Common Knowledge in a Logic of Gossips

Krzysztof R. Apt
Centrum Wiskunde & Informatica
Amsterdam, The Netherlands
University of Warsaw
Warsaw, Poland
k.r.apt@cwi.nl

Dominik Wojtczak
University of Liverpool
Liverpool, UK
d.wojtczak@liv.ac.uk

Gossip protocols aim at arriving, by means of point-to-point or group communications, at a situation in which all the agents know each other secrets. Recently a number of authors studied distributed epistemic gossip protocols. These protocols use as guards formulas from a simple epistemic logic, which makes their analysis and verification substantially easier.

We study here common knowledge in the context of such a logic. First, we analyze when it can be reduced to iterated knowledge. Then we show that the semantics and truth for formulas without nested common knowledge operator are decidable. This implies that implementability, partial correctness and termination of distributed epistemic gossip protocols that use non-nested common knowledge operator is decidable, as well. Given that common knowledge is equivalent to an infinite conjunction of nested knowledge, these results are non-trivial generalizations of the corresponding decidability results for the original epistemic logic, established in [2].

1 Introduction

Common knowledge is a fundamental notion in epistemic reasoning. It has its origins in the book of the philosopher David Lewis, [19], and the article of the sociologist Morris Friedell, [15]. By now this concept was applied in many other fields, including artificial intelligence, psychology, computer science, game theory, and logic. An early work on this subject in computer science and logic is discussed in [14]. For more recent accounts and surveys see e.g., [11] and [20].

Study and use of various logics equipped with the common knowledge operator is a rich field. As example of recent publications let us just mention [7], where an update logic augmented with common knowledge is investigated, and [21], where the correctness of epistemic protocols that rely on common knowledge is studied.

The purpose of this article is to investigate common knowledge in the context of a simple epistemic logic proposed in [1] to express and analyze distributed epistemic gossip protocols. Gossip protocols aim at arriving, by means of point-to-point or group communications, at a situation in which all the agents know each other secrets, see, e.g., the early survey [16] or the book coverage [18]. Distributed epistemic gossip protocols were introduced in [6], and further studied in [5, 17, 1, 12, 9, 10, 8], where in particular various distributed gossiping protocols, their types, epistemic aspects and objectives, and their interpretation as planning problems were analyzed. Such protocols are strikingly simple in their syntax based on epistemic logic (though not semantics), which makes it easier to reason about them.

In [2] we showed that the distributed epistemic gossip protocols introduced in [1] are implementable and proved that the problems of partial correctness and termination of such protocols are decidable, as well. In [3] we built upon these results and showed that the implementability of a distributed epistemic gossip protocol is a $\mathrm{P}_{\|}^{\mathrm{NP}}$-complete problem, while the problems of its partial correctness and termina-

J. Lang (Ed.): TARK 2017
EPTCS 251, 2017, pp. 10–27, doi:10.4204/EPTCS.251.2

tion are in coNP$^{\mathrm{NP}}$. We also established in [4] that fair termination of the distributed epistemic gossip protocols is decidable, as well.

In this paper we extend the results of [2] to the language that includes the common knowledge operator. Given that common knowledge is equivalent to an infinite conjunction of nested knowledge, these results are non-trivial generalizations of the previous results.

The obtained results clarify when and how common knowledge can arise in the context of gossiping. We prove that three or more agents can have common knowledge only of true statements. This is not the case for two agents, even if they do not communicate. We also show that under some assumptions common knowledge of two agents coincides with the 4th fold iterated knowledge. The main open problem is whether in this context common knowledge can always be reduced to iterated knowledge.

2 Syntax

The purpose of this paper is to analyze common knowledge in the context of gossip protocols. To describe it we use a simple modal language introduced in [1], though we allow now the common knowledge operator instead of the agent related knowledge operator.

Throughout the paper we assume a fixed finite set A of at least three ***agents***. We assume that each agent holds exactly one ***secret*** and that there exists a bijection between the set of agents and the set of secrets. We denote by P the set of all secrets.

Assume a fixed ordering on the agents. Each ***call*** concerns two different agents, say a and b, and is written as ab or (a,b), where agent a precedes agent b in the assumed ordering.

Calls are denoted by c, d. Abusing notation we write $a \in \mathsf{c}$ to denote that agent a is one of the two agents involved in the call c (e.g., for $\mathsf{c} := ab$ we have $a \in \mathsf{c}$ and $b \in \mathsf{c}$).

We consider formulas in an epistemic language $\mathcal{L}^{ck}$ defined by the following grammar:

$$\phi ::= F_a p \mid \neg\phi \mid \phi \wedge \phi \mid C_G\phi,$$

where $p \in \mathsf{P}$ and $a \in \mathsf{A}$ and $G \subseteq \mathsf{A}$. Each secret is viewed a distinct constant. We denote the secret of agent a by A, the secret of agent b by B, where $a,b \in \mathsf{A}$ and $A,B \in \mathsf{P}$, and so on. When G is a singleton, say $G = \{a\}$, then we write C_G as K_a, which is the knowledge operator used and studied in the context of this logic in [1] and [2].

We read $F_a p$ as 'agent a is familiar with the secret p', $K_a\phi$ as 'agent a knows that formula ϕ is true', and $C_G\phi$ as 'the group of agents G commonly knows that formula ϕ is true'.

So $F_a p$ is an atomic formula, while $K_a\phi$ and $C_G\phi$ are compound formulas. In what follows we shall distinguish the following sublanguages of $\mathcal{L}^{ck}$:

- $\mathcal{L}_{pr}$, its propositional part, which consists of the formulas that do not use the C_G modalities,
- $\mathcal{L}_{wn}$, which consists of the formulas without the nested use of the C_G modalities.

3 Semantics

We now recall from [1] semantics of the epistemic formulas. To this end we recall first the concept of a gossip situation.

A ***gossip situation*** (in short a ***situation***) is a sequence $\mathsf{s} = (\mathsf{Q}_a)_{a\in\mathsf{A}}$, where $\mathsf{Q}_a \subseteq \mathsf{P}$ for each agent a. Intuitively, Q_a is the set of secrets a is familiar with in situation s. The ***initial gossip situation*** is the one

in which each Q_a equals $\{A\}$ and is denoted by root. We say that an agent a is an ***expert*** in a situation s if he is familiar in s with all the secrets.

Below sets of secrets will be written down as lists. E.g., the set $\{A,B,C\}$ will be written as ABC. Gossip situations will be written down as lists of lists of secrets separated by dots. E.g., if there are three agents, then the gossip situation $(\{A,B\},\{A,B\},\{C\})$ will be written as $AB.AB.C$.

Each call transforms the current gossip situation by modifying the set of secrets the agents involved in the call are familiar with. Consider a gossip situation $\mathsf{s} := (\mathsf{Q}_d)_{d\in\mathsf{A}}$. Then $ab(\mathsf{s}) := (\mathsf{Q}'_d)_{d\in\mathsf{A}}$, where $\mathsf{Q}'_a = \mathsf{Q}'_b = \mathsf{Q}_a \cup \mathsf{Q}_b$, $\mathsf{Q}'_c = \mathsf{Q}_c$, for $c \neq a,b$. This simply says that the only effect of a call is that the secrets are shared between the two agents involved in it.

In [1] computations of the gossip protocols were studied, so both finite and infinite call sequences were used. Here we focus on the finite call sequences as we are only interested in the semantics of epistemic formulas. So to be brief, unless explicitly stated, a ***call sequence*** is assumed to be finite.

The empty sequence is denoted by ε. We use c to denote a call sequence and C to denote the set of all finite call sequences. Given call sequences c and d and a call c we denote by $\mathsf{c.c}$ the outcome of adding c at the end of the sequence c and by $\mathsf{c.d}$ the outcome of appending the sequences c and d. We write $\mathsf{c} \sqsubseteq \mathsf{d}$ to denote the fact that d extends c, i.e., that for some c' we have $\mathsf{c.c}' = \mathsf{d}$.

The result of applying a call sequence to a situation s is defined inductively as follows:
$\varepsilon(\mathsf{s}) := \mathsf{s}$,
$(\mathsf{c.c})(\mathsf{s}) := \mathsf{c}(\mathsf{c}(\mathsf{s}))$.

A gossip situation is a set of possible combinations of secret distributions among the agents. As calls progress in sequence from the initial situation, agents may be uncertain about which one of such secrets distributions is the actual one. This uncertainty is captured by appropriate equivalence relations on the call sequences.

Definition 1 *A* **gossip model** *is a tuple $\mathcal{M} := (\mathsf{C}, \{\sim_a\}_{a\in\mathsf{A}})$, where each $\sim_a \subseteq \mathsf{C}\times\mathsf{C}$ is the smallest relation such that $\varepsilon \sim_a \varepsilon$ and the following conditions hold. Suppose $\mathsf{c} \sim_a \mathsf{d}$.*

(i) If $a \notin \mathsf{c}$, then $\mathsf{c.c} \sim_a \mathsf{d}$ and $\mathsf{c} \sim_a \mathsf{d.c}$.

(ii) If $a \in \mathsf{c}$ and $\mathsf{c}.c(\mathsf{root})_a = \mathsf{d}.c(\mathsf{root})_a$, then $\mathsf{c.c} \sim_a \mathsf{d.c}$.

A gossip model with a designated call sequence is called a **pointed gossip model**.

So for each set of agents there is exactly one gossip model. To illustrate the definition of $\sim_a$ note for instance that by *(i)* we have $ab, bc \sim_a ab, bd$. But we do not have $bc, ab \sim_a bd, ab$ since $(bc, ab)(\mathsf{root})_a = ABC \neq ABD = (bd, ab)(\mathsf{root})_a$.

