Completeness and Decidability of Protocol-Dependent Knowledge in Gossip

Hans van Ditmarsch[1], Malvin Gattinger[2], Wouter Smit[2]

[1]CNRS, IRIT, University of Toulouse, France

[2]ILLC, University of Amsterdam, The Netherlands

Presented at
DaLí 2025: The 6th Workshop on Dynamic Logic - New Trends and Applications
hosted by Shaanxi Normal University, Xi'an, P.R. China

21 October 2025

The Gossip Problem

Classical Problem Definition

- A finite number of n agents hold 1 *secret* each.
- Agents interact by *calling* 1-on-1.
- They share *all* secrets that they know.
- Non-involved agents know that *some* call takes place.
- An agent becomes an *expert* if they know all n secrets.

Goal of Gossip

"Everyone knows everything"
$\rightarrow$ Find the shortest sequence of calls to make all agents experts.

Application $\rightarrow$ Spreading information in distributed systems.

Tijdeman, *On a Telephone Problem* (1971)

How To Gossip

- Call other agents randomly.
- Be civil, use protocols.

Examples of Protocols

Learn New Secrets	– call somebody whose secret you don't know
Call Me Once	– call every agent only once
Tell New Secrets	– call somebody if they don't know your secret

$\rightarrow$ Known as *epidemic protocols* in distributed systems.

Hedetniemi et al, *A survey of gossiping and broadcasting in communication networks* (1988)

Epistemic Protocols

Agents must know when the condition holds to execute the call.

Tell New Secrets

*"Call somebody if **they** don't know your secret."*

- **How do I know what others know?**

Definition (Epistemic Protocols)

When a protocol condition holds, the acting agent knows it does.

$$P_{ab} \to K_a P_{ab}$$

$\to$ **Epistemic logic as a tool for researching gossip protocols.**

The Basic Language of Gossip

Definition (Basic Language – $\mathcal{L}$)

For a finite set of agents $a, b \in Ag$, let

$$\varphi ::= S_a b \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_a\varphi \mid [ab]\varphi$$

- $S_a b$ – *"Agent a knows the secret of agent b"*.
- $K_a\varphi$ – *"Agent a knows that* φ *is true"*.
- $[ab]\varphi$ – *"*φ *is true after call ab"*.

Defining a Protocol

We define P by *protocol conditions* P_{ab} for all agent pairs $a \neq b$.

Call ab is P-legal if P_{ab} holds.

Example (Learn New Secrets)

$\mathrm{LNS}_{xy} := \neg S_x y$ for all x, y

Epistemic and *symmetric*.

Example ('only call *ab* may happen')

$P_{ab} := \top$
$P_{xy} := \bot$ for all other x, y

Epistemic but *not symmetric*.

$\rightarrow$ **Protocol conditions can be viewed as subformulas of** K^P

Expressing protocol-dependent knowledge

Definition (Language $\mathcal{L}^{\mathbb{P}}$)

$$\varphi ::= S_a b \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{K}_{\mathbf{a}}^{\mathbf{P}}\varphi \mid [ab]\varphi$$

Protocol-Dependent Knowledge

- $K_a^P \varphi$ – *"a knows φ given common knowledge of protocol P"*.
- Restrict the epistemic relation to P-permitted call sequences.
- Allows combinations of arbitrary protocols:

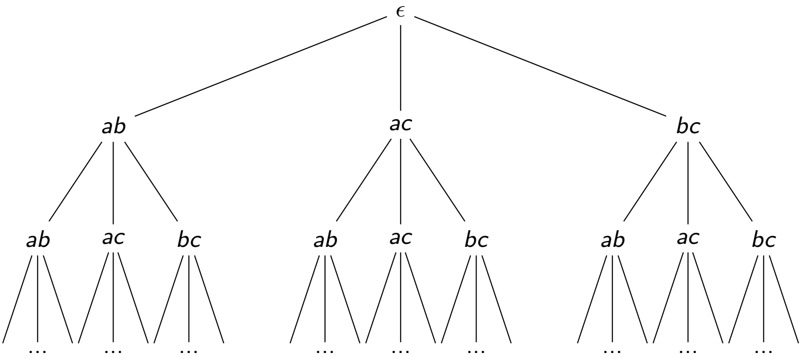
$$K_a^P \varphi \wedge K_a^Q \neg\varphi$$

---

van Ditmarsch et al, *Strengthening Gossip Protocols using Protocol-Dependent Knowledge* (2019)

