Common Knowledge Semantics of Armstrong's Axioms

Zachary Heckle and Pavel Naumov

Department of Mathematics and Computer Science
McDaniel College, Westminster, Maryland 21157, USA
{zbh001,pnaumov}@mcdaniel.edu

Abstract. Armstrong's axioms were originally proposed to describe functional dependency between sets of attributes in relational databases. The database semantics of these axioms can be easily rephrased in terms of distributed knowledge in multi-agent systems. The paper proposes alternative semantics of the same axioms in terms of common knowledge. The main technical result of this work is soundness and completeness of Armstrong's axioms with respect to the proposed semantics. An important implication of this result is an unexpected duality between notions of distributed and common knowledge.

1 Introduction

1.1 Armstrong's Axioms

For any two variables a and b, we say that a functionally determines b if for each possible value of a there is a unique value of b. We denote this by $a \rhd b$. For example, the length of a side of an equilateral triangle functionally determines the area of the triangle: $length \rhd area$.

Similarly, one can define functional dependency between two *sets* of variables. For example, two legs of a right triangle uniquely determine its hypotenuse and area:

$$leg_1, leg_2 \rhd hypotenuse, area.$$

The functional dependency relation has been first studied in the context of database theory, where functional dependency is defined between two sets of attributes. Armstrong [1] proposed the following axiomatization of this relation:

1. *Reflexivity*: $A \rhd B$, if $A \supseteq B$,
2. *Augmentation*: $A \rhd B \to A, C \rhd B, C$,
3. *Transitivity*: $A \rhd B \to (B \rhd C \to A \rhd C)$,

where here and everywhere below A, B denotes the union of sets A and B. He proved soundness and completeness of this logical system with respect to a database semantics. The above axioms became known in database literature as Armstrong's axioms [2, p. 81]. Beeri, Fagin, and Howard [3] suggested a variation of Armstrong's axioms that describes properties of multi-valued dependence.

U. Kohlenbach et al. (Eds.): WoLLIC 2014, LNCS 8652, pp. 181–194, 2014.

Armstrong's axioms also describe properties of functional dependency in settings different from database theory. More and Naumov [4] investigated functional dependency between secrets shared over a network with a fixed topology. They presented a sound and complete axiomatization of this type of functional dependency consisting of Armstrong's axioms and one additional Gateway axiom that captures properties specific to the topology of the network. Harjes and Naumov [5] considered functional dependency between strategies of players in a Nash equilibrium of a strategic game. They gave a sound a complete axiomatization of this relation for games with a fixed dependency graph of a pay-off function. Their axiomatization also consists of Armstrong's axioms and one additional Contiguity axiom that captures properties specific to the topology of the graph. In another work, they axiomatized functional dependency between single strategies in Nash equilibria of cellular games [6]. Instead of considering secrets shared over a network with a fixed topology, one can consider a fixed group of symmetries of such a network. The complete axiomatization of functional dependency in such a setting [7] also consists of Armstrong's axioms and two additional axioms specific to the group of symmetries.

A logical system that simultaneously describes properties of functional dependency between single variables and properties of the nondeducibility relation [8] has been proposed earlier [9]. A different type of dependency in strategic games has been studied by Naumov and Nicholls [10]. They called it *rationally* functional dependence. The axioms of rationally functional dependence are significantly different from Armstrong's axioms discussed in this paper.

1.2 Distributed Knowledge

In the original Armstrong setting, in the functional dependency predicate $A \rhd B$, sets A and B are sets of database attributes. Let us assume now that each of the attributes in a database is known to a specific distinct agent and only to this agent. Furthermore, suppose that each of these agents knows nothing else but the value of the corresponding attribute. Under these assumptions, we can informally identify attributes with the agents that know them. Thus, relation $A \rhd B$ can now be viewed as a relation between sets of agents. Two sets of agents are in this relation if agents in set A collectively know all what is known to each agent in set B. In other words, everything distributively known to agents in set B is also distributively known to agents in set A. To paraphrase it once again: distributed knowledge of a set of agents B is a subset of distributed knowledge of a set of agents A:

$$DK(A) \supseteq DK(B), \qquad (1)$$

where $DK(A)$ informally represents distributed knowledge of set of agents A. Later in this paper, we formally specify the meaning of statement (1) and claim soundness and completeness of Armstrong's axioms with respect to semantics of distributed knowledge. The proofs are given in the appendix. These proofs are, essentially, translations of Armstrong's [1] arguments from database language to Kripke semantics language. The main focus of this paper is on *common* knowledge.

1.3 Common Knowledge

Let $CK(A)$, informally, denote all common knowledge [11] of set of agents A. By analogy with relation (1), one can consider relation

$$CK(A) \supseteq CK(B)$$

between sets of agents A and B. This relation does not satisfy Armstrong's axioms since the Reflexivity axiom does not hold (common knowledge of a subgroup, generally speaking, is not a common knowledge of a group). However, it turns out that relation

$$CK(A) \subseteq CK(B) \tag{2}$$

does satisfy Armstrong's axioms. Furthermore, the main technical result of this paper is the completeness theorem for Armstrong's axioms with respect to common knowledge semantics informally specified by relation (2).

The significant implication of this result is the duality between distributed knowledge and common knowledge captured by relations (1) and (2). Properties of both of them are described by Armstrong's axioms.

In the rest of the paper we first further discuss and formally define relation (1) in terms of epistemic Kripke frames. We then show how this definition can be modified to formally specify relation (2). We conclude the paper with the proof of soundness and completeness of Armstrong's axioms with respect to common knowledge semantics. In the appendix we show soundness and completeness of Armstrong's axioms with respect to distributed knowledge semantics.