To define semantics of the C_G operator we use the relation $\sim_G \subseteq \mathsf{C}\times\mathsf{C}$ defined by

$$\sim_G = (\cup_{a\in G} \sim_a)^*,$$

where * stands for the transitive reflexive closure of a binary relation. As stated in [1], each $\sim_a$ is an equivalence relation. As a result each $\sim_G$ is an equivalence relation, as well.

Finally, we recall the definition of truth.

Definition 2 *Let $(\mathcal{M},\mathsf{c})$ be a pointed gossip model with $\mathcal{M} := (\mathsf{C}, (\sim_a)_{a\in\mathsf{A}})$ and $\mathsf{c} \in \mathsf{C}$. We define the satisfaction relation $\models$ inductively as follows. For convenience we also include the special case of K_a (i.e., $G_{\{a\}}$). The clauses for Boolean connectives are as usual and omitted.*

$$\begin{aligned}
(\mathcal{M},\mathsf{c}) &\models F_a p \quad \textit{iff} \quad p \in \mathsf{c}(\mathsf{root})_a,\\
(\mathcal{M},\mathsf{c}) &\models K_a \phi \quad \textit{iff} \quad \forall \mathsf{d}\ \textit{s.t.}\ \mathsf{c} \sim_a \mathsf{d},\ (\mathcal{M},\mathsf{d}) \models \phi,\\
(\mathcal{M},\mathsf{c}) &\models C_G \phi \quad \textit{iff} \quad \forall \mathsf{d}\ \textit{s.t.}\ \mathsf{c} \sim_G \mathsf{d},\ (\mathcal{M},\mathsf{d}) \models \phi.
\end{aligned}$$

Further

$$\mathcal{M} \models \phi \quad \textit{iff} \quad \forall \mathsf{c}\, (\mathcal{M}, \mathsf{c}) \models \phi.$$

When $\mathcal{M} \models \phi$ we say that ϕ **is true**. □

So a formula $F_a p$ is true whenever secret p belongs to the set of secrets agent a is familiar with in the situation generated by the designated call sequence c applied to the initial situation root. The knowledge operator K_a is interpreted as customary in epistemic logic, using the equivalence relations $\sim_a$, and the C_G operator is defined as in [14].

While $\mathcal{L}^{ck}$ is a pretty standard epistemic language, its semantics is not. Indeed, it describes the truth of formulas after a sequence of calls took place, by analyzing the statements of the form $(\mathcal{M}, \mathsf{c}) \models \phi$. So we actually study here a limited version of a dynamic epistemic logic. To put it differently, we actually consider statements of the form $[\mathsf{c}]\phi$, where $[\ldots]$ is the standard dynamic logic operator, see, e.g., [13]. This explains why the study of the logic $\mathcal{L}^{ck}$ cannot be reduced to a study of a routine epistemic logic.

4 An alternative equivalence relation

To reason about the $\sim_a$ and $\sim_G$ relations it is easier to use an alternative equivalence relation between the call sequences that was introduced in [2]. It is based on a concept of a ***view*** of agent a of a call sequence c, written as c_a, and defined by induction as follows.

[Base]

$$\varepsilon_a := \mathsf{root},$$

[Step]

$$(\mathsf{c}.\mathsf{c})_a := \begin{cases} \mathsf{c}_a \xrightarrow{\mathsf{c}} \mathsf{s} & \text{if } a \in \mathsf{c} \\ \mathsf{c}_a & \text{otherwise,} \end{cases}$$

where the gossip situation s is defined by putting for $d \in \mathsf{A}$

$$\mathsf{s}_d := \begin{cases} \mathsf{c}.\mathsf{c}(\mathsf{root})_d & \text{if } d \in \mathsf{c} \\ \mathsf{s}'_d & \text{otherwise,} \end{cases}$$

where s' is the last gossip situation in c_a.

Intuitively, a view of agent a of a call sequence c is the information he acquires by means of the calls in c he is involved in. It consists of a sequence of gossip situations connected by the calls in which a is involved in. After each such call, say ab, agent a updates the set of gossips he and b are currently familiar with.

Example 3 Let $\mathsf{A} = \{a, b, c\}$ and consider the call sequence (ac, bc, ac). It generates the following successive gossip situations starting from root:

$$A.B.C \xrightarrow{ac} AC.B.AC \xrightarrow{bc} AC.ABC.ABC \xrightarrow{ac} ABC.ABC.ABC.$$

We now compare it with the view of agent a of the sequence (ac, bc, ac), which is

$$A.B.C \xrightarrow{ac} AC.B.AC \xrightarrow{ac} ABC.B.ABC.$$

Thus, in the final gossip situation of this view, agent b is familiar with neither the secret A nor C. □

We now introduce for each agent a an equivalence relation $\equiv_a$ between the call sequences, defined as follows:

$$\mathsf{c} \equiv_a \mathsf{d} \text{ iff } \mathsf{c}_a = \mathsf{d}_a.$$

So according to this definition two call sequences are equivalent for agent a if his views of them are the same. Below we shall rely on the following result from [2].

Theorem 4 (Equivalence) *For each agent a the relations $\sim_a$ and $\equiv_a$ coincide.*

5 Semantic matters

5.1 General considerations

We shall need below an alternative definition of truth of the $C_G\phi$ formulas. Given a sequence $a_1,\ldots,a_k$ of elements of G we abbreviate $K_{a_1}\ldots K_{a_k}\phi$ to $K_{a_1\ldots a_k}\phi$. We also denote the set of finite sequences of elements of G by G^*.

Note 5 ([14]) *For all call sequences c and formulas $C_G\phi \in \mathcal{L}^{ck}$*

$$(\mathcal{M},\mathsf{c}) \models C_G\phi \textit{ iff for all } t \in G^* \ (\mathcal{M},\mathsf{c}) \models K_t\phi.$$

In other words, the formula $C_G\phi$ is equivalent to the infinite conjunction $\bigwedge_{t\in G^*} K_t\phi$. We shall also need the following generalization of the corresponding result from [2] to the logic here studied.

Theorem 6 (Monotonicity) *Suppose that $\phi \in \mathcal{L}^{ck}$ is a formula that does not contain the $\neg$ symbol. Then*

$$\mathsf{c} \sqsubseteq \mathsf{d} \textit{ and } (\mathcal{M},\mathsf{c}) \models \phi \textit{ implies } (\mathcal{M},\mathsf{d}) \models \phi.$$

Proof. By Note 5 and Monotonicity Theorem 4 of [2]. □

Let us focus now on the case of ≥ 3 agents. The following result holds.

Theorem 7 *Suppose that $|G| \geq 3$. Then for all call sequences c and formulas $\phi \in \mathcal{L}^{ck}$*

$$(\mathcal{M},\mathsf{c}) \models C_G\phi \textit{ iff } \mathcal{M} \models \phi.$$

Proof. First we prove that for all c and d

$$\mathsf{c} \sim_G \mathsf{d}. \tag{1}$$

By the transitivity of $\sim_G$ it suffices to prove that $\mathsf{c} \sim_G \varepsilon$. We prove it by induction on the length of c. By definition $\varepsilon \sim_G \varepsilon$. Suppose that for some c we have $\mathsf{c} \sim_G \varepsilon$ and consider a call c. Take $a \in G$ such that $a \notin \mathsf{c}$ (it exists since $|G| \geq 3$). Then $\mathsf{c}.\mathsf{c} \sim_a \mathsf{c}$, so $\mathsf{c}.\mathsf{c} \sim_G \varepsilon$.

By (1) we have $(\mathcal{M},\mathsf{c}) \models C_G\phi$ iff $\forall \mathsf{d}\,(\mathcal{M},\mathsf{d}) \models \phi$, which concludes the proof. □

Theorem 7 states that the formulas commonly known by the agents in a group of at least three agents are precisely the true formulas. An example of such a statement is that each agent is familiar with his secret, i.e., $\bigwedge_{a\in \mathsf{A}} F_aA$. In contrast, a statement that an agent is familiar with the secret of another agent, i.e. F_aB, where $a \neq b$, is not always true, so for all call sequences c we have $(\mathcal{M},\mathsf{c}) \not\models C_GF_aB$, when $|G| \geq 3$.

5.2 The case of two agents

The situation changes when the group consists of two agents. In what follows we abbreviate $C_{\{a,b\}}$ to C_{ab}.

Example 8
(i) Consider the formula

$$\phi := \neg F_a B \vee \bigvee_{c \in \mathsf{A} \setminus \{a,b\}} F_c B.$$

It states that if a is familiar with the secret of b, then also another agent different from a and b is familiar with this secret. Note that $(\mathcal{M}, ab) \models \neg\phi$, i.e., ϕ is not always true. We claim that $(\mathcal{M}, \varepsilon) \models C_{ab}\phi$.

First note that if $\mathsf{c} \sim_a \mathsf{d}$ or $\mathsf{c} \sim_b \mathsf{d}$ and the call ab does not appear in c, then it does not appear in d either. Consequently, if $\mathsf{c} \sim_{\{a,b\}} \varepsilon$, then the call ab does not appear in c.

Conversely, take a call sequence c such that the call ab does not appear in it. We prove by induction on the length of c that $\mathsf{c} \sim_{\{a,b\}} \varepsilon$. By definition $\varepsilon \sim_{\{a,b\}} \varepsilon$. Suppose that for some c we have $\mathsf{c} \sim_{\{a,b\}} \varepsilon$ and consider a call c. Either $a \notin \mathsf{c}$ or $b \notin \mathsf{c}$, so either $\mathsf{c}.\mathsf{c} \sim_a \mathsf{c}$ or $\mathsf{c}.\mathsf{c} \sim_b \mathsf{c}$. Consequently $\mathsf{c}.\mathsf{c} \sim_{\{a,b\}} \varepsilon$.

