *for some* $\Delta' \in B_{k-1}$ *with* $Next(\Delta') \subseteq \Delta'$*.*

4.4 Construction of the Pretableau

For the logic $\mathsf{TEL}^1(\mathsf{LT})_X$ where $\mathsf{sync} \in X$ and either $\mathsf{nol} \in X$ or $\mathsf{nof} \in X$, the procedure splits into three construction parts: (i) of the pretableau, where pre-bubbles and bubbles are added to the tableau; (ii) of the initial tableau, where the pre-bubbles are removed; and (iii) of the final tableau, where bubbles are eliminated. The construction of the pretableau for θ works as follows:

1. For all $\varDelta \in \mathbf{states}(\{\theta\})$, make $\{\varDelta\}$ a pre-bubble in $\mathcal{T}$.
2. Expand each not yet expanded pre-bubble A into bubbles by applying the procedure ExpandPrebubble(A, X), outlined further. For every returned bubble B produce an arrow $A \dashrightarrow B$.
3. Produce temporal successor-prebubbles for each bubble B for which this has not been done so far, by applying the procedure TempSuccessorPrebubbles(B, X) outlined further. Add any such pre-bubble A to $\mathcal{T}$ if it is not already there and produce an arrow $B \xrightarrow{\mathcal{X}} A$.
4. Repeat step 2 and 3 in cycles until no new bubbles or pre-bubbles are created.

When producing successor-pre-bubbles and expanding pre-bubbles, we use the procedures from the basic algorithm for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$ for expanding prestates into states and producing temporal successor-prestates and epistemic alternatives for the states in the bubbles. These operations are performed ‘on the side’, and are not part of the bubble-based tableau construction itself. Yet, for efficiency we keep the expanded states on the side, so that we do not have to recompute full expansions of a state. We describe below first 3 procedures that do not depend on X and then the procedures ExpandPrebubble and TemporalSuccessorPrebubbles that depend on X.

MakeKnowledgeConsistent takes a set of states S as input, and returns a set L of all knowledge-consistent ‘alternatives’ of S. That is, if S' is in the returned set L, then S' is knowledge-consistent and there is a surjective function $f : S \to S'$ such that if $\varDelta \in S$ then $\varDelta \subseteq f(\varDelta)$, i.e. some formulas might be added to every state in S. If S is already knowledge consistent, $L = \{S\}$ is returned. Otherwise, for every state $\varDelta$ in S we collect in $K_\varDelta$ the $\mathbf{K}$-formulas in the states in S which are not in $\varDelta$, and the $\neg\mathbf{K}$-formulas in the states of S are collected in nK. Then the method returns $L = \{\, \{\varDelta_0 \cup \varSigma_0, \dots, \varDelta_n \cup \varSigma_n\} \mid \varSigma_i \in \mathbf{states}(K_{\varDelta_i}), \varDelta_i \cup \varSigma_i$ and $\varSigma_i \cup nK$ are not patently inconsistent for all $i\,\}$, where $\varDelta_0, \dots, \varDelta_n$ are the states in S. However, if there is a $\varDelta \in S$ such that $\varDelta \cup \varSigma_j$ or $\varSigma_j \cup nK$ is patently inconsistent for all $\varSigma_j \in K_\varDelta$, then $\emptyset$ is returned.

The procedure LocalBubble(A, $\varDelta$) (where $\varDelta \in A$ and A is a prebubble) returns a set L consisting of epistemic alternatives for all formulas $\neg\mathbf{K}\varphi$ in $\varDelta$ (i.e. diamond formulas), for which there is no $\varDelta' \in A$ that contains $\neg\varphi$, i.e. it returns $L = \{\, \{\varDelta_0, \dots, \varDelta_n\} \mid \varDelta_i \in \mathbf{states}(\varGamma_i)$ for all $i\,\}$, where $\neg\mathbf{K}\varphi_0, \dots, \neg\mathbf{K}\varphi_n$ are the ‘unfulfilled’ epistemic diamond formulas in $\varDelta$ and $\varGamma_i = \{\neg\varphi_i\} \cup \mathrm{Epi}(\varDelta) \setminus \{\neg\mathbf{K}\varphi_i\}$ for all i. Though, if any of the sets $\mathbf{states}(\varGamma_i) = \emptyset$, then $\emptyset$ is returned.

ExpandToBubble takes as input a knowledge-consistent prebubble S, and returns a set L consisting of bubbles, each containing S. That set is constructed by first adding S to L, and then repeatedly replacing a set S' in L (which is not marked 'closed') with $S' \cup L_1, \ldots, S' \cup L_n$, where $\{L_1, \ldots, L_n\}$ is the set returned by LocalBubble(S', $\varDelta$) for an unmarked $\varDelta \in S'$ (after which $\varDelta \in S' \cup L_i$ is marked). If LocalBubble(S', $\varDelta$) returns $\emptyset$, then S' is marked 'closed'. When each set in L is either marked 'closed' or all states in the set are marked, the 'closed' sets are removed from L, and L is returned.

TemporalSuccessorPrebubbles(B, X) returns a set L of temporal successor pre-bubbles for a bubble B. When $\mathsf{nol} \in X$, all states in B needs to have successor-states in the same bubble, so the method returns $L = \{\, \{\varDelta'_0, \ldots, \varDelta'_n\} \mid \varDelta'_i \in \mathbf{states}(\mathrm{Next}(\varDelta_i))$ for all $i\,\}$, where $\varDelta_0, \ldots, \varDelta_n$ are the states in B. Though, if $\mathbf{states}(\mathrm{Next}(\varDelta_i)) = \emptyset$ for any $\varDelta_i \in B$, the method returns $\emptyset$. When $\mathsf{nol} \notin X$, the successors of the states in B need not be in the same bubble but there should be a successor-bubble for every state in B. Thus, the returned set is $L = \{\, \{\varDelta'\} \mid \varDelta' \in \mathbf{states}(\mathrm{Next}(\varDelta))$ for a $\varDelta \in B\,\}$. If $\mathbf{states}(\mathrm{Next}(\varDelta)) = \emptyset$ for any $\varDelta \in B$, then $L = \emptyset$ is returned.

When $\mathsf{nof} \in X$ or $\{\mathsf{nol}, \mathsf{iis}\} \subseteq X$, the expansion of a prestate (that is not in the first temporal layer) is done with respect to the immediate predecessor bubble, for which the pre-bubble was created. Thus, in these cases we annotate any created successor-pre-bubble with the bubble that created it, and two pre-bubbles are not considered the same, unless they have the same annotation. There are thus $2^{2 \cdot \# sts_\theta}$ possible pre-bubbles, where $\# sts_\theta$ are the number of possible states belonging to a bubble in the tableau for a formula θ. The number of prebubbles is, however, still double-exponential in the length of the input-formula.

Before describing the next procedure, we note that the expanding procedure for prestates into states in the tableau method for $\mathsf{TEL}^1(\mathsf{LT})_\emptyset$ uses analytic cuts to ensure that if $\varDelta \xrightarrow{\neg\mathbf{K}\varphi} \varDelta'$ and $\mathbf{K}\psi \in \varDelta'$, then $\mathbf{K}\psi \in \varDelta$. That is, for any $\alpha \in \varDelta$ where $\alpha = \mathbf{K}\psi$ or $\alpha = \neg\mathbf{K}\psi$, if $\mathbf{K}\varphi \in \mathsf{Sub}(\alpha)$ and there are no $\mathcal{X}$s on the parse tree between α and $\mathbf{K}\varphi$, then $\mathbf{K}\varphi \in \varDelta$ or $\neg\mathbf{K}\varphi \in \varDelta$.

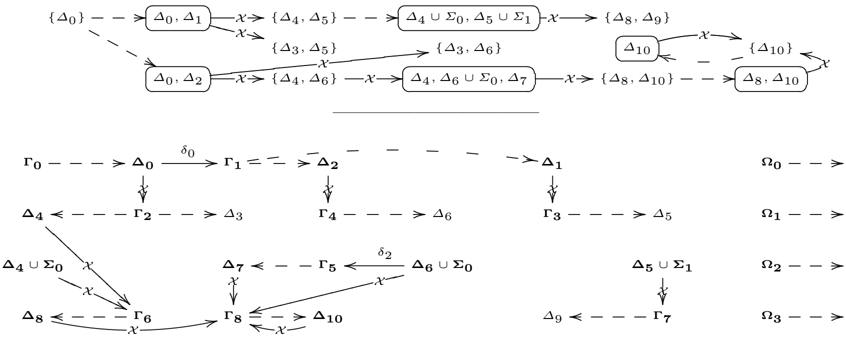
ExpandPrebubble(A, X) works as follows: When $\mathsf{nof} \notin X$ and $\{\mathsf{iis}, \mathsf{nol}\} \not\subseteq X$ (in which case nof is implied) the method first considers all knowledge-consistent versions of A (as returned by MakeKnowledgeConsistent), and then expand these to bubbles (by calls to ExpandToBubble). However, when $\mathsf{nof} \in X$ or $\{\mathsf{iis}, \mathsf{nol}\} \subseteq X$ (in which case nof is implied) things are more complicated. First of all, every state in a bubble B constructed as described above needs to have a predecessor in the bubble B' that created A (i.e. the annotation of A); of course, in the first temporal layer (when the annotation of $A = \emptyset$) this is not required. Secondly, we might later on encounter a state in a bubble that needs predecessors in the bubble B in question, so we have to ensure there are 'enough' states in B. Any state that can possibly be added to B needs to contain, as a minimum, the $\mathbf{K}$-formulas of any other state in B, and thus the states in $\mathbf{states}(K(B))$ contain the 'minimal' formulas for a state belonging to B. Adding a $\varSigma \in \mathbf{states}(K(B))$ with $K(\varSigma) = K(B)$ to B will still yield a bubble, because if $\varSigma$ contains a diamond-formula $\neg\mathbf{K}\varphi$, then there will be a state in B containing $\neg\mathbf{K}\varphi$ (because of the cuts). In temporal layers different from the first, there might have to be added more formulas to these states, but in any case, these states are denoted as the 'minimal' states of B, B_{min}.

The method thus works as follows. To keep the method working within double-exponential time, it builds a 'mini-tableau' on the side: pre-bubbles A', are expanded into knowledge-consistent pre-bubbles (to which A' is linked by a $\xrightarrow{\mathrm{KC}}$-arrow). The knowledge-consistent pre-bubbles S are then expanded into bubbles (to which S is linked by $\xrightarrow{\mathrm{Bubble}}$). For any of these bubbles $\tilde{B}$, it might be the case that not every state Δ in $\tilde{B}$ has a potential predecessor in B', the bubble creating A, i.e. there is no state $\Delta' \in B'$ where $\mathrm{Next}(\Delta') \subseteq \Delta$. So for all states $\Delta \in \tilde{B}$ that do not have a potential predecessor in B' we take any of the 'minimal' states $\Sigma \in B'_{min}$, and try to make this the predecessor of Δ; this step is of course omitted when expanding prebubbles in the first temporal layer. This is done by modifying a copy of $\tilde{B}$, where each Δ without a predecessor has been replaced with $\Delta \cup \Omega$ for a $\Omega \in \mathbf{states}(\mathrm{Next}(\Sigma))$ where $\Delta \cup \Omega$ is not patently inconsistent. $\tilde{B}$ is then linked to each of these 'copies' with an arrow $\xrightarrow{\mathrm{pred}}$. These pre-bubbles are not necessarily knowledge-consistent, so the outlined steps are repeated. We always reuse pre-bubbles, knowledge-consistent pre-bubbles and bubbles whenever possible. At some point, no new pre-bubbles, knowledge-consistent pre-bubbles or bubbles are produced. The bubbles in the mini-tableau, where all states have predecessors, i.e. $\tilde{B}$s for which $\begin{tikzcd} \tilde{B} \arrow[r, "\mathrm{KC}"] & \tilde{B} \arrow[r, "\mathrm{Bubble}"] & \tilde{B} \arrow[ll, bend left, "\mathrm{pred.}"] \end{tikzcd}$, now needs to have the 'minimal' states added to them. For each such bubble $\tilde{B}$ and each $Y \in \mathcal{P}(\{\, \Delta \in \mathbf{states}(K(\tilde{B})) \mid K(\Delta) = K(\tilde{B}) \,\})$ we therefore add $\tilde{B} \cup Y$ to the mini-tableau as a knowledge-consistent pre-bubble, if it is not already there, and we let the states in Y be 'minimal'; if $\tilde{B} \cup Y$ is present with another set of 'minimal' states, we just add the states in Y as 'minimal'. Then we expand the mini-tableau again, until no new pre-bubbles are added. Whenever we add formulas to a 'minimal' state (in making it knowledge-consistent or adding predecessors), we let the modified 'minimal' state be 'minimal' in the resulting pre-bubble. At saturation, we return the bubbles $\tilde{B}$ for which $\begin{tikzcd} \tilde{B} \arrow[r, "\mathrm{KC}"] & \tilde{B} \arrow[r, "\mathrm{Bubble}"] & \tilde{B} \arrow[ll, bend left, "\mathrm{pred.}"] \end{tikzcd}$.

We note that the procedures are so constructed that if $B \xrightarrow{\mathcal{X}} A \dashrightarrow \tilde{B}$, then $\tilde{B}$ is a successor of B if $\mathsf{nol} \in X$, and B is a predecessor of $\tilde{B}$ if $\mathsf{nof} \in X$.

The concept of bubbles and our use of them in the tableau procedure is similar to the assignment of states to equialence classes, that the procedure in [2] makes use of. However, our procedure does not require the input formula to be transformed initially, and instead it uses the bubbles as the main entities in the procedure and construct the temporal relation between bubbles (and thereby points) directly such that the required interaction properties will hold for the model that will be extracted from it. The direct use of bubbles as the main enitites of the tableau further allows for an easy adaption of the method to the asynchronous case (i.e. where sync is not required).

Example 1. Figure 1 contains the pretableau for $\theta = \neg\mathcal{X}\Big(\neg(\neg\mathbf{K}p \wedge \mathbf{K}\neg r) \wedge \neg(\mathcal{X}q \wedge \mathbf{K}u)\Big) \wedge \neg\mathbf{K}\Big(\neg\mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p) \wedge \neg\mathcal{X}(r \wedge \neg\mathbf{K}\neg v)\Big)$ in $\mathsf{TEL}^1(\mathsf{LT})_{\mathsf{sync,nol}}$. To help readability, the bubbles are framed with rounded boxes while the pre-bubbles are not. The pretableau is the part containing the bubbles, while the part consisting of states and prestates just are intermediate results; here, the expanded (pre)states are marked in bold.



$\delta_0 = \neg\mathbf{K}(\neg\mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p)$
$\Gamma_0 = \{\theta\}$
$\Gamma_1 = \{\neg(\neg\mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p)$
$\quad \wedge \neg\mathcal{X}(r \wedge \neg\mathbf{K}\neg v))\}$
$\Gamma_2 = \{\neg(\neg(\neg\mathbf{K}p \wedge \mathbf{K}\neg r)$
$\quad \wedge \neg(\mathcal{X}q \wedge \mathbf{K}u))\}$
$\Gamma_3 = \{\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p)\}$
$\Gamma_4 = \{r \wedge \neg\mathbf{K}\neg v\}$
$\Gamma_5 = \{v, \mathbf{K}u\}$
$\Gamma_6 = \{q\}$
$\Gamma_7 = \{\mathbf{K}\neg q\}$
$\Gamma_8 = \{\top\}$

$\Delta_0 = \{\theta, \neg\mathcal{X}(\neg(\neg\mathbf{K}p \wedge \mathbf{K}\neg r) \wedge \neg(\mathcal{X}q \wedge \mathbf{K}u)),$
$\quad \neg\mathbf{K}(\neg\mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p) \wedge \neg\mathcal{X}(r \wedge \neg\mathbf{K}\neg v)), \top\}$
$\Delta_1 = \Gamma_1 \cup \{\neg\neg\mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p),$
$\quad \mathcal{X}(\mathcal{X}\mathbf{K}\neg q \wedge \mathbf{K}p), \top\}$
$\Delta_2 = \Gamma_1 \cup \{\neg\neg\mathcal{X}(r \wedge \neg\mathbf{K}\neg v), \mathcal{X}(r \wedge \neg\mathbf{K}\neg v, \top\}$
$\Delta_3 = \Gamma_2 \cup \{\neg\neg(\neg\mathbf{K}p \wedge \mathbf{K}\neg r), \neg\mathbf{K}p \wedge \mathbf{K}\neg r, \neg\mathbf{K}p,$
$\quad \mathbf{K}\neg r, \neg r, \mathcal{X}\top, \top\}$
$\Delta_4 = \Gamma_2 \cup \{\neg\neg(\mathcal{X}q \wedge \mathbf{K}u), \mathcal{X}q \wedge \mathbf{K}u, \mathcal{X}q, \mathbf{K}u, u, \top\}$
$\Delta_5 = \Gamma_3 \cup \{\mathcal{X}\mathbf{K}\neg q, \mathbf{K}p, p, \top\}$
$\Delta_6 = \Gamma_4 \cup \{r, \neg\mathbf{K}\neg v, \mathcal{X}\top, \top\}$
$\Delta_7 = \{v, \mathbf{K}u, u, \mathcal{X}\top, \top\}$
$\Delta_8 = \{q, \mathcal{X}\top, \top\}$

$\Omega_0 = K(\Delta_4, \Delta_5) \setminus K(\Delta_4)$
$\quad = K(\Delta_3, \Delta_5) \setminus K(\Delta_3)$
$\quad = K(\Delta_4, \Delta_6) \setminus K(\Delta_6) = \{\mathbf{K}p\}$
$\Sigma_0 = \{\mathbf{K}p, p, \mathcal{X}\top, \top\}$
$\Omega_1 = K(\Delta_4, \Delta_5) \setminus K(\Delta_5) = \{\mathbf{K}u\}$
$\Sigma_1 = \{\mathbf{K}u, u, \mathcal{X}\top, \top\}$
$\Omega_2 = K(\Delta_3, \Delta_5) \setminus K(\Delta_5) = \{\mathbf{K}\neg r\}$
$\Sigma_2 = \{\mathbf{K}\neg r, \neg r\}$
$\Omega_3 = K(\Delta_8, \Delta_9) \setminus K(\Delta_8) = \{\mathbf{K}\neg q\}$
$\Sigma_3 = \{\mathbf{K}\neg q, \neg q, \mathcal{X}\top, \top\}$
$\Delta_9 = \{\mathbf{K}\neg q, \neg q, \top\}$
$\Delta_{10} = \{\top, \mathcal{X}\top\}$

Fig. 1. The pretableau for θ in Example 1

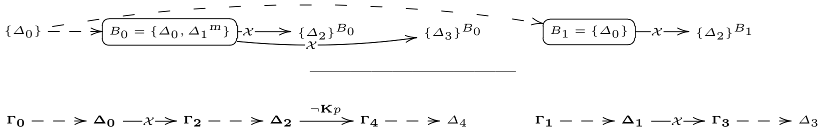
Example 2. Figure 2 contains the pretableau for $\theta = \mathbf{K}\mathcal{X}p \wedge \neg\mathcal{X}\mathbf{K}p$ in $\mathsf{TEL}^1(\mathsf{LT})_{\mathsf{sync,nof}}$. A pretableau's annotation is written in superscript next to it, and minimal states denoted with a ^{m}. When e.g., trying to expand $\{\Delta_2\}^{B_0}$, the produced 'mini-tableau' is

$$\{\Delta_2\} \overset{\text{KC}}{\longrightarrow} \{\Delta_2\} \overset{\text{Bubble}}{\longrightarrow} \{\Delta_2, \Delta_4\}.$$

$\{\Delta_2, \Delta_4\}$ cannot be expanded to a set of states where all elements have predecessors, because the only 'minimal' state in B_0 is Δ_1, and the only state Δ' for which $\Delta_1 \xrightarrow{\mathcal{X}} * \dashrightarrow \Delta'$ is Δ_3, and $\Delta_3 \cup \Delta_4$ is patently inconsistent.

4.5 Construction of the Initial and Final Tableau

After having constructed the pretableau, the initial tableau is then produced from the pretableau by taking each pre-bubble A in the pretableau, redirecting the arrows to and from A and then deleting A. I.e., for every bubbles B



$\Gamma_0 = \{\mathbf{K}\mathcal{X}p \wedge \neg\mathcal{X}\mathbf{K}p\}$, $\Delta_0 = \{\mathbf{K}\mathcal{X}p \wedge \neg\mathcal{X}\mathbf{K}p, \mathbf{K}\mathcal{X}p, \neg\mathcal{X}\mathbf{K}p, \mathcal{X}p, \top\}$, $\Gamma_1 = K(\Delta_0) = \{\mathbf{K}\mathcal{X}p\}$, $\Delta_1 = \{\mathbf{K}\mathcal{X}p, \mathcal{X}p, \top\}$,
$\Gamma_2 = \{\neg\mathbf{K}p, p\}$, $\Delta_2 = \{\neg\mathbf{K}p, p, \top\}$, $\Gamma_3 = \{p\}$, $\Delta_3 = \{p, \top\}$,
$\Gamma_4 = \{\neg p\}$, $\Delta_4 = \{\neg p, \top\}$.

Fig. 2. The pretableau for $\theta = \mathbf{K}\mathcal{X}p \wedge \neg\mathcal{X}\mathbf{K}p$ in Example 2

and B', where $B \xrightarrow{\mathcal{X}} A$ and $A \dashrightarrow B'$, we let $B \xrightarrow{\mathcal{X}} B'$ and delete A. To ease the checking for realization of eventualities, we then add arrows between the individual states in two successive bubbles: if $\Delta \in B$ and $\Delta' \in B'$, and $\text{Next}(\Delta) \subseteq \Delta'$, then we add an arrow $\Delta \cdots\cdots\!> \Delta'$ between Δ in B and Δ' in B', though, technically, the individual states are not entities in the tableaux.

Finally, the phase of building the final tableau from the initial tableau works by repeatedly making calls to two procedures, Elim-NoTempSuc(B) and Elim-UnrealEven(B), for all bubbles B in the tableau, until no bubble gets deleted in a loop. We define these procedures as follows:

Elim-NoTempSuc(bubble B): If there is no bubble B' in the current tableau such that $B \xrightarrow{\mathcal{X}} B'$, then delete B and all arrows associated with it.

Elim-UnrealEven(bubble B): If the condition (E), defined below, is not satisfied in the current tableau, then delete B and all arrows associated with it.

(E) For any $\Delta \in B$ and any eventuality $\xi \in \Delta$ there exists a bubble-path $\mathcal{B} = (B_i)_{0 \leq i \leq m}$ with $B_0 = B$ and a temporal path π such that ξ is realized on $\mathcal{B}$ by π.

Definition 11. *The tableau $\mathcal{T}$ for a formula θ is open if there is a bubble $B \in \mathcal{T}$ and a $\Delta \in B$ such that $\theta \in \Delta$.*

Example 3. Figure 3 shows the initial tableau for the formula θ from Ex. 1. In the final tableau, the two leftmost bubbles are deleted. The tableau is open since $\theta \in \Delta_0$ and $\Delta_0 \in \{\Delta_0, \Delta_2\}$.

The initial tableau for θ in Example 2 simply consists of two bubbles:

In the elimination-procedure, the two bubbles get deleted in the first round, and the initial tableau is empty. Thus, the tableau closes and θ is declared unsatisfiable.

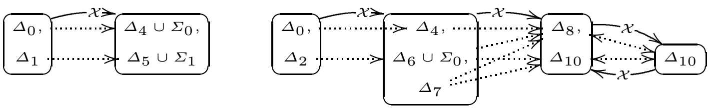


Fig. 3. The initial for θ from Example 1

5 Soundness

Theorem 1. *The tableaux procedure for each* $\mathsf{TEL}^1(\mathsf{LT})_X$ *is sound.*

Soundness of the tableaux method means that if the input formula is satisfiable, then the procedure will indeed produce an open tableau. The argument in a nutshell is that if the input formula θ is satisfiable, then there is also a satisfiable state Δ in **states**$(\{\theta\})$, and the pre-bubble $\{\Delta\}$ will be expanded to a number of bubbles. At least one of them 'survives' in the final tableau. A proof sketch can be found in [1].

6 Completeness

Theorem 2. *The tableaux procedure for each* $\mathsf{TEL}^1(\mathsf{LT})_X$ *is complete.*

Completeness of the procedure means that an open tableau can be turned into a model, or equivalently into a temporal-epistemic Hintikka structure. In somewhat simplified terms, this is done by making runs corresponding to the 'realizing' temporal path of the states in the bubble B, that ensures that the tableau is open, and then doing the same for each state in the bubbles that these paths pass by. A proof sketch can be found in [1].

7 Complexity

Recall that $\#sts_\theta$ denotes the number of possible states in the bubbles in the tableaux for a formula θ, which is exponential in the length of the input formula, while $\#Bs := 2^{\#sts_\theta}$ is the possible number of bubbles in the tableau.

Theorem 3. *The tableaux procedure for each* $\mathsf{TEL}^1(\mathsf{LT})_X$ *runs in 2EXPTIME.*

The proof (see details in [1]) relies on the fact that all presented methods run in time polynomial in the number of bubbles in the tableau, i.e. the procedure runs in double-exponential time.

Theorem 4. *For* $\mathsf{TEL}^1(\mathsf{LT})_X$ *where* $\mathsf{nol} \in X$*, the tableaux-procedure can be modified to work in EXPSPACE.*

Proof. If $\mathsf{nol} \in X$, the bubble-path constructed in Section 5 can be shortened to a suitable size. In the construction we several times find a bubble-path $\mathcal{B}$ starting in a bubble B, so that a state $\Delta \in B$ has an associated path π^Δ such that a given eventuality $\xi \in \Delta$ is realized on $\mathcal{B}$ by π^Δ. $\mathcal{B}$ and π can now be shortened so that

π does not pass through the same state in the same bubble, i.e. the length of π and $\mathcal{B}$ will be at most $\#Bs \cdot \#sts_\theta$; if $B_i, B_j \in \mathcal{B}$ with $B_i = B_j$ and $\pi_i = \pi_j$, then we just remove the bubbles in between B_i and B_{j-1} (including both). The new bubble-path emerging from this operation will be satisfied by possibly another model and state-point-assignment.

In this way, we can obtain a bound on the indexes ρ and m of the ultimately periodic bubble-path $\begin{tikzcd} B \arrow[r, "\mathcal{X}"] & \cdots \arrow[r, "\mathcal{X}"] & B_\rho \arrow[r, "\mathcal{X}"] & \cdots \arrow[r, "\mathcal{X}"] & B_{m-1} \arrow[llll, bend right, "\mathcal{X}"'] \end{tikzcd}$. These bounds can now be used to turn the procedure into a procedure that runs in NEXPSPACE=EXPSPACE. This procedure is similar to the one for LTL with an 'exponential step' added to it. If θ is a satisfiable formula, then the following procedure finds the ultimately periodic bubble-path with indexes ρ and m, and if not, "false" is returned. The procedure works as follows:

1. Guess ρ, m and the starting bubble which is kept in the variable $CurB$; check that $CurB$ *is* a bubble. Return "false" if this is not the case. Set $k = 0$.
2. Guess the successor-bubble of $CurB$, which is stored in the variable $NextB$; check that $NextB$ *is* a bubble and that it *is* a successor-set for $CurB$, and return "false" otherwise. If $\mathsf{nof} \in X$, also check that $CurB$ is a predecessor-set for $NextB$, and return "false" otherwise. Assign $NextB$ to $CurB$, and add one to k.
3. Repeat step 2 until $k = \rho$ ($CurB$ now corresponds to B_ρ). Let the variable $RepB$ store the bubble $CurB$. For all $\Delta \in CurB$ and all eventualities $\varphi \mathcal{U} \psi \in \Delta$, add $\varphi \mathcal{U} \psi$ to the set $Real_\Delta$ (create $Real_\Delta$ if it does not already exist).
4. Guess the successor-bubble of $CurB$, and store it in $NextB$. Check that $NextB$ *is* a bubble, that it *is* a successor-set for $CurB$, and if $\mathsf{nof} \in X$, check that $CurB$ is a predecessor-set for $NextB$. If not, return "false", else for all $\Delta' \in NextB$ create a new $Real_{\Delta'}$. For all states $\Delta \in CurB$, guess the successor $\Delta' \in NextB$ of Δ. For all eventualities $\varphi \mathcal{U} \psi$ in $Real_\Delta$, add $\varphi \mathcal{U} \psi$ to $Real_{\Delta'}$ if $\psi \notin \Delta'$. Then delete $Real_\Delta$, assign $NextB$ to $CurB$, and add 1 to k.
5. Repeat step 4 until $k = m - 1$ ($CurB$ now corresponds to B_{m-1}). Check that $RepB$ is a successor-set of $CurB$, and if $\mathsf{nof} \in X$, check that $CurB$ is a predecessor-set for $RepB$. For all $\Delta \in CurB$, guess the successor $\Delta' \in RepB$ of Δ. Check that all eventualities $\varphi \mathcal{U} \psi \in Real_\Delta$ are realized in Δ', i.e. $\psi \in \Delta'$. If not, return "false".
6. If the algorithm has not terminated so far, return "true".

At any point in time the procedure only keeps 3 bubbles in memory (which takes $3 \cdot \#sts_\theta$ space) and the number of variables $Real_\Delta$ is at most $2 \cdot \#sts_\theta$, and the length of each $Real_\Delta$ is at most $|\theta|$, where $|\theta|$ is the length of the input-formula θ. Thus, the procedure runs in space $\mathcal{O}(poly(\#sts_\theta))$.

8 Concluding Remarks

We have substantially extended and adapted the incremental tableau procedure sketched in [3] to work for all cases of single-agent synchronous temporal-epistemic logics with interactions between time and knowledge considered in

[4] and [5] and have thus developed a uniform, optimal and practically implementable method for deciding satisfiability in these logics. The method is amenable to easy adaptations to systems where the synchrony-assumption is dropped, and to 1-agent branching-time temporal epistemic logics. It can further be extended to the multiagent case, however, it will work in non-elementary time (due to the complexity of these logics). Tableaux for these and other related cases are part of the future agenda of this project.

References

1. Ajspur, M., Goranko, V.: Tableaux-based decision method for single-agent linear time synchronous temporal epistemic logics with interacting time and knowledge. Technical report (2012), http://www2.imm.dtu.dk/ vfgo/papers/AjspurGoranko-ICLA2013-TechReport.pdf
2. Dixon, C., Nalon, C., Fisher, M.: Tableaux for logics of time and knowledge with interactions relating to synchrony. Journal of Applied Non-Classical Logics 14(4), 397–445 (2004)
3. Goranko, V., Shkatov, D.: Tableau-based decision procedure for full coalitional multiagent temporal-epistemic logic of linear time. In: Decker, Sichman, Sierra, Castelfranchi (eds.) Proc. of AAMAS 2009 (2009)
4. Halpern, J.Y., Vardi, M.Y.: The complexity of reasoning about knowledge and time I: Lower bounds. Journal of Computer and System Sciences 38(1), 195–237 (1989)
5. Halpern, J.Y., Vardi, M.Y.: Reasoning about knowledge and time: Synchronous systems, IBM Research Report (1989)
6. Kontchakov, R., Lutz, C., Wolter, F., Zakharyaschev, M.: Temporalizing tableaux. Studia Logica 76(1), 91–134 (2004)
7. Nalon, C., Dixon, C., Fisher, M.: Resolution for synchrony and no learning. In: Schmidt, R., et al. (eds.) Advances in Modal Logic 5, pp. 231–248 (2004)
8. Pratt, V.R.: A practical decision method for propositional dynamic logic. In: Proc. of the 10th Annual ACM Symp. on the Theory of Computing, San Diego, California, pp. 326–337 (1979)
9. Wolper, P.: The tableau method for temporal logic: an overview. Logique et Analyse 28(110-111), 119–136 (1985)

Agent-Time Epistemics and Coordination

Ido Ben-Zvi[1] and Yoram Moses[2]

[1] Department of Computer Science, Technion
idobz@cs.technion.ac.il
[2] Department of Electrical Engineering, Technion
moses@ee.technion.ac.il

Abstract. A minor change to the standard epistemic logical language, replacing K_i with $K_{\langle i,t\rangle}$ where t is an explicit time instance, gives rise to a generalized and more expressive form of knowledge and common knowledge operators. We investigate the communication structures that are necessary for such generalized epistemic states to arise, and the inter-agent coordination tasks that require such knowledge. Previous work has established a relation between linear event ordering and nested knowledge, and between simultaneous event occurrences and common knowledge. In the new, extended, formalism, epistemic necessity is decoupled from temporal necessity. Nested knowledge and event ordering are shown to be related even when the nesting order of the operators does not match the temporal order of occurrence. The generalized form of common knowledge does *not* correspond to simultaneity. Rather, it corresponds to a notion of tight coordination, of which simultaneity is an instance.

1 Introduction

We have recently embarked on an in-depth inquiry concerning the relation between knowledge, coordination and communication-based causality in multi-agent systems [4,5,3]. This study uncovered new structural connections between the three in *synchronous* systems, where agents have accurate clocks, and there are (commonly known) bounds on the time it may take messages to be delivered along any given communication channel. In such a setting, one often reasons about what agents know at particular points in time. Furthermore, one may reason about what an agent knows at one time about what other agents will know (or have known) at various other times. This leads us to consider a formalization in which epistemic operators are indexed by an agent-time pair $\langle i,t\rangle$, called a *node*. Thus, $K_{\langle i,t\rangle}$ refers to what agent i knows at time t, whereas the more traditional epistemic operator K_i refers to what agent i knows at the current time. The new formalism is called *node-based* (or *nb*- for short).

The node-based operators give rise to natural proper generalizations of nested knowledge and of common knowledge. Of particular interest is node-based common knowledge, which is represented by an epistemic operator C_A, in which A is a set of agent-time pairs $\langle i,t\rangle$. For example, $C_{\{\langle i,t\rangle,\langle j,t+3\rangle\}}\varphi$ indicates, among other things, that agent i at time t knows that agent j at time $t+3$ will

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 97–108, 2013.

know that i at time t knew that φ holds. While nb-common knowledge strictly generalizes classical common knowledge, it shares many of the typical properties of common knowledge. However, whereas (traditional) common knowledge is intimately related to simultaneity, nb-common knowledge *is not!* Rather, nb-common knowledge precisely captures what we call *tightly-timed* coordination. Thus, for example, nb-common knowledge arises when agents are coordinated so that they perform their respective actions within exactly pre-specified time differences from each other (e.g., Alice is guaranteed to act precisely 3 time steps before Bob). Simultaneity is a particular instance of tightly-timed coordination.

Statements made using nb-based knowledge operators can be naturally expressed in a temporal-epistemic modal logic containing standard knowledge operators and (future and past) next-time modal operators (similar to the KL_n logic of [11]). Being based on explicit-time operators, the nb-logic is a less useful specification language than such a temporal-epistemic logic would be. The nb-formalism is used in this paper as a tool for capturing the causal structure underlying specific types of distributed coordination. In particular, the notion of tightly-timed coordination is captured by nb-common knowledge. Interestingly, while standard common knowledge can be defined in an epistemic logic that is enriched by a standard fixed-point operator (see [8,10]), there does not appear to be a simple way to define nb-common knowledge by applying such a fixed-point operator in the temporal-epistemic modal framework.[1]

We follow the pattern of investigation presented in [4], where an epistemic analysis is the formal link between a coordination task and the necessary causal structure it requires. Thus, on one hand, epistemic states (such as nb-nested knowledge or nb-common knowledge) are shown to be necessary for performing actions in a coordination task and on the other, causal structures involving communication and time that are required for attaining the epistemic state are identified. As nb-knowledge operators generalize the standard agent-based ones, the results we obtain here generalize and extend the ones of [4,3]. Relating knowledge to communication, we present two "knowledge-gain" theorems (in the spirit of Chandy and Misra's result for systems without clocks [6]). Nb-nested and nb-common knowledge are shown to require more flexible variants of the centipede and the broom communication structures of [4]. The node-based statements have a fairly intuitive and transparent semantic meaning. The statements that serve to characterize natural coordination tasks provide further insight into what these forms of coordination require. Thus, the node-based formalism and agent-time semantics allow us to non-trivially extend the causal theory of multi-agent coordination.

2 Interpreted Systems, Knowledge and Communication

We operate within the *interpreted systems* framework of [8]. In this framework, a set $\mathbb{P} = \{1, \ldots, n\}$ of agents is connected by a communication network, modeled

---

[1] Following the current work, however, Gonczarowski and Moses introduced a notion of a *vectorial* fixed point that does allow this, at a nontrivial technical cost [9].

as a graph, which serves as the exclusive means by which the agents interact with each other.

We assume that, at any given point in time, each agent in the system is in some *local state*. A *global state* is a tuple $g = \langle \ell_e, \ell_1, \ldots, \ell_n \rangle$ consisting of local states of the agents, together with the state ℓ_e of the *environment*. The environment's state accounts for everything that is relevant to the system that is not contained in the state of the agents. A *run* r is a function from time to global states. Intuitively, a run is a complete description of what happens over time in one possible execution of the system. We use $r_i(t)$ to denote agent i's local state ℓ_i at time t in run r, for $i = 1, \ldots, n$. For simplicity, time is taken to range over the natural numbers (time is discrete). *Round* t in run r occurs between time $t - 1$ and t. Agents follow a deterministic protocol $(P = P_1, \ldots, P_n)$, in which every P_i is a function specifying a unique action for each local state of agent i. A *system* $\mathcal{R} = \mathcal{R}(P, \gamma)$ is an exhaustive set of all possible runs of the agents' protocol P in the *context* γ. Here the context determines underlying characteristics of the environment as a whole (see [8]).

As mentioned, we focus on synchronous environments where the clocks of the individual agents are all synchronized, and there are commonly known bounds on message delivery times. For ease of exposition, we assume that agents have *perfect recall*, so that their local states keeps track of all local events that they have experienced.

In order for a well defined system of runs $\mathcal{R}$ to emerge, the context γ needs to be rigorously defined as well. We define a specific context γ^{max}, within which the agents are operating. Most notably, γ^{max} specifies that (a) agents share a universal notion of time and of the network's topology, (b) the communication network has upper bounds on delivery times, (c) there are four kinds of events: message send and receive events, internal actions, and external inputs. The latter occur when a signal is received by an agent from "outside" the system. Finally, (d) all nondeterminism is deferred to the environment agent, which is responsible for message deliveries and external inputs to all other agents. Formally, since all of the agents are following a deterministic protocol, nondeterminism is only introduced into the system by the environment. Moreover, we assume that external inputs are *spontaneous*, or nondeterministic, events, in the sense defined in [4]; they are independent of any other action of the environment, and of any action of the agents preceding the occurrence of such an event.

The standard agent-based epistemic logic of knowledge $\mathcal{L}_0$ is defined by:

$$\mathcal{L}_0 : \qquad \psi \quad ::= \quad \mathsf{occ'd(e)} \mid \psi \wedge \psi \mid \neg\psi \mid K_i\psi \mid E_G\psi \mid C_G\psi,$$

where e is a local (external input or message receive) event, $\mathsf{occ'd(e)}$ is a proposition that is true once e has occurred, i is an agent, and G is a set of agents. Satisfaction of $\mathcal{L}_0$ formulas is defined w.r.t. a triple $(\mathcal{R}, r, t)$. For its semantics in interpreted systems, see [8]. In this paper, we make use of a node-based propositional epistemic language:

$$\mathcal{L}_1 : \qquad \varphi \quad ::= \quad \mathsf{occurs}_t(\mathsf{e}) \mid \varphi \wedge \varphi \mid \neg\varphi \mid K_\alpha\varphi \mid E_A\varphi \mid C_A\varphi,$$

where α denotes an agent-time node and A denotes a set of such nodes. The $\mathsf{occurs}_t(\mathsf{e})$ formulas are the only primitive propositions in $\mathcal{L}_1$. As noted, events occur at particular agents, and these occurrences are recorded in the local states of both the site of occurrence and the environment agent. Notice that all statements in $\mathcal{L}_1$ are "time-stamped," in that they refer to explicit times at which the stated facts should hold. They are thus time-invariant, and state facts about the run, rather than facts whose truth depends on the time of evaluation. Therefore, semantics for formulas of $\mathcal{L}_1$ are given with respect to a system $\mathcal{R}$ and a run $r \in \mathcal{R}$. The semantics is as follows (omitting the standard propositional clauses for $\wedge$ and $\neg$).

Definition 1 ($\mathcal{L}_1$ semantics). *The truth of a formula $\varphi \in \mathcal{L}_1$ is defined with respect to a pair $(\mathcal{R}, r)$.*

- $(\mathcal{R}, r) \models \mathsf{occurs}_t(\mathsf{e})$ *iff event* e *occurs in r by time t*
- $(\mathcal{R}, r) \models K_{\langle i,t\rangle}\varphi$ *iff* $(\mathcal{R}, r') \models \varphi$ *for all runs r' s.t. $r_i(t) = r'_i(t)$.*
- $(\mathcal{R}, r) \models E_A\varphi$ *iff* $(\mathcal{R}, r) \models K_\alpha\varphi$ *for every $\alpha \in A$.*
- $(\mathcal{R}, r) \models C_A\varphi$ *iff* $(\mathcal{R}, r) \models (E_A)^k\varphi$ *for every $k \geq 1$.*

In principle, the node-based semantics, as proposed here, can be seen as a simplified version of a real-time temporal logic with an explicit clock variable [1], and more generally of a hybrid logic [2]. In a precise sense, the node-based framework and $\mathcal{L}_1$ extend the traditional standard framework and $\mathcal{L}_0$. It is possible to define a *"timestamping"* operation $[\![]\!] : \mathcal{L}_0 \times \mathsf{Time} \rightarrow \mathcal{L}_1$ transforming a formula $\psi \in \mathcal{L}_0$ and a time t to a formula $[\![\psi]\!]^t \in \mathcal{L}_1$, such that the following holds:[2]

Lemma 1. $(\mathcal{R}, r, t) \models \psi$ *iff* $(\mathcal{R}, r) \models [\![\psi]\!]^t$ *holds for every $\psi \in \mathcal{L}_0$ and time t.*

In particular, $[\![C_G\psi]\!]^t = C_A[\![\psi]\!]^t$ for $A = \{\langle i,t\rangle : i \in G\}$. It is easy to see that $\mathcal{L}_1$ is strictly more expressive than $\mathcal{L}_0$. For example, while $[\![K_iK_j\mathsf{occ'd}(\mathsf{e})]\!]^3 = K_{\langle i,3\rangle}K_{\langle j,3\rangle}\mathsf{occurs}_3(\mathsf{e})$, the formula $K_{\langle i,3\rangle}K_{\langle j,7\rangle}\varphi$ is not equivalent to an $\mathcal{L}_0$ formula, since $\mathcal{L}_0$ does not allow for the temporal reference point to be shifted when switching from the outer knowledge operator to the inner one. There is a natural connection between $\mathcal{L}_1$ and temporal-epistemic modal languages that extend $\mathcal{L}_0$ by adding temporal operators (see, e.g., [11]). If $(\mathcal{R}, r) \models K_{\langle i,3\rangle}K_{\langle j,7\rangle}\mathsf{occurs}_2(\mathsf{e})$ is true, then $(\mathcal{R}, r, 3) \models K_i \bigcirc^4 K_j \bigcirc^{-5} \mathsf{occ'd}(\mathsf{e})$. The times involved are explicit in the $\mathcal{L}_1$ formula, while in the latter formula they are implicit, derivable from the current time 3 and the multiplicity of the next operators (in this case, for example, $2 = 3+4-5$). It appears that node-based *common knowledge* statements such as $C_{\{\langle i,3\rangle,\langle j,7\rangle\}}\mathsf{occurs}_2(\mathsf{e})$ cannot be expressed even in the temporal-epistemic language, with the standard common knowledge operator C_G, or even with standard fixed-point operators. Our aim in this paper is to utilize the node-based formalism, rather than explore it. Hence, issues of completeness and tractability are left unattended, to be explored at a future date. (We conjecture, however, that deciding satisfiability will be more tractable than in the temporal-epistemic cases studied in [11].)

---

[2] Due to space limitations, all proofs are deferred to the full paper.

It is well-known that common knowledge is closely related to simultaneity [8,7,10]. Indeed, both $C_G\psi \Rightarrow E_G C_G\psi$ and $K_i C_G\psi \Rightarrow C_G\psi$ are valid formulas. (Recall that a formula $\psi \in \mathcal{L}_0$ is *valid* if $(\mathcal{R}, r, t) \vDash \psi$ for all choices of $\mathcal{R}$, run $r \in \mathcal{R}$ and time t.) Thus, the first instant at which $C_G\psi$ holds must involve a simultaneous change in the local states of all members of G. In contrast, simultaneity is *not* an intrinsic property of node-based common knowledge. As an example, consider the node set $A = \{\langle i, 3\rangle, \langle j, 6\rangle\}$. Although we still have that both $K_{\langle i,3\rangle} C_A\varphi \Rightarrow C_A\varphi$ and $C_A\varphi \Rightarrow K_{\langle j,6\rangle} C_A\varphi$ are valid formulas, if the current time is $t = 3$ and i knows that $C_A\varphi$ holds, this does not mean that j currently knows this too. The bond with simultaneity has been broken. As we shall see in Section 4, however, a notion of tight temporal coordination that generalizes simultaneity *is* intrinsic to node-based common knowledge.

In the spirit of the treatment in [8], for a formula $\varphi \in \mathcal{L}_1$ we write $\mathcal{R} \vDash \varphi$ and say that φ is *valid in* (the system) $\mathcal{R}$ if $(\mathcal{R}, r) \vDash \varphi$ for all $r \in \mathcal{R}$. A formula is *valid* if it is valid in all systems. Node-based common knowledge manifests many of the logical properties shown by the standard notion of common knowledge.

Lemma 2. – *Both* $K_{\langle i,t\rangle}$ *and* C_A *are* $S5$ *modalities.*
- $C_A\varphi \Rightarrow E_A(\varphi \wedge C_A\varphi)$ *is valid.*
- *If* $\mathcal{R} \vDash \varphi \Rightarrow E_A(\varphi \wedge \varphi')$ *then* $\mathcal{R} \vDash \varphi \Rightarrow C_A\varphi'$

The second clause of Lemma 2 generalizes the so-called "fixed-point" axiom of common knowledge, while the third clause generalises to the "induction (inference) rule" [8].

Our main goal in this paper is to characterize coordination tasks in terms of the underlying inter-agent communications that they necessitate, and the node-based epistemic language will play an important part in tying in coordination and causal communication. In this our approach follows [4] which, in turn, extends the findings of Lamport [12] and of Chandy and Misra [6]. In [4] we defined *syncausality*, which formalizes information flow via message chains in synchronous systems, extending Lamport's notion of *potential causality.* The relation is defined pairs of agent-time nodes.

Definition 2 (Syncausality [4]). *Fix* $r \in \mathcal{R}$*.* Syncausality *is the smallest relation* $\rightsquigarrow$ *over the nodes of a run* r *satisfying the following four conditions:*

1. *If* $t \le t'$ *then* $\langle i, t\rangle \rightsquigarrow \langle i, t'\rangle$*;*
2. *If a message is sent at* $\langle i, t\rangle$ *in* r *and received at* $\langle j, t'\rangle$*, then* $\langle i, t\rangle \rightsquigarrow \langle j, t'\rangle$*;*
3. *If no message is sent at* $\langle i, t\rangle$ *in* r *over the channel* $i \mapsto j$*, then* $\langle i, t\rangle \rightsquigarrow \langle j, t + max_{ij}\rangle$*; and*
4. *If both* $\langle i, t\rangle \rightsquigarrow \langle h, t''\rangle$ *and* $\langle h, t''\rangle \rightsquigarrow \langle j, t'\rangle$*, then* $\langle i, t\rangle \rightsquigarrow \langle j, t'\rangle$*.*

Syncausality captures *direct* flow of information between agent-time nodes via communication. The first three clauses coincide with Lamport's *happened-before* relation from asynchronous systems, and the third clause accounts for the possibility of information to flow due to a receiver observing that a message was *not* sent, in synchronous systems, based on its clocks and the bounds on message transmission times. In synchronous systems, agents can come to know about remote events without direct information flow. Thus, if Alice sends Bob a message at time t she can know that he received it once after an amount of time equal to the upper bound on transmission from her to Bob. In fact, if Charlie hears about Alice's message, he can also attain knowledge about Bob without direct information flow from Bob to him. Such indirect knowledge is governed by a second relation, called *bound guarantee*:

Definition 3 (Bound guarantee [4]). *Fix synchronous context* γ^{max}. *The* bound guarantee *relation* $\dashrightarrow$ *over runs* r *in systems* $\mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$ *is the smallest relation satisfying the following three conditions:*

1. *If* $t \leq t'$ *then* $\langle i, t\rangle \dashrightarrow \langle i, t'\rangle$*;*
2. *If* $i \mapsto j$ *is a channel, then* $\langle i, t\rangle \dashrightarrow \langle j, t + max_{ij}\rangle$*; and*
3. *If* $\langle i, t\rangle \dashrightarrow \langle h, t''\rangle$ *and* $\langle h, t''\rangle \dashrightarrow \langle j, t'\rangle$*, then* $\langle i, t\rangle \dashrightarrow \langle j, t'\rangle$*.*

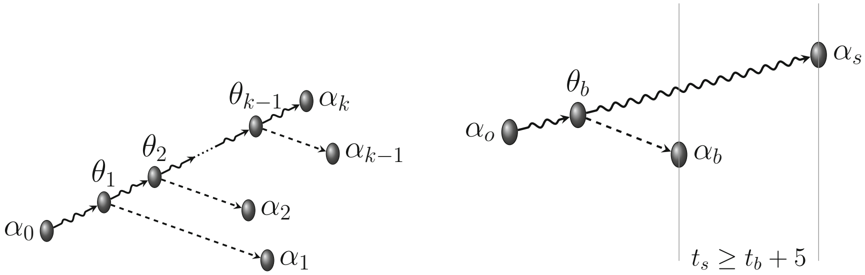
3 Nested Knowledge and Weak Bounds

Spontaneous events, communication, and the passage of time combined form the means by which agents' knowledge evolves [10]. Syncausality and bound guarantees allow us to formalize central aspects of this connection in synchronous systems. The emergence of nested knowledge in $\mathcal{L}_0$ formulas such as $K_i K_j K_h \psi$ was captured in terms of a causal structure called a *centipede* in [4]. This time we consider nb-formulas such as $K_{\langle i,7\rangle} K_{\langle j,3\rangle} K_{\langle h,15\rangle} \varphi$. To capture such formulas, we consider the following generalisation of centipedes:

Definition 4 (Uneven centipede). *Let* $r \in \mathcal{R}$*, and let* $\mathsf{A} = \langle \alpha_0, \alpha_1, \ldots, \alpha_k\rangle$ *be a sequence of nodes. An* (uneven) centipede *for* A *in* r *is a sequence* $\mathsf{B} = \langle \theta_0, \theta_1, \ldots, \theta_k\rangle$ *of nodes such that* $\theta_0 = \alpha_0$*,* $\theta_k = \alpha_k$*,* $\theta_0 \rightsquigarrow \theta_1 \rightsquigarrow \cdots \rightsquigarrow \theta_k$*, and* $\theta_h \dashrightarrow \alpha_h$ *holds for* $h = 1, \ldots, k-1$*.*

We remark that syncausality is a reflexive relation, so that $\theta \rightsquigarrow \theta$ is guaranteed to hold. As a result, the nodes $\theta_0, \ldots, \theta_k$ of B need not be distinct.

Denote $\alpha_h = \langle i_h, t_h\rangle$ for $h = 0, \ldots, k$. Figure 1a shows an uneven centipede, with wavy arrows depicting syncausal links between nodes, and dashed arrows (the "legs" of the centipede) standing for bound guarantees. The syncausal links may depend on the actually realized transmission times of messages, while bound guarantees are based on the *a priori* bounds max_{ij}. This type of centipede is termed *uneven* because the "legs" of the centipede end at nodes at a variety of different times, whereas in the original centipedes of [4] all legs ended at nodes $\langle i_1, t_k\rangle, \langle i_2, t_k\rangle, \ldots$ with the same time component t_k. Intuitively, each of the nodes $\theta_h \in \mathsf{B}$ can serve as a "witness" to the fact that information available at θ_h can be guaranteed to reach α_h's agent i_h by time t_h. Observe that the node α_2 temporally precedes α_1 in Fig. 1a. Roughly speaking, the centipede can be used to establish that α_2 will know that α_1 will know about events at α_0 (under a suitable protocol). In this case, node α_2 occurs at $t_2 < t_1$, temporally



(a) An uneven centipede (b) Vendor example

Fig. 1.

preceding α_1. Causally, or epistemically, it is node α_1 that "precedes" α_2. Events at α_2 may causally depend on those that (will) occur at α_1.

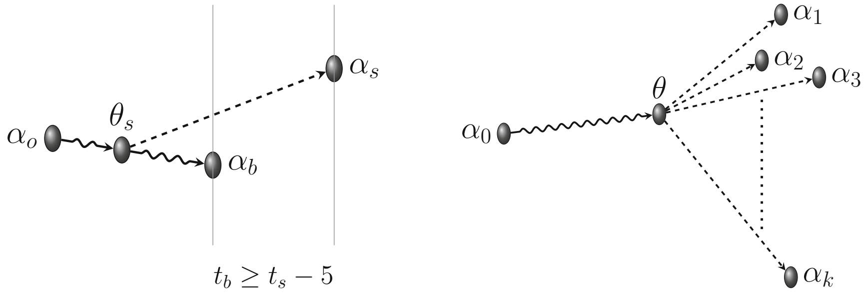
In order to illustrate the connection between distributed coordination, nested nb-knowledge, and uneven centipedes, consider the following simplified example. The online purchase of a book consists of three events: arrival of the order e_o, billing, and shipping, occurring at three distinct agents Oren (o), Bill (b) and Sharon (s). working for the vendor. Suppose, moreover, that the vendor is conservative, and specifies that shipping must take place at least 5 time units after billing. Clearly, billing will not occur before the order has been received, and an efficient system would bill immediately upon learning about the order. In order to ship at t_s, agent s must know that al least 5 time units have elapsed since the billing action was performed. Intuitively, the run must satisfy $K_{\langle s,t_s\rangle}K_{\langle b,t_s-5\rangle}\mathsf{occurs}_{t_s-5}(\mathsf{e}_o)$. Our results will show that this can be true only if an uneven centipede as in Figure 1b exists, with $t_s \geq t_b - 5$: Agent s must receive direct information, by a syncausal chain from some node θ, with proof that b would surely have enough information by $t_s - 5$ to perform the billing action. The latter comes from the bound guarantee relation between θ to α_b.

An interesting variant is the case in which a competing vendor chooses to be more trusting and to favour fast service as a top priority. Rather than shipping the book *at least* 5 units after billing, this vendor requires shipping to occur *at most* 5 time units after billing, possibly even before billing occurs. It may appear natural that this would require a similar centipede, just with the modified requirement that $t_s \leq t_b - 5$. This, however, is not the case. Even though shipping will still typically occur later than billing does, there is a precise sense in which, in causal or epistemic terms, shipping now precedes billing: Sharon can now ship when she learns about the order, but Bill must wait until he knows that Sharon will be able to ship within at most 5 time units. The earlier action causally depends on the later one. In other words, billing at time t_b requires $K_{\langle b,t_b\rangle}K_{\langle s,t_b+5\rangle}\mathsf{occurs}_{t_b+5}(\mathsf{e}_o)$. The corresponding uneven centipede is the one in Figure 2a, in which the epistemic, or causal, ordering is the opposite of the one in Figure 1b.

We now turn to a formal analysis relating coordination with uneven centipedes. The first step is to show that uneven centipedes are the necessary causal structures underlying nested nb-knowledge gain regarding spontaneous events, in the spirit of Chandy and Misra's celebrated *knowledge gain* theorem from [6]:

Theorem 1. *Let* $r \in \mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$*, and let* $\boldsymbol{e}_{\mathsf{s}}$ *be a (spontaneous) external input occurring at* $\alpha_0 = \langle i_0, t_0 \rangle$ *in* r*. If* $(\mathcal{R}, r) \vDash K_{\alpha_k} K_{\alpha_{k-1}} \cdots K_{\alpha_1} \mathsf{occurs}_{t_0}(\boldsymbol{e}_{\mathsf{s}})$ *then there is an uneven centipede for* $\langle \alpha_0, \ldots, \alpha_k \rangle$ *in* r*.*

Theorem 1 is a proper generalization of the knowledge gain theorem for nested knowledge in [4]. Interestingly, its proof is the same in both cases. The more expressive language $\mathcal{L}_1$ thus allows us to obtain a strictly stronger characterization than was possible with $\mathcal{L}_0$. The same will be true for Theorem 3 regarding common knowledge gain in the next section. This is a case where our understanding of what is going on has been limited purely by the expressivity of the formal apparatus of which we made use.



(a) Epistemic vs. temporal precedence (b) An uneven broom

Fig. 2.

We now provide a formal definition for a class of coordination tasks that require nb-nested knowledge. As in our book purchase example above, we are interested in transactions, or patterns of coordinated actions, that are trigerred by a spontaneous external input. The particular pattern considered here is a temporally ordered sequence of response events $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_k$, where each $\boldsymbol{\alpha}_h$ is a particular action, and an agent i_h that should perform it. Moreover, there are bounds $\delta_1, \ldots, \delta_k$ such that $\boldsymbol{\alpha}_1$ must take place at least δ_1 time after the trigger, and for each $j = 2, \ldots, k$ the response $\boldsymbol{\alpha}_j$ must occur at least δ_j units after $\boldsymbol{\alpha}_{j-1}$.

Definition 5 (Weakly Timed Response). *Let* $\boldsymbol{e}_{\mathsf{s}}$ *be the arrival of a particular spontaneous external input. A protocol* P *solves the instance* `WTR` $= \langle \boldsymbol{e}_{\mathsf{s}}, \boldsymbol{\alpha}_1 : \delta_1, \boldsymbol{\alpha}_2 : \delta_2, \ldots, \boldsymbol{\alpha}_{k-1} : \delta_{k-1}, \boldsymbol{\alpha}_k \rangle$ *of the* Weakly Timed Response *problem if it guarantees that each of its runs satisfies*

1. *every response $\boldsymbol{\alpha_h}$, for $h = 1, \ldots, k$, occurs in the run iff the trigger event $\boldsymbol{e}_{\mathsf{s}}$ occurs in the run, and*
2. *if $\boldsymbol{e}_{\mathsf{s}}$ occurs at time t_0 and for all $h = 1, \ldots, k$ the response $\boldsymbol{\alpha}_h$ occurs at node $\alpha_h = \langle i_h, t_h \rangle$, then $t_{h+1} \geq t_h + \delta_h$ for $h = 0, \ldots, k-1$.*

Before formally relating the WTR problem to nb-nested knowledge, another nuance should be observed. Even though agent i_k may not know the exact time at which responses are performed by other agents based on the problem definition, it can work out an upper bound on the time of responses carried out by agents i_1 to i_{k-1}. For example, response $\boldsymbol{\alpha_{k-1}}$ gets carried out at t_{k-1} which is no later than $t_k - \delta_{k-1}$. Response $\boldsymbol{\alpha_{k-2}}$ is then bounded with respect to α_k by $t_{k-2} \leq t_{k-1} - \delta_{k-2} \leq t_k - \delta_{k-1} - \delta_{k-2}$, etc. We will use

$$\beta_h^k = \langle i_h, t_h^k \rangle \qquad \text{where} \;\; t_h^k = t_k - \sum_{j=h}^{k-1} \delta_j$$

to denote this upper limit: the latest possible node at which response $\boldsymbol{\alpha_h}$ gets carried out, given that response $\boldsymbol{\alpha_k}$ is performed at time t_k. Note that $t_h \leq t_h^k$ since by definition t_h^k is an upper bound on t_h. We can now show:

Theorem 2. *Let `WTR` $= \langle \boldsymbol{e}_{\mathsf{s}}, \boldsymbol{\alpha}_1 : \delta_1, \boldsymbol{\alpha}_2 : \delta_2, \ldots, \boldsymbol{\alpha}_{k-1} : \delta_{k-1}, \boldsymbol{\alpha}_k \rangle$ be an instance of* WTR*, and assume that `WTR` is solved in a system $\mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$. Assume that $\boldsymbol{e}_{\mathsf{s}}$ occurs in $r \in \mathcal{R}$, and that $\boldsymbol{\alpha}_k$ takes place at time t_k in r. Then*

$$(\mathcal{R}, r) \vDash \; K_{\alpha_k} K_{\beta_{k-1}^k} \cdots K_{\beta_1^k} \mathsf{occurs}_{t_1^k}(\boldsymbol{e}_{\mathsf{s}}).$$

Thus, every protocol that coordinates responses according to `WTR` must, in particular, ensure that a specific nested nb-knowledge formula will hold. Indeed, observe that if `WTR` $= \langle \boldsymbol{e}_{\mathsf{s}}, \boldsymbol{\alpha}_1 : \delta_1, \boldsymbol{\alpha}_2 : \delta_2, \ldots, \boldsymbol{\alpha}_{k-1} : \delta_{k-1}, \boldsymbol{\alpha}_k \rangle$ is satisfied in the system $\mathcal{R}$, then every sub-instance $\mathtt{WTR}_i = \langle \boldsymbol{e}_{\mathsf{s}}, \boldsymbol{\alpha}_1 : \delta_1, \ldots, \boldsymbol{\alpha}_{i-1} : \delta_{i-1}, \boldsymbol{\alpha}_i \rangle$ with $i < k$ of `WTR` is also satisfied in $\mathcal{R}$. Hence, Theorem 2 ensures that

$$(\mathcal{R}, r) \vDash \; K_{\alpha_i} K_{\beta_{i-1}^i} \cdots K_{\beta_1^i} \mathsf{occurs}_{t_1^i}(\boldsymbol{e}_{\mathsf{s}})$$

must similarly hold, for all $i = 1, \ldots, k$.

Theorem 2 shows that coordinating a solution to a WTR coordination problem requires realising particular nested nb-knowledge formulas at each responding agent. Theorem 1 showed that such nested formulas can be attained only by constructing a corresponding uneven centipede. Combining the two yields the following corollary, directly establishing uneven centipedes as necessary communication patterns for solving WTR problems. Note that the epistemic formalism has played its part and is no longer required in order to state the result.

Corollary 1. *Let `WTR` $= \langle \boldsymbol{e}_{\mathsf{s}}, \boldsymbol{\alpha_1} : \delta_1, \boldsymbol{\alpha_2} : \delta_2, \ldots, \boldsymbol{\alpha_{k-1}} : \delta_{k-1}, \boldsymbol{\alpha_k} \rangle$ be an instance of* WTR*, and assume that P solves `WTR` in γ^{max}. Assume that $\boldsymbol{e}_{\mathsf{s}}$ occurs at node α_0 in $r \in \mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$, and, for $h = 1, \ldots, k$ let $\alpha_h = \langle i_h, t_h \rangle$ be the node at which response $\boldsymbol{\alpha_h}$ is performed. Using the notation of Theorem 2, there is an uneven centipede for $\langle \alpha_0, \beta_1^i, \ldots, \beta_{i-1}^i, \alpha_i \rangle$ in r, for every $i = 1, \ldots, k$.*

4 Common Knowledge and Tight Bounds

In [4], a causal structure called a *broom* was defined and shown to be necessary and sufficient for attaining common knowledge. In this section we examine nb-common knowledge and its relation to communication and coordination. Just as nb-nested knowledge requires an extension to the centipede structure, nb-common knowledge can only arise if the *uneven broom* communication structure, seen in Figure 2b and defined below, is realized in the run. ("Uneven" again comes from the broom's uneven legs.)

Definition 6 (Uneven broom). *Let* α_0 *be a node and* $A = \{\alpha_1, \ldots, \alpha_k\}$ *a set of nodes. Node* θ *is an* (uneven) broom *for* $\langle \alpha_0, A \rangle$ *in* r *if* $\theta \dashrightarrow \alpha_h$ *holds for all* $h = 1, .., k$*, and* $\alpha_0 \rightsquigarrow \hat{\theta}$*.*

The case in which the time components in all nodes of A are identical gives rise to the *broom* structures of [4], where gaining common knowledge is shown to require the construction of a broom. Since coordinating simultaneous actions requires common knowledge [8,7,10], brooms were shown to be necessary for ensuring simultaneity. We now show that the uneven broom captures a necessary causal structure underlying nb-common knowledge to arise.

Theorem 3. *Let* $\boldsymbol{e}_{\mathsf{s}}$ *be an external input occurring at* α_0 *in* r*, and let* $t \geq 0$*. If* $(\mathcal{R}, r) \vDash C_A \mathsf{occurs}_t(\boldsymbol{e}_{\mathsf{s}})$*, then there is a uneven broom* θ *for* $\langle \alpha_0, A \rangle$ *in* r*.*

This theorem shows that attaining nb-common knowledge regarding the occurrence of a spontaneous event can only be done based on a particular individual *pivotal* node (possibly a different node in different runs).

Whereas common knowledge is closely related to simultaneity, nb-common knowledge can be shown to be related to a notion of tightly-timed coordination:

Definition 7 (Tightly Timed Response). *Let* e_{s} *be an external input non-deterministic event. A protocol* P *solves the instance*

$$\mathsf{TTR} = \langle e_{\mathsf{s}}, \boldsymbol{\alpha_1} : \delta_1, \boldsymbol{\alpha_2} : \delta_2, \ldots, \boldsymbol{\alpha_k} : \delta_k \rangle$$

of the Tightly Timed Response *problem if it guarantees that*

1. *every response* $\boldsymbol{\alpha_h}$*, for* $h = 1, \ldots, k$*, occurs in a run iff the trigger event* e_{s} *occurs in that run.*
2. *For every* $h, g \leq k$ *the relative timing of the responses is exactly the difference in the associated delta values:* $t_h - t_g = \delta_h - \delta_g$

Observe that simultaneous coordination (i.e., the *simultaneous response* problem of [4]) can be specified by a TTR instance in which $\delta_1 = \cdots = \delta_k = 0$. Intuitively, a TTR specification determines exact time differences between the times at which any two responses occur. Thus, when an agent performs a response it knows when all other responses occur. As a result, responses in TTR give rise to nb-common knowledge.

Theorem 4. *Assume that P solves an instance* TTR *with trigger $\boldsymbol{e}_{\mathsf{s}}$, in γ^{max}, and let $\mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$. Let $r \in \mathcal{R}$ be a run in which $\boldsymbol{e}_{\mathsf{s}}$ occurs, and let $A = \{\alpha_1, \ldots, \alpha_k\}$ be the nodes at which the responses of* TTR *occur in r. Let $\alpha_h = \langle i_h, t_h \rangle$ be the earliest node in A. Then* $(\mathcal{R}, r) \vDash C_A\ \mathsf{occurs}_{t_h}(\boldsymbol{e}_{\mathsf{s}})$.

This theorem reduces tight coordination to nb-common knowledge. Combining it with Theorem 3, we can show that uneven brooms are necessary for tight coordination:

Corollary 2. *Assume that P solves an instance* TTR *with trigger $\boldsymbol{e}_{\mathsf{s}}$ in γ^{max}, and let $\mathcal{R} = \mathcal{R}(P, \gamma^{\mathsf{max}})$. Let $r \in \mathcal{R}$ be a run in which $\boldsymbol{e}_{\mathsf{s}}$ occurs at α_0, and let A be the nodes at which responses are performed. The time differences between nodes of A conform with* TTR *and there is an uneven broom θ for $\langle \alpha_0, A \rangle$ in r.*

We remark that while Corollaries 1 and 2 state necessary causal conditions for distributed coordination, these are in a precise sense both necessary *and sufficient*. Employing a *full-information* protocol, in which agents send their whole history to all neighbors in every round, proofs that mimic those in [5] show that the agents they can act precisely when the appropriate centipede or broom is realized in the run. The analysis thus provides provably optimal solutions to weakly-timed coordination and tightly-timed coordination, two natural classes of distributed coordination tasks.

5 Discussion

This paper explores the implications of a new formalism for epistemic statements upon the notions of nested and common knowledge. The formalism is used as an intermediate representation, enabling us to relate communication patterns to coordination tasks along the lines of [3,4].

A minor change to the standard epistemic formalism, using node-based formulas and agent-time semantics, allows a proper extension of the state of the art. The fact that the $\mathcal{L}_0$-based analysis of [3,4] carries over smoothly to $\mathcal{L}_1$ shows the very close connection between nested knowledge and nested nb-knowledge, and similarly between common knowledge and nb-common knowledge. Moreover, it yields genuine insight into distributed coordination, by exposing the logical connections between linear ordering and weakly-timed ordering, and between simultaneity and tightly-timed coordination.

Our causal analysis of weakly timed coordination can clearly be carried out using a temporal-epistemic formalism, although the analysis of tightly-timed coordination cannot. Node-based common knowledge is not expressible in $\mathcal{L}_0$. In a follow-up to the current paper, Gonczarowski and Moses define a more general variant of common knowledge, based on a *vectorial fixedpoint* operator [9]. They use a relative-time formalism to show more general connections between distributed coordination and epistemic states than shown here.

In conclusion, this paper uses an extended logic of knowledge as a tool for analysing causality in distributed and multi-agent systems. It provides further evidence for the strong connection between epistemic formalisms, causality and coordination. Many issues remain open to future exploration, including the logical properties of $\mathcal{L}_1$ and agent-time semantics: Expressiveness, completeness, and complexity.

Acknowledgements. We are grateful to the reviewers for their many useful comments. This work was supported in part by Israel Science Foundation (ISF) under Grant 1520/11. The first author was supported in part by the Arlene & Arnold Goldstein Center at the Technions autonomous systems program.

References

1. Alur, R., Henzinger, T.: Logics and Models of Real-time: A Survey. In: Huizing, C., de Bakker, J.W., Rozenberg, G., de Roever, W.-P. (eds.) REX Workshop 1991. LNCS, vol. 600, pp. 74–106. Springer, Heidelberg (1992)
2. Areces, C., ten Cate, B.: Hybrid logics. In: Blackburn, P., Wolter, F., van Benthem, J. (eds.) Handbook of Modal Logics. Elsevier (2006)
3. Ben-Zvi, I.: Causality, Knowledge and Coordination in Distributed Systems. PhD thesis, Technion, Israel (2011)
4. Ben-Zvi, I., Moses, Y.: Beyond Lamport's *Happened-Before*: On the Role of Time Bounds in Synchronous Systems. In: Lynch, N.A., Shvartsman, A.A. (eds.) DISC 2010. LNCS, vol. 6343, pp. 421–436. Springer, Heidelberg (2010)
5. Ben-Zvi, I., Moses, Y.: On interactive knowledge with bounded communication. Journal of Applied Non-Classical Logics 21(3-4), 323–354 (2011)
6. Chandy, K.M., Misra, J.: How processes learn. Distributed Computing 1(1), 40–52 (1986)
7. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Common knowledge revisited. In: Shoham, Y. (ed.) Proc. Sixth Conference on Theoretical Aspects of Rationality and Knowledge, pp. 283–298. Morgan Kaufmann, San Francisco (1996)
8. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning about Knowledge. MIT Press, Cambridge (2003)
9. Gonczarowski, Y., Moses, Y.: Timely common knowledge: Characterising asymmetric distributed coordination via vectorial fixed points (in preparation, 2012)
10. Halpern, J.Y., Moses, Y.: Knowledge and common knowledge in a distributed environment. Journal of the ACM 37(3), 549–587 (1990); A preliminary version appeared in Proc. 3rd ACM Symposium on Principles of Distributed Computing (1984)
11. Halpern, J.Y., Vardi, M.Y.: The complexity of reasoning about knowledge and time, I: lower bounds. Journal of Computer and System Sciences 38(1), 195–237 (1989)
12. Lamport, L.: Time, clocks, and the ordering of events in a distributed system. Communications of the ACM 21(7), 558–565 (1978)

Dynamic Epistemic Logic for Channel-Based Agent Communication

Katsuhiko Sano and Satoshi Tojo

School of Information Science, Japan Advanced Institute of Science and Technology
`{v-sano,tojo}@jaist.ac.jp`

Abstract. This paper studies channel-based agent communication in terms of dynamic epistemic logic. First, we set up two sorted syntax which can deal with not only each agent's belief but also agents and channels between them. Second, we propose a context-sensitive 'inform'-action operator whose effectivity always assumes the existence of channel between agents. Its context-sensitivity can be achieved by downarrow binder from hybrid logic. Third, we provide complete Hilbert-style axiomatizations for both static and dynamic parts of our logic.

1 Introduction

It has been long since the notion of *agent* became the prevalent idea to represent artificial intelligence, where we mean by agent a computer system, situated in some environment, that is capable of flexible autonomous action in order to meet its design objectives [1, p.8]. Since the communication is the most distinguished feature of the presence of intelligence, its logical formalization in rational agents has commonly been accepted as an important research goal. For example, based on the mobile agents platform by FIPA/ACL [2], [3] has added *communication channel* in multi-agent interaction to represent communicability between agents. [4] proposed a research program to investigate how knowledge, belief, and preferences are influenced by social relationship, and set up *Facebook Logic* for an analysis of knowledge in a social network.

In the above history of formalization of agent communication, we raise the following three requirements for our logical study of agent-communication.

(i) An informing action is basically initiated locally; thus, when information is correctly transferred, a sender should have a communication channel to the recipient.
(ii) An existence of channel may vary through a given state.
(iii) An effect of informing action at a state should be valid only on the state.

In this paper, we propose two-dimensional semantics satisfying (ii) and the informing action operator possessing three indices to implement the context-sensitivity, together with a sender and a recipient agent ((i) and (iii)). A semantic core of our paper shared with [4] can be summarized as in the following diagram:

$$w \models B_a(a \text{ is in India}) \rightsquigarrow (w, a) \models B(\text{ - is in India}).$$

We incorporate the information '*a*' of agents into the Kripke semantics of B_a(*a* is in India) (the agent *a* believes that *a* is in India) and regard *B*(- is in India) as

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 109–120, 2013.

a state-dependent property of the agent a, i.e., '- believes that he/she has the property: - is in India'.

