Everyone Knows that Everyone Knows

presentation for EpiP — Epistemic Planning workshop @ ICAPS

October 23, 2020 (post-presentation, with corrected typos)

Hans van Ditmarsch
LORIA, CNRS, University of Lorraine, Nancy, France
hans.van-ditmarsch@loria.fr

partially based on shared work with Rahim Ramezanian and Malvin Gattinger

. . . that is based on prior work with Rasool and Rahim Ramezanian and Malvin

Gossip Protocol

There are n agents. Each agent has a secret to share. Agents communicate by calling each other. When they call, they exchange all secrets they know. The agents keep calling until all agents know all secrets. An agent who knows all secrets is an expert. A call sequence is successful (or 'terminates') if all agents are experts.

There are many variations:

- Secrets are only sent (push), or only received (pull). Secret exchange is pushpull.
- All agents have a global clock (synchrony), or none (asynchrony), or calls are made in rounds (in between synchrony and asynchrony).
- Agents can only call their neighbours: network topology.
- We investigate epistemic gossip protocols. I.e., epistemic: call precondition, termination goal, or message content.

Gossip Protocol — minimum and exp. execution length

Given agents a, b, c, d, four calls $ab;cd;ac;bd$ distribute all secrets. This is the minimum. For $n \geq 4$ agents $2n-4$ [Tijdeman, Labahn].

$$a.b.c.d \stackrel{ab}{\rightarrow} ab.ab.c.d \stackrel{cd}{\rightarrow} ab.ab.cd.cd \stackrel{ac}{\rightarrow}$$
$$abcd.ab.abcd.cd \stackrel{bd}{\rightarrow} abcd.abcd.abcd.abcd$$

If the first two calls overlap, at least five calls are needed.

$$a.b.c.d \stackrel{ab}{\rightarrow} ab.ab.c.d \stackrel{ac}{\rightarrow} abc.ab.abc.d \rightarrow \ldots$$

Some schedules are unsuccessful.

$$a.b.c.d \stackrel{ab}{\rightarrow} ab.ab.c.d \stackrel{ab}{\rightarrow} ab.ab.c.d \rightarrow \ldots$$

If calls are random, the expectation of termination is $n \log n$. The overruling factor is the expectation to randomly select all agents (Coupon Collector). If calls are made in rounds wherein all agents call (combining incoming calls), this is $\log n$. Using network topology, this can be pushed down to $\log^2 n$ [Haeupler].

Epistemic gossip protocol

A gossip protocol can be epistemic in different ways.

- The calling preconditions (protocol conditions) are epistemic.
- The termination goal of the gossip protocol is epistemic.
- The information exchanged between callers is epistemic.

Epistemic protocol conditions

- LNS: you may call an agent if you do not know her secret.
  Originally and better known as NOHO [West, Hedetniemi...]
- CMO: you may call an agent if you have not called her before and if she has not called you before.
- PIG: you may call an agent if you consider it possible that you learn a new secret from her or she from you.
- ANY: you may make any call (not *properly* epistemic)

An agent should *know* whether the protocol condition holds.
The following is **not** epistemic in that sense, because:
you may not know that the protocol condition holds.

- ...: you may call an agent if she does not know your secret.

The termination goal is epistemic

The usual goal is that everyone knows all secrets (all are experts). Consider the goal that everyone knows that everyone knows all secrets. An agent who knows that all agents are experts is a super expert. The new goal is that all agents are super experts. A call sequence satisfying that is super-successful. *Example for 4 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

For $n \geq 4$ agents, we can reach this goal with $\frac{1}{2}(2n-4) + \binom{n}{2}$ calls. Efficiency in getting the first expert is not required. Let any agent call all other agents. In the last call both become expert. This is then the first of $\binom{n}{2}$ calls wherein each pair of agents makes a call. We conjecture that $n - 2 + \binom{n}{2}$ is the minimum.

