ROBERT GOLDBLATT

Parallel Action: Concurrent Dynamic Logic with Independent Modalities

Abstract Regular dynamic logic is extended by the program construct $\alpha \cap \beta$, meaning "α and β executed in parallel". In a semantics due to Peleg, each command α is interpreted as a set of pairs (s,T), with T being the set of states "reachable" from s by a single execution of α, possibly involving several processes acting in parallel. The modalities $<\alpha>$ and $[\alpha]$ are given the interpretations

$<\alpha>A$ is true at s iff there exists T with $sR_\alpha T$ and A true throughout T,

and

$[\alpha]A$ is true at s iff for all T, if $sR_\alpha T$ then A is true throughout T,

which make $<\alpha>$ and $[\alpha]$ no longer interdefinable via negation, as they are in the regular case.

We prove that the logic defined by this modelling is finitely axiomatisable and has the finite model property, hence is decidable. This requires the development a new theory of canonical models and filtrations for "reachability" relations.

Introduction

The system of *concurrent* dynamic logic due to Peleg [3] extends regular dynamic logic by introducing the *combination* $\alpha \cap \beta$ of commands α and β, interpreted as "α and β executed in parallel". We envisage α and β as representing computing processes acting independently *at the same time.* For example, we might contemplate a command of the form *go to l and m*, which causes a program to execute the commands labelled by l and m simultaneously and in parallel. We might also imagine α and β as representing parallel actions by agents other than computers.

Now in regular dynamic logic, a program α is interpreted as a relation R_α on a state–set S, with the presence of the pair (s,t) in R_α signifying that there is an execution of the program that starts in state s and terminates in state t. Associated with α are modalities $[\alpha]$ and $<\alpha>$. The formula $[\alpha]A$ means "after α, A", i.e. "after every terminating execution of α, A is true" (allowing that a non–deterministic α may be executed in more than one way). $<\alpha>A$ means "α enables A", i.e. "there is an execution of α that

Studia Logica **51**: 551–578, 1992.

terminates with A true". These meanings are formalised in the satisfaction relation for a model $\mathcal{M}$ on S by requiring that

$$\mathcal{M} \models_s <\alpha>A \quad \text{iff} \quad \text{there exists } t \in S \text{ with } sR_\alpha t \text{ and } \mathcal{M} \models_t A,$$

and

$$\mathcal{M} \models_s [\alpha]A \quad \text{iff} \quad \text{for all } t \in S,\ sR_\alpha t \quad \text{implies} \quad \mathcal{M} \models_t A.$$

Then $[\alpha]A$ is equivalent to $\neg<\alpha>\neg A$, and $<\alpha>A$ to $\neg[\alpha]\neg A$.

Now in the context of concurrency, the result of an execution started in state s will not be be a single terminal state t, but rather a set T of states representing the terminal situations of all the parallel processes involved. Thus the relation R_α is no longer a set of pairs (s,t), but rather a set of pairs (s,T), with $s \in S$ and $T \subseteq S$. So instead of $R_\alpha \subseteq S \times S$, we have $R_\alpha \subseteq S \times 2^S$.

To keep the two types of relation distinct, we will refer to a subset of $S \times S$ simply as a *binary relation* on S, and a subset of $S \times 2^S$ as a *reachability relation* on S. When $sR_\alpha T$, this signifies that T is "reachable" from s by an execution of α. There may be many ways of executing α, and hence many different state–sets T reachable from s by doing α.

To retain the meaning of $<\alpha>A$ as "there is an execution of α that terminates with A true", we specify

$$\mathcal{M} \models_s <\alpha>A \quad \text{iff} \quad \text{there exists } T \subseteq S \text{ with } sR_\alpha T \text{ and } T \subseteq \mathcal{M}(A), \quad \text{(i)}$$

where

$$\mathcal{M}(A) = \{t \in S : \mathcal{M} \models_t A\}.$$

If $[\alpha]$ continues to be identified with $\neg<\alpha>\neg$, as in Peleg [3], the condition for truth of $[\alpha]A$ at s becomes

$$sR_\alpha T \quad \text{implies} \quad T \cap \mathcal{M}(A) \neq \emptyset.$$

Nerode and Wijesekera [2] suggest that in this context a more appropriate modelling of "after every terminating execution of α, A is true", would be

$$\mathcal{M} \models_s [\alpha]A \quad \text{iff} \quad sR_\alpha T \quad \text{implies} \quad T \subseteq \mathcal{M}(A), \quad \text{(ii)}$$

making $[\alpha]$ and $<\alpha>$ no longer interdefinable via $\neg$.

The extension of the system PDL of regular propositional dynamic logic having $[\alpha]$ and $<\alpha>$ interpreted according to (i) and (ii) has not been investigated in the literature to date. Here we will demonstrate finite axiomatisability and decidability for this extension, by developing the theory of canonical models and filtrations for reachability relations.

Notice that if a binary relation $\overline{R_\alpha}$ is defined by

$$s\overline{R_\alpha}t \quad \text{iff} \quad t \in \bigcup\{T : sR_\alpha T\},$$

then (ii) becomes

$$\mathcal{M} \models_s [\alpha]A \quad \text{iff} \quad s\overline{R_\alpha}t \quad \text{implies} \quad \mathcal{M} \models_t A.$$

This observation will allow us to relate much of the new theory of $[\alpha]$ given by (ii) to our known analysis of the binary relation semantics for PDL, as presented for example in [1]. At the same time, a whole new analysis is needed for $<\alpha>$.

This paper is written in the general notation and framework of [1], to which it may be an advantage if the reader had access.

Syntax and Semantics

The formal language of *Concurrent Propositional Dynamic Logic* ($CPDL$) is as for PDL, with the addition of $\cap$ and the independent treatment of $[\alpha]$ and $<\alpha>$. Given a countable set Φ of atomic formulae and a countable set Π of atomic programs, the syntax of $CPDL$ is generated in Backus–Naur form as follows.

Atomic formulae:	$p \in \Phi$
Atomic programs:	$\pi \in \Pi$
Formulae:	$A \in Fma(\Phi, \Pi)$
Programs:	$\alpha \in Prog(\Phi, \Pi)$

$$A ::= p \mid \bot \mid A_1 \to A_2 \mid <\alpha>A \mid [\alpha]A$$

$$\alpha ::= \pi \mid \alpha_1; \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha_1 \cap \alpha_2 \mid \alpha^* \mid A?$$

Intended meanings of commands are:

$\alpha_1; \alpha_2$	do α_1 and then α_2 (*composition*),
$\alpha_1 \cup \alpha_2$	do either α_1 or α_2 non–deterministically (*alternation*),
$\alpha_1 \cap \alpha_2$	do α_1 and α_2 concurrently (*combination*),
α^*	repeat α some finite number (≥ 0) of times (*iteration*),
$A?$	*test* A: continue if A is true, otherwise "fail".

The truth–functional connectives $\neg$, $\wedge$, $\vee$, and $\leftrightarrow$ are defined in the standard way. We write $\top$ for $\neg\bot$, and **skip** for $\top?$.

A $CPDL$–model is a structure

$$\mathcal{M} = (S, \{R_\alpha : \alpha \in Prog(\Phi, \Pi)\}, V),$$

with R_α a reachability relation on S for each program α, i.e. $R_\alpha \subseteq S \times 2^S$, and V a function from Φ to 2^S. The satisfaction relation *"A is true (holds) at point s in model $\mathcal{M}$"*, denoted $\mathcal{M} \models_s A$, is defined inductively on the formation of A as follows.

$\mathcal{M} \models_s p$	iff	$s \in V(p)$
$\mathcal{M} \not\models_s \bot$		(i.e. not $\mathcal{M} \models_s \bot$)
$\mathcal{M} \models_s (A_1 \to A_2)$	iff	$\mathcal{M} \models_s A_1$ implies $\mathcal{M} \models_s A_2$
$\mathcal{M} \models_s <\alpha>A$	iff	there exists $T \subseteq S$ with $sR_\alpha T$ and $T \subseteq \mathcal{M}(A)$
$\mathcal{M} \models_s [\alpha]A$	iff	for all $T \subseteq S$, $sR_\alpha T$ implies $\mathcal{M} \models_t A$.

A is *true in model* $\mathcal{M}$, denoted $\mathcal{M} \models A$, if it is true at all points in $\mathcal{M}$, i.e. if

$$\mathcal{M} \models_s A \text{ for all } s \in S.$$

Operations on Reachability Relations

Let R and Q be reachability relations on a set S.

Composition. The relation $R \cdot Q \subseteq S \times 2^S$ is defined by

$s(R \cdot Q)T$ iff there exist $U \subseteq S$ with sRU, and a collection $\{T_u : u \in U\}$ of subsets of T with uQT_u for all $u \in U$, such that $T = \bigcup\{T_u : u \in U\}$.

Combination.

$$R \otimes Q = \{(s, T \cup W) : sRT \text{ and } sQW\}.$$

Iteration. Let

$$Id = \{(s, \{s\}) : s \in S\},$$

and define a sequence of reachability relations $R^{(n)}$ inductively by

$$\begin{aligned} R^{(0)} &= Id \\ R^{(n+1)} &= Id \cup R \cdot R^{(n)}. \end{aligned}$$

Then put

$$R^{(*)} = \bigcup\{R^{(n)} : n \in \omega\}.$$

LEMMA 1.
(1) *$Q \subseteq Q'$ implies $R \cdot Q \subseteq R \cdot Q'$.*
(2) *$(R \cup R') \cdot Q = R \cdot Q \cup R' \cdot Q$.*
(3) *$R^{(n)} \subseteq R^{(n+1)}$. Hence the operation $R^{(n)}$ is monotonic in n: $n \leq m$ implies $R^{(n)} \subseteq R^{(m)}$.*

Standard Models

A $CPDL$–model is *standard* if it satisfies

$$\begin{aligned} R_{\alpha;\beta} &= R_\alpha \cdot R_\beta; \\ R_{\alpha\cup\beta} &= R_\alpha \cup R_\beta; \\ R_{\alpha\cap\beta} &= R_\alpha \otimes R_\beta; \\ R_{\alpha^*} &= R_\alpha^{(*)}; \\ R_{A?} &= \{(s,\{s\}) : \mathcal{M} \models_s A\}. \end{aligned}$$

Thus in a standard model, $R_{\mathbf{skip}} = Id$. The standard–model condition on $\cap$ ensures that $<\alpha \cap \beta>A$ gets the meaning "α and β can be executed in parallel so that on termination (in both computations) A is true".