We proceed as follows. Section 2 introduces our static syntax and its two-dimensional semantics, which is the same one as in [4]. Unlike [4], however, we also add a machinery of hybrid logic (nominals, satisfaction operators, and downarrow binder, for readers unfamiliar with hybrid logic, see, e.g., [5]) to the dimension of possible worlds. Section 3 introduces running examples of this paper. Section 4 introduces a dynamic informing action operator and Section 5 investigates its semantic consequences. Section 6.1 gives a complete axiomatization of two-dimensional hybrid logic with frame axioms and global assumptions on models (Theorem 1). As far as the authors know, this is an unknown result of a hybrid expansion of Facebook Logic. Section 6.2 employs reduction axioms for our dynamic operator to give a complete axiomatization of our dynamic logic (Theorem 2). Section 7 concludes this paper.

2 Two-Dimensional Semantics for Agent Beliefs via Channels

Our syntax consists of the set $\mathsf{N}_1 = \{ i, j, ... \}$ of state nominals, the set $\mathsf{N}_2 = \{ n, m, ... \}$ of agent nominals, the set $\mathsf{P} = \{ p, q, ... \}$ of unary *properties* of agents (or, *concept names* in description logics [6]), the belief operator B for agents, the channel operator C, the boolean connectives $\neg$, $\wedge$, the satisfaction operator @, and the downarrow binder $\downarrow$. The set $\mathcal{F}$ of all *formulas* of our syntax is defined inductively as follows:

$$\varphi ::= i \mid n \mid p \mid \neg\varphi \mid \varphi \wedge \psi \mid B\varphi \mid C\varphi \mid @_i\varphi \mid @_n\varphi \mid \downarrow i.\varphi \mid \downarrow n.\varphi,$$

where $i \in \mathsf{N}_1$, $n \in \mathsf{N}_2$ and $p \in \mathsf{P}$. We define $\langle C\rangle\varphi := \neg C \neg\varphi$ and $\langle B\rangle\varphi := \neg B \neg\varphi$. We also introduce the Boolean connectives as ordinary abbreviations. We can read the following formulas intuitively as:

p	'the current agent has a property p'.
Cp	'all the agents accessible via channels from the current agent satisfy p'.
$@_n \langle C\rangle m$	'there is a channel relation from n to m'.
$\langle C\rangle B@_n p$	'some agents accessible via channels from the current agent believe that the agent n satisfies p'.

For the above property (or concept name) p in P, the readers can take Father, Mother, Parents, etc. More examples can be found in [6,4].

Let us move to the semantics. Roughly speaking, we need to incorporate channel structures between agents into Kripke frames of logic of belief. It is also natural to assume that channel structures may vary through worlds from a given Kripke frame. We also reflect this aspect into our semantics. A *social Kripke frame* (*s-frame*, in short) $\mathfrak{F} = (W, A, R, \asymp)$ consists of a non-empty set W of possible worlds, a non-empty set A of agents, A-indexed family $R = (R_a)_{a\in A}$ of binary relations on W[1], and W-indexed family

---

[1] This paper does not assume any assumption on R, but one can impose positive and/or negative introspection as frame conditions, whose corresponding axioms are $Bp \rightarrow BBp$ and $\neg Bp \rightarrow B\neg Bp$, respectively. As for the consistency $\langle B\rangle\top$ of agents' belief, one can add it in a static setting, but our dynamic operator may destroy the corresponding frame condition (the seriality of R_a). See Definition 8.

$\asymp = (\asymp_w)_{w \in W}$ of binary relations on A. R_a is the same concept as an accessibility relation for the agent a in Kripke semantics for logic of belief, while $\asymp_w \subseteq A \times A$ reflect the idea of channel structures varying through worlds[2]. Define $R_a(w) := \{ w' \in W \mid wR_aw' \}$, i.e., all the R_a-accessible worlds from w. A *social Kripke model* (*s-model*, in short) $\mathfrak{M} = (\mathfrak{F}, V)$ is a pair of s-frame $\mathfrak{F}$ and a valuation $V : \mathsf{N}_1 \cup \mathsf{N}_2 \cup \mathsf{P} \to \mathcal{P}(W \times A)$ satisfying $V(i) = \{ w \} \times A$ for some $w \in W$ ($i \in \mathsf{N}_1$), and $V(n) = W \times \{ a \}$ for some $a \in A$ ($n \in \mathsf{N}_2$). If we regard $W \times A$ as a two-dimensional space and W and A as x-axis and y-axis respectively, then the denotation $V(i)$ is a vertical line and the denotation $V(a)$ is a horizontal line over $W \times A$. When $V(i) = \{ w \} \times A$, we usually write $\underline{i}$ to mean w, and so, $V(i) = \{ \underline{i} \} \times A$. Similarly, we use the notation $\underline{n}$ as $V(n) = W \times \{ \underline{n} \}$. Given any s-frame $\mathfrak{F} = (W, A, R, \asymp)$ and a valuation V on $\mathfrak{F}$, we define a *satisfaction relation* $\models$ as follows:

$$\begin{array}{lll}
\mathfrak{M}, (w, a) \models i & \text{iff} & \underline{i} = w, \\
\mathfrak{M}, (w, a) \models n & \text{iff} & \underline{n} = a, \\
\mathfrak{M}, (w, a) \models p & \text{iff} & (w, a) \in V(p), \\
\mathfrak{M}, (w, a) \models \neg \varphi & \text{iff} & \mathfrak{M}, (w, a) \not\models \varphi, \\
\mathfrak{M}, (w, a) \models \varphi \wedge \psi & \text{iff} & \mathfrak{M}, (w, a) \models \varphi \text{ and } \mathfrak{M}, (w, a) \models \psi, \\
\mathfrak{M}, (w, a) \models B\varphi & \text{iff} & wR_aw' \text{ implies } \mathfrak{M}, (w', a) \models \varphi, \text{ for all } w' \in W, \\
\mathfrak{M}, (w, a) \models C\varphi & \text{iff} & a \asymp_w a' \text{ implies } \mathfrak{M}, (w, a') \models \varphi, \text{ for all } a' \in A, \\
\mathfrak{M}, (w, a) \models @_i\varphi & \text{iff} & \mathfrak{M}, (\underline{i}, a) \models \varphi, \\
\mathfrak{M}, (w, a) \models @_n\varphi & \text{iff} & \mathfrak{M}, (w, \underline{n}) \models \varphi, \\
\mathfrak{M}, (w, a) \models \downarrow i. \varphi & \text{iff} & (\mathfrak{F}, V[i := w]), (w, a) \models \varphi, \\
\mathfrak{M}, (w, a) \models \downarrow n. \varphi & \text{iff} & (\mathfrak{F}, V[n := a]), (w, a) \models \varphi,
\end{array}$$

where $V[i := w]$ (or $V[n := a]$) is the same valuation as V except $V(i) = \{ w \} \times A$ (or $V(n) = W \times \{ a \}$, respectively). $\downarrow i.$ and $\downarrow n.$ allow us to 'bookmark' the current world and agent with the labels i and n, respectively. In order to avoid complication of notations, we keep using nominals for bound variables of downarrow binders.

In the literatures of logic of belief, it is common to use the belief operator $B_n p$ (read: 'the agent n believes that φ'). In our setting, we can express the similar content by $@_n B\varphi$ whose semantics is calculated as

$$\mathfrak{M}, (w, a) \models @_n B\varphi \ \text{ iff } \ wR_{\underline{n}}w' \text{ implies } \mathfrak{M}, (w', \underline{n}) \models \varphi, \text{ for all } w' \in W.$$

However, there is also a difference from epistemic/doxastic logics. For example, consider $@_i B$(- is in India). We can regard this formula as the property of agents that he/she believes that he/she is in India at the state i. Therefore, we can talk about properties of agents as well as properties of states.

Note that $B @_n \varphi$ is different from $@_n B\varphi$, because the former tells the belief of the current agent but the latter is concerned with the belief of the agent n. We read $B @_n \varphi$ as 'the current agent believes that the agent n satisfies φ'.

Given any s-model $\mathfrak{M}$ and any set Γ of formulas, $\mathfrak{M}, (w, a) \models \Gamma$ means that $\mathfrak{M}, (w, a) \models \varphi$ for all $\varphi \in \Gamma$. Γ is *valid* on $\mathfrak{M}$ (written: $\mathfrak{M} \models \Gamma$) if $\mathfrak{M}, (w, a) \models \Gamma$ for all (w, a) of $\mathfrak{M}$. Γ is *valid* on $\mathfrak{F}$ if Γ is valid on $(\mathfrak{F}, V)$ for all valuations V on $\mathfrak{F}$.

---

[2] We do not impose any assumption on $\asymp = (\asymp_w)_{w \in W}$ in this paper. For example, however, it might be non-symmetric (the negation of symmetry). If we (informally) define $\asymp$ by $a \asymp_w b$ if the agent a have a phone number of the agent b at a state w, then we can regard $\asymp_w$ as non-symmetric.

3 Running Examples of This Paper

Let us consider the following scenario: Ann just signed up Facebook and has no friend yet. She is very interested in a new mobile (say, iPhone5) but does not decide to buy it. She wants to get more friends in Facebook to listen to opinions from the others. Assume that $\mathsf{P} = \{ p \}$, where 'p' means '- will buy a mobile'.

Definition 1. *Define an* ordinary Kripke model $(S, \mathcal{R}, v)$ *where* $S := \{ s_{\mathbf{u}}, s_{\mathbf{t}}, s_{\mathbf{f}} \}$, $\mathcal{R} := \{ (s_{\mathbf{u}}, s_{\mathbf{t}}), (s_{\mathbf{u}}, s_{\mathbf{f}}) \} \cup \{ (x, x) \,|\, x \in S \}$ *and* $v(p) := \{ s_{\mathbf{t}} \}$.

We can regard $(S, \mathcal{R}, v)$ as a *s-model* for a single agent, say Ann, as follows. Let $A = \{ a \}$ (a means 'Ann') and define $W := S$, $R_a := \mathcal{R}$, $\asymp_x := \emptyset$ for all $x \in S$, and $V(p) = \{ (s_{\mathbf{t}}, a) \}$. Then, one can easily verify that Ann does not believe at $s_{\mathbf{u}}$ that she will buy a mobile and that she will not buy it (i.e., neither Bp nor $B \neg p$ is true at $(s_{\mathbf{u}}, a)$), while she believes at $s_{\mathbf{t}}$ (or $s_{\mathbf{f}}$) that she will buy a mobile (or will not buy it, respectively). This is a reason why we employ the indices **u**, **t**, and **f** in the elements of S.

Suppose that Ann now got a friend, whose name is Bea. Bea and Cate, another user, are friends, but Ann and Cate are not friends yet. In syntactic side, let us set up $\mathsf{N}_2 = \{ \mathsf{AN}, \mathsf{BE}, \mathsf{CA} \}$. How can we construct s-model from the Kripke model $(S, \mathcal{R}, v)$ above? We regarded $(S, \mathcal{R}, v)$ as modeling a single agent. In order to model a community of three agents, it is natural to prepare three copies of $(S, \mathcal{R}, v)$.

Definition 2. *Define* $\mathfrak{M}_1 = (W, A, R, \asymp, V)$ *as follows. Let* $W = S \times S \times S$ *and* $A = \{ a, b, c \}$. *When* $(x_a, x_b, x_c) \in W$, *we assume that* x_a, x_b, *and* x_c *represent the current state of Ann* (a), *Bea* (b), *and Cate* (c), *respectively. As for* R, *we define* R_a *by* $(x_a, x_b, x_c) R_a (x_a, x_b, x_c)$ iff $x_a \mathcal{R} y_a$, R_b *by* $(x_a, x_b, x_c) R_b (x_a, x_b, x_c)$ iff $x_b \mathcal{R} y_b$, *and similarly for* R_c. *Define* $\asymp_{(x_a, x_b, x_c)} = \{ (a, b), (b, a), (b, c), (c, b) \}$ *for all* $(x_a, x_b, x_c) \in W$. *Finally, define a valuation* V *so as* $V(\mathsf{AN}) = W \times \{ a \}$, $V(\mathsf{BE}) = W \times \{ b \}$, $V(\mathsf{CA}) = W \times \{ c \}$ *and* $((x_a, x_b, x_c), a) \in V(p)$ iff $x_a = s_{\mathbf{t}}$, $((x_a, x_b, x_c), b) \in V(p)$ iff $x_b = s_{\mathbf{t}}$, *and* $((x_a, x_b, x_c), c) \in V(p)$ iff $x_c = s_{\mathbf{t}}$. (*remark that we assume* $\mathsf{P} = \{ p \}$, *and an arbitrary valuation suffices for any* $i \in \mathsf{N}_1$.)

An underlying idea of, e.g., R_a is that Ann cannot guess how Bea and Cate can imagine their possible states from the current state.

Example 1. Suppose that all the agents except Cate will not buy a mobile, i.e., $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}) \in W$ is a current tuple of states.

(i) Ann and Bea can see the state $s_{\mathbf{f}}$ from $s_{\mathbf{u}}$, while Cate cannot do that. Then, each of Ann and Bea does not believe that she will buy a mobile, but Cate believes so. In $\mathfrak{M}_1$, Bea is a friend of Cate, and so, $\mathfrak{M}_1, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models \langle C \rangle Bp$ (Bea has a friend who believes that she will buy a mobile).

(ii) Let us also check an example of iterated belief: it is true that Bea does not believe that Ann believes that she will buy a mobile at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_1$. Let us see why. Since Ann's belief state is $s_{\mathbf{u}}$, we obtain $\mathfrak{M}_1, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), a) \models \neg Bp$, which implies $\mathfrak{M}_1, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models \neg @_{\mathsf{AN}} Bp$. Since $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}) R_b (s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ holds, we finally obtain $\mathfrak{M}_1, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models \neg B @_{\mathsf{AN}} Bp$. At $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_1$, we can also verify that Cate does not believe that Ann believes that she will buy a mobile: $\mathfrak{M}_1, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), c) \models \neg B @_{\mathsf{AN}} Bp$. ■

Consider the following modifications to $\mathfrak{M}_1$: Later Bea and Cate are no longer friends, but Ann and Bea are still friends. This gives us another s-model $\mathfrak{M}_2$.

Definition 3. *Define s-model* $\mathfrak{M}_2$ *as the same models as* $\mathfrak{M}_1$ *except that we replace* $\asymp$ *of* $\mathfrak{M}_1$ *with* $\approx_{(x_a,x_b,x_c)} = \{ (a,b), (b,a) \}$ *for all* $(x_a, x_b, x_c) \in W$*.*

Example 2. Now, in $\mathfrak{M}_2$, Bea can no longer access Cate, and so, $\mathfrak{M}_2, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models \neg \langle C \rangle Bp$ (Bea does not have a friend who believes that she will buy a mobile). As for the iterated beliefs above, we can still say that Bea and Cate do not believe that Ann believes that she will buy a mobile at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_2$, because the truth of them is independent of channel structures. ■

Note that both of $\asymp$ of $\mathfrak{M}_1$ and $\approx$ of $\mathfrak{M}_2$ are constant or rigid, i.e., $\asymp_{(x_a,x_b,x_c)}$ is always the same for all $(x_a, x_b, x_c) \in W$ and similarly for $\approx$ (we will consider a channel relation depending on an element of W later in *Example* 3).

4 Dynamic Semantics for Context-Sensitive Agent Communication

When an agent informs one of the other agents of something, our basic assumption is that we need a (context-dependent) channel between those agents. The notion of channel was formalized in terms of $\asymp$-relation in our s-model.

When the agents cooperate to achieve one goal, they need to communicate with each other. Moreover, we assume that it is important to specify *when* agents communicate, since each agent's surroundings are ever changing. Even if a message to an agent a from an agent b is useful to a at an instance t, it may become useless to a at an instant $t + 1$. This is the difference from public announcement logic (PAL) by Plaza [7]. Rather, we share the semantic idea with [8], where *time-dependent* command was proposed.

For this aim, what we want to do is to introduce the action operator $[\varphi!_m]$, whose meaning is 'after the *current agent* informs the agent m of "the current agent satisfies φ" in the *current state*.' If there is a channel from the current agent to m, this action $[\varphi!_m]$ will change m's belief only at the current state. Otherwise, the action $[\varphi!_m]$ will not change m's belief. If φ is $@_n\psi$, then $[(@_n\psi)!_m]$ means 'after the current agent informs, at the current state, the agent m of "the agent n satisfies φ".'

There is a technical problem to introduce $[\varphi!_m]$ into our static syntax. We cannot reduce the occurrences of $[\varphi!_m]$ when our syntax has two kinds of satisfaction operators $@_i$ and $@_n$. That is, $[\varphi!_m]@_i\psi \leftrightarrow @_i[\varphi!_m]\psi$ and $[\varphi!_m]@_n\psi \leftrightarrow @_n[\varphi!_m]\psi$ do not hold in general. Let us concentrate on the first one. Since an inform-action $[\varphi!_m]$ occurs at the world $\underline{i}$ in $@_i[\varphi!_m]\psi$, but it occurs at the current world in $[\varphi!_m]@_i\psi$, the effects of two actions should be different in terms of worlds.

In order to define $[\varphi!_m]$, we borrow the idea of [4, pp.184-6] to define an indexical public announcement operator into this context. That is, we first introduce $[\varphi!^i_{(n,m)}]$ ('after the agent n informs, in the state i, the agent m of "n is φ", ψ') for context-sensitive agent communication, and then define our intended operator $[\varphi!_m]$ with the help of two kinds of downarrow binders.

Let us expand our static syntax with a new dynamic operator $[\varphi!^i_{(n,m)}]$ and denote the set of all formulas of this new syntax by $\mathcal{F}^+$. Given any s-models $\mathfrak{M} = (W, A, R, \asymp, V)$, we can provide the semantic clause for $[\varphi!^i_{(n,m)}]\psi$ as follows.

Table 1. Reduction Axioms for $[\varphi!^{i}_{(n,m)}]$

$[\varphi!^{i}_{(n,m)}]\psi$	$\leftrightarrow \psi \quad (\psi \in \mathsf{P} \cup \mathsf{N}_1 \cup \mathsf{N}_2)$
$[\varphi!^{i}_{(n,m)}]\neg\psi$	$\leftrightarrow \neg[\varphi!^{i}_{(n,m)}]\psi$
$[\varphi!^{i}_{(n,m)}]\psi \wedge \theta$	$\leftrightarrow [\varphi!^{i}_{(n,m)}]\psi \wedge [\varphi!^{i}_{(n,m)}]\theta$
$[\varphi!^{i}_{(n,m)}]C\psi$	$\leftrightarrow C[\varphi!^{i}_{(n,m)}]\psi$
$[\varphi!^{i}_{(n,m)}]B\psi$	$\leftrightarrow ((m \wedge @_n \langle C \rangle m \wedge i) \to B(@_n\varphi \to [\varphi!^{i}_{(n,m)}]\psi))\wedge$
	$(\neg(m \wedge @_n \langle C \rangle m \wedge i) \to B[\varphi!^{i}_{(n,m)}]\psi)$
$[\varphi!^{i}_{(n,m)}]@_j\psi$	$\leftrightarrow @_j[\varphi!^{i}_{(n,m)}]\psi \quad (j \in \mathsf{N}_1)$
$[\varphi!^{i}_{(n,m)}]@_l\psi$	$\leftrightarrow @_l[\varphi!^{i}_{(n,m)}]\psi \quad (l \in \mathsf{N}_2)$
$[\varphi!^{i}_{(n,m)}]\downarrow j.\,\psi$	$\leftrightarrow \downarrow j.\,[\varphi!^{i}_{(n,m)}]\psi \quad (j \in \mathsf{N}_1$ is fresh in $\varphi)$
$[\varphi!^{i}_{(n,m)}]\downarrow l.\,\psi$	$\leftrightarrow \downarrow l.\,[\varphi!^{i}_{(n,m)}]\psi \quad (l \in \mathsf{N}_2$ is fresh in n, m, and $\varphi)$
$[\varphi!^{i}_{(n,m)}][\psi!^{j}_{(l,e)}]\theta$	$\leftrightarrow ((m \wedge @_n \langle C \rangle m \wedge i \wedge e \wedge @_l \langle C \rangle e \wedge j) \to [(\varphi \wedge @_l[\varphi!^{i}_{(n,m)}]\psi)!^{i}_{(n,m)}]\theta)\wedge$
	$(\neg(m \wedge @_n \langle C \rangle m \wedge i) \wedge e \wedge @_l \langle C \rangle e \wedge j) \to [(@_l[\varphi!^{i}_{(n,m)}]\psi)!^{i}_{(n,m)}]\theta)\wedge$
	$(\neg(e \wedge @_l \langle C \rangle e \wedge j) \to [\varphi!^{i}_{(n,m)}]\theta) \quad (n, m, l, e \in \mathsf{N}_2)$

$$\mathfrak{M}, (w, a) \models [\varphi!^{i}_{(n,m)}]\psi \ \text{ iff } \ \mathfrak{M}^{\varphi!^{i}_{(n,m)}}, (w, a) \models \psi,$$

where $\mathfrak{M}^{\varphi!^{i}_{(n,m)}} = (W, A, R^{\varphi!^{i}_{(n,m)}}, \asymp, V)$ and $R_a^{\varphi!^{i}_{(n,m)}}$ is defined by

$$R_a^{\varphi!^{i}_{(n,m)}}(w) = \begin{cases} R_{\underline{m}}(w) \cap [\![\varphi]\!]_{\underline{n}} & \text{if } a = \underline{m} \text{ and } \underline{n} \asymp_w \underline{m} \text{ and } w = \underline{i}; \\ R_a(w) & \text{o.w.} \end{cases}$$

where $[\![\varphi]\!]_a = \{\, w \in W \mid \mathfrak{M}, (w, a) \models \varphi \,\}$ for all $a \in A$.

Similarly to the static syntax, let us define the notion of validity for $\mathcal{F}^+$. Now, we can define the following operators for context-sensitive agent communication:

$[\varphi!_{(n,m)}]\psi := \downarrow i.\,[\varphi!^{i}_{(n,m)}]\psi$.
('after the agent n informs m of "n satisfies φ" in the current state, ψ').
$[\varphi!_m]\psi := \downarrow n.\ \downarrow i.\,[\varphi!^{i}_{(n,m)}]\psi$.
('after the current agent informs m of "I satisfy φ" in the current state, ψ').

Proposition 1. *All the reduction axioms in Table 1 are valid on all s-frames.*

5 Running Examples in Dynamic Context

In order to demonstrate that the action $[\varphi!_{(n,m)}]$ captures our motivation, let us consider the following three successive inform-actions in Example 1 of section 3. Suppose that the current world is $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_1$.

(i) Bea informs Ann that Ann will buy a mobile: $[(@_{\mathsf{AN}}p)!_{(\mathsf{BE},\mathsf{AN})}]$
(ii) Ann informs Bea that Ann believes that she will buy a mobile: $[(Bp)!_{(\mathsf{AN},\mathsf{BE})}]$
(iii) Bea informs Cate that Ann believes that she will buy a mobile: $[(@_{\mathsf{AN}}Bp)!_{(\mathsf{BE},\mathsf{CA})}]$

Recall from Example 1 that, at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_1$, Ann does not believe that she will buy a mobile ($\neg\, @_{\mathsf{AN}}Bp$). Recall also that Bea and Cate do not believe that Ann believes that she will buy a mobile ($\neg\, @_{\mathsf{BE}}B@_{\mathsf{AN}}Bp$ and $\neg\, @_{\mathsf{CA}}B@_{\mathsf{AN}}Bp$). Let us see each effect of the inform-actions above one by one.

After the first inform action $[(@_{\mathsf{AN}} p)!_{(\mathsf{BE},\mathsf{AN})}]$ (this succeeds, since there is a channel from Bea to Ann), Ann's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ becomes $\{ s_{\mathbf{t}} \} \times S \times S = R_a((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})) \cap [\![@_{\mathsf{AN}} p]\!]_b$ [3]. Therefore, after the first action, Ann changes her belief, i.e., she now believes that she will buy a mobile ($@_{\mathsf{AN}} Bp$).

Since there is a channel from Ann to Bea in $\mathfrak{M}_1$, the second action $[(Bp)!_{(\mathsf{AN},\mathsf{BE})}]$ changes Bea's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ into $\{ s_{\mathbf{t}}, s_{\mathbf{u}} \} \times S \times S$ (note that the first action does not change Bea's accessibility relation). After the second inform-action, Bea changes her belief on Ann , i.e., Bea now *believes* that Ann believes that she will buy a mobile ($@_{\mathsf{BE}} B @_{\mathsf{AN}} Bp$) at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$.

Because there is a channel from Bea to Cate in $\mathfrak{M}_1$, the third action $[(@_{\mathsf{AN}} Bp)!_{(\mathsf{BE},\mathsf{CA})}]$ also succeeds in changing Cate's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ into $\{ s_{\mathbf{t}}, s_{\mathbf{u}} \} \times S \times S$. Then, after the above successive inform-actions, Cate changes her belief on Ann, i.e., Cate *believes* that Ann believes that she will buy a mobile ($@_{\mathsf{CA}} B @_{\mathsf{AN}} Bp$) at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$. This example demonstrates that, even if there is no direct channel between Ann and Cate, message passing via channels can change Cate's belief on Ann.

For comparison, consider the effect of the successive actions above at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_2$ from Example 2 of section 3, where there is no channel from Bea to Cate. At this world of $\mathfrak{M}_2$, recall from Example 2 that Cate still does not believe that Ann believes that she will buy a mobile ($\neg @_{\mathsf{CA}} B @_{\mathsf{AN}} Bp$). Unlike the case of $\mathfrak{M}_1$, the third action does not succeed in changing Cate's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$. Therefore, Cate does not change her belief on Ann, i.e., Cate still does not believe that Ann believes that she will buy a mobile ($\neg @_{\mathsf{CA}} B @_{\mathsf{AN}} Bp$) at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$.

Example 3 (Informing Channels). In our running example, channel relations of $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are *rigid*, i.e., channel relations are invariant through all elements of $W = S \times S \times S$. Let us consider non-rigid channels in this example and see an effect of informing a channel itself between agents. Let us take the following requirement on a relationship on Bea and Cate: Bea and Cate are friends in Facebook only when they have the same opinion for deciding to buy a mobile. Following this requirement, define a new channel relation $\sim$ by: $\sim_{(x_a,x_b,x_c)} = \{ (a,b), (b,a), (b,c), (c,b) \}$ (if $x_b = x_c$) and $\sim_{(x_a,x_b,x_c)} = \{ (a,b), (b,a) \}$ (if $x_b \neq x_c$). We define $\mathfrak{M}_3$ as the same s-models except we use $\sim$ instead of $\asymp$. Note that channels between Ann and Bea are still rigid. Throughout this example, we always assume that our current state is $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$. Then, we can say at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_3$ that Bea *does not* believe that she has a friend who will buy a mobile:

$$\mathfrak{M}_3, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models \neg B \langle C \rangle p.$$

This is because $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}) R_b (s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ and Bea does not have a friend who will buy a mobile at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_3$ (note that Bea's belief state $s_{\mathbf{u}}$ is different from Cate's belief state $s_{\mathbf{t}}$).

Suppose that Ann and Cate are not friends in Facebook, but they are so in real life. Cate told Ann that she will buy a mobile and that she wants to be a friend of Bea in Facebook. After chatting with Cate, Ann made the following successive inform-actions in Facebook:

---

[3] Note that $[\![@_{\mathsf{AN}} p]\!]_b = [\![p]\!]_a = \{ s_{\mathbf{t}} \} \times S \times S$ in $\mathfrak{M}_1$ and $R_a((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})) = S \times S \times S$.

(i) Ann informs of Bea that Cate will buy a mobile: $[(@_{\mathsf{CA}} p)!_{(\mathsf{AN},\mathsf{BE})}]$.
(ii) Ann informs of Bea that Cate is a friend of Bea: $[(@_{\mathsf{CA}} \langle C \rangle \mathsf{BE})!_{(\mathsf{AN},\mathsf{BE})}]$.

After the first action at $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ of $\mathfrak{M}_3$ (note that there is always a channel between Ann and Bea), Bea's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ become $S \times S \times \{ s_{\mathbf{t}} \}$. Furthermore, the second action will change Bea's accessible worlds from $(s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}})$ into $S \times \{ s_{\mathbf{t}} \} \times \{ s_{\mathbf{t}} \}$. After these two actions, Bea can only access to the tuple of states where both Bea and Cate will buy a mobile, i.e., Bea and Cate are friends by our definition of $\sim$. Therefore, after the above successive inform-action, Bea now believes that she has a friend who will buy a mobile. That is,

$$\mathfrak{M}_3, ((s_{\mathbf{u}}, s_{\mathbf{u}}, s_{\mathbf{t}}), b) \models [(@_{\mathsf{CA}} p)!_{(\mathsf{AN},\mathsf{BE})}][(@_{\mathsf{CA}} \langle C \rangle \mathsf{BE})!_{(\mathsf{AN},\mathsf{BE})}] B \langle C \rangle p.$$

In this way, an action of informing a channel itself can also change agents' belief. ■

6 Complete Axiomatizations of Static and Dynamic Logics

6.1 Hilbert-Style Axiomatization of Static Logic with Global Assumptions

This section gives a complete axiomatization of our intended logic in the *static* syntax.

If concept names Mother, Father, Parents are in P, it is natural to assume the equivalence $(\mathsf{Mother} \lor \mathsf{Father}) \leftrightarrow \mathsf{Parents}$ (regarded as 'TBox' in description logic [6]). We want to validate this particular equivalence at all agents and worlds in a given s-model. In this sense, we call it a *global assumption*. A global assumption could be any formula of $\mathcal{F}$ but it should be regarded as axioms in the level of s-model but not in the level of s-frame. In what follows, we will give a semantic consequence relation and a deducibility relation of our static syntax under the existence of global assumptions, which will increase an applicability of our framework.

Definition 4. *Given a set Φ of global assumptions and a class F of s-frames, φ is a* local consequence of Ψ under global assumptions Φ for F (*notation: $\Phi; \Psi \models_{\mathsf{F}} \varphi$*) *if, for all $\mathfrak{F} = (W, A, R, \asymp) \in \mathsf{F}$ and all valuations V on $\mathfrak{F}$ such that $(\mathfrak{F}, V) \models \Phi$ holds, $(\mathfrak{F}, V), (w, a) \models \Psi$ implies $(\mathfrak{F}, V), (w, a) \models \varphi$ for all $(w, a) \in W \times A$.*

Note that we restrict our attention to the set of valuations V on $\mathfrak{F}$ such that Φ is valid on s-model $(\mathfrak{F}, V)$ in this definition.

Let us move to the corresponding proof-theoretic derivability relation to $\Phi; \Psi \models_{\mathsf{F}} \varphi$. First of all, we do not allow the following *uniform substitutions* to global assumptions.

Definition 5. *σ is* a uniform substitution *if it is the inductive extension of a mapping sending $p \in \mathsf{P}$ to a formula and a nominal of N_u to a nominal of N_u ($u = 1, 2$).*

If we allows global assumptions to be closed under uniform substitutions, we can derive from $(\mathsf{Mother} \lor \mathsf{Father}) \leftrightarrow \mathsf{Parents}$ that $(\mathsf{Woman} \lor \mathsf{Man}) \leftrightarrow \mathsf{Parents}$, which is undesirable. On the other hand, we want to allow uniform substitutions to logical axioms such as tautologies, basic axioms of modal logic. Therefore, in order to incorporate global assumptions to a deducibility relation, we need to restrict the use of uniform substitutions carefully. First, we define the theoremhood under frame axioms (to capture the information of F in $\Phi; \Psi \models_{\mathsf{F}} \varphi$) and global assumptions Φ, and then define our intended deducibility relation.

Table 2. Axioms and Rules of Two-dimensional Hybrid Logic for Agent Beliefs via Channels

	Modal Axioms
CT	all classical tautologies
K	$\Box(p \to q) \to (\Box p \to \Box q) \quad (\Box \in \{B, C\})$.
	Hybrid Axioms for Nominals and Satisfaction Operators
K@	$@_\alpha(p \to q) \to (@_\alpha p \to @_\alpha q)$, where $\alpha = i$ or n.
Dual	$\neg @_\alpha p \leftrightarrow @_\alpha \neg p$, where $\alpha = i$ or n.
Ref	$@_\alpha \alpha$, where $\alpha = i$ or a.
Intro	$\alpha \land p \to @_\alpha p$, where $\alpha = i$ or n.
Agree	$@_\alpha @_\beta p \to @_\beta p$, where $(\alpha, \beta) = (i, j)$ or (n, m).
Back$_B$	$@_i p \to B @_i p$.
Back$_C$	$@_n p \to C @_n p$.
	Hybrid Axioms for Downarrow Binders
DA$_1$	$@_j(\downarrow j.\varphi \leftrightarrow \varphi[i/j])$
DA$_2$	$@_n(\downarrow m.\varphi \leftrightarrow \varphi[n/m])$
	Interaction Axioms
Com@	$@_n @_i p \leftrightarrow @_i @_n p$
Red@$_1$	$@_i a \leftrightarrow a$
Red@$_2$	$@_n i \leftrightarrow i$
Dcom$B@_2$	$@_n Bp \leftrightarrow @_n B @_n p$
Dcom$C@_1$	$@_i Cp \leftrightarrow @_i C @_i p$
	Rules
MP	$\varphi \to \psi, \varphi / \psi$
Nec$\Box$	$\varphi / \Box\varphi \quad (\Box \in \{B, C\})$.
Nec@	$\varphi / @_\alpha \varphi \quad (\alpha \in \mathsf{N}_1 \cup \mathsf{N}_2)$.
Name	$\alpha \to \varphi / \varphi$, where $\alpha \in \mathsf{N}_1 \cup \mathsf{N}_2$ does not occur in φ.
BG$_B$	$@_i \langle B \rangle j \to @_j \varphi / @_i B\varphi$, where $i, j \in \mathsf{N}_1$ and $j \neq i$ does not appear in φ.
BG$_C$	$@_n \langle C \rangle m \to @_n \varphi / @_n C\varphi$, where $n, m \in \mathsf{N}_2$ and $m \neq n$ does not appear in φ.

Definition 6. *Given any set $\mathcal{A}$ of formulas, regarded as the* frame axioms*, we write $\Phi \vdash_{\mathcal{A}} \varphi$ if φ in the smallest set of formulas that contains Φ and all the* substitution instances *of both $\mathcal{A}$ and all the axioms listed in Table 2 and is closed under all the rules of Table 2. We say that* φ is derivable from Ψ under global assumptions Φ and frame axioms $\mathcal{A}$ (*written: $\Phi; \Psi \vdash_{\mathcal{A}} \varphi$) if there is a finite subset $\Psi' \subseteq \Psi$ such that $\Phi \vdash_{\mathcal{A}} \bigwedge \Psi' \to \varphi$, where $\bigwedge \Psi'$ is the conjunction of all finite elements of Ψ'.*

Remark that we do *not* require global assumptions Φ to be closed under uniform substitutions in this definition, while we require frame axioms $\mathcal{A}$ and the axioms in Table 2 to be closed under uniform substitutions. Therefore, $B(\varphi \to \psi) \to (B\varphi \to B\psi)$ is derivable (from $\emptyset$) under any global assumptions and any frame axioms, but $(\mathsf{Woman} \lor \mathsf{Man}) \leftrightarrow \mathsf{Parents}$ is *not derivable* (from $\emptyset$) under a global assumption $(\mathsf{Mother} \lor \mathsf{Father}) \leftrightarrow \mathsf{Parents}$ and no frame axioms.

Definition 7. *We say that a set Γ of formulas* defines *a class F of s-frames if, for all $\mathfrak{F} \in \mathsf{F}$, Γ is valid on $\mathfrak{F}$ iff $\mathfrak{F} \in \mathsf{F}$.*

In what follows in this paper, we denote the class of all s-frames by $\mathsf{F}_{\mathrm{all}}$.

Proposition 2 (Soundness). *Let $\mathcal{A}$, Φ, $\Psi \cup \{\varphi\} \subseteq \mathcal{F}$ and $\mathcal{A}$ define F. Then, $\Phi; \Psi \vdash_{\mathcal{A}} \varphi$ implies $\Phi; \Psi \models_{\mathsf{F}} \varphi$. In particular, $\Phi; \Psi \vdash_{\emptyset} \varphi$ implies $\Phi; \Psi \models_{\mathsf{F}_{\mathrm{all}}} \varphi$.*

Proof. Let us only check the validity of $@_n Bp \leftrightarrow @_n B @_n p$. Fix any s-model $\mathfrak{M}$ and any (w, a) of $\mathfrak{M}$. Then, $\mathfrak{M}, (w, a) \models @_n Bp$ iff $\mathfrak{M}, (w, \underline{n}) \models Bp$ iff $wR_{\underline{n}}w'$ implies

$\mathfrak{M}, (w', \underline{n}) \models p$ for all $w' \in W$ iff $wR_{\underline{n}}w'$ implies $\mathfrak{M}, (w', \underline{n}) \models @_n p$ for all $w' \in W$ iff $\mathfrak{M}, (w, \underline{n}) \models B@_n p$ iff $\mathfrak{M}, (w, a) \models @_n B@_n p$, as required. $\square$

Let us say that $\varphi \in \mathcal{F}$ is a *pure formula* if it does not contain any symbol from P.

Theorem 1 (Strong Completeness). *Let $\mathcal{A}$ be a set of pure formulas and $\mathcal{A}$ define a class F of s-frames. Given any sets Φ, $\Psi \cup \{\varphi\} \subseteq \mathcal{F}$, $\Phi; \Psi \models_{\mathsf{F}} \varphi$ implies $\Phi; \Psi \vdash_{\mathcal{A}} \varphi$. In particular, $\Phi; \Psi \models_{\mathsf{F}_{\text{all}}} \varphi$ implies $\Phi; \Psi \vdash_{\emptyset} \varphi$.*

Proof (Sketch). A basic idea of the proof is a combination of completeness arguments in [9] (to deal with global assumptions) and [10] (to handle two-dimensionality of our static syntax). We show the contrapositive implication. Let us say that Ψ is $(\mathcal{A}, \Phi)$-*consistent* if $\Phi; \Psi \nvdash_{\mathcal{A}} \bot$. Suppose $\Phi; \Psi \nvdash_{\mathcal{A}} \varphi$, i.e., $\Psi \cup \{\neg\varphi\}$ is $(\mathcal{A}, \Phi)$-consistent. A key idea for global assumptions here is to employ the following 'doubly' @-prefixed formulas: Given any set $\Sigma \subseteq \mathcal{F}$, we define $@\Sigma := \{ @_i @_n \varphi \mid \varphi \in \Sigma \text{ and } (i, n) \in \mathsf{N}_1 \times \mathsf{N}_2 \}$. A subset of $@\mathcal{F}$ is called an *ABox* (we followed the terminology of [9]). A *maximally* $(\mathcal{A}, \Phi)$*-consistent ABox* is a $\subseteq$-maximal element among $(\mathcal{A}, \Phi)$-consistent ABoxes. By Lindenbaum construction, we use fresh nominals as if Henkin-constants in FOL and construct a maximally $(\mathcal{A}, \Phi)$-consistent ABox Σ such that $@_i @_n \Psi \cup \{\neg\varphi\} \subseteq \Sigma$ for some nominals (i, n). Then, we define the Henkin-style canonical model $\mathfrak{M}^{\Sigma} = (W^{\Sigma}, A^{\Sigma}, R^{\Sigma}, \asymp^{\Sigma}, V^{\Sigma})$ consisting of:

- $W^{\Sigma} := \{ |i| \mid i \in \mathsf{N}_1 \}$, where $|i| := \{ j \mid @_i @_n j \in \Sigma \text{ for some } n \in \mathsf{N}_2 \}$.
- $A^{\Sigma} := \{ [n] \mid n \in \mathsf{N}_2 \}$, where $[n] := \{ m \mid @_i @_m j \in \Sigma \text{ for some } i \in \mathsf{N}_1 \}$.
- $|i| R^{\Sigma}_{[n]} |j|$ iff $@_i @_n \langle B \rangle j \in \Sigma$
- $[n] \asymp^{\Sigma}_{|i|} [m]$ iff $@_i @_n \langle C \rangle m \in \Sigma$.
- $(|i|, [n]) \in V(\varphi)$ iff $@_i @_n \varphi \in \Sigma$ $(\varphi \in \mathsf{P} \cup \mathsf{N}_1 \cup \mathsf{N}_2)$.

By $@_i @_n \Psi \cup \{\neg\varphi\} \subseteq \Sigma$, we can show $\mathfrak{M}^{\Sigma}, (|i|, [n]) \models \Psi$ but $\mathfrak{M}^{\Sigma}, (|i|, [n]) \not\models \varphi$ (here we need interaction axioms of Table 2). By construction, we can assure that $\mathfrak{M}^{\Sigma} \models \Phi$. Moreover, $(W^{\Sigma}, A^{\Sigma}, R^{\Sigma}, \asymp^{\Sigma})$ is in F, since $\mathcal{A}$ defines F and $\mathcal{A}$ is a set of pure formulas and all points of W^{Σ} and A^{Σ} are named by some nominals. Therefore, $\Phi; \Psi \not\models_{\mathsf{F}} \varphi$, as required. $\square$

Example 4. (i) $\mathcal{A}_1 = \{ @_n \neg \langle C \rangle n, @_n \langle C \rangle m \to @_m \langle C \rangle n \}$ defines irreflexivity and symmetry of $\asymp_w$ and $\mathcal{A}_2 = \{ @_i \langle B \rangle i, @_i \langle B \rangle j \to @_j \langle B \rangle i, (@_i \langle B \rangle j \wedge @_j \langle B \rangle k) \to @_i \langle B \rangle k \}$ defines that R_a is an equivalence relation. By Theorem 1, the union of those *pure* axioms provides a complete axiomatization of a hybrid expansion of Facebook Logic [4].

(ii) Global axioms $\Phi_1 = \{ (\mathsf{Mother} \vee \mathsf{Father}) \leftrightarrow \mathsf{Parents} \}$ assure us that concept name $\mathsf{Parents}$ has an intended definition in the level of *s*-model. $\Phi_2 = \{ @_{\mathsf{AN}} \langle C \rangle \mathsf{BE}, @_{\mathsf{BE}} \langle C \rangle \mathsf{AN} \}$ assure us that we can restrict our attention to the *s*-models where there are two-way channels between Ann and Bea. We can augment our logic with global assumptions $\Phi_1 \cup \Phi_2$ and frame axioms $\mathcal{A}_1 \cup \mathcal{A}_2$ without losing our completeness result. $\blacksquare$

6.2 Complete Axiomatization of Dynamic Logic via Reduction Axioms

Similarly to the static syntax, we define the notions of definability, semantic consequence relation $\Phi; \Psi \models_{\mathsf{F}} \varphi$, etc. also for the set $\mathcal{F}^+$ of all formulas in the static syntax with $[\varphi!^i_{(n,m)}]$. Given any $\Phi, \Psi \subseteq \mathcal{F}^+$, let us define $\Phi; \Psi \vdash^+_{\mathcal{A}} \varphi$ if there exists some finite subset Ψ' such that $\bigwedge \Psi' \to \varphi$ is in the smallest set of $\mathcal{F}^+$ such that it contains Φ, all reduction axioms of Table 1 and all the substitution instances of both $\mathcal{A}$ and the axioms of Table 2 and that it is closed under all the rules of Table 2. Note that we do not require that global assumptions Φ and the reduction axioms are closed under uniform substitutions. Note that we do not require that global assumptions Φ and the reduction axioms are closed under uniform substitutions. Let us introduce one terminology, which is important for a completeness result of our dynamic logic.

Definition 8. *We say that* $\Sigma \subseteq \mathcal{F}$ *is* invariant under informing actions *if* $\mathfrak{M} \models \Sigma$ *implies* $\mathfrak{M}^{\varphi!^i_{(m,n)}} \models \Sigma$*, for all s-model* $\mathfrak{M}$ *and all dynamic operators* $[\varphi!^i_{(m,n)}]$.

Global assumptions $\Phi_1 \cup \Phi_2$ of Example 4 is invariant under informing actions, since all formulas in the set contain no occurrence of the operator B. One can also check that frame axioms $\mathcal{A}_1 \cup \mathcal{A}_2$ of Example 4 is invariant under informing actions, since the corresponding frame properties of the axioms are preserved under informing actions. However, the axiom $\langle B \rangle \top$ (consistency of agents' belief) is *not* invariant under informing actions.

Theorem 2 (Strong Completeness). *Let* $\Phi \subseteq \mathcal{F}$ *and a set* $\mathcal{A} \subseteq \mathcal{F}$ *of pure formulas define a class* F *of s-frames. Suppose that* Φ *and* $\mathcal{A}$ *are invariant under informing actions. Then, for any* $\Psi \cup \{\varphi\} \subseteq \mathcal{F}^+$, $\Phi; \Psi \vdash^+_{\mathcal{A}} \varphi$ iff $\Phi; \Psi \models_{\mathsf{F}} \varphi$*. In particular,* $\Phi; \Psi \vdash^+_{\emptyset} \varphi$ iff $\Phi; \Psi \models_{\mathsf{F}_{\mathrm{all}}} \varphi$.

Proof. Here we only establish the right-to-left direction (completeness), since soundness follows Proposition 1. By reduction axioms of Table 1, let us fix a translation $\tau : \mathcal{F}^+ \to \mathcal{F}$ such that $\varphi \leftrightarrow \tau(\varphi)$ is valid on F for all $\varphi \in \mathcal{F}^+$. For our goal, let us assume that $\Phi; \Psi \models_{\mathsf{F}} \varphi$. We can show $\Phi; t[\Psi] \models_{\mathsf{F}} t(\varphi)$ in the syntax of $\mathcal{F}$ as follows. Take any s-frame $\mathfrak{F} \in \mathsf{F}$ and any valuation V such that $\mathfrak{M} \models \Phi$, where $\mathfrak{M} = (\mathfrak{F}, V)$. Moreover, assume that $\mathfrak{M}, (w, a) \models t[\Psi]$. We need to establish $\mathfrak{M}, (w, a) \models t(\varphi)$. Then, also in the syntax of $\mathcal{F}^+$, we obtain $\mathfrak{M} \models \Phi$ and $\mathfrak{M}, (w, a) \models t[\Psi]$, which implies $\mathfrak{M}, (w, a) \models \Psi$ by definition of τ. By assumption, $\mathfrak{M}, (w, a) \models \varphi$ hence $\mathfrak{M}, (w, a) \models t(\varphi)$, as desired. Then, we can proceed as follows: $\Phi; t[\Psi] \models_{\mathsf{F}} t(\varphi)$ iff $\Phi; t[\Psi] \vdash_{\mathcal{A}} t(\varphi)$ by Proposition 2 and Theorem 1. By definition of $\vdash^+_{\mathcal{A}}$ in $\mathcal{F}^+$, $\Phi; t[\Psi] \vdash^+_{\mathcal{A}} t(\varphi)$. By the translation τ by reduction axioms, this is equivalent with $\Phi; \Psi \vdash^+_{\mathcal{A}} \varphi$, as required. □

7 Conclusion

In connection with our three requirements: (i), (ii), and (iii) in the introduction, our contribution can be summarized as follows. (i) First, we employed the notion of local announcement, contrary to the *public* announcement operator [7], assuming the existence of channels between agents for the individual announcement. (ii) Next, we proposed that agents' communicability should depend on agents' belief situation. As preceding works, [11] assumed that the social network relations were context-independent. However, we regarded that communicability might change dependent on environments in which the agent is embedded. (iii) Finally, we contended that an effect of informing action at a given state should be valid only on the state. In order to realize the requirement (iii) (locality of an effect of an announcement), we have employed the downarrow binders. One might wonder if this choice is essential for (iii). Moreover, some reader might want not to add nominals for states to epistemic/doxastic logic. It would be interesting to find an alternative way without state-nominals to realize (iii).

We have provided sound and complete axiomatizations of static and dynamic parts of our logic. Here, let us comment on a decidability question. A satisfiability problem for hybrid logic with the downarrow binder is *un*decidable (cf. [5]). Therefore, we conjecture that a satisfiability problem of our two-dimensional syntax with the downarrow binder is also undecidable. Even if we restrict our attention to the fragment *without* the downarrow binder, it is still unknown that the satisfiability problem of the fragment is decidable (see [10]). We leave these satisfiability questions for our further investigation.

References

1. Jennings, N.R., Sycara, K.P., Wooldridge, M.: A roadmap of agent research and development. Journal of Autonomous Agents and Multi-Agent Systems 1(1), 7–36 (1998)
2. Foundation for Intelligent Physical Agents (FIPA): Communicative act library specification (2000), `http://www.fipa.org`
3. van Eijk, R.M., de Boer, F.S., van der Hoek, W., Meyer, J.-J.C.: Process Algebra for Agent Communication: A General Semantic Approach. In: Huget, M.-P. (ed.) Communication in Multiagent Systems. LNCS (LNAI), vol. 2650, pp. 113–128. Springer, Heidelberg (2003)
4. Seligman, J., Liu, F., Girard, P.: Logic in the Community. In: Banerjee, M., Seth, A. (eds.) Logic and Its Applications. LNCS, vol. 6521, pp. 178–188. Springer, Heidelberg (2011)
5. Areces, C., ten Cate, B.: Hybrid logics. In: Blackburn, P., van Benthem, J., Wolter, F. (eds.) Handbook of Modal Logic, pp. 821–868. Elsevier (2007)
6. Baader, F., Lutz, C.: Description logic. In: Blackburn, P., van Benthem, J., Wolter, F. (eds.) Handbook of Modal Logic, pp. 757–820. Elsevier (2007)
7. Plaza, J.A.: Logics of public communications. In: Emrich, M.L., Pfeifer, M.S., Hadzikadic, M., Ras, Z.W. (eds.) Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems, pp. 201–216 (1989)
8. Lewis, D.: A problem about permission. In: Saarinen, E., Hilpinen, R., Niiniluoto, I., Hintikka, M. (eds.) Essays in Honour of Jaakko Hintikka, pp. 163–175. Reidel, Dordrecht (1979)
9. Schröder, L., Pattinson, D.: Named models in coalgebraic hybrid logic. In: Marion, J.Y., Schwentick, T. (eds.) Proceedings of STACS 2010. Leibniz International Proceedings in Informatics, pp. 645–656 (2010)
10. Sano, K.: Axiomatizing hybrid products: How can we reason many-dimensionally in hybrid logic? Journal of Applied Logic 8(4), 459–474 (2010)
11. Pacuit, E., Parikh, R.: Reasoning about communication graphs. In: van Benthem, J., Löwe, B., Gabbay, D. (eds.) Interactive Logic: Games and Social Software. Texts in Logics and Games, pp. 135–157. Amsterdam University Press (2008)

On Kripke's Puzzle about Time and Thought

Rohit Parikh[⋆]
`rparikh@gc.cuny.edu`

Brooklyn College of CUNY and CUNY Graduate Center

Kripke [Kp] formulates the following puzzle.

At any moment of time, Kripke might be thinking of a certain set of times.[1] For example, the set of all times when TV was unknown. Or the set of all times when interplanetary travel will be commonplace and the like. Kripke proceeds.

> However, there is a problem: suppose I think at a certain time t_0 of the set S_0 where S_0 contains all times t at which I'm thinking of a given set S_t of times, and S_t does not include t itself. In conventional notation:
> $$S_0 = \{t | S_t \text{ exists } \& \ t \notin S_t\}$$
> Now, I am thinking of S_0 at a certain time t_0. Is t_0 a member of S_0 or not? The reader can fill in the resulting paradox for herself.

Before addressing Kripke's problem, let us turn to another Harvard philosopher, namely Hilary Putnam who is famous for not being able to distinguish a beech from an elm. Suppose that Putnam is looking at a tree in a friend's backyard and says, "I think that tree might be a beech."

[⋆] Research supported in part by a grant from CUNY's *FRAP* program.

[1] One question which might be raised here is *What does thinking of something amount to?* It is not clear to me what Kripke's notion of 'thinking of something' is. I have used an approach where syntax is an intermediary to semantics which is then used to think of things. Thus I shall take the point of view that thinking of some X is mentally repeating some words intended to denote X. If there is such an X, and is denoted by the expression one has mentally repeated then in normal circumstances one has succeeded in thinking of X. However, surely that is not the only way. Perhaps one thinks of someone by having a picture of him in one's mind. So I might think of Quine, not by saying the word to myself but remembering him. But remembering how? In his office? Giving a lecture at CUNY? If I remember him giving a lecture and someone else remembers him walking through Harvard yard, then are we thinking of different persons? If I read Borges' *The Aleph* in English and Adriana reads it in Spanish then when we think about *The Aleph* are we thinking of the same book? I shall avoid such questions by simply assuming that thinking of Quine amounts to saying the word to oneself provided one satisfies the required conditions viz: one has met Quine or read one of his papers or met someone who knew Quine, or whatever. A second reason for going the linguistic route is that while at least a weak case can be made that one can think of Quine by having a mental image of him, it seems implausible that one can think of S_0 without going the linguistic route. [Sm] discusses some of these questions though in a different context.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 121–126, 2013.

The friend responds, “Do you mean to say that my tree is a member of the set of all beech trees?”, and Putnam responds, “Yes, just that. I think your tree is a member of the set of beech trees.”

Now Putnam does not know whether the tree in question is a beech or not. May we nonetheless say that Putnam is thinking of the set B of beech trees and wondering if the tree in question belongs to B?

Surely yes. Putnam does not need to be able to tell a beech tree by sight in order to think of the set B, just as we can think of Aristotle without having the ability to recognize him by sight. Here is the quote from Putnam:

> Suppose you are like me and cannot tell an elm from a beech tree. We still say that the extension of ‘elm’ in my idiolect is the same as the extension of ‘elm’ in anyone else’s, viz., the set of all elm trees, and that the set of all beech trees is the extension of ‘beech’ in both of our idiolects. Thus ‘elm’ in my idiolect has a different extension from ‘beech’ in your idiolect (as it should). Is it really credible that this difference in extension is brought about by some difference in our concepts? My concept of an elm tree is exactly the same as my concept of a beech tree (I blush to confess).

And again:

> The last two examples depend upon a fact about language that seems, surprisingly, never to have been pointed out: that there is division of linguistic labor. We could hardly use such words as ‘elm’ and ‘aluminum’ if no one possessed a way of recognizing elm trees and aluminum metal; but not everyone to whom the distinction is important has to be able to make the distinction. Let us shift the example; consider gold. Gold is important for many reasons: it is a precious metal; it is a monetary metal; it has symbolic value (it is important to most people that the “gold” wedding ring they wear really consist of gold and not just look gold); etc. Consider our community as a “factory”: in this “factory” some people have the “job” of wearing gold wedding rings; other people have the “job” of selling gold wedding rings; still other people have the job of telling whether or not something is really gold. It is not at all necessary or efficient that every one who wears a gold ring (or a gold cufflink, etc.), or discusses the “gold standard,” etc., engage in buying and selling gold. Nor is it necessary or efficient that every one who buys and sells gold be able to tell whether or not something is really gold in a society where this form of dishonesty is uncommon (selling fake gold) and in which one can easily consult an expert in case of doubt. And it is certainly not necessary or efficient that every one who has occasion to buy or wear gold be able to tell with any reliability whether or not something is really gold.
>
> The foregoing facts are just examples of mundane division of labor (in a wide sense). But they engender a division of linguistic labor: every

> one to whom gold is important for any reason has to acquire the word 'gold'; but he does not have to acquire the method of recognizing whether something is or is not gold.

Thus a chain extending from us to Aristotle enables us to think of him, (see [Kn]), and the community of horticulturists enables Putnam to think of the set B. He can just say the word "beech" or think it, and he thinks of B.

The work of deciding on the denotation of the word "beech" is done by society and it is society which helps Putnam "think of" the set of beech trees by just using the word "beech". There is a linguistic division of labor. Putnam thinks the word "beech" and the community sees to it that he is thinking of the set of beeches.

For another example, I can speak about (and think of) the set of physicists currently at CERN without knowing whether my friend Pran Nath is currently at CERN or not. If he is, then he is a member of the set I am thinking about and if not then not. I *do not need a mental image* of all the physicists lined up in a row, nor do I need to know whether Pran is at Cern. The community does part of the work for me by deciding who is to be counted as a physicist and Pran does part of the work by being at CERN or by not being at CERN. All **I** need is the phrase "the set of physicists currently at CERN.

In Putnam's case, Putnam does not play any role in deciding what a beech tree is and in my case I do not play a role in deciding what the word "physicist" means or who is at CERN. And it is Putnam's non-interference with the meaning of "beech" and my *non-interference* (as we shall see) with physicisthood that enables us to use the word or the phrase to think of something.

Before returning to Kripke's puzzle, let us consider another, practical problem. Mr. Smith wants to listen to a lecture by Kripke, but it turns out that the room in which Kripke is speaking is full. However, CUNY has considerately provided rooms A and B in which a video transmission of the lecture can be heard. Smith goes into room A and starts listening when he suddenly realizes that there a problem. It is Thursday evening, and Smith belongs to a religion which allows him to listen to a lecture on a Thursday only if the room in which he is doing the listening has an odd number of people in it (including Smith himself). Unfortunately (and Smith counts) there are 20 people in room A including Smith. Clearly Smith cannot stay in room A.

But then he looks across the hall and sees that room B only has 11 people in it. "Aha!" says Smith and proceeds to room B. He sits down and starts to listen. But after a minute or two his conscience starts to trouble him and he counts the number of people in room B. The number, alas, is 12. Clearly Smith cannot stay in B and proceeds back to A which, he can now see, only has 19 people. We need not trouble ourselves more with Smith's quandary. Perhaps he just goes home. Or perhaps he pays someone in A to move to room B.

Smith's problem is a convoluted version of a simpler problem. Can I enter an empty elevator? Yes, if all I ask is that the elevator be empty prior to my entering it. But if I demand that the elevator be empty *after* I have entered it, then I am going to be frustrated.[2]

We do have occasion to worry that we are not able to enter a full elevator, especially if we are late for class. But not many of us worry about not being able to enter an empty elevator. “Empty elevator”, in common usage means an elevator which is empty when seen from outside.

As for Smith, it is quite likely that had Russell written to Frege about Smith, Frege might not have been particularly concerned. He might just have advised Smith to convert to a more practical religion.

Let us now return to Kripke’s problem. Let us assume that at each moment of time, Kripke is mentally uttering a word or phrase to himself. Perhaps the phrase is, “the set of all times when TV was unknown.” Let p be the phrase and TVU be that set. The meaning M(p) of p is TVU and by thinking p, Kripke can think of TVU.

Very possibly Kripke does not know exactly when TV became known (known to how many?) but (as I have argued) he can think of the set TVU just by mentally uttering the phrase p.

The meaning function M such that M(p) = TVU is determined by society, i.e., by people including Kripke, but many many others as well, and certain facts about television.

But now what happens if Kripke utters “S_0 ” to himself at time t_0? What set is he thinking of? The answer to that is presumably, M(S_0). We have the expression “S_0” and all we need now is the function M. We can then look to see if $t_0 \in M(S_0)$.

The trouble is that if at time t_0 Kripke had not thought “S_0” but thought p instead, then t_0 would have been in the value M(S_0). For M(p) as a *set of times* would have been empty. But Kripke unwisely did not think p. Instead, he thought “S_0” and by thinking “S_0” he put t_0 out of M(S_0). But no, by putting t_0 out, he put it back in, etc. etc.

The fact that Kripke is thinking “S_0” is not the problem. The problem lies in the fact that Kripke is *interfering* with the meaning function M by thinking “S_0”.

In particular, if Kripke is uttering “S_0” to himself at time t_0, does M(S_0) have the property of containing t_0? Clearly the rest of us cannot help Kripke here. He will have to make up his own mind about M, just as Mr. Smith had to make up his mind whether to go home or pay someone to move from room A to room B, or perhaps convert to some other religion.[3]

In sum, are Kripke’s troubles any worse than Smith’s? I am not convinced that they are. Let me now present a baby result which generalizes Kripke’s examples

---

[2] For an even more alarming example, if a man cannot marry a married woman, and he cannot marry an unmarried woman, then marriage would come to an end. It is clever of mankind to decide that “an unmarried woman” means a woman who is unmarried before she says “I do”.

[3] Or he could go to a room with an even number of people in it, knowing that the number would be odd when he went in.

of TV and interplanetary travel. In both cases, Kripke was able to make use of society's denotation of certain phrases by leaving the meaning function alone.

Let M be a function which takes a moment t of time and a phrase p to produce a set. M may not depend on t at all. For example M(p,t) where p is "the set of all times when TV was unknown" does not depend on t at all – it is not indexical. But we will allow indexicality. Thus if Humpty Dumpty says, "from now on 'horse' means a cow" and we allow him this indulgence, then after Humpty Dumpty's remark, we can think of the set of cows just by using the word "horse". So we allow M to depend on certain data, like Humpty Dumpty's remark about the word "horse". If Kripke uses the function M to think of some set, he can use his own behavior *prior* to the moment of his use of some phrase p.

So let M be such a meaning function M(p,t,d) where p is a noun phrase, t is a time, and d are some data about the world (but only prior to times before t) and the thoughts of everyone including Kripke prior to time t. If two sets of data d and d' agree on all sets of times up to but not including t, then M(p,t,d) and M(p,t,d') are required to be the same.

Definition 1. *Suppose that at time t, some agent a is thinking some expression p, and the meaning function of a's community at time t is M(t, .) then agent a is said to be thinking of the object M(t,p).*[4]

Suppose now that Kripke decides to think "S_0" at time t_0. That fact is not part of the data at time t. So M(S_0, t_0, d) is already determined and either contains t_0 or does not. What Kripke thinks at time t_0 is not part of the data, and does not affect M, but he certainly is free to use an already existing M to think whatever he likes. That Kripke is thinking "S_0" is certainly allowed to be an argument to M, but is not allowed to interfere with M itself.[5]

Conclusion: Can I enter an empty room? Yes, I can, provided that I decide beforehand that "empty" means "empty before I enter."

One can think of other, more benign cases as well. For instance, suppose Kripke thinks at a certain time t_0 of the set T_0 where T_0 contains all times t at which he is thinking of a given set T_t of times, and T_t *does* include t itself.

---

[4] I am ignoring issues where what the agent intends to think of is not denoted by the expression that the agent is actually using. For instance suppose Paul says to Shyamasundar, "How is the weather in Madras these days?" Then Shyamasundar might respond, "There is no such place as Madras. You are probably thinking of Chennai. The weather in Chennai is fine". Here we would say that in using the expression "Madras" Paul is actually thinking of Chennai. I will ignore this problem since it is not germane to Kripke's worries in [Kp]. That issue is, however, addressed by Kripke under speaker meaning [Ks]. See also [D].

[5] What if we want M to be able to depend on physical facts like the sun turning into a giant red star, *after* time t? We can accomodate such a need by making M depend on two kinds of data, linguistic data d_l up to but not including time t, and physical facts d_p including those from times after t.

Is t_0 then a member of T_0? Here, instead of no solution, we have two consistent solutions, rather like the situation with Henkin's problem.

Henkin [H] asked if the formula of Peano Arithmetic which "says", "I am provable" is provable. The formula could be true and provable or it could be false and unprovable. Unlike the Gödel formula which said "I am not provable", Henkin's formula gives no such trouble but leaves us with a choice. Löb [L] eventually gave a positive answer, the Henkin formula is provable. But before Löb did so, both answers, positive and negative, were plausible. Kripke's theory of truth [Kt] goes into similar issues in great depth, but we shall simply stop here.

Acknowledgements. Thanks to Jim Cox, Paul Pedersen, Hilary Putnam, Graham Priest, Noson Yanofsky and the referees for comments.

References

- [D] Donnellan, K.: Refererence and definite descriptions. The Philosophical Review 75, 281–304 (1966)
- [H] Henkin, L.: A problem concerning provability. J. Symbolic Logic 17, 160 (1952)
- [Kt] Kripke, S.: Outline of a theory of truth. Journal of Philosophy 17, 690–716 (1975)
- [Kn] Kripke, S.: Naming and Necessity. Harvard University Press (1980)
- [Ks] Kripke, S.: Speaker's reference and semantic reference. Midwest Studies in Philosophy, 255–276 (1977)
- [Kp] Kripke, S.: A puzzle about time and thought. In: Philosophical Troubles, ch. 13. Oxford University Press (2011)
- [L] Löb, M.H.: Solution of a problem of Leon Henkin. J. Symbolic Logic 20, 115–118 (1955)
- [Pu] Putnam, H.: Meaning and Reference. The Journal of Philosophy 70(19), 699–711 (1973)
- [Sm] Smith, N.: Semantic regularity and the liar paradox. Monist 89, 178–202 (2006)

Yablo Sequences in Truth Theories

Cezary Cieśliński

The University of Warsaw, Institute of Philosophy, Warsaw, Poland

Abstract. We investigate the properties of Yablo sentences and formulas in theories of truth. Questions concerning provability of Yablo sentences in various truth systems, their provable equivalence, and their equivalence to the statements of their own untruth are discussed and answered.

Keywords: truth, Yablo's paradox, omega-liar.

1 Introduction

In 1993 Stephen Yablo presented a new paradox, belonging to the liar-type group, but, as it was claimed, importantly different from the liar (see [12], but cf. also [11] for a similar reasoning). Let $T(x)$ abbreviate "x is true". Consider an infinite sequence of sentences $Y_0, Y_1, Y_2, \ldots$ such that

$$\begin{aligned} Y_0 \text{ states : } & \quad \forall z > 0\ \neg T(Y_z), \\ Y_1 \text{ states : } & \quad \forall z > 1\ \neg T(Y_z), \\ Y_2 \text{ states : } & \quad \forall z > 2\ \neg T(Y_z), \\ & \vdots \end{aligned}$$

In effect Y_n states that all sentences which appear after stage n in the series are not true. Assume now that Y_k is true. Then for any $i > k$, Y_i is not true, and in particular Y_{k+1} is not true. But also for any $i > k+1$, Y_i is not true, so Y_{k+1}, therefore Y_{k+1} is true after all, which is impossible. Since the reasoning goes for an arbitrary k, we know at this point that all Y_k-s are not true. Therefore Y_0 must be true and in this way we obtain a contradiction.

The above reasoning has been presented by Stephen Yablo as a "paradox without self-reference": apparently it involves no direct or indirect self-referential loops, since on the face of it all the Y_n-s say something only about sentences which appear *later* in the sequence (i.e. after stage n). The question whether the paradox is really self-reference free has been much debated in recent literature.[1] However, the possibility of giving here a general, unanimous verdict seems very problematic: the main obstacle is that at present we do not seem to have a clear

---

[1] In particular, Sorensen in [9] defends the non-circularity of Yablo's paradox; but see also [8] and [1] for the criticism of the non-circularity claim.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 127–138, 2013.

concept of self-reference or (more generally) of 'aboutness', against which the issue of self-referentiality of Yablo sentences could be decided.[2]

In view of that, I will avoid here the notion of self-referentiality, adopting instead a different approach. The central notion will be that of *provability* in various systems of truth; the plan is to consider the following main questions: (1) which Yablo sentences are provable/disprovable in a given truth theory? (2) are all Yablo sentences provably equivalent in a given theory? (3) are Yablo sentences like the liars - are they (provably in a given theory) equivalent to the statements of their own untruth? (4) to what extent does the answer to (1)–(3) depend on our choice of a Yablo formula $Y(x)$?

Question (1) is perhaps the most basic one – we want to know after all whether a given theory settles in any way the issue of Yablo sentences. Questions (2) and (3) are motivated by discussions of (non)self-referentiality of Yablo sentences. While the notion of a self-referential sentence remains vague, one can use precise, formal tools in order to investigate whether all Yablo sentences are one and the same *up to provability* in a given theory,[3] and also whether they all fit into (again, up to provability) the familiar Liar-type pattern. Question (4) relates to the fact that in general it is possible to obtain sentences with quite different properties satisfying one and the same formal constraint. We ask in effect if the Yablo condition by itself (corresponding roughly to a general specification of what is stated by each Yablo sentence) is enough to determine the answers to (1) – (3).[4]

2 Preliminaries

We start with introducing the notions of a Yablo formula and a Yablo sentence with respect to a theory S. In what follows we will always assume that S is a theory formulated in the language L_T, specified as the language of first order arithmetic extended with a one place predicate $T(x)$. We will use Feferman's dot notation, so e.g. if φ is a formula with one free variable, the expression "$\forall x T(\ulcorner \varphi(\dot{x}) \urcorner)$" gets a reading: "for all natural numbers x, the result of substituting a numeral denoting x for a variable free in φ is true". In practice if there is no danger of ambiguity, we will often suppress both the dots and the square corners.

---

[2] This observation was made by Leitgeb. After analysing various unsuccessful attempts to express the notion of self-referentiality, he even voices the suspicion that "the talk of self-referentiality is to be banished from scientific contexts" (see [7], p. 13; but see also [10] for a defence of this notion).

[3] The real issue concerns implications "$Y(n) \rightarrow Y(k)$" for $n > k$, since for $n < k$ the implication is trivial given sufficiently strong background theory.

[4] A similar approach was adopted in [3] – a paper devoted to the analysis of Yablo's reasoning with various provability predicates substituted for truth. One of the main issues is then which variants of Yablo sentences are provably equivalent over a background arithmetical theory.

Definition 1. *Let S be a theory in the language L_T. We say that $Y(x)$ is a Yablo formula in S iff it satisfies (provably in S) the Yablo condition, i.e. iff $S \vdash \forall x[Y(x) \equiv \forall z > x \neg T(\ulcorner Y(\dot{z}) \urcorner)]$. Yablo sentences are obtained by substituting numerals for x in $Y(x)$.*

Using familiar diagonal techniques, it is easy to prove the existence of Yablo formulas for all theories extending Robinson's arithmetic.[5]

Theorem 2. *For every theory S in L_T extending Robinson's arithmetic, there is a Yablo formula in S.*

In the proof we employ the diagonal lemma in the following form:

Lemma 3. *Let S be a theory in L_T extending Robinson's arithmetic. Then for every $\varphi(x, y) \in L_T$ there is a formula $\psi(x)$ such that:*

$$S \vdash \psi(x) \equiv \varphi(x, \ulcorner \psi(x) \urcorner)$$

The proof mimics the usual proof of the diagonal lemma for formulas with one free variable.

With the lemma at hand, the argument for Theorem 2 proceeds as follows.

Proof. Fix:

$$\varphi(x, y) := \forall z > x \neg T(sub(y, name(z))).$$

with "$sub(y, s)$" representing the substitution function (which produces the result of substituting s for a free variable in y) and "$name(x)$" representing a function which for an argument x produces as a value a numeral denoting x.[6] By the diagonal lemma, take $Y(x)$ such that:

$$S \vdash Y(x) \equiv \forall z > x \neg T(sub(\ulcorner Y(x) \urcorner, name(z))).$$

Then the formula $Y(x)$ as constructed above is a Yablo formula in S.

Further properties of $Y(x)$ will depend on the choice of S – in particular, on the axioms governing the use of the predicate T. To clear the ground, consider for a start the theory **PAT**, which is obtained from **PA** by extending the language with a new predicate "T". This predicate will be permitted to appear in formulas substituted for schematic axioms of **PA**.[7] Since by Theorem 2 Yablo formulas in **PAT** do exist, one can consider their properties. For **PAT** the following result holds.

---

[5] This method of constructing Yablo sequences was employed by Priest, see [8]; cf. also Ketland's paper [5].

[6] Strictly speaking, in the context of arithmetic with addition and multiplication, both expressions (i.e. *sub* and *name*) should be treated not as function symbols, but as arithmetical formulas representing appropriate functions on natural numbers.

[7] As defined, **PAT** is not really a theory of truth, with "T" being just a new predicate, without any substance to it, but we find it useful to consider it as a borderline case.

Fact 4. *Let $Y(x)$ be a Yablo formula in* **PAT**. *Then:*

(a) $\mathbf{PAT} \nvdash \exists x Y(x)$
(b) $\mathbf{PAT} \nvdash \exists x \neg Y(x)$
(c) If $Y(x)$ contains a free variable x, then for all natural numbers n and k, if $n > k$, then $\mathbf{PAT} \nvdash Y(n) \to Y(k)$

Proof. Since T in **PAT** functions just as a new predicate, $\mathbf{PAT} \nvdash \exists x T(x)$ and also $\mathbf{PAT} \nvdash \exists x \neg T(x)$, therefore both (a) and (b) follow trivially. For (c), assume that $Y(x)$ contains a free variable x. Then for every n and k, if $n \neq k$, then $\ulcorner Y(k) \urcorner \neq \ulcorner Y(n) \urcorner$. Consider a model (N, T) obtained by expanding the standard model N with the set $T = \{Y(n)\}$. Obviously $(N, T) \models \mathbf{PAT}$ and since $n > k$, we have: $(N, T) \models Y(n)$; $(N, T) \nvDash Y(k)$.

To sum it up: Yablo sentences are neither provable, nor disprovable in **PAT**; they are also not provably equivalent in this theory (assuming that they are different). In fact $Y(0), Y(1)...$ is a sequence of weaker and weaker sentences independent from **PAT**. It's also worth noting that Fact 4 is obtained independently of our choice of the formula $Y(x)$, as long as (for condition (c)) it contains a free variable x.

The next sections contain a discussion of the status of Yablo sentences in two truth theories: Friedman-Sheard system **FS** and Kripke-Feferman theory **KF**.

3 The Theory FS

We proceed now to the discussion of the Friedman-Sheard system **FS**, which is obtained by adding to **PAT** compositional truth axioms for negation, binary connectives and quantifiers, together with the rules of necessitation (NEC) and conecessitation (CONEC). We will denote by $\mathbf{FS}^-$ a theory just like **FS**, but with induction restricted to arithmetical formulas only. In effect **FS** is defined as the system extending **PAT** with the following truth-theoretic axioms and rules (Tm^c is the set of constant terms and $Sent_T$ denotes the set of sentences of L_T):

- $\forall s, t \in Tm^c \big(T(s{=}t) \equiv val(s){=}val(t)\big)$
- $\forall x \,\big(\mathrm{Sent}_T(x) \to (T\neg x \equiv \neg Tx)\big)$
- $\forall x \,\forall y \,\big(\mathrm{Sent}_T(x \wedge y) \to (T(x \wedge y) \equiv (Tx \wedge Ty))\big)$
- $\forall x \,\forall y \,\big(\mathrm{Sent}_T(x \vee y) \to (T(x \vee y) \equiv (Tx \vee Ty))\big)$
- $\forall v \,\forall x \,\big(\mathrm{Sent}_T(\forall vx) \to (T(\forall vx) \equiv \forall t \, T(x(t/v)))\big)$
- $\forall v \,\forall x \,\big(\mathrm{Sent}_T(\exists vx) \to (T(\exists vx) \equiv \exists t \, T(x(t/v)))\big)$

Additional rules of inference are:

$$NEC \quad \frac{\phi}{T\phi} \qquad\qquad \frac{T\phi}{\phi} \quad CONEC$$

For more information about **FS** we refer the reader to [4], where both semantics and proof theory of this system is discussed.

