Lecture 5, part 1: Reachability of secret distributions

Knowledge and Gossip — ESSLLI 2022

Malvin Gattinger (ILLC, Amsterdam)

2022-08-12, Galway

https://malv.in/2022/gossip/

Main reference

Hans van Ditmarsch, Malvin Gattinger, Ioannis Kokkinis, Louwe B. Kuijer:
Reachability of Five Gossip Protocols, RP 2019.
https://doi.org/10.1007/978-3-030-30806-3_17

Reachability

Reachability

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

Reachability

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

Motivation

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

Reachability: Definition

Definition

A distribution s is *P-reachable* if s can be obtained by applying a P-permitted call sequence on the initial distribution. (Note: we assume a total N relation here.)

Reachability: Definition

Definition

A distribution s is *P-reachable* if s can be obtained by applying a P-permitted call sequence on the initial distribution. (Note: we assume a total N relation here.)

Example

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

$(ABCD, ABCD, ABC, ABD)$ is ANY-reachable, but not CO-reachable.

Why? 🤔

Reachability: Definition

Definition

A distribution s is *P-reachable* if s can be obtained by applying a P-permitted call sequence on the initial distribution. (Note: we assume a total N relation here.)

Example

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

$(ABCD, ABCD, ABC, ABD)$ is ANY-reachable, but not CO-reachable.

Why? 🤔

W.l.o.g. the sequence must be $ab; ad; bc; ab$, but the last call ab is not CO-allowed!

Reminder: Protocols

		a may call *b* ...
LNS	Learn New Secrets	iff *a* does not have *b*'s secret.
CO	Call 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.

Reminder: Protocols

		a may call b ...
LNS	Learn New Secrets	iff a does not have b's secret.
CO	Call 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.

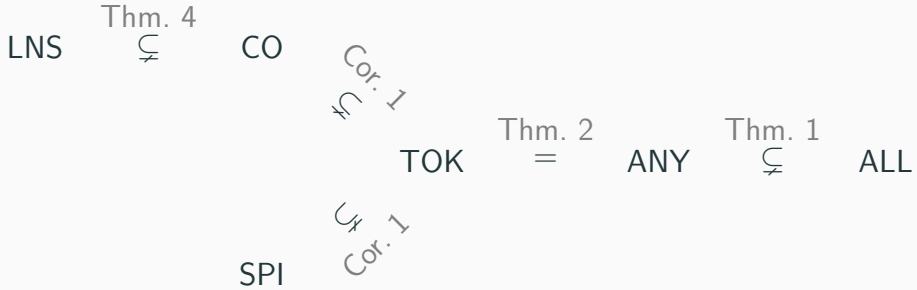
Note: all of these are epistemic (agents know what calls they are allowed to make) and symmetric (no special roles, all agents are treated the same way).

Overview of Results

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).

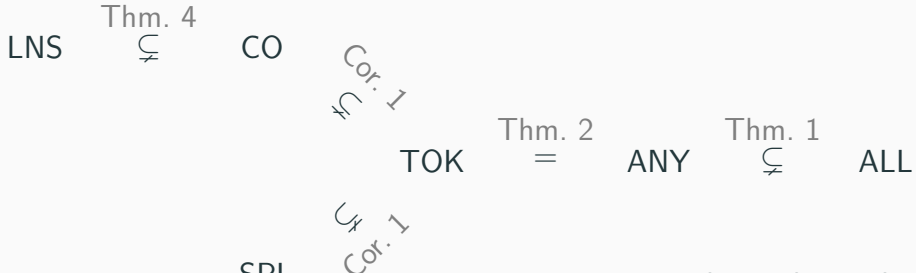
Overview of Results

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).



