ECAI 2014
T. Schaub et al. (Eds.)
© 2014 The Authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-419-0-21

Knowledge and Gossip

Maduka Attamah[1] and **Hans van Ditmarsch**[2] and **Davide Grossi**[1] and **Wiebe van der Hoek**[1]

Abstract. A well-studied phenomenon in network theory are optimal schedules to distribute information by one-to-one communication between nodes. One can take these communicative actions to be 'telephone calls', and this process of spreading information is known as *gossiping* [4]. It is typical to assume a global scheduler who simply executes a possibly non-deterministic protocol. Such a protocol can be seen as consisting of a sequence of instructions *"first, agent a calls b, then c, next, d calls b . . . "*. We investigate *epistemic* gossip protocols, where an agent a will call another agent not because it is so instructed but based on its knowledge or ignorance of the factual information that is distributed over the network. Such protocols therefore don't need a central schedular, but they come at a cost: they may take longer to terminate than non-epistemic, globally scheduled, protocols. We describe various epistemic protocols, we give their logical properties, and we model them in a number of ways.

1 Introduction

Communication protocols have the aim to share knowledge between nodes in a pre-described way. Consider the following scenario.

> *Six friends each know a secret. They can call each other by phone. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?*[3]

Let us generalise this to the case of $n \geq 2$ friends,[4] and focus on protocols that are *sufficient* (in the sense that they spread all secrets). If $n = 2$, the two friends a and b need to make only one phone call, which we denote by ab ('a calls b'). For $n = 3$, the call sequence ab, bc, ca will do. Let us look at a protocol for $n \geq 4$ friends.

Protocol 1 (**n friends**) *Choose four friends from the set of friends* A*, say a, b, c, d, and one of those four, say a. First, a makes $n - 4$ calls to all friends* $\mathsf{A} \setminus \{a, b, c, d\}$*. Then, the calls ab; cd; ac; bd are made. Finally a makes another call to all friends from* $\mathsf{A} \setminus \{a, b, c, d\}$.

This adds up to $(n - 4) + 4 + (n - 4) = 2n - 4$ calls. For $n = 6$ we get $2n - 4 = 8$ calls. An execution sequence for $n = 6$ is

$$ae; af; ab; cd; ac; bd; ae; af \qquad (1)$$

After the protocol, all friends indeed know all secrets. One can show that less than $2n - 4$ calls is insufficient to distribute all secrets.

Another protocol is obtained by imagining the agents lined up along a round-table, such that, starting with agent a_1, each agent passes on its secrets to its neighbour, until we have almost come full circle twice (after $n - 1$ calls, both a_n and a_{n-1} know all secrets, it takes only $n-2$ calls to pass those on to $a_1, a_2, \ldots a_{n-2}$). This gives rise to $2n - 3$ calls, only one more than the minimum of $2n - 4$.

$$a_1a_2; a_2a_3; \ldots; a_{n-1}a_n; a_na_1; a_1a_2, a_2a_3; \ldots; a_{n-2}a_{n-1} \qquad (2)$$

In network theory protocols have been investigated widely in the 1970s and 1980s. Their focus are optimal schedules to distribute information by one-to-one communication between nodes, which has been known as *gossiping*. An overview study is [4]. The minimum of $2n - 4$ for Protocol 1 is presented in (e.g.) [6] and later in [5].

Protocol 1 and also the round-table protocol assume that the friends can coordinate their actions before making any calls. This would be natural for instance if they are a subset of a cohort of students which has common knowledge that some specific exam results will be made available to each of them individually (so friend's a secret is either 'a passed' or 'a failed'). But often such co-ordination is not possible. Suppose all students of the cohort our friends are part of, receive an unexpected invitation for a party. The friends may be curious to find out about each other whether they will accept, in which case they will have to make phone calls based on the knowledge, or better ignorance, they have about the secrets of others. Since in such a distributed protocol several agents may decide to initiate a call at the same time, we assume the presence of an *arbiter* who breaks a tie in such cases. Let us now consider such an epistemic protocol: an agent calls another agent depending on its knowledge (or ignorance) only, and choices are random.

Protocol 2 *As long as not all agents know all secrets, choose agents $a, b \in$* A *such that a does not know b's secret, and let a call b.*

It is easy to see that this protocol will terminate and achieves the epistemic goal that everybody knows every secret. No call sequence obtained from Protocol 1 can be obtained by Protocol 2: in the last four calls from Protocol 1, a contacts friends of which she already knows the secret. Protocol 2 also allows for longer execution sequences than Protocol 1, e.g.,

$$a_1a_2; a_1a_3; \ldots; a_1a_n; a_2a_3; \ldots; a_2a_n; a_3a_4; \ldots; a_{n-1}a_n \qquad (3)$$

This sequence consists of $(n-1)+(n-2)+\cdots+1 = n(n-1)/2$ calls! It is in fact the *longest* possible sequence. There are many such epistemic protocols, of which we will present some in Section 3. First, we formally introduce the logic and semantics to describe knowledge of agents about secrets in networks, and to describe protocols (Section 2). In Section 4 we give a glimpse of many possible extensions.

2 Logical dynamics of gossip

Let a finite set of n *agents* $\mathsf{A} = \{a, b, \ldots, \}$ and a corresponding set of *secrets* (propositional atoms) $\mathsf{P} = \{A, B, \ldots\}$ be given. Upper

[1] University of Liverpool, UK, email: m.k.attamah@liverpool.ac.uk
[2] LORIA, Nancy, France, email: hans.van-ditmarsch@loria.fr

[3] Presented as a puzzle at the 1999 Nationale Wetenschapsquiz (National Science Competition), Netherlands.

[4] We will use the terms 'friends' and 'agents' interchangeably hereafter.

case letters (e.g., A) denote the secrets of the agents denoted by the corresponding lower case letters (e.g., a).