2 Distributed Knowledge Semantics

Definition 1. *A Kripke frame is a triple* $(W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$, *where*

1. W *is a nonempty set of "epistemic worlds",*
2. $\mathcal{A}$ *is a set of "agents",*
3. $\sim_a$ *is an ("indistinguishability") equivalence relation on set* W *for each* $a \in \mathcal{A}$.

For any two epistemic worlds $u, v \in W$ and any set of agents $A \subseteq \mathcal{A}$, we write $u \sim_A v$ if $u \sim_a v$ for each $a \in A$.

According to the standard Kripke semantics of distributed knowledge [12, p. 24], $u \Vdash \Box_B p$ means that $v \Vdash p$ for each $v \in W$ such that $u \sim_B v$. If we want statement $u \Vdash \Box_B p \to \Box_A p$ to be true no matter how propositional variable p is evaluated over the given Kripke frame, we need to require that

$$\{v \in W \mid u \sim_A v\} \subseteq \{v \in W \mid u \sim_B v\}. \tag{3}$$

Epistemic logic usually studies the validity of formulas in a particular epistemic world. In Armstrong's database semantics, however, statement $A \rhd B$ means that the values of the attributes in set B are functionally determined by the values of attributes in set A for *all possible values* of the attributes in set A. Thus, under the corresponding distributed knowledge semantics, statement $A \rhd B$ should mean that (3) is true for each $u \in W$. In other words, informal statement (1) could be formally specified as

$$\forall u, v \in W(u \sim_A v \to u \sim_B v). \tag{4}$$

We use this specification in Definition 3.

Definition 2. *For any set of "agents" $\mathcal{A}$, by $\Phi(\mathcal{A})$ we mean the minimal set of formulas such that*

1. $\bot \in \Phi(\mathcal{A})$,
2. $A \rhd B \in \Phi(\mathcal{A})$ *for all finite subsets* $A, B \subseteq \mathcal{A}$,
3. *if* $\varphi, \psi \in \Phi(\mathcal{A})$, *then* $\varphi \to \psi \in \Phi(\mathcal{A})$.

Definition 3. *For any Kripke frame $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and any $\varphi \in \Phi(\mathcal{A})$, we define relation $K \vDash \varphi$ recursively:*

1. $K \nvDash \bot$,
2. $K \vDash A \rhd B$ *iff for each* $u, v \in W$, *if* $u \sim_A v$, *then* $u \sim_B v$,
3. $K \vDash \varphi \to \psi$ *iff* $K \nvDash \varphi$ *or* $K \vDash \psi$.

Theorem 1 (Armstrong [1]). *$K \vDash \varphi$ for each Kripke frame K whose set of agents contains all agents from formula φ if and only if formula φ is provable from Armstrong's axioms and propositional tautologies using the Modus Ponens inference rule.*

This theorem has been originally proven by Armstrong for database semantics, but, as we show in the appendix, his proof could be easily adopted to Kripke frames.

3 Common Knowledge Semantics

As usual, common knowledge of p between a group of agents A means that each agent knows p, each agent knows that each agent knows p, and so on ad infinitum. In epistemic logic notations [13,12], in epistemic world u there is a common knowledge of p between a group of agents A if for each sequence $a_1, \dots, a_m$ of elements of A, possibly with repetitions,

$$u \Vdash \Box_{a_1}\Box_{a_2}\dots\Box_{a_m}p.$$

Thus, in a given epistemic world u there is a common knowledge of p by the group of agents A if $v_m \Vdash p$ for each sequence $a_1, \dots, a_m$ of elements of A and each sequence of worlds $v_0, v_1, \dots, v_m \in W$ such that

$$u = v_0 \sim_{a_1} v_1 \sim_{a_2} v_2 \sim_{a_3} \cdots \sim_{a_m} v_m.$$

If we want common knowledge of p by group A in epistemic world u to imply common knowledge of p by group B in u no matter how propositional variable p is evaluated over the given Kripke frame, we need to require that

$$\{w_k \in W \mid u = w_0 \sim_{b_1} w_1 \sim_{b_2} w_2 \sim_{b_3} \cdots \sim_{b_n} w_n \text{ and } b_1, \ldots, b_n \in B\} \subseteq \{v_n \in W \mid u = v_0 \sim_{a_1} v_1 \sim_{a_2} v_2 \sim_{a_3} \cdots \sim_{a_m} v_m \text{ and } a_1, \ldots, a_m \in A\}.$$

Hence, for common knowledge by group A to imply common knowledge by group B in *each* epistemic world u we need to require that for each $x, y \in W$, if there exist $n \geq 0$, $w_0, \ldots, w_n \in W$, and $b_1, \ldots, b_n \in B$ such that

$$x = w_0 \sim_{b_1} w_1 \sim_{b_2} w_2 \sim_{b_3} \cdots \sim_{b_n} w_n = y,$$

then there must exist $m \geq 0$, $v_0, \ldots, v_m \in W$, and $a_1, \ldots, a_m \in A$ such that

$$x = v_0 \sim_{a_1} v_1 \sim_{a_2} v_2 \sim_{a_3} \cdots \sim_{a_m} v_m = y.$$

In the definition below, we take this requirement as the formalization of (2).