As it turns out, results concerning Yablo sentences in **FS** do not depend on the choice of a Yablo formula $Y(x)$. Let $Y(x)$ be an arbitrary Yablo formula in $\mathbf{FS}^-$ (analogously for full **FS**). We start with the following observation.

Fact 5. $\mathbf{FS}^{-} \vdash \forall xz[x < z \rightarrow (Y(x) \rightarrow Y(z))]$

The proof is immediate, from the assumption that $Y(x)$ is a Yablo formula in $\mathbf{FS}^{-}$.

Now we will show, that all Yablo sentences are provably equivalent in $\mathbf{FS}^{-}$. In fact a *uniform* equivalence of Yablo sentences is a theorem of $\mathbf{FS}^{-}$:

Theorem 6. $\mathbf{FS}^{-} \vdash \forall xz[Y(x) \equiv Y(z)]$.

Proof. Working in $\mathbf{FS}^{-}$, fix x and z. Assume (wlog) that $x < z$. Then we know (Fact 5) that $Y(x) \rightarrow Y(z)$. For the opposite implication, assume $Y(z)$, i.e. $\forall s > z \neg T(Y(s))$. For an indirect proof, assume also $\neg Y(x)$, i.e. $\exists s > x T(Y(s))$. Therefore $\exists s \leq z T(Y(s))$; fix such an s. Since $Y(z)$, we have also: $\neg T(Y(z+1))$. By applying NEC and compositional axioms to Fact 5, we obtain (as a theorem of $\mathbf{FS}^{-}$): $\forall xz[x < z \rightarrow (T(Y(x)) \rightarrow T(Y(z)))]$. Since $s < z+1$ and $T(Y(s))$, we get: $T(Y(z+1))$, which is a contradiction ending the proof.

Now we present the following two corollaries.

Corollary 7. $\mathbf{FS}^{-} \vdash \forall xz[T(Y(x)) \equiv T(Y(z))]$.

The proof is immediate, by applying NEC and compositional axioms to Theorem 6. We have also:

Corollary 8. $\mathbf{FS}^{-} \vdash \forall x[Y(x) \equiv \neg T(Y(x))]$.

Proof. From left to right, the assumption $Y(x)$ gives us $\neg T(Y(x+1))$, so $\neg T(Y(x))$ by Corollary 7. For the opposite implication, assuming $\neg T(Y(x))$ we obtain $\forall z \neg T(Y(z))$ by Corollary 7; therefore $\forall z > x \neg T(Y(z))$, which gives us $Y(x)$.

Corollary 8 shows that in **FS** each Yablo sentence is a liar - it expresses (up to a provable equivalence) its own untruth. The corollary states that this insight can be proved in $\mathbf{FS}^{-}$ in a uniform manner. Finally we obtain:

Fact 9. *If* **FS** *is consistent, then:*

(a) $\mathbf{FS} \nvdash \exists x Y(x)$ *(b)* $\mathbf{FS} \nvdash \exists x \neg Y(x)$

Proof. For (a), assume that $\mathbf{FS} \vdash \exists x Y(x)$, therefore by Theorem 6 $\mathbf{FS} \vdash \forall x Y(x)$, so in particular $\mathbf{FS} \vdash Y(0)$. An application of NEC and the compositional axiom for general quantifier gives us: $\mathbf{FS} \vdash \forall x T(Y(x))$, so $\mathbf{FS} \vdash T(Y(1))$, but also $\mathbf{FS} \vdash \neg T(Y(1))$ (because $Y(0)$ is provable in **FS**), contradicting the consistency of **FS**.

For (b), assume that $\mathbf{FS} \vdash \exists x \neg Y(x)$, therefore by Theorem 6 $\mathbf{FS} \vdash \forall x \neg Y(x)$. Applying NEC and compositional axioms, we obtain: $\mathbf{FS} \vdash \forall x \neg T(Y(x))$. But then $\mathbf{FS} \vdash \forall x Y(x)$, which together with the first assumption leads to the conclusion that **FS** is inconsistent.

4 The Theory KF

We proceed now to the Kripke-Feferman theory, denoted as **KF**. The truth theoretic axioms are listed below. In what follows they will be denoted as KF1-KF13.

(1) $\forall s \, \forall t \, \big(T(s = t) \equiv val(s) = val(t)\big)$
(2) $\forall s \, \forall t \, \big(T(\neg s = t) \equiv val(s) \neq val(t)\big)$
(3) $\forall x \, \big(\mathrm{Sent}_T(x) \rightarrow (T(\neg\neg x) \equiv Tx)\big)$
(4) $\forall x \, \forall y \, \big(\mathrm{Sent}_T(x \wedge y) \rightarrow (T(x \wedge y) \equiv Tx \wedge Ty)\big)$
(5) $\forall x \, \forall y \, \big(\mathrm{Sent}_T(x \wedge y) \rightarrow (T\neg(x \wedge y) \equiv T\neg x \vee T\neg y)\big)$
(6)-(7) Similarly for disjunction
(8) $\forall v \, \forall x \, \big(\mathrm{Sent}_T(\forall v x) \rightarrow (T(\forall v x) \equiv \forall t \, T(x(t/v)))\big)$
(9) $\forall v \, \forall x \, \big(\mathrm{Sent}_T(\forall v x) \rightarrow (T(\neg\forall v x) \equiv \exists t \, T(\neg x(t/v)))\big)$
(10)-(11) Similarly for the existential quantifier
(12) $\forall t \, (T(Tt) \equiv T(val(t)))$
(13) $\forall t \, \big(T\neg Tt \equiv (T(\neg val(t)) \vee \neg \, \mathrm{Sent}_T(val(t)))\big)$

When discussing **KF**, two additional axioms are often introduced:

CONS $\forall x \, \big(\mathrm{Sent}_T(x) \rightarrow \neg(Tx \wedge T\neg x)\big)$

COMPL $\forall x \, \big(\mathrm{Sent}_T(x) \rightarrow (Tx \vee T\neg x)\big)$

However, we will denote as **KF** the theory with just the axioms KF1-KF13 added to **PAT**. Whenever we discuss a theory with CONS or COMPL, we are going to stipulate it explicitly.

In order to characterize the behaviour of Yablo sentences in **KF**, we will need some basic facts about this theory.

4.1 Basic Properties of KF

The presentation in this section relies heavily on Cantini's paper [2]; the modifications are introduced in order to handle our specific choice of axiomatization for **KF**.

KF has been proposed as a formalization of Kripkean notion of truth, based on strong Kleene evaluation scheme (see [6]). In Kripke's fixed point construction, truth is interpreted as a partial predicate – its interpretation is given by a pair of sets T^+, T^- called the extension and the antiextension. Given a classical model M of Peano arithmetic, we will consider structures $\mathcal{M} = (M, T^+, T^-)$, with T^+ and T^- being the subsets of the domain of M – such structures are called *partial models* for the language L_T (we assume that only the predicate $T(x)$ is partially interpreted; arithmetical expressions are interpreted classically.) For partial models a satisfaction relation can be defined in the following way (the subscript in "$\models_{sk}$" is for "strong Kleene"):[8]

---

[8] For the purposes of Definition 10, it is convenient to extend L_T to the language of the model M, i.e. we add constants for all elements of M. In effect for every $a \in M$, $\varphi(a)$ is a formula (or a sentence) of the extended language.

Definition 10

- $\mathcal{M} \models_{sk} s = t$ *iff* $val(s) = val(t)$*; similarly for negated identities.*
- $\mathcal{M} \models_{sk} Tt$ *iff* $val(t) \in T^+$*.*
- $\mathcal{M} \models_{sk} \neg Tt$ *iff* $val(t) \in T^-$ *or* $\neg Sent(val(t))$*.*
- $\mathcal{M} \models_{sk} \neg\neg\varphi$ *iff* $\mathcal{M} \models_{sk} \varphi$*.*
- $\mathcal{M} \models_{sk} \varphi \wedge \psi$ *iff* $\mathcal{M} \models_{sk} \varphi$ *and* $\mathcal{M} \models_{sk} \psi$*.*
- $\mathcal{M} \models_{sk} \neg(\varphi \wedge \psi)$ *iff* $\mathcal{M} \models_{sk} \neg\varphi$ *or* $\mathcal{M} \models_{sk} \neg\psi$*.*
- *Similarly for disjunction and its negation.*
- $\mathcal{M} \models_{sk} \forall x\varphi(x)$ *iff for all* $a \in M$ $\mathcal{M} \models_{sk} \varphi(a)$*.*
- $\mathcal{M} \models_{sk} \neg\forall x\varphi(x)$ *iff for some* $a \in M$ $\mathcal{M} \models_{sk} \neg\varphi(a)$*.*
- *Similarly for the existential quantifier.*

Since **KF** is a classical theory, its models will be two valued, not partial. However, each model of **KF** can be turned into a partial model with some nice properties.

Definition 11. *For* $(M, T) \models KF$*, we denote:*

- $T^+ = T$
- $T^- = \{z : \neg z \in T^+\}$
- $M^* = (M, T^+, T^-)$

It turns out that M^*, as characterized by Definition 11, satisfies the following:

Theorem 12. *If* $(M, T) \models KF$*, then* $\forall\varphi \in L_T$ $[M^* \models_{sk} \varphi$ *iff* $M^* \models_{sk} T(\varphi)]$.

Idea of the proof. The proof is by induction on positive complexity of φ (see [4], p. 205).[9] For sentence of positive complexity 0 e.g. of the form $\neg T(t)$ we have: $M^* \models_{sk} \neg T(t)$ iff $val(t) \in T^- \vee \neg Sent(val(t))$ iff $\neg val(t) \in T^+ \vee \neg Sent(val(t))$ iff $(M, T) \models T(\neg t) \vee \neg Sent(t)$ iff $(M, T) \models T(\neg T(t))$ iff $\neg T(t) \in T^+$ iff $M^* \models_{sk} T(\neg T(t))$. The rest follows by induction.

Adding Compl or Cons to **KF** produces a theory which is truth-theoretically (although not arithmetically) stronger than **KF**. It can be shown that both directions of the uniform T-schema (i.e. "$\forall x_1...x_n[T(\varphi(x_1...x_n)) \equiv \varphi(x_1...x_n)]$") are provable in theories with Cons and Compl respectively.

Fact 13. *For every* $\varphi(x_1...x_n)$*:*

(a) $KF + \textsc{Cons} \vdash \forall x_1...x_n[T(\varphi(x_1...x_n)) \rightarrow \varphi(x_1...x_n)]$
(b) $KF + \textsc{Compl} \vdash \forall x_1...x_n[\varphi(x_1...x_n)) \rightarrow T(\varphi(x_1...x_n))]$

---

[9] Roughly, the idea is to define the notion of a complexity of a formula in such a way as to guarantee that: atomic and negated atomic formulas have the complexity 0; conjunctions, disjunctions and quantified sentences have the level of complexity greater by one than their disjuncts/conjuncts/formulas after the quantifier; the same for negated conjunctions/disjunctions/quantified sentences; double negation increases the level of complexity by one.

Accordingly, we can't extend **KF** consistently with both $\textsc{Cons}$ and $\textsc{Compl}$ (the full T-schema is known to be inconsistent); it is possible however to add consistently each of this axioms separately.

Idea of the proof. The fact is proved by induction on positive complexity of L_T-formulas. We show only the parts where $\textsc{Cons}$ and $\textsc{Compl}$ are used. This happens in the case when $\varphi := \neg T(x)$. Then we argue as follows.

(a) Working in $KF+\textsc{Cons}$, assume $T(\neg T(a))$, assume also $T(a)$. Then by KF12, $T(T(a))$, which contradicts $\textsc{Cons}$.
(b) Working in $KF+\textsc{Compl}$, assume $\neg T(a)$, assume also $\neg T(\neg T(a))$. Then by $\textsc{Compl}$, $T(T(a))$, so by $KF12$, $T(a)$ - a contradiction.

From Fact 13 the following conclusion about the liar sentence L can be very easily obtained:[10]

Corollary 14. *$KF+\textsc{Cons} \vdash L$; $KF+\textsc{Compl} \vdash \neg L$*

Finally, we introduce the notion of a dual model. It is obtained from a model (M,T) of **KF** by redefining the extension of the truth predicate. The new extension is defined as the set of all M-sentences, whose negations are not in T (cf. Definition 11).

Definition 15. *For $(M,T) \models KF$, we define:*

- $T^d = Sent - T^-$
- $M^d = (M, T^d)$

Note that T^d may be different from T: in particular, it will contain all sentences which were left indeterminate in the original model (i.e. sentences φ such that neither φ nor $\neg\varphi$ belonged to T).

Useful properties of dual models are described by the theorem below.

Theorem 16

(a) If $(M,T) \models KF$, then $(M,T^d) \models KF1\text{-}KF12$
(b) If $(M,T) \models KF+\textsc{Cons}$, then $(M,T^d) \models KF+\textsc{Compl}$

Proof (chosen cases). Assuming that $(M,T) \models KF+\textsc{Cons}$, we show:

1 $M^d \models KF13$, i.e. $\forall t \left(T\neg Tt \equiv (T(\neg val(t)) \vee \neg \mathrm{Sent}_T(val(t)))\right)$.
2 $M^d \models \textsc{Compl}$.

For 1, we show only $(\leftarrow)$. Assume that $M^d \models T\neg t \vee \neg Sent(t)$, so $\neg val(t) \notin T^- \vee \neg Sent(val(t))$; assume also that $M^d \models \neg T\neg Tt$, so $\neg Tt \in T^-$. Then we reason as follows:

(i) $T(t) \in T^+$ (definition of T^-)
(ii) $val(t) \in T^+$ (we know that $(M,T) \models TTt \equiv Tt$)
(iii) $\neg val(t) \in T^-$ (definition of T^-)

---

[10] Corollary 14 is in fact valid about an *arbitrary* sentence L provably (in $KF+\textsc{Cons}$ or $KF+\textsc{Compl}$, respectively) equivalent to the statement of its own untruth.

(*iv*) $\neg Sent(val(t))$ (previous line and our first assumption)
(*v*) $(M, T) \models T(\neg Tt)$ (by $KF13$ and the previous line)
(*vi*) $(M, T) \models \neg T(Tt)$ (by Cons)

So by KF12, $(M, T) \models \neg T(t)$, which means that $val(t) \notin T^+$ - a contradiction.

For 2, we must show: $M^d \models \forall\psi[Sent(\psi) \rightarrow (T(\psi) \vee T(\neg\psi))]$. Fixing a sentence ψ, assume that $\psi \notin T^d$. Then $\psi \in T^-$, so $\neg\psi \in T^+$. By Cons, $\neg\psi \notin T^-$, so $\neg\psi \in T^d$ as required.

4.2 Yablo Sentences in KF and Some Related Theories

In this section we investigate properties of formulas which are Yablo in **KF**, in **KF** + Cons and in **KF** + Compl (cf. Definition 1). Our first observation states that the theory **KF** + Compl uniformly decides its Yablo sentences.

Theorem 17. *Let* $Y(x)$ *be such that* $KF + \text{Compl} \vdash Y(x) \equiv \forall z > x \neg T(Y(z))$. *Then* $KF + \text{Compl} \vdash \forall x \neg Y(x)$.

Proof. Working in KF + Compl, assume $Y(x)$, so $\forall z > x\neg T(Y(z))$, therefore $\forall z > x + 1\neg T(Y(z))$, so $Y(x + 1)$, but also $\neg T(Y(x + 1))$. By Fact 13(b), $T(Y(x + 1))$ – a contradiction.

When moving to **KF** + Cons, things look a bit different. Unlike in the case of KF+Compl (or **FS**, for that matter) there is no uniform answer to the question "assuming that $Y(x)$ is a Yablo formula in **KF** + Cons, does **KF** + Cons prove $Y(n)$?" It turns out that the answers will vary, depending on our choice of $Y(x)$.

Theorem 18. *For every natural number* n*, there are formulas* $Y_0(x)$*,* $Y_1(x)$ *such that:*

(a) Both $Y_0(x)$ *and* $Y_1(x)$ *are Yablo formulas in* **KF** + Cons.
(b) **KF** + Cons $\vdash Y_0(n)$; **KF** + Cons $\vdash \neg Y_1(n)$

Proof. Let n be fixed; let L be the liar sentence. Define:

- $Y_0(x) := x = n \vee (x > n \wedge L)$
- $Y_1(x) := x = n + 1 \vee (x > n + 1 \wedge L)$

Then (b) is obviously satisfied. For the proof of (a), we show only that $Y_0(x)$ is a Yablo formula in **KF** + Cons (the argument for $Y_1(x)$ is very similar). Working in **KF** + Cons, fix x and consider two cases:

Case 1: $x < n$. Then $\neg Y_0(x)$, and since we also have: $T(n = n \vee (n > n \wedge L)$, we obtain: $\exists z > xT(z = n \vee (z > n \wedge L))$. In effect in Case 1 both sides of the Yablo condition are false, which makes the condition true.

Case 2: $x \geq n$. Since L is provable in **KF** + Cons (Corollary 14), we obtain $Y_0(x)$. And we obtain also the right side of the Yablo condition by the following reasoning: fix $z > x$ and assume $T(Y_0(z))$, i.e. $T(z = n \vee (z > n \wedge L))$. Then by compositional principles of **KF** $T(z = n) \vee (T(z > n) \wedge T(L))$. But by assumption $z > n$; in efect $T(L)$ and therefore $\neg L$ – a contradiction, because L is a theorem of **KF** + Cons.

We see in effect, that questions like "does $KF+\textsc{Cons}$ prove $Y(n)$?" do not admit a single answer, independent of our choice of a Yablo formula. In view of this result, narrower classes of Yablo formulas are worth considering. And indeed it turns out that $KF+\textsc{Cons}$ decides a certain narrower, but still quite comprehensive class of Yablo sentences, namely those, which are Yablo in KF itself (without $\textsc{Cons}$):

Theorem 19. *Let $Y(x)$ be such that $KF \vdash Y(x) \equiv \forall z > x \neg T(Y(z))$. Then $KF+\textsc{Cons} \vdash \forall x Y(x)$.*

Proof. Let $(M,T) \models KF+\textsc{Cons}$. (Then $M^d \models KF+\textsc{Compl}$ – see Theorem 16(b).) For an indirect proof, assume that $(M,T) \models \neg Y(a)$. Fix $b >_M a$ such that $(M,T) \models T(Y(b))$. So $Y(b) \in T^+$; $\neg Y(b) \in T^-$; $\neg Y(b) \notin T^d$. Now we show that:

(*) $\forall z >_M bY(z) \in T^-$.

Assume that $z >_M b$ and $Y(z) \notin T^-$. So $Y(z) \in T^d$, and (since $z >_M b$) $M^d \models \neg Y(b)$. Therefore (by Fact 13(b) and Theorem 16(b)) $M^d \models T(\neg Y(b))$; in effect $\neg Y(b) \in T^d$, which is a contradiction.

From (*) it follows that $\forall z >_M bY(z) \notin T^d$, which means that $M^d \models Y(b)$. Therefore $M^d \models Y(b+1)$, so $M^d \models T(Y(b+1))$; but (since $M^d \models Y(b)$) it follows also that $M^d \models \neg T(Y(b+1))$ – a contradiction.

From Theorem 19 it follows directly that if $Y(x)$ is a Yablo formula in **KF**, then $KF+\textsc{Cons} \vdash \forall x > 0 \neg T(Y(x))$. In fact it is possible to show that the formula $Y(0)$ is no exception.

Theorem 20. *If $Y(x)$ is a Yablo formula in* **KF**, *then $KF+\textsc{Cons} \vdash \forall z \neg T(Y(z))$.*

Proof. Define $Y^*(x)$ as the formula: $(x=0 \wedge \forall z \neg T(Y(z))) \vee (x \neq 0 \wedge Y(x-1))$. The theorem is obtained as a direct corollary from Theorem 19 and the fact that $Y^*(x)$ is a Yablo formula in **KF**, i.e. it satisfies provably in **KF**, the usual Yablo condition, i.e.: $Y^*(x) \equiv \forall z > x \neg T(Y^*(z))$.

Given the fact that $Y^*(x)$ is a Yablo formula in **KF**, we can argue as follows. By Theorem 19, $KF+\textsc{Cons} \vdash \forall x Y^*(x)$, so in particular $KF+\textsc{Cons} \vdash \forall x Y^*(0)$, therefore (by the definition of $Y^*(x)$) $KF+\textsc{Cons} \vdash \forall z \neg T(Y(z))$. In effect for the proof of Theorem 20 it is enough to show that we have indeed the Yablo condition for $Y^*(x)$.

For the direction from left to right, assume $Y^*(x)$ and fix $z > x$. Assume $T(Y^*(z))$; then by the definition of $Y^*(x)$ (and by the fact that $z > 0$) we obtain: $T(Y(z-1))$. Then x cannot equal 0, because otherwise by $Y^*(x)$ we would have: $\forall z \neg T(Y(z))$. Since $x \neq 0$, we obtain $Y(x-1)$. But $x-1 < z-1$ (because $z > x, x \neq 0$), so $\neg T(Y(z-1))$ - a contradiction.

For the opposite direction, assume $\forall z > x \neg T(Y^*(z))$; assume also $\neg Y^*(x)$, i.e. $\neg[x=0 \wedge \forall z \neg T(Y(z))] \wedge \neg[x \neq 0 \wedge Y(x-1)]$. Now we consider two cases.

Case 1: $x = 0$. So $\exists z T(Y(z))$. Fixing such a z and putting $a = z + 1$ we obtain: $T(a \neq 0 \wedge Y(a - 1))$, so $T(Y^*(a))$, which (since $x = 0$) contradicts our main assumption.

Case 2: $x \neq 0$. So $\neg Y(x - 1)$, i.e. $\exists z \geq x T(Y(z))$. Fixing such a z and putting $a = z + 1$ we obtain again $T(a \neq 0 \wedge Y(a - 1))$, i.e. $T(Y^*(a))$, which (since $a > x$) contradicts our main assumption.

From Theorems 19 and 20 it follows easily that every Yablo formula is a liar in KF + Cons.

Corollary 21. *If $Y(x)$ is a Yablo formula in* **KF***, then KF+*Cons $\vdash \forall x[Y(x) \equiv \neg T(Y(x))]$.

Finally, we are going to look at what happens in the theory **KF** itself. The first observation is that it doesn't decide any Yablo sentence:

Corollary 22. *Let $Y(x)$ be a Yablo formula in KF. Then $KF \nvdash \exists x Y(x)$ and $KF \nvdash \exists x \neg Y(x)$.*

Proof. By Theorem 17, the first conjunct is verified by an arbitrary model for KF + Compl. By Theorem 19, the second conjunct is verified by an arbitrary model for KF + Cons.

In effect each sentence $Y(n)$ is independent of KF.

Does **KF** (without Cons or Compl) settle the issue of equivalence of Yablo sentences? We will show that it does, but for a restricted class of those Yablo sentences, which are well behaved in partial models.

Theorem 23. *Let $Y(x)$ be a Yablo formula in KF such that for every $(M, T) \models KF$ we have (see Definition 11):*

$$\forall a \in M \ [M^* \models_{sk} Y(a) \text{ iff } M^* \models_{sk} \forall z > a \neg T(Y(z))].$$

Then $KF \vdash \forall x Y(x) \vee \forall x \neg Y(x)$.

Proof. Fix a, b such that $(M, T) \models Y(a) \wedge \neg Y(b)$. So we have: $(M, T) \models \forall z > a \neg T(Y(z))$, and also: $(M, T) \models \exists z > b T(Y(z))$.

Let z be the largest number in M such that $(M, T) \models T(Y(z))$. Then $M^* \models_{sk} T(Y(z))$, so (Theorem 12) $M^* \models_{sk} Y(z)$, therefore by the assumptions of the theorem, $M^* \models_{sk} \forall s > z \neg T(Y(s))$. From this we obtain $M^* \models_{sk} \forall s > z + 1 \neg T(Y(s))$, and so $M^* \models_{sk} Y(z + 1)$ and also $M^* \models_{sk} T(Y(z + 1))$. Eventually $(M, T) \models T(Y(z + 1)$, which contradicts our choice of z.

From Theorem 23 the following corollary can be easily obtained.

Corollary 24. *For $Y(x)$ satisfying the assumptions of the previous theorem:*

$$KF \vdash \forall xy \ [Y(x) \equiv Y(y)]$$

Finally, we observe that the assumptions of Theorem 23 (and Corollary 24) apply to a class of formulas, which are quite important in the discussions concerning Yablo's paradox (cf. Theorem 2 and its proof).

Observation 25 *Let* $Y(x)$ *be the formula obtained by diagonalization from the condition* $\varphi(x, y) := \forall z > x \neg T(sub(y, name(z))$ *(cf. proof of Theorem 2). Then* $Y(x)$ *satisfies the assumptions of Theorem 23.*

Idea of the proof. As in the standard proof of the diagonal lemma, let $F(x, y)$ be $\varphi(x, subst(y, \ulcorner y \urcorner, name(y)))$; then specify $m = \ulcorner F(x, y) \urcorner$ and define $Y(x)$ as $F(x, \overline{m})$. In effect $Y(x)$ becomes: $\varphi(x, subst(\overline{m}, \ulcorner y \urcorner, name(\overline{m}))$. By performing the substitution operations (interpretation of the truth predicate being irrelevant for the results) it can be verified that $M^* \models_{sk} Y(a)$ iff $M^* \models_{sk} \varphi(a, \ulcorner Y(x) \urcorner)$, which corresponds to the Yablo condition for partial models, as required.

5 Summary

We analysed the behaviour of Yablo formulas in truth theories **FS** and **KF**. It turns out that **FS** proves the equivalence of all Yablo sentences in **FS**. In addition, **FS** treats Yablo formulas as liars: they can be shown to be provably equivalent to the statements of their own untruth.

Theories KF + CONS and KF + COMPL both uniformly decide sentences which are Yablo in **KF** (Theorems 17 and 19), although important properties of formulas which are Yablo in KF + CONS depend on the choice of the formula in question (Theorem 18). Yablo formulas obtained by diagonalization in **PAT** are provably equivalent in **KF**.

Acknowledgements. Many thanks to Rafał Urbaniak and Konrad Zdanowski for their useful comments and discussions. The author was supported by a grant from the National Science Centre in Cracow (NCN), decision number DEC-2011/01/B/HS1/03910.

References

1. Beall, J.C.: Is Yablo's Paradox Non-circular? Analysis 61, 176–187 (2001)
2. Cantini, A.: Notes on Formal Theories of Truth. Zeitschrift für Mathematische Logik und Grundlagen der Mathematik 35, 97–130 (1989)
3. Cieśliński, C., Urbaniak, R.: Gödelizing the Yablo Sequence. Journal of Philosophical Logic, doi:10.1007/s10992-012-9244-4
4. Halbach, V.: Axiomatic Theories of Truth. CUP, Cambridge (2011)
5. Ketland, J.: Yablo's Paradox and ω-Inconsistency. Synthese 145(3), 295–302
6. Kripke, S.: Outline of a Theory of Truth. Journal of Philosophy 72, 690–716 (1975)
7. Leitgeb, H.: What is a Self-referential Sentence? Critical Remarks on the Alleged (non-)Circularity of Yablo's Paradox. Logique & Analyse 177-178, 3–14 (2002)
8. Priest, G.: Yablo's Paradox. Analysis 57, 236–242 (1997)
9. Sorensen, R.: Yablo's Paradox and Kindred Infinite Liars. Mind 107, 137–155 (1998)
10. Urbaniak, R.: Leitgeb, "about", Yablo. Logique & Analyse 207, 239–254 (2009)
11. Visser, A.: Semantics and the liar paradox. In: Gabbay, D., Guenthner, F. (eds.) Handbook of Philosophical Logic, vol. IV, pp. 617–706. Kluwer Academic Publishers, Dordrecht (1989)
12. Yablo, S.: Paradox Without Self-reference. Analysis 53, 251–252 (1993)

Moving Up and Down in the Generic Multiverse

Joel David Hamkins[1,2] and Benedikt Löwe[3,4,⋆]

[1] Mathematics Program, The Graduate Center of the City University of New York,
365 Fifth Avenue, New York, NY 10016, United States of America
`jhamkins@gc.cuny.edu`
[2] Department of Mathematics, College of Staten Island of CUNY, Staten Island, NY
10314, United States of America
[3] Institute for Logic, Language and Computation, Universiteit van Amsterdam,
Postbus 94242, 1090 GE Amsterdam, The Netherlands
`b.loewe@uva.nl`
[4] Department Mathematik, Universität Hamburg, Bundesstrasse 55,
20146 Hamburg, Germany

Abstract. We investigate the *modal logic of the generic multiverse* which is a bimodal logic with operators corresponding to the relations "is a forcing extension of" and "is a ground model of". The fragment of the first relation is the *modal logic of forcing* and was studied by the authors in earlier work. The fragment of the second relation is the *modal logic of grounds* and will be studied here for the first time. In addition, we discuss which combinations of modal logics are possible for the two fragments.

1 Introduction

1.1 The Generic Multiverse

Recently, the *generic multiverse* has become a concept of great interest to set theorists and philosophers of mathematics alike:

> The generic multiverse is generated from each universe of the collection by closing under generic extensions (enlargements) and under generic refinements (inner models of a universe which the given universe is a generic extension of). (W. Hugh Woodin, [21])

If you fix a universe of set theory V and iteratively build all set forcing extensions and ground models—and throughout this article unless stated specifically

---

[⋆] The research of the first author has been supported in part by NSF grant DMS-0800762, PSC-CUNY grant 64732-00-42 and Simons Foundation grant 209252. The second author would like to thank the CUNY Graduate Center in New York for their hospitality during his sabbatical in the fall of 2009. In addition, both authors acknowledge the generous support provided to them as visiting fellows during the spring of 2012 at the *Isaac Newton Institute for Mathematical Sciences* in Cambridge and the typographical help of Joel Uckelman.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 139–147, 2013.

otherwise we shall mean always set forcing when discussing forcing—you naturally produce a Kripke structure GM(V) consisting of these worlds together with the accessibility relation $M \sqsubseteq N$ ("N is a forcing extension of M") and its converse relation $N \sqsupseteq M$ ("M is a ground of N"). Hugh Woodin has investigated *multiverse truth*, that is, truth in all models of the generic multiverse, in connection with his programme to solve the alethic status of the continuum hypothesis. The first author has proposed a philosophy of mathematics based on a broader multiverse perspective, where we have many different legitimate concepts of set (not merely those arising by set forcing), and these are instantiated in their corresponding set-theoretic universes, which relate in diverse ways as forcing extensions, large cardinal ultrapowers, definable inner models and so on [9]. Although the generic multiverse of a model of set theory is merely a local neighborhood within the broader multiverse, nevertheless we take it that our project in this article, to study the forcing modalities of the generic multiverse, surely engages with the multiverse perspective.

Due to the fact that the relations $\sqsubseteq$ and $\sqsupseteq$ are converses of each other, the bimodal logic of the Kripke structure $(\mathrm{GM}(V), \sqsubseteq, \sqsupseteq)$ is similar to temporal logics where the modality **F** ("there is a time in the future") is converse to the modality **P** ("there is a time in the past") [20]. It is our overall aim to investigate this bimodal logic of the general multiverse and find out which validities hold in general (provably in ZFC) or in the multiverse generated from specific universes.

1.2 The Modal Logic of Forcing and Related Work

In our previous paper [11], we introduced the modal logic of forcing and proved that the ZFC-provably valid principles of forcing were exactly those in the modal theory known as S4.2. The modal logic of forcing corresponds to the monomodal fragment of the modal logic discussed in §1.1 that only uses the relation $\sqsubseteq$; or to the part of the generic multiverse that is generated only by the operation of taking forcing extensions and not ground models.

In [11], we not only consider the ZFC-provable modal logic of forcing, but also the modal logic of forcing of particular universes V. We show that this modal logic always lies between S4.2 and S5 and that the two extreme values are realized (for more details, cf. §1.4). Various other aspects of the modal logic of forcing are considered in [15,12,3,4,16,19,2,1,10]. The paper [8] presented at ICLA 2009 gives an overview of the status of research and creates a connection between the modal logic of forcing and "set-theoretic geology", i.e., going down from a universe to its ground models. This connection is further developed in this paper.

1.3 The Results of This Paper

As stated above, our overall aim is to understand the bimodal logic of the generic multiverse. However, we know rather little about the general status of the bimodal logic (cf. Footnote 3). Instead of the bimodal theory, we consider the two monomodal fragments (the modal logic of forcing and the modal logic of grounds) and their possible combinations.

The main result of this paper is Theorem 6, constructing a model of set theory whose modal logic of grounds is $\mathsf{S4.2}$. This theorem is the downward analogue of the main result in [11], where we showed that the modal logic of forcing over $\mathbf{L}$ is $\mathsf{S4.2}$. Based on the proof idea of the main result, we then make a foray into the bimodal world, by considering which combinations are possible for the two monomodal fragments; i.e., for which pairs (Λ, Λ^*) can we find a model V such that $\mathrm{ML}(\overline{\Box}, V) = \Lambda$ and $\mathrm{ML}(\underline{\Box}, V) = \Lambda^*$. We consider all possible combinations with $\Lambda, \Lambda^* \in \{\mathsf{S4.2}, \mathsf{S5}\}$.

The paper is organized as follows: in § 1.4, we give the necessary definitions in order to discuss the basic properties of the modal logic of grounds (and how it differs from the modal logic of forcing) in § 2. In § 3, we finally consider the various combinations of upward and downward modal logics. The paper is not self-contained and uses ideas and concepts from the papers [11,18]; the proofs of our theorems are sketches and will be presented in more detail in a planned journal version of the paper.

1.4 Definitions

In the following, we denote by P a countable set of propositional letters; for modal operators $\overline{\Box}$ and $\underline{\Box}$, $\mathcal{L}_{\overline{\Box}}$ and $\mathcal{L}_{\overline{\Box},\underline{\Box}}$ are the monomodal and bimodal propositional languages with the appropriate operators. We assume that the reader is familiar with the standard axioms and systems of monomodal logic, in particular, .2, $\mathsf{S4}$, $\mathsf{S4.2}$, and $\mathsf{S5}$ (if not, there is a summary in [11, § 1]).

By $\mathcal{L}_\in$, we denote the first-order language of set theory with its set of sentences $\mathrm{Sent}(\mathcal{L}_\in)$. Any function $I : \mathrm{P} \to \mathrm{Sent}(\mathcal{L}_\in)$ is called an *interpretation*. An interpretation I generates a valuation of any Kripke structure (F, R) in which the worlds consist of models M of set theory and R is any relation between them: via

$$I^*(M) := \{p\, ;\, M \models I(p)\},$$

(F, R, I^*) becomes a Kripke model (similarly, for the bimodal language if we have two relations on F).

Note that in our special case (when $R = \sqsubseteq$), the validity of a modal formula at a world of the Kripke model is not just a meta-theoretic property of the Kripke model, but can be expressed in the language of set theory: e.g., $\overline{\Box}\varphi$ is interpreted by "for all generic extensions, φ holds" which by the Forcing Theorem [13, Theorem 14.6] is equivalent to "for all Boolean algebras $\mathbb{B}$, we have that $[\![\varphi]\!]_{\mathbb{B}} = \mathbf{1}$". Similarly, if $R = \sqsupseteq$, we can use a theorem of Laver's (cf. [14]) that the ground model is definable with parameters in the forcing extension, in order to see that "for all ground models, φ holds" is expressible in the language of set theory (this observation is due to Reitz, cf. [5, Theorem 8]).

These observations are closely related to Woodin's result about *multiverse truth*:

Theorem 1 (Woodin, 2009). *There is a recursive transformation* $\varphi \mapsto \varphi^*$ *such that* $M \models \varphi^*$ *is equivalent to the statement "for every model* N *in the generic multiverse generated by* M*,* φ *is true".*

The fact that the modalities are expressible in the language of set theory allows us to move from interpretations to *translations*: We call a function $H : \mathcal{L}_{\overline{\Box},\underline{\Box}} \to \mathrm{Sent}(\mathcal{L}_\in)$ a *translation* if

- $H(\varphi \wedge \psi) = H(\varphi) \wedge H(\psi)$,
- $H(\neg\varphi) = \neg H(\varphi)$,
- $H(\overline{\Box}\varphi)$ is the sentence stating "for all forcing extensions M, we have $M \models H(\varphi)$", and
- $H(\underline{\Box}\varphi)$ is the sentence stating "for all grounds M, we have $M \models H(\varphi)$".

Now, we can define the modal logic of the multiverse and two of its fragments: fixing a universe V, we call

$$\mathrm{ML}(\overline{\Box},\underline{\Box},V) := \{\varphi \in \mathcal{L}_{\overline{\Box},\underline{\Box}};\ \text{for all translations } H,\ V \models H(\varphi)\}$$

the *modal logic of the generic multiverse* generated by V. Similarly,

$$\mathrm{ML}(\overline{\Box},V) := \{\varphi \in \mathcal{L}_{\overline{\Box}};\ \text{for all translations } H,\ V \models H(\varphi)\}, \text{ and}$$
$$\mathrm{ML}(\underline{\Box},V) := \{\varphi \in \mathcal{L}_{\underline{\Box}};\ \text{for all translations } H,\ V \models H(\varphi)\}$$

are the *modal logic of forcing* and the *modal logic of grounds* at V, respectively. Metaphorically, we think of forcing extensions going upwards and thus the relation being a ground model going downwards. We therefore use the words "upward" and "downward" to indicate which modalities we are talking about: e.g., if we say that a model V satisfies upward S4.2, we mean that $\mathrm{ML}(\overline{\Box},V) = \mathsf{S4.2}$; similarly, we talk of "upward buttons" and "downward buttons" (see below).

As mentioned, in [11, Theorem 21], we proved that for any universe V, we get that

$$\mathsf{S4.2} \subseteq \mathrm{ML}(\overline{\Box},V) \subseteq \mathsf{S5},$$

and that the two extreme values are obtained. This immediately implies that the ZFC-provable modal logic of forcing

$$\{\varphi \in \mathcal{L}_{\overline{\Box}};\ \text{for all translations } H,\ \mathrm{ZFC} \vdash H(\varphi)\}$$

is exactly S4.2. Two facts about forcing are crucial for this result: the first is that the axiom .2 is always a validity for the modal logic of forcing over any universe V (cf. [15] and [10, Theorem 7] for the theoretical background), providing the lower bound; the second is the existence of independent switches over each model of set theory [11, Theorem 17]. We shall see that the situation is quite different for the modal logic of grounds. Note that it is not known whether the modal logic of forcing can obtain any other value than S4.2 or S5 [11, Question 19].

In order to show upper bounds for a modal logic, we used certain control statements called *buttons* and *switches*: a *switch* is a statement φ such that φ

and $\neg\varphi$ are both necessarily possible. A *button* is a statement φ that is necessarily possibly necessary. These controls are *independent* if they can be operated independently, without affecting the status of the others (cf. [11, p. 1789] or [10, § 4] for more detail). We shall use the abstract results that produce upper bounds from the existence of control statements in the proof sketches in this paper. For this we call a function $\sigma : \mathrm{P} \to \mathcal{L}_\Box$ a *substitution* (this is the purely modal version of our notion of interpretation above); every substitution induces a function $\hat{\sigma}$ on the entire set of modal formulas. If (F, R, v, w) is a pointed Kripke model, we let $\mathrm{ML}(F, R, v, w) := \{\varphi \in \mathcal{L}_\Box\,;$ for all substitutions σ, we have that $F, R, v, w \models \hat{\sigma}(\varphi)\}$.

Theorem 2. *If a pointed reflexive and transitive Kripke model* (F, R, v, w) *has arbitrarily large finite independent families of buttons and switches, then*

$$\mathrm{ML}(F, R, v, w) \subseteq \mathsf{S4.2}$$

[10, Theorem 13].

Theorem 3. *If a pointed reflexive and transitive Kripke model* (F, R, v, w) *has arbitrarily large finite independent families of switches, then*

$$\mathrm{ML}(F, R, v, w) \subseteq \mathsf{S5}$$

[10, Theorem 10].

2 The Modal Logic of Grounds

2.1 Basic Observations

It is easy to see that every $\mathsf{S4}$ assertion is downward valid (since a ground of a ground is a ground), but things are not as easy with the axiom .2. This axiom would be valid if the answer to the following question is "Yes":

Question 4. *Let V be a model of set theory, and M and N two grounds of V, i.e., $V = M[G] = N[H]$ for some generic filters G and H. Is there some model K which is a ground of both M and N, i.e., there are K-generic filters G^* and H^* such that $K[G^*] = M$ and $K[H^*] = N$? In other words, is $\sqsupseteq$ directed among the grounds of V?*

However, we do not know the answer to this question. We shall say that a universe V in whose generic multiverse the answer to Question 4 is "Yes" satisfies the axiom of *downward directedness of grounds* (DDG). In all universes for which we can determine the truth value of DDG, it is true.

The upper bound for the modal logic of forcing was $\mathsf{S5}$, but the situation for the modal logic of grounds is different. We denote by PL (for "propositional logic") the modal logic satisfying $\Box p \leftrightarrow \Diamond p \leftrightarrow p$, i.e., the modal logic of a single reflexive point. By GA, we denote the *ground axiom* of [18] stating that the universe is not a non-trivial forcing extension of an inner model.[1] Clearly, the constructible universe satisfies GA.

Observation 5. *If* $V \models \mathrm{GA}$*, then* $\mathrm{ML}(\underline{\Box}, V) = \mathsf{PL}$.

---

[1] The ground axiom is jointly due to Reitz and the first author; cf. [7,17].

2.2 S4.2 as the Modal Logic of Grounds

The following theorem provides us with a model in which we can determine the modal logic of grounds. Its proof will serve as the underlying idea for the results in §3.

Theorem 6. *If* ZFC *is consistent, then there is a model of* ZFC *whose ground valid assertions are exactly those in the modal theory* S4.2.

Proof sketch. The idea of this proof is to use the *bottomless model* of [18]: Let $\mathrm{Reg}^{\mathbf{L}}$ denote the class of regular $\mathbf{L}$-cardinals. Force over $\mathbf{L}$ with

$$\mathbb{P} = \prod_{\gamma \in \mathrm{Reg}^{\mathbf{L}}} \mathrm{Add}(\gamma, 1),$$

where we use Easton support and we use $\mathrm{Add}(\gamma, 1)$ as defined in $\mathbf{L}$. Let $V = \mathbf{L}[G]$, where G is $\mathbf{L}$-generic for this forcing.

First, following Reitz, we argue that every ground model of V contains a tail $\mathbf{L}[G^\alpha]$, where $G^\alpha = G \upharpoonright \mathbb{P}^\alpha$, and $\mathbb{P}^\alpha = \mathbb{P} \upharpoonright [\alpha, \infty)$. That is, $\mathbb{P}^\alpha$ is the tail forcing, using only the factors from α onward. Suppose that W is a ground of V, so that $W[H] = V = \mathbf{L}[G]$. If the filter G^α is not in W, then it has a name there, and the Boolean value of the statement that this name is decided in certain ways compatible with the actual values of G^α will be a strictly descending sequence of Boolean values in the W-forcing, which violates the chain condition of that forcing (when α is much larger than that forcing). So, for large α, G^α is an element of W.

In [18], Reitz used this to show that V has no bedrock, and we use the same argument to show that for any two grounds M and N, we find α and β such that $\mathbf{L}[G^\alpha]$ is a ground of M and $\mathbf{L}[G^\beta]$ is a ground of N. Then if $\mu := \max\{\alpha, \beta\}$, $\mathbf{L}[G^\mu]$ is a ground of both M and N. This proves that DDG holds in V, and thus .2.

We now show that there are no additional modal validities by using Theorem 2: Divide the regular cardinals above $\aleph_\omega$ into ω many disjoint classes Γ_n, each containing unboundedly many cardinals. Enumerate each class $\Gamma_n = \{\gamma^n_\alpha\,; \alpha < \mathrm{Ord}\}$ in order. Let s_n be the statement "the least α such that there exists an $\mathbf{L}$-generic subset of γ^n_α is even." These statements are all true in V, since the corresponding α is 0 in every case, as the forcing G explicitly adds an $\mathbf{L}$-generic subset of every γ^n_α, including $\alpha = 0$. In any ground model W of V, we can go to a deeper ground which is a tail extension, and then selectively remove additional factors of G on indices in each Γ_n so as to realize any desired configuration of the switches in L. So the s_n's are independent switches. Now let b_n be the statement: "there is no $\mathbf{L}$-generic subset of $\aleph_n^{\mathbf{L}}$". This statement is false in V, but true in any ground model of V omitting the factor at $\aleph_n^{\mathbf{L}}$. Furthermore, once true, the statement remains true in any deeper ground. Thus, each b_n is a button.

Finally, all these buttons and switches are independent, because each is controlled by removing disjoint factors of G.[2] Thus, Theorem 2 yields that $\mathrm{ML}(\underline{\Box}, V) = \mathsf{S4.2}$. $\Box$

It follows that the ZFC-provably valid principles of the modal of logic of grounds is a theory containing $\mathsf{S4}$ and contained within $\mathsf{S4.2}$. If DDG is a theorem of ZFC, the ZFC-provable modal logic of grounds is exactly $\mathsf{S4.2}$.

3 Combinations

So far, we have looked at the modal logic of forcing and the modal logic of grounds in isolation, but ultimately, we are interested in determining the entire bimodal logic of the multiverse. Currently, we know almost nothing about the validity of mixed bimodal formulas beyond those validities that follow from the fact that the modal operators $\overline{\Box}$ and $\underline{\Box}$ are defined by converse relations.[3] However, we can say something about possible combinations of modal logics of forcing with modal logics of grounds (in the case of Theorems 8 and 9 under mild large cardinal assumptions).

Theorem 7. *If* ZFC *is consistent, then there is a model of* ZFC *whose modal logic of forcing and modal logic of grounds are both* $\mathsf{S4.2}$.

Proof sketch. In fact, this is the model V constructed in the proof of Theorem 6: since $\mathsf{S4.2}$ is a general lower bound for the modal logic of forcing, we only have to show that independent upward buttons and switches exist. We have such a family for $\mathbf{L}$,[4] and by observing that the forcing to add G was cardinal-preserving and the GCH holds, we can use the buttons proposed by Rittberg [19] or Friedman, Fuchino and Sakai [2] or, alternatively, our stationary buttons from [11, Theorem 29] (provided that we start the other forcing above ω_1). The switches are GCH at $\aleph_{\omega+n}$. $\Box$

Theorem 8. *If* ZFC+ *"there is an inaccessible cardinal* δ *in* $\mathbf{L}$ *such that* $\mathbf{L}_\delta \prec \mathbf{L}$*" is consistent, then there is a model of set theory whose modal logic of forcing is* $\mathsf{S4.2}$ *and whose modal logic of grounds is* $\mathsf{S5}$.

Proof sketch. This proof is a combination of the construction in Theorem 6 and an idea from [6, Theorem 5]. We start with an inaccessible cardinal δ in $\mathbf{L}$ such that $\mathbf{L}_\delta \prec \mathbf{L}$ and force as in the proof of Theorem 6 with the Easton support product $\mathbb{P} := \prod_{\gamma \in \mathrm{Reg}^{\mathbf{L}}} \mathrm{Add}(\gamma, 1)$ to obtain $\mathbf{L}[G]$. Since δ was inaccessible in $\mathbf{L}$, $\mathbb{P}_\delta$ is just $\mathbb{P}$ as defined in $\mathbf{L}_\delta$ and we took a direct limit at δ; thus, we still

---

[2] Note that $\mathbf{L}$-generic Cohen subsets of different regular cardinals in $\mathbf{L}$ are necessarily mutually generic.

[3] E.g., we know that $p \to \overline{\Box}\neg\underline{\Box}\neg p$ and $p \to \underline{\Box}\neg\overline{\Box}\neg p$ hold.

[4] Note that the buttons provided in the proof of [11, Lemma 6.1] are problematic since we do not know how to prove their independence, but there are other independent buttons in that paper. Cf. the discussion at the end of [10, § 4].

have $\mathbf{L}_\delta[G_\delta] \prec \mathbf{L}[G]$. We claim that $V := \mathbf{L}[G^\delta]$ satisfies the conclusion of the theorem.

Upward S4.2 follows as in the proof of Theorem 7. Let us show that all downward buttons are pushed (this will establish S5 as a lower bound for the modal logic of grounds): If there is a ground pushing a downward button, then this fact is expressible, and so there must be a ground of $\mathbf{L}_\delta[G_\delta]$ pushing that button, and so this same forcing works with $\mathbf{L}[G]$. So there is a small forcing pushing that button. And this small forcing ground will contain $\mathbf{L}[G^\delta]$, so it is already pushed in $\mathbf{L}[G^\delta]$.

In order to show that we have exactly S5 as the modal logic of grounds, we use Theorem 3 and observe that the switches of the proof of Theorem 6 still work. □

We remark that if a universe has an independent family of upward switches and buttons, then so does any ground of that universe. This means that upward S4.2 is downwards necessary. Similarly, if a model has downward buttons and switches, then this remains upward necessary.[5]

Now, we consider the dual situation to that of Theorem 8: upward S5 and downward S4.2.

Theorem 9. *If* ZFC+ *"there is an inaccessible cardinal δ in $\mathbf{L}$ such that $\mathbf{L}_\delta \prec \mathbf{L}$" is consistent, then there is a model of set theory whose modal logic of forcing is* S5 *and whose modal logic of grounds is* S4.2*.*

Proof sketch. Again, this proof is a combination of the constructions in Theorem 6 and [6, Theorem 5]. Start in $\mathbf{L}$ with $\mathbf{L}_\delta \prec \mathbf{L}$ and δ inaccessible in $\mathbf{L}$. Force to $\mathbf{L}[G]$ with the Easton support product $\mathbb{P} := \prod_{\gamma \in \mathrm{Reg}^{\mathbf{L}}} \mathrm{Add}(\gamma, 1)$, as in Theorem 6. As before in the proof of Theorem 8, we still have $\mathbf{L}_\delta[G_\delta] \prec \mathbf{L}[G]$ (as δ was inaccessible in $\mathbf{L}$). We can now appeal to the definability of forcing relation and the fact that $\mathbf{L}_\delta \prec \mathbf{L}$: anything a condition p forces over $\mathbf{L}$ with $\mathbb{P}$ is the same as what it forces over $\mathbf{L}_\delta$ with $\mathbb{P}_\delta$.

Finally, we perform the forcing to obtain upwards S5 from [6, Theorem 5] to obtain $\mathbf{L}[G][h]$. This forcing is the same as the Lévy collapse making δ into ω_1. In $\mathbf{L}[G][h]$, we have upward S5. However, we also have downward .2: any ground of $\mathbf{L}[G][h]$ will contain some tail $\mathbf{L}[G^\alpha]$ just as in Theorem 6, and thus we can take maximums as there to verify .2. But now we also have downward buttons and switches, just as in Theorem 6. □

Theorems 7, 8, and 9 take care of three of the four possible distributions of the theories S4.2 and S5 to the upward and downward modal logics. This naturally raises the question whether it is possible to have S5 in both directions. We'll close this paper with the simple proof of the negative answer to this question:

Theorem 10. *There is no model of set theory such that both its modal logic of forcing and its modal logic of grounds are* S5*. Thus, the upward and downward maximality principles are inconsistent with each other.* □

---

[5] Unfortunately, we cannot conclude that downward S4.2 is upwards necessary, since we do not know whether downward .2 is valid in every model of set theory.

Proof. Let us call an ordinal α a *ground cardinal* if there is a ground in which α is a cardinal. Let γ be the least infinite ground cardinal; clearly, $\gamma \leqslant \omega_1$. The statement "$\gamma = \omega_1$" is a downward button, but its negation is an upward button. So, if we had a model V with $\mathrm{ML}(\overline{\Box}, V) = \mathsf{S5} = \mathrm{ML}(\underline{\Box}, V)$, then $\gamma = \omega_1$ would have to be true by downward $\mathsf{S5}$, but false by upward $\mathsf{S5}$.

References

1. Esakia, L., Löwe, B.: Fatal Heyting algebras and forcing persistent sentences. Studia Logica 100(1-2), 163–173 (2012)
2. Friedman, S., Fuchino, S., Sakai, H.: On the set-generic multiverse (submitted, 2012)
3. Fuchs, G.: Closed maximality principles: implications, separations and combinations. Journal of Symbolic Logic 73(1), 276–308 (2008)
4. Fuchs, G.: Combined maximality principles up to large cardinals. Journal of Symbolic Logic 74(3), 1015–1046 (2009)
5. Fuchs, G., Hamkins, J.D., Reitz, J.: Set-theoretic geology (submitted, 2011)
6. Hamkins, J.D.: A simple maximality principle. Journal of Symbolic Logic 68(2), 527–550 (2003)
7. Hamkins, J.D.: The Ground Axiom. Oberwolfach Reports 2(4), 3160–3162 (2005)
8. Hamkins, J.D.: Some Second Order Set Theory. In: Ramanujam, R., Sarukkai, S. (eds.) ICLA 2009. LNCS (LNAI), vol. 5378, pp. 36–50. Springer, Heidelberg (2009)
9. Hamkins, J.D.: The set-theoretic multiverse. Review of Symbolic Logic 5, 416–449 (2012), doi:10.1017/S1755020311000359
10. Hamkins, J.D., Leibman, G., Löwe, B.: Structural connections between a forcing class and its modal logic (submitted, 2012)
11. Hamkins, J.D., Löwe, B.: The modal logic of forcing. Transactions of the American Mathematical Society 360(4), 1793–1817 (2008)
12. Hamkins, J.D., Woodin, W.H.: The necessary maximality principle for c.c.c. forcing is equiconsistent with a weakly compact cardinal. Mathematical Logic Quarterly 51(5), 493–498 (2005)
13. Jech, T.: Set Theory, 3rd edn. Springer Monographs in Mathematics. Springer, Heidelberg (2003)
14. Laver, R.: Certain very large cardinals are not created in small forcing extensions. Annals of Pure and Applied Logic 149(1-3), 1–6 (2007)
15. Leibman, G.: Consistency strengths of modified maximality principles. PhD thesis, City University of New York (2004)
16. Leibman, G.: The consistency strength of $\mathrm{MP}_{\mathrm{CCC}}(\mathbb{R})$. Notre Dame Journal of Formal Logic 51(2), 181–193 (2010)
17. Reitz, J.: The Ground Axiom. PhD thesis, City University of New York (September 2006)
18. Reitz, J.: The Ground Axiom. Journal of Symbolic Logic 72(4), 1299–1317 (2007)
19. Rittberg, C.J.: The modal logic of forcing. Master's thesis, Westfälische Wilhelms-Universität Münster (2010)
20. van Benthem, J.F.A.K.: The logic of time. A model-theoretic investigation into the varieties of temporal ontology and temporal discourse. Synthese Library, vol. 156. D. Reidel Publishing Co., Dordrecht (1983)
21. Woodin, W.H.: The continuum hypothesis, the generic multiverse of sets, and the ω conjecture (2009) (preprint)

Constructing Cut Free Sequent Systems with Context Restrictions Based on Classical or Intuitionistic Logic*

Björn Lellmann[1] and Dirk Pattinson[2]

[1] Department of Computing, Imperial College London, UK
[2] Research School of Computer Science, The Australian National University

Abstract. We consider a general format for sequent rules for not necessarily normal modal logics based on classical or intuitionistic propositional logic and provide relatively simple local conditions ensuring cut elimination for such rule sets. The rule format encompasses e.g. rules for the boolean connectives and transitive modal logics such as *S4* or its constructive version. We also adapt the method of constructing suitable rule sets by saturation to the intuitionistic setting and provide a criterium for translating axioms for intuitionistic modal logics into sequent rules. Examples include constructive modal logics and conditional logic $\mathbb{VA}$.

1 Introduction

It can hardly be disputed that cut elimination theorems are at the foundation of both theoretical investigation and practical implementation of automated reasoning techniques: the ensuing subformula property implies not only decidability of many logical systems, but also lies – mostly in the form of tableau methods – at the heart of the vast majority of implementations of various logics. Achieving cut elimination is usually a two stage process. First, a (sound and complete) set of sequent rules needs to be exhibited. Second, cut elimination is established. Both steps are equally laborious: finding the 'right' set of rules requires ingenuity and (syntactic) proofs of cut elimination rely on the judicious analysis of a large number of cases. Given the growth of logical systems of interest in particular in computer science, both generic methods with efficient tools for designing cut-free calculi, and meta-theorems that guarantee cut-elimination, decidability, and complexity bounds are therefore increasingly important.

This paper explores the method of cut elimination by saturation and extends previous work into two important directions. First, we can now also allow for the propositional base logic to be intuitionistic which allows us to treat a range of logics that have attracted interest in computer science [17,2]. Second, we generalise the approach to logics given by axioms of arbitrary modal rank. This is achieved by considering sequent rules with *context restrictions* where each premiss only propagates context formulae of a specific form. A prime example for this rule format are e.g. the rules of modal logic *S4*, where a premiss e.g. copies only boxed formulae on the left hand side. This extended rule format necessitates an extension of the previous characterisation of cut-free systems to deal with additional cases in the proof of cut elimination. In order to make full use of the extended rule format we investigate a method for translating axioms into

---

* Supported by EPSRC-Project EP/H016317/1.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 148–160, 2013.

rules which works uniformly for classical and intuitionistic logics. The rules so constructed are by construction sound and complete (in the presence of cut) and give rise to unlabelled sequent systems that are amenable to saturation under cuts between rules. In case the resulting rules fulfil our criteria for cut elimination and are also tractable they give rise to a generic EXPTIME decision algorithm for the logic. Our main contributions are the following: we formalise the notion of a rule with context restrictions (Definition 3), give a general criterion for cut elimination to obtain for a large class of modal logics extending classical or intuitionistic propositional logic (Theorem 16), and show how to construct sequent systems satisfying these requirements from axioms of a certain form (Section 3.2). We illustrate these techniques by reconstructing known cut-free sequent systems for constructive *S4*, constructive *K* and access control logic *CDD*, and also obtain a new cut-free calculus for Lewis' conditional logic *VA*. The techniques used are easily modified to treat e.g. minimal logic [9] or the $\{\wedge, \vee\}$-fragment of intuitionistic logic as base logics, but since we are not aware of modal logics based on either of these we restrict ourselves to the classical and intuitionistic cases.

Related Work: The method of cut elimination by saturation for extensions of classical logic with non-nested axioms was explored e.g. in [16,10]. The idea of contraction closed rule sets for first order and modal logics seems to have been formulated for the first time in [15,14], where also translations of axioms into rules of a labelled sequent system are given. Our rules with context restrictions are weaker versions of the rules with context relations from [3], which also allow the context formulae to change. While context relations are more general than context restrictions, apparently no syntactical criteria for cut elimination in such systems have been established yet. Our translations of axioms for intuitionistic modal logics into rules are motivated by the translations of (non-modal) axioms into structural rules for substructural logic in [6].

2 Preliminaries

Throughout, $\mathcal{V}$ denotes a denumerable set of propositional variables and Λ is a set of connectives with associated arities. We write $\boldsymbol{p}$ for finite sequences of propositional variables. The set of *Λ-formulae* is defined by $\mathcal{F}(\Lambda) \ni A_1, \dots, A_n ::= p \mid \heartsuit(A_1, \dots, A_n)$ for $p \in \mathcal{V}$ and $\heartsuit \in \Lambda$ with arity n. We write $\Lambda(S) = \{\heartsuit(A_1, \dots, A_n) \mid \heartsuit \in \Lambda\ n\text{-ary}, A_1, \dots, A_n \in S\}$ for the set of formulae constructed from S using a single connective in Λ. Uniform substitution of all propositional variables in a formula A using a substitution $\sigma : \mathcal{V} \to \mathcal{F}(\Lambda)$ is denoted by $A\sigma$. The set $\mathcal{S}(F)$ of *(symmetric) sequents* over F consists of tuples of multisets Γ, Δ of formulae in F, written $\Gamma \Rightarrow \Delta$. When dealing with extensions of intuitionistic propositional logic we consider *asymmetric sequents*, in which the right hand side Δ consists of at most one formula. The formulae in Γ occur *negatively* in the sequent, those in Δ *positively*. The multiset union of two multisets Γ and Δ is written Γ, Δ and we identify formulae with singleton multisets. Substitution extends to both multisets of formulae and sequents in the obvious way (perserving multiplicity), e.g. $(A_1, A_2 \Rightarrow B)\sigma = A_1\sigma, A_2\sigma \Rightarrow B\sigma$. We use the systems $\mathsf{G2}cp$ and $\mathsf{G2}ip$ of [18] with axioms $\Gamma, A \Rightarrow \Delta, A$ (where A ranges over the set of formulae) and the intuitionistic left implication rule $\dfrac{\Gamma \Rightarrow A \quad \Gamma, B \Rightarrow C}{\Gamma, A \to B \Rightarrow C}$ as basis for all systems that extend classical respectively intuitionistic propositional logic and write G resp. $\mathsf{G}i$ for these sets of rules. Our structural rules are

$$\frac{\Gamma \Rightarrow \Delta}{\Sigma, \Gamma \Rightarrow \Delta, \Pi}\ \mathsf{W}, \quad \frac{\Gamma, A, A \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta}\ \mathsf{ConL}, \quad \frac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}\ \mathsf{ConR}, \quad \frac{\Gamma \Rightarrow \Delta, A \quad A, \Sigma \Rightarrow \Pi}{\Gamma, \Sigma \Rightarrow \Delta, \Pi}\ \mathsf{Cut}\ .$$

3 Generic Cut Elimination and Construction of Cut-Free Systems

We start our investigation with the observation that while standard sequent rules for the boolean connectives carry over the whole context to the premisses, in standard sequent systems for many modal logics such as *K* or *S4* [19] either no or only modalised context formulae are propagated from conclusion to premisses. At the same time exactly one layer of modalities is added to the principal formulae. In order to fit these different formats into a unified framework we now generalise the notion of a shallow rule [10] using the notion of *context restrictions*, a weaker form of the context relations in [3].

Definition 1. If F is a set of formulae, a *context restriction* C *over* F (or simply a *restriction*) is given by a tuple of sets of formulae in F, i.e. $C = \langle F_1, F_2 \rangle$ with $F_1, F_2 \subseteq F$. We write $\mathfrak{C}(F)$ for the set of context restrictions over F. For a restriction $C = \langle F_1, F_2 \rangle$ and a sequent $\Gamma \Rightarrow \Delta$ we write $(\Gamma \Rightarrow \Delta) \restriction_C$ or $\Gamma \restriction_{F_1} \Rightarrow \Delta \restriction_{F_2}$ for the sequent consisting of the restriction of Γ (resp. Δ) to substitution instances of formulae A with $A \in F_1$ (resp. $A \in F_2$) on the left (resp. right) hand side. An occurrence of a formula in a sequent $\Gamma \Rightarrow \Delta$ *satisfies* context restriction C if it also occurs in $(\Gamma \Rightarrow \Delta) \restriction_C$, and a sequent $\Gamma \Rightarrow \Delta$ satisfies C if $(\Gamma \Rightarrow \Delta) \restriction_C = \Gamma \Rightarrow \Delta$. Finally, a context restriction C' satisfies C if every sequent which satisfies C' also satisfies C.

Example 2. 1. The *trivial restriction* $C_{id} := \langle \{p\}, \{p\} \rangle$ does not restrict a sequent at all, we always have $(\Gamma \Rightarrow \Delta) \restriction_{C_{id}} = \Gamma \Rightarrow \Delta$.

2. The *empty restriction* $C_\emptyset := \langle \emptyset, \emptyset \rangle$ deletes every formula in a sequent: $(\Gamma \Rightarrow \Delta) \restriction_{C_\emptyset} = \ \Rightarrow\ $.

3. The restriction $C_{4\Box} := \langle \{\Box p\}, \emptyset \rangle$ deletes the right side of a sequent and restricts the left side to boxed formulae. E.g.: $(A, C \wedge D, \Box(A \vee B) \Rightarrow \Box D, B) \restriction_{C_{4\Box}} = \Box(A \vee B) \Rightarrow$.

Definition 3. A *rule with context restrictions* (or simply a *rule*) is a tuple $(\ \mathcal{P}; \Sigma \Rightarrow \Pi\ )$ where $\mathcal{P} \subseteq \mathcal{S}(\mathcal{V}) \times \mathfrak{C}(\mathcal{F})$ is the set of *premisses* with associated context restrictions, and $\Sigma \Rightarrow \Pi \in \mathcal{S}(\Lambda(\mathcal{V}))$ are the *principal formulae*, such that no variable occurs twice in the principal formulae and every variable occurs in the principal formulae if it occurs in at least one of the premisses. An *instance* of a rule R is given by a substitution $\sigma : \mathcal{V} \to \mathcal{F}$ and a *context* $\Gamma \Rightarrow \Delta \in \mathcal{S}(\mathcal{F})$ and is written as

$$\frac{\{\ \Gamma \restriction_{F_1}, \Theta\sigma \Rightarrow \Delta \restriction_{F_2}, \Upsilon\sigma \mid (\Theta \Rightarrow \Upsilon; \langle F_1, F_2 \rangle) \in \mathcal{P}\ \}}{\Gamma, \Sigma\sigma \Rightarrow \Delta, \Pi\sigma}\ .$$

Whenever we mention a set of rules we assume that it is closed under injective renaming of variables and for all n-ary $\heartsuit \in \Lambda$ and $\boldsymbol{p} = (p_1, \ldots, p_n)$ and $\boldsymbol{q} = (q_1, \ldots, q_n)$ includes the *congruence rules* $(\{(p_i \Rightarrow q_i; C_\emptyset) \mid i \leq n\} \cup \{(q_i \Rightarrow p_i; C_\emptyset) \mid i \leq n\}; \heartsuit\boldsymbol{p} \Rightarrow \heartsuit\boldsymbol{q})$.

Table 1. Some sequent rules as rules with context restrictions and in standard notation [18,19]

$R_{K_n} := (\{(p_1, \ldots, p_n \Rightarrow q; C_\emptyset)\}; \Box p_1, \ldots, \Box p_n \Rightarrow \Box q)$	$\dfrac{A_1, \ldots, A_n \Rightarrow B}{\Gamma, \Box A_1, \ldots, \Box A_n \Rightarrow \Delta, \Box B}$
$R_{T\Box} := (\{(p \Rightarrow\ ; C_{id})\}; \Box p \Rightarrow)$	$\dfrac{\Gamma, A \Rightarrow \Delta}{\Gamma, \Box A \Rightarrow \Delta}$
$R_{4\Box} := (\{(\ \Rightarrow p\ ; C_{4\Box})\};\ \Rightarrow \Box p)$	$\dfrac{\Box\Sigma \Rightarrow A}{\Gamma, \Box\Sigma \Rightarrow \Delta, \Box A}$

Thus if a formula A is in the left component of a restriction associated with a premiss of a rule, then in an instance of this rule the premiss carries over all substitution instances of A from the left hand side of the context, and dually for the right hand side.

Example 4. The rules of G as well as the rules $\mathcal{R}_K := \{R_{K_n} \mid n \geq 0\}$ of modal logic K and $\mathcal{R}_{S4} := \{R_{T\Box}, R_{4\Box}\}$ of modal logic *S4* from Table 1 are rules with context restrictions.

Definition 5. Let $\mathcal{R}$ be a set of rules and $S \subseteq \mathcal{S}(\mathcal{F})$ a set of sequents. We use the standard notion of *derivations* [18] and say that a sequent $\Gamma \Rightarrow \Delta$ is *$\mathcal{R}$-derivable from* S if there is a derivation of $\Gamma \Rightarrow \Delta$ from S using only instances of rules in $\mathcal{R}$. We then write $S \vdash_{\mathcal{R}} \Gamma \Rightarrow \Delta$. If we consider rules for asymmetric sequents we will indicate this by writing $\vdash^i_{\mathcal{R}}$, and we write $\vdash^{[i]}_{\mathcal{R}}$ if a result holds in both settings. Derivability from $\emptyset$ is denoted by $\vdash^{[i]}_{\mathcal{R}} \Gamma \Rightarrow \Delta$ and derivability in $\mathcal{R}_1 \cup \mathcal{R}_2$ by $\vdash^{[i]}_{\mathcal{R}_1\mathcal{R}_2}$. We write $\mathcal{R}[\mathsf{CutCon}]$ if a statement holds for $\mathcal{R}$ and extensions with Cut and / or Con.

Admissibility of Weakening is shown by a standard induction on the derivations:

Lemma 6. *For every set $\mathcal{R}$ of rules and (asymmetric) sequent $\Gamma \Rightarrow \Delta$ we have* $\vdash^{[i]}_{\mathcal{R}[\mathsf{CutCon}]}$ $\Gamma \Rightarrow \Delta$ *whenever* $\vdash^{[i]}_{\mathcal{R}\mathsf{W}[\mathsf{CutCon}]} \Gamma \Rightarrow \Delta$.

3.1 Cuts between Rules and Cut Elimination

The main tool in the construction of cut free rule sets is the notion of *cuts between rules* from [10,11] that we need to adapt to handle context restrictions. Cut between rules is a two-stage process: first we replace a pair of rules by the rule arising from performing a cut between the conclusions. In a second step we modify the premisses so that variables that no longer appear in the conclusion of the cut are eliminated.

Definition 7. If $\mathcal{P} \subseteq \mathcal{S}(\mathcal{V}) \times \mathfrak{C}(\mathcal{F})$ is a set of premisses with context restrictions, then for $p \in \mathcal{V}$ the *p-elimination of* $\mathcal{P}$ is the set

$$\begin{aligned} \mathcal{P} \ominus p := \{\, (\Gamma, \Sigma \Rightarrow \Delta, \Pi;\ C_1 \cup C_2) \mid (\Gamma \Rightarrow \Delta, p;\ C_1) \in \mathcal{P},\ (p, \Sigma \Rightarrow \Pi;\ C_2) \in \mathcal{P} \,\} \\ \cup \{\, (\Gamma \Rightarrow \Delta;\ C) \mid (\Gamma \Rightarrow \Delta;\ C) \in \mathcal{P},\ p \notin \Gamma, \Delta \,\}, \end{aligned}$$

where for restrictions $C_1 = \langle F_1, F_2 \rangle$ and $C_2 = \langle G_1, G_2 \rangle$ we write $C_1 \cup C_2$ for $\langle F_1 \cup G_1, F_2 \cup G_2 \rangle$. Iterated elimination of variables $\boldsymbol{p} = p_1, \ldots, p_n$ is denoted by $\mathcal{P} \ominus \boldsymbol{p}$. For rules $R = (\mathcal{P}_R; \Gamma \Rightarrow \Delta, \heartsuit\boldsymbol{p})$ and $Q = (\mathcal{P}_Q; \heartsuit\boldsymbol{p}, \Sigma \Rightarrow \Pi)$ the *cut between R and Q on $\heartsuit\boldsymbol{p}$* is the rule $\mathsf{cut}(R, Q, \heartsuit\boldsymbol{p}) :=(\ (\mathcal{P}_R \cup \mathcal{P}_Q) \ominus \boldsymbol{p};\ \Gamma, \Sigma \Rightarrow \Delta, \Pi\ )$. A rule set $\mathcal{R}$ is *principal-cut closed* if it is closed under cuts between rules.

Example 8. 1. The rule sets $\mathsf{G}[i]$ are principal-cut closed, since cuts between rules can be replaced by the *identity rule* $R_{id} := (\{(\Rightarrow ; C_{id})\}; \Rightarrow)$.

2. The rule set $\mathcal{R}_K$ is principal-cut closed, since $\mathsf{cut}(R_{K_n}, R_{K_m}, \Box q) = R_{K_{n+m-1}} \in \mathcal{R}_K$.
3. The rule set $\mathcal{R}_{S4}$ is principal-cut closed, since $\mathsf{cut}(R_{4\Box}, R_{T\Box}, \Box p) = R_{id}$.

Since in the presence of the rules for (intuitionistic) propositional logic it is possible to re-construct the cut formula from the premisses of the cut between two rules, saturating a rule set under cuts between rules does not change the set of derivable sequents:

Lemma 9. *If $\mathcal{R}$ is a set of rules and R is a cut between two rules from $\mathcal{R}$, then $\vdash^{[i]}_{\mathsf{G}[i]\mathsf{CutCon}\mathcal{R}R}$ $\Gamma \Rightarrow \Delta$ iff $\vdash^{[i]}_{\mathsf{G}[i]\mathsf{CutCon}\mathcal{R}}$ $\Gamma \Rightarrow \Delta$.*

Cuts between rules provide us with a means of eliminating cuts on principal formulae of two rules by replacing the cut with an instance of the cut between the two rules and a number of cuts on formulae of lower complexity. Moreover, Lemma 9 guarantees that we may simply add missing cuts to a rule set without jeopardising soundness. While this is enough for axioms without nested modalities [10], in the more general setting with context restrictions we need additional criteria for cuts involving context formulae:

Definition 10. Two restrictions $C_1 = \langle F_1, F_2 \rangle, C_2 = \langle G_1, G_2 \rangle$ *overlap* if there are formulae $A_1 \in F_2, A_2 \in G_1$ and substitutions σ_1, σ_2 with $A_1\sigma_1 = A_2\sigma_2$. A rule set $\mathcal{R}$ is

1. *context-cut closed* if whenever $R_0, R_1 \in \mathcal{R}$ and there are context restrictions C_0 of R_0 and C_1 of R_1 which overlap, then there is $i \in \{0, 1\}$ such that all context restrictions of R_i which overlap C_{1-i} and the principal formulae of R_i satisfy C_{1-i}.
2. *mixed-cut closed* if whenever $R, Q \in \mathcal{R}$ and a principal formula A of R satisfies a context restriction of Q, then all context restrictions of R and all principal formulae of R except for A satisfy all those context restrictions of Q satisfied by A.