Gossip Models

A gossip model

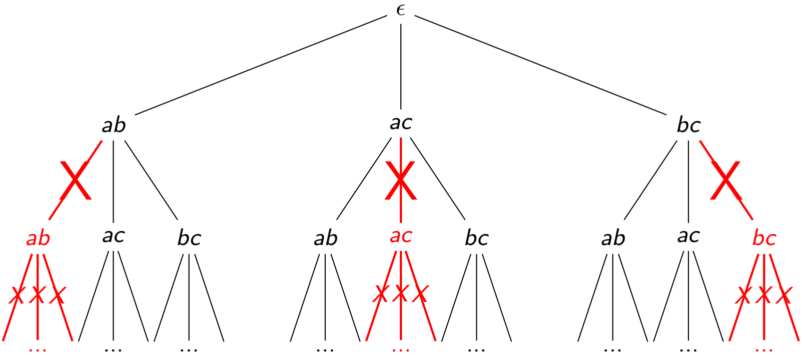


Edges describe *calls*.

The root is the initial setting and empty call sequence ϵ.

Each node is a *call sequence* defined by the path from the root.

Protocol-dependent knowledge in the gossip model



The **Call Me Once** (CMO) protocol.

Red call sequences are CMO-illegal.

K^{CMO} has no epistemic relations to these points in the model.

Defining Gossip Models

We define gossip models in two steps.

1. Separate the initial setting from the rest of the model
2. Allow arbitrary initial settings

H. van Ditmarsch, *The logic of gossiping* (2020)

Initial Models and Gossip Models

We divide the model in two parts: the **initial** and **induced** model.

Initial Model

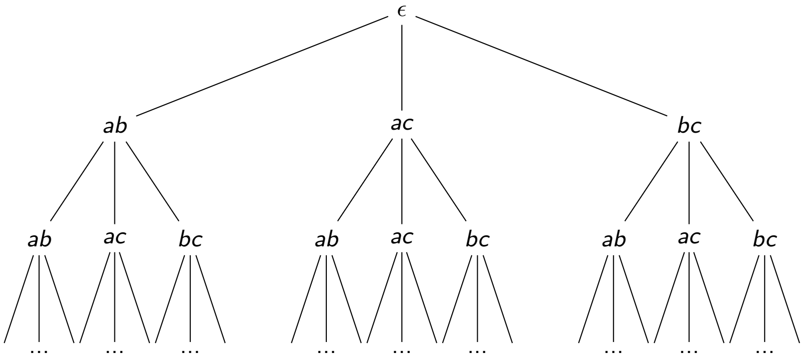
1. Describes the starting point before calls:
   - the initial **distribution of secrets**, and
   - the **knowledge of agents** thereof

(Induced) Gossip Model

1. Adds calls to an initial model
2. Based completely on the initial model

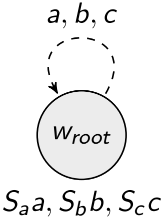
van Ditmarsch et al, *The logic of gossiping* (2020)

Initial Models and Gossip Models



The root ϵ forms the initial model.

The Initial Root Model



Each Agent only knows their own secret.
All agents know that this is the case.

Arbitrary Initial Models

Classic Initial Setting

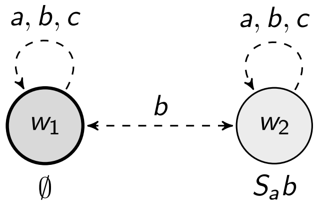
1. Everybody knows only their own secret ($S_a a$ for all a)
2. This is common knowledge among the agents

Generalised Initial Models

1. Arbitrary initial secret distribution
2. Arbitrary initial knowledge

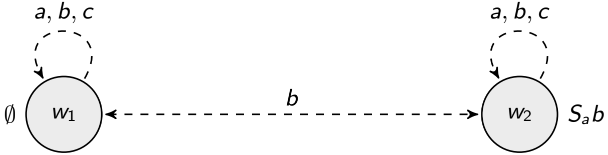
Arbitrary Initial Models

Example



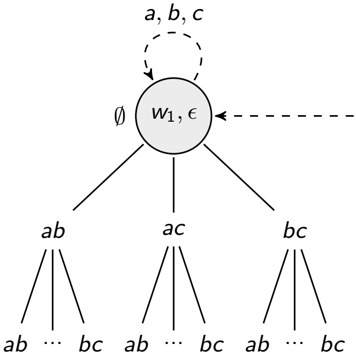
$S_a a, S_b b, S_c c$ hold in all worlds. The actual world is w_1.
Agent b does not know if a knows her secret, while a and c do.

Adding Calls to get a Gossip Model



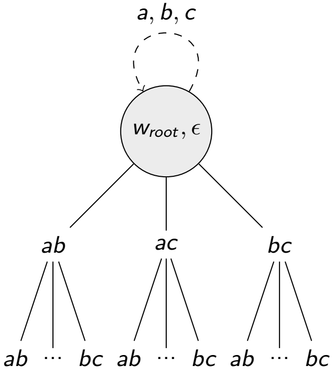
The initial model I.