Definition 4. *Let $\vDash$ be the relation between a Kripke frame $K = (W, \mathcal{A}, \{\sim_a\}_{a \in \mathcal{A}})$ and a propositional formula in $\Phi(\mathcal{A})$ such that:*

1. $K \nvDash \bot$,
2. $K \vDash A \rhd B$ *iff for each $x, y \in W$, if there exist $n \geq 0$, $w_0, \ldots, w_n \in W$, and $b_1, \ldots, b_n \in B$ such that*

$$x = w_0 \sim_{b_1} w_1 \sim_{b_2} w_2 \sim_{b_3} \cdots \sim_{b_n} w_n = y,$$

then there exist $m \geq 0$, $v_0, \ldots, v_m \in W$, $a_1, \ldots, a_m \in A$ such that

$$x = v_0 \sim_{a_1} v_1 \sim_{a_2} v_2 \sim_{a_3} \cdots \sim_{a_m} v_m = y,$$

3. $K \vDash \varphi \to \psi$ *iff* $K \nvDash \varphi$ *or* $K \vDash \psi$.

4 Axioms

For any given set of agents $\mathcal{A}$, our logical system consists of all propositional tautologies in language $\Phi(\mathcal{A})$, the Modus Ponens inference rule, and Armstrong's axioms:

1. *Reflexivity*: $A \rhd B$, if $A \supseteq B$,
2. *Transitivity*: $A \rhd B \to (B \rhd C \to A \rhd C)$,
3. *Augmentation*: $A \rhd B \to A, C \rhd B, C$,

where, as we have mentioned earlier, A, B stands for the union of sets A and B. We write $X \vdash \varphi$ if statement φ is provable in our logical system using additional set of axioms X. We abbreviate $\varnothing \vdash \varphi$ as $\vdash \varphi$.

5 Example

The soundness of Armstrong's axioms with respect to common knowledge semantics will be shown in the next section. Note that soundness of the Reflexivity and Transitivity axioms is intuitively clear, but soundness of the Augmentation axiom is, perhaps, unexpected. Below we illustrate our logical system by stating and proving from Armstrong's axioms an even less intuitively clear property of common knowledge:

Theorem 2. $\vdash A \rhd B \rightarrow (C \rhd D \rightarrow A, C \rhd B, D)$.

Proof. Suppose that $A \rhd B$ and $C \rhd D$. Thus, by the Augmentation axiom, $A, C \rhd B, C$ and $B, C \rhd B, D$. Therefore, by the Transitivity axiom, $A, C \rhd B, D$.
□

6 Soundness

In this section we prove soundness of our logical system with respect to common knowledge semantics. Soundness of propositional tautologies and the Modus Ponens inference rule is straightforward. We prove soundness of each of Armstrong's axioms as a separate lemma.

Lemma 1. *$K \vDash A \rhd B$ for each $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and each $B \subseteq A \subseteq \mathcal{A}$.*

Proof. Consider any $x, y \in W$. Let there exist $n \geq 0$, $w_0, \ldots, w_n \in W$, and $b_1, \ldots,$
$b_n \in B$ such that

$$x = w_0 \sim_{b_1} w_1 \sim_{b_2} w_2 \sim_{b_3} \cdots \sim_{b_n} w_n = y.$$

Note that $b_1, \ldots, b_n \in A$ because $B \subseteq A$. □

Lemma 2. *For each $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and each $A, B, C \subseteq \mathcal{A}$, if $K \vDash A \rhd B$ and $K \vDash B \rhd C$, then $K \vDash A \rhd C$.*

Proof. Consider any $x, y \in W$. Let there exist $n \geq 0$, $w_0, \ldots, w_n \in W$, and $c_1, \ldots,$
$c_n \in C$ such that

$$x = w_0 \sim_{c_1} w_1 \sim_{c_2} w_2 \sim_{c_3} \cdots \sim_{c_n} w_n = y.$$

Thus, by assumption $K \vDash B \rhd C$, there exist $m \geq 0$, $v_0, \ldots, v_m \in W$, and $b_1, \ldots, b_m \in C$ such that

$$x = v_0 \sim_{b_1} v_1 \sim_{b_2} v_2 \sim_{b_3} \cdots \sim_{b_m} v_m = y.$$

Hence, by assumption $K \vDash A \rhd B$, there exist $k \geq 0$, $u_0, \ldots, u_k \in W$, and $a_1, \ldots, a_k \in A$ such that

$$x = u_0 \sim_{a_1} u_1 \sim_{a_2} u_2 \sim_{a_3} \cdots \sim_{a_k} u_k = y.$$

□

Lemma 3. *For each* $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ *and each* $A, B, C \subseteq \mathcal{A}$, *if* $K \vDash A \rhd B$, *then* $K \vDash A, C \rhd B, C$.

Proof. Consider any $x, y \in W$. Let there exist $n \geq 0$, $w_0, \ldots, w_n \in W$, and $e_1, \ldots,$
$e_n \in B \cup C$ such that

$$x = w_0 \sim_{e_1} w_1 \sim_{e_2} w_2 \sim_{e_3} \cdots \sim_{e_{n-1}} w_{n-1} \sim_{e_n} w_n = y.$$

We will show that there exist $m \geq 0$, $v_0, \ldots, v_m \in W$, and $f_1, \ldots, f_m \in A \cup C$ such that

$$x = v_0 \sim_{f_1} v_1 \sim_{f_2} v_2 \sim_{f_3} \cdots \sim_{f_m} v_m = y$$

by induction on n. If $n = 0$, then $x = y$ and $m = 0$.

