Reasoning about Gossip

Hans van Ditmarsch
CNRS

overview lecture

Materials found on http://reasoningaboutgossip.~~org~~ eu

Friends Exchanging Secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

Friends Exchanging Secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

First consider four friends a, b, c, d who hold secrets (with the same name) a, b, c, d.
Four calls $ab.cd.ac.bd$ distribute all secrets.

$$a|b|c|d \stackrel{ab}{\to} ab|ab|c|d \stackrel{cd}{\to} ab|ab|cd|cd \stackrel{ac}{\to}$$
$$abcd|ab|abcd|cd \stackrel{bd}{\to} abcd|abcd|abcd|abcd$$

Now consider friends a, b, c, d, e, f with secrets a, b, c, d, e, f.
Eight calls $ae.af.ab.cd.ac.bd.ae.af$ distribute all secrets.
Minimum $2n - 4$ for $n \geq 4$. [Tijdeman 1971; Baker & Shostak 1972]

Friends Exchanging Secrets

Six friends each know a secret. They can call each other. In each call they exchange all the secrets they know. How many calls are needed for everyone to know all secrets?

First consider four friends a, b, c, d who hold secrets (with the same name) a, b, c, d.
Four calls $ab.cd.ac.bd$ distribute all secrets.

$$a|b|c|d \stackrel{ab}{\to} ab|ab|c|d \stackrel{cd}{\to} ab|ab|cd|cd \stackrel{ac}{\to}$$
$$abcd|ab|abcd|cd \stackrel{bd}{\to} abcd|abcd|abcd|abcd$$

Now consider friends a, b, c, d, e, f with secrets a, b, c, d, e, f.
Eight calls $ae.af.ab.cd.ac.bd.ae.af$ distribute all secrets.
Minimum $2n-4$ for $n \geq 4$. [Tijdeman 1971; Baker & Shostak 1972]

But how does c know that she should call d?
We want epistemic and distributed gossip protocols!

Semantics of Calls

What do agents observe of calls involving them?

Let agent a know secrets X and agent b know secrets Y.
Agents exchange all secrets they know. Yes, but, is this?? :
— a learns b knew Y, b learns a knew X, a, b now know $X \cup Y$.
— only that a, b now know $X \cup Y$.

Under the first assumption they may learn more.
Consider $bc.ab.ad$ and $bc.ab.bd.ad$. Remove ad:

- After $bc.ab$ and after $bc.ab.bd$, a knows ABC.
- After $bc.ab.ad$ and after $bc.ab.bd.ad$, a knows $ABCD$.
- The call sequences are indistinguishable for a.
- If a also learns what d knew before the call ad:
- The call sequences are distinguishable for a.

There are many other ways to exchange information (including full information).

Semantics of Calls

What do agents observe of calls not involving them?

Given agents a, b, c, d. Call ab is taking place. Agent c is not involved.

- callers are observed: c notices a and b making a call: ab.
- calls are observed: c notices when two agents call: ab, ad, bd.
- time is observed: c notices two agents **may** call: ab, ad, bd, ϵ.
- own calls are observed: c notices its own calls: ab, ad, bd, ϵ, $ab.ad$, $ab.ad.bd$, $ab.ab.ab.ab, \ldots$

An *observation relation* determines what call sequences are considered possible. An agent *knows* a proposition if the proposition holds after all indistinguishable call sequences.

[Attamah *et al.*, *Knowledge and Gossip.* ECAI 2014]
[Apt *et al.*, *Epistemic Protocols for Distrib. Gossiping.* TARK 2015]

Gossip Protocol

What is an epistemic distributed gossip protocol?

- A gossip protocol is a program of shape:

  Until all agents know all secrets, choose agents x, y such that x knows that proposition $\varphi(x, y)$ holds, and let x call y.

All agents know all secrets is a termination condition.
The proposition $\varphi(x, y)$ is a call condition.

- More distributed descriptions are possible.
- An execution call sequence of a gossip protocol is successful if it terminates with all agents knowing all secrets.
- A protocol is strongly successful if all (fair) executions are successful.
- A protocol is weakly successful if some execution is successful.

Gossip Protocol

Distributed epistemic gossip protocols with call condition.

ANY
Until all agents know all secrets, any agent x calls any agent y.
LNS/NOHO — Learn New Secrets
Until all agents know all secrets, an agent x calls an agent y whose secret it does not know.
KIG — Known Information Growth
Until all agents know all secrets, an agent x calls an agent y if x knows that x or y will learn a new secret in call xy.
PIG — Possible Information Growth
Until all agents know all secrets, an agent x calls an agent y if x considers possible that x or y will learn a new secret in call xy.

[vD, van Eijck, Pardo, Ramezanian, Schwarzentruber:
Epistemic protocols for dynamic gossip, JAL 2017]

Gossip Protocol — more on LNS

LNS/NOHO — Learn New Secrets
Until all agents know all secrets, an agent x calls an agent y whose secret it does not know.