Overview of Results

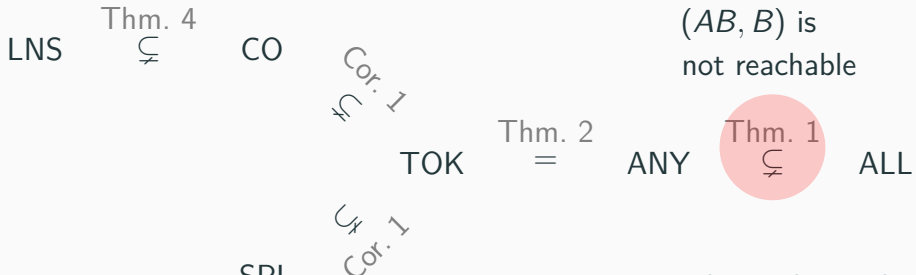
We use a protocol's name for its *extension*: the set of distributions it can reach.
ALL stands for the set of all distributions (including unreachable ones).



and no other inclusions hold.

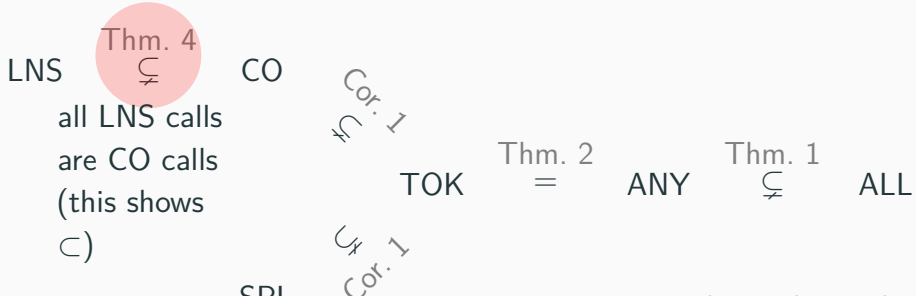
Overview of Results

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).



Overview of Results

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).



and no other inclusions hold.

LNS reaches a proper subset of CO

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!

TOK = ANY

Theorem 2

Every ANY-reachable distribution is TOK-reachable.

TOK = ANY

Theorem 2

Every ANY-reachable distribution is TOK-reachable.

Token Density Lemma

Let s be a TOK-reachable distribution and let a, b be two agents. Then s can be reached by a TOK-call sequence σ such that after the execution of σ at least one of a and b have a token.

SPI != CO

Theorem 3

There is a SPI-reachable distribution that is not CO-reachable.

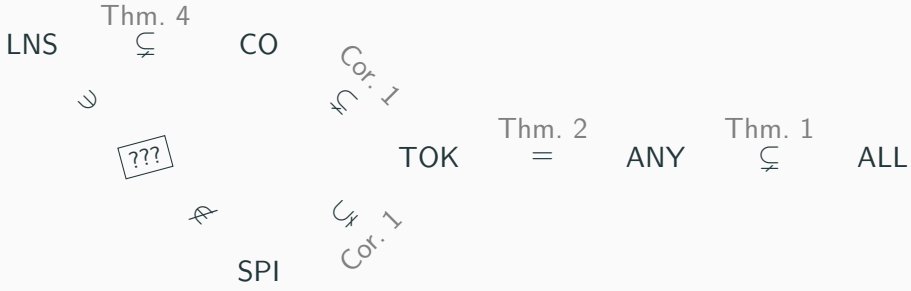
SPI != CO

Theorem 3

There is a SPI-reachable distribution that is not CO-reachable.

Proof. Consider $(ABCD, ABCD, ABC, ABD)$ and make case distinctions.

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI



Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI

Theorem 5 There is an LNS-reachable distribution that is not SPI-reachable.

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI

Theorem 5 There is an LNS-reachable distribution that is not SPI-reachable.

Proof. Consider 16 agents $1, 2, \ldots, 8, a, b, \ldots, h$. Write (ab) for either ab or ba and consider

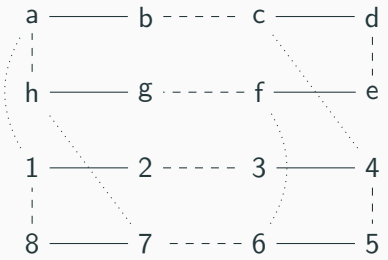
$$\begin{aligned}\sigma := \quad & (12); (34); (56); (78); (ab); (cd); (ef); (gh); \\ & (23); (45); (67); (81); (bc); (de); (fg); (ha); \\ & (1a); (4c); (7h); (6f)\end{aligned}$$

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI

Theorem 5 There is an LNS-reachable distribution that is not SPI-reachable.