Adding Calls to get a Gossip Model



A gossip model $M(I)$ induced from the initial model I.

The Tree Model



The Tree Model $M_{\mathcal{T}}$

The gossip model for the classical initial setting.

Induced from the Initial Root Model $I_{\mathcal{R}}$

Model Classes

Initial Models

$\mathcal{I}$ - Class of Initial Models

$\mathcal{R}$ - Singleton initial root model $I_{\mathcal{R}}$

Gossip Models

$\mathcal{G}$ - Class of (induced) Gossip Models

$\mathcal{T}$ - Singleton tree model $M_{\mathcal{T}}$

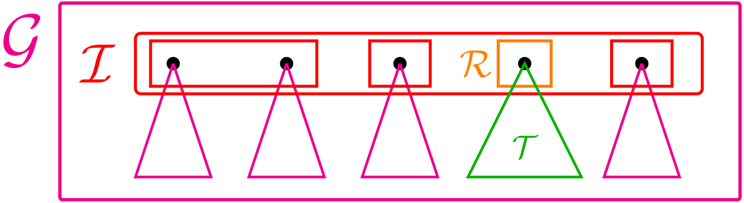


Figure: The classes $\mathcal{I}$, $\mathcal{G}$, $\mathcal{R}$, and $\mathcal{T}$.

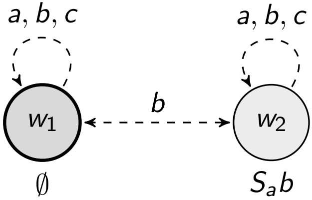
Protocol-Dependent Knowledge in Initial Models

Initial models cannot violate any protocol.

They have **protocol invariance**:

$$\textbf{PI}: K^P\varphi \rightarrow K^Q\varphi$$

Figure: An initial model with one epistemic relation for all protocols



Axiomatisation for Initial Models

Table: Rules and axioms of $\vdash_{\mathcal{R}}$. Omitting **Only** produces $\vdash_{\mathcal{I}}$.

Prop	propositional tautologies	**K**	$K_a^P(\varphi \to \psi) \to (K_a^P\varphi \to K_a^P\psi)$
MP	$\vdash \varphi, \vdash \varphi \to \psi$ imply $\vdash \psi$	**T**	$K_a^P\varphi \to \varphi$
Sub	$\vdash \varphi \leftrightarrow \psi$ implies $\vdash \chi \leftrightarrow \chi[\varphi/\psi]$	**4**	$K_a^P\varphi \to K_a^P K_a^P\varphi$
Own	$S_a a$	**5**	$\neg K_a^P\varphi \to K_a^P\neg K_a^P\varphi$
Only	$O_a a$	**Nec**	$\vdash \varphi$ implies $\vdash K_a^P\varphi$
PFi	$S_a b \to K_a^P S_a b$		
NPi	$\neg S_a b \to K_a^P\neg S_a b$	**PI**	$K^P\varphi \to K^Q\varphi$

$\to$ **Completeness using canonical model construction.**

Call-Free Formulas

Initial Models do not describe calls.

$\vdash_{\mathcal{R}}$ and $\vdash_{\mathcal{I}}$ are only complete for the call-free fragment $\mathcal{L}^{\mathbb{P}}_{-}$.

Using **Call Reductions** we rewrite any formula φ to be call-free.

$$\models_{\mathcal{G}} \varphi \leftrightarrow \mathsf{cr}(\varphi)$$

Call-Free Formulas

Table: Call Reduction Validities on Gossip Models ($\mathcal{G}$).

Call Basics		Call Effects		
Con	$[ab](\varphi \wedge \psi) \leftrightarrow ([ab]\varphi \wedge [ab]\psi)$	**Eff**	$[ab]S_c d \leftrightarrow (S_a d \vee S_b d)$	$c \in \{a, b\}$
Fnc	$[ab]\neg\varphi \leftrightarrow \neg[ab]\varphi$	**Ext**	$[ab]S_c d \leftrightarrow S_c d$	$c \notin \{a, b\}$