[vD, Gattinger, Ramezanian. *Everyone knows that everyone knows.*]

Epistemic messages (and epistemic goal)

If agents can only communicate secrets, we got: $\mathcal{O}(n^2)$

$ab;cd;ac;bd;$	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 may communicate knowledge about secrets, we get: $\mathcal{O}(n)$

$ab;cd;ac;bd;$	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

[Herzig, Maffre. *How to share knowledge by gossiping.* AIComm 2017]
[Cooper *et al.* *The epistemic gossip problem.* Discrete Math. 2019]

Everyone knows that everyone knows — missed calls

Gossip protocol with super expert goal for **engaged agents**:
— super experts no longer answer calls;
— super experts no longer make calls.

Previously, we obtained: (This still is an execution) $\mathcal{O}(n^2)$

$ab; cd; ac; bd;$	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

Now, we alternatively obtain: (Last three calls are missed calls)

$ab; cd; ac; bd;$	all agents know all secrets
$ab; ad;$	agent a knows that all agents know all secrets
$ba;$	agent b knows that all agents know all secrets
$ca;$	agent c knows that all agents know all secrets
$da;$	agent d knows that all agents know all secrets

This takes more calls. But . . . More agents: takes less calls. $\mathcal{O}(n)$
The meaning of a missed call **must** be common knowledge.

Missed calls to experts is a bad idea

Engaged agents do not make and do not answer calls.
If you call an engaged agent, the call is a missed call.

Missed calls to super experts, given the super expert goal:	good
Missed calls to experts, given the expert goal:	bad

good

An agent calling a super expert must be an expert. This is because the super expert knows that all agents are experts, and therefore knows that the agent calling her is an expert. Although no secrets are exchanged in a missed call, no information is lost in that call.

bad

The agent calling the expert is not an expert. Because the expert does not return the call, no secrets are exchanged. Therefore, the caller will still not be an expert. A self-defeating variation!

Protocol knowledge

Consider a logical language consisting of formulas and programs.

- Formula $K_a^{\mathsf{P}}\varphi$ stands for "agent a knows φ given protocol P," where "given protocol P" means that the agents have common knowledge that they all execute protocol P.
- Protocol P is a program of shape "until all agents are super experts, select agents a, b such that protocol condition P_{ab} is satisfied, and execute call ab," where P_{ab} is a formula.

The formulas and the programs should therefore be defined by simultaneous recursion. This is well-defined. Formula $K_a^{\mathsf{P}}\varphi$ can be seen as an inductive construct with $\binom{n}{2} + 1$ arguments, namely φ and all $\binom{n}{2}$ protocol conditions P_{bc} (for $b \neq c$) for the protocol P.

Dually, $K_a^{\mathsf{P}}\varphi$ is true after call sequence σ ($\sigma \models K_a^{\mathsf{P}}\varphi$) iff φ is true after all indistinguishable P-permitted call sequences τ ($\sigma \sim_a^{\mathsf{P}} \tau$), where τ is P-permitted iff for all bc occurring in τ, P_{bc} was true prior to the execution of call bc.

[vD, Gattinger, Kuijer, Pardo. *Strengthening Gossip Protocols*, 2019.]

Protocol knowledge

For example, in CMO (agents may only call each other once) the maximum number of calls between n agents is $\binom{n}{2}$. It is known that all maximal CMO-permitted sequences are successful. Given agents a, b, c, d, a maximal CMO-permitted sequence is

$$\sigma := ab; bc; cd; ad; bd; ac.$$

If time is known (synchronized global clock) and protocol CMO is common knowledge, all agents are now super experts. Otherwise, they are not. For example, σ is indistinguishable for agent a from

$$\tau := ab; bc; cd; ad; cd; ac$$

after which agent b does not know the secret of d and is not an expert. Call sequence τ is not CMO-permitted. But agent a does not know that agents c and d only make CMO-permitted calls. She considers any call sequence possible.

Syntax

The logical language is defined by:

formulas	φ	$:=$	$\top \mid S_a b \mid Cab \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a^{\mathrm{P}}\varphi \mid [\pi]\varphi$
programs	π	$:=$	$?\varphi \mid ab \mid (\pi;\pi) \mid (\pi \cup \pi) \mid \pi^*$

— $S_a b$: agent a knows the secret of agent b
— Cab: a call from a to b took place
— $K_a^{\mathrm{P}}\varphi$: a knows φ given common knowledge of protocol P

Various abbreviations:

— $Exp_a := \bigwedge_{b \in A} S_a b$: a knows all secrets; agent a is an expert.
— $Exp_A := \bigwedge_{a \in A} \bigwedge_{b \in A} S_a b$: all agents are experts (success).
— $K_a^{\mathrm{P}} Exp_A$: a knows everyone is an expert; a is a super expert.
— $E^{\mathrm{P}} Exp_A := \bigwedge_{a \in A} K_a^{\mathrm{P}} Exp_A$: all are super experts (super success).