Proof. Consider 16 agents $1, 2, \ldots, 8, a, b, \ldots, h$. Write (ab) for either ab or ba and consider

$$\begin{aligned}\sigma := \quad & (12);(34);(56);(78);(ab);(cd);(ef);(gh); && \text{solid lines}\\ & (23);(45);(67);(81);(bc);(de);(fg);(ha); && \text{dashed lines}\\ & (1a);(4c);(7h);(6f) && \text{dotted lines}\end{aligned}$$



Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI: example is not SPI

Proof. (continued)

First, check that σ is indeed LNS-permitted.

Suppose, towards a contradiction, that (some variant of) σ is SPI-permitted.

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI: example is not SPI

Proof. (continued)

First, check that σ is indeed LNS-permitted.

Suppose, towards a contradiction, that (some variant of) σ is SPI-permitted.

1. Solid calls: callee of each pair loses its token.

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI: example is not SPI

Proof. (continued)

First, check that σ is indeed LNS-permitted.

Suppose, towards a contradiction, that (some variant of) σ is SPI-permitted.

1. Solid calls: callee of each pair loses its token.
2. Dashed calls: If 1 still has a token, then 2 does not. So 3 must have a token, otherwise (23) could not take place. Same for 4 and 5 etc.
   Hence, in both blocks, either all even or all odd agents lost their token.

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI: example is not SPI

Proof. (continued)

First, check that σ is indeed LNS-permitted.

Suppose, towards a contradiction, that (some variant of) σ is SPI-permitted.

1. Solid calls: callee of each pair loses its token.
2. Dashed calls: If 1 still has a token, then 2 does not. So 3 must have a token, otherwise (23) could not take place. Same for 4 and 5 etc.
   Hence, in both blocks, either all even or all odd agents lost their token.
3. Dotted calls: $(1a)$, $(4c)$, $(7h)$ and $(6f)$ are all combinations of odd and even. Hence at least one of these calls is between two agents that both do not have a token any more. Hence that call is not SPI-permitted!

Distinguishing $LNS \subseteq CO \subseteq TOK$ from SPI: resulting distribution

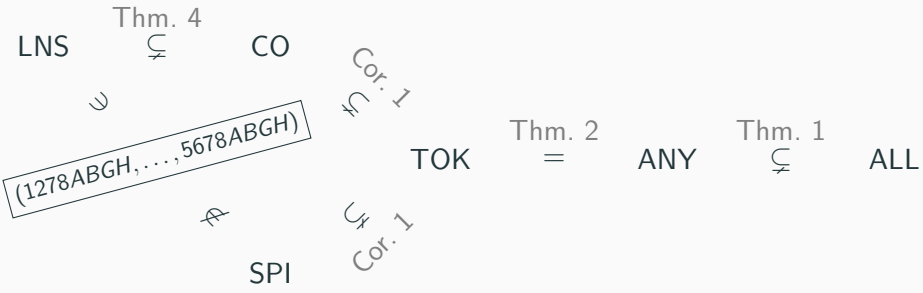
Finally, we can show that the resulting distribution is also not reachable by any other SPI-permitted sequence.

1 :	1278*ABGH*	5 :	3456	*a* :	1278*ABGH*	*e* :	*CDEF*
2 :	1234	6 :	5678*EFGH*	*b* :	*ABCD*	*f* :	5678*EFGH*
3 :	1234	7 :	5678*ABGH*	*c* :	3456*ABCD*	*g* :	*EFGH*
4 :	3456*ABCD*	8 :	1278	*d* :	*CDEF*	*h* :	5678*ABGH*

Claim

Except for the order of calls within the solid / dashed / dotted parts, and the call directions, only σ leads to the distribution above.