Definition 1 (Language) *We consider three types $\mu \in \{-, 0, +\}$ of phone calls ab^μ (see below Definition 11). Define $\mathcal{L}_K$ as*

$$\begin{array}{llll} \mathcal{L}_K \ni & \varphi & ::= & A \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid [\pi]\varphi \\ & \pi & ::= & ?\varphi \mid ab^\mu \mid \mathsf{skip} \mid (\pi\,;\pi) \mid (\pi \cup \pi) \mid \pi^* \end{array}$$

where $a \neq b \in \mathsf{A}$, and $A \in \mathsf{P}$. We also consider the language $\mathcal{L}_{Kw} \subseteq \mathcal{L}_K$ where the atomic formulas are of the form Kw_aB, meaning: 'a knows b's secret', or 'a knows whether *B'.*

Disjunction and implication are defined as usual. We will omit truth definitions for negation and conjunction. The construct $[ab^\mu]\varphi$ stands for 'after a call of type μ between agents a and b, φ (is true)'. We let ab^μ and ba^μ denote the same action. For $(?\varphi\,;\pi)^*\,;?\neg\varphi$ we may write '`while` φ `do` π'. Epistemic protocols will be defined as such programs π but with additional constraints. Informally, a protocol is a program that intends to get all agents to know all secrets.

Definition 2 (Epistemic model) *An epistemic model M is a tuple $M = (S, \sim, V)$ such that*

- *S is a non-empty set of possible worlds,*
- *$\sim : \mathsf{A} \to \mathcal{P}(S \times S)$ assigns an equivalence relation to each agent,*
- *$V : S \to \mathsf{P} \to \{0, 1\}$ is a valuation for each $s \in S$.*

If $M = (S, \sim, V)$, rather than $s \in S$, we will also write $s \in M$. For $\sim(a)$ we write $\sim_a$, and for $V(s)$ we write V_s. A pointed epistemic model *is a pair (M, s) where $s \in M$. We also consider multi-pointed epistemic models (M, S'), where $S' \subseteq S$.*

Epistemic models are also known as $S5$-models, and the $S5$ validities are well-known [3]. The scenarios we envisage will only use some specific $S5$-models. First, given some $\mathsf{Q} \subseteq \mathsf{P}$, let us define $s \equiv_\mathsf{Q} t$ as $[V_s(A) = V_t(A)$ for all $A \in \mathsf{Q}]$.

Definition 3 (Gossip situation) *An epistemic model $(S, \sim, V)$ is a* gossip situation *if $S = \{s \mid s \in \{0, 1\}^{|\mathsf{P}|}\}$ (the domain consists of all valuations), and for every $a \in \mathsf{A}$, $\sim_a$ equals $\equiv_\mathsf{Q}$ for some $\mathsf{Q} \subseteq \mathsf{P}$ with $A \in \mathsf{Q}$. The* initial *(respectively* terminal *gossip) situation is the situation in which, for all agents a, $\mathsf{Q} = \{A\}$ (respectively, $\mathsf{Q} = \mathsf{P}$).*

Definition 4 (Gossip model) *A* gossip model *is a pair $G = (\mathcal{S}, \approx)$, where $\mathcal{S}$ is a set of gossip situations and $\approx$ assigns to each agent an equivalence relation $\approx_a$ on $\mathcal{S}$ satisfying, for all $M = (S, \sim^M, V)$ and $N = (T, \sim^N, W)$:*

$$M \approx_a N \textit{ iff } \exists \mathsf{Q} : \sim_a^M = \equiv_\mathsf{Q}^M \textit{ and } \equiv_\mathsf{Q}^N = \sim_a^N \tag{4}$$

A pointed gossip model *is a pair $(G, M) = ((\mathcal{S}, \approx), M)$, where $M \in G$. The* initial gossip model *is the (singleton) gossip model consisting of the initial gossip situation.*

So a gossip situation encodes that for each a there is a Q such that agent a knows exactly the secrets in Q. A gossip model allows agents to be uncertain which gossip situation is the actual one.

Proposition 5 *A gossip model is an epistemic model.*

Proof Each gossip model G gives rise to an epistemic model $E(G) = (R, \sim, X)$ where

- $R = \{s_M \mid M = (S, \sim, V) \in \mathcal{S}$ and $s \in S\}$;
- $s_M \sim_a t_N$ with $M = (S, \sim^M, V), N = (T, \sim^N, U)$ iff there are v_M and u_N such that $V_v = U_u$, $s \sim_a^M v$, $t \sim_a^N u$, and $M \approx_a N$;
- $X_{s_M} = V_s$.

To demonstrate that $E(G)$ is an $S5$ model one needs to show that $\sim_a$ is an equivalence relation: we leave the details to the reader. □

The pointed gossip model (G, M) corresponds to the multi-pointed epistemic model $(E(G), S)$, where S is the domain of M. We write $\mathcal{G}$ for the class of gossip models, and $\mathcal{G} \models \varphi$ for validities on that class.

Definition 6 (Static operators of $\mathcal{L}_K$ on epistemic models) *Let $M = (S, \sim, V)$ be an epistemic model. We inductively define the interpretation of a formula $\varphi \in \mathcal{L}_K$ on a state $s \in M$.*

$$\begin{array}{lll} M, s \models A & \textit{iff} & V_s(A) = 1 \\ M, s \models K_a\varphi & \textit{iff} & M, t \models \varphi \textit{ for every } t \textit{ such that } s \sim_a t \end{array}$$

Kw_aB abbreviates $K_aB \vee K_a\neg B$. If $M, s \models \varphi$ for all $s \in T \subseteq S$, we write $M, T \models \varphi$. $M, S \models \varphi$ is also written $M \models \varphi$: 'φ is valid on M', and if $M \models \varphi$ for all M, we write $\models \varphi$, for 'φ is valid'.