To understand the meaning of the new iteration operation $R_\alpha^{(*)}$ that interprets α^*, consider the schema

$$<\alpha^*>A \leftrightarrow A \vee <\alpha><\alpha^*>A, \tag{iii}$$

which intuitively is true under the intended meaning of α^* as "repeat α some finite number (≥ 0) of times". In the binary relation semantics for PDL, where R_{α^*} is the ancestral (reflexive transitive closure) R_α^* [1, §10], truth of this schema in standard models is a consequence of the fact that

$$R_\alpha^* = id \cup R_\alpha \circ R_\alpha^*,$$

where

$$id = \{(s,s) : s \in S\}.$$

(Note also that in such standard models, $id = R_{\mathbf{skip}}$, and $A \leftrightarrow <\mathbf{skip}>A$ is true.)

Now in fact to have (iii) come out true in a PDL–model, it would suffice to interpret α^* by any binary relation Q satisfying

$$Q = id \cup R_\alpha \circ Q. \tag{iv}$$

The characteristic property of the ancestral R_α^* is that it is the *least* solution of equation (iv), i.e. if (i) holds then $R_\alpha^* \subseteq Q$. Thus in a PDL–model in which (iii) is true, we must have $R_\alpha^* \subseteq R_{\alpha^*}$. But then by requiring R_{α^*} itself to be the least solution of (iv) we add the converse inclusion $R_{\alpha^*} \subseteq R_\alpha^*$, which is just what is necessary to verify the PDL–axiom

$$Ind: \quad [\alpha^*](A \rightarrow [\alpha]A) \rightarrow (A \rightarrow [\alpha^*]A).$$

Now if we put

$$F(Q) = id \cup R_\alpha \circ Q$$

for an arbitrary binary relation Q, then (iv) asserts that Q is a *fixed point* of the operator F, i.e. $F(Q) = Q$. There is a general theory about fixed points of operators like F that is fundamental to the study of recursive definitions: putting $F^{(0)} = F(\emptyset)$, and $F^{(n+1)} = F(F^{(n)})$, then knowing only that F is *monotonic*, i.e. that

$$Q \subseteq Q' \quad \text{implies} \quad F(Q) \subseteq F(Q'),$$

it can be shown that F must have a least fixed point, namely the relation

$$\bigcup\{F^{(n)} : n \in \omega\}.$$

We applied this theory above in defining $R^{(*)}$, using the monotonic operator

$$F(Q) = Id \cup R \cdot Q$$

on *reachability* relations Q (cf. Lemma 1(1)). Thus $R^{(*)}$ is defined as the least solution of the equation

$$Q = Id \cup R \cdot Q,$$

and so $R_\alpha^{(*)}$ in turn is the least reachability relation that interprets α^* to make schema (iii) come out true.

Further insight into the nature of the relation $R^{(*)}$ is given in Theorem 4(7) below.

LEMMA 2. *If programs $\alpha^{(n)}$ are defined inductively by*

$$\begin{aligned} \alpha^{(0)} &= \mathbf{skip} \\ \alpha^{(n+1)} &= \mathbf{skip} \cup (\alpha; \alpha^{(n)}), \end{aligned}$$

then the following hold in any standard *model.*

(1) $R_{\alpha^{(n)}} = R_\alpha^{(n)}$.

(2) $\mathcal{M} \models_s [\alpha^{(n)}]A$ *iff* $sR_\alpha^{(n)}T$ *implies* $T \subseteq \mathcal{M}(A)$

iff $s\overline{R_\alpha^{(n)}}t$ *implies* $\mathcal{M} \models_t A$.

(3) $\mathcal{M} \models_s <\alpha^{(n)}>A$ *iff there exists* T *with* $sR_\alpha^{(n)}T$ *and* $T \subseteq \mathcal{M}(A)$.

(4) $\mathcal{M} \models_s [\alpha^*]A$ *iff for all* $n \geq 0$, $\mathcal{M} \models_s [\alpha^{(n)}]A$.

(5) $\mathcal{M} \models_s <\alpha^*>A$ *iff for some* $n \geq 0$, $\mathcal{M} \models_s <\alpha^{(n)}>A$.

Reduction to Binary Relations

For an arbitrary reachability relation R, define the binary relation $\overline{R}$ by

$$\begin{array}{ll} s\overline{R}t & \text{iff } t \in \bigcup\{T : sRT\} \\ & \text{iff for some } T \subseteq S,\ sRT \text{ and } t \in T. \end{array}$$

LEMMA 3. *For any CPDL-model $\mathcal{M}$, standard or not,*

$$\mathcal{M} \models_s [\alpha]A \quad \textit{iff} \quad s\overline{R_\alpha}t \quad \textit{implies} \quad \mathcal{M} \models_t A.$$

We now investigate the properties of the relation $\overline{R}$, and for this we need the binary relations $\overline{R}^n$ and the ancestral $\overline{R}^*$, which can be specified using the binary relation composition $\circ$, where

$$R_1 \circ R_2 = \{(s,t) : \exists u(sR_1u \ \&\ uR_2t)\}.$$

We have

$$\begin{array}{rcl} \overline{R}^0 & = & id \\ \overline{R}^{n+1} & = & \overline{R} \circ \overline{R}^n = \overline{R}^n \circ \overline{R} \\ \overline{R}^* & = & \bigcup\{\overline{R}^n : n \in \omega\}. \end{array}$$

THEOREM 4. *For any reachability relations R_i, R, Q:*

(1) $\overline{\bigcup_{i\in I} R_i} = \bigcup_{i\in I} \overline{R_i}$.
(2) $R \subseteq Q$ *implies* $\overline{R} \subseteq \overline{Q}$.
(3) $\overline{R \cdot Q} \subseteq \overline{R} \circ \overline{Q}$.
(4) *If* $Id \subseteq Q$, *then* $\overline{R \cdot Q} = \overline{R} \circ \overline{Q}$.
(5) $\overline{R^{(n+1)}} = id \cup \overline{R} \circ \overline{R^{(n)}}$.
(6) $\overline{R^{(n)}} = \overline{R}^0 \cup \cdots \cup \overline{R}^n$.
(7) $\overline{R^{(*)}} = \overline{R}^*$.

PROOF. (1) and (2) are straightforward, and left as exercises.

(3) Suppose that $s\overline{R \cdot Q}t$. Then $s(R \cdot Q)T$ for some T with $t \in T$. From the definition of $R \cdot Q$, it follows that there exists U with sRU, and some $u \in U$ for which there is a $T_u \subseteq T$ with uQT_u and $t \in T_u$. But then $s\overline{R}u$ and $u\overline{Q}t$, showing that $s\overline{R} \circ \overline{Q}t$.

(4) If $Id \subseteq Q$, we want the converse of (3). Suppose then that $s\overline{R} \circ \overline{Q}t$, so that $s\overline{R}u$ and $u\overline{Q}t$ for some u. Then sRU for some U with $u \in U$, and uQT_u for some T_u with $t \in T_u$. Let

$$T = \bigcup\{\{v\} : u \neq v \in U\} \cup T_u.$$

Since $Id \subseteq Q$, we have $vQ\{v\}$ in general, so it follows (with $T_v = \{v\}$ for $v \neq u$) that $s(R \cdot Q)T$, and hence as $t \in T$ that $s\overline{R \cdot Q}t$.

(5) Since $Id \subseteq R^{(n)}$, $\overline{R \cdot R^{(n)}} = \overline{R} \circ \overline{R^{(n)}}$ by (4). But as $\overline{Id} = id$, (5) then follows from the definition of $R^{(n+1)}$ and (1).

(6) By induction on n. The case $n = 0$ asserts that $\overline{R^{(0)}} = \overline{R}^0$, which is just the true statement that $\overline{Id} = id$.

Assuming the result for n, then from (5) and this induction hypothesis we get

$$\begin{aligned}\overline{R^{(n+1)}} &= id \cup \overline{R} \circ (\overline{R}^0 \cup \cdots \cup \overline{R}^n) \\ &= \overline{R}^0 \cup (\overline{R} \circ \overline{R}^0 \cup \cdots \cup \overline{R} \circ \overline{R}^n) \\ &= \overline{R}^0 \cup \overline{R}^1 \cup \cdots \cup \overline{R}^{n+1},\end{aligned}$$

which gives the result for $n + 1$.

(7) From the definition of $\overline{R^{(*)}}$, applying (1) and then (5), we calculate

$$\begin{aligned}\overline{R^{(*)}} &= \overline{\bigcup_{n\in\omega} R^{(n)}} \\ &= \bigcup_{n\in\omega} \overline{R^{(n)}} \\ &= \bigcup_{n\in\omega} (\overline{R}^0 \cup \cdots \cup \overline{R}^n) \\ &= \bigcup_{n\in\omega} \overline{R}^n \\ &= \overline{R}^* \qquad \blacksquare\end{aligned}$$

COROLLARY 5. *In a standard model $\mathcal{M}$,*

$$\mathcal{M} \models_s [\alpha^*]A \quad \textit{iff} \quad s\overline{R_\alpha}^* t \quad \textit{implies} \quad \mathcal{M} \models_t A.$$

PROOF. In a standard model, Theorem 4(7) implies $\overline{R_{\alpha^*}} = \overline{R_\alpha}^*$, so the result follows from Lemma 3. $\blacksquare$

This Corollary simplifies the determination of truth–values of formulae containing $[\alpha^*]$. For instance, it makes it easy to show that the PDL–axiom *Ind* is true in standard $CPLD$–models.

LEMMA 6. *If $\mathcal{M}$ is standard, then*

$$\mathcal{M} \models [\alpha^*](<\alpha>A \to A) \to [\alpha^*](<\alpha^{(n)}>A \to A),$$

and

$$\mathcal{M} \models [\alpha^*](<\alpha>A \to A) \to (<\alpha^*>A \to A).$$

PROOF. The first result is shown by induction on n. The second then follows by from the first and Lemma 2(5). The details are left to the reader. $\blacksquare$

Normal Logics

A *logic* is defined to be any set $\Lambda \subseteq Fma(\Phi, \Pi)$ such that

- Λ includes all tautologies, and
- Λ is closed under the rule of *Detachment*, i.e., if A, $A \to B \in \Lambda$ then $B \in \Lambda$.