Intuitively, these conditions allow pushing cuts involving context formulae into the premisses of one of the rules and eliminating them by induction on the cut level.

Example 11. 1. The rule sets $\mathsf{G}[i]$ are context- and mixed-cut closed because all the rules involve only the restriction C_{id} or its asymmetric version $C^i_{id} := \langle \{p\}, \emptyset \rangle$. Hence every restriction is satisfied by every principal formula and every other restriction.

2. The rule set $\mathcal{R}_K$ is trivially context- and mixed-cut closed.
3. The rule set $\mathcal{R}_{S4}$ is mixed-cut closed, since the restriction $C_{4\Box}$ satisfies C_{id}. Since the principal formula of $R_{4\Box}$ also satisfies C_{id}, the set is furthermore context-cut closed.

Since in general rules are not invertible and we need to take care of Contraction we will follow Gentzen's original strategy [8] when proving cut elimination and eliminate multicuts $\dfrac{\Gamma \Rightarrow \Delta, A^n \quad A^m, \Sigma \Rightarrow \Pi}{\Gamma, \Sigma \Rightarrow \Delta, \Pi}$ instead of cuts. Thus we also need to deal with multiple principal occurrences of the same formula. We do this by elevating contraction to the level of derivation rules and considering rule sets closed under this operation.

Definition 12 (**[11]**)**.** If $\mathcal{P}$ is a set of premisses with restrictions and $\boldsymbol{p} = (p_1, \ldots, p_n)$ and $\boldsymbol{q} = (q_1, \ldots, q_n)$ are n-tuples of variables, then $\mathcal{P}[\boldsymbol{q} \leftarrow \boldsymbol{p}]$ is the result of replacing every occurrence of q_i in a sequent occurring in a premiss in $\mathcal{P}$ by p_i for all $i = 1, \ldots, n$

and contracting duplicate instances of $p_1, \dots, p_n$. Let $R = (\mathcal{P}; \Gamma, \heartsuit \boldsymbol{p}, \heartsuit \boldsymbol{q} \Rightarrow \Delta)$ be a rule. The *left contraction of* R *on* $\heartsuit \boldsymbol{p}$ *and* $\heartsuit \boldsymbol{q}$ is the rule $\mathsf{ConL}(R, \heartsuit \boldsymbol{p}, \heartsuit \boldsymbol{q}) = (\mathcal{P}[\boldsymbol{q} \leftarrow \boldsymbol{p}]; \Gamma, \heartsuit \boldsymbol{p} \Rightarrow \Delta)$. The *right contraction* $\mathsf{ConR}(R, \heartsuit \boldsymbol{p}, \heartsuit \boldsymbol{q})$ is defined dually. A rule set $\mathcal{R}$ is *contraction closed* if for every rule $R \in \mathcal{R}$ instances of the rules $\mathsf{ConL}(R, \heartsuit \boldsymbol{p}, \heartsuit \boldsymbol{q})$ and $\mathsf{ConR}(R, \heartsuit \boldsymbol{p}, \heartsuit \boldsymbol{q})$ can be simulated by applications of Weakening and Contraction, followed by at most one application of a rule $R' \in \mathcal{R}$ and Weakening. A set of rules is *saturated* if it is contraction, principal-cut, context-cut, and mixed-cut closed.

Example 13. 1. The rules of $G[i]$ and $\mathcal{R}_{S4}$ are trivially contraction closed.

2. $\mathcal{R}_K$ is contraction closed because $\mathsf{ConL}(R_{K_n}, \Box p_{n-1}, \Box p_n) = R_{K_{n-1}} \in \mathcal{R}_K$.

Thus each of $\mathsf{G}[i], \mathcal{R}_K, \mathcal{R}_{S4}$ are saturated.

Theorem 14 (Cut Elimination). *For every saturated set* $\mathcal{R}$ *of rules and (asymmetric) sequent* $\Gamma \Rightarrow \Delta$ *we have* $\vdash^{[i]}_{\mathcal{R}\mathsf{Con}} \Gamma \Rightarrow \Delta$ *whenever* $\vdash^{[i]}_{\mathcal{R}\mathsf{ConCut}} \Gamma \Rightarrow \Delta$.

While saturated rule sets allow for cut elimination, we are also interested in decision procedures via backwards proof search. For this we also need admissibility of Contraction. While contraction closure of the rule set takes care of contractions of two principal formulae of a rule, for contractions of principal and context formulae we use the standard method of copying the relevant principal formulae into the premisses. This might seem a bit coarse but again is necessary because in general the rules are not invertible.

Definition 15. For a rule $R = (\mathcal{P}; \Sigma \Rightarrow \Pi)$ a *modified instance*

$$\frac{\{\, (\Gamma, \Sigma\sigma) \upharpoonright_{F_1}, \Theta\sigma \Rightarrow (\Delta, \Pi\sigma) \upharpoonright_{F_2}, \Upsilon\sigma \mid (\Theta \Rightarrow \Upsilon;\ \langle F_1, F_2 \rangle) \in \mathcal{P} \,\}}{\Gamma, \Sigma\sigma \Rightarrow \Delta, \Pi\sigma}$$

of R is given by a substitution $\sigma : \mathcal{V} \to \mathcal{F}$ and a context $\Gamma \Rightarrow \Delta \in \mathcal{S}(\mathcal{F})$. We write $\vdash_{\mathcal{R}^*}$ for derivability using modified instances instead of instances of rules in $\mathcal{R}$.

Theorem 16 (Admissibility of Contraction). *For every set* $\mathcal{R}$ *of rules and (asymmetric) sequent* $\Gamma \Rightarrow \Delta$ *we have* $\vdash^{[i]}_{\mathcal{R}\mathsf{Con}} \Gamma \Rightarrow \Delta$ *iff* $\vdash^{[i]}_{\mathcal{R}^*\mathsf{Con}} \Gamma \Rightarrow \Delta$ *iff* $\vdash^{[i]}_{\mathcal{R}^*} \Gamma \Rightarrow \Delta$.

If the rule set is furthermore *tractable* in the sense that given a sequent the rules with this sequent as conclusion have codes of size polynomial in the size of the sequent, which can be recognised in space polynomial in the size of the sequent, and given the code of a rule its premisses can be recognised in space polynomial in the code, we get a generic complexity bound for deciding derivability using modified instances. Due to the more general rule format this bound is slightly higher than the PSPACE bound in [10]. Whether this can be improved in general is subject of ongoing work.

Theorem 17. *For a saturated and tractable set* $\mathcal{R}$ *of rules, derivability in* $\mathcal{R}^*$ *is decidable in* EXPTIME.

3.2 Construction of Cut-Free Sequent Systems from Axioms

With Theorems 14 and 16 we have presented a general *criterion* for a sequent system with context restrictions to admit both cut and contraction. Of course now we need to construct sequent systems satisfying this criterion. As in the case without context restrictions [10] these results suggest constructing saturated rule sets by *saturation*: starting with a set of rules with context restrictions simply add missing cuts and contractions until no more new rules are found. In the presence of context restrictions, however, we then need to check that the resulting rule set is also context-cut closed and mixed-cut closed. The following well-known example shows that this need not be the case.

Example 18. The rule set $\mathcal{R}_{S5} :=\{\ (\{(p \Rightarrow\ ; C_{id})\}; \Box p \Rightarrow\ ),\ (\{(\ \Rightarrow p; C_{5\Box})\};\ \Rightarrow \Box p)\ \}$ with $C_{5\Box} := \langle\{\Box p\}, \{\Box p\}\rangle$ is contraction closed and principal- and context-cut closed. It is not mixed-cut closed, since the occurrence of the principal formula $\Box p$ of $R_{T\Box}$ satisfies the restriction $C_{5\Box}$ of $R_{5\Box}$, but the restriction C_{id} does not.

The method of constructing cut-free rule sets by saturation works reasonably well if we start with a set of sequent rules, but often the modal logics of interest are given in a Hilbert-style system by a set of axioms. Thus the first step in constructing a cut free sequent system from such axioms is to translate the axioms into sequent rules. While this can alway be done if the axioms are *non-nested*, i.e. without nested modalities, and the underlying propositional logic is classical, in the general case we need to be more careful. The notion of cuts between rules will be a useful tool in this step as well.

We assume that the underlying propositional logic is classical or intuitionistic. In a first step we extend the method for converting non-nested axioms from [10] to the asymmetric setting using notions from [6]. The main idea is to first treat the modal subformulae in a non-nested axiom like propositional variables, use invertibility of the underlying rule set to break the axiom into a finite number of sequents, and then resolve propositional logic under the modalities by introducing new variables and premisses stating that these variables are equivalent to the original formulae. Finally, these premisses are again broken up using invertibility of the underlying rules. To identify the axioms which can be broken up we loosely follow the idea of the substructural hierarchy from [6] and consider the notions of left resolvable and right resolvable formulae. Intuitively, if a right resolvable formula occurs positively in a sequent, its main (boolean) connective can be broken up. We introduce these notions in a generic form which allows treating classical and intuitionistic logics in the same framework. Also this shows that they are easily adapted to other logics such as minimal or distributive logic.

Definition 19. The sets $\mathcal{F}_r$ of *right resolvable formulae* and $\mathcal{F}_\ell$ of *left resolvable formulae* and their intuitionistic versions ${\mathcal{F}_r}^i$ and ${\mathcal{F}_\ell}^i$ are defined recursively by

1. if $p \in \mathcal{V}$ then $p \in {\mathcal{F}_r}^{[i]}$ and $p \in {\mathcal{F}_\ell}^{[i]}$;
2. $\bot \in {\mathcal{F}_r}^{[i]}$ and $\bot \in {\mathcal{F}_\ell}^{[i]}$;
3. if $A_1, A_2 \in {\mathcal{F}_r}^{[i]}$ then $A_1 \wedge A_2 \in {\mathcal{F}_r}^{[i]}$ and $A_1 \vee A_2 \in \mathcal{F}_r$;
4. if $A_1, A_2 \in {\mathcal{F}_\ell}^{[i]}$ then $A_1 \wedge A_2 \in {\mathcal{F}_\ell}^{[i]}$ and $A_1 \vee A_2 \in {\mathcal{F}_\ell}^{[i]}$;
5. if $A_1 \in {\mathcal{F}_\ell}^{[i]}$ and $A_2 \in {\mathcal{F}_r}^{[i]}$ then $A_1 \to A_2 \in {\mathcal{F}_r}^{[i]}$;
6. if $A_1 \in \mathcal{F}_r$ and $A_2 \in \mathcal{F}_\ell$ then $A_1 \to A_2 \in \mathcal{F}_\ell$

where again we write ${\mathcal{F}_r}^{[i]}$ if a clause applies both to $\mathcal{F}_r$ and ${\mathcal{F}_r}^i$.

Example 20. The formula $p \wedge ((p \vee q) \to r)$ is intuitionistically right resolvable. Both $p \vee q$ and $(p \to q) \to \bot$ are classically right resolvable, but not intuitionistically.

Since the premisses of the right (left) rule for the main connective of a right (left) resolvable formula can be derived from its conclusion in $\mathsf{G}[i]\mathsf{Cut}$, we may decompose an axiom $\overline{\Rightarrow A}$ for $A \in \mathcal{F}_r$ into a number of sequents over $\mathcal{V}$, similar to computing the regular normal form [15] of a formula:

Lemma 21. *Let* $\Gamma \subseteq \mathcal{F}_\ell{}^{[i]}$ *and* $\Delta \subseteq \mathcal{F}_r{}^{[i]}$. *Then there are unique sequents* $\Gamma_i \Rightarrow \Delta_i \in \mathcal{S}(\mathcal{V})$ *such that the axiom* $\overline{\Gamma \Rightarrow \Delta}$ *is equivalent in* $\mathsf{G}[i]\mathsf{CutCon}$ *to* $\overline{\Gamma_1 \Rightarrow \Delta_1}, \dots, \overline{\Gamma_n \Rightarrow \Delta_n}$.

This Lemma is used to break modal axioms into sequents by treating the modalised subformulae as variables. Then the propositional variables are moved into the premisses:

Lemma 22. *For* $\Gamma \Rightarrow \Delta \in \mathcal{S}(\mathcal{V})$ *and* $\Sigma \Rightarrow \Pi \in \mathcal{S}(\Lambda(\mathcal{V}))$ *the axiom* $\overline{\Gamma, \Sigma \Rightarrow \Delta, \Pi}$ *is equivalent in* $\mathsf{G}[i]\mathsf{CutCon}$ *to the rule* $(\{(\Rightarrow p; C_{id}^{[i]}) \mid p \in \Gamma\} \cup \{(p \Rightarrow ; C_{id}) \mid p \in \Delta\}; \Sigma \Rightarrow \Pi)$.

In the case of axioms with modal nesting depth one we now eliminate propositional logic under the modalities by adding new variables for the immediate subformulae and new premisses stating that the variables are equivalent to the original subformulae. Unfortunately the result of this operation is not necessarily a rule in our sense, since the sequents occurring in the premisses do not only include variables. Fortunately, if the modality in question is monotone or antitone (see below), we can cut this "rule" with the monotonicity rule (or its antitone counterpart) to eliminate one of the new premisses. We call the newly introduced premisses the *premisses for the subformula A* and say that the premisses for a subformula can be *resolved* if there are equivalent premisses consisting of sequents over variables. The following Definition and Lemma give criteria on when the premisses can be resolved.

Definition 23. Let $\mathcal{R}$ be a set of rules, $\boldsymbol{p} = p_1, \dots, p_n$ and $\boldsymbol{q} = q_1, \dots, q_n$. For $k \leq n$ a n-ary modality $\heartsuit \boldsymbol{p}$ is *monotone in the k-th argument* if the rule $R_{mon_k} = (\{(p_k \Rightarrow q_k; C_\emptyset)\} \cup \{(p_\ell \Rightarrow q_\ell; C_\emptyset) \mid k \neq \ell \leq n\} \cup \{(q_\ell \Rightarrow p_\ell; C_\emptyset) \mid k \neq \ell \leq n\}; \heartsuit \boldsymbol{p} \Rightarrow \heartsuit \boldsymbol{q})$ is in $\mathcal{R}$. It is *antitone in the k-th argument* if the rule R_{ant_k} with premiss $(q_k \Rightarrow p_k; C_\emptyset)$ instead of $(p_k \Rightarrow q_k; C_\emptyset)$ is in $\mathcal{R}$.

Lemma 24. *Let* $\mathcal{R}$ *be a rule set. Then for a sequent* $\Gamma \Rightarrow \Delta, \heartsuit(\dots, A_k, \dots)$ *the premisses for* A_k *can be resolved if:* $A_k \in \mathcal{F}_\ell{}^{[i]}$ *and* $\heartsuit$ *is monotone in the k-th argument; or* $A_k \in \mathcal{F}_r{}^{[i]}$ *and* $\heartsuit$ *is antitone in the k-th argument; or* $A_k \in \mathcal{F}_\ell{}^{[i]} \cap \mathcal{F}_r{}^{[i]}$. *For a sequent* $\heartsuit(\dots, A_k, \dots), \Gamma \Rightarrow \Delta$ *we have the analogous result with* $\mathcal{F}_\ell{}^{[i]}$ *and* $\mathcal{F}_r{}^{[i]}$ *exchanged.*

The previous Lemmata yield general criteria as to which axioms are translatable into rules. For the sake of brevity we only state the result for unary monotone modalities; The generalisations to non-monotone modalities and higher arities are straightforward.

Definition 25. For $A \in \mathcal{F}_r{}^{[i]}$ and $p \in \mathcal{V}$ we say that p is *positive* (resp. *negative*) in A, if it occurs positively (resp. negatively) in a sequent of the decomposition of the sequent $\Rightarrow A$ according to Lemma 21.

Theorem 26. *Let* A *be a propositional formula with variables* $p_1, \dots, p_n, q_1, \dots, q_m$, *and for* $i = 1, \dots, m$ *let the modality* $\heartsuit_i$ *be unary monotone and* A_i *a propositional* *formula with variables in* $p_1, \ldots, p_n$ *such that:* q_i *is only positive in* A *and* $A_i \in \mathcal{F}_\ell{}^{[i]}$*; or* q_i *is only negative in* A *and* $A_i \in \mathcal{F}_r{}^{[i]}$*; or* $A \in \mathcal{F}_\ell{}^{[i]} \cap \mathcal{F}_r{}^{[i]}$*. Then there is a rule which is equivalent in* $\mathsf{G}[i]\mathsf{CutCon}$ *to the axiom* $\overline{\Rightarrow A\sigma}$ *where* $\sigma(q_i) = \heartsuit_i(A_i)$ *and* $\sigma(p_i) = p_i$*.*

Remark 27. Since for classical propositional logic all propositional formulae are both right and left resolvable, the previous Theorem yields the translation result for non-nested axioms from [10] as a Corollary.

For axioms with nested modalities we may sometimes use a similar procedure if a modalised formula occurs both on the top level of the axiom and under a modality. The idea is to introduce a fresh variable for this formula and apply the methods above to resolve propositional logic under the modalities, but without moving the top level occurrences of the variable into the premisses with Lemma 22. If now the occurrences of this variable in the premisses and the conclusion are all negative (resp. positive), we may it replace it again with the original formula. Since this formula now occurs both in the premisses and the conclusion this often gives rise to a context restriction. We will illustrate this method using examples in the next section.

4 Applications

Example 28 (Constructive K**).** Constructive modal logic K from [4,13] is based on intuitionistic propositional logic and has rules $Reg_\Box = (\{(p \Rightarrow q; C_\emptyset)\}; \Box p \Rightarrow \Box q)$ and $Reg_\Diamond = (\{(p \Rightarrow q; C_\emptyset)\}; \Diamond p \Rightarrow \Diamond q)$ and axioms $(FS1)$ $\Box\top$, $(FS2)$ $(\Box(p \wedge q) \to (\Box p \wedge \Box q)) \wedge ((\Box p \wedge \Box q) \to \Box(p \wedge q))$ and $(FS6)$ $\Diamond(p \to q) \to (\Box p \to \Diamond q)$. Since the propositional part is intuitionistic we base our treatment on the asymmetric setting. The rules $Reg_\Box$ and $Reg_\Diamond$ ensure that both modalities $\Box$ and $\Diamond$ are monotone in the sense of Definition 23. Treating modalised subformulae as variables and using Lemma 21 and the fact that $A \to B$ is intuitionistically left resolvable to break up axiom $(FS6)$ first yields the axiom $\overline{\Diamond(p \to q), \Box p \Rightarrow \Diamond q}$. Now introducing a new variable $r_{p\to q}$ and premisses for subformula $p \to q$ yields

$$\frac{r_{p\to q} \Rightarrow p \to q \qquad p \to q \Rightarrow r_{p\to q}}{\Diamond r_{p\to q}, \Box p \Rightarrow \Diamond q}\;.$$

But now a cut with rule $Reg_\Diamond$ on $\Diamond r_{p\to q}$ and resolving the remaining premiss gives the rule $\dfrac{s, p \Rightarrow q}{\Diamond s, \Box p \Rightarrow \Diamond q}\ R_{FS6}$. The analogous treatment for axioms $(FS2)$ and $(FS1)$ gives the well-known rules $R_{FS2} := (\{(p, q \Rightarrow r; C_\emptyset)\}; \Box p, \Box q \Rightarrow \Box r)$ and $R_{FS1} := (\{(\Rightarrow p; C_\emptyset)\}; \Rightarrow \Box p)$. Now saturating the rule set under cuts yields the rule set

$$\mathcal{R}_{CK} := \left\{\frac{p_1, \ldots, p_n \Rightarrow q}{\Gamma, \Box p_1, \ldots, \Box p_n \Rightarrow \Box q}\ R_{CK_n} \mid n \geq 0\right\} \cup \left\{\frac{p_1, \ldots, p_n, q \Rightarrow r}{\Gamma, \Box p_1, \ldots, \Box p_n, \Diamond q \Rightarrow \Diamond r} \mid n \geq 0\right\}\;.$$

Of course this rule set is not new [4]. The point here is that we constructed it in a purely syntactical way from the axioms of the Hilbert-system.

To illustrate the use of Lemma 22 let us add the T-axioms $(T\Box)$ $\Box p \to p$ and $(T\Diamond)$ $p \to \Diamond p$. Again, the axioms are first broken up into $\overline{\Box p \Rightarrow p}$ and $\overline{p \Rightarrow \Diamond p}$. Then they are transformed into equivalent rules $R_{T\Box} = (\{(p \Rightarrow\ ; C_{id})\}; \Box p \Rightarrow\ )$ and $R_{T\Diamond} = (\{(\ \Rightarrow p; C^{i}_{id})\};\ \Rightarrow \Diamond p)$. Now saturation under cuts would yield the additional rules $(\{(p_1, \dots, p_n \Rightarrow\ ; C_{id})\}; \Box p_1, \dots, \Box p_n \Rightarrow\ )$ and $(\{(p_1, \dots, p_n \Rightarrow r; C^{i}_{id})\}; \Box p_1, \dots, \Box p_n \Rightarrow \Diamond r)$ for $n \geq 0$, but these are simulated by repeated applications of $R_{T\Box}$ and $R_{T\Diamond}$. Thus it is easy to see that the rule sets $\mathcal{R}_{CK}$ and $\mathcal{R}_{CK} \cup \{R_{T\Box}, R_{T\Diamond}\}$ are saturated.

Note that these constructions do not give rise to context restrictions apart from $C_\emptyset$ and $C^{[i]}_{id}$. For this we need to consider axioms with nested modalities. Unfortunately, if we are dealing with nested modalities the translation becomes more involved and much less automatic. Nonetheless, as mentioned before in some cases we can still use the method of cutting rules on principal formulae to construct rules with context restrictions. The main idea is to make use of formulae occurring both under a modality and on the top level of the sequent and to construct a context restriction out of this formula.

Example 29 (Constructive *S4*). Constructive modal logic *CS4* from [17,2] contains the rules $\mathcal{R}_{CK} \cup \{R_{T\Box}, R_{T\Diamond}\}$ and additional axioms $(4\Box)$ $\Box p \to \Box\Box p$ and $(4\Diamond)$ $\Diamond\Diamond p \to \Diamond p$. We make use of the fact that in these we have the same modalised formula occurring on the top level and under a modality as follows: Take axiom $(4\Box)$ and in a first step replace the occurrence of $\Box p$ under the modality by a fresh variable q. The resulting axiom $\Box p \to \Box q$ is broken up into the sequent $\Box p \Rightarrow \Box q$. Then adding the premisses for q we get $\frac{\Box p \Rightarrow q \quad q \Rightarrow \Box p}{\Box p \Rightarrow \Box q}$ and a cut with the monotonicity rule $Reg_\Box$ yields $\frac{\Box p \Rightarrow q}{\Box p \Rightarrow \Box q}$. Now computing principal cuts of a number of instances of this rule with rule R_{CK_n} yields

$$\frac{\Box p_1, \dots, \Box p_m, q_1, \dots, q_k \Rightarrow r}{\Gamma, \Box p_1, \dots, \Box p_m, \Box q_1, \dots, \Box q_k \Rightarrow \Box r}\,.$$

But since the $\Box p_i$ occur both in conclusion and premiss of the rule, this is exactly the rule $R_{4\Box} = (\{(q_1, \dots, q_k \Rightarrow r; C_{4\Box})\}; \Box q_1, \dots, \Box q_k \Rightarrow \Box r)$. Moreover, the rule $\frac{\Box p \Rightarrow q}{\Box p \Rightarrow \Box q}$ is sound by the methods of the last section, and since $R_{4\Box}$ was constructed from this rule and R_{CK_n} by means of principal cuts, Lemma 9 ensures that it is sound as well. A similar process for axiom $(4\Diamond)$ yields the rules $R_{4\Diamond} := (\{(p_1, \dots, p_n, q \Rightarrow C_{4\Diamond})\}; \Box p_1, \dots, \Box p_n, \Diamond q \Rightarrow\ )$ with context restriction $C_{4\Diamond} = \langle \emptyset, \{\Diamond p\}\rangle$. Now adding the missing principal cuts again yields a rule set which is principal-cut closed. It is trivially context-cut closed, and easily checked to be mixed-cut and contraction closed and therefore saturated. Again, the rules are not new, but we constructed them in a purely syntactical way, and their soundness and completeness is guaranteed by construction.

This method can also be applied if the subformula occurs under a modality more than once, or if it is more complex. In the latter case in general this gives rise to more complex context restrictions. The following example shows how sometimes more complex restrictions can be simplified and how context restrictions $C^{[i]}_{id}$ may arise other than as a consequence of Lemma 22.

Example 30 (Access Control Logic *CDD*). Access control logic *CDD* from [1] is based on intuitionistic propositional logic and has indexed normal (and thus monotone) modalities $\bigcirc_k A$ which are interpreted as *principal k says A*. For this example we consider the axiomatisation with the axioms [unit] $p \to \bigcirc_k p$ and [GHO] $\bigcirc_k (p \to \bigcirc_k q) \to (p \to \bigcirc_k q)$ (see [1]). The first axiom straightforwardly translates into the rule $R_{[\mathsf{unit}]} = (\ \{(\ \Rightarrow\ p; C^i_{id})\};\ \Rightarrow \bigcirc_k p\ )$. For the latter axiom we first introduce a variable r for the formula $(p \to \bigcirc_k q)$ under the modality and apply the methods above to obtain

$$\frac{r \Rightarrow p \to \bigcirc_k q}{\Gamma, \bigcirc_k r \Rightarrow p \to \bigcirc_k q}.$$

But now instead of turning this into a rule with context restriction $\langle \emptyset, \{p \to \bigcirc_k q\}\rangle$ we break up the boolean part to arrive at $\frac{r, p \Rightarrow \bigcirc_k q}{\Gamma, \bigcirc_k r, p \Rightarrow \bigcirc_k q}$. Since disjunctions are intuitionistically left resolvable the variable p can be taken to be the context on the left hand side, and this is equivalent to the rule $R_{[\mathsf{GHO}]} = (\ \{(r \Rightarrow\ ; C_{cdd,k})\}; \bigcirc_k r \Rightarrow\ )$ with restriction $C_{cdd,k} := \langle \{p\}, \{\bigcirc_k p\}\rangle$. Since the rules R_{K_n} for $\bigcirc_k$ are simulated by applications of $R_{[\mathsf{unit}]}$ and $R_{[\mathsf{GHO}]}$, this yields the rule set $\mathcal{R}_{CDD} := \{R_{[\mathsf{unit}]}, R_{[\mathsf{GHO}]}\}$ which again is easily seen to be saturated and thus have cut elimination. Of course again this rule set is not new (see e.g. [7,5]) and there are other ways to construct it, but it nicely illustrates how context restrictions arise.

Example 31 (Conditional Logic with Absoluteness). As a final example let us construct a cut-free set of rules with context restrictions for a logic based on classical propositional logic, namely for Lewis' conditional logic $\mathbb{VA}$ from [12]. The language for this logic contains the binary modality $\preccurlyeq$ called *comparative plausibility operator* with the intuitive reading "A is at least as plausible as B" for $A \preccurlyeq B$. The logic $\mathbb{VA}$ is given as an axiomatic extension of the logic $\mathbb{V}$, where the latter is characterised by non-nested axioms only and does not necessitate the use of rules with context restrictions. For this reason we concentrate on the new axioms and make use of the rules $\mathcal{R}_{\mathbb{V}} = \{R_{n,m} \mid n \geq 1, m \geq 0\}$ from [11] for the logic $\mathbb{V}$, where rule $R_{n,m}$ in our notation is given as $(\ \{(s_k \Rightarrow r_1, \dots, r_n, q_1, \dots, q_m; C_\emptyset) \mid k \leq n\} \cup \{(p_k \Rightarrow r_1, \dots, r_n, q_1, \dots, q_{k-1}; C_\emptyset) \mid k \leq m\};\ p_1 \preccurlyeq q_1, \dots, p_m \preccurlyeq q_m \Rightarrow r_1 \preccurlyeq s_1, \dots, r_n \preccurlyeq s_n\ )$.

For $\mathbb{VA}$ we need to add the two *absoluteness axioms* $(p \preccurlyeq q) \to (\bot \preccurlyeq \neg(p \preccurlyeq q))$ and $\neg(p \preccurlyeq q) \to (\bot \preccurlyeq (p \preccurlyeq q))$. We use the fact that the formula $(p \preccurlyeq q)$ occurs both on the top level and under a modality, and in a first step using monotonicity of $\preccurlyeq$ in the second argument convert the two axioms into $\frac{p \Rightarrow \quad q \Rightarrow r \preccurlyeq s}{\Rightarrow p \preccurlyeq q, r \preccurlyeq s}$ and $\frac{p \Rightarrow \quad r \preccurlyeq s, q \Rightarrow}{r \preccurlyeq s \Rightarrow p \preccurlyeq q}$. Now computing a principal cut between the first of these rules and a rule $R_{n,m}$ effectively replaces one negative principal formula of $R_{n,m}$ with a positive contextual formula $r \preccurlyeq s$. Repeating this process we get arbitrarily many positive context formulae $r_k \preccurlyeq s_k$ and thus arrive at the context restriction $\langle \emptyset, \{r \preccurlyeq s\}\rangle$. Similarly, principal cuts with the second rule replace negative principal formulae of $R_{n,m}$ with negative contextual formulae $r \preccurlyeq s$, yielding the context restriction $C_{\mathbb{VA}} := \langle \{r \preccurlyeq s\}, \{r \preccurlyeq s\}\rangle$. As usual, since all the cuts involved were cuts on principal formulae, Lemma 9 guarantees soundness of the resulting rule set. Setting $\mathcal{R}_{\mathbb{VA}} = \{R'_{n,m} \mid n \geq 1, m \geq 0\}$ with $R'_{n,m}$ given as $(\ \{(s_k \Rightarrow r_1, \dots, r_n, q_1, \dots, q_m; C_{\mathbb{VA}}) \mid k \leq n\} \cup \{(p_k \Rightarrow r_1, \dots, r_n, q_1, \dots, q_{k-1}; C_{\mathbb{VA}}) \mid k \leq m\};\ p_1 \preccurlyeq q_1, \dots, p_m \preccurlyeq q_m \Rightarrow r_1 \preccurlyeq s_1, \dots, r_n \preccurlyeq s_n\ )$ thus gives a sound and complete rule set for $\mathbb{VA}$, which is easily checked to be saturated and thus cut-free. As far as we are aware this rule set is new. This yields the following Theorem.

Theorem 32. *The rule set* $\mathsf{G}\mathcal{R}_{\mathbb{VA}}\mathsf{ConCut}$ *is sound and complete for* $\mathbb{VA}$*. Moreover, it is saturated and therefore has cut elimination. Since* $\mathcal{R}_{\mathbb{VA}}$ *is tractable, derivability in this system can be checked in* EXPTIME.

5 Conclusion

We presented a generic cut elimination result for symmetric and asymmetric sequent systems consisting of rules with context restrictions which are saturated, i.e. closed under cuts and contractions. This not only extends previous methods to modal axioms of nesting depth greater than one, but also to logics based on intuitionistic logic. Furthermore, we introduced techniques to translate axioms of a Hilbert style system into sequent rules. All the results and techniques are easily adapted to other base logics such as minimal or distributive logic. Examples included the reconstruction of already known sequent systems for constructive modal logics and the construction of an apparently new sequent system for Lewis' conditional logic $\mathbb{VA}$ in the entrenchment language.

References

1. Abadi, M.: Variations in Access Control Logic. In: van der Meyden, R., van der Torre, L. (eds.) DEON 2008. LNCS (LNAI), vol. 5076, pp. 96–109. Springer, Heidelberg (2008)
2. Alechina, N., Mendler, M., de Paiva, V., Ritter, E.: Categorical and Kripke Semantics for Constructive S4 Modal Logic. In: Fribourg, L. (ed.) CSL 2001 and EACSL 2001. LNCS, vol. 2142, pp. 292–307. Springer, Heidelberg (2001)
3. Avron, A., Lahav, O.: Kripke Semantics for Basic Sequent Systems. In: Brünnler, K., Metcalfe, G. (eds.) TABLEAUX 2011. LNCS (LNAI), vol. 6793, pp. 43–57. Springer, Heidelberg (2011)
4. Bellin, G., de Paiva, V., Ritter, E.: Extended Curry-Howard correspondence for a basic contructive modal logic. In: Areces, C., de Rijke, M. (eds.) M4M-2. ILLC Amsterdam (2001)
5. Benton, P., Bierman, G., de Paiva, V.: Computational types from a logical perspective. J. Funct. Programming 8(2), 177–193 (1998)
6. Ciabattoni, A., Galatos, N., Terui, K.: From axioms to analytic rules in nonclassical logics. In: LICS 2008, pp. 229–240. IEEE Computer Society (2008)
7. Fairtlough, M., Mendler, M.: Propositional lax logic. Inform. and Comput. 137(1), 1–33 (1997)
8. Gentzen, G.: Untersuchungen über das logische Schließen. I. Math. Z. 39(2), 176–210 (1934)
9. Johansson, I.: Der Minimalkalkül, ein reduzierter intuitionistischer Formalismus. Compos. Math. 4, 119–136 (1937)
10. Lellmann, B., Pattinson, D.: Cut Elimination for Shallow Modal Logics. In: Brünnler, K., Metcalfe, G. (eds.) TABLEAUX 2011. LNCS, vol. 6793, pp. 211–225. Springer, Heidelberg (2011)
11. Lellmann, B., Pattinson, D.: Sequent Systems for Lewis' Conditional Logics. In: del Cerro, L.F., Herzig, A., Mengin, J. (eds.) JELIA 2012. LNCS, vol. 7519, pp. 320–332. Springer, Heidelberg (2012)
12. Lewis, D.: Counterfactuals. Blackwell (1973)
13. Mendler, M., Scheele, S.: Cut-free Gentzen calculus for multimodal CK. Inform. and Comput. 209, 1465–1490 (2011)
14. Negri, S.: Proof analysis in modal logic. J. Philos. Logic 34, 507–544 (2005)

15. Negri, S., von Plato, J.: Structural proof theory. Cambridge University Press (2001)
16. Pattinson, D., Schröder, L.: Generic modal cut elimination applied to conditional logics. Log. Methods Comput. Sci. 7(1) (2011)
17. Pfenning, F., Davies, R.: A judgmental reconstruction of modal logic. Math. Structures Comput. Sci. 11(4), 511–540 (2001)
18. Troelstra, A.S., Schwichtenberg, H.: Basic Proof Theory, 2nd edn. Cambridge Tracts Theoret. Comput. Sci. Cambridge University Press (2000)
19. Wansing, H.: Sequent systems for modal logics. In: Gabbay, D.M., Guenthner, F. (eds.) Handbook of Philosophical Logic, vol. 8. Springer (2002)

Cut Elimination for Gentzen's Sequent Calculus with Equality and Logic of Partial Terms

Franco Parlamento[1] and Flavio Previale[2,⋆]

[1] Department of Mathematics and Computer Science
University of Udine, via Delle Scienze 206, 33100 Udine, Italy
`franco.parlamento@uniud.it`
[2] University of Turin, via Carlo Alberto 10, 10123 Torino, Italy

Abstract. We provide a natural formulation of the sequent calculus with equality and establish the cut elimination theorem. We also briefly outline and comment on its application to the logic of partial terms, when "existence" is formulated as equality with a (bound) variable.

Keywords: Sequent Calculus, Equality, Cut Elimination.

1 Introduction

The usual sequent calculus formulations of the predicate calculus with equality (no matter whether classical or intuitionistic) suggested by its, probably better known, formulations as axiomatic systems, which include the axiom $\forall x(x = x)$ and the axiom schema $\forall(x = y \to (F\{v/x\} \to F\{v/y\}))$, satisfy the cut elimination theorem only for cut-formulae which do not contain equalities[1]. See [13] and [14] for example. As part of a broader program of absorbing (mathematical) axioms into rules, while preserving cut eliminability, [7] introduces a structural rule free sequent calculus with equality for which the full cut elimination theorem holds. We will show that a similar result can be obtained by extending Gentzen's original systems with very natural rules not covered by the general schema adopted in [7], which leads to rules with active formulae in the antecedent of a sequent only. We will focus attention on the systems in Gentzen's celebrated "Untersuchungen" [12], which have the $\forall \Rightarrow$ and $\Rightarrow \exists$ rules restricted to variable, rather than arbitrary terms, as they are now commonly understood, when the notation LJ and LK are used[2]. However it will be clear that our treatment and results apply to the extended systems as well. We will denote by L and L^c the current versions of LJ and LK, with the exception that the restricted forms of

---

[⋆] Work supported by funds PRIN-/MIUR of Italy. The authors are grateful to the referees for helpful comments and suggestions.

[1] More precisely, every derivation in such systems can be transformed into one which contains only *inessential cuts*, namely cuts on equalities.

[2] It is only in his subsequent " Die Widerspruchsfreiheit der reinen Zahlentheorie", namely in a context in which all terms are denoting, that Gentzen introduces the extended version of the $\forall \Rightarrow$ and $\Rightarrow \exists$ rules.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 161–172, 2013.

$\forall \Rightarrow$ and $\Rightarrow \exists$ are adopted. A specific motivation to take $L^{=}$ and $L^{c=}$ as basic systems is that it is on their ground, as we will show in a sequel to the present work, that one can develop a satisfactory proof theoretic analysis of partial logic, with *existence* of a reference for a term t expressed by $\exists x(t = x)$, as originally suggested in [5] and [3], in agreement with Quine's Thesis.[3] As we will show it will suffice to add to L and L^c the reflexivity axiom $RFL : \ \Rightarrow t = t$, and the following right *congruence* rule CNG:

$$\frac{\Gamma \Rightarrow F\{v/r\} \quad \Gamma \Rightarrow r = s}{\Gamma \Rightarrow F\{v/s\}}$$

to have adequate sequent calculi $L^{=}$ and $L^{c=}$, for which the cut elimination theorem holds in full generality[4]. While RFL can be considered as a rule which introduces $=$ on the right side of a sequent, such calculi lack a rule which introduces $=$ on the left side. Actually CNG is more of a natural deduction style rule in that, as all the current natural deduction rules, when formulated in the sequent calculus format, it does not introduce a logical constant in the antecedent. A rule which is more in tune with those in L, is the following monic version CNG_M of CNG, which does introduce $=$ on the left:

$$\frac{\Gamma \Rightarrow F\{v/r\}}{\Gamma, r = s \Rightarrow F\{v/s\}}$$

However the following left symmetry rule SYM^L :

$$\frac{\Gamma, r = s \Rightarrow \Delta}{\Gamma, s = r \Rightarrow \Delta}$$

basic to our proof-theoretic analysis, is not admissible in the cut-free part of the systems obtained by adding CNG_M to L or L^c. Thus to have systems for which cut elimination holds we have to add to L or L^c, besides CNG_M, also SYM^L. We will denote by $L^{=}_M$ and $L^{c=}_M$ the systems so obtained. If in $L^{c=}_M$ the rule $\forall \Rightarrow$ and $\Rightarrow \exists$ are extended to arbitrary terms, we obtain a system which is related, actually equivalent, to the system G^e introduced in [6], in its turn inspired by [4].[5] We will prove the cut elimination theorem for $L^{=}_M$ and $L^{c=}_M$ by using in a crucial way the admissibility of CNG in such systems, and then we will transfer the result to the systems $L^{=}$ and $L^{c=}$. In the extended case, the result can be transfered to the system G^e as well, since CNG is a special case of the rule R_2 of G^e and SYM^L is easily seen to be admissible in the cut free part of G^e.

---

[3] So christened in [3] and expressed by Quine's dictum from [10] "to be is to be the value of a variable".

[4] We use the term *congruence rule* to avoid confusion with the substitution rule, which leads from $\Gamma \Rightarrow \Delta$ to $\Gamma\{v/t\} \Rightarrow \Delta\{v/t\}$. The congruence rule for function and relation symbols, leading from $\Gamma \Rightarrow r = s$ to $\Gamma \Rightarrow fr = fs$ and to $\Gamma, Rr \Rightarrow Rs$ respectively, are easily derivable from RFL and CNG.

[5] [6] announces a proof of cut elimination for G^e to be published as part II of the work, but apparently such a part II has never appeared in print.

The overall strategy is to reduce the cut elimination problem, as well as other significant proof-theoretic properties, for the full systems to the same problem for their purely equational part, which is common to the intuitionistic and classical systems. Once the results, obtained for the equational systems, are extended to $L^=$, they become instrumental in giving a syntactic proof of the conservativity of the addition of partial selection functions in the framework of $L^=$, supplemented by the assumption of the *determinateness* of equality, expressed by the axiom $\Rightarrow \forall x \forall y(x = y \vee x \neq y)$. No such extension is needed as far as the conservativity of the addition of partial description functions is concerned[6].

The above treatment of partial logic relies on the adoption of RFL and CNG, which concerns arbitrary terms. We believe that has well grounded motivations. If it appears reasonable to assume as logical an equality like $t = t$ even if t is a non denoting term, in a given context of course, that is expecially so when it comes to the development of the mathematical discourse. Think for example of the identity $1-2 = 1-2$ or the congruence $1+1 = 2 \rightarrow (1+1)-3 = 2-3$ when integers are not (yet) around. A different view is usually taken, (see [11], [14], [1] and [2]), when the *existence* predicate, which, applied to a term t, means that t is a denoting term, is taken as primitive. In that connection a "strict" equality $=$ is introduced with the intended meaning: $r = s$ if and only if r and s are both defined and are equal, together with a "lax" equality $\cong$ with the intended meaning: $r \cong s$ if and only if, r is defined if and only if s is defined, and if they are both defined, then they are equal, which identifies all non denoting terms, like $1-2$ and $1-3$ in the positive integers, thus conflicting with the introduction of the negative ones. On that respect it is of particular interest to note that the restriction of RFL to variables only and of CNG to the case in which one at least among r and s is a variable, together with the addition of the left symmetry rule, with the same restriction, yield systems which appear to be particularly well motivated, when dealing with terms which need not be denoting. As it can be shown that the full systems, with the reflectiom axioms and congruence rules extended to arbitrary terms, are conservative extensions of the ones so obtained, as far as equalities between a term and a variable are concerned, the former systems seem to appropriately formalize the logic surrounding Quine's Thesis. However the content of this paper will be limited to the proof of the cut elimination theorem and to a few of its more immediate applications.

2 The Systems $L^=$ and $L^{c=}$

Given any terms t and s and variable x, $t\{x/s\}$ denotes the term obtained from t by replacing all occurences of x by s. Similarly $F\{x/t\}$ denotes the formula obtained from F by replacing all the free occurrences of x by t. $L^=$ and $L^{c=}$ are obtained from (the current version of) the Gentzen's sequent calculi LJ and LK by restricting the right $\forall$- introduction rule and the left $\exists$-introduction rule to the following form:

---

[6] For the classical case a semantic proof using truth-value semantics can be found in [9].

$$\frac{\Gamma, F\{x/y\} \Rightarrow \Delta}{\Gamma, \forall x F \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \Delta, F\{x/y\}}{\Gamma \Rightarrow \Delta, \exists x F}$$

and adding the RFL axiom: $\Rightarrow t = t$ and the following congruence rule CNG:

$$\frac{\Gamma \Rightarrow \Delta, F\{v/r\} \quad \Gamma \Rightarrow \Delta, r = s}{\Gamma \Rightarrow \Delta, F\{v/s\}}$$

with the appropriate restrictions on $|\Delta|$ for $L^=$, namely $|\Delta| \leq 1$ in the former two rules and $\Delta = \emptyset$ in CNG. $F\{v/s\}$ is said to be the *principal formula* of the displayed congruence rule.

3 The Systems $L^=_M$ and $L^{c=}_M$

$L^=_M$ and $L^{c=}_M$ are obtained from $L^=$ and $L^{c=}$ by replacing CNG with the following rule CNG_M:

$$\frac{\Gamma \Rightarrow \Delta, F\{v/r\}}{\Gamma, r = s \Rightarrow \Delta, F\{v/s\}}$$

and by adding the following left symmetry rule SYM^L:

$$\frac{\Gamma, r = s \Rightarrow \Delta}{\Gamma, s = r \Rightarrow \Delta}$$

with the restrictions $|\Delta| \leq 1$ for $L^=_M$.

4 Reduction of the Congruence Rules to Atomic Formulae

An atomic formula is either an equality $r = s$ or a formula of the form $p(t_1, \ldots, t_n)$, for some n-ary relation symbol p and n-tuple of terms $t_1, \ldots, t_n$.

Proposition 1. *In $L^=$, and $L^{c=}$ the rule CNG is derivable from its restriction to atomic principal formulae. Similarly for $L^=_M$ and $L^{c=}_M$*

Proof. By induction on the complexity of formulae, using the cut rule. □

Warning. In view of the previous proposition we will henceforth refer exclusively to the restriction of CNG and CNG_M to atomic principal formulae, but maintain the notations $L^=, L^{c=}, L^=_M$ and $L^{c=}_M$ for the resulting systems.

5 Reduction of the Cut Rule to Atomic Cut Formulae

In the following S will indicate any of the previously introduced systems and $cf.S$ the system obtained by leaving out the cut rule from S.

Proposition 2. *Every derivation in S can be transformed into a derivation having only* atomic cuts*, namely cuts whose cut formula is atomic.*

Proof. It suffices to apply Gentzen's original argument, to show that if a mix inference has a mix formula which is non atomic, then it can be either eliminated, or reduced to mix inferences on formulae of lower height, or moved upward, treating the case in which one of the two subderivations ends with a *CNG*-inference as if it were a logical inference. □

6 Separated Derivations

Definition 1. *Logical axioms are those of the form $F \Rightarrow F$. They are said to be atomic if F is atomic. A derivation is said to be* separated *if its logical axioms, and cuts are atomic and no logical inference precedes some cut or congruence inference.*

Notation. $\Gamma\sharp A$ will denote any sequence of the form $\Gamma^{(1)}, \dots A, \Gamma^{(n-1)}, A, \Gamma^{(n)}$ such that Γ coincides with $\Gamma^{(1)}, \dots, \Gamma^{(n-1)}, \Gamma^{(n)}$. In other words, $\Gamma\sharp A$ denotes any sequence of formulae from which Γ can be obtained by erasing occurences of A.

Proposition 3. *Every derivation in S can be transformed into a separated derivation of the same end-sequent.*

Proof. Axioms can be reduced to their atomic form (without using the cut rule). Atomic cut and congruence inferences can be either eliminated or moved upward through any application of the logical rules. In more detail, one shows that if $\Gamma \Rightarrow \Delta_1\sharp A$ and $\Lambda\sharp A \Rightarrow \Delta_2$ have separated derivations, then also $\Gamma, \Lambda \Rightarrow \Delta_1, \Delta_2$, has a separated derivation, and that if $\Gamma \Rightarrow \Delta_1\sharp F\{v/r\}$ and $\Lambda \Rightarrow \Delta_1\sharp\ r = s$ have separated derivations, then also $\Gamma, \Lambda \Rightarrow \Delta_1.\Delta_2, F\{v/s\}$ has a separated derivation. The claim then follows by an easy induction on the height of derivations. □

Note 1. The argument works unchanged also for the extended version of the $\forall \Rightarrow$ and the $\Rightarrow \exists$ rules.[7]

---

[7] That one can make the congruence inferences precede the logical inferences in the system $cf.G^e$, denoted there by G_1^e, was noted in [6].

7 Cut Elimination for the Purely Equational Systems $\boldsymbol{EQ}$ and $\boldsymbol{EQ_M}$

Thanks to the previous proposition, cut elimination for S follows from cut elimination for the purely equational subsystem of S, which retains only the axioms, the structural rules and the congruence rule of S, to be denoted with EQ in case S is $L^=$ or $L^{c=}$ and with EQ_M in case S is $L^=_M$ or $L^{c=}_M$. We can therefore turn our attention to EQ and EQ_M. The equational subsystems do not depend on whether the system is classical or intuitionistic, despite the fact that, since classical logic is subsumed by the use of sequents with more than one formula in the consequent, the equational subsystems of $L^{c=}$ and $L^{c=}_M$ would also refer to such generalized sequents. However they can be referred to the simple sequents framework without any loss, as shown by the following fact.

Proposition 4. *$\Gamma \Rightarrow \Delta$ is derivable in EQ (EQ$_M$) if and only if for some D in Δ, there is a derivation of $\Gamma \Rightarrow D$ in EQ (EQ$_M$), which contains only sequents with exactly one formula in the consequent. In particular if $\Gamma \Rightarrow \Delta$ is derivable in EQ (EQ$_M$), then Δ cannot be empty!*

Proof. By induction on the height of a derivation of $\Gamma \Rightarrow \Delta$. In the base case $\Gamma \Rightarrow \Delta$ reduces to an axiom and the claim is obvious, since axioms have either the form $D \Rightarrow D$ or $\Rightarrow D$. Coming to the inductive step, if, for example, $\Gamma \Rightarrow \Delta$ has the form $\Gamma \Rightarrow \Delta^-, F\{v/s\}$ and is obtained by a CNG-inference from $\Gamma \Rightarrow \Delta^-, F\{v/r\}$ and $\Gamma \Rightarrow \Delta^-, r = s$, then by induction hypothesis either there is a formula D in Δ^-, hence also in Δ, such that $\Gamma \Rightarrow D$ has a derivation with the desired property, or both $\Gamma \Rightarrow F\{v/r\}$ and $\Gamma \Rightarrow r = s$ have such derivations. In the latter case it suffices to apply a CNG-inference to establish the claim with $F\{v/s\}$ taken as D. □

Warning. From now on we will therefore assume that EQ and EQ_M are sequent calculi dealing with sequents in which all formulae are atomic and there is at most one formula in the consequent.

7.1 Admissibility of $\boldsymbol{CNG}$ in $\boldsymbol{EQ_M}$

Let SYM denote the following right symmetry rule:

$$\frac{\Gamma \Rightarrow r = s}{\Gamma \Rightarrow s = r}$$

Lemma 1. *SYM is admissible in cf.EQ$_M$*

Proof. By induction on the height of a derivations $\mathcal{D}$ of $\Gamma \Rightarrow r = s$. In the base case, either $\Gamma = \emptyset$ and r coincides with s or Γ is $r = s$. In the former case the conclusion is trivial, in the latter we note that the following is a derivation of $\Gamma \Rightarrow s = r$, namely of $r = s \Rightarrow s = r$:

$$\frac{\Rightarrow r = r}{r = s \Rightarrow s = r}$$

As for the inductive step, the only non trivial case occurs when $\mathcal{D}$ has the form:

$$\frac{\begin{array}{c}\mathcal{D}_0\\ \Gamma \Rightarrow r^\circ\{v/p\} = s^\circ\{v/p\}\end{array}}{\Gamma, p = q \Rightarrow r^\circ\{v/q\} = s^\circ\{v/q\}}$$

By inductive hypothesis applied to $\mathcal{D}_0$, $\Gamma \Rightarrow s^\circ\{v/p\} = r^\circ\{v/p\}$ is derivable in $cf.EQ$, from which, thanks to a CNG_M-inference, it follows that also $\Gamma, p = q \Rightarrow s^\circ\{v/p\} = r^\circ\{v/p\}$ is derivable in $cf.EQ_M$. □

Let CNG^L_M denote the following left congruence rule:

$$\frac{\Gamma, F\{v/r\} \Rightarrow D}{\Gamma, F\{v/s\}, r = s \Rightarrow D}$$

Lemma 2. *The rule CNG^L_M is admissible in $cf.EQ_M$*

Proof. Due to the presence of the rules of contraction and exchange we have to prove the following more general statement: if a sequent of the form

$$\Gamma \sharp F\{v/r\} \Rightarrow D$$

is cut free derivable in EQ_M, then also the sequent $\Gamma, F\{v/s\}, r = s \Rightarrow D$ is cut free derivable in EQ_M. The proof is by induction on the height of a given derivation $\mathcal{D}$ of $\Gamma \sharp F\{v/r\} \Rightarrow D$. If $\mathcal{D}$ consists of a single axiom, we can assume that it is of the form $F\{v/r\} \Rightarrow F\{v/r\}$, and the claim is proved by considering the following derivation:

$$SYM^L\ \cfrac{CNG^L_M\ \cfrac{F\{v/s\} \Rightarrow F\{v/s\}}{F\{v/s\}, s = r \Rightarrow F\{v/r\}}}{F\{v/s\}, r = s \Rightarrow F\{v/r\}}$$

If $\mathcal{D}$ ends with a proper inference, the less trivial case occurs when $\mathcal{D}$ ends with a CNG_M-inference which introduces on the left the formula $F\{v/r\}$, which is therefore an equality, say $p\{v/r\} = q\{v/r\}$. In this case D is of the form $G\{u/q\{v/r\}\}$, and the premiss of the last inference of $\mathcal{D}$ is of the form $\Gamma \sharp p\{v/r\} = q\{v/r\} \Rightarrow G\{u/p\{v/r\}\}$. We have to prove that $\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/q\{v/r\}\}$ is derivable in $cf.EQ_M$. By inductive hypothesis $\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/p\{v/r\}\}$ is derivable in $cf.EQ_M$. Then the desired derivation can be obtained by applying the following further inferences (which subsumes the appropriate exchanges and contractions):

$$SYM^L\ \cfrac{CNG^L_M\ \cfrac{CNG^L_M\ \cfrac{CNG^L_M\ \cfrac{\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/p\{v/r\}\}}{\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/p\{v/s\}\}}}{\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/q\{v/s\}\}}}{\Gamma, p\{v/s\} = q\{v/s\}, r = s, s = r \Rightarrow G\{u/q\{v/r\}\}}}{\Gamma, p\{v/s\} = q\{v/s\}, r = s \Rightarrow G\{u/q\{v/r\}\}}$$

.

□

Note 2. A somewhat simpler argument shows that also the following CNG^L rule:

$$\frac{\Gamma, F\{v/r\} \Rightarrow D \quad \Gamma \Rightarrow r = s}{\Gamma, F\{v/s\} \Rightarrow D}$$

is admissibile in $cf.EQ$. Notice that CNG^L_M and CNG^L are derivable, by means of the cut rule, in EQ_M and EQ respectively

A further, quite useful, reduction, already exploited in [6], that one can make regarding the congruence rules, is expressed in the following definition and property.

Definition 2. *An application*

$$\frac{\Gamma \Rightarrow F\{v/r\}}{\Gamma, r = s \Rightarrow F\{v/s\}}$$

of CNG_M is said to be singular *if F has exactly one free occurrence of v.*

Lemma 3. *CNG_M is derivable by singular applications of CNG_M.*

Lemma 4. *If the sequent $\Lambda \Rightarrow r = s$ is derivable in $cf.EQ_M$, then, for any formula F, also the sequent $\Lambda, F\{v/r\} \Rightarrow F\{v/s\}$ is derivable in the same system.*

Proof. We proceed by induction on the height of a cut-free derivation $\mathcal{D}$ of $\Lambda \Rightarrow r = s$. If $\mathcal{D}$ consists of a single axiom, we have the following two possibilities:

a) $\mathcal{D}$ consists of the RFL axiom $\Rightarrow r = r$, so that Λ is empty and s coincides with r,

b) $\mathcal{D}$ consists of the logical axiom $r = s \Rightarrow r = s$, so that Λ is $r = s$.

In case *a*) the assertion is trivial, since $\Lambda, F\{v/r\} \Rightarrow F\{v/s\}$ is the logical axiom $F\{v/r\} \Rightarrow F\{v/r\}$. In case *b*) the assertion is proved by the following derivation:

$$CNG^L_M \; \frac{F\{v/r\} \Rightarrow F\{v/r\}}{r = s, F\{v/r\} \Rightarrow F\{v/s\}}$$

As for the inductive step, the only non trivial case occurs when $\mathcal{D}$ ends with a CNG_M-inference of the form:

$$\frac{\Lambda^- \Rightarrow r^\circ\{u/p\} = s^\circ\{u/p\}}{\Lambda^-, p = q \Rightarrow r^\circ\{u/q\} = s^\circ\{u/q\}}$$

so that Λ is $\Lambda^-, p = q$, r is $r^\circ\{u/q\}$, s is $s^\circ\{u/q\}$. By the inductive hypothesis, $\Lambda^-, F\{v/r^\circ\{u/p\}\} \Rightarrow F\{v/s^\circ\{u/p\}\}$ is cut-free derivable. Such a derivation can be prolonged into a cut-free derivation of the desired sequent as follows:

$$\begin{array}{ll} CNG_M & \dfrac{\Lambda^-, F\{v/r^\circ\{u/p\}\} \Rightarrow F\{v/s^\circ\{u/p\}\}}{\Lambda^-, F\{v/r^\circ\{u/p\}\}, p = q \Rightarrow F\{v/s^\circ\{u/q\}\}} \\ CNG^L_M & \dfrac{}{\Lambda^-, F\{v/r^\circ\{u/q\}\}, p = q, p = q \Rightarrow F\{v/s^\circ\{u/q\}\}} \\ & \overline{\Lambda^-, p = q, F\{v/r^\circ\{u/q\}\} \Rightarrow F\{v/s^\circ\{u/q\}\}} \end{array}$$

which uses CNG^L_M. The conclusion follows by the admissibility of CNG^L in $cf.EQ_M$ given by Lemma 2 □

Theorem 1. *CNG is admissible in $cf.EQ_M$*

Proof. By Lemma 3, it suffices to show the result for the singular versions of the rules with respect to the singular version of the corresponding cut-free system. Furthermore it is convenient to deal with the non context sharing version of those rules. Thus we have to prove that if two sequents $\Gamma \Rightarrow F\{v/r\}$ and $\Lambda \Rightarrow r = s$ are cut free derivable in the singular version of $cf.EQ_M$, and v has a single free occurrence in F, then also the sequent $\Gamma, \Lambda \Rightarrow F\{v/s\}$ is cut-free derivable in EQ_M. We proceed by induction on the height of a cut-free derivation $\mathcal{D}$ of $\Gamma \Rightarrow F\{v/r\}$, associated with an arbitrary cut-free derivation of $\Gamma \Rightarrow r = s$.

If $\mathcal{D}$ consists of a single axiom, we have the following possibilities:

a) $\mathcal{D}$ consists of the single axiom $\Rightarrow r = r$, thus Γ is empty and $F\{v/r\}$ is $r = r$.

b) $\mathcal{D}$ consists of the single axiom $F\{v/r\} \Rightarrow F\{v/r\}$, thus Γ is $F\{v/r\}$.

In case *a*), since, in F, v has a single occurrence, F itself can have one of the following forms: $r = v, v = r$, (v not in r), so that $F\{v/s\}$ takes one of the two forms $r = s$, $s = r$. In the former case the conclusion holds since $\Lambda \Rightarrow r = s$ is assumed to be cut-free derivable. In the latter case it suffices to apply SYM, which is admissible by Lemma 1, to $\Lambda \Rightarrow r = s$. In case *b*) it suffices to apply the previous lemma.

As for the inductive step, the only non trivial case occurs when $\mathcal{D}$ ends with a CNG_M-inference:

$$\frac{\Gamma^- \Rightarrow G\{u/p\}}{\Gamma^-, p = q \Rightarrow G\{u/q\}}$$

so that Γ is $\Gamma^-, p = q$ and $F\{v/r\}$ is $G\{u/q\}$. Furthermore u, which has a unique free occurrence in G, can be assumed to be distinct from v, since $G\{u/q\}$ is the same as $G'\{u'/q\}$, where G' is obtained from G by replacing the occurrence of u, by a new variable u'. We have three possible cases.

1). The unique relevant occurrence of r and the unique relevant occurrence of q in the same formula $F\{v/r\}$, namely $G\{u/q\}$ do not overlap. Then we can write G as $G^\circ\{v/r\}$, $G\{u/p\}$ as $G^\circ\{v/r, u/p\}$ and $G\{u/q\}$ as $G^\circ\{v/r, u/q\}$. Since $\Lambda \Rightarrow r = s$ is cut-free derivable and $\Gamma^- \Rightarrow G^\circ\{v/r, u/p\}$ admits a cut-free derivation in EQ_M with height less than the height of $\mathcal{D}$, by inductive hypothesis, $\Gamma^- \Rightarrow G^\circ\{v/s, u/p\}$ admits a cut-free derivation in EQ_M. By an application of a final CNG_M to such a derivation we obtain a cut-free derivation of $\Gamma^-, p = q \Rightarrow G^\circ\{v/s, u/q\}$, as desired, since its succedent coincides with $F\{v/s\}$.

2) The unique relevant occurrence of r is a part of the unique relevant occurrence of q (we do not exclude that the two coincide). Then q can be written as $q^\circ\{v/r\}$ and v does not occur in G. Thus F coincides with $G\{u/q^\circ\}$ and $F\{v/r\}$ with $G\{u/q^\circ\{v/r\}\}$. Since $\Lambda \Rightarrow r = s$ is cut-free derivable in EQ_M, by the previous lemma, $\Lambda, p = q^\circ\{v/r\} \Rightarrow p = q^\circ\{v/s\}$ is cut-free derivable in EQ_M as well. Therefore by the inductive hypothesis, $\Gamma^-, \Lambda, p = q^\circ\{v/r\} \Rightarrow G\{u/q^\circ\{v/s\}\}$, namely $\Gamma^-, \Lambda, p = q \Rightarrow F\{v/s\}$ is cut-free derivable, as we had to show.

3) 1) and 2) do not apply. Then the unique relevant occurrence of q is a proper part of the unique relevant occurrence of r. Thus r can be written as $r^\circ\{u/q\}$ and u does not occur free in F. Therefore G coincides with $F\{v/r^\circ\}$ and, for evey term t, $G\{u/t\}$ coincides with $F\{v/r^\circ\{u/t\}\}$. By assumption $\Lambda \Rightarrow r^\circ\{u/q\} = s$ has a cut-free derivation. By applying CNG_M and SYM^L to a cut-free derivation of $\Lambda \Rightarrow r^\circ\{u/q\} = s$ we obtain a cut-free derivation of $\Lambda, p = q \Rightarrow r^\circ\{u/p\} = s$. Therefore, by the inductive hypothesis applied to such a sequent and to the cut-free derivable sequent $\Gamma^- \Rightarrow F\{v/r^\circ\{u/p\}\}$, it follows that also $\Gamma^-, \Lambda, p = q \Rightarrow F\{v/s\}$ is cut-free derivable in EQ_M. □

7.2 Cut Elimination for $\boldsymbol{EQ_M}$

Theorem 2. *The cut rule is admissible in* $cf.EQ_M$*, equivalently, if* $\Gamma \Rightarrow D$ *is derivable in* EQ_M*, then* $\Gamma \Rightarrow D$ *is derivable in* $cf.EQ_M$*. Briefly stated: cut eliminability holds for* EQ_M*.*

Proof. We prove the following more general result: If $\Gamma \Rightarrow A$ and $\Lambda \sharp A \Rightarrow D$ are derivable in $cf.EQ_M$, then also the sequent $\Gamma, \Lambda \Rightarrow D$ is derivable in cf, EQ_M. The proof is by induction on the height of a cut-free derivation $\mathcal{D}$ of $\Lambda \sharp A \Rightarrow D$. In the base case $\mathcal{D}$ necessarily consists of a single logical axiom $A \Rightarrow A$ and our claim trivially follows from the assumption that $\Lambda \Rightarrow A$ is derivale in $cf.EQ_M$. As for the inductive step, the only non trivial case occurs when $\mathcal{D}$ ends with a CNG_M-inference which introduces A on the left, so that A has the form $r = s$, D has the form $G\{v/s\}$ and the premiss of the last CNG_M-inference of $\mathcal{D}$ has the form $\Lambda \sharp r = s \Rightarrow G\{v/r\}$. By induction hypothesis $\Gamma, \Lambda \Rightarrow G\{v/r\}$ is derivable in $cf.EQ_M$. Since $\Gamma \Rightarrow r = s$, is also assumed to be derivable in $cf.EQ_M$, also $\Gamma, \Lambda \Rightarrow r = s$ is derivable in $cf.EQ_M$. Therefore by the admissibility of CNG in $cf.EQ_M$, given by Theorem 1, the sequent $\Gamma, \Lambda \Rightarrow D$ is derivable in $cf.EQ_M$, as we had to prove. □

Note 3. The admissibility of CNG for $cf.EQ_M$ is essential for the proof.

Lemma 5. SYM^L *is admissible in* $cf.EQ$

Proof. By induction on the height of a derivation $\mathcal{D}$ of $\Gamma \sharp r = s \Rightarrow D$ in $cf.EQ$. In the base case $\Gamma \sharp r = s \Rightarrow D$ reduces to the logical axiom $r = s \Rightarrow r = s$. Then it suffices to note that the following is a derivation in $cf.EQ$ of $s = r \Rightarrow r = s$:

$$\dfrac{CNG\ \dfrac{\Rightarrow s = s}{s = r \Rightarrow s = s} \qquad s = r \Rightarrow s = r}{s = r \Rightarrow r = s}$$

The inductive step is also very easy, and we omit the details. □

Corollary 1. *Cut eliminability holds for* EQ*.*

Proof. Since CNG is derivable (using a cut) from CNG_M, any derivation $\mathcal{D}$ in EQ can be transformed into a derivation $\mathcal{D}'$ of the same end-sequent in EQ_M.

By Theorem 2, cuts can be eliminated from $\mathcal{D}'$. Then, by using weakening and exchanges, the applications of CNG_M can be replaced by applications of CNG and finally, by the previous Lemma, the applications of SYM^L can be eliminated. □

7.3 Cut Elimination for the Full Systems

From the previous results we have the following:

Theorem 3. *Cut eliminability holds for* $L_M^=$, $L_M^{c=}$ *as well as for* $L^=$ *and* $L^{c=}$

Proof. By Theorem 3 every derivation can be tranformed into a derivation in which cut-inferences appear only in subderivations which belong to EQ or EQ_M. Then it suffices to apply Theorem 2, in the case of $L_M^=$ and $L_M^{c=}$, or Corollary 1, in the case of $L^=$ and $L^{c=}$, to obtain a cut free derivation. □

8 First Consequences of Cut Elimination

Proposition 5. *Conservatity of logic with equality over logic without equality*
If $=$ *does not occur in* Γ, Δ *and* $\Gamma \Rightarrow \Delta$ *is derivable in* $L^=$ *then* $\Gamma \Rightarrow \Delta$ *is derivable already in* L. *The same hols for* $L^{c=}$, $L_M^=$ *and* $L_M^{c=}$

Proof. Here we apply the cut elimination theorem for $L_M^=$ or $L_M^{c=}$. It suffices to observe that no rule of such systems, different from a cut, eliminates equalities. □

Note 4. For systems with rules which eliminate equalities, the proof may become more involved. For example, that is the case if the system, as the one in [7], has the left reflexivity rule, allowing the elimination of $t = t$ from the antecedent of a sequent, (see [8] pp. 139-141).

Given a sequence Γ of formulae, let $\Gamma_=$ be obtained from Γ by suppressing all the formulae in Γ which are not equalities. The following are easy corollary of Theorem 3.

Proposition 6. *Let* Γ *be a sequence of atomic formulae. Then*
$\Gamma \Rightarrow r = s$ *is derivable in* $L^=$ *if and only if* $\Gamma_= \Rightarrow r = s$ *is derivable in* $cf.EQ$. *The same holds for* $L^{c=}$.

Proposition 7. *Let* Γ *be a sequence of atomic formulae and* R *be an* n*-ary relation symbol different from* $=$. *Then* $\Gamma \Rightarrow Rs_1 \ldots s_n$ *is derivable in* $L^=$ *if and only if in* Γ *there is a formula* $Rr_1 \ldots r_n$ *such that for* $1 \leq i \leq n$, $\Gamma_= \Rightarrow r_i = s_i$ *has a cut-free derivation in* EQ. *The same holds for* $L^{c=}$.

Note 5. Letting $LJ^=$ and $LK^=$ differ from $L_M^=$ and $L_M^{c=}$ only for the adoption of $\forall \Rightarrow$ and $\Rightarrow \exists$ extended to arbitrary terms, we have that the last two properties hold for $LJ^=$ and $LK^=$ as well. In fact, as an immediate consequence of cut elimination, if Γ is a sequence of atomic formulae, then $\Gamma \Rightarrow r = s$ and $\Gamma \Rightarrow Rs_1 \ldots s_n$ are derivable in $LJ^=$ or in $LK^=$ if and only if they are derivable in EQ_M, equivalently in EQ.

References

1. Baaz, M., Iemhoff, M.R.: On the Proof Theory of the Existence Predicate We will show them! Essays in honour of Dov Gabbay, pp. 125–166. College Publication (2005)
2. Feferman, S.: Definedness. Erkenntnis 43, 295–329 (1995)
3. Hintikka, J.: Existential Presupposition and Existential Commitments. Journal of Philosophy 56, 125–137 (1959)
4. Kanger, S.: A Simplified Proof Method for Elementary Logic. In: Braffort, P., Hirshberg, D. (eds.) Computer Programming and Formal Systems, pp. 87–94. North-Holland, Amsterdam (1963)
5. Leblank, H., Hailperin, H.T.: Nondesignating Singulatr Terms. Philosophical Review 68, 239–243 (1959)
6. Lifschitz, A.V.: Specialization of the form of deduction in the predicate calculus with equality and function symbols. In: Orevkov, V.P. (ed.) The Calculi of Symbolic Logic. I, Proceedings of the Steklov Institute of Mathematics 98 (1971)
7. van Plato, J., Negri, S.: Cut Elimination in the Presence of Axioms. The Bulletin of Symbolic Logic 147, 418–435 (1998)
8. van Plato, J., Negri, S.: Structural Proof Theory. Cambridge University Press, Cambridge (2001)
9. Parlamento, F.: Truth-value semantics and functional extensions for classical logic of partial terms based on equality. ArXiv:1112.6331 (2011) (to appear in the Notre Dame J. of Form. Logic)
10. van Quine, W.O.: On What there is. Review of Metaphisics 2, 21–38 (1948)
11. Scott, D.S.: Identity and Existence in Intuitionistic Logic. In: Proc. Res. Symp. on Application of Sheaves 1977, Durham. Lect. Notes Math., vol. 763, pp. 660–696 (1979)
12. Szabo, M.E.: The Collected Papers of Gerhard Gentzen. North Holland, Amsterdam (1969)
13. Takeuti, G.: Proof Theory. Studies in Logic and the Foundations of Mathematics, vol. 81. North Holland, Amsterdam (1975)
14. Troelstra, A.S., Schwichtemberg, H.: Basic Proof Theory. Cambridge Tracts in Theoretical Computer Science, vol. 43. Cambridge University Press, Cambridge (1996)

Logic of Non-monotonic Interactive Proofs[⋆]

Simon Kramer

University of Luxembourg
`simon.kramer@a3.epfl.ch`

Abstract. We propose a monotonic logic of internalised *non-monotonic* or *instant* interactive proofs (LiiP) and reconstruct an existing monotonic logic of internalised monotonic or persistent interactive proofs (LiP) as a minimal conservative extension of LiiP. Instant interactive proofs effect a *fragile* epistemic impact in their intended communities of peer reviewers that consists in the *impermanent* induction of the knowledge of their proof goal by means of the knowledge of the proof with the interpreting reviewer: If my peer reviewer knew my proof then she would *at least then* know that its proof goal is true. Their impact is fragile and their induction of knowledge impermanent in the sense of being the case possibly only at the instant of learning the proof. This accounts for the important possibility of internalising proofs of statements whose truth value can vary, which, as opposed to invariant statements, cannot have persistent proofs. So instant interactive proofs effect a *temporary* transfer of certain propositional knowledge (knowable *ephemeral* facts) via the transmission of certain individual knowledge (knowable *non-monotonic* proofs) in distributed systems of multiple interacting agents.

Keywords: agents as proof- and signature-checkers, constructive Kripke-semantics, interpreted communication, multi-agent distributed systems, interactive and oracle computation, proofs as sufficient evidence.

1 Introduction

The subject matter of this paper is modal logic of interactive proofs, i.e., a novel logic of *non-monotonic* or *instant* interactive proofs (LiiP) [1] as well as an existing logic of monotonic or persistent interactive proofs (LiP) [2]. (We abbreviate interactivity-related adjectives with lower-case letters.) The goal here is to define LiiP axiomatically and semantically as well as to reconstruct LiP as a minimal conservative extension of LiiP. So for distributed and multi-agent systems, whose states and thus truth of statements about states can vary, proof non-monotonicity (as in LiiP) is in a logical sense more primitive than proof

---

[⋆] Work funded with Grant AFR 894328 from the National Research Fund Luxembourg cofunded under the Marie-Curie Actions of the European Commission (FP7-COFUND), and finalised during an invited stay at the Institute of Mathematical Sciences, Chennai, India.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 173–184, 2013.

monotonicity (as in LiP). In contrast, proof monotonicity is perhaps more intuitive than proof non-monotonicity within formal physical theories validated by experiment and surely within mathematical theories known to be consistent.

Rephrasing [3, Section 1.1] model-theoretically, the proof modality of LiiP internalises a non-monotonic notion of proof in the sense that it can happen that a proposition ϕ can be proved with a (non-monotonic) proof M to an agent a in some system state s, but not anymore in some subsequent state s' in which a will have learnt additional or lost previously learnt data M'. See [1] for formal application examples. Like in LiP [2], we understand interactive *proofs as sufficient evidence* to intended *resource-unbounded* (though unable to guess) proof- and signature-checking agents (designated verifiers).