Let $n > 0$. By the induction hypothesis, there exist $k \geq 0$, $u_0, \ldots, u_k \in W$, and $g_1, \ldots, g_k \in A \cup C$ such that

$$x = u_0 \sim_{g_1} u_1 \sim_{g_2} u_2 \sim_{g_3} \cdots \sim_{g_k} u_k = w_{n-1}.$$

Case I: $e_n \in C$. Then,

$$x = u_0 \sim_{g_1} u_1 \sim_{g_2} \cdots \sim_{g_k} u_k = w_{n-1} \sim_{e_n} w_n = y$$

and $g_1, g_2, \ldots, g_k, e_n \in A \cup C$.
Case II: $e_n \in B$. By assumption $K \vDash A \rhd B$, there exist $\ell \geq 0$, $t_0, t_1, \ldots, t_\ell \in W$, and $h_0, h_1, \ldots, h_\ell \in A$ such that

$$w_{k-1} = t_0 \sim_{h_1} t_1 \sim_{h_2} \cdots \sim_{h_\ell} t_\ell = w_n.$$

Therefore,

$$x = u_0 \sim_{g_1} u_1 \sim_{g_2} u_2 \sim_{g_3} \cdots \sim_{g_k} u_k = w_{n-1} = t_0 \sim_{h_1} t_1 \sim_{h_2} \cdots \sim_{h_\ell} t_\ell = w_n = y,$$

where $g_1, g_2, \ldots, g_k, h_1, h_2, \ldots, h_\ell \in A \cup C$. □

7 Two-World Kripke Frames

In this section we define a simple two-world Kripke frame. Later, multiple instances of such frames will be combined together to prove completeness of Armstrong's axioms with respect to common knowledge semantics.

Definition 5. *For any set of agents* $\mathcal{A}$ *and any subset* $D \subseteq \mathcal{A}$, *let* $K(\mathcal{A}, D)$ *be the Kripke frame* $(W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ *such that*

1. W *is the two-element set* $\{w_0, w_1\}$,
2. $w_0 \sim_a w_1$ *if and only if* $a \notin D$.

Informally, D is the set of all "distinguishers" who can distinguish world w_0 from world w_1.

Lemma 4. *For any set of agents $\mathcal{A}$ and any subset $D \subseteq \mathcal{A}$, $K(\mathcal{A}, D) \vDash A \rhd B$ if and only if at least one of the following conditions is satisfied:*

1. $A \nsubseteq D$,
2. $B \subseteq D$.

Proof. ($\Rightarrow$) Suppose $K \vDash A \rhd B$ as well as $A \subseteq D$ and $B \nsubseteq D$. Since $B \nsubseteq D$, there exists $b_0 \in B$ such that $b_0 \notin D$. Thus, $w_0 \sim_{b_0} w_1$, by Definition 5. Hence, by the assumption $K \vDash A \rhd B$, there exist $n \geq 0$, $v_0, \dots, v_n \in W$, and $a_1, \dots, a_n \in A$ such that

$$w_0 = v_0 \sim_{a_1} v_1 \sim_{a_2} \cdots \sim_{a_{n-1}} v_{n-1} \sim_{a_n} v_n = w_1,$$

which is a contradiction to $A \subseteq D$ and Definition 5.
($\Leftarrow$) First, assume that $A \nsubseteq D$. Thus, there exists $a_0 \in A$ such that $a_0 \notin D$. Hence, by Definition 5, $x \sim_{a_0} y$ for each $x, y \in W$. Thus, $K(\mathcal{A}, D) \vDash A \rhd B$.

Next, suppose $B \subseteq D$. To prove $K(\mathcal{A}, D) \vDash A \rhd B$, consider any $x, y \in W$. Let $n \geq 0$, $v_0, \dots, v_n \in W$, and $b_1, \dots, b_n \in B$ be such that

$$x = v_0 \sim_{b_1} v_1 \sim_{b_2} \cdots \sim_{b_{n-1}} v_{n-1} \sim_{b_n} v_n = y.$$

Thus, $x = y$ by the assumption $B \subseteq D$ and Definition 5. □

8 Product of Kripke Frames

In this section we define a composition operation on Kripke frames and prove a fundamental property of this operation. Later we use this operation to combine several different two-world frames, defined in the previous section, into a single Kripke frame needed to prove completeness of Armstrong's axioms with respect to common knowledge semantics.

Definition 6. *For any set of agents $\mathcal{A}$ and any family of Kripke frames $\{K^i\}_{i=0}^n = \{(W^i, \mathcal{A}, \{\sim_a^i\}_{a\in\mathcal{A}})\}_{i=0}^n$ we define the product $\prod_{i=0}^n K^i$ to be the Kripke frame $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$, where*

1. *W is the Cartesian product $\prod_{i=0}^n W^i$ of the sets of epistemic words of individual frames,*
2. *for any $\langle u_i\rangle_{i\leq n}, \langle v_i\rangle_{i\leq n} \in W$, let $\langle u_i\rangle_{i\leq n} \sim_a \langle v_i\rangle_{i\leq n}$ if $u_i \sim_a^i v_i$ for each $i \leq n$.*

Theorem 3. *Let $\mathcal{A}$ be any set of agents. If A and B are any two finite subsets of $\mathcal{A}$ and $\{K^i\}_{i=1}^n$ is any family of Kripke frames with set of agents $\mathcal{A}$, then $\prod_{i=1}^n K^i \Vdash A \rhd B$ if and only if $K^i \Vdash A \rhd B$ for each $i \leq n$.*