Truth in a gossip situation is global (the proof is by induction on φ):

Proposition 7 *If M is a gossip situation and $\varphi \in \mathcal{L}_{Kw}$, then $M \models \varphi$ or $M \models \neg\varphi$.*

Definition 8 (Static operators of $\mathcal{L}_{Kw}$ on gossip models) *Let (G, M) be a pointed gossip model:*

$$\begin{array}{lll} G, M \models_g Kw_aB & \textit{iff} & M \models Kw_aB \\ G, M \models_g K_a\psi & \textit{iff} & G, N \models_g \psi \textit{ for every } N \textit{ s.t. } M \approx_a N \end{array}$$

Proposition 9 *Let (G, M) be a gossip model and $\varphi \in \mathcal{L}_{Kw}$. Then*

$$G, M \models \varphi \textit{ iff } E(G), S \models \varphi$$

where $E(G)$ is as in Proposition 5 and S is the domain of M.

To help sharpen the reader's intuition, we list some elementary validities on gossip situations.

Proposition 10 *Let $M = (S, \sim, V)$ be a gossip situation, with $\sim_a = \equiv_\mathsf{Q}$, and let $\psi \in \mathcal{L}_{Kw}$. Then:*

1. $M \models K_a\psi \to K_bK_a\psi$
2. $M \models Kw_aB$ *iff* $B \in \mathsf{Q}$

In gossip situations, all knowledge is public (item 1), and the secrets known by a are completely determined by $\sim_a$. As a consequence of this, for the full language $\mathcal{L}_K$, we have for instance $E(G), S \models K_a(B \vee C) \to (K_aB \vee K_aC)$, where S is the domain of M: agents know 'full' secrets. Note that this is not an $S5$-validity: our models provide a conservative extension of $S5$.

A gossip situation M is a description of who knows which secret. In a gossip situation, if $\sim_a$ equals $\equiv_\mathsf{Q}$ for $\mathsf{Q} \subseteq \mathsf{P}$, this means that agent a knows exactly the value of the secrets in Q (as in item 2 of Proposition 10). An alternative way to represent a gossip situation M is by a function $f_M : \mathsf{A} \to \mathcal{P}(\mathsf{P})$ where $f_M(a)$ denotes the secrets that are known by agent a. So: $M \models Kw_aD$ iff $D \in f_M(a)$. We may represent such a function as a list: $AB.ABC.ABC.D$ for instance is the function f where a knows the secrets A and B, b knows A, B and C, etc.

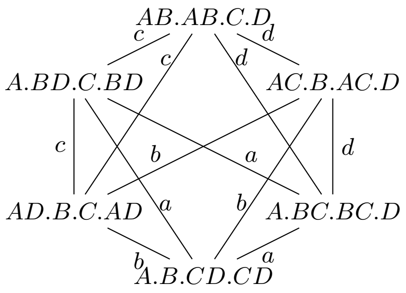

Figure 1. The result of a call between a and b. The actual gossip situation is $AB.AB.C.D$.

We also can describe gossip models similarly: they can be represented as $\mathcal{F} = (F, \approx)$ where F is a set of functions $\mathsf{A} \to \mathcal{P}(\mathsf{P})$ and $\approx_a$ an equivalence relation for every agent a, defined by $f \approx_a g$ iff $f(a) = g(a)$. An advantage of this functional representation is its succinctness: Figure 1 gives an example.

We now proceed to define the interpretation of calls between two agents a and b, and of the interpretation of protocols consisting of such calls. We first consider calls, and then, protocols. We distinguish three kinds of calls, ab^- (non-epistemic, synchronous), ab^0 (epistemic, synchronous) and ab^+ (epistemic, asynchronous). Given some such call, the agents a and b are the *callers* and all other agents are the *non-callers*.

The ab^- call models a telephone call in the 'traditional' network systems setting of gossiping protocols: it is common knowledge between all agents that a and b are making a call, but the non-callers may not know the value of the secrets the callers exchange. We could say that all agents are sitting in a circle round a table, so the non-callers can observe the callers, but we imagine the callers to talk softly, so that the non-callers cannot hear what the callers say. They only know that the callers exchange all secrets they know.

The ab^0 call models a telephone call between a and b where the non-callers may not know who are making a call. But they know that a call is made. (The system is synchronized.) For example, given four agents a, b, c, d, when a and b are making a call, then c considers it possible that the call was between a and d, or between b and d; c only knows that it was not involved in the call itself.

The ab^+ call is like ab^0 but with the additional option that the non-callers consider it possible that no call took place at all (the skip action). This is the standard way to model asynchronous communication with $S5$-preserving model transformations.

Definition 11 (Call in a gossip situation)
Let $M = (S, \sim, V)$ be a gossip situation.

$$\begin{array}{lll} M \models [ab^\mu]\psi & \textit{iff} & M^{ab} \models \psi \\ M \models [\mathsf{skip}]\psi & \textit{iff} & M \models \psi \end{array}$$

where $M^{ab} = (S, \sim', V)$ such that $\sim'_a = \sim'_b = \sim_a \cap \sim_b$, and for all $c \neq a, b$, $\sim'_c = \sim_c$.

The action of calling has no precondition. Two agents always can make a call. Their distributed factual knowledge thus becomes shared between the two. This is the intersection of $\sim_a$ and $\sim_b$ in the definition. The mode μ of a call is irrelevant for its interpretation in a gossip situation. The skip action has no informative or other consequences.