A protocol P is a program of the following shape:

$$\mathrm{P} := \Big(\bigcup_{a \neq b \in A} (?(\neg K_a^{\mathrm{P}} Exp_A \wedge \mathrm{P}_{ab}); ab) \Big)^*; ?E^{\mathrm{P}} Exp_A$$

where formula P_{ab} is the protocol condition for call ab of protocol P.

Semantics

The semantics contains this clause for knowledge:

$\sigma \models K_a^{\mathsf{P}} \varphi \quad$ iff $\quad \tau \models \varphi$ for all τ such that $\sigma \approx_a^{\mathsf{P}} \tau$

The epistemic relation is defined inductively by clauses such as:

if $\sigma \approx_a^{\mathsf{P}} \tau$, $I_b^\sigma = I_b^\tau$, $\sigma \models \neg K_a^{\mathsf{P}} Exp_A \land \mathsf{P}_{ab}$, $\tau \models \neg K_a^{\mathsf{P}} Exp_A \land \mathsf{P}_{ab}$, and ($\sigma \models K_b^{\mathsf{P}} Exp_A$ iff $\tau \models K_b^{\mathsf{P}} Exp_A$), then $\sigma; ab \approx_a^{\mathsf{P}} \tau; ab$

BLUE: super experts do not make calls
GREEN: protocol P is common knowledge
RED: super experts do not answer calls

[vD, Gattinger, Ramezanian. Everyone knows that everyone knows. 2020]

Semantics — $\approx_a$ and $\models$ by simultaneous recursion

I $(= I^\epsilon)$ is the identity relation on A; $I^{\sigma;ab} = I^\sigma \cup (\{(a,b),(b,a)\} \circ I^\sigma)$

$$
\begin{array}{lll}
\sigma \models \top & \text{iff} & \textit{always} \\
\sigma \models S_a b & \text{iff} & I^\sigma_a b \\
\sigma \models Cab & \text{iff} & ab \in \sigma \\
\sigma \models \neg\varphi & \text{iff} & \sigma \not\models \varphi \\
\sigma \models \varphi \wedge \psi & \text{iff} & \sigma \models \varphi \text{ and } \sigma \models \psi \\
\sigma \models K^{\mathrm{P}}_a \varphi & \text{iff} & \tau \models \varphi \text{ for all } \tau \text{ such that } \sigma \approx^{\mathrm{P}}_a \tau \\
\sigma \models [\pi]\varphi & \text{iff} & \tau \models \varphi \text{ for all } \tau \text{ such that } \sigma[\![\pi]\!]\tau
\end{array}
$$

where

$$
\begin{array}{lll}
\sigma[\![?\varphi]\!]\tau & \text{iff} & \sigma \models \varphi \text{ and } \tau = \sigma \\
\sigma[\![ab]\!]\tau & \text{iff} & \tau = \sigma; ab \\
\sigma[\![\pi;\pi']\!]\tau & \text{iff} & \text{there is } \rho \text{ such that } \sigma[\![\pi]\!]\rho \text{ and } \rho[\![\pi']\!]\tau \\
\sigma[\![\pi \cup \pi']\!]\tau & \text{iff} & \sigma[\![\pi]\!]\tau \text{ or } \sigma[\![\pi']\!]\tau \\
\sigma[\![\pi^*]\!]\tau & \text{iff} & \text{there is } n \in \mathbb{N} \text{ such that } \sigma[\![\pi^n]\!]\tau \qquad (\pi^0 = ?\top)
\end{array}
$$

Asynchronous setting: replace $\sigma \approx^{\mathrm{P}}_a \tau$ by $\sigma \sim^{\mathrm{P}}_a \tau$ in clause $K^{\mathrm{P}}_a \varphi$.