The members of Λ are referred to as *theorems*, and we usually write $\vdash_\Lambda A$ to mean that A is a Λ–theorem (i.e. $A \in \Lambda$), and $\nvdash_\Lambda A$ when $A \notin \Lambda$.

A logic is *normal* if it contains all instances of the schema

$$\text{B-}K: \quad [\alpha](A \to B) \to ([\alpha]A \to [\alpha]B),$$

and is closed under the rule of *Necessitation*, i.e.,

$$\text{if } \vdash_\Lambda A, \text{ then } \vdash_\Lambda [\alpha]A.$$

AXIOMS FOR $CPDL$

Let $CPDL$ be the smallest normal logic in $Fma(\Phi, \Pi)$ that contains the schemata

B-*Comp*:	$[\alpha;\beta]A \leftrightarrow [\alpha][\beta]A,$
B-*Alt*:	$[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A,$
B-*Comb*:	$[\alpha \cap \beta]A \leftrightarrow (<\alpha>\top \to [\beta]A) \wedge (<\beta>\top \to [\alpha]A),$
B-*Mix*:	$[\alpha^*]A \to A \wedge [\alpha][\alpha^*]A,$
B-*Ind*:	$[\alpha^*](A \to [\alpha]A) \to (A \to [\alpha^*]A),$
B-*Test*:	$[A?]B \leftrightarrow (A \to B),$
D-*K*:	$[\alpha](A \to B) \to (<\alpha>A \to <\alpha>B),$
D-*Comp*:	$<\alpha;\beta>A \leftrightarrow <\alpha><\beta>A,$
D-*Alt*:	$<\alpha \cup \beta>A \leftrightarrow <\alpha>A \vee <\beta>A,$
D-*Comb*:	$<\alpha \cap \beta>A \leftrightarrow <\alpha>A \wedge <\beta>A,$
D-*Mix*:	$A \vee <\alpha><\alpha^*>A \to <\alpha^*>A,$
D-*Ind*:	$[\alpha^*](<\alpha>A \to A) \to (<\alpha^*>A \to A),$
D-*Test*:	$<A?>B \leftrightarrow (A \wedge B),$
B-*D*:	$[\alpha]\bot \vee <\alpha>\top,$

(The B- and D- prefixes stand for "Box" and "Diamond".) For the sake of legibility we will abbreviate $\vdash_{CPDL} A$ simply to $\vdash A$.

It will be shown that this logic has the finite model property with respect to standard $CPDL$–models, i.e. any non–theorem of $CPDL$ is falsifiable in a finite model of this type.

LEMMA 7.

(1)(Soundness) *If* $\vdash A$, *then* A *is true in all standard* $CPDL$*-models.*
(2) $\vdash A \to B$ *implies* $\vdash [\alpha]A \to [\alpha]B$.
(3) $\vdash A \to B$ *implies* $\vdash <\alpha>A \to <\alpha>B$.
(4) $\vdash [\alpha]A \vee <\alpha>\top$.
(5) $\vdash [\alpha]A \to (<\alpha>B \to <\alpha>(A \wedge B))$.

Deducibility and Consistency

If $\Gamma \cup \{A\} \subseteq Fma(\Phi, \Pi)$, then A is *deducible from* Γ, denoted $\Gamma \vdash A$, if there exist $B_0, \ldots, B_{n-1} \in \Gamma$ such that

$$\vdash B_0 \to (\cdots \to (B_{n-1} \to A) \cdots)$$

(in the case $n = 0$, this means that $\vdash A$). We write $\Gamma \nvdash A$ when A is not deducible from Γ.

Γ is *consistent* if $\Gamma \nvdash \bot$.

MAXIMAL SETS

A set $\Gamma \subseteq Fma(\Phi, \Pi)$ is *maximal* if

- Γ is consistent, and
- for any $A \in Fma(\Phi, \Pi)$, either $A \in \Gamma$ or $\neg A \in \Gamma$.

Any maximal set Γ satisfies the following properties, which will be used extensively below without reference.

- $\Gamma \vdash A$ implies $A \in \Gamma$.
- If $A \notin \Gamma$, then $\Gamma \cup \{A\}$ is not consistent. Hence if $\Gamma \subseteq \Delta$ and Δ is consistent, then $\Gamma = \Delta$ (whence the use of the adjective "maximal").
- For any formula A, *exactly one* of A and $\neg A$ belongs to Γ, i.e.,

$$\neg A \in \Gamma \quad \text{iff} \quad A \notin \Gamma.$$

- $CPDL \subseteq \Gamma$.
- $\bot \notin \Gamma$.
- $(A \to B) \in \Gamma$ iff $(A \in \Gamma$ implies $B \in \Gamma)$.
- $A \wedge B \in \Gamma$ iff $A, B \in \Gamma$.
- $A \vee B \in \Gamma$ iff $A \in \Gamma$ or $B \in \Gamma$.
- $(A \leftrightarrow B) \in \Gamma$ iff $(A \in \Gamma$ iff $B \in \Gamma)$.

Every consistent set can be extended to a maximal set (Lindenbaum's Lemma). From this it can be shown that for any $\Gamma \subseteq Fma(\Phi, \Pi)$,

$\Gamma \vdash A$ *iff* A *belongs to every maximal set that includes* Γ

(cf. §2 of [1] for details).

Now let S^m be the set of all maximal subsets of $Fma(\Phi, \Pi)$. For each formula A, let

$$\|A\| = \{s \in S^m : A \in s\}.$$

For each $s \in S^m$ and program α, let

$$s_\alpha = \{A : [\alpha]A \in s\}, \quad \text{and}$$
$$\|s_\alpha\| = \{t \in S^m : s_\alpha \subseteq t\}.$$

Thus $\|s_\alpha\| = \bigcap\{\|A\| : [\alpha]A \in s\}$.

THEOREM 8.

(1) $\vdash A$ *iff* $\|A\| = S^m$.
(2) $\vdash A \to B$ *iff* $\|A\| \subseteq \|B\|$.
(3) $\|A \vee B\| = \|A\| \cup \|B\|$.
(4) $\|A \wedge B\| = \|A\| \cap \|B\|$.
(5) $\|s_\alpha\| \subseteq \|A\|$ *implies* $[\alpha]A \in s$.
(6) *If* $\|s_\alpha\| \cap \|B\| \subseteq \|A\|$ *and* $<\alpha>B \in s$, *then* $<\alpha>A \in s$.
(7) *If* $s, u \in S^m$ *and* $s_\alpha \subseteq u$, *then* $\|u_\beta\| \subseteq \|s_{\alpha;\beta}\|$.
(8) $\|s_{\alpha\cup\beta}\| = \|s_\alpha\| \cup \|s_\beta\|$.
(9) *If* $<\alpha>\top, <\beta>\top \in s$, *then* $\|s_{\alpha\cap\beta}\| = \|s_\alpha\| \cup \|s_\beta\|$.

PROOF. (1)–(4) follow from properties of maximal sets, as above.

(5) If $\|s_\alpha\| \subseteq \|A\|$, then every maximal extension of s_α contains A, and so $s_\alpha \vdash A$. Hence

$$\vdash B_0 \to (\cdots \to (B_{n-1} \to A)\cdots)$$

for some n, and some formulae B_i with $[\alpha]B_i \in s$. Then using Necessitation (directly if $n = 0$) and axiom B-K,

$$\vdash [\alpha]B_0 \to (\cdots \to ([\alpha]B_{n-1} \to [\alpha]A)\cdots),$$

from which $[\alpha]A \in s$ follows because s contains all theorems and is closed under Detachment.

(6) Let $t \in S$ have $s_\alpha \subseteq t$. Then if $B \in t$, $t \in \|s_\alpha\| \cap \|B\|$, so as $\|s_\alpha\| \cap \|B\| \subseteq \|A\|$, then $A \in t$. Thus $(B \to A) \in t$. This shows that $\|s_\alpha\| \subseteq \|B \to A\|$, so

by (5), $[\alpha](B \to A) \in s$. But then by axiom D-K, $(<\alpha>B \to <\alpha>A) \in s$, giving the desired result that if $<\alpha>B \in s$ then $<\alpha>A \in s$.

(7) Let $s_\alpha \subseteq u$. Then if $t \in \|u_\beta\|$, we reason as follows. If $A \in s_{\alpha;\beta}$, then $[\alpha;\beta]A \in s$, so $[\alpha][\beta]A \in s$ by axiom B-*Comp*, whence $[\beta]A \in s_\alpha \subseteq u$, giving $A \in u_\beta \subseteq t$. This shows $s_{\alpha;\beta} \subseteq t$, i.e. $t \in \|s_{\alpha;\beta}\|$.

(8) Here we want to show that

$$s_{\alpha\cup\beta} \subseteq t \quad \text{iff} \quad s_\alpha \subseteq t \text{ or } s_\beta \subseteq t.$$

The implication from right to left is straightforward, with the aid of B-*Alt*. For the converse, suppose that $s_\alpha \not\subseteq t$ and $s_\beta \not\subseteq t$. Then there must be formulae A and B with $[\alpha]A, [\beta]B \in s$, but $A \notin t$ and $B \notin t$. Now $[\alpha]A \to [\alpha](A \vee B)$ is a theorem (cf. Lemma 7(2)), so $[\alpha](A \vee B) \in s$. Similarly, $[\beta](A \vee B) \in s$. Hence by B-*Alt*, $[\alpha \cup \beta](A \vee B) \in s$. Since $(A \vee B) \notin s$, this shows that $s_{\alpha\cup\beta} \not\subseteq t$.

(9) If $<\alpha>\top, <\beta>\top \in s$, then by axiom B-*Comb*,

$$[\alpha \cap \beta]A \in s \quad \text{iff} \quad [\alpha]A \in s \text{ and } [\beta]A \in s.$$

But this allows us to prove that

$$s_{\alpha\cap\beta} \subseteq t \quad \text{iff} \quad s_\alpha \subseteq t \text{ or } s_\beta \subseteq t,$$

in the same manner as for (8). ∎

Reachability for Maximal Sets

Let $s \in S^m$ and $T \subseteq S^m$. For each program α, put

$$sR_\alpha T \quad \text{iff} \quad \text{there exists } B \text{ with } <\alpha>B \in s \text{ and } T = \|s_\alpha\| \cap \|B\|.$$

THEOREM 9.