Definition 12 (Semantics of calls in a gossip model) *Let (G, M) be given, where $G = (\mathcal{S}, \approx)$ and $M \in \mathcal{S}$. We define $[\![\mathsf{skip}]\!] = \{((G, M), (G, M))\}$ and, for the types of call $ab^\star$, with $\star \in \{-, 0, +\}$:*

$$[\![ab^\mu]\!] \quad = \quad \{((G, M), (G^{\mathsf{call}\mu}, M^{ab}))\}$$

where (for all modes μ) $G^{\mathsf{call}\mu} = (\mathcal{S}^\mu, \approx^\mu)$, such that

$$\begin{array}{lll} \mathcal{S}^- & = & \{N^{ab} \mid N \in \mathcal{S}\} \\ \mathcal{S}^0 & = & \{N^{cd} \mid N \in \mathcal{S} \textit{ and } c \neq d \in \mathsf{A}\} \\ \mathcal{S}^+ & = & \mathcal{S}^0 \cup \{M\} \end{array}$$

and (see Definition (4)) for any $N, N' \in \mathcal{S}^\mu$: $N \approx^\mu_a N'$ iff (there is a $\mathsf{Q} \subseteq \mathsf{P}$ such that $\sim^N_a = \equiv^N_{\mathsf{Q}}$ and $\equiv^{N'}_{\mathsf{Q}} = \sim^{N'}_a$). For the actions $\alpha \in \{\mathsf{skip}, \mathsf{call}^-, \mathsf{call}^0, \mathsf{call}^+\}$, we then define $G, M \models [\alpha]\varphi$ iff for all $((G, M), (G', M')) \in [\![\alpha]\!]$, $(G', M') \models \varphi$.

As a result of a call ab^-, for each existing gossip situation in a gossip model we get exactly one new gossip situation, namely the one in which a and b have exchanged their information. A call ab^0 has as a result that we have to consider the execution of any call between two agents in every gossip situation, not only the call between a and b in the actual gossip situation M. Given n agents, we thus get $\binom{n}{2} = n(n-1)/2$ copies of the gossip model before the call, each of those models being the result of one particular call between two agents. For ab^+ we also need to take the gossip situation in which nothing happened into account. Given four agents a, b, c, d, the result of the call ab^0 is given in Figure 1.

Proposition 13 *The execution of ab^- calls on the initial gossip model preserves the property that it is common knowledge who knows which secrets.*

In other words, after a ab^- call, consider an agent c and a secret D. For every other agent e, agent c knows if agent e knows whether D. This property obviously does not hold for ab^0 calls.

Proposition 14 *There is no common knowledge of information growth after ab^+ calls.*

After an ab^+ call, an agent $c \neq a, b$ considers it possible that no call was made at all.

Proposition 15 *Let $a, b, c \in \mathsf{A}$, and $D \in \mathsf{P}$. Let $\varphi, \psi \in \mathcal{L}_{Kw}$, and let φ contain no K operator in the scope of a negation. Let $\mu, \mu' \in \{-, 0, +\}$. Then*

1. $\mathcal{G} \models [ab^\mu]Kw_c D \leftrightarrow [ab^{\mu'}]Kw_c D$
2. $\mathcal{G} \models [ab^0]\varphi \to [ab^-]\varphi$
3. $\mathcal{G} \models [ab^+]\varphi \to [ab^-]\varphi$
4. $\mathcal{G} \models [ab^-]\psi \leftrightarrow [ab^0]\psi$ *if* $|\mathsf{A}| = 3$.

The first item of this proposition says that the secrets one knows does not depend on the type of call. None of the reversed implications of 2 and 3 of Proposition 15 is valid on gossip models. Also, Proposition 15 does not apply to general epistemic postconditions $K_c\psi$; we have for instance that $[ab^0]K_c\psi \to [ab^-]K_c\psi$ is *not* valid on gossip models: take $\psi = \neg K_c Kw_b A$.

The proposition below highlights some specific properties of each of the basic call programs.

Proposition 16 *Let a gossip model $G = (\mathcal{S}, \approx)$ for at least four agents a, b, c, d be given, and $\psi \in \mathcal{L}_{Kw}$; μ, the 'mode' of the call, is a variable over $\{0, +, -\}$. Then:*

1. $G \models K_c Kw_b D \rightarrow K_c[ab^\mu]Kw_a D$ *for* $\mu \in \{0, +, -\}$*;*
2. $G \models [ab^\mu]K_c \neg init$ *only for* $\mu \in \{0, -\}$*;*
3. $G \models \neg K_c Kw_a B \rightarrow [ab^\mu]\neg K_c Kw_a B$ *only for* $\mu \in \{0, +\}$*;*
4. $G \models K_c Kw_b D \rightarrow [ab^\mu]K_c Kw_a D$ *only for* $\mu \in \{-\}$*;*
5. $G \models init \rightarrow [ab^\mu]\neg K_c \neg init$ *only for* $\mu \in \{+\}$*.*
6. $G \models init \rightarrow [ab^\mu](K_c \bigvee_{x \neq y} Kw_x Y \wedge \neg \bigvee_{x \neq y} K_c Kw_x Y)$ *only for* $\mu \in \{0\}$*;*

where init is a designated atom denoting the initial situation.

Items 1 - 6 show that indeed, all modes of making calls are different. Loosely speaking, the first item says that any agent (c) knows that any call between a and b brings about that both get to know each other's secrets. Contrast this to item 4: only for the mode $\mu = -$, agent c knows that the call happens and remembers its predicted effects. Item 2, which is only true for the modes 0 and $-$, says that a call in the initial situation indeed brings something about: at least some agent will have learned some new secret. Note that the fact that at least one agent learns at least one secret given an arbitrary state is not generally true: it may be that a call takes place between two agents who are unable to tell each other anything new. As a consequence of item 3, agent c can only know that a learned a new secret as the consequence of the call when the call is made in $-$-mode, or if c is involved in the call. Item 5 says that after an ab^+-call, an outsider does not know anything has happened. Finally, item 6 tells us that after an ab^0-call in the initial situation, an outsider knows that somebody learned something, but the outsider does not know who learned something.