We conclude that $\mathsf{c} \sim_{\{a,b\}} \varepsilon$ iff the call ab does not appear in c. But for any such c we have $(\mathcal{M}, \mathsf{c}) \models \phi$. This proves that $(\mathcal{M}, \varepsilon) \models C_{ab}\phi$.

This shows that even without any call two agents can commonly know a formula that is not always true.

(ii) We also have $(\mathcal{M}, ab) \models C_{ab}(F_a B \wedge F_b A)$, i.e., two agents can commonly know some non-trivial information about themselves.

Indeed, if the call ab appears in c, then $(\mathcal{M}, \mathsf{c}) \models F_a B \wedge F_b A$ and that if the call ab appears in c and $\mathsf{c} \sim_a \mathsf{d}$ or $\mathsf{c} \sim_b \mathsf{d}$, then it also appears in d. □

On the other hand for two agents the following partial analogue of Theorem 7 holds.

Theorem 9 *For all call sequences* c *that do not contain the call ab and all formulas* $\phi \in \mathcal{L}^{ck}$ *that do not contain the* $\neg$ *symbol*

$$(\mathcal{M}, \mathsf{c}) \models C_{ab}\phi \text{ iff } \mathcal{M} \models \phi.$$

Proof. Suppose $(\mathcal{M}, \mathsf{c}) \models C_{ab}\phi$. As noticed in Example 8(i) $\mathsf{c} \sim_{\{a,b\}} \varepsilon$, so $(\mathcal{M}, \varepsilon) \models \phi$. By the Monotonicity Theorem 6 for all call sequences d we have $(\mathcal{M}, \mathsf{d}) \models \phi$. So $\models \phi$. Further, $\models \phi$ implies $(\mathcal{M}, \mathsf{c}) \models C_{ab}\phi$ for arbitrary call sequences c and formulas $C_{ab}\phi$. □

Example 8(ii) shows that the restriction that the call ab does not appear in c cannot be dropped and Example 8(i) shows that the claim does not hold for formulas that do contain the $\neg$ symbol.

Next, we show that for formulas that do not contain the $\neg$ symbol common knowledge for the group of two agents coincides with the 4th fold iterated knowledge.

Consider an agent a and a call sequence c. We say that a call is ***a-irrelevant*** in c if its removal does not affect the view (in the sense of Section 4) of agent a of the call sequence. Starting from c we repeatedly remove from the current call sequence the first not yet analyzed call if it is a-irrelevant and otherwise we keep it. We call the outcome of such an iteration the ***a-simplification*** of c.

Example 10 Suppose,

$$\mathsf{c} = bf.cd.bc.ce.df.ef.bh.\underline{af}.bg.\underline{ag}.\underline{ah},$$

where for the visibility we underlined the a-calls. Then the a-simplification of c results in the deletion of the calls bf and cd and equals

$$bc.ce.df.ef.bh.\underline{af}.bg.\underline{ag}.\underline{ah}.$$

The views of agent a of both call sequences are as follows.

$A.B.C.D.E.F.D.H \xrightarrow{af}$
$ABCDEF.B.C.D.E.ABCDEF.G.H \xrightarrow{ag}$
$ABCDEFGH.B.C.D.E.ABCDEF.ABCDEFGH.H \xrightarrow{ah}$
$ABCDEFGH.B.C.D.E.ABCDEF.ABCDEFGH.ABCDEFGH$

□

Below we say that two calls are ***linked*** if exactly one agent participates in both of them. Consider now a call sequence c with no a-irrelevant calls that does not contain the call ab. We focus on the b-calls in c. By the assumption about c for each b-call c in c there is a sequence of calls $\mathsf{c}_1, \ldots, \mathsf{c}_k$ in c such that

- $\mathsf{c} = \mathsf{c}_1$,
- $b \in \mathsf{c}_1$,
- for $i \in \{1, \ldots, k-1\}$ $a \notin \mathsf{c}_i$,
- for $i \in \{1, \ldots, k-1\}$ the calls c_i and c_{i+1} are linked.
- $a \in \mathsf{c}_k$.

We say then that c_1 ***leads to*** c_k. Further, we call each b-call in c that leads to the earliest possible a-call in c ***b-essential for*** a and call each other b-call in c ***b-inessential for*** a. Intuitively, agent a learns the secret of b only through the b-essential calls. In contrast, he can learn other secrets both through the b-essential and the b-inessential calls.

Example 11 Consider the call sequence

$$bc.ce.df.ef.bh.\underline{af}.bg.\underline{ag}.\underline{ah}$$

from Example 10. The only b-essential call for a is bc as it leads to af. In turn, in the call sequence $bh.ce.df.ef.\underline{af}.bg.bc.\underline{ag}$ the b-essential calls for a are bh and bg as both of them lead to ag and no b-call leads to the earlier a-call af. □

Consider now the first b-call in c, call it bc, that is b-inessential for a and suppose that ad is the first a-call in c to which bc leads to, where c and d may coincide. If $c = d$, then we delete bc from c and otherwise we replace bc by cd. Intuitively, we 'reroute' the information collected by agent b in the b-inessential calls leading to ad using agent d. This does not affect agent's a view of the call sequence since he does not learn the secret of b through the b-inessential calls.

We repeat this operation, starting with c, for all b-calls that are b-inessential for a and denote the resulting call sequence by $R_{ab}(\mathsf{c})$.

Example 12 Consider the call sequence

$$bc.ce.df.ef.bh.\underline{af}.bg.\underline{ag}.\underline{ah}$$

from Example 10. The b-inessential calls are bh and bg and both lead to ag. So

$$R_{ab}(bc.ce.df.ef.bh.\underline{af}.bg.\underline{ag}.\underline{ah}) = bc.ce.df.ef.gh.\underline{af}.\underline{ag}.\underline{ah}.$$

□

The following lemma establishes the relevant property of $R_{ab}(\mathsf{c})$.

Lemma 13 *Consider a call sequence* c *with no a-irrelevant calls that does not contain the call ab. Then* $\mathsf{c} \equiv_a R_{ab}(\mathsf{c})$.

Proof. Since c does not contain the call ab, the views of a of c and $R_{ab}(\mathsf{c})$ have the same sequences of the a-calls.

By definition agent a does not learn the secret of b through the b-inessential calls for a. So the replacement (or possibly deletion) of b in all b-inessential calls has no effect on the status of this secret in the views of a of both sequences.

Let bc be the first b-inessential for a call in c and suppose that ad is the first a-call in c it leads to. Let c' be the outcome of the first step of producing $R_{ab}(\mathsf{c})$. So it is obtained from c by replacing bc by cd if $c \neq d$, and by deleting bc otherwise. We show that the views of the agent a of the call sequences c and c' are the same. First, note that no a-call earlier than ad can be effected by the change in c, because ad is the first a-call bc leads to.

Consider the $c \neq d$ case first. The set of secrets an agent is familiar with at the same point in c and c' may differ as a result of bc being replaced by cd. However, we argue that it is impossible for the agent a to notice this difference. Let us consider a call ax in c, where $x \in \mathsf{A}$ and the sets of secrets, S and S', agent e is familiar before ax is made in c and c', respectively.

- If ax takes place before bc then S and S' are the same.
- If ax is in-between the calls bc and ad then again the sets S and S' are the same, because ad is the first a-call that bc leads to.
- If ax is the call ad then we have the following. First, just before this call a is already familiar with all the secrets b is familiar with before the call bc is made in c, because ad is the first a-call bc leads to. So a is still familiar with all these secrets in c'. Thus the only secrets that may be lost by replacing bc by cd are the ones that c is familiar with at that point. However, these secrets are passed to d and a still learns them all in c' through the call ad.
- If ax takes place after the call ad then the difference between S and S' could be at most in the set of secrets a learned through the call bc. However, a already knows these secrets after the call ad is made, so $S = S'$.[1]

The reasoning for the $c = d$ case is completely analogous and omitted.

By iterating the above argument, starting with c, we obtain $R_{ab}(\mathsf{c})$ without affecting the view of the agent a. □

The following consequence of the above lemma is crucial. Here $\equiv_{abab}$ stands for the the composition of the relations $\equiv_a$, $\equiv_b$, $\equiv_a$ and $\equiv_b$, i.e.,

$$\equiv_{abab} = \equiv_a \circ \equiv_b \circ \equiv_a \circ \equiv_b,$$

where $\circ$ is the composition of two binary relations.

Theorem 14 *Consider a call sequence* c *that does not contain the call ab. Then*

$$\mathsf{c} \equiv_{abab} \varepsilon.$$

[1] Note that this crucially depends on the fact that from any call each involved agent learns the union of the sets of secrets the callers are familiar with and not the set of secrets the other caller is familiar with.

Proof. Let c_1 be the a-simplification of c and $\mathsf{c}_2 = R_{ab}(\mathsf{c}_1)$. Then $\mathsf{c} \equiv_a \mathsf{c}_1$ and by Lemma 13 $\mathsf{c}_1 \equiv_a \mathsf{c}_2$, so $\mathsf{c} \equiv_a \mathsf{c}_2$.

If there are no b-calls in c_2, then $\mathsf{c}_2 \equiv_b \varepsilon$, so $\mathsf{c} \equiv_{ab} \varepsilon$, from which the conclusion follows since $\varepsilon \equiv_{ab} \varepsilon$. Otherwise let c_3 be the prefix of c_2 that ends with the last b-call. Then $\mathsf{c}_2 \equiv_b \mathsf{c}_3$.