Optimality: minimum length of sequences with LNS permitted calls:
The minimum LNS length is $2n - 4$, the maximum is $n(n-1)/2$.

For four agents, a minimal call sequence is *ab.cd.ac.bd*.
A maximal call sequence is *ab.ac.ad.bc.bd.cd*.
There are also executions with five calls, e.g. *ab.ac.ad.bd.cd*.

Expectation: the expected length of call sequences given random scheduling of LNS permitted calls is (probably) $O(n \log n)$.

NOHO: [Hedetniemi et al., Networks 1988] (and before)
LNS: [Attamah et al., ECAI 2014]
[vD, Kokkinis, Stockmarr: *Reachability and Expectation in Gossiping*.]

Reachability

- Something like $ab|ab|c$ is a secret distribution.
- Some secrets distributions are reachable by a call sequence from the initial secret distribution $a|b|c$: for example $ab|ab|c$, $abc|abc|abc$, ...
- Other secret distributions are unreachable: $a|bc|c$, ...
- Secret distributions may be reachable with some gossip protocols but not with other gossip protocols: $abcd|abcd|abc|abd$ is reachable in ANY but not in LNS.

[vD, Gattinger, Kuijer, Kokkinis: *Reachability of Five Gossip Protocols*. Workshop Reachability Problems 2019]

Dynamic Gossip

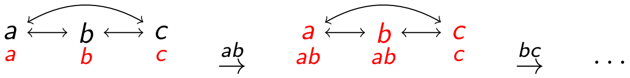
LNS — **Learn New Secrets (Dynamic)**
Until all agents know all secrets, an agent x calls an agent y whose number it knows and whose secret it does not know. (In a call, the callers exchange all secrets and all numbers they know.)

On fully connected graphs there is no difference.

Before, we displayed this as:

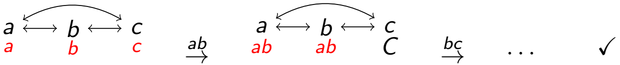
$$a|b|c \quad \stackrel{ab}{\rightarrow} \quad ab|ab|c \quad \stackrel{bc}{\rightarrow} \quad \ldots$$

Now, we display this with *gossip graphs* as:

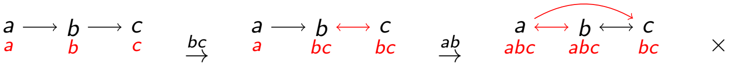


Dynamic Gossip — Learn New Secrets (with numbers)

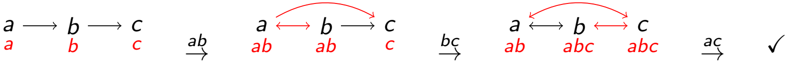
On fully connected graphs there is no difference.



On weakly connected graphs deadlock is possible. (After *bc*.*ab* agent *c* cannot call agent *a*, because *c* does not have *a*'s number.)



But on the same gossip graph deadlock can also be avoided. (After *ab*.*bc* agent *a* calls agent *c*.)



When can deadlock sometimes or always be avoided and when not?

[vD, van Eijck, Pardo, Ramezanian, Schwarzentruber. *Dynamic Gossip*. Bulletin of the Iranian Mathematical Society, 2019]

Logic and Axiomatization

Logical languages

$$
\begin{array}{lll}
\varphi & := & b_a \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_a\varphi \\
\varphi & := & b_a \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_a\varphi \mid [ab]\varphi \\
\varphi & := & b_a \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_a\varphi \mid [\pi]\varphi \\
\pi & ::= & ?\varphi \mid ab \mid \pi.\pi \mid \pi \cup \pi \mid \pi^*
\end{array}
$$

— b_a means that agent a holds (knows) the secret of b;
— $K_a\varphi$ means that agent a knows proposition φ;
— $[ab]\varphi$ means that after call ab proposition φ holds.

A modality $[ab]$ may be interpreted in various ways:
— action model
— PDL action
— communication pattern
— . . .

Logic and Axiomatization

Axiomatizations

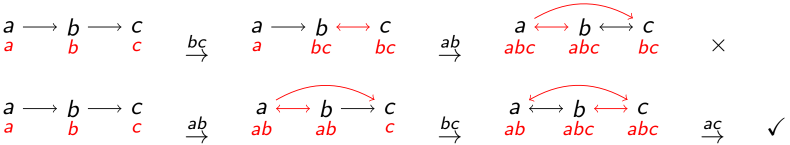
- Synchrony: only finitely many call sequences are indistinguishable from a given call sequence.
- Asynchrony: infinitely many call sequences are indistinguishable from a given call sequences . . .
- . . . but only finitely many with different informative conseq.
- so that (finitary) axiomatizations are after all possible.