Proposition 17 *Not every gossip model can be the result of a sequence of calls from the initial gossip model.*

For instance, it is not possible to reach a gossip situation (or a gossip model containing such a gossip situation) in which agent a knows everybody's secret, but all other agents only know their own secret.

Modelling calls as action models The logic that we introduced is a dynamic epistemic logic [1], as it has epistemic modalities, that are interpreted by accessibility relations in a given epistemic model, and also dynamic epistemic modalities, that are interpreted as epistemic model transformers. (A link between dynamic epistemic logic and gossiping was given in the thesis [7, Section 6.6], and in work that followed from that.) A well-known dynamic epistemic logic is *action model logic* (a.k.a. event model logic; see [1]). The different call actions can be alternatively described as action models. This we will now do. As a consequence, with some restrictions, our logic of knowledge and gossip has a complete axiomatization. The restrictions are that: the translation requires action models with preconditions such as 'agent a knows that A is true and that B is false', formulas that are in $\mathcal{L}_K$ but not in $\mathcal{L}_{Kw}$, so that it is a translation from a formula $\varphi \in \mathcal{L}_{Kw}$ with a dynamic $[ab^\mu]$ operator into a formula in action model logic with (program-free) $\psi \in \mathcal{L}_K$, not $\mathcal{L}_{Kw}$. Another restriction is that we allow Kleene-* operations on programs, but that the axiomatization is for the *-free fragment of programs. Apart from a complete axiomatization with respect to the class of all ($S5$) models, one could also consider a complete axiomatization with respect to the class of gossip models. This would e.g. contain axioms such as $A \rightarrow K_a A$ (all agents know their own secret), a matter we have not resolved yet but consider to look into further.

The agents a and b calling each other exchange all the secrets they know. So, they can distinguish calls wherein either of them knows a different number of secrets. So, for each agent we need to list: (i) the secrets that it knows to be true, (ii) the secrets that it knows to be false, and (iii) the secrets it does not know. Those in i and ii are in non-overlapping subsets and iii can be their complement.

Given the n secrets P, agent a may currently know that the secrets in $\mathsf{Q}_a^+ \subseteq \mathsf{P}$ are true and those in $\mathsf{Q}_a^- \subseteq \mathsf{P}$ are false (and suppose $\mathsf{Q}_a^+ \cup \mathsf{Q}_a^- = \mathsf{Q}_a$), and be ignorant about the rest; whereas agent b may currently know that the secrets in $\mathsf{Q}_b^+ \subseteq \mathsf{P}$ are true and that those in $\mathsf{Q}_b^- \subseteq \mathsf{P}$ are false (and we let $\mathsf{Q}_b^+ \cup \mathsf{Q}_b^- = \mathsf{Q}_b$). We now define ($Ig_a C = \neg Kw_a C$):

$$\begin{array}{lcl} \delta(\mathsf{Q}_a^+, \mathsf{Q}_a^-, \mathsf{Q}_b^+, \mathsf{Q}_b^-) & ::= & \bigwedge_{C \in \mathsf{Q}_a^+} K_a C \wedge \bigwedge_{C \in \mathsf{Q}_a^-} K_a \neg C \wedge \\ & & \bigwedge_{C \in \mathsf{P} \setminus \mathsf{Q}_a} Ig_a C \wedge \\ & & \bigwedge_{C \in \mathsf{Q}_b^+} K_b C \wedge \bigwedge_{C \in \mathsf{Q}_b^-} K_b \neg C \wedge \\ & & \bigwedge_{C \in \mathsf{P} \setminus \mathsf{Q}_b} Ig_b C \end{array}$$

This formula $\delta(\mathsf{Q}_a^+, \mathsf{Q}_a^-, \mathsf{Q}_b^+, \mathsf{Q}_b^-)$ is a *precondition* of an action in the domain of any of the action models we need for the translation.

We first define the action model for the call ab^-, as it is easier. In this case, all agents know that the call between a and b takes place. They only do not know the value of the exchanged secrets.

Definition 18 (Action model for ab^-) *The action model* U^{ab-} *consists of a domain containing different actions for all preconditions of type* $\delta(\mathsf{Q}_a^+, \mathsf{Q}_a^-, \mathsf{Q}_b^+, \mathsf{Q}_b^-)$*. Agents other than* a, b *have the universal accessibility relation on this action model and agents* a, b *have identity accessibility relation. (There is no designated point.)*

Simplifications are possible, e.g., we may require that $A \in \mathsf{Q}_a$ and $B \in \mathsf{Q}_b$; but this does not simplify matters greatly: such a simplified action model $\mathsf{U}^{ab-}_{\mathsf{simp}}$ would have the same update effect on gossip models. The corresponding action model is very large, as there are $O(2^{4n})$ different such preconditions δ. The action model satisfies that all actions are mutually exclusive and that the union of all preconditions is the trivial formula. So always exactly one action fires, and the result is a refinement of the gossip model (no states are eliminated or duplicated, it is merely the case that the accessibility relations for the agents a and b are more refined).

