Symmetries and Epistemic Reasoning

Jeffrey Kane and Pavel Naumov

Department of Mathematics and Computer Science
McDaniel College, Westminster, Maryland 21157, USA

{jmk001,pnaumov}@mcdaniel.edu

Abstract. The paper studies epistemic properties of symmetric communication protocols. It proposes a logical system describing properties common to all protocols with the same group of symmetries. This system is an extension of the standard epistemic logic S5 by a new axiom, capturing properties of symmetry in the modal language. The main results are soundness and completeness theorems for this logical system.

1 Introduction

In this paper we study epistemic properties of symmetric communication protocols. Consider, for example, a variation of the well-known telephone[1] game in which a designated player picks a word and whispers it to the player on her left. The remaining six players, in turn, whisper the word to their left neighbors, possibly modifying it, until the word comes back to the original player. Let us assume that players only use four-letter words and at most one letter is changed at each step. For this example, let us also assume that the original player announces that the word that came back is identical to the word that she sent through the circular communication chain. We are interested in describing what each player knows about the words whispered by the other players.

In this example, the first and the last words are the same, so one can simplify the setting by talking about only six players (excluding the designated player) and the six words whispered by these players. We will refer to such a six-word cyclic sequence $r = (a, b, c, d, e, f)$ as a "run" of the telephone game. Note that each two adjacent words in the run (including words f and a) differ by no more than one letter.

Let run r_1 be the sequence $(math, hath, hate, fate, date, mate)$, as shown in Figure 1. Note that each agent who knows the value of the word a on this run is able to conclude that word d is not $true$ because words a and d are only three steps apart in the circle and thus can not differ by more than three letters. We will denote this epistemic fact by

$$r_1 \Vdash \Box_a(d \neq word). \tag{1}$$

In this example and throughout the rest of the paper, we label the modality not by an agent, as common in epistemic logic, but by the information known to the agent. We have used this approach in an earlier work [1].

[1] This game is also known as Chinese Whispers, Grapevine, Broken Telephone, Whisper Down the Lane, and Gossip.

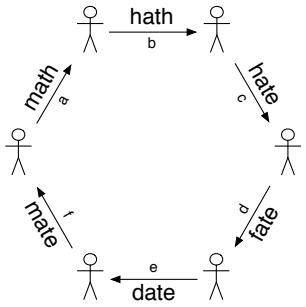

Fig. 1. Run r_1.

Another example of a true epistemic property of run r_1 is

$$r_1 \Vdash \Box_b \Box_a (b \neq word), \tag{2}$$

which states that any agent who knows the value of b on this run is able to conclude that any agent who knows the value of a knows that b is not $word$. This property is true because the words $hath$ and $word$ differ by four letters.

In all prior examples, the atomic propositions were inequality statements. An example of a true epistemic property of run r_1, with a different type of atomic proposition, is

$$r_1 \Vdash \Box_b (\text{ “Word } a \text{ contains at least one letter } h.\text{” }). \tag{3}$$

This property is true because the word $hath$ contains two letters h and any two adjacent words differ by no more than one letter.

Properties (1), (2), and (3) are specific to r_1. For instance, if $r_2 = (cars, caps, taps, tape, cape, care)$, then $r_2 \Vdash \Box_a (d \neq word)$ is false since any agent who knows only the value of a is not able to distinguish the run $(cars, caps, taps, tape, cape, care)$ from the run $(cars, card, cord, word, ward, wars)$. An example of an epistemic property which is true for each run of the telephone game is

$$\Vdash \Box_a (c \neq math) \rightarrow \Box_a (e \neq math). \tag{4}$$

This property is true on any run because of the symmetry in our setting. Namely, $(w_1, w_2, w_3, w_4, w_5, w_6)$ is a run of the telephone game iff $(w_1, w_6, w_5, w_4, w_3, w_2)$ is also such a run, see Figure 2. For a similar reason, the following property is true on any run of the telephone game:

$$\Vdash \Box_a \Box_b (f \neq math) \rightarrow \Box_a \Box_f (b \neq math).$$

Formally, by a symmetry of the telephone game we mean any bijection from the set $\{a, b, c, d, e, f\}$ into the same set that maps a run of the game into another run. In this paper, we will use graphical notations to describe symmetries. The symmetry τ that

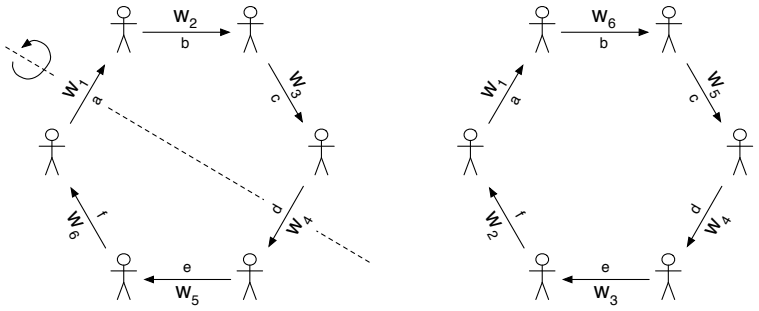

Fig. 2. Sequence $(w_1, w_2, w_3, w_4, w_5, w_6)$ is a run of the telephone game if and only if $(w_1, w_6, w_5, w_4, w_3, w_2)$ is also such a run.

maps the run $(w_1, w_2, w_3, w_4, w_5, w_6)$ to the run $(w_1, w_6, w_5, w_4, w_3, w_2)$ is depicted in Figure 3 (left). All symmetries of the telephone game protocol can be described as combinations of the rotation σ and the flip τ from Figure 3 (left). For example, symmetry μ depicted on the Figure 3 (right) is flip τ followed by rotation σ applied four times: $\sigma^4 \circ \tau$. In abstract algebra, the set of all symmetries of an object is commonly referred to as a group of symmetries of the object.

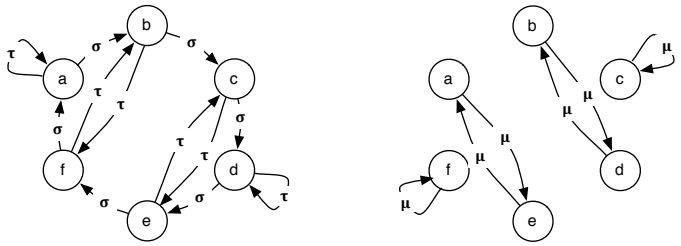

Fig. 3. Symmetries σ, τ, and μ of the telephone game, where $\mu = \sigma^4 \circ \tau$.

