Reachability of Five Gossip Protocols

Hans van Ditmarsch (CNRS, LORIA, Nancy)
Malvin Gattinger (University of Groningen)
Ioannis Kokkinis (TU Dortmund)
Louwe B. Kuijer (University of Liverpool)

11 September 2019 — 13th International Conference on Reachability Problems — RP2019, Brussels

Overview

Gossip

$$(A, B, C, D)$$
$$\Downarrow ab$$
$$(AB, AB, C, D)$$

$$(A, B, C, D)$$
$$\Downarrow ab$$
$$(AB, AB, C, D)$$

$$\Downarrow bc$$
$$(AB, ABC, ABC, D)$$

$$(A, B, C, D)$$
$$\Downarrow ab$$
$$(AB, AB, C, D)$$

$$\Downarrow bc$$
$$(AB, ABC, ABC, D)$$

$$\vdots$$

$$(ABCD, ABCD, ABCD, ABCD)$$

.

The "Telephone Problem"

Given n agents who each know a unique secret,

how many phone calls are needed until everyone knows all secrets?

The "Telephone Problem"

Given n agents who each know a unique secret,
how many phone calls are needed until everyone knows all secrets?

Classical result: $2n - 4$ calls are necessary and sufficient for $n \geq 4$ agents.
See (Hedetniemi, Hedetniemi, and Liestman 1988) for a survey.

Given n agents who each know a unique secret,
how many phone calls are needed until everyone knows all secrets?

Classical result: $2n - 4$ calls are necessary and sufficient for $n \geq 4$ agents.
See (Hedetniemi, Hedetniemi, and Liestman 1988) for a survey.

Applications: distributed databases, social networks, blockchains, ...

But: If there is no central scheduler, most protocols lead to $\mathcal{O}(n \log n)$ many calls!

$\Rightarrow$ How should agents decide who calls whom?

Protocols

A gossip protocol says when an agent a is allowed to call another agent b.

Goals:

- avoid redundancy
- spread all secrets

A gossip protocol says when an agent a is allowed to call another agent b.

Goals:

- avoid redundancy
- spread all secrets

Learn New Secrets

Agent a may call agent b iff a does not have b's secret.

We study five different protocols from the literature:

		a may call b ...
LNS	Learn New Secrets	iff a does not have b's secret.
CO	Call me Once	once (either way).
TOK	Token	iff a has a token. Then a gives her token to b.
SPI	Spider	iff a has a token. Then a takes the token from b.
ANY	Any Call	at any time.

We study five different protocols from the literature:

		a may call b ...
LNS	Learn New Secrets	iff a does not have b's secret.
CO	Call me Once	once (either way).
TOK	Token	iff a has a token. Then a gives her token to b.
SPI	Spider	iff a has a token. Then a takes the token from b.
ANY	Any Call	at any time.

Nice properties:

- epistemic: agents know what calls they are allowed to make
- symmetric: no special roles, all agents are treated the same way

Reachability

Our Research Question

Which **protocol** can reach which **distributions of secrets**?

Which **protocol** can reach which **distributions of secrets**?

Examples

(AB, B) is not reachable by any protocol.

$(ABCD, ABCD, ABC, ABD)$ is reachable by ANY, but not by CO.
(Wlog. the sequence must be $ab; ad; bc; ab$, but the last call ab is not CO-allowed.)

Which **protocol** can reach which **distributions of secrets**?

Examples

(AB, B) is not reachable by any protocol.

$(ABCD, ABCD, ABC, ABD)$ is reachable by ANY, but not by CO.
(Wlog. the sequence must be $ab; ad; bc; ab$, but the last call ab is not CO-allowed.)

Motivation

- agents: which situations should I consider possible?
- outside observer: which protocol are they using?

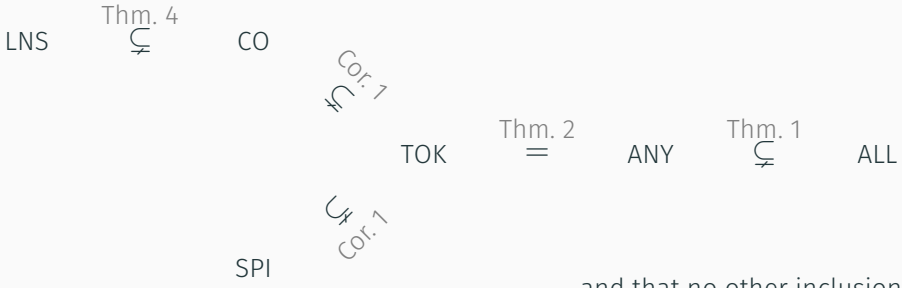
We use a protocol's name for its *extension*: the set of distributions it can reach.