Instant interactive proofs effect a *fragile* epistemic impact in their intended communities $\mathcal{C}$ of peer reviewers that consists in the *impermanent* induction of the (propositional) knowledge (not only belief) of their proof goal ϕ by means of the (individual) knowledge of the proof (the sufficient evidence) M with the designated interpreting reviewer a : If a knew my proof M of ϕ then she would *at least then* know that the proof goal ϕ is true. By individual knowledge we mean knowledge in the sense of the transitive use of the verb "to know," here to know a message, such as the plaintext of an encrypted message. Notation: $a \,\mathsf{k}\, M$ for "agent a knows message M" (cf. Definition 1). This is the classic concept of knowledge *de re* ("of a thing") made explicit for messages, meaning taking them apart (analysing) and putting them together (synthesising). Whereas by propositional knowledge we mean knowledge in the sense of the use of the verb "to know" with a clause, here to know that a statement is true, such as that the plaintext of an encrypted message is (individually) unknown to potential adversaries. Notation: $\mathsf{K}_a(\phi)$ for "agent a knows that ϕ (is true)" (cf. Fact 1). This is the classic concept of knowledge *de dicto* ("of a fact").[1] (We distinguish individual and propositional knowledge with respect to the *"object"* of knowledge [the know*n*], i.e., with respect to a message and clause, respectively. However, individual as well as propositional knowledge can both be individual with respect to the *subject* of knowledge [the know*er*], i.e., an [individual] agent.) With respect to belief, propositional knowledge essentially differs in that it is necessarily true whereas belief is possibly false, as commonly known and accepted [4]. The epistemic impact of our instant interactive proofs is fragile and their induction of knowledge impermanent in the sense of being the case possibly only at the instant of learning the proof. This accounts for the important possibility of internalising proofs of statements, whose truth value can vary, such as statements about system states, which, as opposed to invariant statements, cannot have persistent proofs. Proofs must (not) prove true (false) statements! Standard examples of statements of variable truth value are contingent (e.g., elementary) facts (expressed as atomic formulas) and characteristic formulas of states [5].

In contrast [2], the epistemic impact of *persistent* interactive proofs is *durable* in the sense of being the case necessarily at the instant of learning the proof *and henceforth*, where time can be present implicitly (such as here) or explicitly

---

[1] In a first-order setting, knowledge *de re* and *de dicto* can be related in Barcan-laws.

(in future work). In other words, when a persistent proof can prove a certain statement, the proof will always be able to *robustly* do so, independently of whether or not more messages (data) than just the proof are learnt.

In sum, our instant interactive proofs effect a transfer of propositional knowledge (knowable ephemeral facts) via the transmission of certain individual knowledge (knowable non-monotonic proofs) in multi-agent distributed systems. That is, *L(i)iP is a formal theory of (temporary) knowledge transfer.* The overarching motivation for L(i)iP is to serve in an intuitionistic foundation of interactive computation. See [2] for a programmatic and methodological motivation.

1.1 Contribution

Our technical contribution in this paper is fourfold. For LiiP, we provide an adequate axiomatisation of its oracle-computational and knowledge-constructive Kripke-semantics, and a minimal conservative extension LiiP^+ with a single monotonicity axiom schema making LiiP^+ isomorphic to LiP. For LiP, we provide a substantially simplified semantic interface and a slightly simplified axiomatisation, which is a nice side-effect of obtaining LiiP^+.

The Kripke-semantics for LiiP (like for LiP [2]) is knowledge-constructive in the sense that (cf. Fact 1) our interactive proofs induce the knowledge of their proof goal (say ϕ) in their intended interpreting agents (say a) such that the induced knowledge ($\mathsf{K}_a(\phi)$) is knowledge in the sense of the standard modal logic of knowledge S5 [6,4,7]. Note that our agents here are still resource-*un*bounded with respect to individual and propositional knowledge, though they are still unable to guess that knowledge. (Recall that S5-agents are resource-unbounded, i.e., logically omniscient.) Thus we give an epistemic explication of proofs, i.e., an explication of proofs in terms of the epistemic impact that they effect in their intended interpreting agents (i.e., the knowledge of their proof goal). Technically, we endow the proof modality with a standard Kripke-semantics [5], but whose accessibility relation ${}_M\mathcal{R}_a^{\mathcal{C}}$ we first define constructively in terms of elementary set-theoretic constructions, namely as ${}_M\mathrm{R}_a^{\mathcal{C}}$, and then match to an abstract semantic interface in standard form (which abstractly stipulates the characteristic properties of the accessibility relation [5]). We will say that ${}_M\mathrm{R}_a^{\mathcal{C}}$ *exemplifies* (or *realises*) ${}_M\mathcal{R}_a^{\mathcal{C}}$. (A simple example of a constructive definition of a modal accessibility is the well-known definition of epistemic accessibility as state indistinguishability defined in terms of equality of state projections [6].) Recall, set-theoretically constructive is different from intuitionistically constructive! The Kripke-semantics for LiiP is oracle-computational in the sense that (cf. Definition 3) the individual proof knowledge (say M) can be thought of as being provided by an imaginary computation oracle, which thus acts as a hypothetical provider and imaginary epistemic source of our interactive proofs. The semantic interface of LiP here is simplified in the sense that we are able to eliminate all *a posteriori* constraints from the semantic interface in [2] and thus to manage with only standard, *a priori* constraints, i.e., stipulations.

1.2 Roadmap

In the next section, we introduce our Logic of instant interactive Proofs (LiiP) axiomatically by means of a compact closure operator that induces the Hilbert-style proof system that we seek and that allows the simple generation of application-specific extensions of LiiP [1]. We then state some useful deducible laws within the obtained system. Next, we introduce the set-theoretically constructive semantics and the abstract semantic interface for LiiP, and state the axiomatic adequacy of the proof system with respect to this interface. (See [1] for formal proofs.) In the construction of the semantics, we again make use of a closure operator, but this time on sets of proof terms. Finally in Section 3, we reconstruct LiP as a minimal conservative extension of LiiP.

2 Logic of Instant Interactive Proofs

The Logic of instant interactive Proofs (LiiP) provides a modal *formula language* over a generic message *term language*. The formula language offers the propositional constructors, a relational symbol 'k' for constructing atomic propositions about individual knowledge (e.g., $a\,\mathsf{k}\,M$), and a modal constructor '$::$' for propositions about proofs (e.g., $M ::_a^{\mathcal{C}} \phi$). The message language offers term constructors for message *pairing* and (not necessarily, but possibly cryptographically implemented) *signing*. (Cryptographic signature creation and verification is polynomial-time computable [8]. See [2] for other cryptographic constructors such as encryption and hashing.) In brief, LiiP is a minimal modular extension of classical propositional logic with an interactively generalised additional operator (the proof modality) and proof-term language (only two constructors, *agents as proof- and signature-checkers*). Note, the language of LiiP is identical to the one of LiP [2] modulo the proof-modality notation, which in LiP is '$:$'.

Definition 1 (The language of LiiP). *Let*

- $\mathcal{A} \neq \emptyset$ *designate a non-empty finite set of* agent names *a, b, c, etc.*
- $\mathcal{C} \subseteq \mathcal{A}$ *denote (finite and not necessarily disjoint) communities (sets) of agents $a \in \mathcal{A}$ (referred to by their name)*
- $\mathcal{M} \ni M ::= a \mid B \mid \{\!\!\{M\}\!\!\}_a \mid (M, M)$ *designate our language of* message terms M over $\mathcal{A}$ *with (transmittable) agent names $a \in \mathcal{A}$, application-specific data B (left blank here), signed messages $\{\!\!\{M\}\!\!\}_a$, and message pairs (M, M) (Messages must be grammatically well-formed, which yields an induction principle. So agent names a are logical term constants, the meta-variable B just signals the possibility of an extended term language $\mathcal{M}$, $\{\!\!\{\cdot\}\!\!\}_a$ with $a \in \mathcal{A}$ is a unary functional symbol, and $(\cdot, \cdot)$ a binary functional symbol.)*
- $\mathcal{P}$ *designate a denumerable set of* propositional variables P *constrained such that for all $a \in \mathcal{A}$ and $M \in \mathcal{M}$, $(a\,\mathsf{k}\,M) \in \mathcal{P}$ (for "a knows M") is a distinguished variable, i.e., an* atomic proposition, *(for* individual *knowledge)*
  (So, for $a \in \mathcal{A}$, $a\,\mathsf{k}\,\cdot$ is a unary relational symbol.)

- $\mathcal{L} \ni \phi ::= P \mid \neg\phi \mid \phi\wedge\phi \mid M ::^{\mathcal{C}}_{a} \phi$ *designate our language of* logical formulas ϕ*, where* $M ::^{\mathcal{C}}_{a} \phi$ *reads "*M *is a* $\mathcal{C} \cup \{a\}$-reviewable proof *of* ϕ*" in that "*M *can prove* ϕ *to* a *(e.g., a designated verifying judge) and this is commonly accepted in the pointed community* $\mathcal{C} \cup \{a\}$ *(e.g., for* $\mathcal{C}$ *being a jury)."*

Then LiiP has the following axiom and deduction-rule schemas, with grey-shading indicating the difference to LiP.

Definition 2 (The axioms and deduction rules of LiiP). *Let*

- $\mathit{\Gamma}_0$ *designate an adequate set of axioms for classical propositional logic*
- $\mathit{\Gamma}_1 := \mathit{\Gamma}_0 \cup \{$
  - $a\,\mathsf{k}\,a$ *(knowledge of one's own name string)*
  - $a\,\mathsf{k}\,M \to a\,\mathsf{k}\,\{\![M]\!\}_a$ *(*personal *[the same a] signature* synthesis*)*
  - $a\,\mathsf{k}\,\{\![M]\!\}_b \to a\,\mathsf{k}\,(M, b)$ *(*universal *[any a and b] signature* analysis*)*
  - $(a\,\mathsf{k}\,M \wedge a\,\mathsf{k}\,M') \leftrightarrow a\,\mathsf{k}\,(M, M')$ *([un]pairing)*
  - $(M ::^{\mathcal{C}}_{a} (\phi \to \phi')) \to ((M ::^{\mathcal{C}}_{a} \phi) \to M ::^{\mathcal{C}}_{a} \phi')$ *(Kripke's law, K)*
  - $(M ::^{\mathcal{C}}_{a} \phi) \to (a\,\mathsf{k}\,M \to \phi)$ *(epistemic truthfulness)*
  - $\bigwedge_{b\in\mathcal{C}\cup\{a\}}((\underbrace{(M, b) ::^{\mathcal{C}}_{a} \phi}_{\textit{can prove}}) \to \{\![M]\!\}_a ::^{\mathcal{C}\cup\{a\}}_{b} (\underbrace{a\,\mathsf{k}\,M \wedge M ::^{\mathcal{C}}_{a} \phi}_{\textit{does prove}}))$
    (nominal [in b] peer review)
  - $(M ::^{\mathcal{C}\cup\mathcal{C}'}_{a} \phi) \to M ::^{\mathcal{C}}_{a} \phi$ *(group decomposition)* $\}$

  designate a set of axiom schemas.

Then, $\mathrm{LiiP} := \mathrm{Cl}(\emptyset) := \bigcup_{n\in\mathbb{N}} \mathrm{Cl}^n(\emptyset)$*, where for all* $\mathit{\Gamma} \subseteq \mathcal{L}$ *:*

$$\begin{aligned}
\mathrm{Cl}^0(\mathit{\Gamma}) &:= \mathit{\Gamma}_1 \cup \mathit{\Gamma}\\
\mathrm{Cl}^{n+1}(\mathit{\Gamma}) &:= \mathrm{Cl}^n(\mathit{\Gamma}) \cup\\
&\quad\ \{\ \phi' \mid \{\phi, \phi \to \phi'\} \subseteq \mathrm{Cl}^n(\mathit{\Gamma})\ \} \cup \quad (\text{modus ponens}, \textit{MP})\\
&\quad\ \{\ M ::^{\mathcal{C}}_{a} \phi \mid \phi \in \mathrm{Cl}^n(\mathit{\Gamma})\ \} \cup \quad (\textit{necessitation, N})\\
&\quad\ \{\ (M ::^{\mathcal{C}}_{a} \phi) \leftrightarrow M' ::^{\mathcal{C}}_{a} \phi \mid (a\,\mathsf{k}\,M \leftrightarrow a\,\mathsf{k}\,M') \in \mathrm{Cl}^n(\mathit{\Gamma})\ \}\\
&\qquad (\textit{epistemic bitonicity}).
\end{aligned}$$

We call LiiP *a* base theory*, and* $\mathrm{Cl}(\mathit{\Gamma})$ *an* LiiP-theory *for any* $\mathit{\Gamma} \subseteq \mathcal{L}$.

Notice the logical order of LiiP, which is, due to propositions about (proofs of) propositions, *higher-order propositional.* Further, observe that we assume the existence of a dependable mechanism for signing messages, which we model with the above synthesis and analysis axioms. In *trusted* multi-agent systems, signatures are unforg*ed,* and thus such a mechanism is trivially given by the inclusion of the sender's name in the sent message, or by the sender's sensorial impression on the receiver when communication is immediate. In *dis*trusted multi-agent systems (e.g., the open Internet), a practically unforge*able* signature mechanism can be implemented with classical *certificate-based* or, more directly, with *identity-based* public-key cryptography [8]. We also assume the existence of a pairing mechanism modelling finite sets. Such a mechanism is required by the important application of communication (not only cryptographic) protocols [9, Chapter 3], in which concatenation of high-level data packets is associative, commutative, and idempotent. The key to the validity of K is that we understand interactive proofs as *sufficient evidence* for intended resource-unbounded proof-checking agents (who are though still unable to guess), see [2, Section 3.2.2] for more details. Next, the significance of epistemic truthfulness to interactivity is that in truly distributed multi-agent systems, not all proofs are known by all agents, i.e., agents are not omniscient with respect to messages. Otherwise, why communicate with each other? So there being a proof does not imply knowledge of that proof. When an agent a does not know the proof and the agent cannot generate the proof *ex nihilo* herself by guessing it, only communication from a peer, who thus acts as an oracle, can entail the knowledge of the proof with a. That is, provability and truth are necessarily concomitant in the non-interactive setting, whereas in interactive settings they are not necessarily so [2]. In nominal peer review, "can prove" suggests the proof *potentiality* of (M, b) : "if *a were to* know, e.g., receive, (M, b)" (and thus know her potential interlocutor b's name). Whereas given $\{\![M]\!\}_a$ to b, e.g., in an acknowledgement from a, "does prove" suggests the proof *actuality* of M : "*a does* know, e.g., did receive, (M, b)", otherwise a could not have signed M. See the proof of Corollary 2.5 for a semantic justification of the *raison d'être* of b in (M, b). Then, the justification for the necessitation rule (schema) is that in interactive settings, validities, and thus *a fortiori* tautologies (in the strict sense of validities of the propositional fragment), are in some sense trivialities [2]. To see why, recall that modal validities are true in *all* pointed models [1], and thus not worth being communicated from one point to another in a given model, e.g., by means of specific interactive proofs. (Nothing is logically more embarrassing than talking in tautologies.) Therefore, validities deserve *arbitrary* proofs. What is worth being communicated are truths weaker than validities, namely local truths in the standard model-theoretic sense [1], which may not hold universally. Otherwise why communicate with each other? Finally, observe that epistemic bitonicity is a rule of *logical modularity* that allows the modular generation of structural modal laws from equivalence term laws (cf. Theorem 1).

The grey-shading in Definition 2 indicates that the axioms and rules of LiiP differ from those of LiP in exactly Kripke's law, nominal peer review, and epistemic bitonicity (cf. [2] and Section 3). In LiP, these three LiiP-laws correspond to the *generalised* Kripke-law $(M :_a^{\mathcal{C}} (\phi \to \phi')) \to ((M' :_a^{\mathcal{C}} \phi) \to (M, M') :_a^{\mathcal{C}} \phi')$, (plain) peer review $(M :_a^{\mathcal{C}} \phi) \to \bigwedge_{b \in \mathcal{C} \cup \{a\}} (\{\![M]\!\}_a :_b^{\mathcal{C} \cup \{a\}} (a \,\mathsf{k}\, M \land M :_a^{\mathcal{C}} \phi))$, and epistemic *anti*tonicity "from $a \,\mathsf{k}\, M \to a \,\mathsf{k}\, M'$ deduce $(M' :_a^{\mathcal{C}} \phi) \to M :_a^{\mathcal{C}} \phi$", respectively. The addition of the axiom schema

$$\boxed{(M ::_a^{\mathcal{C}} \phi) \to (M, M') ::_a^{\mathcal{C}} \phi}$$

to LiiP will result in a logic LiiP$^+$ that is isomorphic to LiP (cf. Theorem 4). So in some sense, the essential difference between instant proofs (proofs for at least an instant) and persistent proofs (proofs for eternity) is distilled in this single additional law. Following Artёmov in [10], this law can be interpreted as Lehrer and Paxson's indefeasibility condition for justified true belief [2]. In sum, while both LiP-proofs and LiiP-proofs are indefeasible in the instant when they are learnt (they induce knowledge, not only belief), LiiP-proofs (LiP-proofs) are possibly (necessarily) (in)defeasible in the future of the instant in which they are learnt.

Now note the following macro-definitions: $\top := a\,\mathsf{k}\,a$, $\bot := \neg\top$, $\phi \vee \phi' := \neg(\neg\phi \wedge \neg\phi')$, $\phi \rightarrow \phi' := \neg\phi \vee \phi'$, and $\phi \leftrightarrow \phi' := (\phi \rightarrow \phi') \wedge (\phi' \rightarrow \phi)$. In the sequel, ":iff" abbreviates "by definition, if and only if".

Proposition 1 (Hilbert-style proof system). *Let*

- $\Phi \vdash_{\mathrm{LiiP}} \phi$ *:iff if* $\Phi \subseteq \mathrm{LiiP}$ *then* $\phi \in \mathrm{LiiP}$
- $\phi \dashv\vdash_{\mathrm{LiiP}} \phi'$ *:iff* $\{\phi\} \vdash_{\mathrm{LiiP}} \phi'$ *and* $\{\phi'\} \vdash_{\mathrm{LiiP}} \phi$
- $\vdash_{\mathrm{LiiP}} \phi$ *:iff* $\emptyset \vdash_{\mathrm{LiiP}} \phi$.

In other words, $\vdash_{\mathrm{LiiP}} \subseteq 2^{\mathcal{L}} \times \mathcal{L}$ *is a* system of closure conditions. *For example:*

1. *for all axioms* $\phi \in \Gamma_1$, $\vdash_{\mathrm{LiiP}} \phi$
2. *for* modus ponens, $\{\phi, \phi \rightarrow \phi'\} \vdash_{\mathrm{LiiP}} \phi'$
3. *for necessitation,* $\{\phi\} \vdash_{\mathrm{LiiP}} M ::_a^{\mathcal{C}} \phi$
4. *for epistemic bitonicity,* $\{a\,\mathsf{k}\,M \leftrightarrow a\,\mathsf{k}\,M'\} \vdash_{\mathrm{LiiP}} (M ::_a^{\mathcal{C}} \phi) \leftrightarrow M' ::_a^{\mathcal{C}} \phi$.

(In the space-saving, horizontal Hilbert-notation "$\Phi \vdash_{\mathrm{LiiP}} \phi$*",* Φ *is not a set of hypotheses but a set of premises, cf.* modus ponens, *necessitation, and epistemic bitonicity.) Then* $\vdash_{\mathrm{LiiP}}$ *can be viewed as being defined by a* Cl*-induced Hilbert-style proof system. In fact* $\mathrm{Cl} : 2^{\mathcal{L}} \rightarrow 2^{\mathcal{L}}$ *is a* standard consequence operator, *i.e., a* substitution-invariant compact closure operator.

Proof. See [1].

We are now going to present some useful, deducible *structural* laws of LiiP. Here, "structural" means "deducible exclusively from term axioms". The laws are enumerated in a (total) order that respects (but cannot reflect) their respective proof prerequisites. The laws are also deducible in LiP, in the same order [2]. (All LiiP-deducible laws are also LiP-deducible, but not vice versa.)

Theorem 1 (Some useful deducible structural laws)

1. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, M') \rightarrow a\,\mathsf{k}\,M$ *(left projection, 1-way* `K`*-combinator property)*
2. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, M') \rightarrow a\,\mathsf{k}\,M'$ *(right projection)*
3. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, M) \leftrightarrow a\,\mathsf{k}\,M$ *(pairing idempotency)*
4. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, M') \leftrightarrow a\,\mathsf{k}\,(M', M)$ *(pairing commutativity)*
5. $\vdash_{\mathrm{LiiP}} (a\,\mathsf{k}\,M \rightarrow a\,\mathsf{k}\,M') \leftrightarrow (a\,\mathsf{k}\,(M, M') \leftrightarrow a\,\mathsf{k}\,M)$ *(neutral pair elements)*
6. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, a) \leftrightarrow a\,\mathsf{k}\,M$ *(self-neutral pair element)*
7. $\vdash_{\mathrm{LiiP}} a\,\mathsf{k}\,(M, (M', M'')) \leftrightarrow a\,\mathsf{k}\,((M, M'), M'')$ *(pairing associativity)*
8. $\vdash_{\mathrm{LiiP}} ((M, M) ::_a^{\mathcal{C}} \phi) \leftrightarrow M ::_a^{\mathcal{C}} \phi$ *(proof idempotency)*
9. $\vdash_{\mathrm{LiiP}} ((M, M') ::_a^{\mathcal{C}} \phi) \leftrightarrow (M', M) ::_a^{\mathcal{C}} \phi$ *(proof commutativity)*
10. $\{a\,\mathsf{k}\,M \rightarrow a\,\mathsf{k}\,M'\} \vdash_{\mathrm{LiiP}} ((M, M') ::_a^{\mathcal{C}} \phi) \leftrightarrow M ::_a^{\mathcal{C}} \phi$ *(neutral proof elements)*

11. $\vdash_{\text{LiiP}} ((M, a) ::^{\mathcal{C}}_{a} \phi) \leftrightarrow M ::^{\mathcal{C}}_{a} \phi$ *(self-neutral proof element)*
12. $\vdash_{\text{LiiP}} ((M, (M', M'')) ::^{\mathcal{C}}_{a} \phi) \leftrightarrow ((M, M'), M'') ::^{\mathcal{C}}_{a} \phi$ *(proof associativity)*
13. $\vdash_{\text{LiiP}} (\{\![M]\!\}_{a} ::^{\mathcal{C}}_{a} \phi) \leftrightarrow M ::^{\mathcal{C}}_{a} \phi$ *(self-signing idempotency)*

Proof. See [1].

Like in LiP [2], the preceding 1-way K-combinator property and the following simple corollary of Theorem 1 jointly establish the important fact that our communicating agents can be viewed as combinators in the sense of Combinatory Logic viewed in turn as a (non-equational) theory of (message or proof) term reduction [11]. (The converse of the above K-combinator property does not hold.)

Corollary 1 (S-combinator property)

1. $\vdash_{\text{LiiP}} a\,\mathsf{k}\,((M, M'), M'') \leftrightarrow a\,\mathsf{k}\,(M, (M'', (M', M'')))$
2. $\vdash_{\text{LiiP}} (((M, M'), M'') ::^{\mathcal{C}}_{a} \phi) \leftrightarrow (M, (M'', (M', M''))) ::^{\mathcal{C}}_{a} \phi$

Proof See [1].

We are going to present also some useful deducible *logical* laws of LiiP. Here, “logical” means “not structural” in the previously defined sense. Also these laws are enumerated in an order that respects their respective proof prerequisites, and are deducible in LiP in the same order [2].

Theorem 2 (Some useful deducible logical laws)

1. $\{\phi \rightarrow \phi'\} \vdash_{\text{LiiP}} (M ::^{\mathcal{C}}_{a} \phi) \rightarrow M ::^{\mathcal{C}}_{a} \phi'$ *(regularity)*
2. $\{a\,\mathsf{k}\,M \leftrightarrow a\,\mathsf{k}\,M', \phi \rightarrow \phi'\} \vdash_{\text{LiiP}} (M ::^{\mathcal{C}}_{a} \phi) \rightarrow M' ::^{\mathcal{C}}_{a} \phi'$ *(biepistemic regul.)*
3. $\vdash_{\text{LiiP}} ((M ::^{\mathcal{C}}_{a} \phi) \wedge M ::^{\mathcal{C}}_{a} \phi') \leftrightarrow M ::^{\mathcal{C}}_{a} (\phi \wedge \phi')$ *(proof conjunctions* bis*)*
4. $\vdash_{\text{LiiP}} ((M ::^{\mathcal{C}}_{a} \phi) \vee M ::^{\mathcal{C}}_{a} \phi') \rightarrow M ::^{\mathcal{C}}_{a} (\phi \vee \phi')$ *(proof disjunctions* bis*)*
5. $\vdash_{\text{LiiP}} M ::^{\mathcal{C}}_{a} \top$ *(anything can prove tautological truth)*
6. $\vdash_{\text{LiiP}} \{\![M]\!\}_{b} ::^{\mathcal{C} \cup \{b\}}_{a} b\,\mathsf{k}\,M$ *(authentic knowledge)*
7. $\vdash_{\text{LiiP}} M ::^{\emptyset}_{a} a\,\mathsf{k}\,M$ *(self-knowledge)*
8. $\vdash_{\text{LiiP}} (M ::^{\mathcal{C} \cup \mathcal{C}'}_{a} \phi) \rightarrow ((M ::^{\mathcal{C}}_{a} \phi) \wedge M ::^{\mathcal{C}'}_{a} \phi)$ *(group decomposition* bis*)*
9. $\vdash_{\text{LiiP}} (M ::^{\mathcal{C} \cup \{a\}}_{a} \phi) \leftrightarrow (M ::^{\mathcal{C}}_{a} \phi)$ *(self-neutral group element).*
10. $\vdash_{\text{LiP}} M ::^{\mathcal{C}}_{a} ((M ::^{\mathcal{C}}_{a} \phi) \rightarrow \phi)$ *(self-proof of truthfulness)*
11. $\vdash_{\text{LiP}} M ::^{\mathcal{C}}_{a} (\neg(M ::^{\mathcal{C}}_{a} \bot))$ *(self-proof of proof consistency)*
12. $\vdash_{\text{LiP}} (M ::^{\mathcal{C}}_{a} (M ::^{\mathcal{C}}_{a} \phi)) \leftrightarrow M ::^{\mathcal{C}}_{a} \phi$ *(modal idempotency)*

Proof Like in LiP [2].

Like in LiP, the key to the validity of modal idempotency is that each agent (e.g., a) can act herself as proof-checker, see [2, Section 3.2.2] for more details.

We now continue to present the constructive semantics for LiiP (cf. [2, Section 2.2]) and state some important new and further-used results about it. (See [1] for formal proofs.) The essential differences to the semantics of LiP are grey-shaded.

Definition 3 (Semantic ingredients). *For the knowledge-constructive model-theoretic study of LiiP let*

- $\mathcal{S}$ *designate the* state space*—a set of* system states s
- $\mathrm{msgs}_a : \mathcal{S} \to 2^{\mathcal{M}}$ *designate a* raw-data extractor *that extracts (without analysing) the (finite) set of messages from a system state s that agent $a \in \mathcal{A}$ has either generated (assuming that only a can generate a's signature) or else received* as such *(not only as a strict subterm of another message); that is,* $\mathrm{msgs}_a(s)$ *is a's* data base *in s*
- $\mathrm{cl}^s_a : 2^{\mathcal{M}} \to 2^{\mathcal{M}}$ *designate a* data-mining operator *such that* $\mathrm{cl}^s_a(\mathcal{D}) := \mathrm{cl}_a(\mathrm{msgs}_a(s) \cup \mathcal{D}) := \bigcup_{n\in\mathbb{N}} \mathrm{cl}^n_a(\mathrm{msgs}_a(s) \cup \mathcal{D})$*, where for all $\mathcal{D} \subseteq \mathcal{M}$:*

$$\begin{aligned}
\mathrm{cl}^0_a(\mathcal{D}) &:= \{a\} \cup \mathcal{D}\\
\mathrm{cl}^{n+1}_a(\mathcal{D}) &:= \mathrm{cl}^n_a(\mathcal{D}) \cup\\
&\qquad \{\ (M, M') \mid \{M, M'\} \subseteq \mathrm{cl}^n_a(\mathcal{D})\ \} \cup \quad \textit{(pairing)}\\
&\qquad \{\ M, M' \mid (M, M') \in \mathrm{cl}^n_a(\mathcal{D})\ \} \cup \quad \textit{(unpairing)}\\
&\qquad \{\ \{\![M]\!\}_a \mid M \in \mathrm{cl}^n_a(\mathcal{D})\ \} \cup \quad \textit{(}\text{personal } \textit{signature} \text{ synthesis}\textit{)}\\
&\qquad \{\ (M, b) \mid \{\![M]\!\}_b \in \mathrm{cl}^n_a(\mathcal{D})\ \} \quad \textit{(}\text{universal } \textit{signature} \text{ analysis}\textit{)}
\end{aligned}$$

- $<^M_a \subseteq \mathcal{S} \times \mathcal{S}$ *designate a* data preorder *on states such that for all $s, s' \in \mathcal{S}$, $s <^M_a s'$:iff $\mathrm{cl}^s_a(\{M\}) = \mathrm{cl}^{s'}_a(\emptyset)$, were M can be viewed as* oracle input *in addition to a's* individual-knowledge base $\mathrm{cl}^s_a(\emptyset)$ *(cf. also [2, Section 2.2])*
- $<^M_{\mathcal{C}} := (\bigcup_{a\in\mathcal{C}} <^M_a)^{++}$*, where '$^{++}$' designates the closure operation of so-called* generalised transitivity *in the sense that* $<^M_{\mathcal{C}} \circ <^{M'}_{\mathcal{C}} \subseteq <^{(M,M')}_{\mathcal{C}}$
- $\equiv_a := <^a_a$ *designate an equivalence relation of* state indistinguishability
- ${}_M\mathrm{R}^{\mathcal{C}}_a \subseteq \mathcal{S} \times \mathcal{S}$ *designate a* **concretely constructed** accessibility relation*—short,* **concrete** accessibility*—for the proof modality such that for all $s, s' \in \mathcal{S}$,*

$$s\ {}_M\mathrm{R}^{\mathcal{C}}_a\ s' \ \textit{:iff}\ s' \in \bigcup_{\substack{s <^M_{\mathcal{C}\cup\{a\}} \tilde{s} \text{ and}\\ M \in \mathrm{cl}^{\tilde{s}}_a(\emptyset)}} [\tilde{s}]_{\equiv_a}$$

$$\textit{(iff there is } \tilde{s} \in \mathcal{S} \textit{ s.t. } s <^M_{\mathcal{C}\cup\{a\}} \tilde{s} \textit{ and } M \in \mathrm{cl}^{\tilde{s}}_a(\emptyset) \textit{ and } \tilde{s} \equiv_a s'\textit{)}.$$

Fact 1 establishes the knowledge-constructiveness of our Kripke-model for LiiP (cf. Definition 5).

Fact 1 (Kripke-model knowledge-constructiveness)

$$\textit{for all } s' \in \mathcal{S},\ \textit{if } s\ {}_M\mathrm{R}^{\mathcal{C}}_a\ s' \textit{ then } (\mathfrak{S}, \mathcal{V}), s' \models \phi \textit{ if and only if}$$

$$\textit{for all } \check{s} \in \mathcal{S},\ \textit{if } s <^M_{\mathcal{C}\cup\{a\}} \check{s} \textit{ then } (\mathfrak{S}, \mathcal{V}), \check{s} \models a\,\mathsf{k}\underbrace{M}_{\substack{\textit{sufficient}\\ \textit{evidence}}} \to \mathsf{K}_a(\underbrace{\ \phi\ }_{\substack{\textit{induced}\\ \textit{knowledge}}}),$$

where the standard epistemic modality K_a *is defined like in [4] as*

$$(\mathfrak{S}, \mathcal{V}), \check{s} \models \mathsf{K}_a(\phi) \quad \textit{:iff} \quad \textit{for all } s' \in \mathcal{S},\ \textit{if } \check{s} \equiv_a s' \textit{ then } (\mathfrak{S}, \mathcal{V}), s' \models \phi.$$

Table 1. Satisfaction relation

$$\begin{array}{rl}
(\mathfrak{S},\mathcal{V}),s\models P & \text{:iff } s\in\mathcal{V}(P)\\
(\mathfrak{S},\mathcal{V}),s\models\neg\phi & \text{:iff not } (\mathfrak{S},\mathcal{V}),s\models\phi\\
(\mathfrak{S},\mathcal{V}),s\models\phi\wedge\phi' & \text{:iff } (\mathfrak{S},\mathcal{V}),s\models\phi \text{ and } (\mathfrak{S},\mathcal{V}),s\models\phi'\\
(\mathfrak{S},\mathcal{V}),s\models M::^{\mathcal{C}}_{a}\phi & \text{:iff for all } s'\in\mathcal{S}\text{, if } s\ {}_{M}\mathcal{R}^{\mathcal{C}}_{a}\ s' \text{ then } (\mathfrak{S},\mathcal{V}),s'\models\phi
\end{array}$$

Proof. By elementary-logical transformations of the definiens of ${}_{M}\mathrm{R}^{\mathcal{C}}_{a}$.

Definition 4 (Message ordering and equivalence)

- $M\sqsubseteq^{s}_{a}M'$ *:iff if* $M\in\mathrm{cl}^{s}_{a}(\emptyset)$ *then* $M'\in\mathrm{cl}^{s}_{a}(\emptyset)$
- $M\equiv^{s}_{a}M'$ *:iff* $M\sqsubseteq^{s}_{a}M'$ *and* $M'\sqsubseteq^{s}_{a}M$
- $M\sqsubseteq_{a}M'$ *:iff for all* $s\in\mathcal{S}$, $M\sqsubseteq^{s}_{a}M'$
- $M\equiv_{a}M'$ *:iff for all* $s\in\mathcal{S}$, $M\equiv^{s}_{a}M'$

Corollary 2 (Concrete accessibility)

1. *If* $\mathcal{C}\subseteq\mathcal{C}'$ *then* ${}_{M}\mathrm{R}^{\mathcal{C}}_{a}\subseteq{}_{M}\mathrm{R}^{\mathcal{C}'}_{a}$ *(communal monotonicity).*
2. *If* $M\equiv_{a}M'$ *then* ${}_{M}\mathrm{R}^{\mathcal{C}}_{a}={}_{M'}\mathrm{R}^{\mathcal{C}}_{a}$ *(conditional stability).*
3. *If* $M\in\mathrm{cl}^{s}_{a}(\emptyset)$ *then* $s\ {}_{M}\mathrm{R}^{\mathcal{C}}_{a}\ s$ *(conditional reflexivity).*
4. *If* $s\ {}_{\{\!\{M\}\!\}_{b}}\mathrm{R}^{\mathcal{C}}_{a}\ s'$ *then* $M\in\mathrm{cl}^{s'}_{b}(\emptyset)$ *(signature property).*
5. *For all* $b\in\mathcal{C}\cup\{a\}$, $({}_{\{\!\{M\}\!\}_{a}}\mathrm{R}^{\mathcal{C}\cup\{a\}}_{b}\circ{}_{M}\mathrm{R}^{\mathcal{C}}_{a})\subseteq{}_{(M,b)}\mathrm{R}^{\mathcal{C}}_{a}$ *(communal transitivity).*

Proof. See [1].

Definition 5 (Kripke-model). *We define the* satisfaction relation *'*$\models$*' for LiiP in Table 1, where*

- $\mathcal{V}:\mathcal{P}\to 2^{\mathcal{S}}$ *designates a usual* valuation function, *yet partially predefined such that for all* $a\in\mathcal{A}$ *and* $M\in\mathcal{M}$,

  $$\mathcal{V}(a\,\mathsf{k}\,M):=\{\ s\in\mathcal{S}\mid M\in\mathrm{cl}^{s}_{a}(\emptyset)\ \}$$

  (If agents are Turing-machines then a knowing M *can be understood as a being able to parse* M *on its tape.)*
- $\mathfrak{S}:=(\mathcal{S},\{{}_{M}\mathcal{R}^{\mathcal{C}}_{a}\}_{M\in\mathcal{M},a\in\mathcal{A},\mathcal{C}\subseteq\mathcal{A}})$ *designates a (modal)* frame *for LiiP with an* **abstractly constrained** accessibility relation *— short,* **abstract** accessibility *—* ${}_{M}\mathcal{R}^{\mathcal{C}}_{a}\subseteq\mathcal{S}\times\mathcal{S}$ *for the proof modality such that — the* semantic interface:
  - *if* $\mathcal{C}\subseteq\mathcal{C}'$ *then* ${}_{M}\mathcal{R}^{\mathcal{C}}_{a}\subseteq{}_{M}\mathcal{R}^{\mathcal{C}'}_{a}$
  - *if* $M\equiv_{a}M'$ *then* ${}_{M}\mathcal{R}^{\mathcal{C}}_{a}={}_{M'}\mathcal{R}^{\mathcal{C}}_{a}$
  - *if* $M\in\mathrm{cl}^{s}_{a}(\emptyset)$ *then* $s\ {}_{M}\mathcal{R}^{\mathcal{C}}_{a}\ s$
  - *if* $s\ {}_{\{\!\{M\}\!\}_{b}}\mathcal{R}^{\mathcal{C}}_{a}\ s'$ *then* $M\in\mathrm{cl}^{s'}_{b}(\emptyset)$
  - *for all* $b\in\mathcal{C}\cup\{a\}$, $({}_{\{\!\{M\}\!\}_{a}}\mathcal{R}^{\mathcal{C}\cup\{a\}}_{b}\circ{}_{M}\mathcal{R}^{\mathcal{C}}_{a})\subseteq{}_{(M,b)}\mathcal{R}^{\mathcal{C}}_{a}$
- $(\mathfrak{S},\mathcal{V})$ *designates a (modal)* model *for LiiP.*

Looking back, we recognise that Corollary 2 actually establishes the important fact that our concrete accessibility ${}_M\mathrm{R}_a^{\mathcal{C}}$ in Definition 3 realises all the properties stipulated by our abstract accessibility ${}_M\mathcal{R}_a^{\mathcal{C}}$ in Definition 5; we say that

$${}_M\mathrm{R}_a^{\mathcal{C}} \textit{ exemplifies } (\text{or } \textit{realises}) \ {}_M\mathcal{R}_a^{\mathcal{C}}.$$

Further, observe that LiiP (like LiP) has a Herbrand-style semantics, i.e., logical constants (agent names) and functional symbols (pairing, signing) are self-interpreted rather than interpreted in terms of (other, semantic) constants and functions. This simplifying design choice spares our framework from the additional complexity that would arise from term-variable assignments [5], which in turn keeps our models propositionally modal. Our choice is admissible because our individuals (messages) are finite. (Infinitely long "messages" are non-messages; they can never be completely received, e.g., transmitting irrational numbers as such is impossible.)

Theorem 3 (Axiomatic adequacy). $\vdash_{\mathrm{LiiP}}$ *is* adequate *for* $\models$*, i.e.,:*

1. *if* $\vdash_{\mathrm{LiiP}} \phi$ *then* $\models \phi$ *(axiomatic soundness)*
2. *if* $\models \phi$ *then* $\vdash_{\mathrm{LiiP}} \phi$ *(semantic completeness).*

Proof. Both parts can be proved with standard means: soundness follows as usual from the admissibility of the axioms and rules; and completeness follows by means of the classical construction of canonical models, using Lindenbaum's construction of maximally consistent sets (see [1]).

3 LiP as an Extension of LiiP

In this section, we reconstruct LiP syntactically, as a minimal conservative extension of LiiP with one simplified and one additional axiom schema, as well as semantically, with a simplified semantic interface that has none of the *a posteriori* constraints from [2] but only standard, *a priori* constraints, i.e., stipulations.

Theorem 4. *Define the* LiiP*-theory*

$$\mathrm{LiiP}^+ := \mathrm{Cl}(\{\underbrace{(M ::_a^{\mathcal{C}} \phi) \rightarrow (M, M') ::_a^{\mathcal{C}} \phi}_{\textit{proof extension}}\}),$$

where Cl *is as in Definition 2. Then* LiiP^+ *is isomorphic to* LiP*, in symbols,*

$$\mathrm{LiiP}^+ \cong \mathrm{LiP}.$$

In particular, the generalised Kripke law GK as mentioned before and below is deducible in LiiP^+*, and thus we need only stipulate the simpler standard Kripke law K for LiP, like for LiiP. Moreover,* alternatively to adding *the axiom schema of proof extension to LiiP, we could* equivalently replace *the primitive rule schema of epistemic bitonicity in LiiP with the stronger one of epistemic antitonicity.*

Proof. See [1].

Corollary 3 (Simplified semantic interface for LiP). *A simplified semantic interface for LiP is given by the one for LiiP in Definition 5 but with the abstract accessibility* ${}_{M}\mathcal{R}^{\mathcal{C}}_{a} \subseteq \mathcal{S} \times \mathcal{S}$ *being constrained*

- *such that* $\boxed{\textit{if } M \sqsubseteq_a M' \textit{ then } {}_{M}\mathcal{R}^{\mathcal{C}}_{a} \subseteq {}_{M'}\mathcal{R}^{\mathcal{C}}_{a} \quad \textit{(proof monotonicity)}}$ **instead of** *being constrained by conditional stability;*
- or alternatively *such that* $\boxed{{}_{(M,M')}\mathcal{R}^{\mathcal{C}}_{a} \subseteq {}_{M}\mathcal{R}^{\mathcal{C}}_{a} \quad \textit{(pair splitting)}}$ **in addition to** *being constrained by conditional stability.*

Proof. It is straightforward to check that the semantic constraints of proof monotonicity and pair splitting correspond to the syntactic laws of epistemic antitonicity and proof extension, respectively, which are interdeducible (cf. Theorem 4).

4 Conclusion

We have proposed LiiP with as main contributions those described in Section 1.1. The notion of non-monotonic proofs captured by LiiP has the advantage of being not only operational thanks to our proof-theoretic definition but also declarative thanks to our complementary model-theoretic definition, which gives a constructive epistemic semantics to these proofs in the sense of explicating *what* (knowledge) they effect in agents in the instant of their reception, complementing thereby the (operational) axiomatics, which explicates *how* they do so.

We conclude by mentioning [12] as a piece of related work, discussed in [1].

References

1. Kramer, S.: Logic of non-monotonic interactive proofs (formal theory of temporary knowledge transfer). Technical Report 1208.1842, arXiv (2012), `http://arxiv.org/abs/1208.1842`
2. Kramer, S.: A logic of interactive proofs (formal theory of knowledge transfer). Technical Report 1201.3667, arXiv (2012), `http://arxiv.org/abs/1201.3667`
3. Makinson, D.: How To Go Nonmonotonic. In: Handbook of Philosophical Logic, 2nd edn., vol. 12. Springer (2005)
4. Meyer, J.J., Veltman, F.: Intelligent Agents and Common Sense Reasoning. In: [5]
5. Blackburn, P., van Benthem, J., Wolter, F. (eds.): Handbook of Modal Logic. Studies in Logic and Practical Reasoning, vol. 3. Elsevier (2007)
6. Fagin, R., Halpern, J., Moses, Y., Vardi, M.: Reasoning about Knowledge. MIT Press (1995)
7. Hendricks, V., Roy, O. (eds.): Epistemic Logic: 5 Questions. Automatic Press (2010)
8. Katz, J.: Digital Signatures. Springer (2010)
9. Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edn. Wiley (2008)
10. Artemov, S.: The logic of justifications. The Review of Symbolic Logic 1(4) (2008)
11. Hindley, J., Seldin, J.: Lambda-Calculus and Combinators, 2nd edn. Cambridge University Press (2008)
12. Baltag, A., Renne, B., Smets, S.: The Logic of Justified Belief Change, Soft Evidence and Defeasible Knowledge. In: Ong, L., de Queiroz, R. (eds.) WoLLIC 2012. LNCS, vol. 7456, pp. 168–190. Springer, Heidelberg (2012)

Noninterference for Intuitionist Necessity

Radha Jagadeesan, Corin Pitcher, and James Riely

DePaul University

Abstract. We study indexed necessity modalities in intuitionist S4. These provide the logical foundation required by a variety of applications, such as capability-based policy languages for access control and type theories for exceptional computation. We establish noninterference properties capturing the limitations on information flow between formulas under the scope of necessity modalities with different indices.

1 Introduction

Classical S4 is standard textbook material [11]. The intuitionist versions of S4 are also well explored [6,14,5,10]. We recall briefly. For any formula α, $\Box\alpha$ is also a formula. The necessity modality[1] satisfies the following three axioms and rule of inference.

$$\Box(\alpha \Rightarrow \beta) \Rightarrow \Box\alpha \Rightarrow \Box\beta \qquad \text{(K: distribution)}$$

$$\Box\alpha \Rightarrow \alpha \qquad \text{(T: reflexivity)}$$

$$\Box\alpha \Rightarrow \Box\Box\alpha \qquad \text{(4: transitivity)}$$

$$\text{If } \alpha \text{ is a theorem, so is } \Box\alpha \qquad \text{(N: necessitation)}$$

In this paper, we investigate the metatheory of indexed intuitionist S4 necessity modalities. Let $(\mathscr{L}, \preceq)$ be a preorder and let a, b range over elements of $\mathscr{L}$. We consider a family of modalities, indexed by elements of $\mathscr{L}$, such that:

For each a, the modality $\Box_a$ satisfies [K,T,4,N] above (Necessity modality)
If $b \preceq a$, then $\Box_b\alpha \Rightarrow \Box_a\alpha$ (Principal naturality)

Such indexed necessity operators arise naturally in a variety of settings. We consider two examples from the literature below.

Security Policies. In this example, $(\mathscr{L}, \preceq)$ is a lattice whose elements are security principals. In different applications, principals might represent users, roles, locations, or processes, etc. The ordering in the lattice is the security order: if $b \preceq a$, then b is less secure than a.

The indexed necessitation operator is used to capture the possession of capabilities [8,7]. Let object references, o, be atomic formulas. Then, $\Box_a o$ is intended to specify that a is permitted to possess object reference o. The formula $\Box_b(o \Rightarrow o')$ specifies a guarded object, such as a ciphertext. By distribution (K), b gets the capability to the plaintext, written $\Box_b o'$, whenever it gets the key, written $\Box_b o$.

In this application, principal naturality captures the idea that more secure principals have access to more capabilities.

---

[1] The modality has highest precedence; eg. $\Box\alpha \Rightarrow \beta$ stands for $(\Box\alpha) \Rightarrow \beta$.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 185–196, 2013.

Exceptional computations. The elements of the lattice are sets of exceptions. The ordering in the lattice is the subset order, i.e., $b \preceq a$ if $b \subseteq a$.

The necessity operator is used in the type theory to capture the names of the exceptions that can be raised in evaluating an expression [13,12]. For example, consider $\Box_a \alpha$ for a modality-free intuitionist formula α. An expression has this type if the following conditions hold: if its evaluation terminates normally, it results in a value of type α; and, any exception that it raises during an abnormal evaluation is contained in the set a. Thus, a is an upper bound on the exceptions that can be raised in evaluating an expression of this type; e.g., a pure functional program of type α that does not raise any exceptions is given the type $\Box_\emptyset \alpha$. Since all types are (at least implicitly) under the scope of an indexed modality, axiom (T) plays a limited role in this treatment.

Principal naturality is a conservative coercion that permits us to increase the upper bound on the set of exceptions that could be raised in evaluating an expression.

Noninterference. Noninterference is the idea that there is no information flow between differently indexed modalities. Let α be a modality free formula. The intuitive idea behind noninterference is that if $\Box_a \alpha$ is derivable from some deductively closed set of hypotheses, then it is derivable from a subset of those hypotheses that are in the scope of the modality indexed by a, i.e. the formulas of the form $\Box_a$. Thus, computations of values of a types are isolated from types that are not in the scope of an a indexed modality.

Noninterference implies the non-provability of some simple formulas. Let p be a proposition, and $b \not\preceq a$. Then, the following formulas are not provable.

$$\not\vdash \Box_b p \Rightarrow \Box_a p$$
$$\not\vdash ((\Box_a p \Rightarrow q) \;\&\; \Box_b p) \Rightarrow \Box_a q$$

Noninterference is essential to justify the use of indexed necessity modalities in the modeling of both motivating examples.

- The policies for capabilities are used in access control in a distributed system. The unprovability of $\Box_b p \Rightarrow \Box_a p$ ensures that the logical reasoning does not permit capabilities to be transferred unrestrictedly between principals. The unprovability of $((\Box_a p \Rightarrow q) \;\&\; \Box_b p) \Rightarrow \Box_a q$ ensures that the acquisition of new capabilities (p) by another principal (b) does not create new capabilities for a principal (a) by purely logical reasoning.
- In the modeling of exceptions, the consequences of noninterference are best seen in computational terms using the Curry-Howard isomorphism. The unprovability of the two formulas above captures the intuitive idea that there are no pure terms that can catch and handle the exceptions in $b \setminus a$. More generally, noninterference identifies the computations that can be queried during the evaluation of a pure expression in the scope of a $\Box_a$; clearly, any computation of a type $\Box_b$ cannot be queried if $a \not\subseteq b$.

Results. We describe an intuitionist logic with indexed necessity operators. Our sequent calculus is a multi-principal variant of the sequent calculus for intuitionist S4 described by Bierman and de Paiva [6]. Our particular design is guided by Abadi's formalization of the "says" monad [1] and games models of this monad [4] .

Our statement of noninterference follows Abadi's statement for monadic logics [1]. We describe a translation of logical formulas into intuitionist propositional logic. The main technical result is that the translation preserve provability, i.e., if the source formula is a theorem in our logic (with indexed modalities), the target formula is provable in standard intuitionist propositional logic. This preservation validates the intuitive idea that the proof of a formula $\Box_a\alpha$ does not essentially use formulas that are *not* in the scope of $\Box_a$.

As simple illustrations of the power of this approach, we show how this result is used to establish the non provability of formulas, including the two unprovable formulas considered earlier in this introduction.

Our noninterference theorem has the form, "for all valid proofs, there exists a translated proof that is valid in intuitionist propositional logic." Consequently, our results hold for any stricter logic that supports fewer proofs. In particular, our results hold for the canonical presentation of the Intuitionist S4 necessity modality. Thus, our noninterference theorem is robust: it is independent of our particular modeling of indexed intuitionist necessity.

Related Work. Intuitionist S4 is well explored. For example, Bierman and de Paiva [6] and Alechina, Mendler, de Paiva and Ritter [5] study categorical models of proof and provability. Pfenning and Wong [14] study the proof theory. We do not present a natural deduction system; the above papers discuss the subtle accommodations needed to facilitate the commutative conversions. Goubault-Larrecq and Goubault [10] study the geometry of the proofs of intuitionist S4 using tools from algebraic topology. None of this prior work studies principal-indexed modalities, nor does it address noninterference.

Our exploration of noninterference results is inspired by the modeling of access control using "says" monads and the study of the meta theory of these logics [2,3,9,1,15]. Our proof of noninterference builds on the translation-based proof pioneered in this research [1,15]. Our adaptation of these methods uses normal forms inspired by game semantics of monads [4]. This adaptation perforce has some new ingredients because the necessity modality is not "dual" to monads. The dual of the necessity modality in classical S4 is the possibility modality and not the says modality; the says modalities distributes over conjunction and the possibility modality does not.

Rest of the Paper. In section 2 we describe a sequent calculus for the logic. The following section 3 describes our treatment of non interference. We conclude in section 4. In appendix A, we explicate the internal structure of our translation by a factorization result.

2 Logic

Let p, q range over a set of atomic propositions. Let $(\mathscr{L}, \preceq)$ be a preorder, and let a, b, c range over elements of $\mathscr{L}$.

We consider intuitionist propositional logic with necessity modalities indexed by elements of $\mathscr{L}$. We include conjunction and implication but not disjunction. Formulas are defined inductively as follows.

$$\alpha,\beta,\gamma ::= \texttt{tt} \mid p \mid \alpha \,\&\, \beta \mid \alpha \Rightarrow \beta \mid \Box_a\alpha$$

2.1 *a*-available

The following definition impacts the modality introduction rule on the right. Formally, the format of the definition shadows Abadi's treatment in logics for monads [1].

Definition 1. a-available formulas are inductively defined as follows.

- `tt` is a-available.
- $\Box_b \alpha$ is a-available if either $b \preceq a$ or α is a-available
- $(\beta \Rightarrow \alpha)$ is a-available if α is a-available.
- $(\alpha \mathbin{\&} \beta)$ is a-available if both α and β are a-available.

This definition extends to sets, multisets, and sequences of formulas $\Gamma = \alpha_1 \ldots \alpha_n$ pointwise. $\Gamma = \alpha_1, \ldots, \alpha_n$ is a-available if all $\alpha_1, \ldots, \alpha_n$ are a-available. □

It will turn out that an a-available formula α is one that satisfies $\alpha \Rightarrow \Box_a \alpha$. In standard presentations, these are the formulas of form $\Box_a$. We motivate our more liberal presentation using game semantics[2] [4]: a formula is a-available if the first move in the game happens in the context of a principal lower in $\preceq$ than a. Thus, $\Box_b \alpha$ is a-available if $b \preceq a$ or α is a-available. The first move in $(\beta \Rightarrow \alpha)$ comes from α, so it is a-available if α is. The first moves of $(\alpha \mathbin{\&} \beta)$ comes from either α or β, so it is a-available if both α, β are. `tt` is trivially a-available since it has no moves.

Lemma 2. If $b \preceq a$ and α is b-available, then α is a-available. □

2.2 Sequent Calculus

The sequent calculus for the logic is given in Figure 1. Our sequent calculus is a multi-principal variant of the necessity fragment of the sequent calculus of Bierman and De Paiva [6]. The only modification is in the PROMOTE rule that uses our more generous variation of a-available.

Remark 3. Weakening is admissible [6]. This is the motivation for the weakening built into AXIOM and PROMOTE. We do not present a natural deduction system; subtle accommodations are needed to facilitate the commutative conversions [6,14]. □

Remark 4 (Standard theorems). The standard ingredients for intuitionist necessity are derivable standardly. None of the following derivations use the third or fourth cases of the Definition 1.

$$\frac{}{\Box_a \alpha \vdash \Box_a \Box_a \alpha} \qquad \text{(Comultiplication)}$$

$$\frac{\beta \vdash \alpha}{\Box_a \beta \vdash \Box_a \alpha} \qquad \text{(Functoriality)}$$

$$\frac{}{\Box_b \alpha \vdash \Box_a \alpha}\ b \preceq a \qquad \text{(Principal naturality)}$$

---

[2] Abramsky and Jagadeesan [4] describe game semantics for monads in a form that is easily adapted to the current setting. Merely invert the inequality in the definition of condition (p6) in that paper.

$$\begin{array}{lllll}
\text{(AXIOM)} & \text{(CUT)} & \text{(EXCHANGE)} & \text{(WEAKENING)} & \text{(CONTRACTION)} \\
\dfrac{}{\Gamma,\alpha\vdash\alpha} & \dfrac{\Gamma\vdash\alpha \quad \Delta,\alpha\vdash\beta}{\Gamma,\Delta\vdash\beta} & \dfrac{\Gamma,\gamma,\beta,\Delta\vdash\alpha}{\Gamma,\beta,\gamma,\Delta\vdash\alpha} & \dfrac{\Gamma\vdash\alpha}{\Gamma,\beta\vdash\alpha} & \dfrac{\Gamma,\beta,\beta,\Delta\vdash\alpha}{\Gamma,\beta,\Delta\vdash\alpha}
\end{array}$$

$$\begin{array}{llll}
\text{(\&-L)} & \text{(\&-R)} & (\mathtt{tt}\text{-L}) & (\mathtt{tt}\text{-R}) \\
\dfrac{\Gamma,\beta,\gamma,\Delta\vdash\alpha}{\Gamma,\beta\,\&\,\gamma,\Delta\vdash\alpha} & \dfrac{\Gamma\vdash\alpha \quad \Gamma\vdash\beta}{\Gamma\vdash\alpha\,\&\,\beta} & \dfrac{\Gamma\vdash\alpha}{\Gamma,\mathtt{tt}\vdash\alpha} & \dfrac{}{\Gamma\vdash\mathtt{tt}}
\end{array}$$

$$\begin{array}{llll}
(\Rightarrow\text{-R}) & (\Rightarrow\text{-L}) & \text{(COUNIT)} & \text{(PROMOTE)} \\
\dfrac{\Gamma,\beta\vdash\gamma}{\Gamma\vdash\beta\Rightarrow\gamma} & \dfrac{\Gamma\vdash\beta \quad \Gamma,\gamma\vdash\alpha}{\Gamma,\beta\Rightarrow\gamma\vdash\alpha} & \dfrac{\Gamma,\beta\vdash\alpha}{\Gamma,\Box_a\beta\vdash\alpha} & \dfrac{\Gamma\vdash\alpha}{\Gamma,\Delta\vdash\Box_a\alpha}\ \Gamma\ a\text{-available}
\end{array}$$

Fig. 1. Sequent calculus

Comultiplication is derived using AXIOM on $\Box_a\alpha$ followed by PROMOTE. Functoriality is derived using cut against COUNIT followed byPROMOTE. Principal naturality is derivable starting with AXIOM on α, using cut against COUNIT (on b) followed by PROMOTE. □

Remark 5 (Non-standard theorems). Sequences of nested modalities without intervening connectives can be exchanged, providing commutativity of principals.

$$\overline{\Box_b\Box_a\alpha\vdash\Box_a\Box_b\alpha}$$

COUNIT yields $\Box_a\Box_b\alpha\vdash\alpha$. The second case of definition 1 ensures that $\Box_a\Box_b\alpha$ is a-available, so use of PROMOTE yields $\Box_a\Box_b\alpha\vdash\Box_a\alpha$. The *third* case of definition 1 ensures that $\Box_a\Box_b\alpha$ is b-available, so use of PROMOTE yields the required result.

Let $A=\{a_0,a_1,\ldots,a_n\}$ be a set of principals. Using commutativity of principals, we can define, without ambiguity, $\Box_A\alpha\triangleq\Box_{a_0}\Box_{a_1}\cdots\Box_{a_n}\alpha$.

Another nonstandard new theorem is:

$$\overline{\alpha\Rightarrow\Box_a\beta\vdash\Box_a(\alpha\Rightarrow\Box_a\beta)}$$

Start with AXIOM on $\alpha\Rightarrow\Box_a\beta$. The *third* case of definition 1 ensures that $\alpha\Rightarrow\Box_a\beta$ is a-available since $\Box_a\beta$ is, so use of PROMOTE yields the required result. □

3 Noninterference

We prove noninterference in this section. Our proofs rely on normal forms for formulas. These normal forms are inspired by game semantics. A *unique result formula* is one whose game has a unique starting move. A *multiple result formula* may have multiple starting moves. In syntactic terms, a unique result formula does not have any conjunction at the ultimate result type.

$$\begin{aligned}
\delta &::= \mathtt{tt} \mid p,q \mid \mu\Rightarrow\delta \mid \Box_a\delta && \text{(Unique result formulas)}\\
\mu &::= \delta \mid \mu\,\&\,\delta \mid \delta\,\&\,\mu && \text{(Multiple result formulas)}
\end{aligned}$$

Any formula α is equivalent to a multiple result formula. This is proved by using the following distributivity laws:

$$\begin{array}{lcl} \Box_a(\alpha \mathbin{\&} \beta) & \Leftrightarrow & \Box_a\alpha \mathbin{\&} \Box_a\beta \\ \alpha \Rightarrow (\beta \mathbin{\&} \gamma) & \Leftrightarrow & (\alpha \Rightarrow \beta) \mathbin{\&} (\alpha \Rightarrow \gamma) \end{array}$$

Remark 6. Moving to multiple result formulas does not affect a-availability. Thus, $\Box_b$ $(\alpha \mathbin{\&} \beta)$ is a-available if and only if $\Box_b\alpha \mathbin{\&} \Box_a\beta$ is a-available. Similarly, $\alpha \Rightarrow (\beta \mathbin{\&} \gamma)$ is a-available if and only if $(\alpha \Rightarrow \beta) \mathbin{\&} (a \Rightarrow \gamma)$ is a-available.

Moving to multiple result formulas does not affect provability if axioms are used only on propositions. We use the following basic facts. An induction on the length of the proofs shows that if $\Gamma, \beta \mathbin{\&} \gamma \vdash \alpha$ is provable, then so is $\Gamma, \beta, \gamma \vdash \alpha$ by a proof of smaller length. Similarly, if $\Gamma \vdash \beta \mathbin{\&} \gamma$ is provable, then so are $\Gamma \vdash \beta$ and $\Gamma \vdash \gamma$ by proofs of smaller length.

For any formula α, let $(\alpha)^{\mathtt{mr}}$ be the equivalent multiple result formulas. Similarly, for any multiset of formulas Γ, let $(\Gamma)^{\mathtt{mr}}$ be the equivalent multiset of multiple result formulas. A simple induction on the length of the proof shows that if $\Gamma \vdash \alpha$ is provable, then there is a proof $(\Gamma)^{\mathtt{mr}} \vdash (\alpha)^{\mathtt{mr}}$ containing only multiple result formulas. As a sample case, consider the case when the last rule is $\Rightarrow$-R, so we have the following.

$$\overset{(\Rightarrow\text{-R})}{\frac{\Gamma, \beta \vdash \gamma_1 \mathbin{\&} \gamma_2}{\Gamma \vdash \beta \Rightarrow (\gamma_1 \mathbin{\&} \gamma_2)}}$$

In this case, we also have proofs of $\Gamma, \beta \vdash \gamma_1$ and $\Gamma, \beta \vdash \gamma_2$ of smaller length. So, by induction hypothesis, we have proofs of $(\Gamma, \beta)^{\mathtt{mr}} \vdash (\gamma_1)^{\mathtt{mr}}$ and $(\Gamma, \beta)^{\mathtt{mr}} \vdash (\gamma_2)^{\mathtt{mr}}$. Using $\Rightarrow$-R on each of these proofs followed by an application of &-R yields the required proof of $(\Gamma)^{\mathtt{mr}} \vdash (\beta \Rightarrow \gamma_1)^{\mathtt{mr}} \mathbin{\&} (\beta \Rightarrow \gamma_2)^{\mathtt{mr}}$. $\Box$

In the rest of this section, without loss of generality, we will assume that all the formulas are multiple result formulas and axioms are used only on propositions.

3.1 Translations of Formulas

We describe two translations $\langle\alpha\rangle_a^+$ and $\langle\alpha\rangle_a^-$ on multiple-result formulas by mutual recursion. Both translations yield pure IPL formulas without any modalities. The translation $\langle\cdot\rangle_a^-$ is closest in spirit to the extant treatment of the says monad [1], albeit with modifications designed to accommodate the differences arising from the necessity modality.

The translations share some common features: Both are structural and remove all modalities. Both "delete" information by replacing some chosen subformulas by `tt`.

The intuition is that both translations try to ensure that results of a-available formulas are not influenced by formulas that are not a-available. This is illustrated by considering the translation of $\alpha \Rightarrow \beta$ when β is a-available. In this case, the translations ensure that all the subformulas of α that are not a-available are replaced by `tt`. Viewing via the lens of game semantics, the translations replace the non a-available formulas by the empty game that interprets `tt`. Thus, the Opponent cannot move in these subformula occurrences. The upcoming preservation theorem (Theorem 13) shows that the proof also does not need to make moves in this proposition instance, i.e. this subformula instance is expendable to the proof.

$\langle\cdot\rangle^-_a$ enforces more constraints: it also replaces the results that are not *a*-available by `tt`.

Definition 7. For a formula α in multiple result normal form, define $\langle\alpha\rangle^+_a, \langle\alpha\rangle^-_a$ in IPL as follows.

$$\begin{array}{ll}
\langle \mathtt{tt}\rangle^+_a & = \mathtt{tt} \\
\langle p\rangle^+_a & = p \\
\langle \alpha \,\&\, \beta\rangle^+_a & = \langle\alpha\rangle^+_a \,\&\, \langle\beta\rangle^+_a \\
\langle \Box_b \alpha\rangle^+_a & = \langle\alpha\rangle^+_a \\
\langle \alpha \Rightarrow \beta\rangle^+_a & = \begin{cases} \langle\alpha\rangle^-_a \Rightarrow \langle\beta\rangle^+_a, & \beta\ a-\text{available} \\ \langle\alpha\rangle^+_a \Rightarrow \langle\beta\rangle^+_a, & \text{otherwise} \end{cases}
\end{array}
\qquad
\begin{array}{ll}
\langle \mathtt{tt}\rangle^-_a & = \mathtt{tt} \\
\langle p\rangle^-_a & = \mathtt{tt} \\
\langle \alpha \,\&\, \beta\rangle^-_a & = \langle\alpha\rangle^-_a \,\&\, \langle\beta\rangle^-_a \\
\langle \Box_b \alpha\rangle^-_a & = \begin{cases} \langle\alpha\rangle^-_a, & b \not\preceq a \\ \langle\alpha\rangle^+_a, & b \preceq a \end{cases} \\
\langle \alpha \Rightarrow \beta\rangle^-_a & = \langle\alpha\rangle^-_a \Rightarrow \langle\beta\rangle^-_a
\end{array}$$

These definitions extend pointwise to sets/multisets/sequences of formulas.

$$\langle\alpha_1,\ldots,\alpha_n\rangle^+_a = \langle\alpha_1\rangle^+_a,\ldots,\langle\alpha_n\rangle^+_a$$
$$\langle\alpha_1,\ldots,\alpha_n\rangle^-_a = \langle\alpha_1\rangle^-_a,\ldots,\langle\alpha_n\rangle^+_a$$

Consider propositions p. $\langle p\rangle^+_a$ is p since there are no constraints that need to be enforced. However, since p is not *a*-available, $\langle p\rangle^-_a$ is `tt`.

$\langle\cdot\rangle^+_a$ is fully compositional for all cases except implication $\alpha \Rightarrow \beta$ when β is *a*-available. In this case, we switch to $\langle\alpha\rangle^-_a$ to ensure that only *a*-available formulas influence *a*-available results.

$\langle\cdot\rangle^-_a$ is fully compositional for all cases except $\Box_b\alpha$ when $b \preceq a$. In this case, we switch to $\langle\alpha\rangle^+_a$ because the enclosing modality $\Box_b$ intuitively has satisfied the constraint of making the formula available to a, so we only need to enforce the constraints of $\langle\cdot\rangle^+_a$.

Example 8. (a) $\langle p \Rightarrow q\rangle^+_a = (p \Rightarrow q)$. (b) $\langle p \Rightarrow q\rangle^-_a = \mathtt{tt}$. (c) $\langle p \Rightarrow \Box_a q\rangle^+_a = \langle p \Rightarrow \Box_a q\rangle^-_a = (\mathtt{tt} \Rightarrow q)$ □

Remark 9. The translations $\langle\cdot\rangle^+_a$ and $\langle\cdot\rangle^-_a$ are not semantically robust. They do not respect equivalence of formulas. They have the desired properties explicated below only on formulas in multiple result normal form. □

The translations coincide on *a*-available formulas. This confirms the intuition that they differ only in the availability of the top-level formula.

Lemma 10. If α is a-available, then $\langle\alpha\rangle^+_a = \langle\alpha\rangle^-_a$. □

PROOF. By structural induction on α. The base cases for the induction are when α is of the form `tt` and $\Box_b\beta$ with $b \preceq a$. In these cases, $\langle\alpha\rangle^+_a = \langle\alpha\rangle^-_a$ by definition.
If β,γ are *a*-available: $\langle\beta \,\&\, \gamma\rangle^+_a = \langle\beta\rangle^+_a \,\&\, \langle\gamma\rangle^+_a = \langle\beta\rangle^-_a \,\&\, \langle\gamma\rangle^-_a = \langle\beta \,\&\, \gamma\rangle^-_a$
If γ is *a*-available: $\langle\beta \Rightarrow \gamma\rangle^+_a = \langle\beta\rangle^-_a \Rightarrow \langle\gamma\rangle^+_a = \langle\beta\rangle^-_a \Rightarrow \langle\gamma\rangle^-_a = \langle\beta \Rightarrow \gamma\rangle^-_a$
If $b \not\preceq a$ and β is *a*-available: $\langle\Box_b\beta\rangle^+_a = \langle\beta\rangle^+_a = \langle\beta\rangle^-_a = \langle\Box_b\beta\rangle^-_a$ □

The next two lemmas are the key technical drivers that motivate the consideration of normal forms for formulas in this proof. If the sole result of a single result formula is not a-available, the $\langle\cdot\rangle_a^-$ translation removes all non trivial information from it.

Lemma 11. If a unique result formula δ is not a-available, then $\langle\delta\rangle_a^- \Leftrightarrow \texttt{tt}$. □

PROOF. By structural induction on δ. If δ is of the form $\texttt{tt}$ or p, $\langle\delta\rangle_a^- = \texttt{tt}$ by definition. If δ is not a-available, for any α $\langle\alpha \Rightarrow \delta\rangle_a^- = \langle\alpha\rangle_a^- \Rightarrow \langle\delta\rangle_a^- = \langle\alpha\rangle_a^- \Rightarrow \texttt{tt}$; the result follows. If $b \not\preceq a$ and δ is not a-available: $\langle\Box_b\delta\rangle_a^- = \langle\delta\rangle_a^-$; the result follows by the induction hypothesis. □

We are now able to confirm that the $\langle\cdot\rangle_a^-$ translation is more restrictive than the $\langle\cdot\rangle_a^+$ translation.

Lemma 12. For all μ in multiple result form , $\langle\mu\rangle_a^+ \vdash \langle\mu\rangle_a^-$ is provable. □

PROOF.
Single Result Formulas: Consider first the case when μ is a formula δ in single result form. We prove the result by structural induction on the construction of δ.
If δ is of the form $\texttt{tt}$ or p. In these cases, result follows since $\langle\delta\rangle_a^- = \texttt{tt}$.
If δ is a-available: $\langle\beta \Rightarrow \delta\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^+ \Rightarrow \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^- = \langle\beta \Rightarrow \delta\rangle_a^-$
If δ is not a-available, $\beta \Rightarrow \delta$ is not a-available and result follows since $\langle\beta \Rightarrow \gamma\rangle_a^- = \texttt{tt}$ by lemma 11.
If $b \not\preceq a$: $\langle\Box_b\delta\rangle_a^+ = \langle\delta\rangle_a^+ \Rightarrow \langle\delta\rangle_a^- = \langle\Box_b\delta\rangle_a^-$
If $b \preceq a$: $\langle\Box_b\delta\rangle_a^+ = \langle\delta\rangle_a^+ = \langle\Box_b\delta\rangle_a^-$
Multiple result formulas. Given the result for single-result formulas, the proof for multiple result formulas μ follows by structural induction on the formation of μ. □

3.2 Noninterference Theorem

Theorem 13. Let Γ, α be formulas in multiple result form. If $\Gamma \vdash \alpha$, then:

$$\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+, \; \textit{and}$$
$$\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$$

are provable in intuitionist propositional logic. □

PROOF. Proof by induction on the structure of the proof of $\Gamma \vdash \alpha$.

Induction step for $\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$. The proofs for the inductive case when the last rule is any rule except COUNIT or PROMOTE are all similar. In each of these cases, the inductive step to show $\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$ follows because the translation $\langle(\cdot)\rangle_a^-$ is compositional on the structure of the propositional connectives and the universal quantifier.

For example consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta \;\&\; \gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad\qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta \;\&\; \gamma}$$

By inductive hypothesis, we deduce a proof of $\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^-$ and $\langle\Gamma\rangle_a^- \vdash \langle\gamma\rangle_a^-$. An application of &-R yields $\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^- \mathbin{\&} \langle\gamma\rangle_a^-$ thus completing this case since $\langle\alpha\rangle_a^- = \langle\beta\rangle_a^- \mathbin{\&} \langle\gamma\rangle_a^-$.

If the last rule is COUNIT, i.e.

$$\frac{\Gamma, \beta \vdash \alpha}{\Gamma, \Box_b \beta \vdash \alpha}$$

by induction hypothesis, we have a proof of $\langle\Gamma\rangle_a^-, \langle\beta\rangle_a^- \vdash \langle\alpha\rangle_a^-$. There are two cases depending on the order between b, a.

$b \preceq a$ By definition, $\langle\Box_b\beta\rangle_a^- = \langle\beta\rangle_a^+$. From lemma 12, $\langle\beta\rangle_a^+ \vdash \langle\beta\rangle_a^-$ is provable, so we get required result by use of CUT with the proof above yielded by the induction hypothesis.

$b \not\preceq a$. By definition, $\langle\Box_b\beta\rangle_a^- = \langle\beta\rangle_a^-$. Hence, the induction hypothesis yields the required result.

If the last rule is PROMOTE, i.e.

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \Box_b \alpha}\ \Gamma \text{ is } b\text{-available}$$

There are two cases depending on the order between b, a.

$b \preceq a$ By induction hypothesis on the $\langle\cdot\rangle_a^+$ translation, we have a proof of

$$\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

Since $b \preceq a$, by lemma 2, Γ is also a-available. So, by lemma 10, $\langle\Gamma\rangle_a^+ = \langle\Gamma\rangle_a^-$. Also, by definition, $\langle\Box_b\alpha\rangle_a^- = \langle\alpha\rangle_a^+$.

$b \not\preceq a$. By induction hypothesis, we have a proof of

$$\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$$

By definition, $\langle\Box_b\alpha\rangle_a^- = \langle\alpha\rangle_a^-$.

In either case, the required proof of $\langle\Gamma\rangle_a^- \vdash \langle\Box_b\alpha\rangle_a^-$ coincides with the proof yielded by the induction hypothesis. The additional formulas Δ on the left are added using weakening.

Induction step for $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$. The translation $\langle(\cdot)\rangle_a^+$ is compositional on the structure of & and the modality. So, if the last rule is any except ⇒-R or ⇒-L, the inductive step to show that $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$ holds follows immediately.

For example, consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta \mathbin{\&} \gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad\qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta \mathbin{\&} \gamma}$$

By inductive hypothesis, we deduce a proof of $\langle \Gamma \rangle_a^+ \vdash \langle \beta \rangle_a^+$ and $\langle \Gamma \rangle_a^+ \vdash \langle \gamma \rangle_a^+$. An application of &-R yields $\langle \Gamma \rangle_a^+ \vdash \langle \beta \rangle_a^+ \,\&\, \langle \gamma \rangle_a^+$. This completes this case of the proof since $\langle \alpha \rangle_a^+ = \langle \beta \rangle_a^+ \,\&\, \langle \gamma \rangle_a^+$.

If the last rule is $\Rightarrow$-R or $\Rightarrow$-L and the implication formula in question is $\beta \Rightarrow \gamma$, there are two cases based on whether γ is a-available or not.