The telephone game is just an example of what we refer to as a "protocol". Another example of a protocol is a variation of the telephone game in which any two adjacent words differ by no more than *two* letters. This protocol has the same group of symmetries as the telephone game. In this paper we investigate common epistemic properties of all protocols that have the same group of symmetries. A more general way to state property (4) for an arbitrary protocol is

$$\Vdash \Box_a p \to \Box_a q, \tag{5}$$

where p is a property of the value of c and q is a "symmetric" property of the value of e. The exact meaning of the word "symmetric" in the previous sentence will be given in Definition 3.

The main result of this work is a sound and complete axiomatization of such properties for any fixed group of symmetries. This axiomatization is an extension of a variation of the multi-modal version of epistemic logic S5 [2] by an additional axiom specific to a given group of symmetries.

Properties of symmetry in information [3] and especially in applications to model checking [4] have been studied before. The closest to our current contribution is probably our own article on symmetries and functional dependencies [5]. The setting of that work is similar to our current setting in the sense that we also studied properties of a communication protocol with a given group of symmetries and gave a sound and complete axiomatization of these properties. However, in [5] we studied properties expressible in terms of functional dependence relation and the resulting logical system has been an extension of Armstrong [6] axiomatization of functional dependence. Our current work focuses on properties expressible in an epistemic modal language and the resulting logical system is an extension of multi-modal version of S5.

2 Group Theory Terminology

In this section we review group theory vocabulary used throughout the rest of the paper.

In abstract algebra, a group is a pair $G = (A, \cdot)$, where A is an arbitrary set and $\cdot$ is an associative binary operation on A such that A contains an identity element and an inverse element for each element of Σ.

In this paper, for any fixed set X by a group acting on X we mean an arbitrary set of permutations G of X (bijections from X onto X) such that

1. G is closed with respect to composition $\circ$,
2. G contains identity function,
3. if $\sigma \in G$, then $\sigma^{-1} \in G$.

We assume $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. By a stabilizer set G_x of an element x we mean the set $\{\sigma \in G \mid \sigma(x) = x\}$. In the telephone game example, G_a contains both the identity function and τ. Similarly, G_c contains the identity function and $\mu = \sigma^4 \circ \tau$. It is easy to see that G_x is itself a group. By the orbit $Orbit_G(x)$ of element $x \in X$ with respect to a group G we mean the set $\{\sigma(x) \mid \sigma \in G\}$. In the telephone game example, $Orbit_G(b)$ is the whole set $\{a, b, c, d, e, f\}$ and $Orbit_{G_a}(b)$ is the set $\{b, f\}$.

Given a set of bijections $\{\sigma_1, \ldots, \sigma_n\}$, by $\langle \sigma_1, \ldots, \sigma_n \rangle$ we mean the set of all possible finite combinations of bijections $\sigma_1, \ldots, \sigma_n$. For example, in the telephone game, $\langle \sigma, \tau \rangle$ is the entire group of symmetries of the telephone game.

If set X could be partitioned into sets Y and Z in such a way that each function in G maps Y onto Y and Z onto Z, then we say that group G acts on both Y and Z.

3 Syntax and Semantics

Definition 1. *A signature Σ is a triple $(S, \{P_a\}_{a \in S}, G)$ such that*

1. *S is an arbitrary set of variables,*
2. *$\{P_s\}_{s\in S}$ are disjoint sets of atomic propositions,*
3. *G is a group acting on set S and on set $\bigcup_{s\in S} P_s$,*
4. *$\sigma(p) \in P_{\sigma(s)}$ for each $\sigma \in G$ and each $p \in P_s$,*
5. *$\sigma(p) = p$ for each $s \in S$, each $p \in P_s$, and each $\sigma \in G_s$.*

For example, in the telephone game, the set S is $\{a, b, c, d, e, f\}$. Atomic propositions in the set P_a are meant to represent various statements about variable a. Examples of such statements for the telephone game are "word a contains at least one letter h" and $a \neq math$. Similarly, atomic propositions in set P_b meant to represent various statements about variable b such as "b contains two vowels" or even "b is a palindrome". Group G in the telephone game is $\langle \sigma, \tau \rangle$ and is known in abstract algebra as the dihedral group of order 12.

Next, for any signature Σ we define the set of formulas $\Phi(\Sigma)$. These formulas represent the properties of the protocols with signature Σ that we consider.

Definition 2. *For any signature Σ, let set $\Phi(\Sigma)$ be the smallest set such that*

1. *$\bot \in \Phi(\Sigma)$,*
2. *$P_a \subseteq \Phi(\Sigma)$, for each $a \in S$,*
3. *$\varphi \to \psi \in \Phi(\Sigma)$, for each $\varphi, \psi \in \Phi(\Sigma)$,*
4. *$\Box_a \varphi \in \Phi(\Sigma)$, for each $a \in S$ and each $\varphi \in \Phi(\Sigma)$.*

Definition 3. *A (symmetric) protocol over a signature $(S, \{P_a\}_{a\in S}, G)$ is any triple (V, R, Tr) such that*

1. *$V(a)$ is an arbitrary set of "possible values" of $a \in S$ such that if $a \in Orbit_G(b)$, then $V(a) = V(b)$,*
2. *R is an arbitrary set of functions (called "runs") such that any function $r \in R$ maps each $a \in S$ into an element of $V(a)$ and $r \circ \sigma \in R$ for each $\sigma \in G$,*
3. *Tr is an "atomic truth" predicate such that*
   (a) *$Tr \subseteq \bigcup_{a\in S}(V(a) \times P_a)$ and*
   (b) *Tr is symmetric in the sense that $(v, p) \in Tr$ if and only if $(v, \sigma(p)) \in Tr$, for each $a \in S$, $p \in P_a$, $\sigma \in G$, and $v \in V_a = V_{\sigma(a)}$.*

We will abbreviate $(v, p) \in Tr$ as $Tr(v, p)$. In the telephone game example, $V(a)$, $V(b), \ldots, V(f)$ are all equal to the set of all four-letter words. Atomic truth predicate $Tr(v, p)$ specifies whether an atomic proposition $p \in P_a$ is true for a specific value v of variable a. For example, proposition $p =$ " word a is a palindrome" is true if $v = noon$ but is false if $v = noun$.