All the b-calls in c_3 are b-essential for a in the call sequence c_2 and the a-call through which agent a learns in c_2 the secret of B is located after all these b-essential calls. It follows that $\mathsf{c}_3 \equiv_a \mathsf{c}_4$, where c_4 is the result of removing all b-calls from c_3, because no b-call in c_3 can possibly lead to an a-call in c_3.

Now, c_4 does not contain any b-calls, so $\mathsf{c}_4 \equiv_b \varepsilon$. This proves the claim. □

Example 15 The following example illustrates the call sequences generated in the above proof. Let

$$\mathsf{c} = \underline{ah}.cd.bc.bd.be.\underline{ad}.bf.bg.\underline{af}.$$

Then the a-simplification of c results in removing the calls cd and bg and equals

$$\mathsf{c}_1 = \underline{ah}.bc.bd.be.\underline{ad}.bf.\underline{af}.$$

Subsequently $R_{ab}(\mathsf{c}_1)$ equals

$$\mathsf{c}_2 = \underline{ah}.bc.bd.ef.\underline{ad}.\underline{af}.$$

Next, the prefix of c_2 that ends with the last b-call is

$$\mathsf{c}_3 = \underline{ah}.bc.bd.$$

Finally, the result of removing all b-calls from c_3 equals

$$\mathsf{c}_4 = \underline{ah}$$

and $\mathsf{c}_4 \equiv_b \varepsilon$. □

This brings us to the following conclusion.

Theorem 16 *For all call sequences* c *that do not contain the call ab and all formulas* $\phi \in \mathcal{L}^{ck}$ *that do not contain the* $\neg$ *symbol*

$$(\mathcal{M}, \mathsf{c}) \models K_{abab}\phi \text{ iff } \mathcal{M} \models \phi$$

and

$$(\mathcal{M}, \mathsf{c}) \models K_{baba}\phi \text{ iff } \mathcal{M} \models \phi.$$

Proof. By symmetry it suffices to prove the first equivalence. By Theorem 14 $(\mathcal{M}, \mathsf{c}) \models K_{abab}\phi$ implies $(\mathcal{M}, \varepsilon) \models \phi$, so by the Monotonicity Theorem 6 for all call sequences d we have $(\mathcal{M}, \mathsf{d}) \models \phi$, i.e., $\mathcal{M} \models \phi$.

Further, for arbitrary call sequences c and formulas $\phi \in \mathcal{L}^{ck}$, $\mathcal{M} \models \phi$ implies $(\mathcal{M}, \mathsf{c}) \models K_{abab}\phi$. □

Corollary 17 *For all call sequences* c *that do not contain the call ab and all formulas* $\phi \in \mathcal{L}^{ck}$ *that do not contain the* $\neg$ *symbol*

$$(\mathcal{M}, \mathsf{c}) \models C_{ab}\phi \text{ iff } (\mathcal{M}, \mathsf{c}) \models K_{abab}\phi.$$

Proof. By Theorems 16 and 9. □

This together with Note 5 shows that under the conditions of the above corollary the infinite conjunction $\bigwedge_{t \in G^*} K_t\phi$ is equivalent to the 4th fold iterated knowledge $K_{abab}\phi$. To conclude this analysis we now show that common knowledge for two agents is not equivalent to any shorter knowledge iteration.

Corollary 18 *Let* $\mathsf{c} = ac, bc, ac$. *Then* $(\mathcal{M}, \mathsf{c}) \models K_{aba} F_c A$, $(\mathcal{M}, \mathsf{c}) \models K_{ab} F_c A$ *and* $(\mathcal{M}, \mathsf{c}) \models K_a F_c A$. *Further,* $(\mathcal{M}, \mathsf{c}) \not\models C_{ab} F_c A$.

Proof. Take d such that $\mathsf{c} \sim_a \mathsf{d}$. Then d is of the form $\mathsf{c}_1, ac, \mathsf{c}_2, bc,\ \mathsf{c}_3, ac, \mathsf{c}_4$. Next take d_1 such that $\mathsf{d}_1 \sim_b \mathsf{d}$. Then d is of the form $\mathsf{c}_5, ac, \mathsf{c}_6, bc, \mathsf{c}_7$. Next take d_2 such that $\mathsf{d}_2 \sim_a \mathsf{d}_1$. Then d_2 is of the form $\mathsf{c}_8, ac, \mathsf{c}_9$. So $(\mathcal{M}, \mathsf{d}_2) \models F_c A$, which implies the claim.

The next two claims follow since for all formulas $\phi \in \mathcal{L}^{ck}$, $K_{aba}\phi$ implies both $K_{ab}\phi$ and $K_a\phi$.

Now note that for all sequences $t \in \{a, b\}^*$ that extend *abab* or *baba* and all formulas $\phi \in \mathcal{L}^{ck}$, $K_t\phi$ implies $K_{abab}\phi$ or $K_{baba}\phi$. So Theorem 16 implies that for all such sequences s and all call sequences c that do not contain the call *ab*

$$(\mathcal{M}, \mathsf{c}) \not\models K_s F_c A.$$

Indeed, the formula $F_c A$ is not always true.

Further, by Note 5 we also have for such call sequences c

$$(\mathcal{M}, \mathsf{c}) \not\models C_{ab} F_c A.$$

In particular, this holds for the above call sequence $\mathsf{c} = ac, bc, ac$. □

6 Decidability issues

6.1 Decidability of semantics

We begin with the decidability of the semantics. First we establish some properties of the semantics of common knowledge of two agents.

Consider a call *ab* and a call sequence c. Starting from c we repeatedly remove from the current call sequence a redundant call that differs from *ab*. We call each outcome of such an iteration an ***ab*-reduction** of c. Further, we say that a call sequence c is ***ab*-redundant free** if no call from c that differs from *ab* is redundant in it. Clearly each *ab*-reduction is *ab*-redundant free.

Corollary 19 *Let* d *be an ab-reduction of* c. *Then*

(i) $\mathsf{c} \sim_{\{a,b\}} \mathsf{d}$,

(ii) for all formulas $\phi \in \mathcal{L}_{pr}$, $(\mathcal{M}, \mathsf{c}) \models \phi$ *iff* $(\mathcal{M}, \mathsf{d}) \models \phi$.

Lemma 20 *For each call ab and a call sequence* c *the set of ab-redundant free call sequences* d *such that* $\mathsf{c} \sim_{\{a,b\}} \mathsf{d}$ *is finite.*

Proof. Consider an *ab*-redundant free call sequence d such that $\mathsf{c} \sim_{\{a,b\}} \mathsf{d}$. Then d has the same number, say k, of calls *ab* as c.

Associate with d the sequence of gossip situations

$$\mathsf{d}^0(\mathsf{root}), \mathsf{d}^1(\mathsf{root}), \ldots, \mathsf{d}^m(\mathsf{root}),$$

where m is the length of d, $\mathsf{d}^0 = \varepsilon$, and $\mathsf{d}^k = \mathsf{d}_1, \mathsf{d}_2, \ldots, \mathsf{d}_k$ for $k = 1, \ldots, m$. This sequence monotonically grows, where we interpret the inclusion relation componentwise. Moreover, for all calls d_i different from *ab* the corresponding inclusion is strict. Consequently, m, the length of d, is bounded by $k + |\mathsf{A}|^{|\mathsf{A}|}$, the sum of the number of calls *ab* in c and of the total number of secrets in the gossip situation in which each agent is an expert.

But for each m there are only finitely many call sequences of length at most m. This concludes the proof. □

We can now prove the desired result.

Theorem 21 (Decidability of Semantics) *For each call sequence* c *it is decidable whether for a formula* $\phi \in \mathcal{L}_{wn}$, $(\mathcal{M},\mathsf{c}) \models \phi$ *holds.*

Proof. We use the definition of semantics as the algorithm. We only need to consider the case of the formulas of the form $C_G\phi$, where $\phi \in \mathcal{L}_{pr}$.

If $|G| = 1$, then this is the contents of the Decidability of Semantics Theorem 5 of [2].

If $|G| = 2$, say $A = \{a,b\}$, then according to Corollary 19 we can rewrite the semantics of $C_G\phi$ as follows:

$$(\mathcal{M},\mathsf{c}) \models C_G\phi \quad \text{iff} \quad \forall \mathsf{d} \text{ s.t. } \mathsf{c} \sim_G \mathsf{d} \text{ and } \mathsf{d} \text{ is } ab\text{-redundant free, } (\mathcal{M},\mathsf{d}) \models \phi,$$

and according to Lemma 20 this definition refers to a finite set of call sequences d.

If $|G| \geq 3$, then the decidability follows from Theorem 7 and the Decidability of Truth Theorem 6 established in [2]. □

This result implies that the gossip protocols that use guards with non-nested common knowledge operator are implementable.

6.2 Decidability of truth

Next, we show that truth definition for the formulas of the language $\mathcal{L}_{wn}$ is decidable. Since partial correctness of gossip protocols with common knowledge operator can be expressed as a formula of $\mathcal{L}_{wn}$, this implies that the problem of determining partial correctness of such protocols is decidable.

The key notion is that of an ***epistemic pair-view***. It is a function of a call sequence c, denoted by $\mathsf{EPV}(\mathsf{c})$, defined by

- putting for any pair of agents a,b:
  $\mathsf{EPV}(\mathsf{c})(a,b) = \{\mathsf{d}(\mathsf{root}) \mid \mathsf{c} \sim_{\{a,b\}} \mathsf{d}\}$, and setting
- $\mathsf{EPV}(\mathsf{c})(*) = \mathsf{c}(\mathsf{root})$.