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



Do we need so many 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

Do we need so many 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

Subreachability — Why?

Motivation 1: Reasoning About Others

Agents might reason like this:

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

Subreachability — Why?

Motivation 1: Reasoning About Others

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 or an unknown number of agents.

Subreachability — Why?

Motivation 1: Reasoning About Others

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 or an unknown number of agents.

Motivation 2: Logical Structure of Gossip

Given a syntax and semantics on gossip graphs, what are the validities?

Subreachability — Why?

Motivation 1: Reasoning About Others

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 or an unknown number of agents.

Motivation 2: Logical Structure of Gossip

Given a syntax and semantics on gossip graphs, what are the validities?

$\Rightarrow$ This depends on our *class of models*.

Do we include models which are not reachable from initial graphs?

Subreachability

Definition

We *restrict* a distribution by forgetting/dropping some agents.

Subreachability

Definition

We *restrict* a distribution by forgetting/dropping some agents.

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

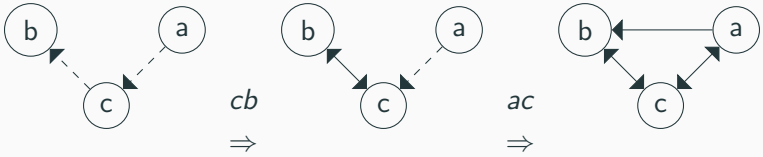
A distribution is P-subreachable if it is a restriction of a P-reachable distribution.

Some unreachable graphs are subreachable!

Example

This graph is not reachable from initial graphs.

But it is subreachable because we can start with the graph below and do $\sigma := (cb); (ac)$ to construct it.



Subreachability — Result

Claim

Every finite gossip graph is subreachable.

Subreachability — Result

Claim

Every finite gossip graph is subreachable.

Definition

- For any $G = (A, N, S)$ let $\mathrm{Size}(G) := |A| + |N \setminus S| + |S \setminus \mathrm{id}_A|$.

  Intuitively, this is the number of things you draw.

Example

$\mathrm{Size}(G) = 3$

- We call $G = (A, N, S)$ *finite* iff $\mathrm{Size}(G) \in \mathbb{N}$.

Proof Idea

We use extra agents to build any given graph step by step.

Proof Idea

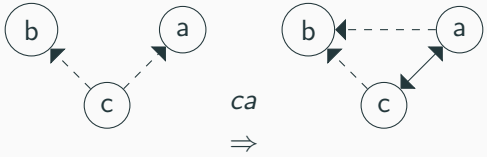
We use extra agents to build any given graph step by step.

1. Adding an agent is easy.

Proof Idea

We use extra agents to build any given graph step by step.

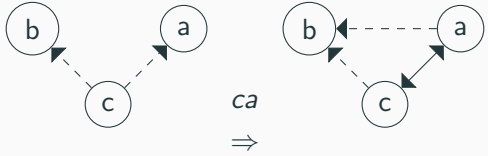
1. Adding an agent is easy.
2. To add an $N \setminus S$-edge from a to b, add someone who knows numbers of a and b and calls a:



Proof Idea

We use extra agents to build any given graph step by step.

1. Adding an agent is easy.
2. To add an $N \setminus S$-edge from a to b, add someone who knows numbers of a and b and calls a:



3. To add an $S \cap N$-edge from a to b, add someone who knows the number of b and whose number is known by a. Then first let c call b and at the end let a call c.

Formal Proof 1/2

Proof. By induction on $\mathrm{Size}(G)$.

Base case: $\mathrm{Size}(G) = 0$ for $G = (A, N, S)$. Then $A = N = S = \varnothing$. Witness: $G_0 := (\varnothing, \varnothing, \varnothing)$ and $\sigma := \epsilon$.

Formal Proof 1/2

Proof. By induction on $\text{Size}(G)$.