(1) $<\alpha>A \in s$ *iff there exists* T *with* $sR_\alpha T$ *and* $T \subseteq \|A\|$.

(2) $<\alpha>\top \in s$ *implies* $sR_\alpha\|s_\alpha\|$.

(3) $s\overline{R_\alpha}t$ *iff* $s_\alpha \subseteq t$.

(4) $[\alpha]A \in s$ *iff* $sR_\alpha T$ *implies* $T \subseteq \|A\|$.

PROOF.

(1) If $<\alpha>A \in s$, then defining $T = \|s_\alpha\| \cap \|A\|$ immediately gives $sR_\alpha T$ and $T \subseteq \|A\|$. Conversely, if $sR_\alpha T \subseteq \|A\|$, then there exists B with $<\alpha>B \in s$ and $T = \|s_\alpha\| \cap \|B\|$. But then $\|s_\alpha\| \cap \|B\| \subseteq \|A\|$, so Theorem 8(6) gives $<\alpha>A \in s$, as desired.

(2) From the definition of R_α, since $\|s_\alpha\| \cap \|\top\| = \|s_\alpha\|$.

(3) If $s\overline{R_\alpha}t$, then $t \in T$ for some T of the form $\|s_\alpha\| \cap \|B\|$. But then $t \in \|s_\alpha\|$, i.e. $s_\alpha \subseteq t$.

Conversely, if $s_\alpha \subseteq t$, then since $\bot \notin t$, we get $[\alpha]\bot \notin s$, so by axiom B-*D*, $<\alpha>\top \in s$. Hence by (2), $sR_\alpha\|s_\alpha\|$. Since $t \in \|s_\alpha\|$, this gives $s\overline{R_\alpha}t$.

(4) By Theorem 8(5) and the definition of s_α, it follows that to have $[\alpha]A \in s$ it is necessary and sufficient that

$$s_\alpha \subseteq t \quad \text{implies} \quad A \in t,$$

which is equivalent by (3) to

$$s\overline{R_\alpha}t \quad \text{implies} \quad A \in t,$$

which in turn holds if, and only if,

$$sR_\alpha T \quad \text{implies} \quad T \subseteq \|A\|. \qquad \blacksquare$$

COROLLARY 10. *If there exists some t with $s\overline{R_\alpha}t$, then $<\alpha>\top \in s$.*

PROOF. If $s\overline{R_\alpha}t$, there must be some T with $sR_\alpha T$. Since $T \subseteq \|\top\|$, 9(1) then gives $<\alpha>\top \in s$. $\blacksquare$

Canonical Model

The canonical model for $CPDL$ is the structure

$$\mathcal{M}^m = (S^m, \{R_\alpha : \alpha \in Prog(\Phi, \Pi)\}, V^m),$$

where S^m is the set of all maximal sets, R_α is as defined prior to Theorem 9, and $V^m(p) = \{s \in S^m : p \in s\}$.

TRUTH LEMMA 11. *For any $A \in Fma(\Phi, \Pi)$,*

$$\mathcal{M}^m(A) = \|A\|,$$

i.e. for all $s \in S^m$,

$$\mathcal{M}^m \models_s A \text{ iff } A \in s.$$

PROOF. By induction on the formation of A. The case $A = p \in \Phi$ holds by definition of V^m, and the truth-functional cases are taken care of by the

properties of maximal sets listed earlier. The inductive cases $A = <\alpha>B$ and $A = [\alpha]B$ follow from 9(1) and 9(4) respectively. ■

As with PDL, the canonical model $\mathcal{M}^m$ determines the logic $CPDL$, but cannot be shown to be standard (cf. [1]). Some properties that it does enjoy, and that will be used in our completeness theorem, are collected in the next result.

THEOREM 12. *The following hold in the canonical CPDL-model.*

(1) *Tests are standard, i.e.* $sR_{A?}T$ *iff* $T = \{s\}$ *and* $\mathcal{M}^m \models_s A$.

(2) *If* $sR_{\alpha;\beta}T$, *then* $s(R_\alpha \cdot R_\beta)W$ *for some* $W \subseteq T$.

(3) *If* $sR_{\alpha\cup\beta}T$, *then* $s(R_\alpha \cup R_\beta)W$ *for some* $W \subseteq T$.

(4) $R_{\alpha\cap\beta} \subseteq R_\alpha \otimes R_\beta$.

PROOF.

(1) Noting that $\mathcal{M}^m \models_s A$ iff $A \in s$, we have that if $\mathcal{M}^m \models_s A$, then $B \in s$ iff $(A \to B) \in s$ for any formula B, so by axiom B-*Test*, $[A?]B \in s$ iff $B \in s$, showing that $s_{A?} = s$. Moreover, this in turn implies that $\|s_{A?}\| = \{s\}$, since s is maximal.

Thus if $sR_{A?}T$, then $T = \|s_{A?}\| \cap \|B\|$ for some B with $<A?>B \in s$. Hence from axiom D-*Test*, $A, B \in s$, whence $\|s_{A?}\| = \{s\}$ as above, and $\{s\} \subseteq \|B\|$. Thus $T = \{s\} \cap \|B\| = \{s\}$, with $\mathcal{M}^m \models_s A$ as desired.

Conversely, if $\mathcal{M}^m \models_s A$ and $T = \{s\}$, then $\|s_{A?}\| = \{s\}$ and $T = \|s_{A?}\| \cap \|A\|$. Hence $sR_{A?}T$, since D-*Test* gives $<A?>A \in s$.

(2) Let $sR_{\alpha;\beta}T$. Then $T = \|s_{\alpha;\beta}\| \cap \|A\|$ for some A with $<\alpha;\beta>A \in s$. Then by D-*Comp*, $<\alpha><\beta>A \in s$, so $sR_\alpha U$, where $U = \|s_\alpha\| \cap \|<\beta>A\|$.

For each $u \in U$, put $T_u = \|u_\beta\| \cap \|A\|$, so that $uR_\beta T_u$, since $<\beta>A \in u$. Also, as $u \in \|s_\alpha\|$, i.e. $s_\alpha \subseteq u$, Theorem 8(7) yields $\|u_\beta\| \subseteq \|s_{\alpha;\beta}\|$, showing that $T_u \subseteq T$. Thus the desired result follows by putting $W = \bigcup\{T_u : u \in U\}$.

(3) If $sR_{\alpha\cup\beta}T$, then $T = \|s_{\alpha\cup\beta}\| \cap \|A\|$ for some A with $<\alpha \cup \beta>A \in s$. Axiom D-*Alt* then implies that one of $<\alpha>A$ and $<\beta>A$ is in s. If, say, $<\alpha>A \in s$, then $sR_\alpha W$, where $W = \|s_\alpha\| \cap \|A\|$. By Theorem 8(8), $\|s_\alpha\| \subseteq \|s_{\alpha\cup\beta}\|$, so $W \subseteq T$. Similarly, if $<\beta>A \in s$, we take $W = \|s_\beta\| \cap \|B\|$, and get $sR_\beta W \subseteq T$. In either case, $s(R_\alpha \cup R_\beta)W \subseteq T$.

(4) If $sR_{\alpha\cap\beta}T$, then $T = \|s_{\alpha\cap\beta}\| \cap \|A\|$ for some A with $<\alpha\cap\beta>A \in s$. Then by D-*Comb*, $<\alpha>A, <\beta>A \in s$, so $sR_\alpha(\|s_\alpha\| \cap \|A\|)$ and $sR_\beta(\|s_\beta\| \cap \|A\|)$. Hence $s(R_\alpha \otimes R_\beta)U$, where

$$U = (\|s_\alpha\| \cap \|A\|) \cup (s_\beta \cap \|A\|) = (\|s_\alpha\| \cup \|s_\beta\|) \cap \|A\|.$$

But since $sR_{\alpha\cap\beta}T \subseteq \|\top\|$, $<\alpha\cap\beta>\top \in s$, so by D-*Comb*, $<\alpha>\top$ and $<\beta>\top$ belong to s, whence by 8(9) $U = T$. ■

Execution Relations

If $s\widetilde{R_\alpha}t$, then intuitively there is an execution of α from s that produces a set T of terminal states including t. We may regard this execution as generating a *tree* of states, with T being the set of leaves of the tree. There will be a path through this tree from s to t, comprising a sequence of executions of atomic programs and/or tests (cf. §2.2 of Peleg [4] for an indication of how to formalise this idea).

If further $t\widetilde{R_\beta}u$, then there will be a similar computation tree containing a path from t to u as a result of executing β from t. We then have $s\widetilde{R_\alpha} \circ \widetilde{R_\beta}u$, but we cannot conclude that $s\widetilde{R_{\alpha\cdot\beta}}t$ without first showing that β–computation trees can be attached to every state in T, and not just t. Nonetheless one might suggest that u has been arrived at from s by an instance of "doing α and then β".

These observations may provide some motivation for the following technical definition of relations R^+_α whose chief purpose is to give a representation of program composition $\alpha;\beta$ by binary relation composition $\circ$, and which will be used in defining filtrations of $CPDL$–models.

Given a $CPDL$–model

$$\mathcal{M} = (S, \{R_\alpha : \alpha \in Prog(\Phi,\Pi)\}, V),$$

define a family $\{R^+_\alpha : \alpha \in Prog(\Phi,\Pi)\}$ of binary relations on S inductively by

$$\begin{aligned} R^+_\pi &= \widetilde{R_\pi}; \\ R^+_{A?} &= \widetilde{R_{A?}}; \\ R^+_{\alpha;\beta} &= R^+_\alpha \circ R^+_\beta; \\ R^+_{\alpha\cup\beta} &= R^+_\alpha \cup R^+_\beta; \\ R^+_{\alpha^*} &= (R^+_\alpha)^*; \end{aligned}$$

and

$$\begin{aligned} sR^+_{\alpha\cap\beta}t \quad \text{iff} \quad & \text{for some } T, \text{ either} \\ & (i)\ sR^+_\alpha t \text{ and } sR_\beta T, \quad \text{or} \\ & (ii) sR_\alpha T \text{ and } sR^+_\beta t. \end{aligned}$$

THEOREM 13. *In a model that is standard except possibly for tests,* $\overline{R_\alpha} \subseteq R_\alpha^+$.

PROOF. By induction on the formation of α. The cases $\alpha = \pi$ and $\alpha = A?$ are immediate by definition of R_α^+. For the inductive cases, assume the result for α and β.