Shape of the reductions (where σ is a finite call sequence):

$$
\begin{array}{lcll}
[ab]K_c\varphi & \leftrightarrow & (\ldots) \bigwedge_{de \sim_c ab} K_c[de]\varphi & \text{synchrony} \\
[ab]K_c\varphi & \leftrightarrow & (\ldots) \bigwedge_{\sigma \sim_c ab} K_c[\tau]\varphi & \text{asynchrony}
\end{array}
$$

[Attamah et al. ECAI 2014] [Apt, Wojtczak. JAIR 2018] [Gattinger. ILLC Diss. Series DS-2018-11] [vD, vd Hoek, Kuijer. The Logic of Gossiping, Artificial Intelligence Journal, 2020]

Common Knowledge of Gossip Protocols



- LNS is weakly successful on $a \longrightarrow b \longrightarrow c$: if b calls first, we get stuck; but if a calls first, any extension is successful.
- We can *strengthen* LNS on this graph to ensure strong success instead of weak success, in different ways:
- $\mathrm{LNS}^{\Box}$ is strongly successful: after σ, a calls b if a knows the number but not the secret of b and knows that there is a successful LNS extension of $\sigma.ab$.
- This assumes common knowledge of the gossip protocol and of the gossip graph, and a global clock.

[vD, Gattinger, Kuijer, Pardo. *Strengthening Gossip Protocols* . . . FLAP (IfCoLog Journal of Logics and their Applications) 2019]

Epistemic Goals

- the standard termination condition (epistemic goal) is success: everyone knows all secrets.
- a stronger epistemic goal is super success: everyone knows that everyone knows all secrets.

Example for four agents:

$ab.cd.ac.bd.$	all agents know all secrets
$ab.ad.$	agent a knows that all agents know all secrets
$bc.$	agent b knows that all agents know all secrets
cd	agents c, d know that all agents know all secrets

If agents only communicate secrets, super success is all they can get. An optimal call sequence consists of $n - 2 + \binom{n}{2}$ calls.

[vD, Gattinger. You can only be luck once. MSCS 2024.]

Epistemic Goals

- the standard termination condition (epistemic goal) is success: everyone knows all secrets.
- a stronger epistemic goal is super success: everyone knows that everyone knows all secrets.

Example for four agents:

$ab.cd.ac.bd.$	all agents know all secrets
$ab.ad.$	agent a knows that all agents know all secrets
$bc.$	agent b knows that all agents know all secrets
cd	agents c, d know that all agents know all secrets

If agents only communicate secrets, super success is all they can get. An optimal call sequence consists of $n - 2 + \binom{n}{2}$ calls.

[vD, Gattinger. You can only be luck once. MSCS 2024.]

What if they can communicate more?

Epistemic Messages

To obtain super success we need $O(n^2)$ calls. We recall:

$ab.cd.ac.bd.$	all agents know all secrets
$ab.ad.$	agent a knows that all agents know all secrets
$bc.$	agent b knows that all agents know all secrets
cd	agents c, d know that all agents know all secrets

Also communicating knowledge, we only need $O(n)$ calls.

$ab.cd.ac.bd.$	all agents know all secrets
$ab.$	agent a informs b that a, c know all secrets
	agent b informs a that b, d know all secrets
	agents a, b know that all agents know all secrets
cd	agent c informs d that a, c know all secrets
	agent d informs c that b, d know all secrets
	agents c, d know that all agents know all secrets

[Cooper et al. *The epistemic gossip problem.* Discrete Math. 2019]
Full information protocols achieve arbitrary epistemic depth!

Gossip Protocols with Errors

We can consider transmission errors as well as faulty agents.
Assume a single transmission error. An agent a may hold value b or $\overline{b}$ for the secret of agent b, where $\underline{b}$ denotes holding both.

After this call sequence the agents correctly know all secrets:

$$a|b|c|d \stackrel{ab^b}{\to} a\overline{b}|ab|c|d \stackrel{bc.bd.cd}{\to} a\overline{b}|abcd|abcd|abcd \stackrel{ab}{\to}$$
$$a\underline{b}cd|abcd|abcd|abcd \stackrel{ab}{\to} abcd|abcd|abcd|abcd$$

But after this call sequence the agents incorrectly know all secrets:

$$a|b|c|d \stackrel{ab^b}{\to} a\overline{b}|ab|c|d \stackrel{ac}{\to} a\overline{b}c|ab|a\overline{b}c|d \stackrel{cd.da}{\to}$$
$$a\overline{b}cd|ab|a\overline{b}cd|a\overline{b}cd \stackrel{ab}{\to} a\underline{b}cd|abcd|a\overline{b}cd|a\overline{b}cd \stackrel{ab}{\to}$$
$$abcd|abcd|a\overline{b}cd|a\overline{b}cd$$

[vd Berg, Gattinger. Dealing with Unreliable Agents in Dynamic Gossip. DaLí 2020.] [Chapter 11 of Reasoning about Gossip.]