Semantics — $\approx_a$ and $\models$ by simultaneous recursion

Synchronous accessibility relation $\approx_a^{\mathsf{P}}$:

- $\epsilon \approx_a^{\mathsf{P}} \epsilon$,
- if $\sigma \approx_a^{\mathsf{P}} \tau$, $a \notin \{b, c, d, e\}$, $\sigma \models \neg K_b^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{bc}$ and $\tau \models \neg K_d^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{de}$, then $\sigma; bc \approx_a^{\mathsf{P}} \tau; de$
- if $\sigma \approx_a^{\mathsf{P}} \tau$, $I_b^\sigma = I_b^\tau$, $\sigma \models \neg K_a^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{ab}$, $\tau \models \neg K_a^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{ab}$ and ($\sigma \models K_b^{\mathsf{P}} Exp_A$ iff $\tau \models K_b^{\mathsf{P}} Exp_A$), then $\sigma; ab \approx_a^{\mathsf{P}} \tau; ab$
- if $\sigma \approx_a^{\mathsf{P}} \tau$, $I_b^\sigma = I_b^\tau$, $\sigma \models \neg K_b^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{ba}$, $\tau \models \neg K_b^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{ba}$ and ($\sigma \models K_a^{\mathsf{P}} Exp_A$ iff $\tau \models K_a^{\mathsf{P}} Exp_A$), then $\sigma; ba \approx_a^{\mathsf{P}} \tau; ba$

Asynchronous accessibility relation $\sim_a^{\mathsf{P}}$:
is as $\approx_a^{\mathsf{P}}$, except that the second clause is replaced by:

- if $\sigma \sim_a^{\mathsf{P}} \tau$, $a \notin \{b, c\}$ and $\sigma \models \neg K_b^{\mathsf{P}} Exp_A \wedge \mathsf{P}_{bc}$, then $\sigma; bc \sim_a^{\mathsf{P}} \tau$

Both relations are the smallest transitive and symmetric closure of the above. They are equivalence relations when restricted to the P-permitted sequences σ without missed calls, otherwise not.

Some observations with this semantics

- Knowledge does not imply truth
  $K_a^{\mathrm{P}}\varphi \to \varphi$ is invalid. This is because a call sequence σ may contain a call bc that is not P-permitted (P_{bc} is false) or wherein b is a super expert. The epistemic relation is then empty: there is no τ with $\sigma \approx_a \tau$. Therefore $\sigma \models K_a^{\mathrm{P}}\bot$.
- If you call a super expert you become a super expert
  $K_b^{\mathrm{P}} Exp_A \to [ab] K_a^{\mathrm{P}} Exp_A$ is valid. If b is a super expert, then a becomes a super expert from missed call ab.

Protocol conditions for the protocols mentioned before:

- $\mathrm{LNS}_{ab} := \neg S_a b$ Learn New Secrets / NOHO
- $\mathrm{CMO}_{ab} := \neg Cab \wedge \neg Cba$ Call Me Once
- $\mathrm{PIG}_{ab} := \hat{K}_a \bigvee_{c \in A}((S_a c \wedge \neg S_b c) \vee (\neg S_a c \wedge S_b c))$
  Possible Information Growth
- $\mathrm{ANY}_{ab} := \top$ ANY call define $K_a\varphi$ as $K_a^{\mathrm{ANY}}\varphi$

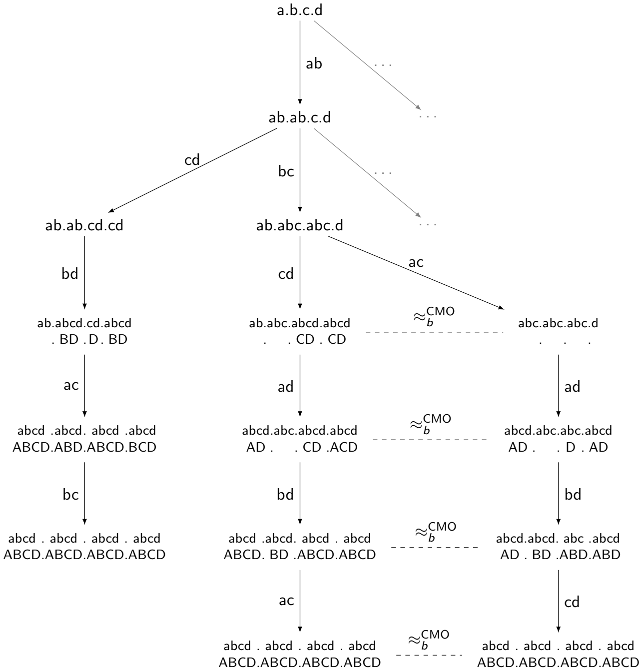
Results for super-successful gossip protocols