The reduction axiom for knowledge after update, associated with this action model U^{ab-}, can be computed from the reduction axiom $[\mathsf{U}, \mathsf{s}]K_a\varphi \leftrightarrow (\mathsf{pre}(\mathsf{s}) \rightarrow \bigwedge_{\mathsf{s} \sim_a \mathsf{t}} K_a[\mathsf{U}, \mathsf{t}]\varphi)$, and taking into account that $[\mathsf{U}]\varphi \leftrightarrow \bigwedge_{\mathsf{s} \in \mathsf{U}}[\mathsf{U}, \mathsf{s}]\varphi$. We get

Definition 19 (Axioms for action model U^{ab-})

$$\begin{array}{lcll} [\mathsf{U}^{ab-}]K_c\varphi & \leftrightarrow & K_c[\mathsf{U}^{ab-}]\varphi & \textit{for } c \neq a, b \\ [\mathsf{U}^{ab-}]K_a\varphi & \leftrightarrow & \bigwedge_{\mathsf{s} \in \mathsf{U}^{ab-}}(\mathsf{pre}(\mathsf{s}) \rightarrow K_a[\mathsf{U}^{ab-}, \mathsf{s}]\varphi) & \\ [\mathsf{U}^{ab-}]K_b\varphi & \leftrightarrow & \bigwedge_{\mathsf{s} \in \mathsf{U}^{ab-}}(\mathsf{pre}(\mathsf{s}) \rightarrow K_b[\mathsf{U}^{ab-}, \mathsf{s}]\varphi) & \end{array}$$

where $\mathsf{pre}(\mathsf{s})$ *for the action* s *associated with* $\delta(\mathsf{Q}_a^+, \mathsf{Q}_a^-, \mathsf{Q}_b^+, \mathsf{Q}_b^-)$ *is just that formula.*

Definition 20 (Action model for ab^0 and ab^+) *For call* ab^0*, we get* $\binom{n}{2} = n(n-1)/2$ *copies of the action model for* ab^-*. Let us consider events* (s, ab) *instead of* s*, with the accessibility relation between* (s, ab) *and* (t, ab) *as for* s *and* t *in* U^{ab-}*, and further* $(\mathsf{s}, ab) \sim_e (\mathsf{t}, cd)$ *if* $e \neq a, b, c, d$*. The point of this action model for call ab is the pair* (s, ab)*. For the call* ab^+*, we merely need to add another 'no call happens' alternative to the action model with precondition true, again indistinguishable from a call ab by any agent other than a and b.*

Similarly to the case for ab^-, we can compute corresponding reduction axioms. This paves the way for a completeness result by standard reduction techniques:

Proposition 21 *The logics with call actions ab^-, ab^0, ab^+ and* skip *have complete axiomatizations.*

From now on, we consider calls ab^0 only, written simply as ab. Our definitions equally apply to protocols with ab^- and ab^+ calls—the adaptations are minor.

Protocols are programs satisfying certain additional constraints, and that model (informally) ways to distribute all secrets over all agents. First, the semantics of complex programs.

Definition 22 (Interpreting complex programs) *The interpretation of calls on pointed gossip models (G, M) of Definition 12 is lifted to arbitrary programs π in a standard way, where again we take into account that for all $\varphi \in \mathcal{L}_{Kw}$, either φ or $\neg\varphi$ is a model validity on a gossip situation: $M \models [\pi]\psi$ iff for all M' such that $M[\![\pi]\!]M'$, $M' \models \psi$.*

$$\begin{array}{lcll}
[\![?\varphi]\!] & = & \{((G,M)(G,M))\} & \textit{iff}\, G,M \models \varphi \\
[\![?\varphi]\!] & = & \emptyset & \textit{iff}\, G,M \models \neg\varphi \\
[\![\pi;\pi']\!] & = & [\![\pi]\!] \cdot [\![\pi']\!] & \\
[\![\pi \cup \pi']\!] & = & [\![\pi]\!] \cup [\![\pi']\!] & \\
[\![\pi^*]\!] & = & [\![\pi]\!]^* &
\end{array}$$

3 Epistemic protocols for gossip

Our epistemic protocols should be seen on a par with *knowledge programs* [3] and with *epistemic planning* [2]. Every agent has its own program where the actions chosen by the agent are conditional on what the agent knows. (An agent also knows its own ignorance.) We assume that an individual agent program of agent a specifies under which conditions a would like to make a call, and to what kind of partner. In case conditions for different agents apply, an arbiter will choose whose request is granted.

Protocol 1 is not an epistemic protocol: the agents appearing in the protocol are *names* and not *variables*, and the actions are selected independently of what an agent knows. Take the case for $n = 6$: although the first three calls could result from an epistemic protocol, in the next step, c has to call d. But there is no way for c to choose his partner d: how would c know that d has been idle from the start?

So we assume sets of variables $\{x, y, z, \dots\}$ and $\{X, Y, Z, \dots\}$ over agents and secrets. We consider a language $\mathcal{L}_\Pi$ for protocols which is obtained from Definition 1 by replacing A by X, a by x and b by y. Define the free variables $FV(X) = \{x\}$, $FV(K_x\varphi) = \{x\} \cup FV(\varphi)$, and $FV([xy]\varphi) = \{x, y\} \cup FV(\varphi)$. Moreover, $FV(\neg\varphi) = FV(\varphi)$ and $FV(\varphi_1 \wedge \varphi_2) = FV(\varphi_1) \cup FV(\varphi_2)$. We also allow the following constructs in the language, with the associated free variables for them:

$$FV(\bigwedge_{z \in \mathsf{A}} \varphi) = FV(\bigvee_{z \in \mathsf{A}} \varphi) = FV(\cup_{z \in \mathsf{A}}\varphi) = FV(\varphi) \setminus \{z\}$$

We say that ψ is about x and y, and write $\psi(x, y)$ if $FV(\psi) = \{x, y\}$. As an example, take $\psi(x, y) = K_x \bigvee_{z \in \mathsf{A}}(Kw_y Z \wedge \neg Kw_x Z)$ (x knows that y knows a secret that x does not know).

Definition 23 (Epistemic protocol) *To define an epistemic protocol Π, we assume $\psi(x, y)$ to be a formula about x and y. We then define for every Π a* calling condition *(for x to call y) $cc(x, y, \Pi)$ as*

$$cc(x, y, \Pi) = K_x\psi(x, y)$$

An epistemic gossip protocol *Π is then a program of the form*

$$\texttt{while} \bigvee_{x,y \in \mathsf{A}} cc(x, y, \Pi) \text{ do} \bigcup_{x,y \in \mathsf{A}} (?cc(x, y, \Pi)\,; xy) \qquad (5)$$

In words: as long as there are two agents x and y for which the condition is true, choose such a pair and let them make the call. Less restrictive definitions of protocols are definitely plausible: the termination condition might be different from the calling condition, and the calling condition might be different for different agents, for example. Since $(K_x\psi_1 \vee K_x\psi_2)$ is equivalent to $K_x(K_x\psi_1 \vee K_x\psi_2)$, our definition does allow for test which are based on cases.