If γ is not a-available, the $\langle \cdot \rangle_a^+$ translation is still compositional, i.e. $\langle \beta \Rightarrow \gamma \rangle_a^+ = \langle \beta \rangle_a^+ \Rightarrow \langle \gamma \rangle_a^+$ and the proof is similar to case above.

If γ is a-available, $\langle \beta \Rightarrow \gamma \rangle_a^+ = \langle \beta \rangle_a^- \Rightarrow \langle \gamma \rangle_a^+$.

$\Rightarrow$-R: The last rule is:

$$\frac{\Gamma, \beta \vdash \gamma}{\Gamma \vdash \beta \Rightarrow \gamma}$$

From induction hypothesis, we deduce the existence of a proof of

$$\langle \Gamma \rangle_a^-, \langle \beta \rangle_a^- \vdash \langle \gamma \rangle_a^-$$

and hence using $\langle \beta \Rightarrow \gamma \rangle_a^- = \langle \beta \rangle_a^- \Rightarrow \langle \gamma \rangle_a^-$, a proof of:

$$\langle \Gamma \rangle_a^- \vdash \langle \beta \Rightarrow \gamma \rangle_a^-$$

Since $\beta \Rightarrow \gamma$ is a-available, $\langle \beta \Rightarrow \gamma \rangle_a^- = \langle \beta \Rightarrow \gamma \rangle_a^+$ by lemma 10. So, we deduce :

$$\langle \Gamma \rangle_a^- \vdash \langle \beta \Rightarrow \gamma \rangle_a^+$$

From lemma 12, the sequents $\langle \alpha \rangle_a^+ \vdash \langle \alpha \rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut, we get a proof of: $\langle \Gamma \rangle_a^+ \vdash \langle \beta \Rightarrow \gamma \rangle_a^+$ as required.

$\Rightarrow$-L: The last rule is:

$$\frac{\Gamma \vdash \beta \qquad \Gamma, \gamma \vdash \alpha}{\Gamma, \beta \Rightarrow \gamma \vdash \alpha}$$

From induction hypothesis, we deduce the existence of proofs:

$$\langle \Gamma \rangle_a^- \vdash \langle \beta \rangle_a^- \qquad\qquad \langle \Gamma \rangle_a^+, \langle \gamma \rangle_a^+ \vdash \langle \alpha \rangle_a^+$$

From lemma 12, the sequents $\langle \alpha \rangle_a^+ \vdash \langle \alpha \rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut with the left proof, we get a proof of:

$$\langle \Gamma \rangle_a^+ \vdash \langle \beta \rangle_a^-$$

Using $\Rightarrow$-L with the right proof above yields a proof of:

$$\langle \Gamma \rangle_a^+, \langle \beta \rangle_a^- \Rightarrow \langle \gamma \rangle_a^+ \vdash \langle \alpha \rangle_a^+$$

Required result follows since $\langle \beta \Rightarrow \gamma \rangle_a^+ = \langle \beta \rangle_a^- \Rightarrow \langle \gamma \rangle_a^+$. □

The main use of this theorem is to prove that certain sequents are not provable. We illustrate with very simple examples.

Example 14. In all the following examples, we use theorem 13 for $\langle\cdot\rangle_a^-$.

- If $p \vdash \Box_a p$ is provable, so is $\texttt{tt} \vdash p$.
- Let $b \not\leq a$. If $\Box_b p \vdash \Box_a p$ is provable , so is $\texttt{tt} \vdash p$ in IPL.
- Let $b \not\leq a$. If $\Box_b p, \Box_a(p \Rightarrow q) \vdash \Box_a q$ is provable, so is $\texttt{tt}, p \Rightarrow q \vdash q$.

Since $\texttt{tt} \vdash p$ and $p \Rightarrow q \vdash q$ are unprovable in IPL, all the above three sequents are unprovable. $\Box$

4 Conclusions

Recent research in both type theories and security have used indexed necessity modalities of intuitionist S4 as the logical foundations. Noninterference between the different indices is a key metatheoretic property that is essential to the soundness of this modeling. In this paper, we establish noninterference for indexed intuitionist necessity modalities.

Our work is inspired by noninterference theorems for monads—logically speaking, the "says" modality from logics for access control. However, to the best of our knowledge, noninterference has not been investigated for the necessity modality. The dual of the necessity modality is not the says modality but the possibility modality. So, our proof incorporates novelties in the form of normal forms for intuitionist S4 inspired by game semantics.

Our desire is to ultimately build a similar metatheory for a modal logic that incorporates *both* kinds of modalities. Such logics are already used for security policies and in type theories for functional languages.

This research was supported by NSF CCF-0915704.

References

1. Abadi, M.: Access control in a core calculus of dependency. ENTCS 172, 5–31 (2007)
2. Abadi, M., Banerjee, A., Heintze, N., Riecke, J.G.: A core calculus of dependency. In: POPL, pp. 147–160 (1999)
3. Abadi, M., Burrows, M., Lampson, B.W., Plotkin, G.D.: A calculus for access control in distributed systems. ACM Trans. Program. Lang. Syst. 15(4), 706–734 (1993)
4. Abramsky, S., Jagadeesan, R.: Game semantics for access control. ENTCS 249, 135–156 (2009)
5. Alechina, N., Mendler, M., de Paiva, V., Ritter, E.: Categorical and Kripke Semantics for Constructive S4 Modal Logic. In: Fribourg, L. (ed.) CSL 2001. LNCS, vol. 2142, pp. 292–307. Springer, Heidelberg (2001)
6. Bierman, G.M., de Paiva, V.C.V.: On an intuitionistic modal logic. Studia Logica 65 (2000, 2001)
7. DeYoung, H., Pfenning, F.: Reasoning about the consequences of authorization policies in a linear epistemic logic. Technical Report 1213, CMU-CS (2009)
8. Garg, D., Bauer, L., Bowers, K.D., Pfenning, F., Reiter, M.K.: A Linear Logic of Authorization and Knowledge. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 297–312. Springer, Heidelberg (2006)

9. Garg, D., Pfenning, F.: Non-interference in constructive authorization logic. In: CSFW, pp. 283–296 (2006)
10. Goubault-Larrecq, J., Goubault, E.: On the geometry of intutionist s4 proofs. Homology, Homotopy and Applications 5(2), 137–209 (2003)
11. Hughes, G.E., Cresswell, M.J.: An introduction to modal logic (1972)
12. Malecha, G., Chong, S.: A more precise security type system for dynamic security tests. In: Proceedings of the 5th ACM SIGPLAN PLAS Workshop, PLAS 2010, pp. 4:1–4:12 (2010)
13. Nanevski, A.: A Modal Calculus for Exception Handling. In: Intuitionistic Modal Logics and Applications Workshop (IMLA 2005), Chicago, IL (June 2005)
14. Pfenning, F., Wong, H.-C.: On a modal λ-calculus for S4. In: Proc. of the Eleventh MFPS. ENTCS, vol. 1 (1995)
15. Tse, S., Zdancewic, S.: Translating dependency into parametricity. In: Proc. of the Ninth ACM ICFP, ICFP 2004, pp. 115–125 (2004)

A Factoring the Translation

The translations $\langle\cdot\rangle_a^+$ and $\langle\cdot\rangle_a^-$ can be factored into two pieces:

- Translations $(|\cdot|)_a^+$ and $(|\cdot|)_a^-$ remove principals and result in formulas in the fragment of our logic that uses modalities indexed only by a. Thus, the target of this translation is a variant of Intutionist S4.
- The standard forgetful translation from Intuitionist S4 into intuitionist propositional logic simply erases all modalities.

For a formula α in multiple result normal form, define $(|\alpha|)_a^+, (|\alpha|)_a^-$ as follows. The only differences are in the cases for the modality.

$$\begin{array}{ll}
(|\mathtt{tt}|)_a^+ & = \mathtt{tt} \\
(|p|)_a^+ & = p \\
(|\alpha \mathbin{\&} \beta|)_a^+ & = (|\alpha|)_a^+ \mathbin{\&} (|\beta|)_a^+ \\
(|\Box_b \alpha|)_a^+ & = \begin{cases} (|\alpha|)_a^+, & b \not\preceq a \\ \Box_a (|\alpha|)_a^+, & b \preceq a \end{cases} \\
(|\alpha \Rightarrow \beta|)_a^+ & = \begin{cases} (|\alpha|)_a^- \Rightarrow \langle\beta\rangle_a^+, & \beta\ a-\text{available} \\ (|\alpha|)_a^+ \Rightarrow \langle\beta\rangle_a^+, & \text{otherwise} \end{cases}
\end{array}$$

$$\begin{array}{ll}
(|\mathtt{tt}|)_a^- & = \mathtt{tt} \\
(|p|)_a^- & = \mathtt{tt} \\
\langle\alpha \mathbin{\&} \beta\rangle_a^- & = (|\alpha|)_a^- \mathbin{\&} (|\beta|)_a^- \\
(|\Box_b \alpha|)_a^- & = \begin{cases} (|\alpha|)_a^-, & b \not\preceq a \\ \Box_a (|\alpha|)_a^+, & b \preceq a \end{cases} \\
\langle\alpha \Rightarrow \beta\rangle_a^- & = \langle\alpha\rangle_a^- \Rightarrow \langle\beta\rangle_a^-
\end{array}$$

We are able to prove the analogue of theorem 13. If $\Gamma \vdash \alpha$, then:

$$\begin{array}{l}
(|\Gamma|)_a^+ \vdash (|\alpha|)_a^+, \text{ and} \\
(|\Gamma|)_a^- \vdash (|\alpha|)_a^-
\end{array}$$

are provable. The proof uses the analogues for Lemmas 10–12 that are listed below.

1. If α is a-available, then $(|\alpha|)_a^+ = (|\alpha|)_a^-$; furthermore, $(|\alpha|)_a^+$ is a-available.
2. If a single result formula δ is not a-available, then $(|\delta|)_a^- = \mathtt{tt}$.
3. For all μ in multiple result form , $(|\mu|)_a^+ \vdash (|\mu|)_a^-$ is provable.

Many-Valued Logics, Fuzzy Logics and Graded Consequence: A Comparative Appraisal

Soma Dutta[1], Sanjukta Basu[2], and Mihir Kr. Chakraborty[3]

[1] IBRAD, Kolkata, India
somadutta9@gmail.com
[2] Rabindra Bharati University, Kolkata, India
juktab@gmail.com
[3] Jadavpur University and Indian Statistical Institute, Kolkata, India
mihirc4@gmail.com

Abstract. In this paper a comparative study of many-valued logics, fuzzy logics and the theory of graded consequence has been made focussing on consequence, inconsistency and sorites paradox.

1 Introduction

What brings many-valued logic, fuzzy logic and theory of graded consequence (GCT) on a common platform is that each considers bivalence inadequate and embraces multivalence for interpreting their proposed theories. Traditionally, different systems of many-valued logic admitted values other than truth and falsehood from different motivations. The second and the third decade of the last century saw a sprouting of different systems of many-valued logic. However, treatment of vagueness was far from the original motive behind any of these many-valued systems [18]. Generally the set of truth values admitted in different systems of many-valued logic is some subset of the real interval [0, 1].

For Zadeh's proposed system of fuzzy logic based on fuzzy set theory [21], the unit interval [0, 1] was a natural choice for interpreting vague sentences which occur either as premises or as conclusions of inferences in most cases of human reasoning. A further development of fuzzy logic in a more formal way was carried out in [10–14, 16].

A general set up for generating a system of logics with a notion of graded consequence was proposed by Chakraborty [3, 4] to gauge the strength of 'derivability' of a conclusion from a set of premises which may hold in degrees. Where the approach of GCT differs from other many-valued and fuzzy logical approaches is that it admits degrees of truth not only of predications at the object level, but of predications at the meta-level and if required at a level higher than that also.

In this paper a comparative study of many-valued logics, fuzzy logics and the theory of graded consequence has been made focussing on consequence, inconsistency and sorites paradox. We arrange the content of the paper in three different sections; the fisrt two focus on the notions of 'consequence', 'inconsistency', and the last one on the treatment of 'Sorites paradox'.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 197–209, 2013.

2 Notion of Consequence: A Comparative Appraisal

Existing approaches towards reasoning with imprecise concepts allow the object level to be many-valued, while maintaining meta-level statements to be of yes/no type. A comment made by Pelta [17] is relevant in this regard: "*Until now the construction of superficial many-valued logics, that is, logics with an arbitrary number (bigger than two) of truth values but always incorporating a binary consequence relation, has prevailed in investigations of logical many-valuedness*".

In contrast, the philosophy behind GCT is: '*if object level formulae are having many-valued truth values then it generally cannot be denied that meta-level sentences also happen to be so*' [3].

One may wonder what could be the motivation for incorporating grade in metalanguage. After all metalinguistic sentences are of mathematical nature. One immediate answer may be given from the standard of mathematics itself viz., generalization, which is a usual motivation behind mathematical research, and that has been echoed in the above quote. We may recall the history of many-valued logics itself. Though for incorporation of a third value there had been various extraneous reasons e.g. inclusion of future contingents, or taking 'undecided' and 'unknown' also as (truth) values of sentences, there had been no apparent reason for extension to an infinite set of truth values. This was simply generalization as done in mathematical practice. The infinite value set obtained a meaning only in mid-sixties after the advent of fuzzy set theory [21] and incorporation of vague predicates also in logic and computer applications. But a more down-to-earth reason may be given. Since seventies, primarily because of the needs of computer scientists the classical notion of consistency was being felt to be inadequate for application. Notions of partial consistency, and inconsistency tolerant systems were brought in within the discourse [8, 2]. In traditional logic consistency is a hard notion yielding either 'yes' or 'no' answers. Thus consistency to a certain degree was a concept quite naturally waiting at the door steps in search of a theory. Linking consistency with consequence is a long-practised methodology in classical logic. A similar approach with graded (in)consistency automatically leads to graded consequence. Apart from all these, if we examine the nature of actual (not normative) inferences made by human brain we notice that from certain premises the brain often makes inferences not very strongly. The procedure itself might have weakness, tentativeness and vagueness. Cases of medical decision making offer ample instances.

2.1 Theory of Graded Consequence Relation

A graded consequence relation is a fuzzy relation, say $|\!\sim$ between the power set of formulae $P(F)$ and F satisfying the following set of axioms [3, 4].

(GC1) If $\alpha \in X$ then $gr(X \mid\!\sim \alpha) = 1$ (Reflexivity).

(GC2) If $X \subseteq Y$ then $gr(X \mid\!\sim \alpha) \leq gr(Y \mid\!\sim \alpha)$ (Monotonicity).

(GC3) $\inf_{\beta \in Y} gr(X \mid\!\sim \beta) * gr(X \cup Y \mid\!\sim \alpha) \leq gr(X \mid\!\sim \alpha)$ (Cut).

The intended meaning of '$gr(X \mid\!\sim \alpha)$' is the truth value of the meta-linguistic sentence 'α is a consequence of X'. This value is not necessarily the topmost (1) or the least (0) of the lattice, the value set, and it is read as ‘the degree to which α is a consequence of X’. The ‘$*$’ and ‘inf’ used in (GC3) are the operators for computing the meta-linguistic ‘**and**’ and ‘**for all**’ present in the statement ‘**for all** $\beta \in Y$, $X \vdash \beta$ **and** $X \cup Y \vdash \alpha$ *imply* $X \vdash \alpha$’, the classical cut condition. $|\!\sim$ is the many-valued counterpart of $\vdash$, the two-valued notion of ‘consequence’. To elucidate, let us consider formulae $\alpha, \beta, \ldots$ and sets of formulae $X, Y, \ldots$ as object level entities. Then in meta level, one can form sentences of the form ‘X’ $|\!\sim$ ‘α’, ‘X’$|\!\sim x$, $x \in$‘X’, where ‘X’, ‘α’ are the terms of the meta level language representing the names of the respective object level entities, x is a meta level variable ranging over object level formulae, and $\in$, $|\!\sim$ are predicates of the meta level language. So, the cut condition, which is a meta-meta level statement, in symbols can be presented as *imply*($\ulcorner \forall x($**if** $x \in$ ‘Y’**then** ‘X’ $|\!\sim x)$ **and** ‘$X \cup Y$’$|\!\sim$‘α’ $\urcorner$, $\ulcorner$ ‘X’$|\!\sim$‘α’ $\urcorner$), where expressions within $\ulcorner\ \urcorner$ are meta level sentences and at meta-meta level those sentences are named is in quotes $\ulcorner\ \urcorner$. So, expressions with $\ulcorner\ \urcorner$ are meta-meta linguistic terms and ‘*imply*’ is a meta-meta linguistic predicate. The lattice order relation ‘$\leq$’ takes care of the meta-meta level relation ‘*imply*’. Hence, in graded context (GC3) ascertains that the truth value of the meta level sentence $\forall x($**if** $x \in$ ‘Y’**then** ‘X’ $|\!\sim x)$ **and** ‘$X \cup Y$’$|\!\sim$‘α’ is less or equal to the truth value of the sentence ‘X’ $|\!\sim$ ‘α’. The value set say, L along with the operators for meta linguistic connectives forms a complete residuated lattice $(L, *, \rightarrow, 0, 1)$.

That logic activity, generally, comprises of three levels, namely, object, meta and meta-meta, and proper distinction between them plays a crucial role in establishing well-formedness of a sentence pertaining to a specific level have been discussed elaborately in [7].

From the semantic angle the graded counterpart of the notion of consequence is a generalization of the notion of semantic consequence proposed by Shoesmith and Smiley [19]. Classically, ‘α is a semantic consequence of X’ is defined by the meta-linguistic sentence ‘for all T_i belonging to the collection of all state-of-affairs, if all members of X are true under T_i, then α is true under T_i’. In [19], the definition has been generalized by replacing the constraint of ‘all state-of-affairs’ by ‘any collection of state-of-affairs’, say $\{T_i\}_{i \in I}$. A rationale for taking an arbitrary collection of state-of-affairs according to [19] is: ‘*the necessity with which conclusions follow is relative to the presuppositions of an argument, and different argument may have different presuppositions. But whatever idea of necessity is involved there is a corresponding idea of possibility*’. This leads to the new version viz., ‘*To say that a conclusion follows from a given set of premises is to say that each possible state-of-affairs in which all the premises are true is one in which the conclusion is true*’ [19]. Instead of presuppositions we prefer to use the more general word ‘context’. So each $\{T_i\}_{i \in I}$ constitutes a context, which may be treated as a collection of worlds of Kripke semantics. Besides, from the angle of pure mathematics, a passage from all valuations to arbitrary number of valuations is an elegant generalization.

In GCT, $\{T_i\}_{i \in I}$ represents any collection of fuzzy sets assigning values to the formulae. Thus, the proposed logic turns out to be context dependent. The meta-level sentence for semantic consequence, i.e., $(\Sigma) \quad \forall T_i\{X \subseteq T_i \rightarrow_m \alpha \in T_i\}$, is evaluated by the expression $\inf_i\{\inf_{\gamma \in X} T_i(\gamma) \rightarrow T_i(\alpha)\}$, where $\inf_{\gamma \in X} T_i(\gamma)$, $T_i(\alpha)$ are the respective values of the meta level sentences '$X \subseteq T_i$' and '$\alpha \in T_i$' (see [4, 6]), and $\rightarrow$ is the residuum of $*$, the monoidal operator of $(L, *, \rightarrow, 0, 1)$, computing $\rightarrow_m$, the meta-linguistic 'if-then'. It is to be noted that the value assigned to the meta-linguistic sentence 'α is a semantic consequence of X' can also be explained maintaining the proper distinction between levels [7].

So, in graded context 'α is a semantic consequence of X', denoted by $X \mid\approx \alpha$, is not a crisp notion; rather, it is a matter of grade and the value of $X \mid\approx \alpha$, i.e., $gr(X \mid\approx \alpha) = \inf_i\{\inf_{\gamma \in X} T_i(\gamma) \rightarrow T_i(\alpha)\}$. In [4], a soundness-completeness like result has been proved connecting a graded consequence relation $\mid\sim$ axiomatized by (GC1) to (GC3) with $\mid\approx$, the semantic counterpart.

The notion of axiomatic graded consequence [5], is determined with respect to $\mathcal{A}$, a logical base of axioms and $\mathcal{R}$, rules. A context, say $\{T_i\}_{i \in I}$, determining the truth values of the basic formulae needs to be prefixed also. The tautologihood degree of the axioms present in $\mathcal{A}$ and degree of the rules present in $\mathcal{R}$ depend on $\{T_i\}_{i \in I}$. The tautologihood degree of an axiom α is $inf_i T_i(\alpha)$, which is the value of the meta-linguistic sentence '$\forall_T\ (\alpha \in T)$'. To illustrate the degree of a rule, let us consider the rule Modus Ponens (MP). For all instances of $(\{\alpha, \alpha \supset \beta\}, \beta)$, the degree to which β is related to $\{\alpha, \alpha \supset \beta\}$ is $\inf_{\alpha,\beta} gr(\{\alpha, \alpha \supset \beta\} \mid\approx \beta)$ i.e., $\inf_{\alpha,\beta}\inf_i\{(T_i(\alpha) \wedge T_i(\alpha \supset \beta)) \rightarrow T_i(\beta)\}$, which is the degree of the rule MP. Now, given a pair $(\mathcal{A}, \mathcal{R})$, where say, $\mathcal{R}$ consists of MP only, a derivation of a formula α_n from a set of formulae X, is an ordered pair of sequences viz. $(\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle, \langle \mid \alpha_1 \mid, \mid \alpha_2 \mid, \ldots, \mid \alpha_n \mid \rangle)$. In this pair of sequences the first sequence consists of formulae used in the derivation and the second sequence indicates the values associated with each step. The value associated with i-th step will be 1 if α_i comes from the premise X. The value will be tautologihood degree of α_i if α_i is taken from $\mathcal{A} \setminus X$ and $|\alpha_i|$ will be the degree of MP if α_i is obtained by applying MP on the previous formulae $\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}$. The value of the meta-linguistic sentence '$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ is a derivation of α_n from X', formally written as $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle D(X, \alpha_n)$, is $\mid \alpha_1 \mid * \mid \alpha_2 \mid * \ldots * \mid \alpha_n \mid$. Finally, the value of the meta level sentence 'α_n is an axiomatic consequence of X', that is 'there is a sequence of formulae which is a derivation of α_n from X', is computed by $\sup_{\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle} \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle D(X, \alpha_n)$. This notion of axiomatic graded consequence satisfies (GC1)-(GC3) [5].

The above discussion explains that in GCT assignment of values to sentences like, 'α is a consequence of X', whether it be axiomatic or semantic, is not arbitrary; it depends on the sentence unfolding the meaning of the concept.

2.2 Notion of Consequence in Many-Valued Logics

In many-valued logics, the notion of semantic consequence is defined usually in two ways; one, say '$\models_1$', is defined in terms of a designated subset of the set of values of the wffs and the other, say '$\models_2$', is defined in terms of the order relation present in the value set and a composition operator conjoining the values of the premises. Let us now concentrate on the definition of $\models_1$.

According to the definition of $\models_1$, $X \models_1 \alpha$ iff for the collection of all valuations, say $\{T_i\}_{i\in I}$ mapping formulae to $[0,1]$, for all $\gamma \in X$, $T_i(\gamma) \in D$ i.e. $T_i(X) \subseteq D$, implies $T_i(\alpha) \in D$, where D, the designated set of values, is a proper subset of $[0,1]$ not containing 0.

There is no ambiguity regarding the two-valued nature of the notion of semantic consequence of many-valued logics. Let us see how this notion of semantic consequence is placed in the proposed scheme for graded semantic consequence. In order to cast the definition in our sense, let us do the following construction. Let for each T_i, T_i^D be a mapping defined by, $T_i^D(\alpha) = 1$, if $T_i(\alpha) \in D$
$= 0$, otherwise.

Identifying, the function T_i^D with the set it determines, the above definition reduces to 'for all T_i^D, $X \subseteq T_i^D$ implies $\alpha \in T_i^D$'.

Theorem. Given the collection of all valuations, say $\{T_i\}_{i\in I}$, $|\!\approx$ generated by $\{T_i^D\}_{i\in I}$ with the operator $\to_c$, defined by $a \to_c b = 1$, if $a \leq b$
$= 0$ otherwise,
computing the meta-level implication $\to_m$ of (Σ) coincides with $\models_1$.

Theorem. $|\!\approx$ generated by $\{T_i^D\}_{i\in I}$, in the above mentioned sense, is a graded consequence relation.

These two theorems give a general scheme for reproducing the completeness theorem of many-valued logics in terms of GCT by fixing $\{T_i^D\}_{i\in I}$ to be the context determining the tautologihood degrees and degrees of rules of $(\mathcal{A}, \mathcal{R})$, the axiomatic base of the particular logic of concern.

2.3 Notion of Consequence in Fuzzy Logics

Most of the mainstream fuzzy logics frequently use the term 'degree of consequence', but does not really mean the notion of consequence is graded. The idea of approximate rule prevalent in fuzzy logics may illustrate the point.

2.3.1 Modus Ponens as a Special Case of Derivation in Fuzzy Logics

As introduced by Goguen [12] the approximate rule Modus Ponens is such that "*If you know P is true at least to the degree a and P ⊃ Q at least to the degree b then conclude that Q is true at least to the degree a.b.*"

Assuming the value set for formulae as [0, 1] and '.' as the usual product operation, the above-mentioned approximate rule takes the form:

$$\frac{\begin{array}{l}(P,\ a)\\ (P \supset Q,\ b)\end{array}}{(Q,\ a.b)}$$

Fig. 1.

That is, as proposed by Goguen, a many-valued rule of inference can be viewed as a crisp relation from $P(F \times [0,1])$ to $(F \times [0,1])$.

Pavelka's [16] interpretation of a many-valued rule of inference is as follows. A many-valued rule of inference r consists of two components $\langle r', r'' \rangle$, where the first (grammatical) component r' operates on formulae and the second (evaluation) component r'' operates on truth values and says *how the truth value of the conclusion is to be computed from the truth values of the premises.*

So, it is clear from Pavelka's own words that the value, which is being attached to the concluding formula, is the *truth value of the conclusion* - not of the 'so called' many-valued rule. Pavelka, himself puts a many-valued rule MP in a form which is similar to the form presented above.

'From partially true premises partially true conclusion can be deduced'- this is the central idea of Peter Hajek's [14] fuzzy logical system, known as Rational Pavelka Logic (RPL). Identifying the pair (P, a) with the formula $\overline{a} \supset P$, where $\overline{a}$ is the wff denoting the truth value a, it can be shown that the many-valued rule MP mentioned in **Fig. 1** can be obtained as a derived rule in RPL.

So, from the above discussion it is evident that neither Goguen, nor Pavelka, nor Hajek considered a rule of inference in fuzzy context as a fuzzy relation between a set of formulae and a single formula. And this is clearly not the case in the context of graded consequence (see section 2.1). One can argue that presentation of a fuzzy rule in the form of **Fig. 1** is nothing but a variant form of writing the same rule as a fuzzy relation say, $MP(\{(\alpha, a)(\alpha \supset \beta, b)\}\ \beta)$ with relatedness grade $a.b$ or $r''(a, b)$. In this connection readers are referred to [7] where it has been observed that if the principle of 'use and mention' of a symbol is to be maintained then this correspondence gives rise to a difficulty in placing a rule as a well-formed concept of the meta level language.

Rule being a special case of derivation, it can be guessed that 'consequence' in fuzzy logic is such that given a set of formulae, along with their truth values, a formula with certain truth value either can be derived or not derived. However, the way '$C(X)(\alpha)$' is read in fuzzy logic creates a confusion.

This becomes more visible if one goes through the distinction of levels maintaining the principle of 'use' and 'mention' of a symbol in a logical discourse [7]. A formula α, a set of formulae X - all these are linguistic elements of level-0. **'**α**'** is a consequence of **'**X**'**, **'**X**'** is inconsistent - these are level-1 statements, and value of these statements should be computed by a reasonable, definite method as it is maintained for computing values of level-0 formulae. This is exactly lacking in the understanding of the meta level concepts of the existing fuzzy logics.

2.3.2 Notion of Provability in Hajek's Rational Pavelka Logic

According to Hajek [14] the notion of 'provability degree of a formula α from a set of formulae X' is given by the value $\sup\{r : X \vdash (\alpha, r)\}\ \ldots (\mathrm{A})$.

In RPL, (α, r) is a level-0 formula and hence one can place $X \vdash (\alpha, r)$ in level-1. For a crisp set X of formulae, given a crisp set of axioms and crisp rules of inference, a formula of the form '(α, r) is a derivation of X', is a two-valued notion. So what does this 'provability degree of α from X' mean? The definition (A) suggests to compute the supremum of all those r for which (α, r) is derived from X. This leads to a number of problems.

1. It should be natural to think that, the provability degree of a formula α from a set of formulae X would be the truth value of the statement 'α is provable

from X' i.e., 'there is a derivation of α from X'. But expression (A) does not seem to compute this sentence.
2. As 'sup' usually is meant to compute meta-linguistic 'there exists' to make the definition of 'α is provable from X' closer to the expression (A) if we assume that (A) is assumed to compute the sentence 'there is a derivation of (α, r) from X', then also difficulty arises because, $X \vdash (\alpha, r)$ is a two-valued notion. So, how does this 'r' come in the scenario to get counted under 'sup'?
3. Semantically, $X \vdash (\alpha, r)$ means in every model of X, the value of α should be at least r. This fact can not be unfolded at the same level where $X \vdash (\alpha, r)$ lies.

2.3.3 Notion of Proof in the Context of Pavelka's Fuzzy Logic

The notion of proof, as introduced by Pavelka [16], also has some difficulties. Given a fuzzy set $\mathcal{A}$ of formulae, interpreted as axioms and a set $\mathcal{R}$ of rules of inference, an $\mathcal{R}$-proof is defined as a finite non-empty string $\omega = \langle \omega_1, \omega_2, \ldots, \omega_n \rangle$ over $\mathrm{F} \cup (\ \mathrm{F} \times \{\ 0\ \}\ ) \cup (\ \mathrm{F} \times \mathcal{R} \times N^+\ )$. That is for each ω_i $(i = 1, 2, \ldots, n)$ either ω_i is (x) or $(x, 0)$ or $(x, r, \langle i_1, i_2, \ldots, i_n \rangle)$, where $x = \lceil \omega_i$, the formula under consideration at the i-th term of ω.

If $\omega_i = (x, r, \langle i_1, i_2, \ldots, i_n \rangle)$, $(i = 1, 2, \ldots, n)$ then $x = r'$ $(\lceil \omega_{i_1}, \lceil \omega_{i_2}, \ldots, \lceil \omega_{i_n})$ where r' is the grammatical component of the rule r (see Section 2.3.1). For an $\mathcal{R}$-proof $\omega = \langle \omega_1, \omega_2, \ldots, \omega_n \rangle$ of $\lceil \omega_n$ from a fuzzy set of formulae X there is a function $\widehat{\omega} : L^F \mapsto L$ such that (i) if length of ω is 1, then either $\omega = (x)$ or $(x, 0)$. If $\omega = (x)$ then $\widehat{\omega}(X) = Xx$ i.e. the membership degree of x in the fuzzy subset X and if $\omega = (x, 0)$ then $\widehat{\omega}(X) = \mathcal{A}x$ i.e. the membership degree of x in the fuzzy set of axioms $\mathcal{A}$. (ii) If $\omega = \langle \omega_1, \omega_2, \ldots, \omega_n \rangle$ then

$$\begin{array}{ll} \widehat{\omega}(X) = Xx & \text{if } \omega_n = (x) \\ \quad = \mathcal{A}x & \text{if } \omega_n = (x, 0) \\ \quad = r''(\widehat{\omega}_{i_1}(X), \widehat{\omega}_{i_2}(X), \ldots, \widehat{\omega}_{i_n}(X)) & \text{if } \omega_n = (x, r, \langle i_1, \ldots, i_n \rangle),\ i_1, \ldots, i_n < n. \end{array}$$

So, it can be noticed that the value of $\langle \omega_1, \omega_2, \ldots, \omega_n \rangle$, a proof of $\lceil \omega_n$ from X, only takes care of the value of the last step of the derivation. This does not seem to be the value of the sentence '$\langle \omega_1 \rangle$ is a proof of $\lceil \omega_1$ from X **and** $\langle \omega_1, \omega_2 \rangle$ is a proof of $\lceil \omega_2$ from X **and** ... **and** $\langle \omega_1, \omega_2, \ldots, \omega_n \rangle$ is a proof of $\lceil \omega_n$ from X'.

Like any definition by recursion, in Pavelka's definition of proof also value of each step is computed with the help of the value of a segment of the proof preceeding that particular step. But 'proof' as a whole should refer to the complete chain of steps and the same applies to the value of proof too. In the context of graded consequence value of a proof is not computed by recursion.

2.3.4 Łukasiewicz Fuzzy Propositional Logic

In Łukasiewicz fuzzy propositional logic [1] concepts like $\text{Fuzzy}_{\text{Ł}}$ entailment, degree entailment, n-degree entailment, fuzzy consequence are introduced.

A formula α is a $\text{Fuzzy}_{\text{Ł}}$ entailment of a set of formulae Γ if for every fuzzy truth-value assignment, which is a fuzzy set from the set of all formulae to the set [0, 1], if every member of Γ gets the value 1 then α gets the value 1. It is quite clear that the notion of $\text{Fuzzy}_{\text{Ł}}$ degree entailment is actually the same as the $\models_1$ where the designated set is $\{1\}$, and $\models_1$ is a two-valued concept.

On the other hand, α is said to be a degree entailment of Γ if for any fuzzy truth-value assignment, the infimum of the values assumed by all members of Γ is less or equal to the value obtained by α. This coincides with the definition of $\models_2$ when the lattice meet is taken to be the composition operator conjoining the premises. An argument is said to be degree valid if its premises degree entails its conclusion. So, degree entailment and degree valid both are 'yes/no concepts'.

Then in [1], for an argument which is not degree valid, a notion like approximate degree of validity has been introduced. Given an argument having Γ as the set of premises and α as the conclusion, and a fuzzy truth-value assignment V, a function say d_V, called downward distance, has been defined by
$d_V(\Gamma, \alpha) = \inf_{\gamma \in \Gamma} V(\gamma) - V(\alpha)$, if $\inf_{\gamma \in \Gamma} V(\gamma) - V(\alpha) > 0$
$= 0$, otherwise.
Now the argument is said to be n-degree valid if $n = 1 - \sup_V d_V(\Gamma, \alpha)$. So, here an attempt to attach a value to the meta-linguistic notion 'an argument is valid' is found. But this again proposes a method of computation which does not have any connection with the defining criterion of the concept 'an argument is valid'. Also presence of '$-$' implies that the definition only applies in [0, 1].

The notion of fuzzy consequence defined in [1], is exactly the same as the notion of semantic consequence defined by Pavelka [16]. Given a fuzzy set of formulae Γ, the fuzzy consequence of Γ, denoted by $FC(\Gamma)$, is a fuzzy set such that for any formula α, $FC(\Gamma(\alpha)) = \inf_T\{T(\alpha) : \Gamma \subseteq T\}$. In [7], it has been discussed that in presenting $FC(\Gamma(\alpha))$ according to the scheme (Σ), given in section 2.1, one needs to have two implication operators to compute the meta-linguistic connective 'if-then' present in the notion viz., '[**if** for all T, (for all γ (**if** $\gamma \in \Gamma$ **then** $\gamma \in T$)) **then** $\alpha \in T$]'. So, one may be skeptic in accepting $FC(\Gamma)(\alpha)$ as a proper reading for 'degree of consequence of α from Γ'.

So, in GCT the value of 'α is a consequence of X' happens to be the value of its defining sentence, while the other existing fuzzy logics proposed to attach such a value which cannot be claimed as the value of its defining sentence.

3 Notion of Inconsistency: A Comparative Appraisal

If object level formulae are accepted to assume values other than 0 and 1, then it is quite immediate that a formula and its negation need not be false together. So, one can think of a non-zero threshold for a formula of the form $\alpha \wedge \neg\alpha$. For instance, in Łukasiewicz logic [18] this value is $\frac{1}{2}$. Then what about the notions like, 'for any α, $\{\alpha, \neg\alpha\} \vdash \beta$ for any β' or '$\{\alpha, \neg\alpha\}$ is inconsistent'? Let us briefly revisit the notion of inconsistency in the logics of our present concern.

3.1 Inconsistency in the Theory of Graded Consequence

The classical notion of inconsistency, in the graded context, has been assumed [5] as a fuzzy subset $INCONS$ of $P(F)$. Given any set of formulae X, $INCONS(X)$, read as the inconsistency degree of X, is postulated [5] by the following axioms.
(I1) If $X \subseteq Y$ then $INCONS(X) \leq INCONS(Y)$.

(I2) $INCONS(X \cup \{\neg\alpha\}) * INCONS(X \cup Y) \leq INCONS(X)$ for any $\alpha \in Y$.
(I3) There is some $k > 0$ such that for any α, $INCONS(\{\alpha, \neg\alpha\}) \geq k$.

This notion of graded inconsistency is equivalent to the notion of graded consequence, extended with the axioms (GC4) and (GC5)[5].
(GC4) There is some $k > 0$ such that for any α, $inf_\beta\ gr(\{\alpha, \neg\alpha\} \mid\!\sim \beta) \geq k$.
(GC5) $gr(X \cup \{\alpha\} \mid\!\sim \beta) * gr(X \cup \{\neg\alpha\} \mid\!\sim \beta) \leq gr(X \mid\!\sim \beta)$.

So, the point to be noted here is that the classical connection between consequence and inconsistency is preserved in this context too, where both the notions of consequence and inconsistency are matters of grades.

3.2 Notion of Inconsistency in Many-Valued/fuzzy Logics

In Pavelka's fuzzy logical system though $C(X)(\alpha)$ has been regarded as the degree to which α is a consequence of X, the notion of consistency (inconsistency) has been introduced absolutely crisply. According to Pavelka [16], a fuzzy set of formulae X is said to be consistent if $C(X) \neq F$, and inconsistent otherwise. So, no question of grade arises here.

On the other hand, in Ha$\acute{j}$ek's fuzzy logic [14], a set of formulae X is said to be inconsistent if $X \vdash 0$ i.e. $X \vdash \overline{0} \supset 1$ or in other words, $X \vdash (\overline{0}, 1)$.

At this point, the question which arises is that if, for some set X of formulae, $X \vdash (\overline{0}, r)$, where $r \neq 1$, whether the underlying logic of Ha$\acute{j}$ek accepts the set X as a partially inconsistent set. As understood from [14], the answer seems to be 'no'. This definition reflects that Ha$\acute{j}$ek also intended to introduce the notion of inconsistency as a two-valued concept. This attitude towards the notion of inconsistency, found in both of these fuzzy logical systems, poses question. Because there are tacit mentions of the terms like, 'degree of consequence', 'provability degree' etc., in both of these systems and if these terms are really genuine in addressing many-valuedness of 'the notion of consequence' then how can they be commensurable to 'the notion of inconsistency' which is a two-valued concept.

4 Solution to Sorites Paradox: A Comparative Appraisal

A sorites paradox involving a vague predicate P can be stated as follows.
One starts with Px_1 and a collection of conditional premises of the form 'if Px_i, then Px_{i+1}', for $1 \leq i \leq n$. Then, by repetitive application of MP, one arrives at the obviously false conclusion Px_n, for some suitably large n.

4.1 Sorites Paradox: In the Context of Tye's Many-Valued Logic

Michael Tye [20] adopts a three-valued semantics framed after Kleene's three-valued logic. The third value is called 'indefinite'. Tye observed that there are borderline bald men with say, n hairs, who would not cease to be bald by addition of one hair on his head. Thus, there is some n, for which both the statements 'a man with n hairs on his head is bald' and 'a man with $n + 1$ hairs on his head is bald' are indefinite. Hence according to Kleene's three-valued matrix for 'if-then' ('$\supset$'), for such n, the conditional statement 'if a man with n hairs on his head is bald then a man with $n+1$ hairs on his head is bald' will be indefinite.

According to Tye, the initial few statements in the array, having the form 'a man with n hairs on his head is bald', where n ranges from 0 to 1,000,000, are true, also the last few statements of the same form are false, and in between somewhere in the array, there are statements that are indefinite. But one could never say where in the array, the statements of the form 'a man with n hairs on his head is bald' cease to be true and become indefinite, and also at which point in the array indefinite statements end and false statements begin.

Tye's approach respects tolerance of a vague predicate to minute changes. But by admitting one of the premises to be non-true he dissolves the paradox instead of giving any solution to the paradoxical situation where starting from true premises, following a valid rule(s) of inference, one arrives at a false conclusion.

4.2 Sorites Paradox: in the Context of Goguens's Fuzzy Logic

As an example of fuzzy logical approach to the sorites paradox, we present Goguen's [12] approach based on fuzzy set theory. According to Goguen, the conditional statements of the form 'if a man with i hairs on his head is bald then a man with j hairs on his head is bald' should provide a way so that from the truth value of 'a man with i hairs on his head is bald' one can derive the truth value of the statement' a man with j hairs on his head is bald'. He suggested to represent the conditional premise by a fuzzy relation $H(i, j)$, read as, 'the relative baldness of a man with j hairs on his head with respect to the baldness of a man with i hairs on his head' so that $H(i, j)$ satisfies the following equation. $B(j) = H(i, j) \,.\, B(i)$, where '$B$' denotes a fuzzy set corresponding to 'bald'. That is, $H(i, j) = \frac{B(j)}{B(i)}$. Now, as the fuzzy set B, representing 'bald' is continuous and monotone decreasing in nature, for some k, $H(k-1, k)$ is non-unit. Hence, if $B(0)$ is 1, then for the series of natural numbers, from 0 to 1,000,000, $B(1,000,000) = \prod_{i=1}^{1,000,000} H(i-1, i)$, which is a result of repetitive product of non-unit numbers and that might be close to zero as the number of steps increases. This explains why the conclusion of the sorites appears to be false.

There are two problems in this solution. The first is the same as in Tye's case, where one of the premises is admitted to be non-true. The second is the case where it is admitted that for some k, $H(k-1, k)$ is non-unit, i.e. $B(k-1) < B(k)$. This goes against the idea that a vague predicate is tolerant to mintue changes.

4.3 Sorites Paradox: In the Context of Graded Consequence

According to GCT, solution to the Sorites paradox can be presented as below.

1. A man with 1 hair on his head is bald. ...1

2. A man with 1 hair on his head is bald $\supset$ A man with 2 hairs on his head is bald. ...1

3. A man with 2 hairs on his head is bald. ...$|\ MP\ |$

$\vdots$

2×1,000,000 +1. A man with 1,000,000 hairs on his head is bald. ...$|\ MP\ |$

Hence from the given premises, the conclusion 'A man with 1,000,000 hairs on his head is bald' can be derived to the degree $\mid MP \mid * \mid MP \mid * \ldots * \mid MP \mid$, taking the value associated with each step under consideration. Now, to compute the truth value of the conditional sentence of the form 'A man with m hairs on his head is bald $\supset$ A man with $m + 1$ hairs on his head is bald' an implication operator, say $\rightarrow_o$ is needed. Any standard fuzzy implication operator satisfies $a \rightarrow_o b \geq b$. Now, to compute the degree of the rule MP, all possible cases of $\{\alpha, \alpha \supset \beta\}$ implies β have to be considered. As T_i's are the fuzzy subsets interpreting the vague predicate 'bald' for some α representing a sentence of the form 'A man with m hairs on his head is bald' and some β representing a sentence, say 'A man with n hairs on his head is bald' for some $m < n$, $T_i(\alpha) > T_i(\beta)$. So, as $T_i(\alpha) \rightarrow_o T_i(\beta) \geq T_i(\beta)$ we have $T_i(\alpha) \wedge (T_i(\alpha) \rightarrow_o T_i(\beta)) \geq T_i(\beta)$. It is to be noted that not for all $\rightarrow_o$, $a \wedge (a \rightarrow_o b)$ is necessarily b. Hence for some α, β, $\{T_i(\alpha) \wedge (T_i(\alpha) \rightarrow_o T_i(\beta))\} \rightarrow T_i(\beta)$ is not equals to 1. That is, the calculation for the grade of MP given in Section 2.1 indicates that $\mid MP \mid$ is not necessarily 1. So, in this context, as indicated by the calculation above, the value of the derivation of the conclusion approaches to zero as the number of steps increases. And the point to be noted here is that, the conditional statements of the form 'A man with m hairs on his head is bald $\supset$ A man with $m + 1$ hairs on his head is bald' need not get a non-unit truth value; more specifically, the truth value 1 may be assigned to them, always.

Edgington [9] also embraces a degree-theoretic approach to give an account of reasoning in vague context. What distinguishes her approach from other degree theories, including GCT, is that it uses probability theory as providing a general structure for calculating logical compositions (not necessarily truth functional) of different degrees of verity of sentences. In her approach, each conditional premise of the form '$Px_n \supset Px_{n+1}$ has a degree of verity slightly less than clearly true (1). However, as the deduction proceeds small unverities (1 - degree of verity) of the premises mount up to yield a conclusion which is clearly false (0). Yet each step of the argument is valid; because, the unverity of the conclusion never exceeds the sum of the unverities of the premises. This is how Edgington distinguishes arguments, where fall in the values of the conclusion is constrained by the values of the premises, from 'genuinely invalid' arguments, where such constraint does not work.

Hence, in opposition to Tye's many-valued approach, Goguen's fuzzy approach, and Edgington's degree-theoretic approach, GCT neither needs to assume one of the premises to be non-true, nor needs to assume existence of a cut off point violating the linguistic rule for vague predicates.

5 Conclusion

In summing up we can say, in many-valued and fuzzy logics, 'consequence' is either a crisp notion or it has been assigned a grade which does not seem to be the 'truth value' of the concept underlying it, or it fails to preserve the classical consequence-inconsistency connection. GCT makes a point of difference here.

Sorites, a long chain of arguments involving a vague predicate is a paradoxical phenomenon in the context of reasoning in vague/imprecise context. In section 4, we have seen that the idea of a 'paradox' is getting distorted in both Tye's three valued approach and Goguen's fuzzy set theoretic approach to sorites paradox. Besides, Goguen's proposal of assigning a non-unit truth value to some of the conditional premises seems to negate that vague predicates are tolerant to minute changes. The same is the case with Edgington's approach.

Before ending, we would like to quote a line from Parikh [15] who in a different manner proposed a system of logic dealing with vague sentences. As a point of note against the 'so called' fuzzy approach to deal with observationality (property of a vague predicate, whose impreciseness cannot even be removed theoretically) he commented "*... we seem to have come no closer to observationality by moving from two valued logic to real valued, fuzzy logic. A possible solution ... is to use continuous valued logic not only for the object language but also for the metalanguage.*"

In addition to the above, the theory of graded consequence insists that the method of assigning grades to the meta concepts needs to respect the underlying meanings of these concepts.

References

1. Bergmann, M.: An Introduction to Many-valued and Fuzzy Logic: Semantics, Algebras and Derivation Systems. Cambridge University Press (2008)
2. Bertossi, L., Hunter, A., Schaub, T.: Introduction to Inconsistency Tolerance. In: Bertossi, L., Hunter, A., Schaub, T. (eds.) Inconsistency Tolerance. LNCS, vol. 3300, pp. 1–14. Springer, Heidelberg (2005)
3. Chakraborty, M.K.: Use of fuzzy set theory in introducing graded consequence in multiple valued logic. In: Gupta, M.M., Yamakawa, T. (eds.) Fuzzy Logic in Knowledge-Based Systems, Decision and Control, pp. 247–257. Elsevier Science Publishers, B.V., North Holland (1988)
4. Chakraborty, M.K.: Graded Consequence: further studies. Journal of Applied Non-Classical Logics 5(2), 127–137 (1995)
5. Chakraborty, M.K., Basu, S.: Graded Consequence and some Metalogical Notions Generalized. Fundamenta Informaticae 32, 299–311 (1997)
6. Chakraborty, M.K., Dutta, S.: Graded Consequence Revisited. Fuzzy Sets and Systems 161, 1885–1905 (2010)
7. Chakraborty, M.K., Dutta, S.: Grade in Metalogical Notions: a Comparative Study of Fuzzy Logics. Mathware and Soft Computing (accepted)
8. Dunn, P.E., et al.: Inconsistency tolerance in weighted argument systems. In: Decker, Sichman, Sierra, Castelfranchi (eds.) Proc. of 8th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2009), Budapest, Hungary, May 10-15, pp. 851–858 (2009)
9. Edgington, D.: Vagueness by degrees. In: Keefe, R., Smith, P. (eds.) Vagueness: A Reader, pp. 294–316. MIT Press, Massachusetts (1997)
10. Esteva, E., Godo, L., Noguera, C.: On Completeness results for Predicate Łukasiewicz, Product, Gödel and Nilpotent Minimum Logics expanded with truth constants. Mathware and Soft Computing XIV(3), 233–246 (2007)

11. Gerla, G.: Fuzzy Logic: Mathematical Tools for Approximate Reasoning. Kluwer Academic Publishers (2001)
12. Goguen, J.A.: The logic of inexact concepts. Synthese 19, 325–373 (1968)
13. Gottwald, S.: An Approach to Handle Partially Sound Rules of Inference. In: Bouchon-Meunier, B., Yager, R.R., Zadeh, L.A. (eds.) IPMU 1994. LNCS, vol. 945, pp. 380–388. Springer, Heidelberg (1995)
14. Hájek, P.: Metamathematics of Fuzzy Logic. Kluwer Academic Publishers (1998)
15. Parikh, R.: The Problem of Vague Predicates. In: Cohen, R.S., Wartofsky, M. (eds.) Language, Logic, and Method, pp. 241–261. D. Ridel Publishing Company (1983)
16. Pavelka, J.: On fuzzy logic I, II, III Zeitscher for Math. Logik und Grundlagen d. Math. 25, 45–52, 119–134, 447–464 (1979)
17. Pelta, C.: Wide Sets, Deep Many-valuedness and Sorites Arguments. Mathware and Soft Computing 11, 5–11 (2004)
18. Rescher, N.: A Survey of Many-valued Logic. Mc.Graw-Hill Book Company, New York (1969)
19. Shoesmith, D.J., Smiley, T.J.: Multiple Conclusion Logic. Cambridge University Press (1978)
20. Tye, M.: Sorites paradoxes and the semantics of vagueness. In: Tomberlin, J.E. (ed.) Philosophical Perspectives 8: Logic and Language, pp. 189–206. Ridgeview Publishing Co., Atascadero (1994)
21. Zadeh, L.A.: Fuzzy sets. Information and Control 8, 338–353 (1965)

Fuzzy Preorder, Fuzzy Topology and Fuzzy Transition System

S.P. Tiwari and Anupam K. Singh

Department of Applied Mathematics
Indian School of Mines
Dhanbad-826004, India
{sptiwarimaths,anupam09.bhu}@gmail.com
http://www.ismdhanbad.ac.in

Abstract. The purpose of this work is to show that the observations made regarding fuzzy transition systems can be easily obtained by using the fuzzy preordered and fuzzy topological concepts.

1 Introduction and Preliminaries

The study of fuzzy automata was initiated by Wee [25] and Santos [21] in 1960's after the introduction of fuzzy set theory by Zadeh [26]. Much later, a considerably simpler notion of a fuzzy finite state machine (which is almost identical to a fuzzy automaton) was introduced by Malik, Mordeson and Sen [14, 15]. Somewhat different notions were introduced subsequently in [6, 7, 8, 9, 10, 18]. In these studies, the membership values in the closed interval $[0, 1]$ were considered. During the recent years, the researchers began to work on fuzzy automata with membership values in complete residuated lattices, lattice-ordered monoids and some other kind of lattices [4, 11, 12, 16, 17, 19, 20].

Recently, in [5] the concept of fuzzy transition systems (fuzzy finite automata over residuated lattice, in the sense of [14]) were introduced and studied. The concept of subsystems of a fuzzy transition system proposed in [5] is a natural generalization of the concept of subsystem introduced in [14], whose topological study was done in [2, 24].

In this paper, we introduce and study the concepts of fuzzy preordered set and fuzzy topology (in which the fuzzy sets have the membership values in resiaduated lattice) and then show that the results shown in [5] are easy consequences of results shown for fuzzy preordered set and fuzzy topology. Also, we point out that some new results for fuzzy transition systems can be obtained with the help of fuzzy preordered sets. In [5] the concept of direct sum of fuzzy transition systems were proposed. Here, in this paper, chiefly inspired from [23], we introduce the concept of product of fuzzy transition systems and show that this product is a categorical product.

Now, we recall the following concepts of residuated lattice from [1].

Definition 1. *A **residuated lattice** is an algebra $\mathcal{L} = (L, \wedge, \vee, \otimes, \rightarrow, 0, 1)$ such that*

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 210–219, 2013.

(i) $(L, \wedge, \vee, 0, 1)$ *is a lattice with the least element* 0 *and the greatest element* 1*,*
(ii) $(L, \otimes, 1)$ *is a commutative monoid with unit* 1*, and*
(iii) $\otimes$ *and* $\rightarrow$ *form an adjoint pair, i.e., for all* $x, y, z \in L, x \otimes y \leq z \Leftrightarrow x \leq y \rightarrow z$*.*

If, in addition $(L, \vee, \wedge, 0, 1)$ *is a complete lattice, then* $\mathcal{L}$ *is called a* **complete residuated lattice***.*

The precomplement on L is the mapping $\neg : L \longrightarrow L$ such that $\neg x = x \rightarrow 0, \forall x \in X$. Some of the basic properties of complete residuated lattices, which we use, are as follows:

(i) $a \otimes b \leq c \Leftrightarrow a \leq b \rightarrow c$;
(ii) $1 \rightarrow a = a$;
(iii) $(a \rightarrow b) \otimes (b \rightarrow c) \leq a \rightarrow c$;
(iv) $a \otimes b \rightarrow c = a \rightarrow (b \rightarrow c)$;
(v) $a \otimes (\vee_{i \in J} b_i) = \vee_{i \in J}(a \otimes b_i)$.

The concepts of fuzzy sets, fuzzy relations, fuzzy topologies and fuzzy transition systems, we study in this paper, have the membership values in a complete residuated lattice. For example, a *fuzzy subset* of a nonempty set X is a function from X to L and a *fuzzy relation* on X is a function from $X \times X$ to L. Throughout, L^X denotes the family of all fuzzy subsets of X and $\underline{\alpha}$ denotes the α-valued constant fuzzy subset of X.

2 Fuzzy Preordered Set and Fuzzy Topology

The concept of fuzzy topology induces by upper sets of a fuzzy preordered sets with the membership values in $[0, 1]$ has been introduced and studied in [27]. In this section, we study the concepts associated with upper(lower) sets of a fuzzy preordered set with the membership values in a complete residuated lattice. We show that the collection of upper(lower) sets of a fuzzy preordered set form a fuzzy topology. We begin with the following concept of fuzzy preordered set.

Definition 2. [22] *Let* R *be a fuzzy relation on* X*. Then* R *is called*

(i) **reflexive** *if* $\forall x \in X, R(x, x) = 1$, and
(ii) **transitive** *if* $\forall x, y, z \in X, R(x, y) \otimes R(y, z) \leq R(x, z)$.

A reflexive and transitive fuzzy relation is called a **fuzzy preorder**. If R is a fuzzy preorder on X, then the pair (X, R) is called a **fuzzy preordered set**.

Given a fuzzy preordered set (X, R), let $R^{op} \in L^{X \times X}$ such that $R^{op}(x, y) = R(y, x)$. Then (X, R^{op}) is also a fuzzy preordered set.

Definition 3. *Let* (X, R) *be a fuzzy preorderd set. Then* $\lambda \in L^X$ *is called an* **upper set** *of* (X, R) *if* $\lambda(x) \otimes R(x, y) \leq \lambda(y), \forall x, y \in X$*. Dually,* $\lambda \in L^X$ *is called a* **lower set** *of* (X, R) *if* $\lambda(y) \otimes R(x, y) \leq \lambda(x), \forall x, y \in X$*.*

Upper sets of a fuzzy preorderd set appear under several different names in the literature (cf., [27]). One can easily observe that $\lambda \in L^X$ is an upper set of fuzzy preordered set (X, R) if and only if λ is a lower set of (X, R^{op}).

Proposition 1. *Let* (X, R) *be a fuzzy preordered set. Then* $\lambda \in L^X$ *is an upper set of* (X, R) *if and only if* $\lambda : (X, R) \longrightarrow (L, \rightarrow)$ *is an order preserving map.*

Proof. Let $\lambda \in L^X$ be an upper set of fuzzy preordered set (X, R). Then $\lambda(x) \otimes R(x, y) \leq \lambda(y), \forall x, y \in X$, or that $R(x, y) \leq \lambda(x) \rightarrow \lambda(y), \forall x, y \in X$. Thus $\lambda : (X, R) \longrightarrow (L, \rightarrow)$ preserves order. Converse follows similarly.

Proposition 2. $\lambda \in L^X$ *is a lower set of a fuzzy preordered set* (X, R) *if and only if* $\lambda : (X, R^{op}) \longrightarrow (L, \rightarrow)$ *is an order preserving map.*

Proof. Similar to that of Proposition 1.

Proposition 3. *Let* (X, R) *be a fuzzy preordered set and* $z \in X$*. Then* $[z]^R \in L^X$ *such that* $[z]^R(x) = R(z, x)$ *is an upper set of* (X, R) *and* $[z]_R \in L^X$ *such that* $[z]_R(x) = R(x, z)$ *is a lower set of* (X, R)

Proof. Follows from the transitivity of R.

Proposition 4. *Let* λ *be an upper(lower) set in a fuzzy preordered set* (X, R)*. Then for each* $a \in L, \lambda \rightarrow a$ *is a lower (upper) set in* (X, R)*.*

Proof. Let λ be an upper set of a fuzzy preordered set (X, R). Then $\lambda(x) \otimes R(x, y) \leq \lambda(y), \forall x, y \in X$. To show that $\lambda \rightarrow a$ is a lower set, it is enough to show that $(\lambda(y) \rightarrow a) \otimes R(x, y) \leq \lambda(x) \rightarrow a, \forall x, y \in X$, or that $(\lambda(y) \rightarrow a) \otimes R(x, y) \otimes \lambda(x) \leq a, \forall x, y \in X$. Now, $(\lambda(y) \rightarrow a) \otimes R(x, y) \otimes \lambda(x) \leq (\lambda(y) \rightarrow a) \otimes \lambda(y) \leq a$. Thus $\lambda \rightarrow a$ is a lower set. Similarly, it can be prove that if λ is a lower set of a fuzzy preordered set (X, R), then for each $a \in L, \lambda \rightarrow a$ is an upper set of (X, R).

Proposition 5. *Let* λ *be an upper(lower) set in a fuzzy preordered set* (X, R)*. Then for each* $a \in L, a \otimes \lambda$ *is a upper (lower) set in* (X, R)*.*

Proof. Let λ be an upper set of a fuzzy preordered set (X, R) and $a \in L$. Then $\lambda(x) \otimes R(x, y) \leq \lambda(y), \forall x, y \in X$, which implying that $a \otimes \lambda(x) \otimes R(x, y) \leq a \otimes \lambda(y), \forall x, y \in X$. Thus $a \otimes \lambda$ is an upper set in (X, R). The proof for the case of lower set follows similarly.

The following is the concept of fuzzy topology in the sense of Lowen [13].

Definition 4. *A* **fuzzy topology** τ *on* X *is a subset of* L^X*, which is closed under arbitrary suprema and finite infima and which contains all constant fuzzy sets. The fuzzy sets in* τ *are called* **open**.

Proposition 6. *If* (X, R) *is a fuzzy preordered set then the family* τ *of its all upper sets satisfies the following conditions,* $\forall \lambda_i \in \tau$ *and* $\forall \alpha \in L$*:*

(i) $\underline{\alpha} \in \tau$,
(ii) $\vee_{i \in J}\lambda_i \in \tau$,
(iii) $\wedge_{i \in J}\lambda_i \in \tau$.

Proof. (i) is obvious. Let $\lambda_i \in \tau, i \in J$. Then $\lambda_i(x) \otimes R(x, y) \leq \lambda_i(y), \forall x, y \in X$ and $\forall i \in J$. Now, $(\vee_{i \in J}\lambda_i(x)) \otimes R(x, y) = \vee_{i \in J}(\lambda_i(x) \otimes R(x, y)) \leq \vee_{i \in J}\lambda_i(y)$. Thus $\vee_{i \in J}\lambda_i \in \tau$. Also, $(\wedge_{i \in J}\lambda_i(x)) \otimes R(x, y) \leq \lambda_i(x) \otimes R(x, y) \leq \lambda_i(y), \forall i \in J$. Thus $(\wedge_{i \in J}\lambda_i(x)) \otimes R(x, y) \leq \wedge_{i \in J}\lambda_i(y)$. Hence $\wedge_{i \in J}\lambda_i \in \tau$.

Thus the family of upper sets of a fuzzy preordered set (X, R) forms a fuzzy topology on X, which we shall denoted by τ_R. The family of lower sets of a fuzzy preordered set also form a fuzzy topology, which is given below.

Proposition 7. *If (X, R) is a fuzzy preordered set then the family τ of its all lower sets satisfies the following conditions, $\forall \lambda_i \in \tau$ and $\forall \alpha \in L$:*

(i) $\underline{\alpha} \in \tau$,
(ii) $\vee_{i \in J}\lambda_i \in \tau$,
(iii) $\wedge_{i \in J}\lambda_i \in \tau$.

The following gives the characterization of fuzzy relation of fuzzy preordered set through it's upper sets.

Proposition 8. *Let $\mathcal{F}$ be the family of all upper sets of a fuzzy preordered set (X, R). Then $R(x, y) = \wedge\{\lambda(x) \to \lambda(y) : \lambda \in \mathcal{F}\}, \forall x, y \in X$.*

Proof. Let λ be an upper set of fuzzy preordered set (X, R). Then for all $x, y \in X, \lambda(x) \otimes R(x, y) \leq \lambda(y)$, or that $R(x, y) \leq \lambda(x) \to \lambda(y)$, i.e., $R(x, y) \leq \wedge\{\lambda(x) \to \lambda(y) : \lambda \in \mathcal{F}\}$. Also for $z \in X$, as $z^R(x)$ is an upper set in (X, R), $\wedge\{z^R(x) \to z^R(y) : z \in X\} \leq R(x, x) \to R(x, y) = 1 \to R(x, y) = R(x, y)$. Thus $\wedge\{\lambda(x) \to \lambda(y) : \lambda \in \mathcal{F}\} \leq R(x, y)$. Hence $R(x, y) = \wedge\{\lambda(x) \to \lambda(y) : \lambda \in \mathcal{F}\}, \forall x, y \in X$.

Proposition 9. *Let $\mathcal{F}'$ be the family of all lower sets of a fuzzy preordered set (X, R). Then $R(x, y) = \wedge\{\lambda(y) \to \lambda(x) : \lambda \in \mathcal{F}'\}, \forall x, y \in X$.*

Proof. Similar to that of Proposition 8.

Proposition 10. *Let λ be an upper (lower) set of a fuzzy preordered set (X, R). Then for each $a \in L, a \to \lambda$ is an upper(lower) set in (X, R).*

Proof. Let $x, y \in X$. Then $(a \to \lambda(x)) \otimes (\lambda(x) \to \lambda(y)) \leq (a \to \lambda(y)$, or that $(\lambda(x) \to \lambda(y)) \leq (a \to \lambda(x)) \to (a \to \lambda(y))$. Thus $R(x, y) \leq (a \to \lambda(x)) \to (a \to \lambda(y))$ (cf., Proposition 8), whereby $(a \to \lambda(x)) \otimes R(x, y) \leq a \to \lambda(y)$. Hence $a \to \lambda$ is an upper set in (X, R).

Before stating next, recall from [5] that for fuzzy relations $R, S \in L^{X \times X}$, their *composition* $R \circ S$ is a fuzzy relation on X given by $(R \circ S)(x, y) = \vee\{R(x, z) \otimes S(z, y) : z \in X\}$.

Proposition 11. *Given a fuzzy preordered set* (X, R)*,* $\lambda \in L^X$ *is an upper set if and only if* λ *is a solution to a fuzzy relational equation* $\chi \circ R = \chi$*, where* $\chi \in L^X$ *is an unknown.*

Proof. Let λ be an upper set of a fuzzy preordered set (X, R). Then $\lambda \circ R \leq \lambda$. Also, from the reflexivity of R, $\lambda \leq \lambda \circ R$. Thus $\lambda \circ R = \lambda$, or that λ is a solution of fuzzy relational equation $\chi \circ R = \chi$. Converse is trivial.

Proposition 12. *Given a fuzzy preordered set* (X, R)*,* $\lambda \in L^X$ *is a lower set if and only if* λ *is a solution to a fuzzy relational equation* $R \circ \chi = \chi$*, where* $\chi \in L^X$ *is an unknown.*

Proof. Similar to that of Proposition 11.

Proposition 13. *Let* (X, R) *be a fuzzy preordered set and* $\lambda \in L^X$*. Then*

(i) if λ *is an upper set,* $\neg\lambda$ *is a lower set, and*
(ii) if λ *is a lower set,* $\neg\lambda$ *is an upper set.*

Proof. (i) Let λ be an upper set in fuzzy preordered set (X, R). Then for all $x, y \in X, \lambda(x) \otimes R(x, y) \leq \lambda(y)$, or that $\neg(\lambda(x) \otimes R(x, y)) \geq \neg\lambda(y)$. Now, $\neg(\lambda(x) \otimes R(x, y)) \geq \neg\lambda(y) \Rightarrow (\lambda(x) \otimes R(x, y)) \to 0 \geq \neg\lambda(y) \Rightarrow (R(x, y) \otimes \lambda(x)) \to 0 \geq \neg\lambda(y) \Rightarrow R(x, y) \to (\lambda(x)) \to 0) \geq \neg\lambda(y) \Rightarrow R(x, y) \to \neg\lambda(x) \geq \neg\lambda(y) \Rightarrow \neg\lambda(y) \otimes R(x, y) \leq \neg\lambda(x)$. Thus $\neg\lambda$ is a lower set.

(ii) The proof is similar as above.

Remark 1. Let $\neg$ be involutive. Then $\lambda \in L^X$ is an upper set if and only if $\neg\lambda$ is a lower set.

Definition 5. *A map* $f : (X, R) \longrightarrow (Y, S)$ *between fuzzy preordered sets is called* **order preserving** *if* $R(x, y) \leq S(f(x), f(y)), \forall x, y \in X$*.*

Proposition 14. *Let the map* $f : (X, R) \longrightarrow (Y, S)$ *between fuzzy preordered sets be order preserving. Then inverse image of an upper(lower) set of* (Y, S) *is an upper(lower) set of* (X, R)*.*

Proof. Let $x, y \in X$ and $\lambda \in L^Y$ be an upper set of (Y, R). Then $f^{-1}(\lambda)(x) \otimes R(x, y) \leq \lambda(f(x)) \otimes R(x, y) \leq \lambda(f(x)) \otimes S(f(x), f(y)) \leq \lambda(f(y)) \leq f^{-1}(\lambda)(y)$. Thus $f^{-1}(\lambda)$ is an upper set of (X, R).

3 Fuzzy Topology and Fuzzy Transition System

In this section, we show that the results for fuzzy transition systems introduced in [5] are easy consequences of the results shown in the previous section for fuzzy preordered sets and fuzzy topologies. Finally, we introduce the concept of product of fuzzy transition systems and show that this product is a categorical product. We begin with the following concept of fuzzy transition system introduced in [5].

Definition 6. *A* ***fuzzy transition system*** *is a triple $\mathcal{T} = (Q, X, \delta)$, where Q is a nonempty set (of states of $\mathcal{T}$), X is a monoid (the input monoid of $\mathcal{T}$) whose identity shall be denoted as e, and δ is an L-valued subset of $Q \times X \times Q$, i.e., a map $\delta : Q \times X \times Q \to L$ such that $\forall p, q \in Q$,*

$$\delta(q, e, p) = \begin{cases} 1 \text{ if } q = p \\ 0 \text{ if } q \neq p \end{cases}$$

and, $\delta(q, xy, p) = \vee\{\delta(q, x, r) \otimes \delta(r, y, p) : r \in Q\}, \forall x, y \in X$.

We now introduce the following concept of homomorphism between fuzzy transition systems (which is identical to homomorphism between fuzzy automata introduced in [14]).

Definition 7. *A* **homomorphism** *from a fuzzy transition system (Q, X, δ) to a fuzzy transition system (R, Y, λ) is a pair (f, g) of maps, where $f : Q \to R$ and $g : X \to Y$ are functions such that*

$$\forall (q, x, p) \in Q \times X \times Q, \quad \lambda(f(q), g(x), f(p)) \geq \delta(q, x, p).$$

It can be seen that the class of all fuzzy transition systems and their homomorphisms forms a category **FTS** (under obvious composition of maps).

Definition 8. *A* ***reverse fuzzy transition system*** *of a fuzzy transition system $\mathcal{T} = (Q, X, \delta)$ is a fuzzy transition system $\bar{\mathcal{T}} = (Q, X, \bar{\delta})$, where $\bar{\delta} : Q \times X \times Q \to L$ is a map such that $\bar{\delta}(p, x, q) = \delta(q, x, p), \forall p, q \in Q$ and $\forall x \in X$.*

Definition 9. *Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system. Then $\lambda \in L^Q$ is called*

- *(i) a* **subsystem** *of $\mathcal{T}$ if $\lambda(p) \otimes \delta(p, x, q) \leq \lambda(q), \forall p, q \in Q$ and $\forall x \in X$;*
- *(ii) a* **reverse subsystem** *of $\mathcal{T}$ if $\lambda(q) \otimes \delta(p, x, q) \leq \lambda(p), \forall p, q \in Q$ and $\forall x \in X$.*
- *(iii) a* **double subsystem** *of $\mathcal{T}$ if it is both subsystem and reverse subsystem of $\mathcal{T}$.*

Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system. Define $R_\delta(p, q) = \vee\{\delta(p, x, q) : x \in X\}, p, q \in Q$. Then R_δ is a fuzzy preorder on Q. Now, we have the following.

Proposition 15. *Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system and $\lambda \in L^Q$. Then the following are equivalent:*

- *(i) λ is a subsystem of $\mathcal{T}$.*
- *(ii) λ is τ_{R_δ}-open.*
- *(iii) λ is a solution to a fuzzy relational equation $\chi \circ R_\delta = \chi$, where $\chi \in L^Q$ is an unknown.*

Proof. Follows from Propositions 6 and 11.

Proposition 16. *Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system and $\lambda \in L^Q$. Then the following are equivalent:*

(i) *λ is a reverse subsystem of $\mathcal{T}$.*
(ii) *λ is $\tau_{R_{\overline{\delta}}}$-open.*
(iii) *λ is a solution to a fuzzy relational equation $R_{\overline{\delta}} \circ \chi = \chi$, where $\chi \in L^Q$ is an unknown.*

Proof. Follows from Propositions 7 and 12.

Proposition 17. *Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system and $\lambda \in L^Q$. Then*

(i) *if λ is a reverse subsystem, then $\neg\lambda$ is a subsystem.*
(ii) *if λ is a subsystem, then $\neg\lambda$ is a reverse subsystem.*

Proof. Follows from Proposition 13.

Proposition 18. *Let $\mathcal{T} = (Q, X, \delta)$ be a fuzzy transition system and $\lambda \in L^Q$. Then*

(i) *λ is a double subsystem of $\mathcal{T}$.*
(ii) *λ is both τ_{R_δ} and $\tau_{R_{\overline{\delta}}}$-open.*

Proof. Follows from Propositions 6 and 7.

Proposition 19. *Let (Q, X, δ) and (R, Y, μ) be fuzzy transition systems. If $f : Q \longrightarrow R$ is a homomorphism, then $f : (Q, \tau_\delta) \longrightarrow (R, \tau_\mu)$ is fuzzy continuous.*

Proof. Follows from Proposition 14.

Some other results for subsystems and reverse subsystems of fuzzy transition systems can also be derived from Propositions 1, 2, 3, 4 and 5.

In the remaining part of this section, we give an example to indicate that the approach outlined here can also lead to some 'new' concepts for fuzzy transition systems. Specifically, we try to introduce the concept of product of fuzzy transition systems.

An examination of the 'categorical product' in the category **FTS** leads to a concept of 'product' of fuzzy transition systems, which we illustrate here for two fuzzy transition systems $\mathcal{T} = (Q, X, \delta)$ and $\mathcal{S} = (R, Y, \lambda)$ as follows.

($X \times Y$, appearing below is the 'direct product' of the monoids X and Y. Thus it is the cartesian product of X and Y, considered as a monoid, whose binary operation is defined as $(x, y)(x', y') = (xx', yy')$, for $(x, y), (x', y') \in X \times Y$, and whose identity element is (e_X, e_Y), where e_X and e_Y are the identities of X and Y respectively.)

Define

$$\nu : (Q \times R) \times (X \times Y) \times (Q \times R) \to L$$

as

$$\nu((q, r), (x, y), (q', r')) = \delta(q, x, q') \otimes \lambda(r, y, r')$$

$\forall((q, r), (x, y), (q', r')) \in (Q \times R) \times (X \times Y) \times (Q \times R)$.

Then

$$\nu((q,r),(e_X,e_Y),(q',r')) = \delta(q,e_X,q') \otimes \lambda(r,e_Y,r') \\ = \begin{cases} 1 \text{ if } (q,r) = (q',r') \\ 0 \text{ if } (q,r) \neq (q',r'). \end{cases}$$

Next, for $(x',y') \in X \times Y$,

$$\begin{aligned} &\nu((q,r),(x,y)(x',y'),(q',r')) \\ &= \nu((q,r),(xx',yy'),(q',r')) \\ &= \delta(q,xx',q') \otimes \lambda(r,yy',r') \\ &= [\vee\{\delta(q,x,s) \otimes \delta(s,x',q') : s \in Q\}] \otimes [\vee\{\lambda(r,y,t) \otimes \lambda(t,y',r') : t \in R\}] \\ &= \vee\{(\delta(q,x,s) \otimes \delta(s,x',q')) \otimes (\lambda(r,y,t) \otimes \lambda(t,y',r')) : s \in Q, t \in R\}. \end{aligned}$$

On the other hand,

$$\begin{aligned} &\vee\{\nu((q,r),(x,y),(s,t)) \otimes \nu((s,t),(x',y'),(q',r')) : s \in Q, t \in R\} \\ &= \vee\{(\delta(q,x,s) \otimes \lambda(r,y,t)) \otimes (\delta(s,x',q') \otimes \lambda(t,y',r')) : s \in Q, t \in R\} \\ &= \vee\{(\delta(q,x,s) \otimes \delta(s,x',q')) \otimes (\lambda(r,y,t) \otimes \lambda(t,y',r')) : s \in Q, t \in R\}. \end{aligned}$$

Thus, $\nu((q,r),(x,y)(x',y'),(q',r'))$

$= \vee\{\nu((q,r),(x,y),(s,t)) \otimes \nu((s,t),(x',y'),(q',r')) : s \in Q, t \in R\}$.