Composition:

$$\begin{aligned} \overline{R_{\alpha;\beta}} &= \overline{R_\alpha \cdot R_\beta} && \text{standard condition for } \alpha;\beta \\ &\subseteq \overline{R_\alpha} \circ \overline{R_\beta} && 4(3) \\ &\subseteq R_\alpha^+ \circ R_\beta^+ && \text{hypothesis on } \alpha \text{ and } \beta \\ &= R_{\alpha;\beta}^+. \end{aligned}$$

Alternation:

$$\begin{aligned} \overline{R_{\alpha\cup\beta}} &= \overline{R_\alpha \cup R_\beta} && \text{standard condition for } \alpha \cup \beta \\ &= \overline{R_\alpha} \cup \overline{R_\beta} && 4(1) \\ &\subseteq R_\alpha^+ \cup R_\beta^+ && \text{hypothesis on } \alpha \text{ and } \beta \\ &= R_{\alpha\cup\beta}^+. \end{aligned}$$

Iteration:

$$\begin{aligned} \overline{R_{\alpha^*}} &= \overline{R_\alpha^{(*)}} && \text{standard condition for } \alpha^* \\ &= \overline{R_\alpha}^* && 4(7) \\ &\subseteq (R_\alpha^+)^* && \text{hypothesis on } \alpha \\ &= R_{\alpha^*}^+. \end{aligned}$$

Combination: If $s\overline{R_{\alpha\cap\beta}}t$, then by the standard condition there are T, W with $sR_\alpha T$, $sR_\beta W$, and $t \in T \cup W$. Now if $t \in T$, then $s\overline{R_\alpha}t$, so $sR_\alpha^+ t$ by the hypothesis on α, whence as $sR_\beta W$ we get $sR_{\alpha\cap\beta}^+ t$. On the other hand, if $t \in W$ we similarly get $sR_\beta^+ t$ and $sR_\alpha T$, leading again to the desired conclusion $sR_{\alpha\cap\beta}^+ t$. ■

THEOREM 14. *Let* $\mathcal{M}$ *be a model that is standard except possibly for tests. If* α *is any program, then for all formulae* A *we have*

$$\mathcal{M} \models_s [\alpha]A \quad \textit{iff} \quad sR_\alpha^+ t \quad \textit{implies} \quad \mathcal{M} \models_t A.$$

PROOF. Since in general

$$\mathcal{M} \models_s [\alpha]A \quad \text{iff} \quad s\overline{R_\alpha}t \quad \text{implies} \quad \mathcal{M} \models_t A$$

(Lemma 3), the fact that $\overline{R_\alpha} \subseteq R_\alpha^+$ implies directly that the statement of the Theorem holds from right to left. We prove the converse by induction on the formation of α.

The cases $\alpha = \pi$ and $\alpha = A?$ are immediate, as then $R_\alpha^+ = \overline{R_\alpha}$. For the inductive cases, assume the result for α and β.

Composition. Let $\mathcal{M} \models_s [\alpha;\beta]A$ and $sR_{\alpha;\beta}^+t$. Then there exists u with sR_α^+u and uR_β^+t. Since $\mathcal{M}$ is standard for composition, it verifies B-*Comp*, and so $\mathcal{M} \models_s [\alpha][\beta]A$. The induction hypothesis on α then gives $\mathcal{M} \models_u [\beta]A$, from which the hypothesis on β yields the desired conclusion $\mathcal{M} \models_t A$.

Alternation. If $\mathcal{M} \models_s [\alpha \cup \beta]A$ and $sR_{\alpha\cup\beta}^+t$, then either sR_α^+t or sR_β^+t, so as $\mathcal{M}$ verifies B-*Alt*, the hypothesis on α and β leads to $\mathcal{M} \models_t A$.

Iteration. Let $\mathcal{M} \models_s [\alpha^*]A$. Then we first show that for any n,

$$s(R_\alpha^+)^n t \quad \text{implies} \quad \mathcal{M} \models_t [\alpha^*]A. \tag{†}$$

The base case $n = 0$ is immediate, since then $s = t$. Assuming the result for n, suppose that $s(R_\alpha^+)^{n+1}t$. Then for some u, $s(R_\alpha^+)^n u$ and uR_α^+t. By the hypothesis on n, $\mathcal{M} \models_u [\alpha^*]A$. Hence $\mathcal{M} \models_u [\alpha][\alpha^*]A$, since $\mathcal{M}$ verifies B-*Mix*, so by the hypothesis on α, $\mathcal{M} \models_t [\alpha^*]A$. This completes the inductive proof of (†).

Now if $sR_{\alpha^*}^+t$, then $s(R_\alpha^+)^n t$ for some n, and so $\mathcal{M} \models_t [\alpha^*]A$ by (†). Again since $\mathcal{M}$ verifies B-*Mix*, this implies $\mathcal{M} \models_t A$.

Combination. Let $\mathcal{M} \models_s [\alpha \cap \beta]A$ and $sR_{\alpha\cap\beta}^+t$. Then there exists T such that either (i) sR_α^+t and $sR_\beta T$, or else (ii) $sR_\alpha T$ and sR_β^+t.

Now if (i) holds, then $sR_\beta T$ implies $\mathcal{M} \models_s <\beta>\top$, so as $\mathcal{M}$ verifies B-*Comb*, $\mathcal{M} \models_s [\alpha]A$. But then the hypothesis on α gives $\mathcal{M} \models_t A$. Similarly, if (ii) holds we are led to $\mathcal{M} \models_t A$ by the other conjunct of B-*Comb* and the hypothesis on β. ∎

Filtrations

The technique of "filtration" is designed to collapse the canonical model to a finite model while leaving invariant the truth/falsity of a prescribed formula. Here we adapt to *CPDL* the method as expounded in [1, §§4,10].

A set Γ of formulae is defined to be *closed* if the following hold:

Γ is closed under subformulae;
$[B?]D \in \Gamma$ implies $B \in \Gamma$;
$[\alpha;\beta]B \in \Gamma$ implies $[\alpha][\beta]B \in \Gamma$;
$[\alpha \cup \beta]B \in \Gamma$ implies $[\alpha]B, [\beta]B \in \Gamma$;
$[\alpha \cap \beta]B \in \Gamma$ implies $[\alpha]B, [\beta]B, <\alpha>\top, <\beta>\top \in \Gamma$;
$[\alpha^*]B \in \Gamma$ implies $[\alpha][\alpha^*]B \in \Gamma$;
$<B?>D \in \Gamma$ implies $B \in \Gamma$;
$<\alpha;\beta>B \in \Gamma$ implies $<\alpha><\beta>B \in \Gamma$;
$<\alpha \cup \beta>B \in \Gamma$ implies $<\alpha>B, <\beta>B \in \Gamma$;
$<\alpha \cap \beta>B \in \Gamma$ implies $<\alpha>B, <\beta>B \in \Gamma$;
$<\alpha^*>B \in \Gamma$ implies $<\alpha><\alpha^*>B \in \Gamma$.

By methods that are well–established (e.g. Lemma 10.5 of [1]), it can be shown that

LEMMA 15. *For any $A \in Fma(\Phi, \Pi)$ there is a finite closed set Γ with $A \in \Gamma$.*

Now let Γ be a finite closed set. Take $Prog_\Gamma$ to be the smallest set of programs that includes all atomic programs and tests occurring in members of Γ, and is closed under ;, $\cup$, $\cap$, and *. For $s, t \in S^m$, put

$$s \sim_\Gamma t \quad \text{iff} \quad s \cap \Gamma = t \cap \Gamma,$$
$$|s| = \{t \in S^m : s \sim_\Gamma t\},$$
$$S_\Gamma = \{|s| : s \in S^m\},$$

and for $T \subseteq S^m$, and $X \subseteq S_\Gamma$, put

$$|T| = \{|s| : s \in T\},$$
$$S_X = \{s \in S^m : |s| \in X\}.$$

LEMMA 16.

(1) *$T \subseteq U$ implies $|T| \subseteq |U|$.*
(2) *$X \subseteq Y$ implies $S_X \subseteq S_Y$.*
(3) *$S_X \subseteq T$ implies $X \subseteq |T|$.*
(4) *$X = |S_X|$.*
(5) *$T \subseteq S_{|T|}$.*
(6) *$|s| = S_{\{|s|\}}$.*

The finiteness of Γ ensures that S_Γ is finite. Moreover, each subset of S_Γ is *definable* by a formula which is a truth–functional combination of members

of Γ, i.e. if $X \subseteq S_\Gamma$ then there is some such formula A_X such that for all $s \in S$,

$$A_X \in s \quad \text{iff} \quad |s| \in X$$

(cf. Definability Lemmas 8.14 and 9.7 of [1] for details).

Now let

$$\mathcal{M}' = (S_\Gamma, \{\rho_\alpha : \alpha \in Prog_\Gamma\}, V_\Gamma),$$

be a $CPDL$–model based on S_Γ, with

$$V_\Gamma(p) = \begin{cases} \{|s| : s \in V^m(p)\}, & \text{if } p \in \Gamma; \\ \emptyset, & \text{otherwise.} \end{cases}$$

Then the reachability relation ρ_α on S_Γ is defined to be a Γ–*filtration* of the relation R_α from the canonical model $\mathcal{M}^m$ if, and only if, the following four conditions are satisfied.

(B1) $s\overline{R_\alpha}t$ implies $|s|\rho_\alpha^+|t|$.

(B2) $|s|\overline{\rho_\alpha}|t|$ implies $\{B : [\alpha]B \in s \cap \Gamma\} \subseteq t$.

(D1) $sR_\alpha T$ implies $|s|\rho_\alpha X$ for some $X \subseteq |T|$.

(D2) if $|s|\rho_\alpha X$ and $S_X \subseteq \|B\|$, then $<\alpha>B \in \Gamma$ implies $<\alpha>B \in s$.

ρ_α will be called *strong* if it satisfies

$$sR_\alpha T \text{ implies } |s|\rho_\alpha|T|.$$

Any strong relation ρ_α obviously satisfies (D1). But it also satisfies (B1): if $s\overline{R_\alpha}t$ then $sR_\alpha T$ for some T with $t \in T$, hence $|s|\rho_\alpha|T|$ and $|t| \in |T|$, showing $|s|\overline{\rho_\alpha}|t|$. But then $|s|\rho_\alpha^+|t|$ since in general $\overline{\rho_\alpha} \subseteq \rho_\alpha^+$ by Theorem 13.