Definition 24 (Extension and situation sequences of a protocol) *The* extension *$\Sigma(\Pi)$ of a protocol Π is the set of its execution sequences of calls. The gossip situation sequences $GSS(\Pi)$ are all sequences of gossip situations it generates.*

If protocols have the same extension, they obviously have the same meaning and situation sequences. But protocols may have the situation sequences and still have different extensions: Obviously the two call sequences $ab; ac; ab$ and $ab; ac; bc$ are different, yet they generate the same gossip situation sequences, i.e. $A.B.C \rightarrow AB.AB.C \rightarrow ABC.AB.ABC \rightarrow ABC.ABC.ABC$.

We now present some examples. Since a protocol is completely determined by its condition $cc(x, y, \Pi)$, we only give those conditions for the protocols here. Obviously, there is a connection between the logical strength of this condition for Π and the set of its extension:

Proposition 25 *For any protocols Π and Π',*

$$\models cc(x, y, \Pi) \rightarrow cc(x, y, \Pi') \textit{ implies } \Sigma(\Pi) \subseteq \Sigma(\Pi')$$

In order to make a given protocol common knowledge to all agents, we need to slightly adjust the semantics of calls, that is, for each protocol Π, we have to replace $\mathcal{S}^0$ of Definition 12 by

$$\mathcal{S}^0_\Pi = \{N^{cd} \mid N \in \mathcal{S} \;\&\; cd \in \Pi(N)\} \qquad (6)$$

where $\Pi(N)$ is the set of calls that are enabled by the protocol Π in N. Syntactically, we need to restrict the language: $\mathcal{L}_K(\Pi)$ is obtained by adapting the object language $\mathcal{L}_K$ in such a way, that the only program π that occurs is the program of the form (5).

Protocol 3 (Learn New Secrets (LNS))

$$cc(x, y, \Pi_3) = K_x \neg Kw_x Y$$

Protocol 3 is the same as Protocol 2. The condition for x to call y in Π_3 in words is simple: x calls any agent whose secret he yet does not know. The minimum length of a call sequence for this protocol is $2n - 4$ and the maximum length is $n(n - 1)/2$. For the minimum, consider the following sequence, which is a variant of Protocol 1: fix four different agents a, b, c, d from A. First, a makes $n - 4$ calls to all $\mathsf{A} \setminus \{a, b, c, d\}$. Then, the calls $ab; cd; ac; bd$ are made. Finally all agents from $\mathsf{A} \setminus \{a, b, c, d\}$ call agent b. For the maximum, the sequence that constitutes (3) is an example.

Protocol 4 (Known Information Growth (KIG))

$$cc(x, y, \Pi_4) = K_x(\bigvee_{z \in \mathsf{A}} Kw_x Z \,\nabla\, Kw_y Z)$$

Here, ∇ denotes exclusive or. In order for x to call y, condition $cc(x, y, \Pi_4)$ requires that x should know that some secret is currently known by only one of x and y: So, x will call y if x knows this call will produce new knowledge. Contrast this with $cc(x, y, \Pi_{4.dr})$: under the latter, x is allowed to call y if there is some secret Z of which x knows that only one of x and y knows it. The condition

$cc(x, y, \Pi_4)$ is a knowledge *de dicto* requirement: let us show that our language also allows for a knowledge *de re* condition:

$$cc(x, y, \Pi_{4.dr}) = K_x \bigvee_{z \in \mathsf{A}} K_x(Kw_x Z \nabla Kw_y Z)$$

Note that this condition is equivalent to $\bigvee_{z \in \mathsf{A}} K_x(Kw_x Z \nabla Kw_y Z)$. To appreciate the difference between the two KIG protocols, suppose we have four agents and a call sequence starting with $\sigma = ab; bc; cd$. After this sequence, $cc(a, b, \Pi_4)$ holds (a knows he was not involved in the last two calls, so b must have learned something new), but $cc(a, b, \Pi_{4.dr})$ does not (a does not know *what* b has learned). However, after $\sigma; bd$, agent a *does* know that b must have learned C, and so now both $cc(a, b, \Pi_4)$ and $cc(a, b, \Pi_{4.dr})$ are true. This also demonstrates a difference between the LNS and the KIG protocols: the latter two protocols allow for two agents a and b to call each other more than once in a sequence, the former does not.

On the one hand, the condition for KIG (unless explicitly specified, we assume *de dicto* versions of protocols) assumes a cooperative agent x: even if he knows that only y will benefit from the call, x will make it. However, on the other hand those conditions may look rather strong: under certain circumstances, it may be reasonable for x to call y even if x is not sure this will result in growth of information. Let us write $\hat{K}_\varphi = \neg K_a \varphi \wedge \neg K_a \neg\varphi$, i.e., for a, φ is an epistemic possibility. In standard epistemic logic, $K_a \hat{K}_a \psi \leftrightarrow \hat{K}_a \psi$. We now define the two final epistemic protocols.

Protocol 5 (Possible Information Growth (PIG))

$$cc(x, y, \Pi_5) = K_x \hat{K}_x (\bigvee_{z \in \mathsf{A}} Kw_x Z \nabla Kw_y Z)$$

$$cc(x, y, \Pi_{5.dr}) = K_x \bigvee_{z \in \mathsf{A}} K_x \hat{K}_x (Kw_x Z \nabla Kw_y Z)$$

In words, x is allowed to call y, if, according to $cc(x, y, \Pi_5)$, x considers it possible that some secret becomes shared knowledge by such a call. ($\Pi_{5.dr}$ is the *de re* variant: note that $cc(x, y, \Pi_{5.dr})$ is equivalent to $\bigvee_{z \in \mathsf{A}} \hat{K}_x(Kw_x Z \nabla Kw_y Z)$).