So $\mathsf{EPV}(\mathsf{c})(a,b)$ is the set of all gossip situations obtained by means of call sequences that are $\sim_{\{a,b\}}$-equivalent to c. Further, as $\sim_{\{a,a\}} = \sim_a$, $\mathsf{EPV}(\mathsf{c})(a,a)$ is the set of all gossip situations consistent with agent a's observations made throughout c. Finally, $\mathsf{EPV}(\mathsf{c})(*)$ is the actual gossip situation after c takes place. Note that for any $a,b \in \mathsf{A}$, if $\mathsf{c} \sim_{\{a,b\}} \mathsf{d}$ then $\mathsf{EPV}(\mathsf{c})(b,a) = \mathsf{EPV}(\mathsf{c})(a,b) = \mathsf{EPV}(\mathsf{d})(a,b) = \mathsf{EPV}(\mathsf{d})(b,a)$.

The following holds.

Lemma 22 *For each call sequence* c *and agents* a,b*, the set* $\mathsf{EPV}(\mathsf{c})(a,b)$ *is finite and can be effectively constructed.*

Proof. For any $a \in \mathsf{A}$, $\mathsf{EPV}(\mathsf{c})(a,a)$ coincides with the epistemic view $\mathsf{EV}(\mathsf{c})(a)$, as defined in [2]. Hence, we can compute $\mathsf{EPV}(\mathsf{c})(a,a)$ as in Lemma 3 of [2].

Consider now a pair of agents a,b such that $a \neq b$. To construct the set $\mathsf{EPV}(\mathsf{c})(a,b)$ it suffices by Corollary 19 to consider the ab-redundant free call sequences d and by Lemma 20 there are only finitely many such call sequences d for which $\mathsf{d} \sim_{\{a,b\}} \mathsf{c}$. □

Our interest in epistemic pair-views stems from the following important observation.

Lemma 23 *Suppose that* $\mathsf{EPV}(\mathsf{c}) = \mathsf{EPV}(\mathsf{d})$*. Then for all formulas* $\phi \in \mathcal{L}_{wn}$, $(\mathcal{M},\mathsf{c}) \models \phi$ *iff* $(\mathcal{M},\mathsf{d}) \models \phi$.

Proof. A straightforward proof by induction shows that for a formula $\psi \in \mathcal{L}_{pr}$ and arbitrary call sequences c' and d',

$$\mathsf{c}'(\mathsf{root}) = \mathsf{d}'(\mathsf{root}) \text{ implies that } (\mathcal{M},\mathsf{c}') \models \psi \text{ iff } (\mathcal{M},\mathsf{d}') \models \psi. \tag{2}$$

Since $\mathsf{EPV}(\mathsf{c})(*) = \mathsf{c}(\mathsf{root})$ and $\mathsf{EPV}(\mathsf{d})(*) = \mathsf{d}(\mathsf{root})$, this settles the case for $\phi = F_a p$.

Next, consider the case of the formulas of the form $C_G\phi$, where $\phi \in \mathcal{L}_{wn}$.

If $|G| = 1$, then $G = \{a\}$ for some $a \in \mathsf{A}$ and C_G is the same as K_a. Since $\mathsf{EPV}(\mathsf{c}) = \mathsf{EPV}(\mathsf{d})$ implies $\mathsf{EV}(\mathsf{c}) = \mathsf{EV}(\mathsf{d})$, where the epistemic view $\mathsf{EV}()$ is defined as in [2], the claim follows by Lemma 4 of [2].

If $|G| = 2$, then $G = \{a,b\}$ for some $a,b \in \mathsf{A}$. By (2) and the definition of $\mathsf{EPV}(\mathsf{c})$

$$(\mathcal{M},\mathsf{c}) \models C_G\phi \quad \text{iff} \quad \forall \mathsf{c}' \text{ s.t. } \mathsf{c}'(\mathsf{root}) \in \mathsf{EPV}(\mathsf{c})(a,b),\ (\mathcal{M},\mathsf{c}') \models \phi.$$

So the claim follows since $\mathsf{EPV}(\mathsf{c})(a,b) = \mathsf{EPV}(\mathsf{d})(a,b)$.

If $|G| \geq 3$, then by Theorem 7 both $(\mathcal{M},\mathsf{c}') \models C_G\phi$ and $(\mathcal{M},\mathsf{d}') \models C_G\phi$ are equivalent to $\models \phi$.

This settles the case for $C_G\phi$. The remaining cases of negation and conjunction follow directly by the induction. □

The above lemma is useful because the epistemic pair-view of each call sequence is finite, in contrast to the set of call sequences. Next, we provide an inductive definition of $\mathsf{EPV}(\mathsf{c.c})(a,b)$ the importance of which will become clear in a moment.

Lemma 24 *For any call sequence* c *and call* $\mathsf{c} = ab$ *for agents* $a,b \in \mathsf{A}$

$$\mathsf{EPV}(\mathsf{c.c})(a,b) = \{\mathsf{c}(\mathsf{s}) \mid \mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b), \mathsf{c}(\mathsf{s})_a = \mathsf{c}(\mathsf{c}(\mathsf{root}))_a \textit{ and } \mathsf{c}(\mathsf{s})_b = \mathsf{c}(\mathsf{c}(\mathsf{root}))_b\}.$$

Proof.

($\subseteq$) Take $\mathsf{s}' \in \mathsf{EPV}(\mathsf{c.c})(a,b)$. By the definition of $\mathsf{EPV}(\mathsf{c.c})(a,b)$ there exists a call sequence d such that $\mathsf{d.c} \sim_{\{a,b\}} \mathsf{c.c}$ and $\mathsf{s}' = \mathsf{d.c}(\mathsf{root})$. So $\mathsf{s}' = \mathsf{c}(\mathsf{s})$, where $\mathsf{s} = \mathsf{d}(\mathsf{root})$. We prove now that $\mathsf{d} \sim_{\{a,b\}} \mathsf{c}$ and as a result $\mathsf{s} = \mathsf{d}(\mathsf{root}) \in \mathsf{EPV}(\mathsf{c})(a,b)$.

Note that $\mathsf{d.c} \sim_{\{a,b\}} \mathsf{c.c}$ implies that there exists a sequence $t_1 \dots t_k \in \{a,b\}^*$ such that for some call sequences $\mathsf{d}_1, \mathsf{d}_2, \dots, \mathsf{d}_{k-1}$ we have $\mathsf{d.c} \sim_{t_1} \mathsf{d}_1\mathsf{.c} \sim_{t_2} \mathsf{d}_2\mathsf{.c} \sim_{t_3} \dots \sim_{t_{k-1}} \mathsf{d}_{k-1}\mathsf{.c} \sim_{t_k} \mathsf{c.c}$. Note that for any $t \in \{a,b\}$ and call sequences c', d' we have that $\mathsf{c}'\mathsf{.c} \sim_t \mathsf{d}'\mathsf{.c}$ implies $\mathsf{c}' \sim_t \mathsf{d}'$, because $\sim_t$ is the minimal relation satisfying the conditions stated in Definition 1. It follows that $\mathsf{d} \sim_{t_1} \mathsf{d}_1 \sim_{t_2} \mathsf{d}_2 \sim_{t_3} \dots \sim_{t_{k-1}} \mathsf{d}_{k-1} \sim_{t_k} \mathsf{c}$, so by definition $\mathsf{d} \sim_{\{a,b\}} \mathsf{c}$.

Further, by the definition of the $\sim_c$ relations, we also have that for $i \in \{0,\dots,k-1\}$ both $\mathsf{d}_i\mathsf{.c}(\mathsf{root})_a = \mathsf{d}_{i+1}\mathsf{.c}(\mathsf{root})_a$ and $\mathsf{d}_i\mathsf{.c}(\mathsf{root})_b = \mathsf{d}_{i+1}\mathsf{.c}(\mathsf{root})_b$, where $\mathsf{d}_0 = \mathsf{d}$ and $\mathsf{d}_k = \mathsf{c}$. So $\mathsf{d.c}(\mathsf{root})_a = \mathsf{c.c}(\mathsf{root})_a$ and $\mathsf{d.c}(\mathsf{root})_b = \mathsf{c.c}(\mathsf{root})_b$.

But $\mathsf{s} = \mathsf{d}(\mathsf{root})$, so we get that $\mathsf{c}(\mathsf{s})_a = \mathsf{c}(\mathsf{c}(\mathsf{root}))_a$ and $\mathsf{c}(\mathsf{s})_b = \mathsf{c}(\mathsf{c}(\mathsf{root}))_b$.

($\supseteq$) Take $\mathsf{s}' \in \{\mathsf{c}(\mathsf{s}) \mid \mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b), \mathsf{c}(\mathsf{s})_a = \mathsf{c}(\mathsf{c}(\mathsf{root}))_a \text{ and } \mathsf{c}(\mathsf{s})_b = \mathsf{c}(\mathsf{c}(\mathsf{root}))_b\}$. So for some gossip situation s we have $\mathsf{s}' = \mathsf{c}(\mathsf{s})$, $\mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b)$, $\mathsf{c}(\mathsf{s})_a = \mathsf{c}(\mathsf{c}(\mathsf{root}))_a$, and $\mathsf{c}(\mathsf{s})_b = \mathsf{c}(\mathsf{c}(\mathsf{root}))_b$. The fact that $\mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b)$ implies that there exists a call sequence d such that $\mathsf{d} \sim_{\{a,b\}} \mathsf{c}$ and $\mathsf{s} = \mathsf{d}(\mathsf{root})$. Now, this and $\mathsf{c}(\mathsf{d}(\mathsf{root}))_a = \mathsf{c}(\mathsf{s})_a = \mathsf{c}(\mathsf{c}(\mathsf{root}))_a$ imply by definition that $\mathsf{d.c} \sim_a \mathsf{c.c}$, so a fortiori $\mathsf{d.c} \sim_{\{a,b\}} \mathsf{c.c}$. So $\mathsf{d.c}(\mathsf{root}) \in \mathsf{EPV}(\mathsf{c.c})(a,b)$. Consequently also $\mathsf{s}' \in \mathsf{EPV}(\mathsf{c.c})(a,b)$, because $\mathsf{s}' = \mathsf{c}(\mathsf{s}) = \mathsf{d.c}(\mathsf{root})$. □

This allows us to conclude that $\mathsf{EPV}(\mathsf{c.c})$ can be computed using $\mathsf{EPV}(\mathsf{c})$ and c only, i.e., without referring to c. More precisely, denote the set of epistemic pair-views by $\widetilde{EPV}$ and recall that C denotes the set of calls. Then the following holds.