The model $\mathcal{M}'$ will be called a Γ–*filtration* of the canonical model $\mathcal{M}^m$ if ρ_α is a Γ–filtration of R_α for all $\alpha \in Prog_\Gamma$.

FILTRATION LEMMA 17. *Let $\mathcal{M}'$ be a Γ–filtration of $\mathcal{M}^m$ that is standard except possibly for tests. Then for any $B \in \Gamma$ and $s \in S^m$,*

$$\mathcal{M}^m \models_s B \text{ iff } \mathcal{M}' \models_{|s|} B.$$

PROOF. By induction on the formation of B. The case $B = p \in \Phi$ is given by the definitions of V_Γ and $\sim_\Gamma$, the case $B = \bot$ is immediate, and the inductive case $B = (B_1 \to B_2)$ is straightforward.

For the inductive case for $[\alpha]$, assume the result for B. Then if $[\alpha]B \in \Gamma$ and $\mathcal{M}' \models_{|s|} [\alpha]B$, since $\mathcal{M}'$ is standard except possibly for tests we get that

$$|s|\rho_\alpha^+|t| \quad \text{implies} \quad \mathcal{M}' \models_{|t|} B,$$

by Theorem 14. From (B1) and the induction hypothesis on B, we then get

$$s\overline{R_\alpha}t \quad \text{implies} \quad \mathcal{M}^m \models_t B.$$

This in turn gives $\mathcal{M}^m \models_s [\alpha]B$ by Lemma 3.

Conversely, if $\mathcal{M}^m \models_s [\alpha]B$, i.e. $[\alpha]B \in s$, then from (B2) and the induction hypothesis we get that

$$|s|\overline{\rho_\alpha}|t| \quad \text{implies} \quad \mathcal{M}' \models_{|t|} B,$$

which implies $\mathcal{M}' \models_{|s|} [\alpha]B$ by Lemma 3 again.

Now for the inductive case of $<\alpha>$. First, if $<\alpha>B \in \Gamma$ and $\mathcal{M}^m \models_s <\alpha>B$, then there exists $T \subseteq S^m$ with $sR_\alpha T \subseteq \|B\|$. Thus if the Lemma holds for B, then for $t \in T$ we have $B \in t$, whence $\mathcal{M}' \models_{|t|} B$, showing that $|T| \subseteq \mathcal{M}'(B)$. But by (D1), $|s|\rho_\alpha X$ for some $X \subseteq |T|$. Then $X \subseteq \mathcal{M}'(B)$, giving $\mathcal{M}' \models_{|s|} <\alpha>B$.

Conversely, if $\mathcal{M}' \models_{|s|} <\alpha>B$, then $|s|\rho_\alpha X$ for some $X \subseteq \mathcal{M}'(B)$. The inductive hypothesis on B then yields $S_X \subseteq \|B\|$, and so (D2) gives $\mathcal{M}^m \models_s <\alpha>B$. ∎

Existence of Filtrations

For $\alpha \in Prog_\Gamma$, define

$$|s|\,\rho_\alpha^\lambda X \quad \text{iff} \quad \begin{array}{ll} \text{(i)} & |t| \in X \ \text{ implies } \ \{B : [\alpha]B \in s \cap \Gamma\} \subseteq t; \ \text{ and} \\ \text{(ii)} & S_X \subseteq \|B\| \text{ and } <\alpha>B \in \Gamma \ \text{ implies } \ <\alpha>B \in s. \end{array}$$

THEOREM 18. *ρ_α^λ is a Γ-filtration of R_α, and is in fact the largest one.*

PROOF. First we show that ρ_α^λ is strong, taking care of (B1) and (D1). So, let $sR_\alpha T$, with the objective of showing that $|s|\rho_\alpha|T|$, i.e. that (i) and (ii) above hold with $X = |T|$. We have $T = \|s_\alpha\| \cap \|C\|$, for some C with $<\alpha>C \in s$.

Now for (i), if $|t| \in |T|$, then $t \sim_\Gamma u$ for some $u \in T$, so that if $[\alpha]B \in s \cap \Gamma$ then $T \subseteq \|B\|$ as $sR_\alpha T$, hence $B \in u$, and so $B \in t$ as $B \in \Gamma$.

For (ii), suppose that $S_{|T|} \subseteq \|B\|$ and $<\alpha>B \in \Gamma$. Then as $T \subseteq S_{|T|}$, we have $sR_\alpha T \subseteq \|B\|$, and so $<\alpha>B \in s$ follows by Theorem 9(1). This completes the proof that ρ_α^λ is strong.

Next we show that (B2) holds for ρ_α^λ: if $|s|\overline{\rho_\alpha^\lambda}|t|$ then $|s|\rho_\alpha^\lambda X$ and $|t| \in X$ for some X, so that by part (i) of the definition of ρ_α^λ, $\{B : [\alpha]B \in s \cap \Gamma\} \subseteq t$.

Noting that (D2) for ρ_α^λ is immediate from (ii), we have now shown that ρ_α^λ is a filtration. The proof that it is the largest is left as an exercise. ■

The Finite Model

Given a finite closed Γ, construct a model

$$\mathcal{M}_\Gamma = (S_\Gamma, \{\rho_\alpha : \alpha \in Prog_\Gamma\}, V_\Gamma),$$

by letting ρ_π be *any* Γ–filtration of R_π,

$$\rho_{B?} = \{(|s|, \{|s|\}) : \mathcal{M}^m \models_s B\},$$

and otherwise defining ρ_α inductively by the standard–model condition on α.

THEOREM 19. *$\mathcal{M}_\Gamma$ is a Γ–filtration of the canonical CPDL–model $\mathcal{M}^m$.*

PROOF. We have to show that ρ_α is a Γ–filtration of R_α for each $\alpha \in Prog_\Gamma$.

Tests. Suppose $B? \in Prog_\Gamma$. If $sR_{B?}T$, then by 12(1), $T = \{s\}$ and $\mathcal{M}^m \models_s B$. Hence $|T| = \{|s|\}$, and so $|s|\rho_{B?}|T|$ by definition of $\rho_{B?}$. This shows that $\rho_{B?}$ is strong, and so fulfils (B1) and (D1).

For (B2), let $|s|\overline{\rho_{B?}}|t|$, so that $|s| = |t|$ and $B \in s$. Then if $[B?]D \in s \cap \Gamma$, we get $D \in s$ via B-*Test*, and so $D \in t$ as $s \sim_\Gamma t$.

For (D2), let $|s|\rho_{B?}X$ and $S_X \subseteq \|D\|$. Then $X = \{|s|\}$ and $B \in s$, so that $s \in S_X$, giving $D \in s$. Hence by D-*Test*, $<B?>D \in s$.

This completes the proof that $\rho_{B?}$ is a Γ–filtration of $R_{B?}$.

The proof of the first filtration condition (B1) in the inductive cases will use the following idea. Given $s \in S^m$, let A_s be a formula such that for all $t \in S^m$,

$$A_s \in t \quad \text{iff} \quad |s|\rho_\alpha^+|t|$$

(A_s exists by the definability of any subset of S_Γ noted earlier). Then to show that

$$s\overline{R_\alpha}t \quad \text{implies} \quad |s|\rho_\alpha^+|t|,$$

it suffices to prove that $[\alpha]A_s \in s$, for then if $s\overline{R_\alpha}t$ we get $A_s \in t$ as desired.

Composition. Suppose that $(\alpha;\beta) \in Prog_\Gamma$, and, inductively, that ρ_α and ρ_β are Γ–filtrations of R_α and R_β, respectively.

(B1): For $s \in S$, let A_s be a formula having

$$A_s \in t \quad \text{iff} \quad |s|\rho^+_{\alpha;\beta}|t|.$$

If $s\overline{R_\alpha}u\overline{R_\beta}t$, then by (B1) for α and β, $|s|\rho^+_\alpha|u|\rho^+_\beta|t|$. Hence $|s|\rho^+_\alpha \circ \rho^+_\beta|t|$, i.e. $|s|\rho^+_{\alpha;\beta}|t|$ by definition of $\rho^+_{\alpha;\beta}$, and so $A_s \in t$. This shows that $[\alpha][\beta]A_s \in s$, and hence by axiom B-*Comp*, $[\alpha;\beta]A_s \in s$ as needed to ensure that $s\overline{R_{\alpha;\beta}}t$ implies $|s|\rho^+_{\alpha;\beta}|t|$.

(B2): Let $|s|\overline{\rho_{\alpha;\beta}}|t|$, i.e. $|s|\overline{\rho_\alpha \cdot \rho_\beta}|t|$. Then $|s|\overline{\rho_\alpha} \circ \overline{\rho_\beta}|t|$ by Theorem 4(3), so for some u, $|s|\overline{\rho_\alpha}|u|$ and $|u|\overline{\rho_\beta}|t|$. Then if $[\alpha;\beta]B \in s \cap \Gamma$, $[\alpha][\beta]B \in s \cap \Gamma$ by *Comp*, so (B2) for α and β give $[\beta]B \in u$ and thence $B \in t$.

(D1): Let $sR_{\alpha;\beta}T$. Then by Theorem 12(2), there exists $U \subseteq S^m$ with $sR_\alpha U$, such that for each $u \in U$ there exists $T_u \subseteq T$ with $uR_\beta T_u$. By (D1) for α there exists $X \subseteq S_\Gamma$ with $|s|\rho_\alpha X \subseteq |U|$. Then if $x \in X$, we have $x = |u|$ for some $u \in U$, so by (D1) for β, there exists $Y_x \subseteq S_\Gamma$ with $x\rho_\beta Y_x \subseteq |T_u| \subseteq |T|$. Thus putting

$$Z = \bigcup\{Y_x : x \in X\},$$

we have $|s|(\rho_\alpha \cdot \rho_\beta)Z$, hence $|s|\rho_{\alpha;\beta}Z \subseteq |T|$.

(D2): If $|s|\rho_{\alpha;\beta}X$, i.e. $|s|(\rho_\alpha \cdot \rho_\beta)X$, then there exists $Y \subseteq S_\Gamma$ with $|s|\rho_\alpha Y$, such that $X = \bigcup\{X_y : y \in Y\}$, with $y\rho_\beta X_y$ for all $y \in Y$.