Proof. Let $\{K^i\}_{i=1}^n = \{(W^i, \mathcal{A}, \{\sim_a^i\}_{a\in\mathcal{A}})\}_{i=1}^n$.
($\Rightarrow$) Assume $i_0 \leq n$ and $x, y \in W^{i_0}$ are such that there exist $k \geq 0$, $v_0, \dots, v_k \in W$, and $b_1, \dots, b_k \in B$ such that

$$x = v_0 \sim_{b_1} v_1 \sim_{b_2} v_2 \sim_{b_3} \cdots \sim_{b_k} v_k = y.$$

We will show that there exist $m \geq 0$, $u_0, \dots, u_m \in W$, and $a_1, \dots, a_m \in A$ such that

$$x = u_0 \sim_{a_1} u_1 \sim_{a_2} u_2 \sim_{a_3} \cdots \sim_{a_m} u_m = y.$$

Indeed, due to Definition 1, for each $i \leq n$ there is at least one epistemic world $w^i \in W^i$. Then,

$$\langle w_1, \dots, w_{i_0-1}, v_0, w_{i_0+1}, \dots, w_n\rangle \sim_{b_1} \langle w_1, \dots, w_{i_0-1}, v_1, w_{i_0+1}, \dots, w_n\rangle \sim_{b_2}$$
$$\langle w_1, \dots, w_{i_0-1}, v_2, w_{i_0+1}, \dots, w_n\rangle \sim_{b_3} \cdots \sim_{b_k} \langle w_1, \dots, w_{i_0-1}, v_k, w_{i_0+1}, \dots, w_n\rangle$$

due to Definition 6 and reflexivity of relations $\{\sim_{b_i}\}_{i=1}^k$. Hence, by the assumption of the theorem, there exist $m \geq 0$, $\langle z_0^1, z_0^2, \dots, z_0^n\rangle$, $\langle z_1^1, z_1^2, \dots, z_1^n\rangle$, $\dots, \langle z_m^1, z_m^2, \dots, z_m^n\rangle$ in $\prod_{i=1}^n W^i$, and $a_1, \dots, a_m$ in A such that

$$\langle w_1, \dots, w_{i_0-1}, v_0, w_{i_0+1}, \dots, w_n\rangle = \langle z_0^1, z_0^2, \dots, z_0^n\rangle \sim_{a_1} \langle z_1^1, z_1^2, \dots, z_1^n\rangle \sim_{a_2}$$
$$\cdots \sim_{a_m} \langle z_m^1, z_m^2, \dots, z_m^n\rangle = \langle w_1, \dots, w_{i_0-1}, v_k, w_{i_0+1}, \dots, w_n\rangle.$$

Therefore, by Definition 6,

$$x = v_0 = z_0^{i_0} \sim_{a_1} z_1^{i_0} \sim_{a_2} z_2^{i_0} \sim_{a_3} \cdots \sim_{a_m} z_m^{i_0} = v_k = y.$$

($\Leftarrow$) Consider any $X, Y \in \prod_{i=1}^n W^i$. Suppose there exist $m \geq 0$, $b_1, \dots, b_m \in B$, and $\langle w_0^1, \dots, w_0^n\rangle$, $\langle w_1^1, \dots, w_1^n\rangle$, $\dots$, $\langle w_m^1, \dots, w_m^n\rangle$ in $\prod_{i=1}^n W^i$ such that

$$X = \langle w_0^1, \dots, w_0^n\rangle \sim_{b_1} \langle w_1^1, \dots, w_1^n\rangle \sim_{b_2}$$
$$\langle w_2^1, \dots, w_2^n\rangle \sim_{b_3} \cdots \sim_{b_m} \langle w_m^1, \dots, w_m^n\rangle = Y.$$

Thus, by Definition 6, for each $i \leq n$,

$$w_0^i \sim_{b_1} w_1^i \sim_{b_2} \cdots \sim_{b_m} w_m^i.$$

Hence, by the assumption of the theorem, for each $i \leq n$ there exist $k^i \geq 0$, $u_0^i, \dots, u_{k^i}^i \in W^i$, and $a_1^i, a_2^i, \dots, a_{k^i}^i \in A$ such that

$$w_0^i = u_0^i \sim_{a_1^i} u_1^i \sim_{a_2^i} u_2^i \sim_{a_3^i} \cdots \sim_{a_{k^i}^i} u_{k^i}^i = w_m^i.$$

Therefore, by Definition 6,

$$X = \langle w_0^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle = \langle u_0^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_1^1}$$
$$\langle u_1^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_2^1} \langle u_2^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_3^1} \cdots \sim_{a_{k^1}^1}$$
$$\langle u_{k^1}^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle = \langle w_m^1, w_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle =$$
$$\langle w_m^1, u_0^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_1^2} \langle w_m^1, u_1^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_2^2}$$
$$\langle w_m^1, u_2^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle \sim_{a_3^2} \cdots \sim_{a_{k^2}^2} \langle w_m^1, u_{k^2}^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle =$$
$$\langle w_m^1, w_m^2, w_0^3, \dots, w_0^{n-1}, w_0^n\rangle = \cdots = \langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, w_0^n\rangle =$$
$$\langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, u_0^n\rangle \sim_{a_1^n} \langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, u_1^n\rangle \sim_{a_2^n}$$
$$\langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, u_2^n\rangle \sim_{a_3^n} \cdots \sim_{a_{k^n}^n} \langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, u_{k^1}^n\rangle =$$
$$\langle w_m^1, w_m^2, w_m^3, \dots, w_m^{n-1}, w_m^n\rangle = Y.$$

□

9 Star Closure

In this section we introduce a technical notion of A^* closure of a set of agents A and prove basic properties of this notion. The closure is used in the next section to prove the completeness theorem.

Let $\mathcal{A}$ be any finite set of agents and M be any fixed subset of $\Phi(\mathcal{A})$.

Definition 7. *For any subset $A \subseteq \mathcal{A}$, let A^* be the set*

$$\{a \in \mathcal{A} \mid M \vdash A \rhd a\}.$$

Set A^* is finite due the assumption that set $\mathcal{A}$ is finite.