Corollary 25 *There exists a function* $f : \widetilde{EPV} \times \mathsf{C} \to \widetilde{EPV}$ *such that for any call sequence* c*, call* c*, and pair of agents* $a,b \in \mathsf{A}$

$$\mathsf{EPV}(\mathsf{c.c})(a,b) = f(\mathsf{EPV}(\mathsf{c}),\mathsf{c}).$$

Proof. First note that $\mathsf{EPV}(\mathsf{c.c})(*) = \mathsf{c}(\mathsf{EPV}(\mathsf{c})(*))$.

Suppose now that $a \neq b$. If $\mathsf{c} = ab$, then by Lemma 24 $\mathsf{EPV}(\mathsf{c.c})(a,b)$ is a function of $\mathsf{EPV}(\mathsf{c})(a,b)$ and c. If $\mathsf{c} \neq ab$, say $a \notin \mathsf{c}$, then $\mathsf{c.c} \sim_a \mathsf{c}$ and hence $\mathsf{c.c} \sim_{\{a,b\}} \mathsf{c}$, which implies $\mathsf{EPV}(\mathsf{c.c})(a,b) = \mathsf{EPV}(\mathsf{c})(a,b)$.

Suppose next that $a = b$. By the definition of $\sim_a$ for all d we have $\mathsf{EPV}(\mathsf{d})(a,a) = \mathsf{EV}(\mathsf{d})(a)$, so by Corollary 2 of [2] $\mathsf{EPV}(\mathsf{c.c})(a,a)$ is a function of $\mathsf{EPV}(\mathsf{c})(a,a)$ and c. □

Consider a call sequence c. If for some prefix $\mathsf{c}_1.\mathsf{c}_2$ of c, we have $\mathsf{EPV}(\mathsf{c}_1) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2)$, then we say that the call subsequence c_2 is ***pair-epistemically redundant*** in c and that c is ***pair-epistemically redundant***.

We say that c is ***pair-epistemically non-redundant*** if it is not pair-epistemically redundant. Equivalently, a call sequence $\mathsf{c}_1.\mathsf{c}_2 \ldots.\mathsf{c}_k$ is pair-epistemically non-redundant if the set

$$\{\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2.\ldots.\mathsf{c}_i) \mid i \in \{1,\ldots,k\}\}$$

has k elements.

Lemma 26 (Pair-Epistemic Stuttering) *Suppose that* $\mathsf{c} := \mathsf{c}_1.\mathsf{c}_2.\mathsf{c}_3$ *and* $\mathsf{d} := \mathsf{c}_1.\mathsf{c}_3$*, where* c_2 *is pair-epistemically redundant in* c*. Then* $\mathsf{EPV}(\mathsf{c}) = \mathsf{EPV}(\mathsf{d})$.

Proof. Let $\mathsf{c}_3 = \mathsf{c}_1.\mathsf{c}_2.\ldots.\mathsf{c}_k$. First note that thanks to Corollary 2 of [2] we have $\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2.\mathsf{c}_1) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1)$, since $\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2.\mathsf{c}_1) = f(\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2),\mathsf{c}_1) = f(\mathsf{EPV}(\mathsf{c}_1),\mathsf{c}_1) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1)$ due to the pair-epistemic redundancy of c_2 in c. Repeating this argument for all $i \in \{1,\ldots,k\}$ we get that

$$\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2.\mathsf{c}_1.\mathsf{c}_2.\ldots.\mathsf{c}_i) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1.\mathsf{c}_2.\ldots.\mathsf{c}_i).$$

In particular $\mathsf{EPV}(\mathsf{c}) = \mathsf{EPV}(\mathsf{d})$. □

Corollary 27 *For every call sequence* c *there exists a pair-epistemically non-redundant call sequence* d *such that for all formulas* $\phi \in \mathcal{L}_{wn}$*,* $(\mathcal{M},\mathsf{c}) \models \phi$ *iff* $(\mathcal{M},\mathsf{d}) \models \phi$.

Proof. By the repeated use of the Pair-Epistemic Stuttering Lemma 26 and Lemma 23. □

Next, we prove the following crucial lemma.

Lemma 28 *For any given model* $\mathcal{M}$*, there are only finitely many pair-epistemically non-redundant call sequences.*

Proof. Note that each epistemic pair-view is a function from $\mathsf{A} \times \mathsf{A} \cup \{*\}$ to the set of functions from A to $2^{|\mathsf{P}|}$ (this is an overestimation because for $*$ this set has only one element). There are $k = 2^{(|\mathsf{A}|^2+1)\cdot 2^{|\mathsf{A}|\cdot|\mathsf{P}|}}$ such functions, so any call sequence longer than k has a pair-epistemically redundant call subsequence. But there are only finitely many call sequences of length at most k. This concludes the proof. □

Finally, we can establish the announced result.

Theorem 29 (Decidability of Truth) *For any formula* $\phi \in \mathcal{L}_{wn}$*, it is decidable whether* $\mathcal{M} \models \phi$ *holds.*

Proof. Recall that $\mathcal{M} \models \phi$ iff $\forall \mathsf{c}\ (\mathcal{M},\mathsf{c}) \models \phi$. By Corollary 27 we can rewrite the latter as

$$\forall \mathsf{c} \text{ s.t. } \mathsf{c} \text{ is pair-epistemically non-redundant, } (\mathcal{M},\mathsf{c}) \models \phi.$$

But according to Lemma 28 there are only finitely many pair-epistemically non-redundant call sequences and by Lemma 23 their set can be explicitly constructed. □

6.3 Decidability of termination with common knowledge operator

Finally, we show that it is decidable to determine whether a gossip protocol that uses guard with non-nested common knowledge operator (in short: a common knowledge protocol) terminates. For an example of such a protocol see Appendix A.

First, we establish monotonicity of gossip situations and epistemic pair-views with respect to call sequence extensions, w.r.t. suitable partial orderings. Intuitively, we claim that as the call sequence gets longer each agent acquires more information.

Definition 30 *For any two gossip situations* s,s' *we write* $\mathsf{s} \leq_{\mathsf{A}} \mathsf{s}'$ *if for all* $a \in \mathsf{A}$ *we have* $\mathsf{s}_a \subseteq \mathsf{s}'_a$.

Note 31 (Note 1 of [2]) *For all call sequences* c *and* d *such that* $\mathsf{c} \sqsubseteq \mathsf{d}$ *we have* $\mathsf{c}(\mathsf{root}) \leq_{\mathsf{A}} \mathsf{d}(\mathsf{root})$.

Definition 32 *For any two epistemic pair-views* $V,V' \in \widetilde{\mathsf{EPV}}$ *we write* $V \leq_{\mathsf{EPV}} V'$ *if for all* $a,b \in \mathsf{A}$ *there exists* $X \subseteq V(a,b)$ *and an surjective (onto) function* $g : X \to V'(a,b)$ *such that for all* $\mathsf{s} \in X$ *we have* $\mathsf{s} \leq_{\mathsf{A}} g(\mathsf{s})$.

Lemma 33 $\leq_{\mathsf{EPV}}$ *is a partial order.*

Proof.
(Reflexivity) For any epistemic pair-view V, we have $V \leq_{\mathsf{EPV}} V$, because for each $a,b \in \mathsf{A}$ we can pick $V(a,b)$ as X and the identity function on $V(a,b)$ as g.

(Transitivity) Suppose V,V',V'' are three epistemic pair-views such that $V \leq_{\mathsf{EPV}} V'$ and $V' \leq_{\mathsf{EPV}} V''$. Then, from the definition of $\leq_{\mathsf{EPV}}$, for any $a,b \in \mathsf{A}$ there exist $X \subseteq V(a,b)$, $Y \subseteq V'(a,b)$, and surjective functions $g : X \to V'(a,b)$ and $h : Y \to V''(a,b)$. Let $Z = \{\mathsf{s} \in X \mid g(\mathsf{s}) \in Y\}$. Note that $g|_Z : Z \to Y$, i.e. the restriction of g to Z, is surjective. The composition $g|_Z \circ h : Z \to V''(a,b)$ is also surjective and for any gossip situation $\mathsf{s} \in Z$ the following holds $\mathsf{s} \leq_{\mathsf{A}} g|_Z(\mathsf{s}) \leq_{\mathsf{A}} h(g|_Z(\mathsf{s})) = (g|_Z \circ h)(\mathsf{s})$.

(Antisymmetry) Suppose V,V' are two epistemic pair-views such that $V \leq_{\mathsf{EPV}} V'$ and $V' \leq_{\mathsf{EPV}} V$. Then, from the definition of $\leq_{\mathsf{EPV}}$, for any $a,b \in \mathsf{A}$ there exist $X \subseteq V(a,b)$, $Y \subseteq V'(a,b)$, and surjective functions $g : X \to V'(a,b)$ and $h : Y \to V(a,b)$. Let $Z = \{\mathsf{s} \in X \mid g(\mathsf{s}) \in Y\}$. Note that $g|_Z : Z \to Y$, i.e. the restriction of g to Z, is surjective. Moreover, $g|_Z \circ h : Z \to V(a,b)$ is also surjective, and because $Z \subseteq V(a,b)$ is finite, $Z = V(a,b)$, $g|_Z = g$, and $g \circ h$ is a permutation on $V(a,b)$. Similarly we can show that $Y = V'(a,b)$. Since $(g \circ h)$ is a permutation on a finite set, there exists k such that $(g \circ h)^k$ is the identity function on $V(a,b)$.