Now suppose $S_X \subseteq \|B\|$ and $<\alpha;\beta>B \in \Gamma$. We want $<\alpha;\beta>B \in s$. But if $t \in S_Y$, then $|t| \in Y$ and $S_{X_{|t|}} \subseteq S_X \subseteq \|B\|$, so as $<\beta>B \in \Gamma$ and $|t|\rho_\beta X_{|t|}$, (D2) for β gives $<\beta>B \in t$. This shows that $S_Y \subseteq \|<\beta>B\|$. Since $<\alpha><\beta>B \in \Gamma$ and $|s|\rho_\alpha Y$, (D2) for α then gives $<\alpha><\beta>B \in s$, so D-*Comp* yields $<\alpha;\beta>B \in s$ as desired.

Alternation.

(B1). Let A_s be a formula having

$$A_s \in t \quad \text{iff} \quad |s|\rho^+_{\alpha\cup\beta}|t|.$$

Using (B1) for α and β and the definition of $\rho^+_{\alpha\cup\beta}$, we get $A_s \in t$ whenever $s\overline{R_\alpha}t$ or $s\overline{R_\beta}t$. Hence $[\alpha]A_s, [\beta]A_s \in s$, so $[\alpha \cup \beta]A_s \in s$ by B-*Alt*.

(B2). If $|s|\overline{\rho_{\alpha\cup\beta}}|t|$, then either $|s|\overline{\rho_\alpha}|t|$ or else $|s|\overline{\rho_\beta}|t|$. Since B-*Alt* gives $[\alpha \cup \beta]B \in s$ only if $[\alpha]B, [\beta]B \in s$, (B2) for α and β then readily yield $\{B : [\alpha \cup \beta]B \in s \cap \Gamma\} \subseteq t$.

(D1). If $sR_{\alpha\cup\beta}T$, then by 12(3) there exists $W \subseteq T$ with $sR_\alpha W$ or $sR_\beta W$. Assuming (D1) for α and β, it follows that there is some $X \subseteq |W|$ with $|s|\rho_\alpha X$ or $|s|\rho_\beta X$. Hence $|s|\rho_{\alpha\cup\beta}X \subseteq |T|$.

(D2). Let $|s|\rho_{\alpha\cup\beta}X$, $S_X \subseteq \|B\|$, and $<\alpha\cup\beta>B \in \Gamma$. Then either $|s|\rho_\alpha X$ or $|s|\rho_\beta X$, and $<\alpha>B, <\beta>B \in \Gamma$. Hence by (D2) for α and β, one of $<\alpha>B$, and $<\beta>B$ is in s, implying $<\alpha\cup\beta>B \in s$ by D-*Alt*.

Combination.

(B1). Let A_s be a formula having

$$A_s \in t \quad \text{iff} \quad |s|\rho^+_{\alpha\cap\beta}|t|.$$

We show that

$$(<\alpha>\top \to [\beta]A_s),\ (<\beta>\top \to [\alpha]A_s) \in s, \tag{$\dagger$}$$

which gives $[\alpha\cap\beta]A_s \in s$ by B-*Comb*.

To prove ($\dagger$), let $<\alpha>\top \in s$. Then $sR_\alpha T$ for some T, and so by (D1) for α, $|s|\rho_\alpha X$ for some X. Then if $s\overline{R_\beta}t$ we have $|s|\rho^+_\beta|t|$ by (B1) for β, so with $|s|\rho_\alpha X$ we get $|s|\rho^+_{\alpha\cap\beta}|t|$, hence $A_s \in t$. This shows that $[\beta]A_s \in s$. We have now shown that $(<\alpha>\top \to [\beta]A_s) \in s$. The proof that $(<\beta>\top \to [\alpha]A_s) \in s$ is similar.

(B2). Let $|s|\overline{\rho_{\alpha\cap\beta}}|t|$. Then there exist X, Y with $|s|\rho_\alpha X$, $|s|\rho_\beta Y$, and either $|t| \in X$ or $|t| \in Y$.

Now suppose $[\alpha\cap\beta]B \in s \cap \Gamma$. Then $<\alpha>\top, <\beta>\top \in \Gamma$. Since $S_X, S_Y \subseteq \|\top\|$, (D2) for α and β then give $<\alpha>\top, <\beta>\top \in s$. Hence axiom B-*Comp* implies $[\beta]B, [\alpha]B \in s$. But if $|t| \in X$, then $|s|\rho_\alpha|t|$, so (B2) for α gives $B \in t$. If however $|t| \in Y$, we get the same conclusion from (B2) for β.

(D1). If $sR_{\alpha\cap\beta}T$, then by 12(4) there exist W_1, W_2 with $sR_\alpha W_1$, $sR_\beta W_2$, and $T = W_1 \cup W_2$. By (D1) for α and β, it follows that there exist X_1, X_2 with $|s|\rho_\alpha X_1 \subseteq |W_1|$ and $|s|\rho_\beta X_2 \subseteq |W_2|$. Hence

$$|s|\rho_{\alpha\cap\beta}(X_1 \cup X_2) \subseteq |W_1| \cup |W_2| \subseteq |T|.$$

(D2). Let $|s|\rho_{\alpha\cap\beta}X$, $S_X \subseteq \|B\|$, and $<\alpha\cup\beta>B \in \Gamma$. Then by definition of $\rho_{\alpha\cap\beta}$, there exist Y, Z with $|s|\rho_\alpha Y$, $|s|\rho_\beta Z$, and $X = Y \cup Z$. But $<\alpha>B, <\beta>B \in \Gamma$, and $S_Y, S_Z \subseteq S_X \subseteq \|B\|$, so by (D2) for α and β we get $<\alpha>B, <\beta>B \in s$. Axiom D-*Comb* then implies $<\alpha\cap\beta>B \in s$.

Iteration.

(B1). Let A_s be a formula having

$$A_s \in t \quad \text{iff} \quad |s|\rho^+_{\alpha^*}|t|.$$

We show that

$$\vdash A_s \to [\alpha]A_s. \tag{$\dagger$}$$

For, if $t \in S^m$ and $A_s \in t$, then $|s|(\rho_\alpha^+)^*|t|$, and so $|s|(\rho_\alpha^+)^n|t|$ for some $n \geq 0$. Then if $t\overline{R_\alpha}u$, (B1) for α implies $|t|\rho_\alpha^+|u|$, hence $|s|(\rho_\alpha^+)^{n+1}|u|$, so $|s|\rho_{\alpha^*}^+|u|$, and therefore $A_s \in u$. This shows $[\alpha]A_s \in t$, as required for (†).

By Necessitation for $[\alpha^*]$ and axiom B-*Ind*, we then have $(A_s \to [\alpha^*]A_s) \in s$. But $A_s \in s$ as $|s|(\rho_\alpha^+)^0|s|$, so $[\alpha^*]A_s \in s$, yielding (B1) for α^*.

(B2). Since $\overline{\rho_{\alpha^*}} = \overline{\rho_\alpha^{(*)}} = (\overline{\rho_\alpha})^*$, we want to show that

$$|s|(\overline{\rho_\alpha})^*|t| \quad \text{implies} \quad \{B : [\alpha^*]B \in s \cap \Gamma\} \subseteq t.$$

First we show, for all $n \geq 0$, that

$$|s|(\overline{\rho_\alpha})^n|t| \quad \text{implies} \quad \{[\alpha^*]B : [\alpha^*]B \in s \cap \Gamma\} \subseteq t. \tag{‡}$$

The case $n = 0$ is immediate, since $|s| = |t|$ implies $s \cap \Gamma = t \cap \Gamma$. Assuming the result for n, suppose $|s|(\overline{\rho_\alpha})^{n+1}|t|$. Then $|s|(\overline{\rho_\alpha})^n|u|$ and $|u|(\overline{\rho_\alpha})|t|$, for some u. Thus if $[\alpha^*]B \in s \cap \Gamma$, we have $[\alpha^*]B \in u$ by the hypothesis on n, and so $[\alpha][\alpha^*]B \in u \cap \Gamma$ by the axiom B-*Mix* and the definition of Γ. But then $[\alpha^*]B \in t$, by (B2) for α. This completes the inductive proof of (‡).

It follows that if $|s|(\overline{\rho_\alpha})^*|t|$, we have $|s|(\overline{\rho_\alpha})^n|t|$ for some n, so if $[\alpha^*]B \in s \cap \Gamma$, (‡) gives $[\alpha^*]B \in t$, and then B-*Mix* gives $B \in t$.

(D1). For any set $T \subseteq S^m$, let A_T be a formula such that for all $s \in S^m$,

$$A_T \in s \quad \text{iff} \quad |s|\rho_{\alpha^*}X \text{ for some } X \subseteq |T|.$$

We will prove

$$T \subseteq \|A_T\|, \tag{†}$$

and

$$\vdash <\alpha>A_T \to A_T. \tag{‡}$$

From these we derive (D1) for α^* as follows. If $sR_{\alpha^*}T$, then from (†) we get $<\alpha^*>A_T \in s$ (Theorem 9(1)). But from (‡) by Necessitation for α^* and axiom D-*Ind*,

$$\vdash <\alpha^*>A_T \to A_T,$$

so $A_T \in s$, giving $|s|\rho_{\alpha^*}X$ for some $X \subseteq |T|$ as desired.

To prove (†), let $t \in T$. Then $|t|\rho_{\alpha^*}\{|t|\}$, since $Id \subseteq \rho_\alpha^{(*)} = \rho_{\alpha^*}$, and $\{|t|\} \subseteq |T|$, so with $X = \{|t|\}$ we fulfill $A_T \in t$, and hence $t \in \|A_T\|$.

For (‡) it suffices to show that any maximal set containing $<\alpha>A_T$ must also contain A_T. So, let $s \in S^m$ have $<\alpha>A_T \in s$. Then $sR_\alpha U$ for some $U \subseteq \|A_T\|$. By (D1) for α, $|s|\rho_\alpha X$ for some $X \subseteq |U|$. Thus for some $k \in \omega$ we have $X = \{|u_0|, \ldots, |u_{k-1}|\}$, for some $u_0, \ldots, u_{k-1} \in U$.