This shows that $(Q \times R, X \times Y, \nu)$ is a fuzzy transition system, which we shall refer to as the *product* of the fuzzy transition systems $\mathcal{T} = (Q,X,\delta)$ and $\mathcal{S} = (R,Y,\lambda)$ and will denote it as $\mathcal{T} \times \mathcal{S}$.

Remark 2. This product may be interpreted as the 'parallel composition' of $\mathcal{T}$ and $\mathcal{S}$ cf., e.g., Dörfler [3].

Proposition 20. *The product $\mathcal{T} \times \mathcal{S}$ of $\mathcal{T}, \mathcal{S} \in$ **FTS** is the categorical product in* **FTS**.

Proof. : We first need to identify the two 'projection morphisms' from $\mathcal{T} \times \mathcal{S}$ to $\mathcal{T}$ and $\mathcal{S}$ in **FTS**. Let $\mathcal{T} = (Q,X,\delta)$ and $\mathcal{S} = (R,Y,\lambda)$. Let $h_1 : Q \times R \to Q, h_2 : Q \times R \to R, k_1 : X \times Y \to X$ and $k_2 : X \times Y \to Y$ be the projection maps associated with the cartesian products $Q \times R$ and $X \times Y$. We show that $(h_1,k_1) : \mathcal{T} \times \mathcal{S} \to \mathcal{T}$ and $(h_2,k_2) : \mathcal{T} \times \mathcal{S} \to \mathcal{S}$ are **FTS**-morphisms. Let $((p_1,q_1),(x,y),(p_2,q_2)) \in (Q \times R) \times (X \times Y) \times (Q \times R)$. Then $\delta(h_1(p_1,q_1),k_1(x,y),h_1(p_2,q_2)) = \delta(p_1,x,p_2) \geq \delta(p_1,x,p_2) \otimes \lambda(q_1,y,q_2) = \nu((p_1,q_1),(x,y),(p_2,q_2))$. Thus $\delta(h_1(p_1,q_1),k_1(x,y), h_1(p_2,q_2)) \geq \nu((p_1,q_1),(x,y),(p_2,q_2)), \forall((p_1,q_1),(x,y),(p_2,q_2)) \in (Q \times R) \times (X \times Y) \times (Q \times R)$, whereby $(h_1,k_1) : \mathcal{T} \times \mathcal{S} \to \mathcal{T}$ is an **FTS**-morphism. Similarly, $(h_2,k_2) : \mathcal{T} \times \mathcal{S} \to \mathcal{S}$ can be seen to be an **FTS**-morphism. Next, let $\mathcal{T}' = (Q',X',\delta') \in$ **FTS** and two **FTS**-morphisms $(f_1,g_1) : M' \to M$ and $(f_2,g_2) : M' \to N$ be given. We show that there exists a unique **FTS**-morphism $(f,g) : M' \to M \times N$ such that the following diagram commutes.

$$\begin{tikzcd}
& M' \arrow[dl, "(f_1,g_1)"'] \arrow[d, dotted, "(f,g)"] \arrow[dr, "(f_2,g_2)"] & \\
M & M \times N \arrow[l, "(h_1,k_1)"] \arrow[r, "(h_2,k_2)"'] & N
\end{tikzcd}$$

Here, $(h_1, k_1) : M \times N \to M$ and $(h_2, k_2) : M \times N \to N$ are the projection maps. We choose the f and g in following way.

Let $f : Q' \to Q \times R$ and $g : X' \to X \times Y$ be the maps given by $f(q') = (f_1(q'), f_2(q'))$ and $g(x') = (g_1(x'), g_2(x')), \forall (q', x') \in Q' \times X'$. Let $(q', x', r') \in Q' \times X' \times Q'$. As both (f_1, g_1) and (f_2, g_2) are **FTS**-morphisms, $\delta(f_1(q'), g_1(x'), f_1(r')) \geq \delta'(q', x', r')$ and $\lambda(f_2(q'), g_2(x'), f_2(r')) \geq \delta'(q', x', r')$, whereby $\delta(f_1(q'), g_1(x'), f_1(r')) \otimes \lambda(f_2(q'), g_2(x'), f_2(r')) \geq \delta'(q', x', r')$. Thus $\nu(f(q'), g(x'), f(r')) = \nu((f_1(q'), f_2(q')), (g_1(x'), g_2(x')), (f_1(r'), f_2(r'))) = \delta(f_1(q'), g_1(x'), f_1(r')) \otimes \lambda(f_2(q'), g_2(x'), f_2(r')) \geq \delta'(q', x', r')$. Hence (f, g) is an **FTS**-morphism. Also, the definitions of f and g are such that we obviously have $(h_1, k_1) \circ (f, g) = (f_1, g_1)$ and $(h_2, k_2) \circ (f, g) = (f_2, g_2)$.

To prove the uniqueness of (f, g), let there exist another **FTS**-morphism $(f', g') : M' \to M \times N$ such that $(h_1, k_1) \circ (f', g') = (f_1, g_1)$ and $(h_2, k_2) \circ (f', g') = (f_2, g_2)$, i.e., $h_1 \circ f' = f_1, k_1 \circ g' = g_1, h_2 \circ f' = f_2$, and $k_2 \circ g' = g_2$. We then have $h_1 \circ f' = h_1 \circ f, k_1 \circ g' = k_1 \circ g, h_2 \circ f' = h_2 \circ f$, and $k_2 \circ g' = k_2 \circ g$, whereby $f = f'$ and $g = g'$. Thus $(f', g') = (f, g)$, proving the uniqueness of (f, g). Hence $M \times N$ is the categorical product.

4 Conclusion

In this paper, we have tried to study the concept of upper sets and lower sets of a fuzzy preordered set. We showed that their collection form fuzzy topologies. Finally, we have used such concepts for the study of fuzzy transition systems.

Acknowledgments. The authors are grateful to:
- the reviewer(s) for their suggestions for improvement of the paper,
- the Council of Scientific and Industrial Research, New Delhi, for provided research grant under which this work has been carried out.

References

1. Blount, K., Tsinakis, C.: The structure of residuated lattices. International Journal of Algebra and Computation 13, 437–461 (2003)
2. Das, P.: A fuzzy topology associated with a fuzzy finite state machine. Fuzzy Sets and Systems 105, 469–479 (1999)
3. Dörfler, W.: The Direct Product of Automata and Quasiautomata. In: Mazurkiewicz, A. (ed.) MFCS 1976. LNCS, vol. 45, pp. 270–276. Springer, Heidelberg (1976)
4. Guo, X.: Grammar theory based on lattice-order monoid. Fuzzy Sets and Systems 160, 1152–1161 (2009)
5. Ignjatović, J., Ćiric, M., Bogdanović, S.: Determinization of fuzzy automata with membership values in complete residuated lattices. Information Sciences 178, 164–180 (2008)
6. Jun, Y.B.: Intuitionistic fuzzy finite state machines. Journal of Applied Mathematics and Computing 17, 109–120 (2005)
7. Jun, Y.B.: Intuitionistic fuzzy finite switchboard state machines. Journal of Applied Mathematics and Computing 20, 315–325 (2006)

8. Jun, Y.B.: Quotient structures of intuitionistic fuzzy finite state machines. Information Sciences 177, 4977–4986 (2007)
9. Kim, Y.H., Kim, J.G., Cho, S.J.: Products of T-generalized state machines and T-generalized transformation semigroups. Fuzzy Sets and Systems 93, 87–97 (1998)
10. Kumbhojkar, H.V., Chaudhri, S.R.: On proper fuzzification of fuzzy finite state machines. International Journal of Fuzzy Mathematics 4, 1019–1027 (2008)
11. Li, Y., Pedrycz, W.: Fuzzy finite automata and fuzzy regular expressions with membership values in lattice-orderd monoids. Fuzzy Sets and Systems 156, 68–92 (2005)
12. Lihua, W., Qiu, D.: Automata theory based on complete residuated lattice-valued logic: Reduction and minimization. Fuzzy Sets and Systems 161, 1635–1656 (2010)
13. Lowen, R.: Fuzzy topological spaces and fuzzy compactness. Jour. Math. Anal. Appl. 56, 621–633 (1976)
14. Mordeson, J.N., Malik, D.S.: Fuzzy Automata and Languages: Theory and Applications. Chapman and Hall/CRC, London, Boca Raton (2002)
15. Malik, D.S., Mordeson, J.N., Sen, M.K.: Submachines of fuzzy finite state machine. Journal of Fuzzy Mathematics 2, 781–792 (1994)
16. Qiu, D.: Automata theory based on quantum logic: Some characterizations. Information and Computation 190, 179–195 (2004)
17. Qiu, D.: Automata theory based on quantum logic: Reversibilities and pushdown automata. Theoretical Computer Science 386, 38–56 (2007)
18. Qiu, D.: Characterizations of fuzzy finite automata. Fuzzy Sets and Systems 141, 391–414 (2004)
19. Qiu, D.: Automata theory based on complete residuated lattice-valued logic(I). Science in China 44, 419–429 (2001)
20. Qiu, D.: Automata theory based on complete residuated lattice-valued logic(II). Science in China 45, 442–452 (2002)
21. Santos, E.S.: Maximin automata. Information and Control 12, 367–377 (1968)
22. She, Y.H., Wang, G.J.: An axiomatic approach of fuzzy rough sets based on residuated lattices. Computer and Mathematics with Applications 58, 189–201 (2009)
23. Srivastava, A.K., Tiwari, S.P.: A Topology for Fuzzy Automata. In: Pal, N.R., Sugeno, M. (eds.) AFSS 2002. LNCS (LNAI), vol. 2275, pp. 485–490. Springer, Heidelberg (2002)
24. Srivastava, A.K., Tiwari, S.P.: On relationships among fuzzy approximation operators, fuzzy topology, and fuzzy automata. Fuzzy Sets and Systems 138, 197–204 (2003)
25. Wee, W.G.: On generalizations of adaptive algorithm and application of the fuzzy sets concept to pattern classification. Ph. D. Thesis, Purdue University, Lafayette, IN (1967)
26. Zadeh, L.A.: Fuzzy Sets. Information and Control 8, 338–353 (1965)
27. Lai, H., Zhang, D.: Fuzzy preorder and fuzzy topology. Fuzzy Sets and Systems 157, 1865–1885 (2006)

Public Announcements for Non-omniscient Agents

Fernando R. Velázquez-Quesada

Grupo de Lógica, Lenguaje e Información, Universidad de Sevilla
`FRVelazquezQuesada@us.es`

Abstract. A public announcement is the most basic form of communication between agents. The effects of such action have been studied within the field of *dynamic epistemic logic*, in particular, in the so called *public announcement logic*. Nevertheless, being a direct extension of *epistemic logic*, what public announcement logic has studied is actually the effect of a public announcement on the knowledge of an *omniscient* agent. The present work studies different forms of public announcement and how they affect the knowledge of *non-omniscient* agents. More precisely, we recall the definitions of the so called *implicit* and *explicit* public announcements and present some of their properties in our setting. Then, after arguing that these definitions still assume some form of logical omniscience, we introduce two forms of non-omniscient public announcements that fit better the intuition behind the involved agents.

1 Introduction

Public announcement logic (*PAL*; [1,2]) studies the effect of the most basic communicative action on the knowledge of epistemic logic agents, and it has served as the basis for the study of more complex announcements [3] and other forms of epistemic changes [4,5]. The framework relies on a natural interpretation of what the public announcement of a given formula χ does: it eliminates those epistemic possibilities that do not satisfy χ. Despite its simplicity, *PAL* has proved to be a fruitful field for interesting research, like the characterisation of *successful formulas* (those that are still true after being truthfully announced: [6,7]), the characterisation of schematic validities [8] and many others [9].

Being based on *epistemic logic* (*EL*; [10,11]), *PAL* inherits many of its properties, including the fact that every agent knows every validity and their knowledge is closed under implications. Thus, what *PAL* studies is actually the way a public announcement affects the knowledge of *omniscient* agents.

But we also have non-omniscient agents: those that might not know every validity, or that might know some φ and $\varphi \to \psi$ without knowing ψ. They represent more faithfully not only human agents (after all, the purpose of disciplines like Mathematics and Computer Science is to fill in the logical consequences of what we already know) but also computational ones (they might lack of space and/or time to derive all the logical consequences of their information). Different forms of public announcements affect these kind of agents in a different way.

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 220–232, 2013.

The present work studies different forms of public announcements and the different ways they affect the knowledge of a non-omniscient agent. We start in Section 2 by recalling an *awareness-like* extension of the *EL* framework in order to represent the knowledge of such an agent. Then in Section 3 we recall the definitions of the so called *implicit* and *explicit* public announcements, presenting also the way they affect our defined explicit and implicit knowledge. In Section 4 we argue that such public announcements still assume some form of logical omniscience, and we present an operation that is more adequate: what we call a *non-omniscient public announcement* in two versions, plain and attentive. For each one of them we introduce a modality in order to describe its effects within the formal language, and we also provide a sound and complete axiom system for both. We finish on Section 5 with our conclusions and further lines of research.

Related Works. As we will see, our approach assumes that the lack of logical omniscience comes from the fact that the agent has not acknowledged as true every formula that is so in each possible world: she has not performed yet every possible inference step. This is, of course, just one of the many reasons why an agent might not be logically omniscient: she might be unaware of certain propositions [12], she might not have the needed inferences abilities [13], or she might not have enough resources [14]. Public announcements and in general epistemic actions affect particular kind of agents in different ways [15].

2 Representing Non-omniscient Agents

The framework we will use for representing the knowledge of non-omniscient agents is based on the idea of distinguishing between the agent's *implicit* knowledge, what she can eventually get, and her *explicit* knowledge, what she actually has. This framework follows the lines of the *awareness logic* of [12], but there will be a change in the main intuition.

The key idea in *awareness logic* is that an agent might not be logically omniscient because she might not be *aware of* (she might not entertain) some formulas. Thus, in order to know a given φ *explicitly*, it is not enough for φ to be the case in all the agent's epistemic possibilities: she also needs to be *aware of* φ.[1] In the present work we will use another idea. We assume that the agent is *aware of* every formula of the language, but she might be non-omniscient because she might not have realised that some formulas are the case in a given world. Thus, she might know explicitly some φ and $\varphi \to \psi$ without knowing ψ explicitly simply because she has not performed the needed inference step to acknowledge ψ. (See [16] for a framework that involves both ideas.)

This intuition affects the definition of explicit knowledge, which will be provided and discussed after presenting the formal language, the semantic model and the formulas' semantic interpretation.

---

[1] Note that, under some reasonable definitions of the notion of *awareness of*, like awareness closed under sub-formulas or based on atomic propositions, the agent is still a perfect reasoner: she knows explicitly every validity she is aware of, and if she knows explicitly some φ and $\varphi \to \psi$, then she also knows ψ explicitly.

Definition 1 (Language). *Let* $\mathtt{P}$ *be a set of atomic propositions. Formulas* φ, ψ *of the* language $\mathcal{L}$ *are built according to the rule*

$$\varphi ::= p \mid \mathrm{A}\,\varphi \mid \neg\varphi \mid \varphi \vee \psi \mid \Box\,\varphi$$

with $p \in \mathtt{P}$*. Other connectives (*$\wedge$*,* $\rightarrow$*,* $\leftrightarrow$*) as well as the existential modal operator (*$\Diamond$*) are defined in the standard way (*$\Diamond\,\varphi := \neg\Box\,\neg\varphi$ *for the latter).*

Formulas of the form $\Box\,\varphi$ are read not as "the agent knows φ" (as in classical *EL*), but rather as "the agent knows φ *implicitly*". Formulas of the form $\mathrm{A}\,\varphi$ are read not as "the agent is *aware of* φ" (as in *awareness logic*), but rather as "the agent *has acknowledged that* φ is the case".

Definition 2 (Semantic model). *Let* $\mathtt{P}$ *be the set of atomic propositions. A* semantic model *is a tuple* $M = \langle W, R, V, \mathsf{A}\rangle$ *where (1)* W *is a non-empty set of so-called* possible worlds*; (2)* $R \subseteq (W \times W)$ *is the agent's* epistemic indistinguishability *equivalence relation; (3)* $V : W \to \wp(\mathtt{P})$ *is an* atomic valuation*; (4)* $\mathsf{A} : W \to \wp(\mathcal{L})$ *is the acknowledgement set function, returning the set of formulas of* $\mathcal{L}$ *that the agent has acknowledged as true at each possible world.*

The pair (M, w)*, consisting of a semantic model* M *and a distinguished world* w *in it is called a* pointed semantic model*.*

Definition 3 (Semantic interpretation). *Let* (M, w) *be a pointed semantic model with* $M = \langle W, R, V, \mathsf{A}\rangle$*. Atomic propositions, negations and disjunctions are evaluated as usual. For the rest,*

$$\begin{array}{lll} (M,w) \Vdash \mathrm{A}\,\varphi & \textit{iff} & \varphi \in \mathsf{A}(w) \\ (M,w) \Vdash \Box\,\varphi & \textit{iff} & \textit{for all } u \in W\textit{, Rwu implies } (M,u) \Vdash \varphi \end{array}$$

When $(M, w) \Vdash \varphi$*, we say that* φ *is true at* w *in* M*. We will denote by* $[\![\varphi]\!]^M$ *the set of worlds in* M *in which* φ *is true (i.e.,* $[\![\varphi]\!]^M := \{w \in W \mid (M, w) \Vdash \varphi\}$*).*

Implicit and Explicit Knowledge. An important consequence of the main idea behind the framework is that, given a world w and a formula φ, the agent might not be able to tell whether φ is true at w.[2] In fact, for her there are not only worlds that she identifies as satisfying φ (those where $\varphi \wedge \mathrm{A}\,\varphi$ holds) and worlds she identifies as satisfying $\neg\varphi$ (those where $\neg\varphi \wedge \mathrm{A}\,\neg\varphi$ holds): there are also 'φ-uncertain' worlds (those where neither $\varphi \wedge \mathrm{A}\,\varphi$ nor $\neg\varphi \wedge \mathrm{A}\,\neg\varphi$ hold). This gives us the following definitions of implicit and explicit knowledge.

Definition 4. *The agent knows* φ implicitly*,* $K_{\mathrm{Im}}\varphi$*, when* φ *is the case in every epistemically possible world. She knows* φ explicitly*,* $K_{\mathrm{Ex}}\varphi$*, when she recognises every epistemically possible world as a* φ*-world (i.e., as a world satisfying* φ*).*

$$K_{\mathrm{Im}}\varphi := \Box\,\varphi \qquad\qquad K_{\mathrm{Ex}}\varphi := \Box\,(\varphi \wedge \mathrm{A}\,\varphi)$$

---

[2] This is different from standard *EL* where, given any w and any φ, the agent can *always* tell φ's truth-value at w. An *EL*-agent's uncertainty comes not from her not knowing whether a given formula holds at a certain world, but rather from her not knowing which one the real world is.

If a given φ *is known explicitly, then it is also know implicitly, as* $\Box(\varphi \land \mathrm{A}\,\varphi)$ *implies* $\Box\,\varphi$. *An agent is logically omniscient when the other direction holds, i.e., when* $\Box\,\varphi$ *implies* $\Box(\varphi \land \mathrm{A}\,\varphi)$. *This happens when she has acknowledged as true the formulas that are so in every epistemically possible world (*$\Box(\varphi \rightarrow \mathrm{A}\,\varphi)$*).*

The formula that characterises the worlds the agent recognises as satisfying φ, $\varphi \land \mathrm{A}\,\varphi$, *will be useful later; hence we will abbreviate it as* φ^{Ag}.

We can also define notions of implicit and explicit epistemic possibility:

$$\widehat{K}_{\mathrm{Im}}\varphi := \Diamond\,\varphi \qquad\qquad \widehat{K}_{\mathrm{Ex}}\varphi := \Diamond(\varphi \land \mathrm{A}\,\varphi)$$

Different from the relation between implicit possibility ($\Diamond\,\varphi$) and implicit knowledge ($\Box\,\varphi$), explicit possibility ($\Diamond(\varphi \land \mathrm{A}\,\varphi)$) is *not* the modal dual of explicit knowledge ($\Box(\varphi \land \mathrm{A}\,\varphi)$). Still, the definition is proper: φ is *explicitly* possible for an agent when she has an epistemic possibility she identifies as satisfying φ.

Axiom System. The standard $\mathsf{S5}$ axiom system schema (propositional tautologies, the *K*, *T*, *4* and *B* axioms, modus ponens and necessitation) is sound and complete for the language $\mathcal{L}$ with respect to our semantic models. We do not need special axioms for formulas of the form $\mathrm{A}\,\varphi$ (the only novel primitive) because (1) they are evaluated simply as atoms of a special signature, and (2) their 'valuation function' A does not need to satisfy any particular property.

3 Implicit and Explicit Public Announcements

With the 'static' framework defined, we can turn our attention to the definition of a public announcement for these kind of agents. Here are two known possibilities.

3.1 Implicit Public Announcement

The simplest way for representing a public announcement in this setting is to use the *PAL* approach directly: the announcement simply discards those worlds where the announced χ does not hold, restricting the epistemic indistinguishability relation to the new domain and leaving unaffected the other model components. This is what an *implicit public announcement* [17] does.

Definition 5 (Implicit public announcement). *Let* $M = \langle W, R, V, \mathsf{A}\rangle$ *be a semantic model and let* χ *be a formula in* $\mathcal{L}$. *The semantic model* $M_{\chi!^{\mathrm{Im}}} = \langle W', R', V', \mathsf{A}'\rangle$ *is given by* $W' := W \setminus [\![\neg\chi]\!]^M$, $R' := R \cap (W' \times W')$ *and, for every* $w \in W'$, $V'(w) := V(w)$ *and* $\mathsf{A}'(w) := \mathsf{A}(w)$. *An implicit public announcement of* χ *simply discards worlds where* χ *fails, i.e., worlds satisfying* $\neg\chi$. *Note how this operation (as all the others subsequently introduced) preserves equivalence relations and thus keeps us in our relevant model class.*

In order to describe the effects of an implicit public announcement within the formal language we introduce an existential modality $\langle \chi!^{\mathrm{Im}}\rangle$ for every formula χ (its universal counterpart is defined as its modal dual, as usual: $[\chi!^{\mathrm{Im}}]\,\varphi := \neg\langle\chi!^{\mathrm{Im}}\rangle\,\neg\varphi$). The semantic interpretation of these modalities as follows.

Definition 6. *Let* (M, w) *be a pointed semantic model.*

$$(M, w) \Vdash \langle \chi!^{\mathrm{Im}} \rangle\, \varphi \qquad \text{iff} \qquad (M, w) \Vdash \chi \quad \text{and} \quad (M_{\chi!^{\mathrm{Im}}}, w) \Vdash \varphi$$

Note the precondition: in order for χ *to be announced, it needs to be true.*

Axiom System. We follow the *reduction axioms* approach, providing axioms that allow us to translate formulas with the new modalities into formulas without them. Soundness follows from the validity of these axioms; completeness follows from the fact that we can translate any formula of the extended language into a provably equivalent one without the new modalities, for which the 'static' axiom system S5 is complete. We refer to [4] for details of this technique.

Theorem 1 ([17]). *The axiom system S5 plus the axioms and rules of Table 1 form a sound and complete axiom system for the language* $\mathcal{L}$ *plus the implicit public announcement modality with respect to our semantic models.*

The reduction axioms for atomic propositions, negations, disjunctions and the universal modality $\Box$ are standard. The new one, for formulas of the form $\mathrm{A}\,\varphi$, simply establishes that an implicit public announcement after which the agent has acknowledged that φ is the case is possible ($\langle \chi!^{\mathrm{Im}} \rangle\, \mathrm{A}\,\varphi$) iff the announcement is possible (χ) and the agent has already acknowledged φ ($\mathrm{A}\,\varphi$).

Table 1. Axioms and rules for implicit public announcement.

$!^{\mathrm{Im}}_{p}$	$\vdash \langle \chi!^{\mathrm{Im}} \rangle\, p \leftrightarrow (\chi \wedge p)$	$!^{\mathrm{Im}}_{A}$	$\vdash \langle \chi!^{\mathrm{Im}} \rangle\, \mathrm{A}\,\varphi \leftrightarrow (\chi \wedge \mathrm{A}\,\varphi)$
$!^{\mathrm{Im}}_{\neg}$	$\vdash \langle \chi!^{\mathrm{Im}} \rangle\, \neg\varphi \leftrightarrow \big(\chi \wedge \neg\langle \chi!^{\mathrm{Im}} \rangle\, \varphi\big)$	$!^{\mathrm{Im}}_{N}$	From $\vdash \varphi$ infer $\vdash [\chi!^{\mathrm{Im}}]\, \varphi$
$!^{\mathrm{Im}}_{\vee}$	$\vdash \langle \chi!^{\mathrm{Im}} \rangle\, (\varphi \vee \psi) \leftrightarrow \big(\langle \chi!^{\mathrm{Im}} \rangle\, \varphi \vee \langle \chi!^{\mathrm{Im}} \rangle\, \psi\big)$		
$!^{\mathrm{Im}}_{\Box}$	$\vdash \langle \chi!^{\mathrm{Im}} \rangle\, \Box\,\varphi \leftrightarrow \big(\chi \wedge \Box\,(\chi \to [\chi!^{\mathrm{Im}}]\, \varphi)\big)$		

How an Implicit Public Announcement Affects the Agent'S Knowledge. Axiom $!^{\mathrm{Im}}_{\Box}$ already describes the way an implicit announcement affects implicit knowledge: it is possible to announce χ so that afterwards the agent knows φ *implicitly* exactly when χ is the case and the agent already knows *implicitly* that φ will be the case after a truthful implicit public announcement of χ.

$$\langle \chi!^{\mathrm{Im}} \rangle\, K_{\mathrm{Im}}\varphi \leftrightarrow \big(\chi \wedge K_{\mathrm{Im}}(\chi \to [\chi!^{\mathrm{Im}}]\, \varphi)\big) \tag{1}$$

The effect of the operation is better understood when we focus on its effects on the knowledge of formulas γ whose truth-value is not affected by the announcement.[3] In such cases (i.e., when we have $\gamma \leftrightarrow [\chi!^{\mathrm{Im}}]\, \gamma$, like when γ is purely propositional) the agent only needs to know implicitly that χ implies γ.

$$\langle \chi!^{\mathrm{Im}} \rangle\, K_{\mathrm{Im}}\gamma \leftrightarrow \big(\chi \wedge K_{\mathrm{Im}}(\chi \to \gamma)\big) \tag{2}$$

---

[3] Announcements affect the agent's knowledge, and so the truth-value of formulas describing it can change. The best known examples are 'Moore-like' formulas that become false after being truthfully announced [6,7].

If besides being unaffected by the announcement, γ is the announced formula, then we only need the precondition of the action.

$$\langle \gamma!^{\mathrm{Im}} \rangle\, K_{\mathrm{Im}} \gamma \leftrightarrow \gamma \tag{3}$$

In other words, under the given conditions (the action does not affect γ's truth-value), the agent will know γ implicitly after its truthful implicit public announcement: exactly what one would expect from such operation.

The case of explicit knowledge is different. In order for the agent to know explicitly a given φ after an implicit announcement of χ, she needs to know implicitly that both φ and $\mathrm{A}\,\varphi$ will be the case after the announcement. But the action does not affect A-sets, so she needs to know implicitly that a truthful announcement of χ will make φ true and that if χ is the case, so is $\mathrm{A}\,\varphi$.

$$\langle \chi!^{\mathrm{Im}} \rangle\, K_{\mathrm{Ex}} \varphi \leftrightarrow \big(\chi \wedge K_{\mathrm{Im}}(\chi \rightarrow [\chi!^{\mathrm{Im}}]\,\varphi) \wedge K_{\mathrm{Im}}(\chi \rightarrow \mathrm{A}\,\varphi)\big) \tag{4}$$

In the case of the knowledge of formulas γ whose truth-value is not affected by the announcement, the second and third conjunct of the right-hand side can be combined (cf. validity (2)).

$$\langle \chi!^{\mathrm{Im}} \rangle\, K_{\mathrm{Ex}} \gamma \leftrightarrow \big(\chi \wedge K_{\mathrm{Im}}(\chi \rightarrow (\gamma \wedge \mathrm{A}\,\gamma))\big) \tag{5}$$

If, additionally, γ is the announced formula, then the agent only needs to know implicitly that γ implies $\mathrm{A}\,\gamma$. In other words, in order for the agent to know explicitly any such formula γ after its announcement, before the announcement she should have acknowledged every epistemically possible γ-world as such:

$$\langle \gamma!^{\mathrm{Im}} \rangle\, K_{\mathrm{Ex}} \gamma \leftrightarrow (\gamma \wedge K_{\mathrm{Im}}(\gamma \rightarrow \mathrm{A}\,\gamma)) \tag{6}$$

3.2 Explicit Public Announcement

An implicit announcement does not affect what the agent has acknowledged as true. Still, one would expect for a public announcement not only to allow the agent to discard situations where the announcement does not hold, but also to make her realise that the announced formula is the case in every surviving world. This is what an explicit public announcement [18,17] does.

Definition 7 (Explicit public announcement). *Let $M = \langle W, R, V, \mathsf{A}\rangle$ be a semantic model and let χ be a formula in $\mathcal{L}$. The semantic model $M_{\chi!^{\mathrm{Ex}}} = \langle W', R', V', \mathsf{A}'\rangle$ differs from $M_{\chi!^{\mathrm{Im}}}$ (Definition 5) only in the definition of A', which is now given, for every $w \in W'$, by $\mathsf{A}'(w) := \mathsf{A}(w) \cup \{\chi\}$.*

Definition 8. *Let (M, w) be a pointed semantic model.*

$$(M, w) \Vdash \langle \chi!^{\mathrm{Ex}} \rangle\, \varphi \quad \textit{iff} \quad (M, w) \Vdash \chi \;\; \textit{and} \;\; (M_{\chi!^{\mathrm{Ex}}}, w) \Vdash \varphi$$

Theorem 2 ([18,17]). *The axiom system $\mathsf{S5}$ plus the axioms and rules of Table 2 form a sound and complete axiom system for the language $\mathcal{L}$ plus the explicit public announcement modality with respect to our semantic models.*

Again, reduction axioms for atomic propositions, negations, disjunctions and the universal modality are standard. The one for acknowledgement formulas comes now in two parts. An explicit public announcement of χ after which the agent has acknowledged a different φ is possible ($\langle \chi!^{\mathrm{Ex}} \rangle \, \mathrm{A} \, \varphi$) iff the announcement is possible (χ) and the agent has already acknowledged φ ($\mathrm{A} \, \varphi$). If φ is the announced χ, then we only need for the announcement to be possible (χ).

Table 2. Axioms and rules for explicit public announcement

$!^{\mathrm{Ex}}_{p} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, p \;\leftrightarrow\; (\chi \wedge p)$

$!^{\mathrm{Ex}}_{\neg} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, \neg\varphi \;\leftrightarrow\; (\chi \wedge \neg \langle \chi!^{\mathrm{Ex}} \rangle \, \varphi)$

$!^{\mathrm{Ex}}_{\vee} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, (\varphi \vee \psi) \;\leftrightarrow\; (\langle \chi!^{\mathrm{Ex}} \rangle \, \varphi \vee \langle \chi!^{\mathrm{Im}} \rangle \, \psi)$

$!^{\mathrm{Ex}}_{\Box} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, \Box \, \varphi \;\leftrightarrow\; (\chi \wedge \Box \, (\chi \to [\chi!^{\mathrm{Ex}}] \, \varphi))$

$!^{\mathrm{Ex}}_{A} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, \mathrm{A} \, \varphi \;\leftrightarrow\; (\chi \wedge \mathrm{A} \, \varphi)$ for $\varphi \neq \chi$

$!^{\mathrm{Ex}}_{A} \vdash \langle \chi!^{\mathrm{Ex}} \rangle \, \mathrm{A} \, \chi \;\leftrightarrow\; \chi$

$!^{\mathrm{Ex}}_{N}$ From $\vdash \varphi$ infer $\vdash [\chi!^{\mathrm{Ex}}] \, \varphi$

How an Explicit Public Announcement Affects the Agent'S Knowledge. An explicit public announcement affects the agent's *implicit* knowledge just like the implicit public announcement does. In the general case, it is possible to announce χ explicitly so that afterwards the agent knows φ *implicitly* exactly when χ is the case and the agent already knows *implicitly* that φ will be the case after a truthful explicit public announcement of χ (cf. validity (1)).

$$\langle \chi!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Im}}\varphi \;\leftrightarrow\; \big(\chi \wedge K_{\mathrm{Im}}(\chi \to [\chi!^{\mathrm{Ex}}] \, \varphi)\big) \tag{7}$$

For knowledge about formulas γ whose truth-value is not affected by the action, the agent only needs to know $\chi \to \gamma$ implicitly (cf. validity (2)).

$$\langle \chi!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Im}}\gamma \;\leftrightarrow\; \big(\chi \wedge K_{\mathrm{Im}}(\chi \to \gamma)\big) \tag{8}$$

If additionally γ is the announced formula, then the agent will know it implicitly after the formula's truthful explicit announcement. (cf. validity (3)).

$$\langle \gamma!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Im}}\gamma \;\leftrightarrow\; \gamma \tag{9}$$

With respect to the action's effect on explicit knowledge in the general case, an explicit public announcement works like an implicit one (cf. validity (4)).

$$\langle \chi!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Ex}}\varphi \;\leftrightarrow\; \big(\chi \wedge K_{\mathrm{Im}}(\chi \to [\chi!^{\mathrm{Ex}}] \, \varphi) \wedge K_{\mathrm{Im}}(\chi \to \mathrm{A} \, \varphi)\big) \tag{10}$$

For formulas γ whose truth-value is not affected by the announcement we also get a similar behaviour (cf. validity (5)).

$$\langle \chi!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Ex}}\gamma \;\leftrightarrow\; \big(\chi \wedge K_{\mathrm{Im}}(\chi \to (\gamma \wedge \mathrm{A} \, \gamma))\big) \tag{11}$$

What distinguishes an explicit announcement from an implicit one is how it affects the *explicit* knowledge of the announced formula. If the action does not change γ's truth-value, the agent will know it after its truthful explicit announcement (cf. validity (6)).

$$\langle \gamma!^{\mathrm{Ex}} \rangle \, K_{\mathrm{Ex}}\gamma \;\leftrightarrow\; \gamma \tag{12}$$

4 Non-omniscient Public Announcements

The two recalled public announcements behave properly, but they still make an omniscience assumption: an announcement of χ makes the agent discard those worlds where χ does not hold, i.e., worlds satisfying $\neg\chi$. This is reasonable for an omniscient agent, who can always tell whether χ holds at any given state. But for our non-omniscient agent there might be worlds in which she cannot tell whether χ holds. When χ is announced, she cannot discard *every* world that satisfies $\neg\chi$; the best she can do is to discard those worlds *she identifies* as satisfying $\neg\chi$, i.e., worlds satisfying $(\neg\chi)^{\mathrm{Ag}}$ [19].

We also have two options about the way this form of announcement affects the formulas the agent has acknowledged: the announced formula is acknowledged or it is not. Interestingly, these two possibilities can be now related to whether the agent will remember later that the announcement took place.

4.1 Non-omniscient Public Announcement

This public announcement is similar to the *implicit* one (Definition 5) in that it does not affect A-sets. Still, it differs in that it eliminates worlds that satisfy $(\neg\chi)^{\mathrm{Ag}}$ (i.e., $\neg\chi \wedge \mathrm{A}\,\neg\chi$), rather than those that satisfy only $\neg\chi$.

Definition 9 (Non-omniscient public announcement). *Take a semantic model* $M = \langle W, R, V, \mathsf{A}\rangle$ *and let* χ *be a formula in* $\mathfrak{L}$. *The semantic model* $M_{\chi^{+}!} = \langle W', R', V', \mathsf{A}'\rangle$ *differs from* $M_{\chi!^{\mathrm{Im}}}$ *(Definition 5) only in the definition of its set of possible worlds, given now by* $W' := W \setminus [\![(\neg\chi)^{\mathrm{Ag}}]\!]^{M}$.

Definition 10. *Let* (M, w) *be a pointed semantic model.*

$$(M, w) \Vdash \langle \chi^{+}!\rangle\, \varphi \qquad \textit{iff} \qquad (M, w) \Vdash \chi \quad \textit{and} \quad (M_{\chi^{+}!}, w) \Vdash \varphi$$

Theorem 3. *The axiom system S5 plus the axioms and rules of Table 3 form a sound and complete axiom system for the language* $\mathfrak{L}$ *plus the* $\langle\chi^{+}!\rangle$ *modalities with respect to our semantic models.*

The axiom for $\Box$ is the interesting one. Different from the previous cases, the precondition of the action and the condition a world should satisfy to survive the operation are not the same: in order to announce χ we still need for it to be true, but now the worlds that will survive are not those that satisfy it but rather those that the agent does not recognise as satisfying its negation: $\neg(\neg\chi)^{\mathrm{Ag}}$.[4]

The Effect of a Non-omniscient Public Announcement. This operation has some effects that may look counter-intuitive at first. It allows the agent to discard epistemic possibilities recognised as satisfying $\neg\chi$, so one could expect for the announcement to create explicit knowledge about the announced formula, but this is not the case, even when the truth-value of the announced formula

---

[4] To put it in a simpler way, from the operation's definition we can see that the worlds that will be eliminated are those satisfying $(\neg\chi)^{\mathrm{Ag}}$; then the surviving ones are those that do not satisfy such formula, that is, those that satisfy its negation.

Table 3. Axioms and rules for non-omniscient announcement

$^{+}!_{p}$	$\vdash \langle \chi^{+}! \rangle\, p \leftrightarrow (\chi \wedge p)$	$^{+}!_{\mathrm{A}}$	$\vdash \langle \chi^{+}! \rangle\, \mathrm{A}\, \varphi \leftrightarrow (\chi \wedge \mathrm{A}\, \varphi)$
$^{+}!_{\neg}$	$\vdash \langle \chi^{+}! \rangle\, \neg\varphi \leftrightarrow \big(\chi \wedge \neg \langle \chi^{+}! \rangle\, \varphi\big)$	$^{+}!_{N}$	From $\vdash \varphi$ infer $\vdash [\chi^{+}!]\, \varphi$
$^{+}!_{\vee}$	$\vdash \langle \chi^{+}! \rangle\, (\varphi \vee \psi) \leftrightarrow \big(\langle \chi^{+}! \rangle\, \varphi \vee \langle \chi^{+}! \rangle\, \psi\big)$		
$^{+}!_{\Box}$	$\vdash \langle \chi^{+}! \rangle\, \Box\, \varphi \leftrightarrow \big(\chi \wedge \Box\, (\neg(\neg\chi)^{\mathrm{Ag}} \rightarrow [\chi^{+}!]\, \varphi)\big)$		

is not affected by the operation. The reason is that the agent might not have recognised every $\neg\chi$-world as such before χ's announcement, and hence some of them might survive the operation. And even if the agent recognised every $\neg\chi$-world (i.e., even if the operation eliminate all such worlds), this does not imply that the agent has acknowledged that χ is the case in every surviving world: even though the operation might give her *implicit* knowledge of χ (only χ-worlds are left), this knowledge does not need to be explicit. To put it shortly, $[\gamma^{+}!]\, K_{\mathrm{Ex}}\gamma$ is not valid, even when γ is a formula whose truth-value is not affected by the announcement.

So what does a non-omniscient announcement of χ achieve? It has a very simple effect: it only *eliminates* $\neg\chi$ from the agent's *explicit possibilities*. More precisely, if γ's truth-value is not affected by the operation, after its announcement the agent does not consider $\neg\gamma$ *explicitly* possible anymore:

$$[\gamma^{+}!]\, \neg\widehat{K}_{\mathrm{Ex}}\neg\gamma$$

That this formula is valid follows from the fact that the operation eliminates every world satisfying $\neg\gamma \wedge \mathrm{A}\,\neg\gamma$. Since the operation does not change γ's truth-value, after it there will be no world satisfying $\neg\gamma \wedge \mathrm{A}\,\neg\gamma$ (that is, $\Diamond\, (\neg\gamma \wedge \mathrm{A}\,\neg\gamma)$, precisely the definition of $\widehat{K}_{\mathrm{Ex}}\neg\gamma$, will not be the case).[5]

Still, some readers might find this operation odd: intuitively, a public announcement of a given χ should allow the agent to discard *every* $\neg\chi$-possibility. And indeed this should be the case. Even a non-omniscient agent should be able to discard every-$\neg\chi$ possibility after χ is publicly announced; we just need to be precise about *when* each one of these possibilities will be eliminated.

Here is a more detailed analysis of the full process. After χ is announced, an *omniscient* agent *discards immediately every* $\neg\chi$*-world* because she can identify every one of them. A non-omniscient agent, on the other hand, will only *discard immediately those* $\neg\chi$*-worlds she identifies*; the rest should be discarded *only after they are recognised as such*, that is, only after the agent has recognised that the world contradicts the announcement.

Now, even though a non-omniscient public announcement eliminates those worlds the agent recognises as satisfying $\neg\chi$, it does not give her any tool to take care of the $\neg\chi$-worlds that had not been recognised when the announcement took place (and hence are still epistemically possible). In other words, after using the

---

[5] The fact that there are γ's for which $[\gamma^{+}!]\, \neg\widehat{K}_{\mathrm{Ex}}\neg\gamma$ is valid while $[\gamma^{+}!]\, K_{\mathrm{Ex}}\gamma$ is not only emphasises that explicit possibility is not the modal dual of explicit knowledge.

announcement to eliminate some epistemic possibilities, the agent ‘forgets’ that such epistemic action took place and then she will not be able to eliminate the surviving $\neg\chi$-worlds even after she recognises them as such.

An *attentive* non-omniscient public announcement, on the other hand, allows the agent to ‘keep track’ of the announcements that have been made, and therefore allows her to take care of worlds that should have been eliminated before once that they are properly identified.

4.2 Attentive Non-omniscient Public Announcement

Definition 11 (Attentive non-omniscient public announcement). *Let* $M = \langle W, R, V, \mathsf{A} \rangle$ *be a semantic model and let* χ *be a formula in* $\mathcal{L}$*. The semantic model* $M_{\chi^{\times}!} = \langle W', R', V', \mathsf{A}' \rangle$ *differs from* $M_{\chi^{+}!}$ *(Definition 9) only in the definition of* A'*, which is now given, for every* $w \in W'$*, by* $\mathsf{A}'(w) := \mathsf{A}(w) \cup \{\chi\}$*.*

Definition 12. *Let* (M, w) *be a pointed semantic model.*

$$(M, w) \Vdash \langle \chi^{\times}! \rangle\, \varphi \qquad \textit{iff} \qquad (M, w) \Vdash \chi \quad \textit{and} \quad (M_{\chi^{\times}!}, w) \Vdash \varphi$$

Theorem 4. *The axiom system S5 plus the axioms and rules of Table 4 form a sound and complete axiom system for the language* $\mathcal{L}$ *plus the* $\langle \chi^{\times}! \rangle$ *modalities with respect to our semantic models.*

Table 4. Axioms and rules for attentive non-omniscient announcement

${}^{\times}!_{p} \vdash \langle \chi^{\times}! \rangle\, p \leftrightarrow (\chi \wedge p)$	${}^{\times}!_{\mathrm{A}} \vdash \langle \chi^{\times}! \rangle\, \mathrm{A}\, \varphi \leftrightarrow (\chi \wedge \mathrm{A}\, \varphi)$ for $\varphi \neq \chi$
${}^{\times}!_{\neg} \vdash \langle \chi^{\times}! \rangle\, \neg\varphi \leftrightarrow \big(\chi \wedge \neg\langle \chi^{\times}! \rangle\, \varphi\big)$	${}^{\times}!_{\mathrm{A}} \vdash \langle \chi^{\times}! \rangle\, \mathrm{A}\, \chi \leftrightarrow \chi$
${}^{\times}!_{\vee} \vdash \langle \chi^{\times}! \rangle\, (\varphi \vee \psi) \leftrightarrow \big(\langle \chi^{+}! \rangle\, \varphi \vee \langle \chi^{\times}! \rangle\, \psi\big)$	${}^{\times}!_{N}$ From $\vdash \varphi$ infer $\vdash [\chi^{\times}!]\, \varphi$
${}^{\times}!_{\Box} \vdash \langle \chi^{\times}! \rangle\, \Box\, \varphi \leftrightarrow \big(\chi \wedge \Box\, (\neg(\neg\chi)^{\mathrm{Ag}} \rightarrow [\chi^{\times}!]\, \varphi)\big)$	

The axioms are exactly like those for the plain non-omniscient public announcement (Table 3) except in the case of formulas of the form $\mathrm{A}\, \varphi$. Just like in the explicit public announcement case here (Table 2) we have two cases, indicating that the only new acknowledged formula is the just announced one.

The Effect of an Attentive Non-omniscient Public Announcement. Again, consider formulas γ whose truth-value is not affected by the announcement. As we have seen, a plain non-omniscient announcement does not give the agent explicit knowledge of γ, even if she has recognised every epistemically possible $\neg\gamma$-world as such. An *attentive* non-omniscient public announcement behaves similarly in the general case, but if the agent has recognised every $\neg\gamma$-world as such, then after γ's announcement the agent will know γ explicitly:

$$[\gamma^{\times}!]\, K_{\mathrm{Ex}}\gamma$$

This is because the agent recognises every $\neg\gamma$-world, so after γ's announcement every $\neg\gamma$-world will be discarded. The action does not change γ's truth-value so every remaining world will still satisfy γ and, because of the action, the agent will recognise each one of them as a γ-world.

But even if the agent has not recognised every $\neg\chi$-world as such, this form of announcement gives the agent the possibility to deal with them as soon as they are identified. By acknowledging χ in the surviving worlds the agent knows that they should satisfy it. Then, if at a later stage the agent identifies a surviving $\neg\chi$-world as such[6], this world will satisfy both $\mathrm{A}\,\neg\chi$ (because of its recent identification) and $\mathrm{A}\,\chi$ (because of the announcement's effect). Such 'contradicting' worlds can then be safely eliminated by the proper *depuration* action

Definition 13 (Depuration). *Let* $M = \langle W, R, V, \mathsf{A}\rangle$ *be a semantic model and let* χ *be a formula in* $\mathcal{L}$*; define* $C_\chi := \mathrm{A}\,\chi \land \mathrm{A}\,\neg\chi$*, the formula characterising* χ*-contradicting worlds. The semantic model* $M_{\chi\sharp} = \langle W', R', V', \mathsf{A}'\rangle$ *is given by* $W' := W \setminus [\![C_\chi]\!]^M$*,* $R' := R \cap (W' \times W')$ *and, for every* $w \in W'$*,* $V'(w) := V(w)$ *and* $\mathsf{A}'(w) := \mathsf{A}(w)$*.*

Definition 14. *Let* (M, w) *be a pointed extended possible worlds model.*

$$(M, w) \Vdash \langle\chi\sharp\rangle\,\varphi \qquad \textit{iff} \qquad (M, w) \Vdash \neg C_\chi \quad \textit{and} \quad (M_{\chi\sharp}, w) \Vdash \varphi$$

Theorem 5. *The axiom system* S5 *plus the axioms and rules of Table 5 form a sound and complete axiom system for the language* $\mathcal{L}$ *plus the* $\langle\chi\sharp\rangle$ *modalities with respect to our semantic models.*

Table 5. Axioms and rules for the depuration action

$\sharp_p$	$\vdash \langle\chi\sharp\rangle\, p \leftrightarrow (\neg C_\chi \land p)$	$\sharp_{\mathrm{A}}$	$\vdash \langle\chi\sharp\rangle\, \mathrm{A}\,\varphi \leftrightarrow (\neg C_\chi \land \mathrm{A}\,\varphi)$
$\sharp_\neg$	$\vdash \langle\chi\sharp\rangle\, \neg\varphi \leftrightarrow \big(\neg C_\chi \land \neg\langle\chi\sharp\rangle\,\varphi\big)$	$\sharp_N$	From $\vdash \varphi$ infer $\vdash [\chi\sharp]\,\varphi$
$\sharp_\lor$	$\vdash \langle\chi\sharp\rangle\,(\varphi \lor \psi) \leftrightarrow \big(\langle\chi^{+}!\rangle\,\varphi \lor \langle\chi\sharp\rangle\,\psi\big)$		
$\sharp_\Box$	$\vdash \langle\chi^{+}!\rangle\,\Box\,\varphi \leftrightarrow \big(\neg C_\chi \land \Box\,(\neg C_\chi \rightarrow [\chi\sharp]\,\varphi)\big)$		

The axioms are exactly like those for a standard public announcement (e.g., those for implicit public announcement: Table 1), with $\neg C_\chi$ being both the action's precondition and what each world needs to satisfy to survive the operation.

This operation takes care of removing the worlds that have been found to be inconsistent. With its help we can now sketch the full story of the effect of an attentive non-omniscient public announcement. After χ is announced, a non-omniscient agent eliminates immediately those $\neg\chi$-worlds she has identified so far. Some $\neg\chi$-worlds will survive, but the announcement also makes the agent acknowledge χ in the remaining worlds ($\mathrm{A}\,\chi$ will be true in all of them). Then, whenever further actions make the agent recognise some $\neg\chi$-worlds as such, she will realise that they contradict the previous announcement. At this point she can perform a *depuration*, allowing her to discard these worlds, as expected.

---

[6] E.g., via an inference, a change in awareness or the creation of a justification.

5 Conclusions and Further Work

We have recalled the effect of two known forms of public announcements on the knowledge of a non-omniscient agent. Then we have introduced another two that fit better the intuition behind the involved agents.

Further Work. (a) A study of the effect of this action on agents that are not logically omniscience for other reasons ([20] already explores the effect in agents that do not satisfy the *perfect recall* property). (b) An exploration of the multi-agent case, in particular, of the way an agent sees how a public announcement affects the knowledge of others. (c) A study of model update operations in which the precondition is not the same as what the worlds should satisfy to survive.

References

1. Plaza, J.: Logics of public communications. In: Proc. of the 4th Int. Symposium on Methodologies for Intelligent Systems, ORNL/DSRD-24, pp. 201–216 (1989)
2. Gerbrandy, J., Groeneveld, W.: Reasoning about information change. Journal of Logic, Language, and Information 6(2), 147–196 (1997)
3. Baltag, A., Moss, L., Solecki, S.: The logic of public announcements, common knowledge and private suspicions. Tech. Rep. SEN-R9922, CWI (1999)
4. van Ditmarsch, H., van der Hoek, W., Kooi, B.: Dynamic Epistemic Logic. Springer (2007)
5. van Benthem, J.: Logical Dynamics of Information and Interaction. CUP (2011)
6. van Ditmarsch, H., Kooi, B.: The secret of my success. Synthese 151(2), 201–232 (2006)
7. Holliday, W.H., Icard, T.F.: Moorean phenomena in epistemic logic. In: Advances in Modal Logic, pp. 178–199. College Publications (2010)
8. Holliday, W.H., Hoshi, T., Icard III, T.F.: Schematic Validity in Dynamic Epistemic Logic: Decidability. In: van Ditmarsch, H., Lang, J., Ju, S. (eds.) LORI 2011. LNCS, vol. 6953, pp. 87–96. Springer, Heidelberg (2011)
9. van Benthem, J.: Open problems in logical dynamics. In: Mathematical Problems from Applied Logic I, pp. 137–192. Springer, New York (2006)
10. Hintikka, J.: Knowledge and Belief. Cornell University Press, Ithaca (1962)
11. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning about knowledge. The MIT Press, Cambridge (1995)
12. Fagin, R., Halpern, J.Y.: Belief, awareness, and limited reasoning. Artificial Intelligence 34(1), 39–76 (1988)
13. Jago, M.: Epistemic logic for rule-based agents. Journal of Logic, Language and Information 18(1), 131–158 (2009)
14. Alechina, N., Logan, B., Whitsey, M.: A complete and decidable logic for resource-bounded agents. In: AAMAS, pp. 606–613. IEEE Computer Society (2004)
15. Ågotnes, T., Alechina, N.: Special issue on Logics for Resource Bounded Agents. Journal of Logic, Language and Information 18(1) (2009)
16. Grossi, D., Velázquez-Quesada, F.R.: *Twelve Angry Men*: A Study on the Fine-Grain of Announcements. In: He, X., Horty, J., Pacuit, E. (eds.) LORI 2009. LNCS, vol. 5834, pp. 147–160. Springer, Heidelberg (2009)

17. van Benthem, J., Velázquez-Quesada, F.R.: The dynamics of awareness. Synthese 177 (Suppl.1), 5–27 (2010)
18. Velázquez-Quesada, F.R.: Inference and update. Synthese 169(2), 283–300 (2009)
19. Hamami, Y.: The interrogative model of inquiry meets dynamic epistemic logics. Master's thesis, ILLC, UvA, Amsterdam, The Netherlands (2010).
20. Liu, F.: Diversity of agents and their interaction. Journal of Logic, Language and Information 18(1), 23–53 (2009)

Subset Space Logic with Arbitrary Announcements

Philippe Balbiani[1], Hans van Ditmarsch[2], and Andrey Kudinov[3]

[1] Institut de recherche en informatique de Toulouse, CNRS — Université de Toulouse
[2] LORIA, CNRS - Université de Lorraine, France & IMSc, Chennai, India
[3] Institute for Information Transmission Problems RAS & Higher School of Economics, Moscow, Russia & Moscow Institute of Physics and Technology, Russia

Abstract. In this paper we introduce public announcements to Subset Space Logic (SSL). In order to do this we have to change the original semantics for SSL a little and consider a weaker version of SSL without the cross axiom. We present an axiomatization, prove completeness and show that this logic is PSPACE-complete. Finally, we add the arbitrary announcement modality which expresses "true after any announcement", prove several semantic results, and show completeness for a Hilbert-style axiomatization of this logic.

1 Introduction

Subset Space Logic (SSL) was introduced in [6] as logic of knowledge and efforts. The language of SSL includes two modalities K (correspond to knowledge, $K\varphi$ reads as "the agent knows that φ is true") and $\Box$ (correspond to efforts, $\Diamond\varphi = \neg\Box\neg\varphi$ reads as "φ is true after some efforts"). A formula in this setting evaluates in a pair (x, U), where x is "the actual state of the world" and U is "the epistemic state": the set of states of the world indistinguishable from the real one by the agent. In this context making an effort correspond to shrinking the epistemic state.

Over the years several ways to extend this language were suggested. For example multiple agents were introduced in [13], and the overlap operator in [12]. Another very natural way to extend SSL is with the public announcements operators. The effect of public announcement that φ is that the subset space is reduced to all pairs (x, U) that satisfy the formula φ. In other words, this models some form of external information being provided to the system, that is considered reliable (and thus taken to be true), which results in uncertainty reduction for the knowing agent, but also in uncertainty reduction for the amount of effort needed to make a proposition true or get to know if after that effort: public announcement affects both the K and the $\Box$ formulas.

It is intriguing and somewhat of a challenge to distinguish the "$\Diamond\varphi$", interpreted as "φ is true after some effort", from the quantifier '$\langle!\rangle\varphi$', interpreted as "φ is true after some announcement". Isn't an announcement also a form of effort? We do not have a conclusive answer to what the difference is, but two

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 233–244, 2013.

suggestions. Firstly, note that the φ in $\Diamond\varphi$ is interpreted in the same model, not in a changed model, unlike the φ in $\langle ! \rangle\varphi$ that is interpreted in a model restriction, a changed model. Therefore, the $\Diamond$ has more the flavor of a conditional logical interpretation (conditional on the agent doing some effort, φ is true), unlike the public announcement version. Let "ψ" incorporate the effort; as known, "φ is true conditional on ψ" is very different from "φ is true after announcement of ψ'. Secondly, we could imagine an application wherein the $\Diamond$ in $\Diamond\varphi$ represents a form of agency in contrast to $\langle ! \rangle\varphi$ that represents the effects of externally driven changes. As known, in public announcement logic there is no clear parallel for agency.

Our main motivation for this logic was to demonstrate that one can fruitfully add a dynamic aspect similar to that in dynamic epistemic logic to a very different logic, and "make it work".

A first attempt to extend SSL with public announcements was by Can Başkent in his master thesis [3]. We think that this semantics for public announcement in SSL is not well-defined; and also other intrinsic problems are not easy to overcome (see Appendix). To address these issues we propose a weaker version of SSL (wSSL) without the cross axiom; and to prove completeness we also modified the semantics somewhat.

We further extended this public announcement SSL with the arbitrary/any announcement operator of [2]. This models what can be known and which further effort still needs to be taken (in the SSL setting) after *any* announcement, i. e., after any external information has been incorporated.

We should also mention the work of Ågotnes and Wáng [1] where they take a different approach. Instead of adding public announcements operators to SSL they give an alternative semantics for PAL, using subset spaces instead of model updates.

2 Subset Space Logic

2.1 Syntax and Semantics

Let *Var* be a countable set of propositional variables (with typical members denoted p, q, etc). The set *For* of all formulas over *Var* (with typical members denoted φ, ψ, etc) is defined by the rule

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid (\varphi \vee \psi) \mid K\varphi \mid \Box\varphi.$$

It is usual to omit parentheses if this does not lead to any ambiguity. We shall say that a formula φ is Boolean iff φ contains neither the modal connective K, nor the modal connective $\Box$. The notion of a subformula is standard. We adopt the standard definitions for the remaining Boolean connectives. As usual, we define $\hat{K}\varphi ::= \neg K\neg\varphi$ and $\Diamond\varphi ::= \neg\Box\neg\varphi$. We inductively define the degree of a formula φ (denoted $\deg(\varphi)$) as follows: **(i)** $\deg(p) = 0$; **(ii)** $\deg(\bot) = 0$; **(iii)** $\deg(\neg\varphi) = \deg(\varphi)$; **(iv)** $\deg(\varphi \vee \psi) = \max(\{\deg(\varphi), \deg(\psi)\})$; **(v)** $\deg(K\varphi) = \deg(\Box\varphi) = \deg(\varphi) + 1$.

Let $|\varphi|$ denote the length of φ and $Var(\varphi)$ be the set variables in φ.

Definition 1. *A* (wSSL-)frame *is a structure of the form* $\mathcal{F} = (X, S, W)$ *where* X *is a nonempty set of states (denoted* x*,* y*, etc),* $S \subset \mathcal{P}(X)$ *is a nonempty set of nonempty subsets of* X *(denoted* U*,* V*, etc) and* W *is a nonempty set of pairs* (x, U) *such that* $x \in X$*,* $U \in S$ *and* $x \in U$*. Given a frame* $\mathcal{F} = (X, S, W)$*, let* $\rightarrow_K^{\mathcal{F}}$ *and* $\rightarrow_\Box^{\mathcal{F}}$ *be the binary relations on* W *defined as follows:* **(i)** $(x, U) \rightarrow_K^{\mathcal{F}} (y, V)$ *iff* $U = V$*;* **(ii)** $(x, U) \rightarrow_\Box^{\mathcal{F}} (y, V)$ *iff* $x = y$ *and* $U \supseteq V$*.*

Note that in this definition set S does not play any significant role and can be replaced with $\mathcal{P}(X)$ without any effect on validity.

We show first that

Lemma 1. *1.* $\rightarrow_K^{\mathcal{F}}$ *is an equivalence relation.*
2. $\rightarrow_\Box^{\mathcal{F}}$ *is reflexive and transitive.*

Definition 2. *Given a frame* $\mathcal{F} = (X, S, W)$*, a* valuation *on* $\mathcal{F}$ *is a function* θ *assigning to each* $p \in Var$ *a subset* $\theta(p)$ *of* X*. We inductively define the satisfaction of a formula* φ *in a frame* $\mathcal{F} = (X, S, W)$ *with respect to a valuation* θ *on* $\mathcal{F}$ *at* $(x, U) \in W$ *(denoted* $\mathcal{F}, \theta, (x, U) \models \varphi$*) as follows:*

- $\mathcal{F}, \theta, (x, U) \models p$ *iff* $x \in \theta(p)$*;*
- *all logical connectives are treated as usual;*
- $\mathcal{F}, \theta, (x, U) \models K\varphi$ *iff* $\forall (y, V) \in W \big((x, U) \rightarrow_K^{\mathcal{F}} (y, V) \Rightarrow \mathcal{F}, \theta, (y, V) \models \varphi\big)$*;*
- $\mathcal{F}, \theta, (x, U) \models \Box\varphi$ *iff* $\forall (y, V) \in W \big((x, U) \rightarrow_\Box^{\mathcal{F}} (y, V) \Rightarrow \mathcal{F}, \theta, (y, V) \models \varphi\big)$*.*

Remark. If for some $S \subseteq 2^X$ we take $W = \{(x, U) \,|\, x \in X,\ x \in U \in S\}$ then frame (X, S, W) is equivalent to (validates the same formulas) the classical subset space (X, S, θ) (see [6]). So these models can be viewed at as a generalization of subset spaces. Consider the cross axiom ($CA = \Diamond\hat{K}p \rightarrow \hat{K}\Diamond p$) which is valid in any classical subset space and can be false in a wSSL-model. Indeed consider two sets $V \subset U$ and two points $x, y \in V$ such that $\{(x, V), (x, U), (y, V)\} = W$ and $(y, V) \models p$, then $(x, U) \models \Diamond\hat{K}p \wedge \neg\hat{K}\Diamond p$.

We shall say that a formula φ is *universally satisfied* in a frame $\mathcal{F} = (X, S, W)$ with respect to a valuation θ on $\mathcal{F}$ (denoted $\mathcal{F}, \theta \models \varphi$) iff for all $(x, U) \in W$, $\mathcal{F}, \theta, (x, U) \models \varphi$. A formula φ is said to be *valid in a frame* $\mathcal{F} = (X, S, W)$ (denoted $\mathcal{F} \models \varphi$) iff for all valuations θ on $\mathcal{F}$, $\mathcal{F}, \theta \models \varphi$. We shall say that a formula φ is *valid* (denoted $\models \varphi$) iff for all frames $\mathcal{F} = (X, S, W)$, $\mathcal{F} \models \varphi$. So, by Lemma 1 and standard arguments we have

Proposition 1. *1.* $\models K\varphi \rightarrow \varphi$*,* $\models \varphi \rightarrow K\hat{K}\varphi$ *and* $\models K\varphi \rightarrow KK\varphi$*.*
2. $\models \Box\varphi \rightarrow \varphi$ *and* $\models \Box\varphi \rightarrow \Box\Box\varphi$*.*

Proposition 2. *If* φ *is a Boolean formula then* $\models \varphi \rightarrow \Box\varphi$*.*

2.2 Axiomatization and Completeness

The axioms of $wSSL$ are all instances of Boolean tautologies plus the following formulas: **(i)** $K(\varphi \rightarrow \psi) \rightarrow (K\varphi \rightarrow K\psi)$; **(ii)** $\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi)$; **(iii)** $K\varphi \rightarrow \varphi$; **(iv)** $\varphi \rightarrow K\hat{K}\varphi$; **(v)** $K\varphi \rightarrow KK\varphi$; **(vi)** $\Box\varphi \rightarrow \varphi$; **(vii)** $\Box\varphi \rightarrow$

$\Box\Box\varphi$; **(viii)** if φ is a Boolean formula then $\varphi \to \Box\varphi$. The rules of inference of $wSSL$ are: **(i)** modus ponens (from φ and $\varphi \to \psi$ infer ψ); **(ii)** K-generalization (from φ infer $K\varphi$); **(iii)** $\Box$-generalization (from φ infer $\Box\varphi$). A formula φ is said to be $wSSL$-provable iff φ belongs to the least set of formulas containing all axioms of $wSSL$ and closed with respect to all rules of inference of $wSSL$.

Using induction one can easily prove

Proposition 3. *Let φ be a formula. If φ is $wSSL$-provable then $\models \varphi$.*

The following result is expected but more difficult to prove.

Proposition 4. *Let φ be a formula. If $\models \varphi$ then φ is $wSSL$-provable.*

We shall say that a set Γ of formulas is a $wSSL$-theory iff it satisfies the following conditions: **(i)** Γ contains the set of all $wSSL$-provable formulas; **(ii)** Γ is closed under the rule of inference of modus ponens. Obviously, the least $wSSL$-theory is the set $Pr(wSSL)$ of all $wSSL$-provable formulas whereas the greatest $wSSL$-theory is the set of all formulas. A $wSSL$-theory Γ is said to be consistent iff $\bot \notin \Gamma$. Let us remark that the only inconsistent $wSSL$-theory is the set of all formulas. We shall say that a $wSSL$-theory Γ is maximal iff for all formulas φ, $\varphi \in \Gamma$, or $\neg\varphi \in \Gamma$. Let Γ be a $wSSL$-theory. For all formulas φ, let $\Gamma + \varphi$ be the set of all formulas ψ such that $\varphi \to \psi \in \Gamma$. It is a simple matter to check that $\Gamma + \varphi$ is a $wSSL$-theory. Moreover, $\Gamma + \varphi$ is consistent iff $\neg\varphi \notin \Gamma$. The proposition below is a variant of well known Lindenbaum's lemma. See [5, Lemma 4.17] for the proof of a similar result.

Proposition 5. *Let Γ be a $wSSL$-theory. If Γ is consistent then there exists a maximal consistent $wSSL$-theory Δ such that $\Gamma \subseteq \Delta$.*

Let Γ be a $wSSL$-theory. Let: **(i)** $K\Gamma$ be the set of all formulas φ such that $K\varphi \in \Gamma$; **(ii)** $\Box\Gamma$ be the set of all formulas φ such that $\Box\varphi \in \Gamma$. It is easy to prove that $K\Gamma$ is a $wSSL$-theory and $\Box\Gamma$ is a $wSSL$-theory using distribution axioms and $\Box$- and K-generalization rules.

Our first task is to define the canonical model of $wSSL$. The canonical model of $wSSL$ is the structure $\mathcal{M}^c = (S^c, R^c_K, R^c_\Box, \theta^c)$ defined as follows: **(i)** S^c is the set of all maximal consistent $wSSL$-theories; **(ii)** R^c_K is the binary relation on S^c defined by $\Gamma R^c_K \Delta$ iff $K\Gamma \subseteq \Delta$; **(iii)** $R^c_\Box$ is the binary relation on S^c defined by $\Gamma R^c_\Box \Delta$ iff $\Box\Gamma \subseteq \Delta$; **(iv)** θ^c is the function assigning to each $p \in Var$ the subset $\theta^c(p)$ of S^c defined by $\Gamma \in \theta^c(p)$ iff $p \in \Gamma$. It is worth noting at this point the following:

Lemma 2. *1. R^c_K is an equivalence relation.*
2. $R^c_\Box$ is reflexive and transitive.

Considering $\mathcal{M}^c$ as a Kripke model where the modal connectives K and $\Box$ are interpreted by means of the binary relations R^c_K and $R^c_\Box$, the proposition below contains a result that can be proved by induction on φ. See [5, Lemma 4.21] for the proof of a similar result.

Proposition 6. *Let φ be a formula. For all $\Gamma \in S^c$, we have $\mathcal{M}^c, \Gamma \models \varphi$ iff $\varphi \in \Gamma$.*

Let Γ_0 be a maximal consistent $wSSL$-theory. Our second task is to unravel $\mathcal{M}^c$ around Γ_0. The unraveling of $\mathcal{M}^c$ around Γ_0 is the structure $\mathcal{M}^u = (S^u, R_K^u, R_\Box^u, \theta^u)$ defined as follows: **(i)** S^u is the set of all finite sequences $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m)$ such that m is a nonnegative integer, $i_1, \ldots, i_m \in \{K, \Box\}$ and $\Gamma_1, \ldots, \Gamma_m \in S^c$ are such that $\Gamma_0 R_{i_1}^c \Gamma_1$, …, $\Gamma_{m-1} R_{i_m}^c \Gamma_m$; **(ii)** R_K^u is the binary relation on S^u defined by $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) R_K^u (j_1, \Delta_1, \ldots, j_n, \Delta_n)$ iff there exists a nonnegative integer o such that $o \leq m$, $o \leq n$, $(i_1, \Gamma_1, \ldots, i_o, \Gamma_o) = (j_1, \Delta_1, \ldots, j_o, \Delta_o)$, $i_{o+1} = \ldots = i_m = K$ and $j_{o+1} = \ldots = j_n = K$; **(iii)** $R_\Box^u$ is the binary relation on S^u defined by $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) R_\Box^u (j_1, \Delta_1, \ldots, j_n, \Delta_n)$ iff $m \leq n$, $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) = (j_1, \Delta_1, \ldots, j_m, \Delta_m)$ and $j_{m+1} = \ldots = j_n = \Box$; **(iv)** θ^u is the function assigning to each $p \in Var$ the subset $\theta^u(p)$ of S^u defined by $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) \in \theta^u(p)$ iff $p \in \Gamma_m$. We adopt the convention that an empty sequence (say, when $m = 0$, or $n = 0$ above) has value Γ_0. For all $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) \in S^u$, let $\sharp_\Box(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) = Card(\{\alpha\colon \alpha$ is a positive integer such that $\alpha \leq m$ and $i_\alpha = \Box\})$. By Lemma 2, we infer immediately the following.

Lemma 3. *1. R_K^u is an equivalence.*
2. $R_\Box^u$ is reflexive and transitive.

Considering $\mathcal{M}^u$ as a Kripke model where the modal connectives K and $\Box$ are interpreted by means of the binary relations R_K^u and $R_\Box^u$, the proposition below contains a result that can be proved by induction on φ.

Proposition 7. *Let φ be a formula. For all $(i_1, \Gamma_1, \ldots, i_m, \Gamma_m) \in S^u$, we have $\mathcal{M}^u, (i_1, \Gamma_1, \ldots, i_m, \Gamma_m) \models \varphi$ iff $\mathcal{M}^c, \Gamma_m \models \varphi$.*

Proof. See [5, Lemma 4.52] for the proof that $\mathcal{M}^c$ is a bounded morphic image of $\mathcal{M}^u$ and [5, Proposition 2.14] for the proof that modal satisfaction is invariant under bounded morphisms.

Let $\equiv^u$ be the symmetric and transitive closure of $R_\Box^u$ and $\preceq^u$ be the transitive closure of $R_K^u \circ R_\Box^u$. Obviously, $\equiv^u$ is reflexive, symmetrical and transitive and $\preceq^u$ is reflexive and transitive. Let $\boldsymbol{\Gamma} \in S^u$. The equivalence class modulo $\equiv^u$ with $\boldsymbol{\Gamma}$ as its representative is denoted $[\boldsymbol{\Gamma}]_{\equiv^u}$. The set of all equivalence classes of S^u modulo $\equiv^u$ is denoted $S^u/\equiv^u$. Let us define function $f : S^u \to \mathcal{P}(S^u/\equiv^u)$ defined as follows

$$f(\boldsymbol{\Gamma}) = \{[\boldsymbol{\Gamma}]_{\equiv^u} \mid \boldsymbol{\Gamma} \preceq^u \boldsymbol{\Delta}\}\,.$$

To continue, another technical lemma is necessary.

Lemma 4. *Let $\boldsymbol{\Gamma}, \boldsymbol{\Delta} \in S^u$.*

1. *If $f(\boldsymbol{\Gamma}) = f(\boldsymbol{\Delta})$ then $\boldsymbol{\Gamma} R_K^u \boldsymbol{\Delta}$.*
2. *If $\boldsymbol{\Gamma} \equiv^u \boldsymbol{\Delta}$ and $f(\boldsymbol{\Gamma}) \supseteq f(\boldsymbol{\Delta})$ then $\boldsymbol{\Gamma} R_\Box^u \boldsymbol{\Delta}$.*

Our third task is to spatialize $\mathcal{M}^u$. The spatialization of $\mathcal{M}^u$ consists of the frame $\mathcal{F}^s = (X^s, S^s, W^s)$ and the valuation θ^s on $\mathcal{F}^s$ defined as follows: **(i)** $X^s = S^u/\equiv^u$; **(ii)** S^s is the range of f; **(iii)** $W^s = \{([\boldsymbol{\Gamma}]_{\equiv^u}, f(\boldsymbol{\Gamma})) \mid \boldsymbol{\Gamma} \in S^u\}$; **(iv)** valuation θ^s is as follows $\theta^s(p) = \{[\boldsymbol{\Gamma}]_{\equiv^u} \mid \boldsymbol{\Gamma} \in \theta^u(p)\}$. The interesting result is the following

Proposition 8. *Let* φ *be a formula. For all* $\boldsymbol{\Gamma} \in S^u$, *we have* $\mathcal{F}^s, \theta^s, ([\boldsymbol{\Gamma}]_{\equiv^u}, f(\boldsymbol{\Gamma})) \models \varphi$ *iff* $\mathcal{M}^u, \boldsymbol{\Gamma} \models \varphi$.

Now, we can proceed to the

Proof of Proposition 4. Suppose φ is not $wSSL$-provable. Hence, $Pr(wSSL)+\neg\varphi$ is a consistent $wSSL$-theory. Thus, by Proposition 5, there exists a maximal consistent $wSSL$-theory Γ_0 such that $Pr(wSSL) + \neg\varphi \subseteq \Gamma_0$. Obviously, $\varphi \notin \Gamma_0$. Therefore, by Proposition 6, $\mathcal{M}^c, \Gamma_0 \not\models \varphi$. Consequently, by Proposition 7, $\mathcal{M}^u, \Gamma_0 \not\models \varphi$. Hence, by Proposition 8, $\mathcal{F}^s, \theta^s, ([\Gamma_0]_{\equiv^u}, f(\Gamma_0)) \not\models \varphi$. Thus, $\not\models \varphi$. $\dashv$

2.3 Decidability and Complexity

Fix a formula φ with $\deg(\varphi) = k$. Let $\varphi^\star$ be the conjunction of the following formulas: **(i)** $\neg\varphi$; **(ii)** for all $p \in Var(\varphi)$, $(K\Box)^k(p \to \Box p)$; **(iii)** for all $p \in Var(\varphi)$, $(K\Box)^k(\neg p \to \Box\neg p)$. In the above formulas, $(K\Box)^k$ means $K\Box$ repeated k times. We first prove a simple lemma.