Note that for any $\mathsf{s} \in V(a,b)$, we have $\mathsf{s} \leq_{\mathsf{A}} (g \circ h)(\mathsf{s})$, because $\mathsf{s} \leq_{\mathsf{A}} g(\mathsf{s}) \leq_{\mathsf{A}} h(g(\mathsf{s})))$. Now consider the sequence: $\mathsf{s} \leq_{\mathsf{A}} (g \circ h)(\mathsf{s}) \leq_{\mathsf{A}} (g \circ h)^2(\mathsf{s}) \leq_{\mathsf{A}} \ldots \leq_{\mathsf{A}} (g \circ h)^k(\mathsf{s}) = \mathsf{s}$. In fact, all of the elements in this sequence have to be the same, because $\leq_{\mathsf{A}}$ is a partial order. In particular, this shows that $(g \circ h)(\mathsf{s}) = \mathsf{s}$. Therefore, $g \circ h$ is the identity function on $V(a,b)$. Now, for any $\mathsf{s} \in V(a,b)$ we have that $\mathsf{s} \leq_{\mathsf{A}} g(\mathsf{s}) \leq_{\mathsf{A}} h(g(\mathsf{s})) = (g \circ h)(\mathsf{s}) = \mathsf{s}$, so g is the identity function as well. This shows that $V(a,b) = V'(a,b)$ for all $a,b \in \mathsf{A}$. □

The next lemma formalizes the intuition that information captured by the epistemic pair-view grows along a call sequence.

Lemma 34 *For all two call sequences such that* $\mathsf{c} \sqsubseteq \mathsf{d}$ *we have* $\mathsf{EPV}(\mathsf{c}) \leq_{\mathsf{EPV}} \mathsf{EPV}(\mathsf{d})$.

Proof. Let $\mathsf{d} = \mathsf{c}.\mathsf{c}'$. Take $a,b \in \mathsf{A}$. By a repeated application of Lemma 24 we get $\mathsf{EPV}(\mathsf{c}.\mathsf{c}')(a,b) = \{\mathsf{c}'(\mathsf{s}) \mid \mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b)$ and $\forall \mathsf{c}'' \sqsubseteq \mathsf{c}'\ (\mathsf{c}''(\mathsf{s})_a = \mathsf{c}''(\mathsf{c}(\mathsf{root}))_a \wedge \mathsf{c}''(\mathsf{s})_b = \mathsf{c}''(\mathsf{c}(\mathsf{root}))_b)\}$. It suffices then to pick $X = \{\mathsf{s} \in \mathsf{EPV}(\mathsf{c})(a,b) \mid \forall \mathsf{c}'' \sqsubseteq \mathsf{c}'\ (\mathsf{c}''(\mathsf{s})_a = \mathsf{c}''(\mathsf{c}(\mathsf{root}))_a \wedge \mathsf{c}''(\mathsf{s})_b = \mathsf{c}''(\mathsf{c}(\mathsf{root}))_b)\}$ and set $g(\mathsf{s}) =$

$\mathsf{c}'(\mathsf{s})$ for all $\mathsf{s} \in X$. It is easy to check that such $g : X \to \mathsf{EPV}(\mathsf{d})$ is surjective, so $\mathsf{EPV}(\mathsf{c}) \leq_{\mathsf{EPV}} \mathsf{EPV}(\mathsf{d})$, as claimed. □

We can now draw the following useful conclusion.

Lemma 35 *Suppose that* c *is pair-epistemically redundant. Then a prefix* $\mathsf{c}_1.\mathsf{c}$ *of it exists such that* c_1 *is pair-epistemically non-redundant and* $\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}) = \mathsf{EPV}(\mathsf{c}_1)$.

Proof. Let $\mathsf{c}_1.\mathsf{c}_2$ be the shortest prefix of c such that $\mathsf{EPV}(\mathsf{c}_1) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2)$. Then c_1 is pair-epistemically non-redundant. Let $\mathsf{c}_2 = \mathsf{c}_1 \ldots . \mathsf{c}_l$. By Lemma 34 we have

$$\mathsf{EPV}(\mathsf{c}_1) \leq_{\mathsf{EPV}} \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1) \leq_{\mathsf{EPV}} \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1.\mathsf{c}_2) \leq_{\mathsf{EPV}} \ldots \leq_{\mathsf{EPV}}$$
$$\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1.\mathsf{c}_2 \ldots . \mathsf{c}_l) = \mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_2) = \mathsf{EPV}(\mathsf{c}_1).$$

Since $\leq_{\mathsf{EPV}}$ is a partial order, $\mathsf{EPV}(\mathsf{c}_1.\mathsf{c}_1) = \mathsf{EPV}(\mathsf{c}_1)$ holds. □

Finally we can establish the desired result. In the proof we shall use the following observation.

Theorem 36 (Stuttering) *Suppose that* $\mathsf{c} := \mathsf{c}_1.\mathsf{c}.\mathsf{c}_2$ *and* $\mathsf{d} := \mathsf{c}_1.\mathsf{c}.\mathsf{c}.\mathsf{c}_2$. *Then for all formulas* $\phi \in \mathcal{L}^{ck}$, $(\mathcal{M}, \mathsf{c}) \models \phi$ *iff* $(\mathcal{M}, \mathsf{d}) \models \phi$.

Proof. This is a direct consequence of the corresponding Stuttering Theorem 3 from [2] and Note 5. □

Theorem 37 (Decidability of Termination) *Given a common knowledge gossip protocol it is decidable to determine whether it always terminates.*

Proof. We first prove that a gossip protocol may fail to terminate iff it can generate a call sequence $\mathsf{c}.\mathsf{c}$ such that c is pair-epistemically non-redundant and $\mathsf{EPV}(\mathsf{c}.\mathsf{c}) = \mathsf{EPV}(\mathsf{c})$.
($\Rightarrow$) Let $\overline{\mathsf{c}}$ be an infinite sequence of calls generated by the protocol. There are only finitely many pair-epistemic views, so some prefix c of $\overline{\mathsf{c}}$ is pair-epistemically redundant. The claim now follows by Lemma 35.

($\Leftarrow$) Suppose that the protocol generates a sequence of calls $\mathsf{c}.\mathsf{c}$ such that c is pair-epistemically non-redundant and $\mathsf{EPV}(\mathsf{c}.\mathsf{c}) = \mathsf{EPV}(\mathsf{c})$.

Let ϕ be the guard associated with the call c, i.e., $\phi \to \mathsf{c}$ is a rule used in the considered protocol. By assumption $(\mathcal{M}, \mathsf{c}) \models \phi$, so by Lemma 23 $(\mathcal{M}, \mathsf{c}.\mathsf{c}) \models \phi$. By the repeated application of the Stuttering Theorem 36 we get that for all $i \geq 1$, $(\mathcal{M}, \mathsf{c}.\mathsf{c}^i) \models \phi$. Consequently, $\mathsf{c}.\mathsf{c}^\omega$ is an infinite sequence of calls that can be generated by the protocol.

The above equivalence shows that determining whether the protocol always terminates is equivalent to checking that it cannot generate a call sequence $\mathsf{c}.\mathsf{c}$ such that c is pair-epistemically non-redundant and $\mathsf{EPV}(\mathsf{c}.\mathsf{c}) = \mathsf{EPV}(\mathsf{c})$.

But given a call sequence, by the Decidability of Semantics Theorem 21, it is decidable to determine whether it can be generated by the protocol and by Lemma 22 it is decidable to determine whether a call sequence is pair-epistemically non-redundant. Further, by Lemma 28 there are only finitely many pair-epistemically non-redundant call sequences, so the claim follows. □

7 Conclusions

We studied here various aspects of common knowledge in the context of a natural epistemic logic used to express and reason about distributed epistemic gossip protocols. We showed that the semantics and truth in this logic are decidable in the absence of nested modalities. The first result implies that the gossip

protocols relying on such a use of the common knowledge operator are implementable and the second one that their partial correctness is decidable, since partial correctness of these gossip protocols can be expressed as a formula of the considered language. Further, we proved that the termination of these gossip protocols is decidable, as well.

There are a number of interesting open problems related to this work. An obvious question is whether our results can be extended to formulas that admit nested modalities.

In Corollary 17 we showed that under certain conditions common knowledge for two agents is equivalent to the 4th fold iterated knowledge. An intriguing question is whether this result holds for arbitrary call sequences and arbitrary formulas. If not, is then common knowledge always equivalent to some finite iterated knowledge?

Finally, it would be interesting to clarify which formulas two agents can commonly know, i.e., given a call sequence c to characterize the formulas ϕ for which $(\mathcal{M}, \mathsf{c}) \models C_{ab}\phi$ holds. Example 8 indicates that this problem is non-trivial even without any call being performed.

Acknowledgments

We thank the referees for helpful comments. First author he was partially supported by NCN grant 2014/13/B/ST6/01807. The second author was partially supported by EPSRC grants EP/M027287/1 and EP/P020909/1.

References

[1] K. R. Apt, D. Grossi & W. van der Hoek (2016): *Epistemic Protocols for Distributed Gossiping*. In: *Proceedings of the 15th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2015)*, *EPTCS* 215, pp. 51–66, doi:10.4204/EPTCS.215.5.