Notice that $\Pi_{5.dr}$ (and, therefore Π_5, see Proposition 26) may loop and therefore termination is not guaranteed! For example, for four agents, consider the following infinite sequence $\sigma \in \Sigma(\Pi_{5.dr})$: $\sigma = ab; cd; ab; cd; ab; \ldots$. After every even round (i.e., after every call cd) in σ, we have $K_a \hat{K}_a (Kw_a C \nabla Kw_b C)$, i.e., a considers it possible that b has learned C, while C is unknown to a, namely if the second call were bc. Therefore, after $ab; cd$, ab can be chosen according to the protocol.

Unlike the PIG protocols, both KIG protocols terminate, as is argued as follows. Consider the set $S = \{(a, B) \mid \neg Kw_a B\}$. Initially, $|S| = n(n-1)$. The calling condition for the KIG protocols implies that $S \neq \emptyset$, and, moreover, every round of the protocol removes at least one member from S.

Proposition 26 *Let* Π_1 *denote Protocol 1:*

1. $\Sigma(\Pi_3) \subsetneq \Sigma(\Pi_{4.dr}) \subsetneq \Sigma(\Pi_4) \subsetneq \Sigma(\Pi_{5.dr}) \subsetneq \Sigma(\Pi_5)$
2. $\Sigma(\Pi_1) \not\subseteq \Sigma(\Pi_3)$ *and* $\Sigma(\Pi_1) \subsetneq \Sigma(\Pi_{5.dr})$

Protocol 3 and the protocols for KIG are different. Consider the call sequence $\sigma = ab; bc; bd; cd$. Then $\sigma; ab$ is not the start of a sequence in $\Sigma(\Pi_3)$ (two agents never call each other twice). But it *is* a start under KIG: after σ, we have $K_a Kw_b D$ (since a was not involved in the last three calls, he knows that b has learned D).

Proposition 27 *Let* $\Pi =^s \Pi'$ *denote that the shortest sequence in* $\Sigma(\Pi)$ *has the same length as the shortest sequence in* $\Sigma(\Pi')$*. Then:*

$$\Pi_1 =^s \Pi_3 =^s \Pi_4 =^s \Pi_5$$

Let the expected execution length $EL(\Pi)$ *be the average length of* $\sigma \in \Sigma(\Pi)$ *if this set is finite, and* ∞ *otherwise. Let* $\Pi <^e \Pi'$ *denote that either* $EL(\Pi) < EL(\Pi') \in \mathbb{N}$ *, or* $EL(\Pi) \neq \infty = EL(\Pi')$*.*

$$\Pi_1 <^e \Pi_3 \text{ and } \Pi_4 <^e \Pi_5$$

The following can be readily checked by hand:

Proposition 28 *For LNS and three agents, there are 24 different call sequences, all of length 3, and 6 different gossip situation sequences. For KIG (*de dicto*), the numbers are 96 and 6, respectively. The LNS protocol for four agents generates 624 different call sequences.*

Proposition 29 *For every execution call sequence of Protocol 5 there is an execution sequence of Protocol 3 with the same meaning (i.e., inducing same information transitions, see Definition 24).*

4 Conclusion

We made a first step in proposing and analysing *epistemic* gossip protocols, where an agent will call another agent based on its current knowledge. Such protocols may take longer to terminate than non-epistemic, globally scheduled, protocols. We described various such protocols, we gave some logical properties, and we modelled them in action model logic.

Concerning further research, we conjecture and wish to prove that the shortest execution length cannot be guaranteed by *any* epistemic protocol. Moreover, for a number of epistemic protocols, we wish to make an exhaustive analysis of execution lengths and to have a tool that can help us demonstrate some basic facts for small groups of agents. We intend to develop epistemic gossip protocols for parallel calls, and also, to investigate epistemic *broadcast* protocols (here, one agent communicates all his secrets to all others). Other challenging questions involve a network structure for the communication, which may be known (or not) to the agents. It is interesting to drop the assumption of uniformity of protocols, and address strategic issues, for example: can an agent ensure he is the first to know all secrets, or, for that matter, not the last?

ACKNOWLEDGEMENTS

We thank the referees for their comments. Hans van Ditmarsch is also affiliated to IMSc, Chennai, as an associated researcher. He acknowledges support from ERC starting grant EPS 313360.

REFERENCES

[1] A. Baltag and L.S. Moss, 'Logics for epistemic programs', *Synthese*, **139**, 165–224, (2004). Knowledge, Rationality & Action 1–60.

[2] T. Bolander and M.B. Andersen, 'Epistemic planning for single and multi-agent systems', *Journal of Applied Non-classical Logics*, **21(1)**, 9–34, (2011).

[3] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi, *Reasoning about Knowledge*, MIT Press, Cambridge MA, 1995.

[4] S.M. Hedetniemi, S.T. Hedetniemi, and A.L. Liestman, 'A survey of gossiping and broadcasting in communication networks', *Networks*, **18**, 319–349, (1988).

[5] C.A.J. Hurkens, 'Spreading gossip efficiently', *Nieuw Archief voor Wiskunde*, **5/1(2)**, 208–210, (2000).

[6] R. Tijdeman, 'On a telephone problem', *Nieuw Archief voor Wiskunde*, **3(XIX)**, 188–192, (1971).

[7] H. van Ditmarsch, *Knowledge games*, Ph.D. dissertation, University of Groningen, 2000. ILLC Dissertation Series DS-2000-06.