Base case: $\text{Size}(G) = 0$ for $G = (A, N, S)$. Then $A = N = S = \varnothing$. Witness: $G_0 := (\varnothing, \varnothing, \varnothing)$ and $\sigma := \epsilon$.

Induction hypothesis: Suppose all G with $\text{Size}(G) = k$ are subreachable.

Formal Proof 1/2

Proof. By induction on $\text{Size}(G)$.

Base case: $\text{Size}(G) = 0$ for $G = (A, N, S)$. Then $A = N = S = \varnothing$. Witness: $G_0 := (\varnothing, \varnothing, \varnothing)$ and $\sigma := \epsilon$.

Induction hypothesis: Suppose all G with $\text{Size}(G) = k$ are subreachable.

Induction step: Take G' such that $\text{Size}(G') = k + 1$.

Let G be a subgraph of G' such that either

1. G' has one disconnected agent more than G,
2. G' has one $N \setminus S$ edge more than G, or
3. G' has one $S \cap N$ edge more than G.

Formal Proof 1/2

Proof. By induction on $\mathrm{Size}(G)$.

Base case: $\mathrm{Size}(G) = 0$ for $G = (A, N, S)$. Then $A = N = S = \varnothing$. Witness: $G_0 := (\varnothing, \varnothing, \varnothing)$ and $\sigma := \epsilon$.

Induction hypothesis: Suppose all G with $\mathrm{Size}(G) = k$ are subreachable.

Induction step: Take G' such that $\mathrm{Size}(G') = k + 1$.

Let G be a subgraph of G' such that either

1. G' has one disconnected agent more than G,
2. G' has one $N \setminus S$ edge more than G, or
3. G' has one $S \cap N$ edge more than G.

In all cases $\mathrm{Size}(G) = k$, so by induction hypothesis G is subreachable.
Hence there are $G_0 = (A_0, N_0, \mathrm{id}_A)$ and σ such that $G \sqsubseteq (G_0)^\sigma$.

Formal Proof 2/2

Now, we consider the three cases:

1. If G' has one disconnected agent more than G, say c, then let $G'_0 := (A_0 \cup \{c\}, N_0, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := \sigma$.

Formal Proof 2/2

Now, we consider the three cases:

1. If G' has one disconnected agent more than G, say c, then let $G'_0 := (A_0 \cup \{c\}, N_0, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := \sigma$.
2. If G' has one $N \setminus S$ edge more than G, say $(a, b) \in (N \setminus S)$, let c be a fresh agent, $G'_0 := (A_0 \cup \{c\}, N_0 \cup \{(c, a), (c, b)\}, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := \sigma; (ca)$.

Formal Proof 2/2

Now, we consider the three cases:

1. If G' has one disconnected agent more than G, say c, then let $G'_0 := (A_0 \cup \{c\}, N_0, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := \sigma$.
2. If G' has one $N \setminus S$ edge more than G, say $(a, b) \in (N \setminus S)$, let c be a fresh agent, $G'_0 := (A_0 \cup \{c\}, N_0 \cup \{(c, a), (c, b)\}, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := \sigma; (ca)$.
3. If G' has one $S \cap N$ edge more than G, say $(a, b) \in (N \cap S)$, let c be a fresh agent, $G'_0 := (A_0 \cup \{c\}, N_0 \cup \{(a, c), (c, b)\}, \mathrm{id}_{A_0 \cup \{c\}})$ and $\sigma' := (cb); \sigma; (ac)$.

In each case we can check that $G' \sqsubseteq (G'_0)^{\sigma'}$. Hence G' is subreachable. □

Subreachability with protocols.

Theorem 6

All graphs are P-subreachable for any of the five P above.

Subreachability with protocols.

Theorem 6

All graphs are P-subreachable for any of the five P above.

Proof. The previous construction can be tweaked to yield P-permitted sequences.

Conclusion

Conclusion

Summary

- TOK and ANY reach the same distributions, all others differ, with some inclusions.
- Given enough agents, all distributions are *sub*reachable by any protocol.

Additional 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.

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