Definition 4. *For any run $r \in R$ of a protocol (V, R, Tr) over a signature $\Sigma = (S, \{P_a\}_{a\in S}, G)$ and any formula $\varphi \in \Phi(\Sigma)$, we define relation $r \Vdash \varphi$ recursively:*

1. *$r \nVdash \bot$,*
2. *$r \Vdash p$ for $p \in P_a$ if $Tr(r(a), p)$,*
3. *$r \Vdash \varphi_1 \to \varphi_2$ if $r \nVdash \varphi_1$ or $r \Vdash \varphi_2$,*
4. *$r \Vdash \Box_a \psi$ if $r' \Vdash \psi$ for all $r' \in R$ such that $r'(a) = r(a)$.*

Definition 5. *For any signature $\Sigma = (S, \{P_s\}_{s\in S}, G)$ and any $\sigma \in G$, we extend σ from acting on set S and set $\bigcup_{s\in S} P_s$ to acting on set S and set $\Phi(\Sigma)$ as follows:*

1. $\sigma(\bot) = \bot$,
2. $\sigma(\psi_1 \to \psi_2) = \sigma(\psi_1) \to \sigma(\psi_2)$,
3. $\sigma(\Box_a \psi) = \Box_{\sigma(a)}\sigma(\psi)$.

Furthermore, we assume that $\sigma \in G$ also acts on sets of formulas in $\Phi(\Sigma)$ in such a way that $\sigma(X) = \{\sigma(\psi) \mid \psi \in X\}$.

4 Axioms

1. Distributivity: $\Box_a(\varphi \to \psi) \to (\Box_a\varphi \to \Box_a\psi)$,
2. Reflexivity: $\Box_a\varphi \to \varphi$,
3. Transitivity: $\Box_a\varphi \to \Box_a\Box_a\varphi$,
4. Euclideanity: $\neg\Box_a\varphi \to \Box_a\neg\Box_a\varphi$,
5. Self-Awareness: $p \to \Box_a p$ if $p \in P_a$,
6. Stability: $\Box_a\sigma(\varphi) \to \Box_a\varphi$, where $\sigma \in G_a$.

We write $\vdash_\Sigma \varphi$ if $\varphi \in \Phi(\Sigma)$ is provable from the axioms above and propositional tautologies in the language $\Phi(\Sigma)$ using the Modus Ponens inference rule and the Necessitation inference rule:

$$\frac{\varphi}{\Box_a\varphi}.$$

We write $X \vdash_\Sigma \varphi$ if φ is provable from the *theorems* of our logical system using only Modus Ponens rule and the additional set of axioms X. We will omit the subscript Σ when its value is clear from the context.

Lemma 1. *For each $\varphi \in \Phi(\Sigma)$, each $X \subseteq \Phi(\Sigma)$ and each $\sigma \in G$, if $X \vdash \varphi$, then $\sigma(X) \vdash \sigma(\varphi)$.*

Proof. Induction on the length of the proof of φ. If φ is an axiom, then $\sigma(\varphi)$ is also an axiom. If φ is derived from ψ and $\psi \to \varphi$ by Modus Ponens rule, then $\sigma(\varphi)$ could be derived from $\sigma(\psi)$ and $\sigma(\psi \to \varphi)$ by Modus Ponens rule because $\sigma(\psi \to \varphi) = \sigma(\psi) \to \sigma(\varphi)$ due to Definition 5. □

5 Examples

Soundness and completeness of our logical system will be established later in this paper. In this section we give several examples of proofs in our logical system. We will start with property (5) from the introduction.

Proposition 1. *Let $p \in P_c$ and $q \in P_e$. If group $G = \langle\sigma, \tau\rangle$ is acting, as shown on Figure 3, on set $S = \{a, b, c, d, e, f\}$, and additionally $\tau(q) = p$, then*

$$\vdash \Box_a p \to \Box_a q.$$

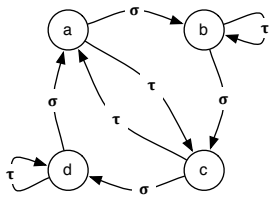

Fig. 4. Group $\langle \sigma, \tau \rangle$ acting on set $\{a, b, c, d\}$.

Proof. Note that $\tau(a) = a$. Hence, $\tau \in G_a$. Thus, by the Stability axiom, $\Box_a \tau(q) \to \Box_a q$. Therefore, $\Box_a p \to \Box_a q$. □

Proposition 2. *Let $p \in P_b$ and $q \in P_d$. If group $G = \langle \sigma, \tau \rangle$ is acting, as shown on Figure 4, on set $S = \{a, b, c, d\}$, and additionally $\sigma^2(q) = p$, then*

$$\vdash \Box_a p \to \Box_a q.$$

Proof. Note that $\tau \circ \sigma^2 \in G_a$. Thus, by the Stability axiom,

$$\vdash \Box_a (\tau \circ \sigma^2) q \to \Box_a q.$$

Due to our assumptions, $\sigma^2(q) = p$. In addition, by part 5 of Definition 1, $\tau(p) = p$. Hence, $(\tau \circ \sigma^2)q = p$. Therefore, $\vdash \Box_a p \to \Box_a q$. □

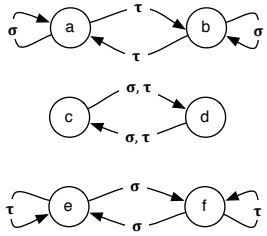

Fig. 5. Group $\langle \sigma, \tau \rangle$ acting on set $\{a, b, c, d, e, f\}$.

Proposition 3. *Let $p \in P_c$ and $q \in P_d$. If group $G = \langle \sigma, \tau \rangle$ is acting, as shown on Figure 5, on set $S = \{a, b, c, d, e, f\}$, and additionally $\sigma(q) = p$ and $\tau(p) = q$, then*

$$\vdash \Box_a \Box_e p \to \Box_a \Box_f p.$$

Proof. Since $\sigma \in G_a$, by the Stability axiom,

$$\vdash \Box_a(\sigma(\Box_f q)) \to \Box_a \Box_f q.$$

In other words,

$$\vdash \Box_a \Box_e p \to \Box_a \Box_f q. \tag{6}$$

At the same time, $\tau \in G_f$. Thus, by the Stability axiom,

$$\vdash \Box_f(\tau(p)) \to \Box_f p.$$

Hence,

$$\vdash \Box_f q \to \Box_f p.$$

Thus, by the Necessitation rule,

$$\vdash \Box_a(\Box_f q \to \Box_f p).$$

By the Distributivity axiom,

$$\vdash \Box_a \Box_f q \to \Box_a \Box_f p.$$

Finally, taking into account Statement (6),

$$\vdash \Box_a \Box_e p \to \Box_a \Box_f p.$$

□

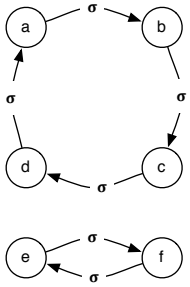

Fig. 6. Group $\langle\sigma\rangle$ acting on set $\{a, b, c, d, e, f\}$.