Now for each i with $0 \leq i < k$ we have $A_T \in u_i$, since $U \subseteq \|A_T\|$, and so $|u_i|\rho_{\alpha^*}Y_i$ for some $Y_i \subseteq |T|$. Since $\mathcal{M}_\Gamma$ is standard for α^*, it follows that $|u_i|\rho_\alpha^{(n_i)}Y_i$ for some n_i. Let n be the maximum of $n_0, \ldots, n_{k-1}$. Then since the reachability relations $\rho_\alpha^{(m)}$ increase monotonically with m (Lemma 1(3)), we have $|u_i|\rho_\alpha^{(n)}Y_i$ for all $i < k$. Thus if $Y = \bigcup\{Y_i : 0 \leq i < k\}$, then $|s|(\rho_\alpha \cdot \rho_\alpha^{(n)})Y$, hence $|s|\rho_\alpha^{(n+1)}Y$, and so $|s|\rho_\alpha^{(*)}Y$. Therefore we have $|s|\rho_{\alpha^*}Y \subseteq |T|$, which ensures that $A_T \in s$ as desired.

(D2). If $|s|\rho_{\alpha^*}X$, then $|s|\rho_\alpha^{(n)}X$ for some n. Hence it suffices to prove that for all $n \geq 0$, and all $s \in S^m$,

$$\text{if } |s|\rho_\alpha^{(n)}X \text{ and } S_X \subseteq \|B\|, \text{ then } <\alpha^*>B \in \Gamma \text{ implies } <\alpha^*>B \in s. \qquad (\dagger)$$

For the case $n = 0$, if $|s|\rho_\alpha^{(0)}X$, i.e. $|s|Id\,X$, then $X = \{|s|\}$, so if $S_X \subseteq \|B\|$, then as $s \in S_X$ it follows that $B \in s$, and hence that $<\alpha^*>B \in s$ by axiom D-*Mix*.

Now make the inductive assumption that $(\dagger)$ holds for n, and let $|s|\rho_\alpha^{(n+1)}X$, $S_X \subseteq \|B\|$, and $<\alpha^*>B \in \Gamma$. Then either $|s|\rho_\alpha^{(0)}X$, whence the desired result follows as above, or else $|s|(\rho_\alpha \cdot \rho_\alpha^{(n)})X$. In the latter case there must then be some Y with $|s|\rho_\alpha Y$ such that $X = \bigcup\{X_y : y \in Y\}$, with $y\rho_\alpha^{(n)}X_y$ for all $y \in Y$.

Then if $t \in S_Y$, we have $|t| \in Y$, so $S_{X_{|t|}} \subseteq S_X \subseteq \|B\|$, whence as $|t|\rho_\alpha^{(n)}X_{|t|}$, the hypothesis on n gives $<\alpha^*>B \in t$. Thus $S_Y \subseteq \|<\alpha^*>B\|$. But $<\alpha><\alpha^*>B \in \Gamma$, and $|s|\rho_\alpha Y$, so by (D2) for α, $<\alpha><\alpha^*>B \in s$. Hence by D-*Mix* we get our desideratum $<\alpha^*>B \in s$.

This show that $(\dagger)$ holds for $n+1$, completing the inductive proof that it holds for all n, and hence completing the proof of Theorem 19. ■

COROLLARY 20. *$\mathcal{M}_\Gamma$ is a standard CPDL-model.*

PROOF. By definition, $\mathcal{M}_\Gamma$ is standard except possibly for tests. Since it is a filtration of $\mathcal{M}^m$, the Filtration Lemma 17 then implies that

$$\rho_{B?} = \{(x, \{x\}) : \mathcal{M}_\Gamma \models_x B\}$$

for $B? \in Prog_\Gamma$, so that $\mathcal{M}_\Gamma$ is also standard for tests. ■

THEOREM 21. *Any non-theorem of CPDL is falsifiable in a finite standard CPDL-model. Hence CPDL has the finite model property with respect to standard models, and is decidable.*

PROOF. Suppose $\nvdash A$. Then there is some maximal set s with $A \notin s$, so that $\mathcal{M}^m \not\models_s A$. Let Γ be a finite closed set containing A (Lemma 15).

Then $\mathcal{M}_\Gamma$ is a finite standard model in which A is false at $|s|$ (Theorems 19 and 20, and Filtration Lemma 17).

Since $CPDL$ is finitely axiomatisable, its decidability then follows as in [1, §4]. ■

Normality for $<\alpha>$

A natural condition to impose on models is that

$$sR_\alpha T \quad \text{implies} \quad T \neq \emptyset,$$

i.e.

$$\text{not-}sR_\alpha\emptyset,$$

since if $sR_\alpha T$ then T is the result of a terminating execution of α from s: termination implies the existence of a terminal state.

The corresponding axiom schema is

$$\text{D-}N: \qquad \neg<\alpha>\bot,$$

which is always true under the binary relation semantics. Indeed it requires only the schema

$$[\alpha]\neg A \rightarrow \neg<\alpha>A$$

to derive D-N from $[\alpha]\top$, which itself is a theorem of any logic that is normal for $[\alpha]$.

LEMMA 22.

(1) *Let Λ be a normal logic containing $CPDL$.*

(i) *Relative to Λ, the schema* D-N *is equivalent to each of the schemata*

$$[\alpha]\neg A \rightarrow \neg<\alpha>A$$

$$<\alpha>\neg A \rightarrow \neg[\alpha]A,$$

i.e. Λ contains one of these three schemata if, and only if, it contains the others.

(ii) *If $\vdash_\Lambda \neg<\pi>\bot$ for all atomic programs π, then $\vdash_\Lambda \neg<\alpha>\bot$ for all programs α.*

(iii) *If $\vdash_\Lambda \neg<\alpha>\bot$, then in the canonical model for Λ, not-$sR_\alpha\emptyset$.*

(2) *In a standard model, if not-$sR_\pi\emptyset$ for all atomic π, then not-$sR_\alpha\emptyset$ for all α.*

To prove the finite model property for the smallest normal logic obtained by adding D-N to $CPDL$, we modify the closure conditions on Γ to require that $<\pi>\bot \in \Gamma$ whenever π occurs in Γ. Then in the finite filtration $\mathcal{M}_\Gamma$ it can be shown that not-$|s|\rho_\pi\emptyset$ for all atomic $\pi \in Prog_\Gamma$. To see this, observe that if $|s|\rho_\pi\emptyset$, then since $S_\emptyset = \emptyset = \|\bot\|$, property (D2) of ρ_π implies $<\pi>\bot \in s$, which is inconsistent with D-N.

By Lemma 22(2) above, it then follows that not-$|s|\rho_\alpha\emptyset$ for all $\alpha \in Prog_\Gamma$, and so $\mathcal{M}_\Gamma$ is a D-N-model.

Sequential Atoms

The reachability relation R_α will be called *sequential* if

$$sR_\alpha T \quad \text{implies} \quad T = \{t\} \text{ for some } t.$$

The corresponding axiom schema is

$$Seq_\alpha: \quad [\alpha]\neg A \leftrightarrow \neg<\alpha>A,$$

from which $\neg<\alpha>\bot$ is derivable (22(1)(i)).

LEMMA 23. *In the canonical model for a normal logic containing $CPDL$ and Seq_α,*

$$<\alpha>A \in s \quad \text{iff} \quad \textit{there exists } t \textit{ with } s\overline{R_\alpha}t \textit{ and } A \in t.$$

PROOF. Recall that $s\overline{R_\alpha}t$ iff $s_\alpha \subseteq t$. Thus if $<\alpha>A \in s$, it suffices to show $s_\alpha \cup \{A\}$ is consistent. But if it were not, then $s_\alpha \vdash \neg A$, hence $[\alpha]\neg A \in s$ (8(5)), so $\neg<\alpha>A \in s$ by Seq_α, contrary to the consistency of s.

Conversely, if $s_\alpha \subseteq t$ and $A \in t$, then $\neg A \notin t$, so $[\alpha]\neg A \notin t$, whence by Seq_α and maximality of s, $<\alpha>A \in s$.

By a *sequential model* we will mean one in which the *atomic* relations R_π are sequential, so that parallelism depends on the presence of the combination connective $\alpha \cap \beta$ on programs. The (normal) logic determined by the class of sequential models is decidable, and is generated by adding the schemata Seq_π for all atomic π to $CPDL$. To show this, we modify the definition of

ρ_π in $\mathcal{M}_\Gamma$, by defining it as the following sequential reachability relation on S_Γ.

$$x\rho_\pi\{y\} \quad \text{iff} \quad \exists s \in x\ \exists t \in y\,(s\overline{R_\pi}t).$$

Thus

$$x\rho_\pi^+ y \quad \text{iff} \quad x\overline{\rho_\pi}y \quad \text{iff} \quad \exists s \in x\ \exists t \in y\,(s_\pi \subseteq t),$$

from which it follows readily that ρ_π meets filtration conditions (B1) and (B2).

To prove (D1) for ρ_π, let $sR_\pi T$ in the canonical model. Then $T \neq \emptyset$, since $\neg{<}\pi{>}\bot$ is derivable from Seq_π. Taking any $t \in T$, we get $s\overline{R_\pi}t$, and so $|s|\rho_\pi\{|t|\} \subseteq |T|$.

For (D2), let $|s|\rho_\pi X$, $S_X \subseteq \|B\|$, and ${<}\pi{>}B \in \Gamma$. Then there is some $s' \in |s|$, and some t such that $X = \{|t|\}$ and $s'\overline{R_\pi}t$. But then $t \in S_X$, so $B \in t$, and hence by Lemma 23, ${<}\pi{>}B \in s'$. Since ${<}\pi{>}B \in \Gamma$, we then get ${<}\pi{>}B \in s$ as desired.

This completes the proof that ρ_π is a Γ–filtration of R_π whenever $\pi \in Prog_\Gamma$. Thus $\mathcal{M}_\Gamma$ in this case is a finite sequential model that is a filtration of the canonical model. The rest of the story is as usual. ■

References

[1] ROBERT GOLDBLATT, **Logics of Time and Computation**, Lecture Notes No. 7, CSLI, Stanford, 1987. (Revised edition in preparation.)

[2] A. NERODE and D. WIJESEKERA, *Constructive concurrent dynamic logic I*, **technical report** '90 – 43, Mathematical Sciences Institute, Cornell University, 1990.

[3] DAVID PELEG, *Concurrent dynamic logic*, **JACM** 34 (1987), pp. 450 – 479.

[4] DAVID PELEG, *Communication in concurrent dynamic logic*, **J. Comp. Syst. Sci.** 35 (1987), pp. 23 – 58.

VICTORIA UNIVERSITY OF WELLINGTON
P.O.BOX 600
WELLINGTON, NEW ZEALAND

Received December 16, 1991.