Lemma 5. *$A \subseteq A^*$, for each $A \subseteq \mathcal{A}$.*

Proof. Let $a \in A$. By the Reflexivity axiom, $\vdash A \rhd a$. Hence, $a \in A^*$. □

Lemma 6. *$M \vdash A \rhd A^*$, for each $A \subseteq \mathcal{A}$.*

Proof. Let $A^* = \{a_1, \ldots, a_n\}$. By the definition of A^*, $M \vdash A \rhd a_i$, for each $i \leq n$. We will prove, by induction on k, that $M \vdash (A \rhd a_1, \ldots, a_k)$ for each $0 \leq k \leq n$.
Base Case: $M \vdash A \rhd \varnothing$ by the Reflexivity axiom.
Induction Step: Assume that $M \vdash (A \rhd a_1, \ldots, a_k)$. By the Augmentation axiom,

$$M \vdash A, a_{k+1} \rhd a_1, \ldots, a_k, a_{k+1}. \tag{5}$$

Recall that $M \vdash A \rhd a_{k+1}$. Again by the Augmentation axiom, $M \vdash (A \rhd A, a_{k+1})$. Hence, $M \vdash (A \rhd a_1, \ldots, a_k, a_{k+1})$, by (5) and the Transitivity axiom. □

10 Completeness

We are now ready to prove completeness of Armstrong's axioms with respect to common knowledge semantics.

Theorem 4. *If $K \vDash \varphi$ for each Kripke frame K whose set of agents contains all agents in formula φ, then $\vdash \varphi$.*

Proof. Suppose $\nvdash \varphi$. Let $\mathcal{A}$ be the finite set of all agents mentioned in formula φ and M be a maximal consistent subset of $\Phi(\mathcal{A})$ containing formula $\neg\varphi$.

Definition 8. *Let Kripke frame K be $\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, A^*)$.*

Lemma 7. *$M \vdash B \rhd C$ if and only if $K \vDash B \rhd C$, for all subsets B and C of $\mathcal{A}$.*

Proof. $(\Rightarrow)$ First, suppose that $M \vdash B \rhd C$ and $\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, A^*) \nvDash B \rhd C$. Thus, by Theorem 3, there exists $A_0 \subseteq \mathcal{A}$ such that $K(\mathcal{A}, A_0^*) \nvDash B \rhd C$. Hence, by Lemma 4, $B \subseteq A_0^*$ and

$$C \nsubseteq A_0^*. \tag{6}$$

Then, by the Reflexivity axiom, $\vdash A_0^* \rhd B$. By assumption $M \vdash B \rhd C$ and the Transitivity axiom, $M \vdash A_0^* \rhd C$. By Lemma 6, $M \vdash A_0 \rhd A_0^*$. Thus, by the

Transitivity axiom, $X \vdash A_0 \rhd C$. By the Reflexivity axiom, $\vdash C \rhd c$ for all $c \in C$. Hence, by the Transitivity axiom, $M \vdash A_0 \rhd c$ for all $c \in C$. Then, $c \in A_0^*$ for all $c \in C$. Thus, $C \subseteq A_0^*$, which is a contradiction to (6).
($\Leftarrow$) Next, suppose $\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, A^*) \vDash B \rhd C$. Then, $K(\mathcal{A}, B^*) \vDash B \rhd C$. Hence, by Lemma 4, either $B \nsubseteq B^*$ or $C \subseteq B^*$. The former is not possible due to Lemma 5. Thus, $C \subseteq B^*$. Hence, by the Reflexivity axiom, $\vdash B^* \rhd C$. Note that $M \vdash B \rhd B^*$, by Lemma 6. Therefore, by the Transitivity axiom, $M \vdash B \rhd C$. □

Lemma 8. *$\psi \in M$ if and only if $K \vDash \psi$ for each $\psi \in \Phi(\mathcal{A})$.*

Proof. Induction on the structural complexity of formula ψ. The base case follows from Lemma 7. The induction step follows from Definition 4 as well as maximally and consistency of set M in the standard way. □

Note that $K \nvDash \psi$ due to assumption $\neg\varphi \in M$, Lemma 8, and consistency of set M. This concludes the proof of Theorem 4. □

11 Conclusion

In this paper we proposed common knowledge semantics for Armstrong's axioms and proved corresponding soundness and completeness theorems. This result shows that relations (1) and (2) have the same logical properties and, thus, demonstrates a certain duality between common knowledge and distributed knowledge.

A possible extension of our work could be developing a logical system that deals with relations (1) and (2) at the same time. Another possible extension of this work is to consider common knowledge on hypergraphs in the same way that it has been done [4] for distributed knowledge.

A Appendix: Distributed Knowledge Semantics

In this appendix we prove soundness and completeness of Armstrong's axioms with respect to the distributed knowledge semantics specified by Definition 3. Thus, everywhere in this section $\vDash$ refers to the relation from Definition 3 and not the one from Definition 4. The main result of this section is the completeness proof. In the presentation of this proof we follow the general outline of our completeness proof with respect to common knowledge semantics. In particular, we reuse earlier defined notions of two-world Kripke frames, product of Kripke frames, and star closure.

A.1 Soundness

In this section we prove soundness of our logical system with respect to distributed knowledge semantics. Soundness of propositional tautologies and the Modus Ponens inference rule is straightforward. We prove soundness of each of Armstrong's axioms as a separate lemma.