Proposition 4. *Let $p \in P_a$ and $q \in P_c$. If group $G = \langle\sigma\rangle$ is acting, as shown on Figure 6, on set $S = \{a, b, c, d, e, f\}$, and, additionally, $\sigma^2(p) = q$ and $\sigma^2(q) = p$, then*

$$\vdash \Box_e \Box_b(p \vee q) \to \Box_d(p \vee q).$$

Proof. Since $\sigma^2 \in G_e$, by the Stability axiom,

$$\Box_e \sigma^2 (\Box_d (q \vee p)) \rightarrow \Box_e \Box_d (q \vee p).$$

In other words,

$$\Box_e (\Box_b (p \vee q)) \rightarrow \Box_e \Box_d (q \vee p).$$

By the Reflexivity axiom,

$$\Box_e (\Box_b (p \vee q)) \rightarrow \Box_d (q \vee p). \tag{7}$$

Note now that $q \vee p \rightarrow p \vee q$ is a propositional tautology. Thus, by the Necessitation rule,

$$\Box_d (q \vee p \rightarrow p \vee q).$$

By the Distributivity axiom,

$$\Box_d (q \vee p) \rightarrow \Box_d (p \vee q).$$

Therefore, taking into account statement (7),

$$\Box_e (\Box_b (p \vee q)) \rightarrow \Box_d (p \vee q).$$

□

6 Soundness

Soundness of propositional tautologies and the Modus Ponens inference rule is straightforward. We will prove soundness of the Necessitation rule and of the remaining six axioms as separate lemmas.

Lemma 2 (necessitation). *If $r \Vdash \varphi$ for any run r of any protocol over a signature Σ, then $r \Vdash \Box_a \varphi$ for any run r of any protocol over Σ.*

Proof. Consider any run r of a protocol over signature Σ. It will be sufficient to show that $r' \Vdash \varphi$ for each r' of the same protocol such that $r'(a) = r(a)$, which is true due to the assumption of the lemma. □

Lemma 3 (distributivity). *For any run r of a protocol $\mathcal{P}$, if $r \Vdash \Box_a (\varphi \rightarrow \psi)$ and $r \Vdash \Box_a \varphi$, then $r \Vdash \Box_a \psi$.*

Proof. Let r' be any run of $\mathcal{P}$ such that $r'(a) = r(a)$. We will show that $r' \Vdash \psi$. Indeed, by the first assumption, $r' \Vdash \varphi \rightarrow \psi$. By the second assumption, $r' \Vdash \varphi$. Therefore, by Definition 4, $r' \Vdash \psi$. □

Lemma 4 (reflexivity). *For any run r of a protocol $\mathcal{P}$, if $r \Vdash \Box_a \varphi$, then $r \Vdash \varphi$.*

Proof. The lemma follows from Definition 4 and the fact that $r(a) = r(a)$. □

Lemma 5 (transitivity). *For any run r of a protocol $\mathcal{P}$, if $r \Vdash \Box_a \varphi$, then $r \Vdash \Box_a \Box_a \varphi$.*

Proof. Consider any run r' of the protocol $\mathcal{P}$ such that $r'(a) = r(a)$. It will be sufficient to show that $r' \Vdash \Box_a\varphi$. Consider now any run r'' of the same protocol such that $r''(a) = r'(a)$. We need to prove that $r'' \Vdash \varphi$, which is true due to the fact $r''(a) = r'(a) = r(a)$ and the assumption $r \Vdash \Box_a\varphi$. □

Lemma 6 (Euclideanity). *For any run r of a protocol $\mathcal{P}$, if $r \nVdash \Box_a\varphi$, then $r \Vdash \Box_a\neg\Box_a\varphi$.*

Proof. By the assumption $r \nVdash \Box_a\varphi$, there exists a run r' of the protocol $\mathcal{P}$ such that $r'(a) = r(a)$ and $r' \nVdash \varphi$. Consider any run r'' of the protocol $\mathcal{P}$ such that $r''(a) = r(a)$. It will be sufficient to show that $r'' \nVdash \Box_a\varphi$, which follows from $r''(a) = r(a) = r'(a)$ and $r' \nVdash \varphi$. □

Lemma 7 (self-awareness). *For any run r of a protocol $\mathcal{P}$ and any $p \in P_a$, if $r \Vdash p$, then $r \Vdash \Box_a p$.*

Proof. If $r \Vdash p$, then $Tr(r(a), p)$ by Definition 4. Thus, $Tr(r'(a), p)$ for each run r' of the protocol P such that $r'(a) = r(a)$. Hence, by Definition 4, $r' \Vdash p$ for each run r' of the protocol P such that $r'(a) = r(a)$. Therefore, again by Definition 4, $r \Vdash \Box_a p$. □

Our proof of soundness for the Stability axiom relies on the following lemma. As we mentioned before, by $f \circ g$ we denote the composition of functions f and g such that $(f \circ g)(x) = f(g(x))$.

Lemma 8. *For any run r of a protocol $\mathcal{P}$ over a signature $(S, \{P_a\}_{a\in S}, G)$ and any $\sigma \in G$, if $r \Vdash \varphi$, then $(r \circ \sigma) \Vdash \sigma^{-1}(\varphi)$.*

Proof. Induction on structural complexity of formula φ.

