Reasoning about Gossip

Hans van Ditmarsch
CNRS

- Gossip protocol

Materials found on http://reasoningaboutgossip.eu

Call Condition and Termination Condition

Let us begin slightly vague:

> *A gossip protocol is a procedure that, until a termination condition is satisfied, selects a call for execution that satisfies a call condition.*

Call condition: Assume a set $\mathcal{G}$ of gossip graphs containing G, and a call sequence σ. We recall pair (G, σ) is a gossip state.

- A call condition for a call ab is a property P_{ab} that can be determined with respect to gossip state (G, σ), and that is epistemic and symmetric. Assume a knows the number of b.
- epistemic: P_{ab} holds for all (H, τ) such that $(H, \tau) \sim_a (G, \sigma)$.
- symmetric: replacing designated a, b in P_{ab} by c, d gets P_{cd}.

Termination condition: An agent who knows all secrets is an expert. All agents are experts is a termination condition. An agent who knows that all agents know all secrets is a super expert. *All agents are super experts* is another termination condition.

Gossip Protocol

Given is a set $\mathcal{G}$ of initial gossip graphs with $G \in \mathcal{G}$ designated. A gossip protocol P is a non-deterministic algorithm with G and the empty sequence ϵ as input and a call sequence σ as output. The typical termination condition is that all agents are experts.

> **Gossip Protocol** *While not all agents are experts, choose $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and P_{ab} holds, and execute call ab.*

Protocol-permitted The condition that b is a neighbour of a is not considered part of the protocol condition. A call ab is possible if b is a neighbour of a. A call sequence is possible if it consists of possible calls. Given G and σ, possible call ab is P-permitted (protocol-permitted) if P_{ab} holds. A call sequence is P-permitted if all calls in the sequence are P-permitted (ϵ is always P-permitted).

Protocol Extension Given a set $\mathcal{G}$ of gossip graphs and $G \in \mathcal{G}$, the extension $\mathrm{P}(G)$ of protocol P on G is the set of P-permitted call sequences on G. We write $\mathrm{P}(\mathcal{G}) \subseteq \mathrm{P}'(\mathcal{G})$ if $\mathrm{P}(G) \subseteq \mathrm{P}'(G)$ for all $G \in \mathcal{G}$; $\mathrm{P} \subseteq \mathrm{P}'$ if $\mathrm{P}(\mathcal{G}) \subseteq \mathrm{P}'(\mathcal{G})$ for all $\mathcal{G}$ (protocol $=$ extension).

Different Views on Distributed Gossip Protocols

Gossip Protocol *While not all agents are experts, choose $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and* P_{ab} *holds, and execute call ab.*

An alternative formulation avoids abnormal termination ('getting stuck'):

While not all agents are experts and there are $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and P_{ab} *holds, choose $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and* P_{ab} *holds, and execute call ab.*

If we omit the termination condition we require stabilization:

Choose $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and P_{ab} *holds, and execute call ab.*

Different Views on Distributed Gossip Protocols

Gossip Protocol *While not all agents are experts, choose $a, b \in A$ with $a \neq b$ such that b is a neighbour of a and P_{ab} holds, and execute call ab.*

The distributed nature of gossip protocol appears as follows:

Each $a \in A$ runs ***a*-program**: choose $b \in A$ with $a \neq b$ such that b is a neighbour of a and P_{ab} holds, and execute call ab (or else fail). The environment ϵ runs **ϵ-program**: while not all agents are experts, choose $a \in A$ and execute ***a*-program**.

Again, if we delete 'while not all agents are experts' we require stabilization instead of termination.

Observation Model

Given (arbitrary) observation relations $\sim_a$ and set $\mathcal{G}$ of initial gossip graphs, the observation model $\mathcal{M}(\mathcal{G})$ consists of all pairs (G, σ) s.t. $G \in \mathcal{G}$ and σ is possible, and relations $(G, \sigma) \sim_a (H, \tau)$ and $(G, \sigma) \rightarrow (G, \sigma.ab)$ connecting gossip states (we may write $\rightarrow_{ab}$ instead of $\rightarrow$ to denote the executed call). Special cases:

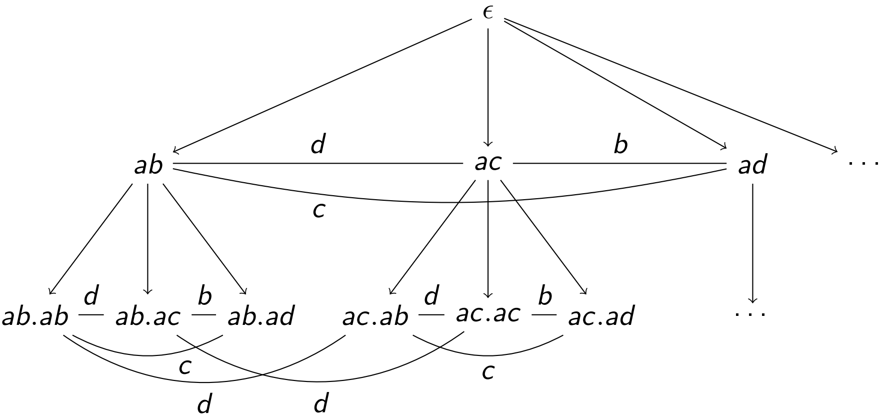
- $\mathcal{G} = \{G\}$: G is common knowledge among the agents
- $\mathcal{G}$ is the the set of all lines, all circles, all trees, ...
- $\mathcal{G} = \{I\}$: the initial secret distribution is common knowledge
- $\boldsymbol{\mathcal{S}}$: the set of all sets of initial gossip graphs ($\boldsymbol{\mathcal{I}}$: all secr. dist.)