Lemma 9. *$K \vDash A \rhd B$ for each $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and each $B \subseteq A \subseteq \mathcal{A}$.*

Proof. Consider any $x, y \in W$. Suppose that $x \sim_A y$. Therefore, $x \sim_B y$ due to assumption $B \subseteq A$. □

Lemma 10. *For each $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and each $A, B, C \subseteq \mathcal{A}$, if $K \vDash A \rhd B$ and $K \vDash B \rhd C$, then $K \vDash A \rhd C$.*

Proof. Consider any $x, y \in W$. Suppose that $x \sim_A y$. Hence, $x \sim_B y$ by assumption $K \vDash A \rhd B$. Thus, $x \sim_C y$ by assumption $K \vDash B \rhd C$. □

Lemma 11. *For each $K = (W, \mathcal{A}, \{\sim_a\}_{a\in\mathcal{A}})$ and each $A, B, C \subseteq \mathcal{A}$, if $K \vDash A \rhd B$, then $K \vDash A, C \rhd B, C$.*

Proof. Consider any $x, y \in W$. Suppose that $x \sim_{A,C} y$. Thus, $x \sim_A y$ and $x \sim_C y$. Hence, $x \sim_B y$ by assumption $K \vDash A \rhd B$. Therefore, $x \sim_{B,C} y$. □

A.2 Completeness

We start with the distributed knowledge version of Lemma 4.

Lemma 12. *For any set of agents $\mathcal{A}$ and any subset $D \subseteq \mathcal{A}$, $K(\mathcal{A}, D) \vDash A \rhd B$ if and only if at least one of the following conditions is satisfied:*

1. *$A \cap D \neq \varnothing$,*
2. *$B \cap D = \varnothing$.*

Proof. ($\Rightarrow$) Suppose that $A \cap D = \varnothing$ and $B \cap D \neq \varnothing$. The former, by Definition 5, implies that $w_0 \sim_A w_1$, where w_0 and w_1 are the two worlds of Kripke frame $K(\mathcal{A}, D)$. The latter implies that there exists $b_0 \in B \cap D$. Thus, $w_0 \sim_B w_1$ due to assumption $K(\mathcal{A}, D) \vDash A \rhd B$. Hence, $w_0 \sim_{b_0} w_1$ because $b_0 \in B$, which is a contradiction to Definition 5 since $b_0 \in D$.
($\Leftarrow$) First, suppose that $A \cap D \neq \varnothing$. Thus, there exists $d_0 \in A \cap D$. To show that $K(\mathcal{A}, D) \vDash A \rhd B$, consider any $x, y \in \{w_0, w_1\}$ and assume that $x \sim_A y$. We will show that $x \sim_B y$. Indeed, $x \sim_A y$ implies that $x \sim_{d_0} y$ since $d_0 \in A$. Thus, $x = y$ by Definition 5 and assumption $d_0 \in D$. Therefore, $x \sim_B y$ due to reflexivity of relation $\sim_B$.

Second, assume that $B \cap D = \varnothing$. Thus, $x \sim_B y$ for each $x, y \in \{w_0, w_1\}$ due to Definition 5. Therefore, $K(\mathcal{A}, D) \vDash A \rhd B$, by Definition 3. □

Next is the distributed knowledge version of Theorem 3.

Theorem 5. *Let $\mathcal{A}$ be any set of agents. If A and B are any two finite subsets of $\mathcal{A}$, and $\{K^i\}_{i=1}^n$ is any family of Kripke frames with set of agents $\mathcal{A}$, then $\prod_{i=1}^n K^i \Vdash A \rhd B$ if and only if $K^i \Vdash A \rhd B$ for each $i \leq n$.*

Proof. ($\Rightarrow$) Consider any $i_0 \leq n$ and any $x, y \in W^{i_0}$ such that $x \sim_A y$. We will show that $x \sim_B y$. By Definition 1, for each $i \leq n$ there is at least one epistemic world $w^i \in W^i$. Note that

$$\langle w_1, w_2, \ldots, w_{i_0-1}, x, w_{i_0+1}, \ldots, w_n \rangle \sim_A \langle w_1, w_2, \ldots, w_{i_0-1}, y, w_{i_0+1}, \ldots, w_n \rangle$$

due to Definition 6, assumption $x \sim_A y$, and reflexivity of relation $\sim_A$. Hence,

$$\langle w_1, w_2, \ldots, w_{i_0-1}, x, w_{i_0+1}, \ldots, w_n \rangle \sim_B \langle w_1, w_2, \ldots, w_{i_0-1}, y, w_{i_0+1}, \ldots, w_n \rangle$$

by assumption $\prod_{i=1}^n K^i \Vdash A \rhd B$. Therefore, $x \sim_B y$ by Definition 6.
($\Leftarrow$) Consider any tuples $\langle x_1, x_2, \ldots, x_n \rangle$ and $\langle y_1, y_2, \ldots, y_n \rangle$ in $\prod_{i=1}^n W^i$ such that

$$\langle x_1, x_2, \ldots, x_n \rangle \sim_A \langle y_1, y_2, \ldots, y_n \rangle.$$

By Definition 6, $x_i \sim_A y_i$ for each $i \le n$. Hence, $x_i \sim_B y_i$ for each $i \le n$, due to the assumption of the theorem. Therefore, $\langle x_1, x_2, \ldots, x_n \rangle \sim_B \langle y_1, y_2, \ldots, y_n \rangle$. □

We are now ready to prove completeness of Armstrong's axioms with respect to distributed knowledge semantics. This result has been earlier claimed as a part of Theorem 1.

Theorem 6. *If $K \vDash \varphi$ for each Kripke frame K whose set of agents contains all agents in formula φ, then $\vdash \varphi$.*

Proof. Suppose $\nvdash \varphi$. Let $\mathcal{A}$ be the finite set of all agents mentioned in formula φ and M be a maximal consistent subset of $\Phi(\mathcal{A})$ containing formula $\neg\varphi$.