1. If $\varphi \equiv \bot$, then $r \nVdash \bot$ by Definition 4.
2. Let $\varphi \equiv p$ for some $a \in S$ and some $p \in P_a$. If $r \Vdash p$, then by Definition 4, $Tr(r(a), p)$. Thus, $Tr(r(\sigma(\sigma^{-1}(a))), p)$. Hence, $Tr(r(\sigma(\sigma^{-1}(a))), \sigma^{-1}(p))$ by item 3b of Definition 3. Notice now that $\sigma^{-1}(p) \in P_{\sigma^{-1}(a)}$ due to Definition 1. Therefore, $(r \circ \sigma) \Vdash \sigma^{-1}(p)$ by Definition 4.
3. Let $\varphi \equiv \psi_1 \to \psi_2$. Assume $r \Vdash \psi_1 \to \psi_2$. Then by Definition 4, $r \nVdash \psi_1$ or $r \Vdash \psi_2$.
   First suppose $r \nVdash \psi_1$. In other words, $r \nVdash \sigma(\sigma^{-1}(\psi_1))$. Thus, $(r \circ \sigma \circ \sigma^{-1}) \nVdash \sigma(\sigma^{-1}(\psi_1))$. Then, $(r \circ \sigma) \nVdash \sigma^{-1}(\psi_1)$ by the contrapositive of the Induction Hypothesis for bijection σ^{-1}. Hence, by Definition 4, $(r \circ \sigma) \Vdash \sigma^{-1}(\psi_1) \to \sigma^{-1}(\psi_2)$. Therefore, by Definition 5, $(r \circ \sigma) \Vdash \sigma^{-1}(\psi_1 \to \psi_2)$.
   Next suppose $r \Vdash \psi_2$. Then, by the Induction Hypothesis, $(r \circ \sigma) \Vdash \sigma^{-1}(\psi_2)$. Thus, by Definition 4, $(r \circ \sigma) \Vdash \sigma^{-1}(\psi_1) \to \sigma^{-1}(\psi_2)$. Therefore, by Definition 5, $(r \circ \sigma) \Vdash \sigma^{-1}(\psi_1 \to \psi_2)$.
4. Let $\varphi \equiv \Box_a\psi$ for some $a \in S$. Let $r \Vdash \Box_a\psi$. We need to show $(r \circ \sigma) \Vdash \sigma^{-1}(\Box_a\psi)$. By Definition 5, this is equivalent to $(r \circ \sigma) \Vdash \Box_{\sigma^{-1}(a)}\sigma^{-1}(\psi)$. Consider any r' of the protocol $\mathcal{P}$ such that $r'(\sigma^{-1}(a)) = (r \circ \sigma)(\sigma^{-1}(a))$. It will be sufficient to show that $r' \Vdash \sigma^{-1}(\psi)$. Note that $r'(\sigma^{-1}(a)) = r(a)$. Thus, by the assumption $r \Vdash \Box_a\psi$ and Definition 4, $(r' \circ \sigma^{-1}) \Vdash \psi$. Then, by the Induction Hypothesis, $(r' \circ \sigma^{-1} \circ \sigma) \Vdash \sigma^{-1}(\psi)$. Therefore, $r' \Vdash \sigma^{-1}(\psi)$. □

Lemma 9 (stability). *For any run r of a protocol $\mathcal{P}$ over a signature $(S, \{P_a\}_{a\in S}, G)$ and any $\sigma \in G_a$, if $r \Vdash \Box_a\sigma(\varphi)$, then $r \Vdash \Box_a\varphi$.*

Proof. Consider an arbitrary run r' of the protocol $\mathcal{P}$ such that $r'(a) = r(a)$. It will be sufficient to show $r' \Vdash \varphi$. By Lemma 8, $r \Vdash \Box_a\sigma(\varphi)$ implies $(r \circ \sigma) \Vdash \Box_{\sigma^{-1}(a)}\varphi$. Hence, $(r \circ \sigma) \Vdash \Box_a\varphi$ because $\sigma \in G_a$ and thus $\sigma^{-1} \in G_a$ as well. Notice that $(r \circ \sigma)(a) = r(a) = r'(a)$, because $\sigma \in G_a$ and due to the assumption $r'(a) = r(a)$. Therefore, by Definition 4, $r' \Vdash \varphi$. □

7 Completeness

In this section, we will prove the completeness of our logical system. The completeness argument follows the standard outline of a modal logic completeness, with additional considerations for the symmetry of our setting.

Theorem 1. *Let $\Sigma = (S, \{P_a\}_{a\in S}, G)$ be an arbitrary signature and let $\varphi \in \Phi(\Sigma)$. If $r \Vdash \varphi$ for each run $r \in R$ of each protocol (V, R, Tr) over Σ, then $\vdash_\Sigma \varphi$.*

Proof. Suppose that $\nvdash_\Sigma \varphi$. We will construct a protocol $\mathcal{P} = (V, R, Tr)$ over Σ and a run $r \in R$ such that $r \nVdash \varphi$. Let X_0 be any maximal and consistent (in the sense $X_0 \nvdash_\Sigma \bot$) subset of $\Phi(\Sigma)$ such that $\neg\varphi \in X_0$. By $\mathbb{X}$ we mean the set of all maximal and consistent subsets of $\Phi(\Sigma)$. Thus, for instance $X_0 \in \mathbb{X}$.

Definition 6. *For any $X, Y \in \mathbb{X}$ let $X \sim_a Y$ mean that $\Box_a\psi \in X$ if and only if $\Box_a\psi \in Y$ for each $\psi \in \Phi(S)$.*

Lemma 10. *Relation $\sim_a$ is an equivalence relation on $\mathbb{X}$, for each $a \in S$.* □

By $\mathbb{X}_a$ we mean the set of equivalence classes with respect to the relation $\sim_a$, and by $[X]_a$ we mean the equivalence class of X. We will later use these classes to define the values in $V(a)$ of protocol $\mathcal{P}$. The next lemma is a standard lemma in the proofs of completeness for modal logics.

Lemma 11. *For any $X \in \mathbb{X}$ and any ψ such that $\Box_a\psi \notin X$, there is $Y \in \mathbb{X}$ such that $Y \sim_a X$ and $\neg\psi \in Y$.*

Proof. We will first show that the following set is consistent:

$$\{\Box_a\omega \mid \Box_a\omega \in X\} \cup \{\neg\Box_a\eta \mid \neg\Box_a\eta \in X\} \cup \{\neg\psi\}.$$

Towards a contradiction, let there be $\Box_a\omega_1, \ldots, \Box_a\omega_n, \neg\Box_a\eta_1, \ldots, \neg\Box_a\eta_k \in X$ such that

$$\vdash \Box_a\omega_1 \to (\cdots \to (\Box_a\omega_n \to (\neg\Box_a\eta_1 \to (\cdots \to (\neg\Box_a\eta_k \to \psi)\ldots)))\ldots).$$

By the Necessitation rule,

$$\vdash \Box_a(\Box_a\omega_1 \to (\cdots \to (\Box_a\omega_n \to (\neg\Box_a\eta_1 \to (\cdots \to (\neg\Box_a\eta_k \to \psi)\ldots)))\ldots)).$$