$\mathcal{M}_{\mathsf{P}}(\mathcal{G})$ is the restriction of $\mathcal{M}(\mathcal{G})$ to protocol extension $\mathsf{P}(\mathcal{G})$. It consists of all gossip states (G, σ) such that σ is P-permitted.

We informally allow infinite call sequences denoted σ^ω. With infinite branch $\epsilon \rightarrow ab \rightarrow ab.cd \rightarrow ab.cd.ef \rightarrow \dots$ in the observation model we associate infinite call sequence $ab.cd.ef \dots$ An infinite call sequence is P-permitted if any (therefore) finite prefix is P-permitted.

Example Observation Model

Partial view of observation model for initial secret distribution ι and agents a, b, c, d. It has more branches and has infinite depth.



This was synchronous. Asychronously, $ab \sim_a ab.ab$, $ab \sim_a ab.ac$, . . .

Maximal, Fair, Successful, Terminal, Gossip Problem

Given gossip protocol P, set of initial gossip graphs $\mathcal{G}$, $G \in \mathcal{G}$, and P-permitted call sequence σ (or perm. infinite call sequence σ^ω):

- σ is **maximal** if for any call ab, $\sigma.ab$ is not permitted.
- σ^ω is **fair** if for any call ab, if for all i there is $j > i$ such that call ab is P-permitted after $\sigma^\omega|j$, then for all i there is $j > i$ such that $\sigma^\omega[j] = ab$. (σ^ω is unfair if it is not fair)
- σ is **successful** if after σ all agents are experts.
- σ is **terminal** if σ is an execution of protocol P.

Terminal may not be maximal! Further, given gossip protocol P:

- P is strongly successful on $\mathcal{G}$ if for all $G \in \mathcal{G}$, all maximal $\sigma \in \mathsf{P}(G)$ and all fair infinite $\sigma^\omega \in \mathcal{M}_\mathsf{P}(G)$ are successful.
- P is weakly successful on $\mathcal{G}$ if for all $G \in \mathcal{G}$, there is maximal $\sigma \in \mathsf{P}(G)$ or a fair infinite $\sigma^\omega \in \mathcal{M}_\mathsf{P}(G)$ that is successful.

Protocol P is wea/str successful if it is wea/str successful on $\boldsymbol{\mathcal{S}}$ (often, $\mathcal{I}$). The gossip problem is whether P is wea/str successful.

Distributed Epistemic Gossip Protocols

$$
\begin{array}{lcl}
\text{ANY}_{ab} & = & \top \\
\text{CMO}_{ab} & = & ab, ba \notin \sigma \\
\text{wCMO}_{ab} & = & ab \notin \sigma \\
\text{LNS}_{ab} & = & b \notin S_a^\sigma \\
\text{PIG}_{ab} & = & \exists \tau \sim_a \sigma, \exists c, c \in S_a^\tau \setminus S_b^\tau \text{ or } c \in S_b^\tau \setminus S_a^\tau \\
\text{KIG}_{ab} & = & \forall \tau \sim_a \sigma, \exists c, c \in S_a^\tau \setminus S_b^\tau \text{ or } c \in S_b^\tau \setminus S_a^\tau \\
\text{SPI}_{ab} & = & \text{spider: if } a \text{ calls } b, a \text{ gets the token (if any) from } b \\
\text{TOK}_{ab} & = & \text{token: if } a \text{ calls } b, a \text{ hands her token to } b
\end{array}
$$

ANY	=	any call is permitted
CMO	=	after call *ab*, *a* and *b* may not call each other
wCMO	=	after call *ab*, *a* may not call *b*
LNS	=	*a* does not know ('hold') the secret of *b*
PIG	=	*a* considers possible that *a* or *b* will learn a secret
KIG	=	*a* knows that *a* or *b* will learn a secret
SPI	=	token holders may make a call, and then keep their token
TOK	=	token holders may make a call, and then lose their token

Relations between Gossip Protocols

- $\mathsf{LNS}, \mathsf{CMO}, \mathsf{wCMO}$ only permit finite call sequences.
- $\mathsf{ANY}, \mathsf{PIG}$ permit infinite call sequences.
- ANY permits fair infinite call sequences on $\mathcal{I}$
- PIG does not permit fair infinite call sequences on $\mathcal{I}$
- $\mathsf{LNS} = \mathsf{KIG}$ (that is, extensions $\mathsf{LNS} \subseteq \mathsf{KIG}$ and $\mathsf{KIG} \subseteq \mathsf{LNS}$) for asynchronous observation relations
- all gossip protocols are successful on $\mathcal{I}$ (initial secret distr.)

Lots more to follow in the coming lectures, for synchronous relations, for arbitrary initial gossip graphs, for . . . For now, another comparison of protocol extensions:

Gossip Protocol Extension Hierarchy