ALL stands for the set of all distributions (including unreachable ones).

We use a protocol's name for its *extension*: the set of distributions it can reach.

ALL stands for the set of all distributions (including unreachable ones).

We show that



and that no other inclusions hold.

We use a protocol's name for its *extension*: the set of distributions it can reach.

ALL stands for the set of all distributions (including unreachable ones).

We show that

and that no other inclusions hold.

We use a protocol's name for its *extension*: the set of distributions it can reach.

ALL stands for the set of all distributions (including unreachable ones).

We show that

and that no other inclusions hold.

Theorem 4

There is a CO-reachable distribution that is not LNS-reachable, hence LNS $\subsetneq$ CO.

Proof.

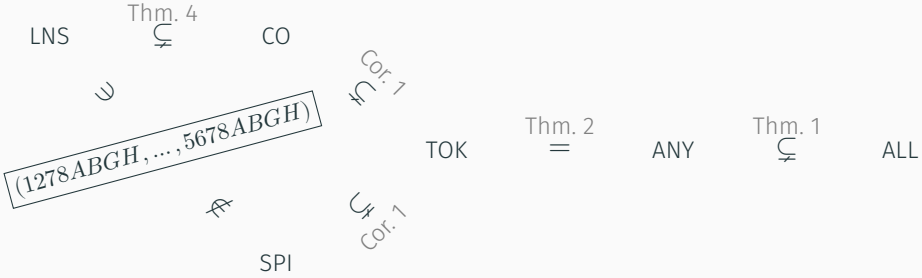
$$t = (ABCDEF, ABC, ABCDE, ABCDEF, DEF, ABDEF)\,.$$

is wlog only reached by

$$ab; cb; ed; ef; cd; af; ad$$

but the last call is not LNS permitted!

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI using 16 agents



Up to five agents, many protocols reach the same (number of non-isomorphic) distributions:

n	LNS	CO	SPI	TOK = ANY
2	2	2	2	2
3	4	4	4	4
4	15	15	16	16
5	97	97	111	111

For LNS and ANY, see https://oeis.org/A307085 and https://oeis.org/A318154.

See (Ditmarsch, Kokkinis, and Stockmarr 2017) and (Kokkinis 2019) for the counter.

Subreachability

Definition
We *restrict* a distribution by forgetting/dropping some agents and their secrets.

Examples

- (AB, ABC, ABC) restricted to $\{A, C\}$ is (A, AC).
- $(ABC, ABCD, ACD, AD)$ restricted to $\{A, B, C\}$ is (ABC, ABC, AC).

Definition
A distribution is P-subreachable if it is a restriction of a P-reachable distribution.

Agents might reason like this:

> *There are only two agents beside me and a call happened, so they now know each other's secrets.*

But this could be prevented by:

- limited computational power
- unknown number of agents

Theorem

All distributions are *sub*reachable by all five protocols.

Sketch of Proof

By induction on the number of known secrets.

Use additional agents to build the distribution step by step.

See also (Gattinger 2018).

Conclusion

Summary

- Gossip: spreading secrets among agents in a peer-to-peer network.
- Which distributions are reached by five distributed epistemic gossip protocols?
- TOK and ANY reach the same distributions, all others differ, with some inclusions.
- Given enough agents, all distributions are *sub*reachable by any protocol.

Future work

- parallel gossip: more distributions are ANY-reachable!
  - Distinguishing counterexamples no longer work! Does reachability collapse?
- complex epistemic conditions, e.g. “call iff you believe you will learn a secret this way”

$\Rightarrow$ for more, see `https://malv.in`

References

Ditmarsch, H. van, I. Kokkinis, and A. Stockmarr. 2017. “Reachability and Expectation in Gossiping.” In *Proceedings of the 20th PRIMA*, edited by B. An, A. Bazzan, J. Leite, S. Villata, and L. van der Torre, 93–109. Springer. https://doi.org/10.1007/978-3-319-69131-2/_6.

Gattinger, Malvin. 2018. “New Directions in Model Checking Dynamic Epistemic Logic.” PhD thesis, University of Amsterdam. https://malv.in/phdthesis.

Hedetniemi, S. M., S. T. Hedetniemi, and A. L. Liestman. 1988. “A Survey of Gossiping and Broadcasting in Communication Networks.” *Networks* 18: 319–49. https://doi.org/10.1002/net.3230180406.

Kokkinis, Ioannis. 2019. “Implementation for Reachability and Expectation in Gossiping.” https://github.com/Jannis17/gossip_protocol_expectation.