By multiple applications of the Distributivity axiom,

$$\vdash \Box_a\Box_a\omega_1 \to (\cdots \to (\Box_a\Box_a\omega_n \to (\Box_a\neg\Box_a\eta_1 \\ \to (\cdots \to (\Box_a\neg\Box_a\eta_k \to \Box_a\psi)\dots)))\dots).$$

By multiple applications of the Transitivity axiom,

$$\vdash \Box_a\omega_1 \to (\cdots \to (\Box_a\omega_n \to (\Box_a\neg\Box_a\eta_1 \\ \to (\cdots \to (\Box_a\neg\Box_a\eta_k \to \Box_a\psi)\dots)))\dots).$$

By multiple applications of the Euclideanity axiom,

$$\vdash \Box_a\omega_1 \to (\cdots \to (\Box_a\omega_n \to (\neg\Box_a\eta_1 \to \\ (\cdots \to (\neg\Box_a\eta_k \to \Box_a\psi)\dots)))\dots).$$

Hence, by multiple applications of the Modus Ponens rule,

$$\Box_a\omega_1, \dots, \Box_a\omega_n, \neg\Box_a\eta_1, \dots, \neg\Box_a\eta_k \vdash \Box_a\psi.$$

Thus, $X \vdash \Box_a\psi$, which is a contradiction with maximality of X and the assumption $\Box_a\psi \notin X$. Let Y be a maximal consistent set containing

$$\{\Box_a\omega \mid \Box_a\omega \in X\} \cup \{\neg\Box_a\eta \mid \neg\Box_a\eta \in X\} \cup \{\neg\psi\}.$$

We are only left to show that if $\Box_a\eta \in Y$, then $\Box_a\eta \in X$ for each $\Box_a\eta \in \Phi(\Sigma)$. Indeed, assume that $\Box_a\eta \notin X$. Then, $\neg\Box_a\eta \in X$ by the maximality of X. Hence, $\neg\Box_a\eta \in Y$ due to the choice of Y. Therefore, $\Box_a\eta \notin Y$ due to consistency of Y. □

The following lemma shows that the symmetries which act on S and $\Phi(\Sigma)$ also could be viewed as acting on $\mathbb{X}$.

Lemma 12. *$\sigma(X) \in \mathbb{X}$, for each $X \in \mathbb{X}$ and each $\sigma \in G$.*

Proof. To prove maximality of the set $\sigma(X)$, consider any formula $\varphi \in \Phi(S)$. It will be sufficient to show that either $\varphi \in \sigma(X)$ or $(\varphi \to \bot) \in \sigma(X)$. Indeed, consider the formula $\sigma^{-1}(\varphi)$. Due to the assumption of maximality of the set X, either $\sigma^{-1}(\varphi) \in X$ or $\sigma^{-1}(\varphi \to \bot) \in X$. Therefore, either $\varphi \in \sigma(X)$ or $(\varphi \to \bot) \in \sigma(X)$ by Definition 5.

To prove consistency of the set $\sigma(X)$, suppose that $\sigma(X) \vdash \bot$. Thus, $\sigma^{-1}(\sigma(X)) \vdash \sigma^{-1}(\bot)$ by Lemma 1. Therefore, by Definition 5, $X \vdash \bot$, which is a contradiction with the assumption of consistency of the set X. □

Lemma 13. *If $X \sim_a Y$, then $\sigma(X) \sim_{\sigma(a)} \sigma(Y)$, for each $\sigma \in G$, each $X, Y \in \mathbb{X}$, and each $a \in S$.*

Proof. Let $\Box_{\sigma(a)}\psi \in \sigma(X)$. Thus, $\sigma^{-1}(\Box_{\sigma(a)}\psi) \in X$. Hence, $\Box_a\sigma^{-1}(\psi) \in X$. Then, $\Box_a\sigma^{-1}(\psi) \in Y$ by the assumption $X \sim_a Y$. Hence, $\sigma(\Box_a\sigma^{-1}(\psi)) \in \sigma(Y)$. In other words, $\Box_{\sigma(a)}\psi \in \sigma(Y)$. □

It follows from the previous lemma that symmetry σ now also can be viewed as acting on $\bigcup_{a\in S}\mathbb{X}_a$ in such a way that $\sigma([X]_a) = [\sigma(X)]_{\sigma(a)}$.

Lemma 14. *For any $X \in \mathbb{X}$, any $a \in S$, and any $\sigma \in G_a$, $\sigma(X) \sim_a X$.*

Proof. Suppose that $\Box_a\psi \in X$. Thus, $\sigma(\Box_a\psi) \in \sigma(X)$. Hence, $\Box_a\sigma(\psi) \in \sigma(X)$, by the assumption $\sigma \in G_a$. Therefore, $\Box_a\psi \in \sigma(X)$, by the Stability axiom and maximality of $\sigma(X)$.

Assume now that $\Box_a\psi \in \sigma(X)$. Thus, $\sigma^{-1}(\Box_a\psi) \in X$. Hence, $\Box_a\sigma^{-1}(\psi) \in X$, because $\sigma \in G_a$ and thus $\sigma^{-1} \in G_a$. Therefore, $\Box_a\psi \in X$ by the Stability axiom and due to maximality of X. □

Recall that by the orbit $Orbit_G(a)$ of element $a \in S$ with respect to group G we mean the set $\{\sigma(a) \mid \sigma \in G\}$. Orbits partition set S into disjoint subsets. We pick a unique representative from each orbit. If $a \in S$, then the unique representative of $Orbit_G(a)$ is denoted by $\widehat{a}$. For each $a \in S$ we also pick any $\mu_a \in G$ such that $\mu_a(\widehat{a}) = a$. We are now ready to define the protocol $\mathcal{P} = (V, R, Tr)$.

Definition 7. *For any $a \in S$, let $V(a) = \mathbb{X}_{\widehat{a}}$.*

The following lemma verifies that $\mathcal{P}$ satisfies condition 1 from Definition 3.

Lemma 15. *$V(a) = V(\sigma(a))$ for each $a \in S$ and each $\sigma \in G$.*

Proof. Note that $\widehat{a} = \widehat{\sigma(a)}$ because the elements a and $\sigma(a)$ belong to the same orbit. Thus, $V(a) = \mathbb{X}_{\widehat{a}} = \mathbb{X}_{\widehat{\sigma(a)}} = V(\sigma(a))$. □

Definition 8. *Let set R contain all functions $r(s)$ on the set S such that*

1. *$r(a) \in V(a)$ for each $a \in S$,*
2. *$\bigcap_{a\in S}\mu_a(r(a)) \neq \varnothing$.*

The first condition of the above definition mirrors Definition 3. Informally, the second condition requires the values of the same run to be "consistent" with each other. The technical lemma below shows that the intersection of a family of sets is not dependent on the indexing of the family.