[2] K. R. Apt & D. Wojtczak (2016): *On Decidability of a Logic of Gossips*. In: *Proceedings of the 15th European Conference, JELIA 2016*, *Lecture Notes in Computer Science* 10021, Springer, pp. 18–33, doi:10.1007/978-3-319-48758-8_2.

[3] K.R. Apt, E. Kopczyński & D. Wojtczak (2017): *On the Computational Complexity of Gossip Protocols*. In: *Proceedings of 26th IJCAI*. To appear.

[4] K.R. Apt & D. Wojtczak (2017): *Decidability of Fair Termination of Gossip Protocols*. In: *Proceedings of the IWIL Workshop and LPAR Short Presentations*, Kalpa Publications, pp. 73–85.

[5] M. Attamah, H. van Ditmarsch, D. Grossi & W. van der Hoek (2014): *A Framework for Epistemic Gossip Protocols*. In: *Proceedings of the 12th European Conference on Multi-Agent Systems (EUMAS 2014), Revised Selected Papers*, 8953, Springer, pp. 193–209, doi:10.1007/978-3-319-17130-2_13.

[6] M. Attamah, H. van Ditmarsch, D. Grossi & W. van der Hoek (2014): *Knowledge and Gossip*. In: *Proceedings of ECAI'14*, IOS Press, pp. 21–26, doi:10.3233/978-1-61499-419-0-21.

[7] J. van Benthem, J. van Eijck & B. Kooi (2005): *Common Knowledge in Update Logics*. In: *Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2005)*, pp. 253–261, doi:10.1145/1089933.1089960.

[8] M.C. Cooper, A. Herzig, F. Maffre, F. Maris & P. Régnier (2016): *A simple account of multiagent epistemic planning*. In: *Proceedings of ECAI 2016*, IOS Press, pp. 193–201, doi:10.3233/978-1-61499-672-9-193.

[9] M.C. Cooper, A. Herzig, F. Maffre, F. Maris & P. Regnier (2016): *Simple Epistemic Planning: Generalised Gossiping*. In: *Proceedings of ECAI 2016*, *Frontiers in Artificial Intelligence and Applications* 285, IOS Press, pp. 1563–1564, doi:10.3233/978-1-61499-672-9-1563.

[10] H. van Ditmarsch, J. van Eijck, P. Pardo, R. Ramezanian & F. Schwarzentruber (2017): *Epistemic Protocols for Dynamic Gossip*. *J. of Applied Logic* 20(C), pp. 1–31, doi:10.1016/j.jal.2016.12.001.

[11] H. van Ditmarsch, J. van Eijck & R. Verbrugge (2009): *Common Knowledge and Common Belief*. In J. van Eijck & R. Verbrugge, editors: *Discourses on Social Software*, Amsterdam University Press, pp. 99–122.

[12] H. van Ditmarsch, D. Grossi, A. Herzig, W. van der Hoek & L.B. Kuijer (2016): *Parameters for Epistemic Gossip Problems*. In: *Proceedings of the 12th Conference on Logic and the Foundations of Game and Decision Theory (LOFT 2016)*. Available at https://pdfs.semanticscholar.org/74b5/2c025f335ba487cac612019e39ce6c818448.pdf.

[13] H. van Ditmarsch, W. van der Hoek & B. Kooi (2007): *Dynamic Epistemic Logic*. *Synthese Library* 337, Springer, doi:10.1007/978-1-4020-5839-4.

[14] R. Fagin, J. Halpern, M. Vardi & Y. Moses (1995): *Reasoning about knowledge*. MIT Press, Cambridge, Massachusetts.

[15] M.F. Friedell (1969): *On the structure of shared awareness*. *Behavioral Science* 14(1), pp. 28–39, doi:10.1002/bs.3830140105.

[16] S.M. Hedetniemi, S.T. Hedetniemi & A.L. Liestman (1988): *A survey of gossiping and broadcasting in communication networks*. *Networks* 18(4), pp. 319–349, doi:10.1002/net.3230180406.

[17] A. Herzig & F. Maffre (2017): *How to Share Knowledge by Gossiping*. *AI Communications* 30(1), pp. 1–17, doi:10.3233/AIC-170723. Available at http://content.iospress.com/articles/ai-communications/aic723.

[18] J. Hromkovic, R. Klasing, A. Pelc, P. Ruzicka & W. Unger (2005): *Dissemination of Information in Communication Networks - Broadcasting, Gossiping, Leader Election, and Fault-Tolerance*. Texts in Theoretical Computer Science. An EATCS Series, Springer, doi:10.1007/b137871.

[19] D.K. Lewis (1969): *Convention, a Philosophical Study*. Harvard University Press, Cambridge (MA).

[20] P. Vanderschraaf & G. Sillari (2014): *Common Knowledge*. In: *The Stanford Encyclopedia of Philosophy*. Available at https://plato.stanford.edu/entries/common-knowledge.

[21] Y. Wang, L. Kuppusamy & J. van Eijck (2009): *Verifying epistemic protocols under common knowledge*. In: *Proceedings of the 12th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2009)*, ACM, pp. 257–266, doi:10.1145/1562814.1562848.

A Example: a common knowledge protocol

To illustrate gossip protocols that employ the common knowledge operator assume that the agents are nodes of an undirected connected graph (V,E) and that the calls can take place only between pairs of agents connected by an edge. Let N_i denote the set of neighbours of node i.

Consider a gossip protocol with the following program for agent i (we use here the syntax introduced in [1]):

$$*[[]_{j\in N_i, B\in \mathsf{P}} F_iB \wedge \neg C_{ij}F_jB \to (i,j)].$$

Informally, agent i calls a neighbour j if i is familiar with some secret (here B) and there is no common knowledge between i and j that j is familiar with this secret.

Partial correctness of a protocol states that upon its termination the formula $\bigwedge_{i,j\in \mathsf{A}} F_iJ$ holds.

To prove partial correctness of the above protocol consider the exit condition

$$\bigwedge_{(i,j)\in E} \bigwedge_{B\in \mathsf{P}} (F_iB \to C_{ij}F_jB).$$

For all agents i and j and secrets B, the formula $C_{ij}F_jB \rightarrow F_jB$ is true, so the exit condition implies

$$\bigwedge_{(i,j)\in E} \bigwedge_{B\in \mathsf{P}} (F_iB \rightarrow F_jB).$$

Consider now an agent i and the secret J of agent j. Let $j = i_1, \ldots, i_h = i$ be a path that connects j with i. The above formula implies that for $g \in \{1, \ldots, h-1\}$ we have $\bigwedge_{B\in \mathsf{P}}(F_{i_g}B \rightarrow F_{i_{g+1}}B)$. By combining these $h-1$ formulas we get $\bigwedge_{B\in \mathsf{P}}(F_jB \rightarrow F_iB)$. But F_jJ is true, so we conclude F_iJ. Consequently $\bigwedge_{i,j\in \mathsf{A}} F_iJ$, as desired.

To prove termination we need the following observation.

Lemma 38 *For all call sequences* $\mathsf{c}.(i,j)$ *and secrets* B

$$(\mathcal{M}, \mathsf{c}.(i,j)) \models F_iB \wedge F_jB \text{ implies } (\mathcal{M}, \mathsf{c}.(i,j)) \models C_{ij}(F_iB \wedge F_jB).$$

Proof. Suppose that $(\mathcal{M}, \mathsf{c}.(i,j)) \models F_iB \wedge F_jB$. Take some d such that $\mathsf{c}.(i,j) \sim_{\{i,j\}} \mathsf{d}$. So there exists a sequence of call sequences $\mathsf{c}_1, \ldots, \mathsf{c}_k$ such that

$$\mathsf{c}.(i,j) = \mathsf{c}_1 \sim_{m_1} \mathsf{c}_2 \sim_{m_2} \ldots \sim_{m_k} \mathsf{c}_k = \mathsf{d},$$

where each m_h is i or j.

By the repeated use of the Equivalence Theorem 4 each of the call sequences $\mathsf{c}_1, \ldots, \mathsf{c}_k$ contains the call (i,j) that corresponds with the last call of $\mathsf{c}.(i,j)$. Let $\mathsf{d}_1.(i,j), \ldots, \mathsf{d}_k.(i,j)$ be the corresponding prefixes of $\mathsf{c}_1, \ldots, \mathsf{c}_k$.

By the Equivalence Theorem 4 and the definition of a view given there we also have

$$\mathsf{d}_1.(i,j)_i = \mathsf{d}_1.(i,j)_j = \mathsf{d}_2.(i,j)_i = \mathsf{d}_2.(i,j)_j.$$

By the assumption this implies $(\mathcal{M}, \mathsf{d}_2.(i,j)) \models F_iB \wedge F_jB$, since $\mathsf{d}_1.(i,j) = \mathsf{c}.(i,j)$.

Repeating this procedure we conclude that $(\mathcal{M}, \mathsf{d}_k.(i,j)) \models F_iB \wedge F_jB$ and hence $(\mathcal{M}, \mathsf{d}) \models F_iB \wedge F_jB$. This implies the claim. □

Now, by the definition of semantics for all call sequences $\mathsf{c}.(i,j)$ and secrets B, $(\mathcal{M}, \mathsf{c}) \models F_iB$ implies $(\mathcal{M}, \mathsf{c}.(i,j)) \models F_iB \wedge F_jB$, which implies by Lemma 38 that $(\mathcal{M}, \mathsf{c}.(i,j)) \models C_{ij}(F_iB \wedge F_jB)$ and hence $(\mathcal{M}, \mathsf{c}.(i,j)) \models C_{ij}F_jB$. This shows that after each call (i,j) the size of the set $\{(i,j,B) \mid \neg C_{ij}F_jB\}$ decreases.