Calls and Protocol-Dependent Knowledge

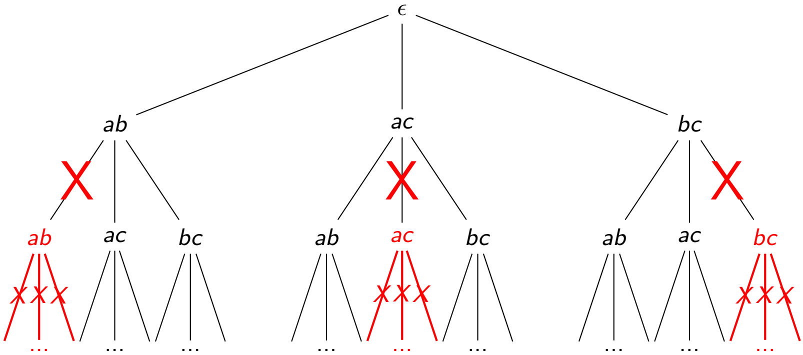
Obs$_1$	$[ab]K_a^P\varphi \leftrightarrow (P_{ab} \to \bigvee_{R \subseteq \mathbb{S}}(O_b R \wedge K_a^P(P_{ab} \to (O_b R \to [ab]\varphi))))$	
Obs$_2$	$[ab]K_b^P\varphi \leftrightarrow (P_{ab} \to \bigvee_{R \subseteq \mathbb{S}}(O_a R \wedge K_b^P(P_{ab} \to (O_a R \to [ab]\varphi))))$	
Pri	$[ab]K_c^P\varphi \leftrightarrow (P_{ab} \to \bigwedge_{d,e \neq a} K_c^P(P_{de} \to [de]\varphi))$	$c \notin \{a, b\}$

An axiomatisation for Gossip Models

Extending to Gossip Models is not possible

Axiomatisation for initial models but not for gossip models.
We **cannot** extend this axiomatisation:

1. **PI** no longer holds after calls are made.
2. Gossip models are not **S5**.



An axiomatisation for Gossip Models

Truth in gossip models and initial models are closely related.

$I, w \models \mathrm{cr}([\sigma]\varphi)$	**Truth in the initial model**
$\Updownarrow$	*Root states equivalent to the initial model*
$M(I), (w, \epsilon) \models \mathrm{cr}([\sigma]\varphi)$	**Truth in root of gossip model**
$\Updownarrow$	*Validity of call reductions*
$M(I), (w, \epsilon) \models [\sigma]\varphi$	**Truth in root of gossip model**
$\Updownarrow$	*Truth preserved under calls*
$M(I), (w, \sigma) \models \varphi$	**Truth anywhere in the gossip model**

Idea:
Check if φ holds after each call sequence σ using $\vdash_{\mathcal{I}}$ and $\vdash_{\mathcal{R}}$.

An axiomatisation for Gossip Models

Idea:
Check if φ holds after each call sequence σ using $\vdash_{\mathcal{I}}$ and $\vdash_{\mathcal{R}}$.

Definition (Proof System $\mathcal{G}$)

$$\vdash_{\mathcal{G}} \varphi \iff \forall \sigma : \vdash_{\mathcal{I}} \mathsf{cr}([\sigma]\varphi)$$

Problem:
There are infinitely many call sequences.

An axiomatisation for Gossip Models

Problem:
There are infinitely many call sequences.

Solution:
Bound the number of call sequences that need to be verified.

Bound by modal degree *(m-bisimulation)*

1. Finitely many atoms ($S_a a$) for n agents holding n secrets.
2. Let $f(m)$ be the finitely many semantically different formulas up to modal degree m.
3. For φ with modal degree $d(\varphi) = m$ we only need to check call sequences of length $|\sigma| \leq f(m)$.

Proof System for Gossip Models

Definition (Proof System $\vdash_{\mathcal{G}}$)

Let $\varphi \in \mathcal{L}^{\mathbb{P}}$ and $m = d(\varphi)$. We define $\vdash_{\mathcal{G}}$ as follows, where $f(m)$ is the number of m-bisimilarity classes.

$$\vdash_{\mathcal{G}} \varphi \iff \forall \sigma : |\sigma| \leq f(m) \text{ we have } \vdash_{\mathcal{I}} \mathrm{cr}([\sigma]\varphi)$$

Definition (Proof System $\vdash_{\mathcal{T}}$)

Let $\varphi \in \mathcal{L}^{\mathbb{P}}$ and $m = d(\varphi)$. We define $\vdash_{\mathcal{T}}$ as follows, where $f(m)$ is the number of m-bisimilarity classes.

$$\vdash_{\mathcal{T}} \varphi \iff \forall \sigma : |\sigma| \leq f(m) \text{ we have } \vdash_{\mathcal{R}} \mathrm{cr}([\sigma]\varphi)$$

Results & Conclusion

Summary

Results

- 4 proof systems for protocol-dependent knowledge in gossip.
- Each sound, complete, and decidable.
- Builds on *van Ditmarsch (2019)* and *van Ditmarsch (2020)*.
- $\vdash_{\mathcal{G}}$ and $\vdash_{\mathcal{T}}$ defined in terms of $\vdash_{\mathcal{I}}$ and $\vdash_{\mathcal{R}}$ without extending.
- The protocol-dependent knowledge modality K^P is strictly more expressive than the standard modality K.

Future Work

- Study protocol-dependent knowledge outside of gossip.