Lemma 16. *If $\{Y_a\}_{a\in S}$ is an arbitrary family of sets and f is any bijection of S onto S, then*

$$\bigcap_{a\in S} Y_a = \bigcap_{a\in S} Y_{f(a)}.$$

Proof. Since f is a bijection, the left side and the right side of the equality intersect the same family of sets (indexed differently). □

The next lemma demonstrates that $\mathcal{P}$ satisfies condition 2 of Definition 3.

Lemma 17. *$r \circ \sigma \in R$ for each $r \in R$ and each $\sigma \in G$.*

Proof. We need to show that $r \circ \sigma$ satisfies both conditions from Definition 8. We will do it separately.

1. Assume that $a \in S$. We will show that $(r \circ \sigma)(a) \in V(a)$. Indeed, $(r \circ \sigma)(a) = r(\sigma(a)) \in V(\sigma(a))$, hence, by Lemma 15, $(r \circ \sigma)(a) \in V(a)$.
2. We will now show that $\bigcap_{a \in S} \mu_a(r \circ \sigma(a)) \neq \varnothing$. Indeed, by Definition 8, there is a set X such that $X \in \bigcap_{a \in S} \mu_a(r(a))$. Hence, $X \in \mu_a(r(a))$ for each $a \in S$. Thus,

$$(\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1})X \in (\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1})\mu_a(r(a)),$$

for each $a \in S$. Hence,

$$(\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1})X \in \sigma(\mu_{\sigma^{-1}(a)}(r(a))), \tag{8}$$

for each $a \in S$. Note now that $(\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1})(a) = (\sigma \circ \mu_{\sigma^{-1}(a)})(\widehat{a}) = \sigma(\sigma^{-1}(a)) = a$ by the choice of $\widehat{a}$ and μ_a. Thus, $\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1} \in G_a$. Hence, by Lemma 14, $(\sigma \circ \mu_{\sigma^{-1}(a)} \circ \mu_a^{-1})X \sim_a X$. Then, due to (8),

$$X \in \sigma(\mu_{\sigma^{-1}(a)}(r(a))),$$

for each $a \in S$. Thus,

$$\sigma^{-1}(X) \in \sigma^{-1}(\sigma(\mu_{\sigma^{-1}(a)}(r(a)))),$$

for each $a \in S$. Then,

$$\sigma^{-1}(X) \in \mu_{\sigma^{-1}(a)}(r(a)),$$

for each $a \in S$. Hence,

$$\sigma^{-1}(X) \in \bigcap_{a \in S} \mu_{\sigma^{-1}(a)}(r(a)).$$

Then, by Lemma 16,

$$\sigma^{-1}(X) \in \bigcap_{a \in S} \mu_a(r(\sigma(a))).$$

Therefore, $\bigcap_{a \in S} \mu_a(r \circ \sigma(a)) \neq \varnothing$.

□

Definition 9. *For any $a \in S$, any $X \in \mathbb{X}$, and any $p \in P_a$, let $Tr([X]_{\widehat{a}}, p)$ be true if $p \in \bigcap \mu_a([X]_{\widehat{a}})$.*

The next lemma confirms that $\mathcal{P}$ satisfies condition 3 of Definition 3.

Lemma 18. *For any $a \in S$, any $p \in P_a$, any $\sigma \in G$, and any $X \in \mathbb{X}$, if $p \in \bigcap \mu_a([X]_{\widehat{a}})$, then $\sigma(p) \in \bigcap \mu_{\sigma(a)}([X]_{\widehat{a}})$.*

Proof. It will be sufficient to show that $\bigcap \mu_a([X]_{\widehat{a}}) \subseteq \sigma^{-1}(\bigcap \mu_{\sigma(a)}([X]_{\widehat{a}}))$. To demonstrate the latter, we will prove that $\mu_a(Y) \sim_{\hat{a}} \sigma^{-1}(\mu_{\sigma(a)}(Y))$ for each $Y \in \mathbb{X}$. Indeed, by the definition of μ_a and μ_{σ_a}, we have $\mu_{\sigma(a)}^{-1}(\sigma(\mu_a(\hat{a}))) = \hat{a}$. Hence, $\mu_{\sigma(a)}^{-1} \circ \sigma \circ \mu_a \in G_{\hat{a}}$. Thus, $\mu_{\sigma(a)}^{-1}(\sigma(\mu_a(Y)) \sim_{\hat{a}} Y$, by Lemma 14. Therefore, $\mu_a(Y) \sim_{\hat{a}} \sigma^{-1}(\mu_{\sigma(a)}(Y))$. □

We have now shown that $\mathcal{P}$ is a protocol over signature Σ. The next lemma is a variation of the standard induction lemma in proofs of completeness.

Lemma 19. *For any $r \in R$, any formula $\psi \in \Phi(\Sigma)$, and any $X \in \bigcap_{a\in S} \mu_a(r(a))$,*

$$r \Vdash \psi \qquad \textit{if and only if} \qquad \psi \in X.$$

Proof. Induction on structural complexity of formula ψ. If $\psi \equiv \bot$, then the required follows from Definition 4 and consistency of the set X.

Assume that $\psi \equiv p \in P_{a_0}$. ($\Rightarrow$) : If $r \Vdash p$, then, by Definition 4, $Tr(r(a_0), p)$. Hence, by Definition 9, $p \in \bigcap \mu_{a_0}(r(a_0))$. Recall that $X \in \bigcap_{a\in S} \mu_a(r(a))$. Thus, $X \in \mu_{a_0}(r(a_0))$. Therefore, $p \in X$. ($\Leftarrow$) : If $p \in X$, then $\Box_{a_0} p \in X$ due to maximality of X and the Self-Awareness axiom. Thus, by Definition 6, $\Box_{a_0} p \in Y$ for each Y such that $X \sim_{a_0} Y$. Hence, due to maximality of Y and the Reflexivity axiom, $p \in Y$ for each Y such that $X \sim_{a_0} Y$. Then, $p \in \bigcap \mu_{a_0}(r(a_0))$ because $X \in \mu_{a_0}(r(a_0))$. Hence, by Definition 9, $Tr(r(a_0), p)$. Therefore, by Definition 4, $r \Vdash p$.