Lemma 5. *The following conditions are equivalent:*

1. $\varphi^\star$ *is satisfied in a Kripke model of the form* $\mathcal{M} = (S, R_K, R_\Box, \theta)$ *where* R_K *is reflexive, symmetrical and transitive,* $R_\Box$ *is reflexive and transitive and the modal connectives* K *and* $\Box$ *are interpreted by means of the binary relations* R_K *and* $R_\Box$*.*
2. $\not\models \varphi$.

Proposition 9. *The membership problem in the set of all valid formulas is in* $PSPACE$*.*

Proof. By Lemmas 5, the membership problem in the set of all valid formulas is reducible to the membership problem in $S5 \otimes S4$. Since the membership problem in $S5 \otimes S4$ is in $PSPACE$ [14, Theorem 7], then the membership problem in the set of all valid formulas is in $PSPACE$.

Let $Q_1p_1 \ldots Q_np_n\varphi(p_1, \ldots, p_n)$ be a QBF and consider the new propositional variables $q_0, q_1, \ldots, q_n$. Let $[Q_1p_1 \ldots Q_np_n\varphi(p_1, \ldots, p_n)]$ be the conjunction of the following formulas: **(i)** q_0; **(ii)** $K\Box(q_{i-1} \to \hat{K}\Diamond(q_i \wedge Kp_i) \wedge \hat{K}\Diamond(q_i \wedge K\neg p_i))$ for each positive integer i such that $i \leq n$ and $Q_i = \forall$; **(iii)** $K\Box(q_{i-1} \to \hat{K}\Diamond(q_i \wedge Kp_i) \vee \hat{K}\Diamond(q_i \wedge K\neg p_i))$ for each positive integer i such that $i \leq n$ and $Q_i = \exists$; **(iv)** $K(q_n \to \varphi)$. The next lemma explains the relationship between $[Q_1p_1 \ldots Q_np_n\varphi(p_1, \ldots, p_n)]$ and $Q_1p_1 \ldots Q_np_n\varphi(p_1, \ldots, p_n)$.

Lemma 6. *A Q* $A = Q_1p_1 \ldots Q_np_n\varphi(p_1, \ldots, p_n)$ *holds iff* $[A]$ *is satisfied.*

Proposition 10. *The membership problem in the set of all valid formulas is* $PSPACE$*-hard.*

Proof. By Lemma 6, the QBF-validity problem is reducible to the membership problem in the set of all valid formulas. Since the QBF-validity problem is $PSPACE$-hard [16, Theorem 19.1], then the membership problem in the set of all valid formulas is $PSPACE$-hard.

3 Subset Space Logic with Announcements

3.1 Syntax and Semantics

We consider an extension $wSSL_a$ of $wSSL$ with announcements operators.

The set For_a of all formulas with announcements over Var (with typical members denoted φ, ψ, etc) is defined by the rule

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid (\varphi \vee \psi) \mid K\varphi \mid \Box\varphi \mid [\varphi]\psi.$$

We define $\langle\varphi\rangle\psi ::= \neg[\varphi]\neg\psi$.

The definition of the satisfiability of the formula $[\varphi]\psi$ in a frame $\mathcal{F} = (X, S, W)$ with respect to a valuation θ on $\mathcal{F}$ at $(x, U) \in W$ is defined as follows: $\mathcal{F}, \theta, (x, U) \models [\varphi]\psi$ iff if $\mathcal{F}, \theta, (x, U) \models \varphi$ then $(X, S, W_{|\varphi}), \theta, (x, U) \models \psi$ where $W_{|\varphi} = \{(y, V)$: $(y, V) \in W$ is such that $\mathcal{F}, \theta, (y, V) \models \varphi\}$. The following propositions are basic.

Proposition 11. *The following formulas are valid:* $[\varphi]p \leftrightarrow (\varphi \to p)$, $[\varphi]\bot \leftrightarrow \neg\varphi$, $[\varphi]\neg\psi \leftrightarrow (\varphi \to \neg[\varphi]\psi)$, $[\varphi](\psi \vee \chi) \leftrightarrow ([\varphi]\psi \vee [\varphi]\chi)$, $[\varphi]K\psi \leftrightarrow (\varphi \to K[\varphi]\psi)$, $[\varphi]\Box\psi \leftrightarrow (\varphi \to \Box[\varphi]\psi)$, $[\varphi][\psi]\chi \leftrightarrow [\langle\varphi\rangle\psi]\chi$.

Let tr: $For_a \to For$ be the standard meaning-preserving translation from For_a to For. It can be defined inductively in a standard way using equivalences from Proposition 11. This translation has been considered in several places (cf. [7]).

Proposition 12. *For all formulas φ in For_a, there exists a formula $\psi(= tr(\varphi))$ in For such that $\models \varphi \leftrightarrow \psi$.*

3.2 Axiomatization/Completeness

The axioms of $wSSL_a$ are all axioms of $wSSL$ plus all the formulas from Proposition 11. The rules of inference of $wSSL_a$ are all rules of inference of $wSSL$ plus the following rule of inference: $[\varphi]$-generalization (from ψ infer $[\varphi]\psi$).

For our purpose, the following crucial property of the translation tr can be proved by induction.

Proposition 13. *Let φ be a formula in For_a. $tr(\varphi) \leftrightarrow \varphi$ is $wSSL_a$-provable. And if φ is $wSSL_a$-provable then $\models \varphi$.*

Referring to Proposition 4, we obtain the

Proposition 14. *Let φ be a formula in For_a. If $\models \varphi$ then φ is $wSSL_a$-provable.*

Proof. Suppose φ is not $wSSL_a$-provable. Hence, by Proposition 13, $tr(\varphi)$ is not $wSSL_a$-provable. Thus, $tr(\varphi)$ is not $wSSL$-provable. Therefore, by Proposition 4, $\not\models tr(\varphi)$. Consequently, by Proposition 12, $\not\models \varphi$.

3.3 Decidability and Complexity

We will following the line of reasoning suggested in [15]. Proof details are omitted.

Proposition 15. *The membership problem in the set of all valid formulas is in PSPACE.*

Proposition 16. *The membership problem in the set of all valid formulas is PSPACE-hard.*

Proof. By Proposition 10.

4 Subset Space Logic with Arbitrary Announcements

4.1 Syntax and Semantics

We consider an extension $wSSL_{aa}$ of $wSSL_a$ wherein we can express what becomes true without explicit reference to announcements realizing that.

The set For_{aa} of all formulas with arbitrary announcements over Var (with typical members denoted φ, ψ, etc) is defined by the rule

$$\varphi ::= p \mid \bot \mid \neg\varphi \mid (\varphi \vee \psi) \mid K\varphi \mid \Box\varphi \mid [\varphi]\psi \mid [!]\varphi.$$

We define $\langle ! \rangle\varphi ::= \neg[!]\neg\varphi$. For the definition of the [!]-special rule of inference in section 4.2, we will need formulas of a special form, called admissible forms. Let $\sharp$ be a new propositional variable. The set $AF(Var)$ of all admissible forms over Var (with typical members denoted A, B, etc) is defined by the rule

$$A ::= \sharp \mid \varphi \to A \mid KA \mid \Box A.$$

Note that in each admissible form A, $\sharp$ has a unique occurrence. Given an admissible form $A(\sharp)$ and a formula φ, let $A(\varphi)$ be the result of the replacement of $\sharp$ in its place in A with φ. The definition of the satisfiability of the formula $[!]\varphi$ in a frame $\mathcal{F} = (X, S, W)$ with respect to a valuation θ on $\mathcal{F}$ at $(x, U) \in W$ is defined as follows: $\mathcal{F}, \theta, (x, U) \models [!]\varphi$ iff for all formulas ψ in For_a, if $\mathcal{F}, \theta, (x, U) \models \psi$ then $(X, S, W_{|\psi}), \theta, (x, U) \models \psi$. The following propositions are basic.

Proposition 17. *The following formulas are valid:* $[!]\varphi \to \varphi$, $[!]\varphi \to [!][!]\varphi$, $[!]\langle ! \rangle\varphi \to \langle ! \rangle[!]\varphi$, $\langle ! \rangle[!]\varphi \to [!]\langle ! \rangle\varphi$.

The following proposition can be proved similar to Proposition 3.9 in [2].

Proposition 18. $\models K[!]\varphi \to [!]K\varphi$.

Although for all formulas φ, $K[!]\varphi \to [!]K\varphi$ is valid, there exists formulas φ such that $[!]K\varphi \to K[!]\varphi$ is not valid.

Example 1. For example, one may consider the formula $\varphi = \Diamond\hat{K}p$. In the frame $\mathcal{F} = (X, S, W)$ where $X = \{x, y\}$, $S = \{\{x\}, \{x, y\}\}$ and $W = \{(x, \{x\}), (x, \{x, y\}), (y, \{x, y\})\}$, with respect to a valuation θ on $\mathcal{F}$ such that $\theta(p) = \{x\}$, $(x, \{x, y\})$ does not satisfy $[!]K\varphi \to K[!]\varphi$.

Let us show that there exists a formula that is equivalent to no formula in For_a.

Example 2. To illustrate the truth of this, take the case of the formula $\varphi = [!](\Box\hat{K}\Diamond Kp \to \Diamond Kp)$ and assume that $[!]$-free formula ψ is equivalent to φ and let q is a new variable $q \notin Var(\psi)$. Consider the frame $\mathcal{F} = (X, S, W)$ where $X = \{x, y\}$, $S = \{\{x, y\}\}$ and $W = \{(x, \{x, y\}), (y, \{x, y\})\}$, the valuation θ on $\mathcal{F}$ such that $\theta(p) = \{x\}$, $\theta(q) = \emptyset$ and $\theta(r) = \emptyset$ for each propositional variable $r \neq p, q$, the frame $\mathcal{F}' = (X', S', W')$ where

$$\begin{aligned} X' &= \{x'_1, x'_2, y'_1, y'_2\}, \\ S' &= \{\{x'_1, y'_1\}, \{x'_1, x'_2, y'_1, y'_2\}\}, \\ W' &= \{(x'_1, \{x'_1, y'_1\}), (x'_1, X'), (y'_1, \{x'_1, y'_1\}), (y'_1, X'), (x'_2, X'), (y'_2, X')\} \end{aligned}$$

and the valuation θ' on $\mathcal{F}'$ such that $\theta'(p) = \{x'_1, x'_2\}$, $\theta'(q) = \{x'_1, y'_1\}$ and $\theta(r) = \emptyset$ for each propositional variable $r \neq p, q$.

It easy to check that M and $M' = (F', \theta')$ are bisimilar in the language without q (bisimilation connects elements without prime and corresponding elements with prime and an index). So ψ is true or false at all bisimilar pairs simultaneously. Formula $\Box\hat{K}\Diamond Kp \to \Diamond Kp$ is true in M and after any restriction and hence $M, (x, X) \models \varphi$ and $M, (x, X) \models \psi$ and $M', (x'_1, X') \models \psi$. But $M', (x'_1, X') \not\models \psi$ because $M', (x'_1, X') \not\models [p \vee \neg q](\Box\hat{K}\Diamond Kp \to \Diamond Kp)$.

4.2 Axiomatization and Completeness

The axioms of $wSSL_{aa}$ are all axioms of $wSSL_a$ plus the following formulas: $[!]\varphi \to [\psi]\varphi$ for all formulas ψ in For_a. The rules of inference of $wSSL_{aa}$ are all rules of inference of $wSSL_a$ plus the following rule of inference: $[!]$-special rule (from $\{A([\psi]\varphi)$: ψ is a formula in $For_a\}$ infer $A([!]\varphi)$). A formula φ is said to be $wSSL_{aa}$-provable iff φ belongs to the least set of formulas containing all axioms of $wSSL_{aa}$ and closed with respect to all rules of inference of $wSSL_{aa}$. Here, the first result is

Proposition 19. *Let φ be a formula. If φ is $wSSL_{aa}$-provable then $\models \varphi$.*

Proof. It suffices to demonstrate the following properties: **(i)** the axioms of $wSSL_{aa}$ are valid; **(ii)** the rules of inference of $wSSL_{aa}$ preserve validity. The proof is left to the reader, we only describe the case of the $[!]$-special rule of inference. Let A be an admissible form and φ be a formula such that $\not\models A([!]\varphi)$. Hence, there exists a frame $\mathcal{F} = (X, S, W)$ such that $\mathcal{F} \not\models A([!]\varphi)$. Thus, there exists a valuation θ on $\mathcal{F}$ such that $\mathcal{F}, \theta \not\models A([!]\varphi)$. Therefore, there exists $(x, U) \in W$ such that $\mathcal{F}, \theta, (x, U) \not\models A([!]\varphi)$. By induction on A, one easily sees that there exists a formula ψ in For_a such that $\mathcal{F}, \theta, (x, U) \not\models A([\psi]\varphi)$. Consequently, $\mathcal{F}, \theta \not\models A([\psi]\varphi)$. Hence, $\mathcal{F} \not\models A([\psi]\varphi)$. Thus, $\not\models A([\psi]\varphi)$.

Proposition 20. *Let φ be a formula. If $\models \varphi$ then φ is $wSSL_{aa}$-provable.*

Proposition 20 is more difficult to establish than Proposition 19 and we defer proving it till the end of the section. In the meantime, we present some useful results. We shall define $wSSL_{aa}$-theories as sets $\mathit{\Gamma}$ of formulas satisfying the following conditions: **(i)** $\mathit{\Gamma}$ contains the set of all $wSSL_{aa}$-provable formulas; **(ii)** $\mathit{\Gamma}$ is closed under the rule of inference of modus ponens; **(iii)** $\mathit{\Gamma}$ is closed under the [!]-special rule. Of course, the analogue for $wSSL_{aa}$-theories of Proposition 5 holds. See [2, Lemma 4.12] for the proof of a similar result. We shall define the canonical model of $wSSL_{aa}$ in the same way as we have defined the canonical model of $wSSL$. Of course, the analogue for the canonical model of $wSSL_{aa}$ of Lemma 2 holds. Let $\mathcal{M}^c = (S^c, R^c_K, R^c_\Box, \theta^c)$ be the canonical model of $wSSL_{aa}$. Considering $\mathcal{M}^c$ as a Kripke model where the modal connectives K and $\Box$ are interpreted by means of the binary relations R^c_K and $R^c_\Box$ and where the modal connective [!] is interpreted as in $APAL$ (PAL with arbitrary announcements) [2], the proposition below contains a result that can be proved by induction on φ. See [2, Lemma 4.13] for the proof of a similar result.

Proposition 21. *Let φ be a formula. For all $\mathit{\Gamma} \in S^c$, we have for all finite sequences $(\psi_1, \ldots, \psi_n)$ of formulas, $\mathcal{M}^c, \mathit{\Gamma} \models [\psi_1] \ldots [\psi_n]\varphi$ iff $[\psi_1] \ldots [\psi_n]\varphi \in \mathit{\Gamma}$.*

We shall define the unraveling of the canonical model of $wSSL_{aa}$ in the same way as we have defined the unraveling of the canonical model of $wSSL$. Of course, the analogue for the unraveling of the canonical model of $wSSL_{aa}$ of Lemma 3 holds. Let $\mathit{\Gamma}_0$ be a maximal consistent $wSSL_{aa}$-theory and $\mathcal{M}^u = (S^u, R^u_K, R^u_\Box, \theta^u)$ be the unraveling of $\mathcal{M}^c$ around $\mathit{\Gamma}_0$. Considering $\mathcal{M}^u$ as a Kripke model where the modal connectives K and $\Box$ are interpreted by means of the binary relations R^u_K and $R^u_\Box$ and where the modal connective [!] is interpreted as in $APAL$ [2], the proposition below contains a result that can be proved by induction on φ.

Proposition 22. *Let φ be a formula. For all $(i_1, \mathit{\Gamma}_1, \ldots, i_m, \mathit{\Gamma}_m) \in S^u$, we have for all finite sequences $(\psi_1, \ldots, \psi_n)$ of formulas, $\mathcal{M}^u, (i_1, \mathit{\Gamma}_1, \ldots, i_m, \mathit{\Gamma}_m) \models [\psi_1] \ldots [\psi_n]\varphi$ iff $\mathcal{M}^c, \mathit{\Gamma}_m \models [\psi_1] \ldots [\psi_n]\varphi$.*

Let $\equiv^u$ be the symmetric and transitive closure of $R^u_\Box$ and $\preceq^u$ be the transitive closure of $R^u_K \circ R^u_\Box$. Obviously, $\equiv^u$ is reflexive, symmetrical and transitive and $\preceq^u$ is reflexive and transitive. Let $\boldsymbol{\Gamma} \in S^u$. The equivalence class modulo $\equiv^u$ with $\boldsymbol{\Gamma}$ as its representative is denoted $[\boldsymbol{\Gamma}]_{\equiv^u}$. The set of all equivalence classes of S^u modulo $\equiv^u$ is denoted $S^u/\equiv^u$. Let f be the function assigning to each $\boldsymbol{\Gamma} \in S^u$ the subset $f(\boldsymbol{\Gamma})$ of $S^u/\equiv^u$ defined by $[\boldsymbol{\Delta}]_{\equiv^u} \in f(\boldsymbol{\Gamma})$ iff $\boldsymbol{\Gamma} \preceq^u \boldsymbol{\Delta}$. Since $\preceq^u$ is reflexive, then $[\boldsymbol{\Gamma}]_{\equiv^u} \in f(\boldsymbol{\Gamma})$. We shall spatialize $\mathcal{M}^u$ in the same way as we have spatialized the unraveling of the canonical model of $wSSL$. The spatialization of $\mathcal{M}^u$ consists of the frame $\mathcal{F}^s = (X^s, S^s, W^s)$ and the valuation θ^s on $\mathcal{F}^s$ defined as follows: **(i)** X^s is the set of all equivalence classes of S^u modulo $\equiv^u$; **(ii)** S^s is the range of f; **(iii)** W^s is the set of all pairs $([\boldsymbol{\Gamma}]_{\equiv^u}, f(\boldsymbol{\Gamma}))$ such that $\boldsymbol{\Gamma} \in S^u$; **(iv)** θ^s is the function assigning to each $p \in \mathit{Var}$ the subset $\theta^s(p)$ of X^s defined by $[\boldsymbol{\Gamma}]_{\equiv^u} \in \theta^s(p)$ iff $\boldsymbol{\Gamma} \in \theta^u(p)$. The interesting result is the following

Proposition 23. *Let φ be a formula. For all $\boldsymbol{\Gamma} \in S^u$, we have for all finite sequences $(\psi_1, \ldots, \psi_n)$ of formulas, $\mathcal{F}^s, \theta^s, ([\boldsymbol{\Gamma}]_{\equiv^u}, f(\boldsymbol{\Gamma})) \models [\psi_1] \ldots [\psi_n]\varphi$ iff $\mathcal{M}^u, \boldsymbol{\Gamma} \models [\psi_1] \ldots [\psi_n]\varphi$.*

4.3 Decidability/Complexity

As for the membership problem in the set of all valid formulas, we do know whether it is decidable or not. Remark that the membership problem in the set of all valid formulas defined in the Section 4 of [2] was proved to be undecidable by French and van Ditmarsch [9].

5 Variants and Open Problems

There are several ways to continue this research. One way is by adding overlap operator or (and) by considering multiple agents, as in the interesting recent [1]. The other way is to try to return to the classical subset spaces, in particular we can ask what formulas can be announced so that the restricted model would still be a classical subset space.

Acknowledgements. We make a point of thanking the colleagues of the *Institut de recherche en informatique de Toulouse* who, by the discussions we had with them, contributed to the development of the work we present today. In particular, we want to thank Andreas Herzig for his helpful comments and his useful suggestions. We thank Yì Wáng for his encouragement and observations. We thank the ICLA reviewers for their constructive comments.

References

1. Wáng, Y.N., Ågotnes, T.: Subset Space Public Announcement Logic. In: Lodaya, K. (ed.) ICLA 2013. LNCS, vol. 7750, Springer, Heidelberg (2013)
2. Balbiani, P., Baltag, A., van Ditmarsch, H., Herzig, A., Hoshi, T., de Lima, T.: 'Knowable' as 'known after an announcement'. The Review of Symbolic Logic 1, 305–334 (2008)
3. Başkent, C.: Topics in Subset Space Logic. Master Thesis of the Universiteit van Amsterdam (2007)
4. Başkent, C.: Public Announcement Logic in Geometric Frameworks. Fundamenta Informaticae 114, 1–17 (2012)
5. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge University Press (2001)
6. Dabrowski, A., Moss, L., Parikh, R.: Topological reasoning and the logic of knowledge. Annals of Pure and Applied Logic 78, 73–110 (1996)
7. Van Ditmarsch, H., van der Hoek, W., Kooi, B.: Dynamic Epistemic Logic. Springer (2007)
8. Van Ditmarsch, H., Ruan, J., Verbrugge, R.: Sum and product in dynamic epistemic logic. Journal of Logic and Computation 18, 563–588 (2008)
9. French, T., Van Ditmarsch, H.: Undecidability for arbitrary public announcement logic. In: Advances in Modal Logic, pp. 23–42 (2008)
10. Goldblatt, R.: Logics of Time and Computation. Center for the Study of Language and Computation (1992)

11. Halpern, J.: The effect of bounding the number of primitive propositions and the depth of nesting on the complexity of modal logic. Artificial Intelligence 65, 361–372 (1995)
12. Heinemann, B.: Regarding overlaps in topologic. In: AiML, vol. 6. Kings College Publications, London (2006)
13. Heinemann, B.: Topology and Knowledge of Multiple Agents. In: Geffner, H., Prada, R., Machado Alexandre, I., David, N. (eds.) IBERAMIA 2008. LNCS (LNAI), vol. 5290, pp. 1–10. Springer, Heidelberg (2008)
14. Kurucz, A.: Combining modal logics. In: Blackburn, P., van Benthem, J., Wolter, F. (eds.) Handbook of Modal Logic, pp. 869–924. Elsevier (2007)
15. Lutz, C.: Complexity and succinctness of public announcement logic. In: AAMAS, pp. 137–143 (2006)
16. Papadimitriou, C.: Computational Complexity. Addison-Wesley (1994)
17. Parikh, R., Moss, L., Steinsvold, C.: Topology and epistemic logic. In: Handbook of Spatial Logics, pp. 299–341. Springer (2007)
18. Plaza, J.: Logics of public communications. Synthese 158, 165–179 (2007)

Appendix

A Counterexample to PAL SSL

In the original text [3] by Can Başkent the definition is inconsistent. In a more recent text (see [4]) this definition has been corrected, but unfortunately other problems remain. In the following text we will try to present the intrinsic difficulties of introducing public announcements to SSL.

Let us consider the following subset space (in classical sense, see [6]) $M = (X, O, V)$, where $X = \{x, y\}$, $O = P(X)$ — all subsets of X, and the valuation is such that $V(p) = \{y\}$. Then consider formula $\varphi = K\neg p \vee \Box p$. The list of all neighborhood situations where φ is true is following

$$(\varphi) = \{(x, \{x\}), (y, X), (y, \{y\})\}$$

So as suggested in [3] to construct the restricted model $M_\varphi = (X_\varphi, O_\varphi, V_\varphi)$ we need to take

$$X_\varphi = (\varphi)_1 = \{x \mid \exists U((x, U) \in (\varphi))\}, \quad O_\varphi = \{U \cap X_\varphi \mid \exists x((x, U) \in (\varphi))\}$$

In our case

$$X_\varphi = X \quad O_\varphi = O \text{ and } M_\varphi = M.$$

So the restricted model after the announcement of formula φ which is not valid in M is $M_\varphi = M$. This is a problem because formula $[\varphi]K\varphi \leftrightarrow (\varphi \to K[\varphi]\varphi$ which should be an axiom of PAL is not universally true. In particular $(y, X) \nvDash [\varphi]K\varphi$ and $(y, X) \vDash K[\varphi]\varphi$.

The problem as we see it is that subset space frame has inner structure similar to product of frames and the set of situations where a formula is true not always preserves this structure. One way to confront this problem is to consider generalized subset spaces. In this paper we explore this way.

Subset Space Public Announcement Logic

Yì N. Wáng[1,3,⋆] and Thomas Ågotnes[2,3,1]

[1] Department of Computing, Mathematics and Physics
Bergen University College, Norway
[2] Institute of Logic and Intelligence, Southwest University, China
[3] Department of Information Science and Media Studies
University of Bergen, Norway
`yi.wang@hib.no`, `thomas.agotnes@infomedia.uib.no`

Abstract. The logic of public announcements has received great interest in recent years. In this paper we give an account of public announcements in terms of the semantics of subset space logic (SSL). In particular, we give a natural interpretation of the language of public announcement logic (PAL) in subset models, and show that it embeds PAL. We give sound and complete axiomatisations of different variants of the logic. Unlike in other work combining PAL and SSL, the goal is not to import PAL operators with update semantics into SSL, but to give an alternative semantics for PAL: using neighborhoods *instead* of model updates.

Keywords: subset space logic, epistemic logic, public announcement logic, expressivity, arbitrary announcements, topology.

1 Introduction

Epistemic logics [1, 2] formalise reasoning about knowledge. In recent years there has been a great interest in *dynamic* epistemic logics [3]; extension of epistemic logics for reasoning about the epistemic pre- and post-conditions of different types of events. The simplest, and most well-understood, dynamic epistemic logic is *public announcement logic (PAL)* [4], where events are taken to be truthful public announcements. From the logical point of view, standard epistemic logic is the modal logic S5, and occurrences of events are modeled by updating (i.e., modifying) the S5 models.

A different approach to making epistemic logic dynamic is *subset space logic*, originally due to Moss and Parikh [5]. In this logic the semantics of knowledge modalities, as well as modalities modeling potentially information-changing *effort*, is a topological one in terms of so-called *subset structures*. Different from standard topological semantics for modal logic originating in [6, 7], however, this logic uses a variant of the semantics where a state is not merely a *(full information) point*, but rather what is called an *epistemic scenario* consisting of a point together with an *epistemic range*. The epistemic range is not fixed: it can shrink as the result of an effort made by the agent. The possible consequences of efforts are modeled explicitly in the semantic structures.

[⋆] The author gratefully acknowledges funding support from the Major Project of National Social Science Foundation of China (No. 11&ZD088).

K. Lodaya (Ed.): ICLA 2013, LNAI 7750, pp. 245–257, 2013.

That there are close conceptual relationships between dynamic epistemic logics and subset space logic is obvious: both model knowledge dynamics. In this paper we study one aspect of the relationship between PAL and subset space logic. In particular, we give a natural interpretation of the language of PAL in subset structures, explaining changes made by public announcements in terms of the explicitly modeled subset space rather than using model updates. The resulting logic embeds public announcement logic.

The idea of interpreting public announcement operators in subset structures is not entirely new. Baskent [8, 9] gives an interpretation of the combined PAL and subset logic language in subset structures, and proves completeness of PAL with respect to this semantics. However, the interpretation of public announcement operators is defined in terms of *updates on subset structures*. The goal of the current paper is to give an interpretation of the PAL language in subset structures that is closer to the key conceptual idea of subset space logic, namely that all the possible consequences of efforts are explicitly represented in the semantic structures, as an *alternative* to update semantics, which is very different from extending subset space logic with update semantics for public announcement logic as done in [8, 9]. Recent work in [10] also uses the same type of update semantics as in [8, 9]. We discuss related work further in Section 6.

Our resulting logic is weaker than PAL; not all subset models correspond to PAL models. We give a sound and complete axiomatisation of the resulting logic. Suitably restricting the class of subset models, we also get soundness and completeness of PAL with respect to our interpretation in subset structures. Thus, we obtain a new and alternative semantics for traditional public announcement logic, as well as a weaker and conceptually interesting logic. We also investigate some other variants of the logical language, and discuss expressive power.

In this paper we only consider the single-agent version of PAL (see also Section 6).

The remainder of the paper is organised as follows. In the next section we briefly review public announcement logic and subset space logic. In Section 3 we give the interpretation of the PAL language in subset structures, and discuss the expressivity of different variants of the language. Then, in Section 4, we investigate translations between Kripke semantics and subset space semantics, and, in Section 5, we study axiomatisations of the resulting logics. We conclude with a discussion in Section 6. Some proofs are unfortunately sketched or omitted due to lack of space.

2 Background

Let PROP be a countable set of propositional variables.

2.1 Public Announcement Logic

Public announcement logic (PAL) [4] extends classical (static) epistemic logic (EL) with an operator which can be used to express public announcements. It is one of the simplest dynamic epistemic logics, and has been investigated extensively in the past few decades. We introduce below some basic definitions and results of classical epistemic logic and public announcement logic which we will use later. For a full introduction we refer to [3]. The definition of PAL is normally parameterised by a set of agents, but in this paper we will only be concerned with the single-agent case and when we refer to PAL in the following we implicitly mean that variant.

Definition 1 (Languages). *The languages of (single-agent) classical epistemic logic, $\mathcal{EL}$, and of (single-agent) public announcement logic, $\mathcal{PAL}$, are:*

$$\begin{array}{rl}(\mathcal{EL}) & \varphi ::= \bot \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K\varphi \\ (\mathcal{PAL}) & \varphi ::= \bot \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K\varphi \mid [\varphi]\varphi,\end{array}$$

where $p \in$ PROP. We write $\hat{K}\varphi$ as a shorthand for $\neg K \neg\varphi$, and $\langle\varphi\rangle\psi$ for $\neg[\varphi]\neg\psi$.

Interpretation of these languages is defined in terms of *epistemic (Kripke, S5) models* $\mathfrak{M} = (M, \sim, V)$ consisting of a set of *states/points* M, an *indistiguishability relation* $\sim$ which is an equivalence relation on M, and a *valuation function* $V :$ PROP $\rightarrow M$.

Definition 2 (Kripke semantics). *Given an epistemic model $\mathfrak{M} = (M, \sim, V)$ and a point $m \in M$, the satisfaction relation, $\Vdash$, is defined as follows. $\mathfrak{M}, m \nVdash \bot$, and:*

$$\begin{array}{lll}\mathfrak{M}, m \Vdash p & \textit{iff} & m \in V(p) \\ \mathfrak{M}, m \Vdash \neg\varphi & \textit{iff} & \mathfrak{M}, m \nVdash \varphi \\ \mathfrak{M}, m \Vdash \varphi \wedge \psi & \textit{iff} & \mathfrak{M}, m \Vdash \varphi \mathbin{\&} \mathfrak{M}, m \Vdash \psi \\ \mathfrak{M}, m \Vdash K\varphi & \textit{iff} & \forall n \in M.\ (m \sim n \Rightarrow \mathfrak{M}, n \Vdash \varphi) \\ \mathfrak{M}, m \Vdash [\varphi]\psi & \textit{iff} & \mathfrak{M}, m \Vdash \varphi \Rightarrow \mathfrak{M}|\varphi, m \Vdash \psi,\end{array}$$

In the above, $\mathfrak{M}|\varphi$ is the submodel of $\mathfrak{M}$ having $[\![\varphi]\!]^{\mathfrak{M}}$, where $[\![\varphi]\!]^{\mathfrak{M}} = \{n \mid \mathfrak{M}, n \Vdash \varphi\}$ is the truth set *of φ in $\mathfrak{M}$, as states and where $\sim$ and V are restricted to $[\![\varphi]\!]^{\mathfrak{M}}$.* Validity *is defined as usual.* ⊣

$\mathcal{PAL}$ is as expressive as $\mathcal{EL}$ [4]. A sound and complete axiomatisation for EL is the well-known Hilbert system **S5** (Fig. 1). The axiomatisation **PAL** for PAL (Fig. 1) is obtained by adding to **S5** reduction axioms for the public announcement operators [4, 11, 12].

(PC)	Instances of tautologies	(MP)	$\vdash \varphi \mathbin{\&} \vdash \varphi \rightarrow \psi \Rightarrow \vdash \psi$
(N)	$\vdash \varphi \Rightarrow \vdash K\varphi$	(K)	$K(\varphi \rightarrow \psi) \rightarrow K\varphi \rightarrow K\psi$
(T)	$K\varphi \rightarrow \varphi$	(5)	$\neg K\varphi \rightarrow K\neg K\varphi$
(AP)	$[\varphi]p \leftrightarrow (\varphi \rightarrow p), p \in$ PROP	(AN)	$[\varphi]\neg\psi \leftrightarrow (\varphi \rightarrow \neg[\varphi]\psi)$
(AC)	$[\varphi](\psi \wedge \chi) \leftrightarrow ([\varphi]\psi \wedge [\varphi]\chi)$	(AK)	$[\varphi]K\psi \leftrightarrow (\varphi \rightarrow K[\varphi]\psi)$
(AM)	$[\varphi][\psi]\chi \leftrightarrow [\varphi \wedge [\varphi]\psi]\chi$		

Fig. 1. PAL, the axiomatisation of public announcement logic, and the sub-system **S5** consisting of (PC), (MP), (N), (K), (T) and (5). The 4 axiom, i.e., $K\varphi \rightarrow KK\varphi$, meaning *positive introspection*, is often also included, but technically redundant — it can be derived in **S5**.

2.2 Subset Space Logic

The study of subset space logic (SSL) was initiated in [5]. One of the main motivations was to characterise epistemic efforts in a reasonably simple framework. Below we briefly introduce the classical subset space logic, and we refer to [13] for more details.

Definition 3 (Language). *The language* $\mathcal{SSL}$ *has the following grammar:*

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K\varphi \mid \Box\varphi,$$

where $p \in \textsc{prop}$. *We write* $\hat{K}\varphi$ *as a shorthand for* $\neg K \neg\varphi$, *and* $\Diamond\varphi$ *for* $\neg\Box\neg\varphi$.

Intuitively, $K\varphi$ reads as "φ is known in the current situation", while $\Diamond\varphi$ reads as "there is a refinement of knowledge (e.g., a new evidence) under which φ is true". One of the most interesting $\mathcal{SSL}$-sentences is $\neg K\varphi \wedge \Diamond K\varphi$, which reads as "$\varphi$ is not known under the current situation, but there is a refinement of knowledge to make φ known". Formally the semantics is defined as follows.

Definition 4 (Subset structures). *A pair* $(X, \mathcal{O})$ *is called a* subset space*, if* X *is a non-empty set and* $\mathcal{O} \subseteq \wp(X)$. *A* subset model *is a tuple* $\mathcal{X} = (X, \mathcal{O}, V)$ *where* $(X, \mathcal{O})$ *is a subset space and* $V : \textsc{prop} \to \wp(X)$ *is an evaluation function.*

For historical reasons, elements of $\mathcal{O}$ are called *open sets* or simply *opens*. For any subset model $\mathcal{X} = (X, \mathcal{O}, V)$, we take a point $x \in X$ as a factual state, and an $O \in \mathcal{O}$ as an *epistemic range* or *evidence*. A pair (x, O) is called an *epistemic scenario* (or simply *scenario*) of $\mathcal{X}$ if it holds that $x \in O$. The set of all epistemic scenarios of $\mathcal{X}$ is denoted by $ES(\mathcal{X})$. A *pointed subset space* (resp. *pointed subset model*) is a subset space (resp. subset model) together with an epistemic scenario of it.

Definition 5 (Semantics). *Let* $\mathcal{X} = (X, \mathcal{O}, V)$ *be a subset model, and* $(x, O) \in ES(\mathcal{X})$. *The satisfaction relation,* $\models$, *is given as follows:*

$$\begin{array}{lll}
\mathcal{X}, x, O \models p & \textit{iff} & x \in V(p) \\
\mathcal{X}, x, O \models \neg\varphi & \textit{iff} & \mathcal{X}, x, O \not\models \varphi \\
\mathcal{X}, x, O \models \varphi \wedge \psi & \textit{iff} & \mathcal{X}, x, O \models \varphi \;\&\; \mathcal{X}, x, O \models \psi \\
\mathcal{X}, x, O \models K\varphi & \textit{iff} & \forall y \in O.\, \mathcal{X}, y, O \models \varphi \\
\mathcal{X}, x, O \models \Box\varphi & \textit{iff} & \forall U \in \mathcal{O}.\, (x \in U \subseteq O \Rightarrow \mathcal{X}, x, U \models \varphi).
\end{array}$$

We stress that satisfaction is undefined for a pair (x, O) *with* $x \notin O$. *We write* $\mathcal{X} \models \varphi$ *(read as "*φ *is globally true in the subset model* $\mathcal{X}$*"), if* $\mathcal{X}, (x, O) \models \varphi$ *holds for all* $(x, O) \in ES(\mathcal{X})$. *In a similar fashion, we can define the validity of* φ *in a subset space* $(X, \mathcal{O})$ *(notation:* $X, \mathcal{O} \models \varphi$*), global validity (notation:* $\models \varphi$*), and so on.* ⊣

A sound and complete [5, 14] axiomatisation **SSL** of subset space logic is given in Fig. 2. Among the axioms and rules, PC, K•, T•, 5•, N• and MP compose an S5 system for the knowledge operator K, while PC, K∘, T∘, 4∘, N∘ and MP compose an S4 system for the refinement operator $\Box$. There are two extra axioms: AP which stands for *atomic persistence* and Cr for *cross*.

(PC) Instances of tautologies	(MP) $\vdash \varphi$ & $\vdash \varphi \to \psi \Rightarrow \vdash \psi$
(K•) $K(\varphi \to \psi) \to K\varphi \to K\psi$	(K∘) $\Box(\varphi \to \psi) \to \Box\varphi \to \Box\psi$
(T•) $K\varphi \to \varphi$	(T∘) $\Box\varphi \to \varphi$
(5•) $\neg K\varphi \to K\neg K\varphi$	(4∘) $\Box\varphi \to \Box\Box\varphi$
(N•) $\vdash \varphi \Rightarrow \vdash K\varphi$	(N∘) $\vdash \varphi \Rightarrow \vdash \Box\varphi$
(Cr) $K\Box\varphi \to \Box K\varphi$	(AP) $(p \to \Box p) \wedge (\neg p \to \Box\neg p), p \in \textsc{prop}$

Fig. 2. The axiomatisation **SSL** of subset space logic

3 Incorporating Public Announcements into SSL

The key question related to incorporating public announcements into subset space logic is: how to model changes made by public announcements in terms of subset models? As discussed in the introduction, the goal is to give an interpretation of the public announcement operators using neighborhood refinement in place of model updates.

3.1 How to Model Public Announcements in SSL?

Observe that the interpretation of the formula $[\varphi]\psi$ in PAL is in the following pattern:

$$\mathfrak{M}, m \Vdash [\varphi]\psi \quad \text{iff} \quad \mathfrak{M}, m \Vdash \mathsf{pre}(\varphi) \Rightarrow \mathfrak{M}', m \Vdash \psi$$

where $\mathsf{pre}(\varphi)$ stands for the *precondition* for announcing φ, while $\mathfrak{M}'$ is the model resulting from publicly announcing φ in the current model $\mathfrak{M}$. In classical public announcement logic, $\mathsf{pre}(\varphi)$ is φ merely itself; only announcements of true formulae can result in a (possible) change of a model. The above pattern has been used in various dynamic epistemic logics, such as arbitrary public announcement logic [15], group announcement logic [16], and action model logic [17]. Subset space logics with public announcements introduced in [9, 10] are in this pattern as well.

Following this pattern, we propose the following definition, using the subset space instead of model updates:

$$\mathcal{X}, x, O \models [\varphi]\psi \quad \text{iff} \quad \mathcal{X}, x, O \models \mathsf{pre}(\varphi) \Rightarrow \mathcal{X}, x, \llparenthesis\varphi\rrparenthesis^O \models \psi,$$

where $\llparenthesis\varphi\rrparenthesis^O = \{y \in O \mid \mathcal{X}, y, O \models \varphi\}$, and $\mathcal{X}, x, O \models \mathsf{pre}(\varphi)$ iff $x \in \llparenthesis\varphi\rrparenthesis^O \in \mathcal{O}$. In other words, an announcement can be made only when the truth set of the announced formula under the current neighborhood is indeed a valid sub-neighborhood.

We have a few more remarks on the formula $\mathsf{pre}(\varphi)$. The definition of the meaning of $\mathsf{pre}(\varphi)$ (i) makes it a precondition stronger than merely φ, (ii) behaves like an executability check of φ in the sense of [18–20], and (iii) is in the flavor of the $\Box$-operator under the classical neighborhood semantics for modal logic.

3.2 Logics and Expressivity

We will work with the languages $\mathcal{EL}$ and $\mathcal{PAL}$, of course, reinterpreted in the *subset semantics* (defined below).

Definition 6 (Subset semantics). *The following is a simultaneous definition of satisfaction for $\mathcal{EL}$ and $\mathcal{PAL}$. Given a subset model $\mathcal{X}$ and a scenario (x, O),*

$$\begin{array}{lll}
\mathcal{X}, x, O \not\models \bot & & \\
\mathcal{X}, x, O \models p & \textit{iff} & x \in V(p) \\
\mathcal{X}, x, O \models \neg\varphi & \textit{iff} & \mathcal{X}, x, O \not\models \varphi \\
\mathcal{X}, x, O \models \varphi \wedge \psi & \textit{iff} & \mathcal{X}, x, O \models \varphi \,\&\, \mathcal{X}, x, O \models \psi \\
\mathcal{X}, x, O \models K\varphi & \textit{iff} & \forall y \in O.\, \mathcal{X}, y, O \models \varphi \\
\mathcal{X}, x, O \models [\varphi]\psi & \textit{iff} & x \in \llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O} \Rightarrow \mathcal{X}, x, \llparenthesis\varphi\rrparenthesis^{O} \models \psi
\end{array}$$

where $\llparenthesis\varphi\rrparenthesis^{\mathcal{X},O} = \{y \in O \mid \mathcal{X}, y, O \models \varphi\}$ *is the* truth set of φ in $\mathcal{X}$ at O. *We often hide the parameter* $\mathcal{X}$ *of* $\llparenthesis\varphi\rrparenthesis^{\mathcal{X},O}$ *(and simply write* $\llparenthesis\varphi\rrparenthesis^{O}$*), as it is usually clear from the context. Validity is defined as usual. Note that* $\llparenthesis\varphi\rrparenthesis^{O} \subseteq O$ *always holds.* $\dashv$

We shall call the above defined semantics *subset semantics*, in comparison to Kripke semantics. As discussed in Section 3.1, we are interested in the sentence $\mathsf{pre}(\varphi)$, which is interpreted in subset semantics by

$$\mathcal{X}, x, O \models \mathsf{pre}(\varphi) \quad \text{iff} \quad x \in \llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O}.$$

It is easy to verify that $\mathsf{pre}(\varphi)$ is definable in $\mathcal{PAL}$ by $\neg[\varphi]\bot$. We treat $\mathsf{pre}(\varphi)$ as an abbreviation of $\neg[\varphi]\bot$, as long as it is not primitive in the language.

Proposition 7. *For any $\varphi, \psi \in \mathcal{PAL}$, the following hold:*

1. $\models \neg\mathsf{pre}(\bot)$
2. $\models \mathsf{pre}(\varphi) \to \neg\mathsf{pre}(\neg\varphi)$
3. $\models \mathsf{pre}(\varphi) \to \varphi$
4. $\models \mathsf{pre}(\varphi) \to \mathsf{pre}(\mathsf{pre}(\varphi))$
5. $\models K\varphi \to \mathsf{pre}(\varphi)$
6. $\models \varphi$ *implies* $\models K\varphi$
7. $\models \mathsf{pre}(\varphi) \to K(\varphi \to \mathsf{pre}(\varphi))$
8. $\models \neg(\varphi \to \mathsf{pre}(\varphi)) \to K\neg\mathsf{pre}(\varphi)$
9. $\models (\varphi \leftrightarrow \psi) \to (\mathsf{pre}(\varphi) \leftrightarrow \mathsf{pre}(\psi))$
10. $\not\models \mathsf{pre}(\varphi \to \psi) \to (\mathsf{pre}(\varphi) \to \mathsf{pre}(\psi))$
11. $\models \varphi$ *implies* $\models \mathsf{pre}(\varphi)$

Proof. 1 through 3 are easy. We first show 4 here. For any $\mathcal{X} = (X, \mathcal{O}, V)$ and any epistemic scenario (x, O), suppose $\mathcal{X}, x, O \models \mathsf{pre}(\varphi)$. Then, $\llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O}$, and therefore $\llparenthesis\mathsf{pre}(\varphi)\rrparenthesis^{O} = \{y \in O \,|\, \mathcal{X}, y, O \models \mathsf{pre}(\varphi)\} = \{y \in O \,|\, y \in \llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O}\} = \llparenthesis\varphi\rrparenthesis^{O}$. Hence, $\mathcal{X}, x, O \models \mathsf{pre}(\mathsf{pre}(\varphi))$ iff $x \in \llparenthesis\mathsf{pre}(\varphi)\rrparenthesis^{O} \in \mathcal{O}$ iff $x \in \llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O}$ iff $\mathcal{X}, x, O \models \mathsf{pre}(\varphi)$. Thus, we have $\mathcal{X}, x, O \models \mathsf{pre}(\mathsf{pre}(\varphi))$ under the supposition. Now we show 5. $\mathcal{X}, x, O \models K\varphi$ iff $\forall y \in O.\, \mathcal{X}, y, O \models \varphi$. Therefore $\llparenthesis\varphi\rrparenthesis^{O} = O$, and so $x \in \llparenthesis\varphi\rrparenthesis^{O} \in \mathcal{O}$. Hence $\mathcal{X}, x, O \models \mathsf{pre}(\varphi)$. Other proofs are omitted. $\square$

We now move on to discussing the expressive power of the defined languages.

Definition 8 (Partial bisimulation). *Given any two subset models, $\mathcal{X} = (X, \mathcal{O}, V)$ and $\mathcal{X}' = (X', \mathcal{O}', V')$, a non-empty relation $\rightleftarrows^{p}$ between $ES(\mathcal{X})$ and $ES(\mathcal{X}')$ is called a* partial bisimulation *between $\mathcal{X}$ and $\mathcal{X}'$, if the following hold for all $(x, O) \in ES(\mathcal{X})$ and $(x', O') \in ES(\mathcal{X}')$ such that $(x, O) \rightleftarrows^{p} (x', O')$:*

Atom *For any propositional variable p, $x \in V(p)$ iff $x' \in V(p)$;*
K-forth *If $y \in O$, then there is $y' \in O'$ such that $(y, O) \rightleftarrows^{p} (y', O')$;*
K-back *If $y' \in O'$, then there is $y \in O$ such that $(y, O) \rightleftarrows^{p} (y', O')$.*
We write $(\mathcal{X}, x, O) \rightleftarrows^{p} (\mathcal{X}', x', O')$, if $\mathcal{X} \rightleftarrows^{p} \mathcal{X}'$ links (x, O) and (x', O'). $\dashv$

Proposition 9 **($\mathcal{EL}$-invariance of partial bisimulation).** *Partial bisimulation implies $\mathcal{EL}$-equivalence. Namely, for any subset models $\mathcal{X}$ and $\mathcal{X}'$, any $(x, O) \in ES(\mathcal{X})$ and $(x', O') \in ES(\mathcal{X}')$,*

$$(\mathcal{X}, x, O) \rightleftarrows^{p} (\mathcal{X}', x', O') \quad \Rightarrow \quad \forall \varphi \in \mathcal{EL}.\ (\mathcal{X}, x, O \models \varphi \Leftrightarrow \mathcal{X}', x', O' \models \varphi).$$

Theorem 10. *$\mathcal{PAL}$ is strictly more expressive than $\mathcal{EL}$ (in subset semantics).*

Proof. We show that the $\mathcal{PAL}$-formula $\mathsf{pre}(p)$ is not equivalent to any $\mathcal{EL}$-formula. By Proposition 9, it suffices to show that $\mathsf{pre}(p)$ can distinguish two subset models which are partially bisimilar. Consider two subset models $\mathcal{X} = (\{x, y\}, \{\{x\}, \{x, y\}\}, V)$ and $\mathcal{Y} = (\{x, y\}, \{\{x\}\}, V)$ with $V(p) = \{x, y\}$. The relation $\{((x, \{x, y\}), (x, \{x\})), ((y, \{x, y\}), (x, \{x\}))\}$ reveals $(\mathcal{X}, x, \{x, y\}) \rightleftarrows^{p} (\mathcal{Y}, x, \{x\})$. But $\mathcal{X}, x, \{x, y\} \models \mathsf{pre}(p)$ while $\mathcal{Y}, x, \{x\} \not\models \mathsf{pre}(p)$. □

Theorem 11. *The following $\mathcal{PAL}$-formulae are valid (with $p \in$ PROP):*

$$\begin{array}{llll}
[\varphi]\bot & \leftrightarrow \neg \mathit{pre}(\varphi) & [\varphi](\psi \wedge \chi) & \leftrightarrow [\varphi]\psi \wedge [\varphi]\chi \\
[\varphi]p & \leftrightarrow \mathit{pre}(\varphi) \rightarrow p & [\varphi]K\psi & \leftrightarrow \mathit{pre}(\varphi) \rightarrow K[\varphi]\psi \\
[\varphi]\neg\psi & \leftrightarrow \mathit{pre}(\varphi) \rightarrow \neg[\varphi]\psi & [\varphi][\psi]\chi & \leftrightarrow [\mathit{pre}(\varphi) \wedge [\varphi]\mathit{pre}(\psi)]\chi.
\end{array}$$

4 Translations between Kripke Semantics and Subset Semantics

We work in the language $\mathcal{PAL}$. As a convention, we denote by PAL_K the logic resulting from interpreting $\mathcal{PAL}$ in Kripke models (i.e., standard public announcement logic), and by PAL_S the result of interpreting the same language in subset models. We write $\mathfrak{K}$ for the set of all $S5$ Kripke models, and $\mathfrak{S}$ the set of all subset models.

It is well known that in the single-agent setting, every $S5$ model is equivalent to an $S5$ model whose component relation is a *universal relation*, i.e., a model $(M, \sim, V)$ such that $\sim = M \times M$. In this section we implicitly assume (without loss of generalisation) that all $S5$ models are of this kind. The reason is that it simplifies the presentation, in particular because these $S5$ models are quite similar to standard subset models, as the reader will see.

Definition 12 **($\mathfrak{K}$-$\mathfrak{S}$-translation).** *We define a translation $\kappa : \mathfrak{K} \rightarrow \mathfrak{S}$ as follows. Let $\mathfrak{M} = (M, \sim, V)$ be an $S5$ model. Its translation, $\kappa(\mathfrak{M})$, is the subset model $(X, \mathcal{O}, \nu)$, such that $X = M$, $\mathcal{O} = \{[\![\varphi]\!]^{\mathfrak{M}|\psi} \mid \varphi, \psi \in \mathcal{PAL}\}$, and $\nu = V$.* ⊣

Theorem 13 **(κ-equivalence).** *Given an $S5$ model $\mathfrak{M} = (M, \sim, V)$, and $m \in M$, for any $\mathcal{PAL}$-formulae φ and α such that $\mathfrak{M}, m \Vdash \alpha$, it holds that $\mathfrak{M}|\alpha, m \Vdash \varphi$ iff $\kappa(\mathfrak{M}), m, [\![\alpha]\!]^{\mathfrak{M}} \models \varphi$.*

Proof. By induction on φ. Let $\kappa(\mathfrak{M}) = (X, \mathcal{O}, \nu)$. Note that i) for any φ, $[\![\varphi]\!]^{\mathfrak{M}|\top} = [\![\varphi]\!]^{\mathfrak{M}}$, and ii) $X \in \mathcal{O}$, since $X = [\![\top]\!]^{\mathfrak{M}}$. The base case and Boolean cases are easy to verify.

$$\begin{array}{lll} \mathfrak{M}|\alpha, m \Vdash K\psi & \text{iff} & \forall n \in \llbracket\alpha\rrbracket^{\mathfrak{M}}.\ \mathfrak{M}|\alpha, n \Vdash \psi \quad (\text{note that } \sim = M \times M) \\ & \text{iff} & \forall n \in \llbracket\alpha\rrbracket^{\mathfrak{M}}.\ \kappa(\mathfrak{M}), n, \llbracket\alpha\rrbracket^{\mathfrak{M}} \models \psi \qquad (\text{IH}) \\ & \text{iff} & \kappa(\mathfrak{M}), m, \llbracket\alpha\rrbracket^{\mathfrak{M}} \models K\psi. \end{array}$$

$$\begin{array}{ll} & \mathfrak{M}|\alpha, m \Vdash [\chi]\psi \\ \text{iff} & \mathfrak{M}|\alpha, m \Vdash \chi \Rightarrow \mathfrak{M}|\alpha|\chi, m \Vdash \psi \\ \text{iff} & \mathfrak{M}|\alpha, m \Vdash \chi \Rightarrow \mathfrak{M}|(\alpha \wedge [\alpha]\chi), m \Vdash \psi \qquad (\text{cf. [3, Proposition 4.17]}) \\ \text{iff} & \kappa(\mathfrak{M}), m, \llbracket\alpha\rrbracket^{\mathfrak{M}} \models \chi \Rightarrow \kappa(\mathfrak{M}), m, \llbracket\alpha \wedge [\alpha]\chi\rrbracket^{\mathfrak{M}} \models \psi \qquad (\text{IH}) \\ \text{iff} & m \in \llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}} \in \mathcal{O} \Rightarrow \kappa(\mathfrak{M}), m, \llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}} \models \psi \qquad (*) \\ \text{iff} & \kappa(\mathfrak{M}), m, \llbracket\alpha\rrbracket^{\mathfrak{M}} \models [\chi]\psi. \end{array}$$

We show $(*)$ in the above. First show that the antecedents match. Bottom up is clear; from top down, $m \in \llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}}$ is also clear. From $\llbracket\chi\rrbracket^{\mathfrak{M}|\alpha} = \llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}}$ which is guaranteed by IH, it follows that $\llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}} \in \mathcal{O}$ by the definition of κ. Then we show that the consequents are equivalent. It suffices to show $\llbracket\alpha \wedge [\alpha]\chi\rrbracket^{\mathfrak{M}} = \llparenthesis\chi\rrparenthesis^{\llbracket\alpha\rrbracket^{\mathfrak{M}}}$ under the condition $\mathfrak{M}, m \Vdash \alpha$. This is easy from definitions and IH. □

Corollary 14. *Given an $S5$ model $\mathfrak{M} = (M, \sim, V)$, and $m \in M$, for any $\mathcal{PAL}$-formula φ, $\mathfrak{M}, m \Vdash \varphi$ iff $\kappa(\mathfrak{M}), m, X \models \varphi$, where X is the domain of $\kappa(\mathfrak{M})$.*

Corollary 15. *PAL$_K$ is not weaker than PAL$_S$, i.e., all validities of PAL$_S$ are also validities of PAL$_K$.*

But is PAL$_K$ (strictly) stronger than PAL$_S$, namely, is there a $\mathcal{PAL}$-formula which is valid in PAL$_K$ but not in PAL$_S$? The answer is yes. Recall that the K-axiom for pre, i.e., $\mathsf{pre}(\varphi \to \psi) \to (\mathsf{pre}(\varphi) \to \mathsf{pre}(\psi))$, is not valid in PAL$_S$ (Proposition 7.10). This formula is valid in PAL$_K$, since in PAL$_K$ it is equivalent to $(\varphi \to \psi) \to (\varphi \to \psi)$. This translation illustrates a similarity between the pre-operator under subset semantics and the $\Box$-operator under neighborhood semantics (as we already mentioned in Section 3.1), giving weaker logical principles than under Kripke semantics.

We obtain standard public announcement logic by restricting the class of subset models. Let $\mathcal{X} = (X, \mathcal{O}, V)$ be a subset model. We say $\mathcal{X}$ is a *public announcement subset model* (*PASM* for short), if $\mathcal{O} = \{\llparenthesis\varphi\rrparenthesis^{\llparenthesis\psi\rrparenthesis^X} \mid \varphi, \psi \in \mathcal{PAL}\}$. Namely, $\mathcal{X}$ being a PASM requires that:

- (“All evidence is announceable”) for all $O \in \mathcal{O}$, there exists $\mathcal{PAL}$-formulae φ and ψ such that $O = \{x \mid \mathcal{X}, x, \llparenthesis\psi\rrparenthesis^X \models \varphi\}$, i.e., $O = \llparenthesis\varphi\rrparenthesis^{\llparenthesis\psi\rrparenthesis^X}$; and
- (“All announcements are evidence”) for all φ and ψ, $\llparenthesis\varphi\rrparenthesis^{\llparenthesis\psi\rrparenthesis^X} \in \mathcal{O}$.

Theorem 16 (Correspondence). *Every $S5$ model is equivalent to a PASM, and vice versa. That is, given a pointed $S5$ model, there exists a pointed PASM satisfying exactly the same $\mathcal{PAL}$-formulae; and given a pointed PASM, there exists a pointed $S5$ model satisfying exactly the same $\mathcal{PAL}$-formulae.*

Proof. Given an $S5$ model $\mathfrak{M}$, let $\kappa(\mathfrak{M}) = (X, \mathcal{O}, V)$. It suffices to show that $\kappa(\mathfrak{M})$ is a PASM. We show that $\llbracket\varphi\rrbracket^{\mathfrak{M}|\psi} = \llparenthesis\varphi\rrparenthesis^{\llparenthesis\psi\rrparenthesis^X}$ for every $\mathcal{PAL}$-formulae φ and ψ. First, $\llbracket\psi\rrbracket^{\mathfrak{M}} = \llparenthesis\psi\rrparenthesis^X$, for $m \in \llbracket\psi\rrbracket^{\mathfrak{M}}$ iff $\mathfrak{M}, m \Vdash \psi$ iff (by Corollary 14) $\kappa(\mathfrak{M}), m, X \models \psi$ iff $m \in \llparenthesis\psi\rrparenthesis^X$. Therefore, $m \in \llbracket\varphi\rrbracket^{\mathfrak{M}|\psi}$ iff $\mathfrak{M}|\psi, m \Vdash \varphi$ iff (by Theorem 13) $\kappa(\mathfrak{M}), m, \llbracket\psi\rrbracket^{\mathfrak{M}} \models \varphi$ iff $\kappa(\mathfrak{M}), m, \llparenthesis\psi\rrparenthesis^X \models \varphi$ iff $m \in \llparenthesis\varphi\rrparenthesis^{\llparenthesis\psi\rrparenthesis^X}$.

Given a PASM $\mathcal{X} = (X, \{(\!|\varphi|\!)^{(\!|\psi|\!)^X} \mid \varphi, \psi \in \mathcal{PAL}\}, V)$, it suffices to show that there exists an $S5$ model $\mathfrak{M}$ such that $\kappa(\mathfrak{M}) = \mathcal{X}$. Let $\mathfrak{M} = (X, X \times X, V)$, then $\kappa(\mathfrak{M}) = (X, \{[\![\varphi]\!]^{\mathfrak{M}|\psi} \mid \varphi, \psi \in \mathcal{PAL}\}, V)$. We get $\kappa(\mathfrak{M}) = \mathcal{X}$ as $[\![\varphi]\!]^{\mathfrak{M}|\psi} = (\!|\varphi|\!)^{(\!|\psi|\!)^X}$ is already shown above. □

We immediately get soundness and completeness of the standard axiomatisation of PAL, with respect to public annuouncement subset models:

Corollary 17. *The axiomatisation* ***PAL*** *(Fig. 1) is sound and complete with respect to the class of all PASMs.*

In the next section we study axiomatisations of the full class of subset models.

5 Axiomatisations

We introduce axiomatisations for public announcement logic under subset semantics, and show that they are sound and complete with respect to all subset models. Similarly to the notations PAL_K and PAL_S, we denote by EL_K and EL_S the static epistemic logic (for the language $\mathcal{EL}$) interpreted in Kripke semantics and subset semantics, respectively.

5.1 Axiomatisation of $\mathcal{EL}$

In Section 2.1 we noted that **S5** axiomatises EL_K. In this section we show that it also axiomatises EL_S. Namely, we show that **S5** is sound and complete with respect to the class of all subset models.

Theorem 18 (Soundness of S5). ***S5*** *is sound with respect to the class of all subset models. That is, for all $\mathcal{EL}$-formula φ, $\vdash_{\mathbf{S5}} \varphi$ implies $\models \varphi$.*

Proof. $\vdash_{\mathbf{S5}} \varphi$ implies $\vdash_{\mathbf{SSL}} \varphi$, and the theorem follows from soundness of **SSL**. □

Completeness is also straightforward. Consider a subset model $(X, \mathcal{O}, V)$ with a scenario (x, O). Since there is no update operator in the language, the set $\mathcal{O}$ of all opens is equivalent to the singleton set $\{O\}$ for no other opens are accessible. Thus the neighborhood O is simply an equivalence relation. The pointed subset model $((X, \mathcal{O}, V), (x, O))$ can therefore be truth-preservingly translated into a pointed $S5$ model. We leave out the formal proof of the following theorem.

Theorem 19 (Completeness of S5). *The axiomatisation* ***S5*** *is strongly complete with respect to the class of all subset models.* □

5.2 Axiomatisation of $\mathcal{PAL}$

We introduce a new language $\mathcal{EL}^+$ for technical reasons. It adds to $\mathcal{EL}$ the clause $\mathsf{pre}(\varphi)$ explicitly, i.e., it has the following grammar rule:

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K\varphi \mid \mathsf{pre}(\varphi).$$

Satisfaction is defined just as that for $\mathcal{EL}$ and $\mathcal{PAL}$ (in subset semantics; Section 3), except that the pre-operator is now primitive. Clearly, $\mathcal{EL}^+$ is as expressive as $\mathcal{PAL}$ (see the reduction principles in Theorem 11).

The axiomatisation $\mathbf{EL}^+$ of $\mathcal{EL}^+$ (Fig. 3) is obtained by adding to **S5** the axioms $\mathrm{T}_{\mathsf{pre}}$, 4_{pre}, Int1, Int2, KP and Cl.

(PC)	Instances of all tautologies	(K)	$K(\varphi \to \psi) \to K\varphi \to K\psi$
(T)	$K\varphi \to \varphi$	(5)	$\neg K\varphi \to K\neg K\varphi$
($\mathrm{T}_{\mathsf{pre}}$)	$\mathsf{pre}(\varphi) \to \varphi$	(4_{pre})	$\mathsf{pre}(\varphi) \to \mathsf{pre}(\mathsf{pre}(\varphi))$
(Int1)	$\mathsf{pre}(\varphi) \to K(\varphi \to \mathsf{pre}(\varphi))$	(Int2)	$\neg(\varphi \to \mathsf{pre}(\varphi)) \to K\neg\mathsf{pre}(\varphi)$
(KP)	$K\varphi \to \mathsf{pre}(\varphi)$	(Cl)	$(\varphi \leftrightarrow \psi) \to (\mathsf{pre}(\varphi) \leftrightarrow \mathsf{pre}(\psi))$
(MP)	$\vdash \varphi \;\&\; \vdash \varphi \to \psi \Rightarrow \vdash \psi$	(N)	$\vdash \varphi \Rightarrow \vdash K\varphi$

Fig. 3. $\mathbf{EL}^+$. Some axioms are redundant. E.g., T can be derived from KP and $\mathrm{T}_{\mathsf{pre}}$.

Theorem 20 (Soundness of $\mathbf{EL}^+$). *$\mathbf{EL}^+$ is sound with respect to the class of all subset models. That is, for any $\mathcal{EL}^+$-formula φ, $\vdash_{\mathbf{EL}^+} \varphi$ implies $\models \varphi$.*

Proof. For any axiom of $\mathcal{EL}^+$, if it is an $\mathcal{EL}$-formula, then we can see that it is also an axiom of **S5**. Therefore, its validity follows from the soundness of **S5**. The validity of all the extra axioms are shown in Proposition 7. □

For completeness of $\mathbf{EL}^+$, given a consistent set Φ of $\mathcal{EL}^+$-formulae, it suffices to find a subset model for it. For **S5** the canonical model method can be used, but this does not work for $\mathbf{EL}^+$ because the pre-operator has impact on the open sets in a subset model. Therefore, we use a more flexible model construction method. Instead of building a canonical model which uses the set of all maximal consistent sets of formulae (MCSs) as it domain, we rather pick up the MCSs that we need, and build a model stepwise. This method is derived from the *step-by-step method* (see, e.g., [21, Chapter 4]), although we construct a model "row by row" rather than a countable series of finite approximations of a desired model. Using this method, we get the following:

Theorem 21 (Completeness of $\mathbf{EL}^+$). *The axiomatisation $\mathbf{EL}^+$ is strongly complete with respect to the class of all subset models.*

We now move on to $\mathcal{PAL}$. The axiomatisation **PAL** is given in Fig. 4. It contains all axioms and rules of $\mathbf{EL}^+$, together with the reduction principles introduced in Theorem 11 as axioms. A subtlety is that we need to make sure that the reduction axioms are not circular. This is shown by the following.

Definition 22 (Complexity of $\mathcal{PAL}$-formulae). *The complexity $c : \mathcal{PAL} \to \mathbb{N}$ is defined as follows:*

(PC)	Instances of all tautologies	(K)	$K(\varphi \to \psi) \to K\varphi \to K\psi$
(T)	$K\varphi \to \varphi$	(5)	$\neg K\varphi \to K\neg K\varphi$
($\mathrm{T_{pre}}$)	$\mathsf{pre}(\varphi) \to \varphi$	(4_{pre})	$\mathsf{pre}(\varphi) \to \mathsf{pre}(\mathsf{pre}(\varphi))$
(Int1)	$(\mathsf{pre}(\varphi) \to K(\varphi \to \mathsf{pre}(\varphi))$	(Int2)	$\neg(\varphi \to \mathsf{pre}(\varphi)) \to K\neg\mathsf{pre}(\varphi)$
(Cl)	$(\varphi \leftrightarrow \psi) \to (\mathsf{pre}(\varphi) \leftrightarrow \mathsf{pre}(\psi))$	(KP)	$K\varphi \to \mathsf{pre}(\varphi)$
(MP)	$\vdash \varphi \;\&\; \vdash \varphi \to \psi \Rightarrow \vdash \psi$	(N)	$\vdash \varphi \Rightarrow \vdash K\varphi$
($[]p$)	$[\varphi]p \leftrightarrow (\mathsf{pre}(\varphi) \to p)$	($[]\neg$)	$[\varphi]\neg\psi \leftrightarrow (\mathsf{pre}(\varphi) \to \neg[\varphi]\psi)$
($[]\wedge$)	$[\varphi](\psi \wedge \chi) \leftrightarrow ([\varphi]\psi \wedge [\varphi]\chi)$	($[]K$)	$[\varphi]K\psi \leftrightarrow (\mathsf{pre}(\varphi) \to K[\varphi]\psi)$
($[][]$)	$[\varphi][\psi]\chi \leftrightarrow [\mathsf{pre}(\varphi) \wedge [\varphi]\mathsf{pre}(\psi)]\chi$		

Fig. 4. Axiomatisation **PAL**, where any formula of the form $\mathsf{pre}(\varphi)$ is a shorthand for $\neg[\varphi]\bot$

$$\begin{array}{llll} c(\bot) & = 0 & c(\varphi \wedge \psi) & = 1 + \max(c(\varphi), c(\psi)) \\ c(p) & = 1 & c(K\varphi) & = 1 + c(\varphi) \\ c(\neg\varphi) & = 1 + c(\varphi) & c([\varphi]\psi) & = (4 + c(\varphi)) \cdot c(\psi). \end{array}$$

Proposition 23. *i) $c(\varphi) > c(\psi)$ if ψ is a subformula of a $\mathcal{PAL}$-formula φ; and ii) for all the five reduction axioms of the form $\alpha \leftrightarrow \beta$, $c(\alpha) > c(\beta)$.* ☐

Now, by Theorem 11 and the soundness of $\mathbf{EL}^+$, we easily get soundness of **PAL**. Completeness of **PAL** is also easy: from the completeness of $\mathbf{EL}^+$, any SSL validity is an $\mathbf{EL}^+$-theorem, and thus also a **PAL**-theorem (of course, in terms of the language $\mathcal{PAL}$). We state these results as follows.

Theorem 24 (Soundness and completeness). *PAL is sound and strongly complete with respect to the class of all subset models.* ☐

6 Discussion

In this paper we defined a natural interpretation of the language of public announcement logic in subset models. The resulting logic is strictly weaker than PAL. We studied the expressivity of some variants of the language, and proved completeness with respect to the complete model class. On a suitably restricted model class it coincides with PAL, giving an alternative semantics for this logic.

As mentioned in the introduction, there is existing work [8–10] which is seemingly close to the work presented in this paper, in that public announcement operators are interpreted in subset space structures, but this closeness is only superfiscial. In particular, the subset space *plays no role* in the interpretation of the public announcement operators in [8–10]; it is only used to interpret the effort modality, while the public announcement operators are interpreted by updates on the current epistemic range. If the language used in these papers is restricted to the PAL language, as in the current paper, the subset space plays no role at all. The goal of the current paper is, on the other hand, exactly to give an account of public announcements in terms of subset spaces.

In this paper we considered only the single-agent variant of PAL. This is both for simplicity of presentation, and because although there have been several proposals for multi-agent extensions of subset space logic [9, 22–24] none of them seem adequate, having problems with the semantics of nested formulae [9, 24] or not being extensions of standard multi-agent epistemic logic with a knowledge operator for each agent [22, 23]. However, we believe that the results of this paper can be relatively easily extended to a suitably defined multi-agent version of subset space logic. The classical subset space logic is known to be decidable [14], or more precisely, PSPACE-complete [10]. We are interested in a complexity result for $\mathcal{PAL}$ (in subset semantics). Also of interest for future work is extensions with arbitrary refinement operators and the relationship to arbitrary public announcement logic [15] and group announcement logic [16], as well as action model logic [17].

Acknowledgment. We gratefully thank the four ICLA reviewers for extremely helpful comments.

References

1. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning About Knowledge. The MIT Press, Cambridge (1995)
2. Meyer, J.J.C., van der Hoek, W.: Epistemic Logic for AI and Computer Science. Cambridge University Press, Cambridge (1995)
3. van Ditmarsch, H., van der Hoek, W., Kooi, B.: Dynamic Epistemic Logic. Springer (2007)
4. Plaza, J.A.: Logics of public communications. In: Emrich, M.L., Pfeifer, M.S., Hadzikadic, M., Ras, Z.W. (eds.) Proc. of ISMIS, pp. 201–216 (1989)
5. Moss, L.S., Parikh, R.: Topological reasoning and the logic of knowledge. In: Moses, Y. (ed.) Proc. of TARK, pp. 95–105 (1992)
6. McKinsey, J.C.C.: A solution of the decision problem for the lewis systems s2 and s4, with an application to topology. Journal of Symbolic Logic 6(4), 117–134 (1941)
7. McKinsey, J.C.C., Tarski, A.: The algebra of topology. Ann. Math. 45(1), 141–191 (1944)
8. Başkent, C.: Public announcement logic in geometric frameworks. Fundamenta Informaticae 114, 1–17 (2012)
9. Başkent, C.: Topics in subset space logic. Master's thesis, ILLC, UvA (2007)
10. Balbiani, P., van Ditmarsch, H., Kudinov, A.: Subset Space Logic with Arbitrary Announcements. In: Lodaya, K. (ed.) ICLA 2013. LNCS, vol. 7750, Springer, Heidelberg (2013)
11. Kooi, B., van Benthem, J.: Reduction axioms for epistemic actions. In: Schmidt, R., Pratt-Hartmann, I., Reynolds, M., Wansing, H. (eds.) Proc. of AiML 2004, pp. 197–211 (2004)
12. Kooi, B.: Expressivity and completeness for public update logics via reduction axioms. Journal of Applied Non-Classical Logics 17(2), 231–253 (2007)
13. Parikh, R., Moss, L.S., Steinsvold, C.: Topology and epistemic logic. In: Aiello, M., Pratt-Hartmann, I.E., van Benthem, J.F. (eds.) Handbook of Spatial Logics, pp. 299–341 (2007)
14. Dabrowski, A., Moss, L.S., Parikh, R.: Topological reasoning and the logic of knowledge. Annals of Pure and Applied Logic 78(1-3), 73–110 (1996)
15. Balbiani, P., Baltag, A., van Ditmarsch, H., Herzig, A., Hoshi, T., de Lima, T.: 'knowable' as 'known after an announcement'. Review of Symbolic Logic 1(3), 305–334 (2008)
16. Ågotnes, T., Balbiani, P., van Ditmarsch, H., Seban, P.: Group announcement logic. Journal of Applied Logic (2009)
17. Baltag, A., Moss, L.S.: Logics for epistemic programs. Synthese 139, 165–224 (2004)
18. van Benthem, J., Gerbrandy, J., Pacuit, E.: Merging frameworks for interaction: Del and etl. In: Proc. of TARK 2007, pp. 72–81 (2007)

19. van Benthem, J., Gerbrandy, J., Hoshi, T., Pacuit, E.: Merging frameworks for interaction. Journal of Philosophical Logic 38(5), 491–526 (2009)
20. Hoshi, T.: Merging DEL and ETL. JOLLI 19(4), 413–430 (2010)
21. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge University Press (2001)
22. Heinemann, B.: Topology and Knowledge of Multiple Agents. In: Geffner, H., Prada, R., Machado Alexandre, I., David, N. (eds.) IBERAMIA 2008. LNCS (LNAI), vol. 5290, pp. 1–10. Springer, Heidelberg (2008)
23. Heinemann, B.: Logics for multi-subset spaces. JANCL 20(3), 219–240 (2010)
24. Wen, X., Liu, H., Huang, F.: An Alternative Logic for Knowability. In: van Ditmarsch, H., Lang, J., Ju, S. (eds.) LORI 2011. LNCS, vol. 6953, pp. 342–355. Springer, Heidelberg (2011)

Author Index