Definition 9. *Let Kripke frame K be*

$$\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, \mathcal{A} \setminus A^*).$$

Lemma 13. *$M \vdash B \rhd C$ if and only if $K \vDash B \rhd C$, for all finite subsets B and C of $\mathcal{A}$.*

Proof. ($\Rightarrow$) Suppose that $M \vdash B \rhd C$ and

$$\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, \mathcal{A} \setminus B^*) \nvDash B \rhd C.$$

Thus, by Theorem 5, there exists $A_0 \subseteq \mathcal{A}$ such that $K(\mathcal{A}, \mathcal{A} \setminus A_0^*) \nvDash B \rhd C$. Hence, by Lemma 12,

$$B \cap (\mathcal{A} \setminus A_0^*) = \varnothing$$

and

$$C \cap (\mathcal{A} \setminus A_0^*) \neq \varnothing.$$

In other words, $B \subseteq A_0^*$ and

$$C \nsubseteq A_0^*. \tag{7}$$

Then, by the Reflexivity axiom, $\vdash A_0^* \rhd B$. By assumption $M \vdash B \rhd C$ and the Transitivity axiom, $M \vdash A_0^* \rhd C$. By Lemma 6, $M \vdash A_0 \rhd A_0^*$. Thus, by the Transitivity axiom, $M \vdash A_0 \rhd C$. By the Reflexivity axiom, $\vdash C \rhd c$ for all $c \in C$.

Hence, by the Transitivity axiom, $M \vdash A_0 \rhd c$ for all $c \in C$. Then, $c \in A_0^*$ for all $c \in C$. Thus, $C \subseteq A_0^*$, which is a contradiction to (7).
($\Leftarrow$) Suppose $\prod_{A \subseteq \mathcal{A}} K(\mathcal{A}, \mathcal{A} \setminus A^*) \vDash B \rhd C$. Then, $K(\mathcal{A}, \mathcal{A} \setminus B^*) \vDash B \rhd C$, by Theorem 5. Hence, by Lemma 12, either $B \cap (\mathcal{A} \setminus B^*) \neq \varnothing$ or $C \cap (\mathcal{A} \setminus B^*) = \varnothing$. In other words, either $B \nsubseteq B^*$ or $C \subseteq B^*$. The former is not possible due to Lemma 5. Thus, $C \subseteq B^*$. Hence, by the Reflexivity axiom, $\vdash B^* \rhd C$. Note that $M \vdash B \rhd B^*$ by Lemma 6. Therefore, by the Transitivity axiom, $M \vdash B \rhd C$. □

Lemma 14. *$\psi \in M$ if and only if $K \vDash \psi$ for each $\psi \in \Phi(\mathcal{A})$.*

Proof. Induction on the structural complexity of formula ψ. The base case follows from Lemma 13. The induction step follows from the maximally and consistency of set M in the standard way. □

Note that $K \nvDash \psi$ due to assumption $\neg\varphi \in M$, Lemma 14, and consistency of set M. This concludes the proof of Theorem 6. □

References

1. Armstrong, W.W.: Dependency structures of data base relationships. In: Proc. IFIP Congress on Information Processing 1974, Stockholm, pp. 580–583. North-Holland, Amsterdam (1974)
2. Garcia-Molina, H., Ullman, J., Widom, J.: Database Systems: The Complete Book, 2nd edn. Prentice-Hall (2009)
3. Beeri, C., Fagin, R., Howard, J.H.: A complete axiomatization for functional and multivalued dependencies in database relations. In: SIGMOD 1977: Proceedings of the 1977 ACM SIGMOD International Conference on Management of Data, pp. 47–61. ACM, New York (1977)
4. More, S.M., Naumov, P.: The functional dependence relation on hypergraphs of secrets. In: Leite, J., Torroni, P., Ågotnes, T., Boella, G., van der Torre, L. (eds.) CLIMA XII 2011. LNCS, vol. 6814, pp. 29–40. Springer, Heidelberg (2011)
5. Harjes, K., Naumov, P.: Functional dependence in strategic games. In: 1st International Workshop on Strategic Reasoning, Rome, Italy. Electronic Proceedings in Theoretical Computer Science 112, pp. 9–15 (March 2013)
6. Harjes, K., Naumov, P.: Cellular games, nash equilibria, and Fibonacci numbers. In: Grossi, D., Roy, O., Huang, H. (eds.) LORI. LNCS, vol. 8196, pp. 149–161. Springer, Heidelberg (2013)
7. Kane, J., Naumov, P.: Symmetry in information flow. Annals of Pure and Applied Logic 165(1), 253–265 (2014)
8. Sutherland, D.: A model of information. In: Proceedings of Ninth National Computer Security Conference, pp. 175–183 (1986)
9. Kelvey, R., Miner More, S., Naumov, P., Sapp, B.: Independence and functional dependence relations on secrets. In: Proceedings of 12th International Conference on the Principles of Knowledge Representation and Reasoning, Toronto, pp. 528–533. AAAI (2010)
10. Naumov, P., Nicholls, B.: Rationally functional dependence. In: 10th Conference on Logic and the Foundations of Game and Decision Theory, LOFT (2012)
11. Lewis, D.: Convention: a philosophical study. Harvard University Press (1969)
12. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning about knowledge. MIT Press, Cambridge (1995)
13. Halpern, J.Y., Moses, Y.: Knowledge and common knowledge in a distributed environment. J. ACM 37(3), 549–587 (1990)