Let $\psi \equiv \Box_{a_0}\omega$.

($\Rightarrow$) : Suppose that $\Box_{a_0}\omega \notin X$. Thus, by Lemma 11, there is $Y \sim_{a_0} X$ such that $\omega \notin Y$. Let $r'(a) = [\mu_a^{-1}(Y)]_{\widehat{a}}$ for each $a \in S$. We will show $r' \in R$ using Definition 8. Indeed,

$$\bigcap_{a\in S} \mu_a(r'(a)) = \bigcap_{a\in S} \mu_a([\mu_a^{-1}(Y)]_{\widehat{a}}) = \bigcap_{a\in S} [Y]_a \ni Y.$$

We will now show that $r'(a_0) = r(a_0)$. Indeed, $X \in \bigcap_{a\in S} \mu_a(r(a))$ by the assumption of the lemma. Hence, $X \in \mu_{a_0}(r(a_0))$. Thus, $\mu_{a_0}^{-1}(X) \in \mu_{a_0}^{-1}(\mu_{a_0}(r(a_0)))$. In other words, $\mu_{a_0}^{-1}(X) \in r(a_0)$. Recall now that $X \sim_{a_0} Y$. Hence, by Lemma 13, $\mu_{a_0}^{-1}(X) \sim_{\widehat{a_0}} \mu_{a_0}^{-1}(Y)$. Thus, $\mu_{a_0}^{-1}(Y) \in r(a_0)$. Therefore, $r'(a_0) = [\mu_{a_0}^{-1}(Y)]_{\widehat{a_0}} = r(a_0)$.

Finally, recall that $\omega \notin Y$. Thus, by the Induction Hypothesis, $r' \nVdash \omega$. Therefore, by Definition 4, $r \nVdash \Box_{a_0}\omega$.

($\Leftarrow$) : Suppose that $\Box_{a_0}\omega \in X$. Consider any $r' \in R$ such that $r'(a_0) = r(a_0)$. It will be sufficient to show that $r' \Vdash \omega$. Indeed, by Definition 8, there is $X' \in \bigcap_{a\in S} \mu_a(r'(a))$. In particular, $X' \in \mu_{a_0}(r'(a_0))$. Thus, $X' \in \mu_{a_0}(r(a_0))$. Recall that $X \in \bigcap_{a\in S} \mu_a(r(a))$. Hence, $X \in \mu_{a_0}(r(a_0))$. Thus, both X' and X belong to the same equivalence class $\mu_{a_0}(r(a_0))$. Then, $X \sim_{a_0} X'$. Thus, $\Box_{a_0}\omega \in X'$ by the assumption $\Box_{a_0}\omega \in X$ and Definition 6. Hence, $\omega \in X'$, by the Reflexivity axiom and the maximality of the set X'. Therefore, by the Induction Hypothesis, $r' \Vdash \omega$.

The case $\psi \equiv \psi_1 \to \psi_2$ follows from Definition 4 and maximality and consistency of the set X in the standard way. □

To finish the proof of the completeness theorem, consider $r_0(a) = [\mu_a^{-1}(X_0)]_{\widehat{a}}$ as a function of argument a. We will show that $r_0 \in R$. Indeed, $r_0(a) \in V(a)$ because $[X_0]_a \in \mathbb{X}_a$ and $[\mu_a^{-1}(X_0)]_{\widehat{a}} \in \mathbb{X}_{\widehat{a}} = V(a)$. In addition, $\bigcap_{a\in S} \mu_a(r_0(a)) \neq \varnothing$ because

$$\bigcap_{a\in S} \mu_a(r_0(a)) = \bigcap_{a\in S} \mu_a([\mu_a^{-1}(X_0)]_{\widehat{a}}) = \bigcap_{a\in S} [X_0]_a \ni X_0. \tag{9}$$

We now finish the proof of the completeness theorem by showing that $r_0 \nVdash \varphi$. Indeed, recall that $\neg\varphi \in X_0$. By Lemma 19 and due to Statement (9), $r_0 \Vdash \neg\varphi$. Therefore, by Definition 4, $r_0 \nVdash \varphi$. □

8 Conclusion

In this paper we introduced a modal logical system for reasoning about knowledge in symmetric protocols and proved soundness and completeness of this system.

The modal language described in this paper can be generalized to distributed knowledge [7] modality $\Box_A$, where A is a subset of S. Informally, statement $r \Vdash \Box_A \varphi$ means that any agent who knows all values in set A on run r will be able to conclude φ. Formally, the last part of Definition 4 can be changed to

4. $r \Vdash \Box_A \psi$ if $r' \Vdash \psi$ for all $r' \in R$ such that $r'(a) = r(a)$ for each $a \in A$.

Axioms of our logical system can be trivially re-written to handle distributed knowledge. For example, the Stability axiom generalizes to $\Box_A \sigma(\varphi) \rightarrow \Box_A \varphi$, where $\sigma \in \cap_{a \in A} G_a$. However, to be natural, such generalization will have to allow atomic propositions to express properties of values of any subset of S. For example, proposition $p_{\{a,b\}}$ could state that $a = b$. The proof of completeness presented in this paper does not work in this new setting because it is not clear how $\hat{A}$ should be defined so that it can be used in the generalized Definition 9. Complete axiomatization of epistemic logic of distributed knowledge for symmetric protocols remains an open problem.

References

1. Kane, J., Naumov, P.: Epistemic logic for communication chains. In: 14th conference on Theoretical Aspects of Rationality and Knowledge (TARK '13), January 2013, Chennai, India. (2013) 131–137
2. Hintikka, J.: Knowledge and Belief - An Introduction to the Logic of the Two Notions. Contemporary philosophy. Cornell University Press, Ithaca, NY (1962)
3. Murtagh, F.: Symmetry in data mining and analysis: A unifying view based on hierarchy. Proceedings of the Steklov Institute of Mathematics **265** (2009) 177–198
4. Miller, A., Donaldson, A.F., Calder, M.: Symmetry in temporal logic model checking. ACM Comput. Surv. **38**(3) (2006)
5. Kane, J., Naumov, P.: Symmetry in information flow. Annals of Pure and Applied Logic (to appear).
6. Armstrong, W.W.: Dependency structures of data base relationships. In: Information processing 74 (Proc. IFIP Congress, Stockholm, 1974). North-Holland, Amsterdam (1974) 580–583
7. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning about knowledge. MIT Press, Cambridge, MA (1995)