'terminate faster' means 'smaller minimum length s-s. call sequence'

- ANY is super-successful (i.e., all fair executions are s-s.)
- PIG is super-successful
- synchronous known CMO is super-successful
- synchronous ANY is faster then asynchronous ANY.
  $ab; ac; ab; cb$ is asynchr. s-s, but prefix $ab; ac; ab$ is synchr. s-s.
- Protocols with engaged agents (may) terminate faster than without ... but may also halt.
- ANY with engaged agents terminates faster:
  $3n - 4$ versus $n - 2 + \binom{n}{2}$ / $\mathcal{O}(n)$ versus $\mathcal{O}(n^2)$
  The minima are for asynchronous and are not proved.
  And how about expectation? $\mathcal{O}(n \log n)$ versus $\mathcal{O}(n^2)$?
- synchronous known CMO with engaged agents is not s-s.
- many of these results require the model checker GoMoChe
  `https://github.com/m4lvin/gossip`

GoMoChe — https://github.com/m4lvin/gossip

Gomoche Gompa (Monastery), Nepal


a.b.c.d
ab
ab.ab.c.d
cd
bc
ab.ab.cd.cd
ab.abc.abc.d
bd
cd
ac
ab.abcd.cd.abcd
. BD . D . BD
ab.abc.abcd.abcd
. . CD . CD
≈b CMO
abc.abc.abc.d
. . .
ac
ad
ad
abcd .abcd. abcd .abcd
ABCD.ABD.ABCD.BCD
abcd.abc.abcd.abcd
AD . . CD .ACD
≈b CMO
abcd.abc.abc.abcd
AD . . D . AD
bc
bd
bd
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD
abcd .abcd. abcd . abcd
ABCD. BD .ABCD.ABCD
≈b CMO
abcd.abcd. abc .abcd
AD . BD .ABD.ABD
ac
cd
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD
≈b CMO
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD

Skip calls

Recall *ab*; *bc*; *cd*; *ad*; *bd*; *ac* in the synchronous known CMO tree.
After prefix *ab*; *bc*; *cd*; *ad*; *bd*, only agent *b* is not a super expert.
No call involving *b* is CMO-permitted: *b* has been in *ab*, *bc*, *bd*.
The final call *ac* is CMO permitted. But not with 'engaged agents'.
If no next call is made, *b* would become super expert.

Add an atomic call *skip* to the language of programs.
skip means 'the time to make one call has passed'. (It is not $?\top$.)
skip is permitted iff all P-permitted callers are super experts ...
... and some agent not P-permitted to call is not a super expert.
This requires careful finetuning of the semantics.
CMO with engaged agents and *skip* is again super-successful.

Skip calls

Recall *ab*; *bc*; *cd*; *ad*; *bd*; *ac* in the synchronous known CMO tree.
After prefix *ab*; *bc*; *cd*; *ad*; *bd*, only agent *b* is not a super expert.
No call involving *b* is CMO-permitted: *b* has been in *ab*, *bc*, *bd*.
The final call *ac* is CMO permitted. But not with 'engaged agents'.
If no next call is made, *b* would become super expert.

Add an atomic call *skip* to the language of programs.
skip means 'the time to make one call has passed'. (It is not $?\top$.)
skip is permitted iff all P-permitted callers are super experts ...
... and some agent not P-permitted to call is not a super expert.
This requires careful finetuning of the semantics.
CMO with engaged agents and *skip* is again super-successful.

Did you notice agents have common knowledge of all secrets?
In CK clusters of 5 calls the first two calls do not overlap.
In CK clusters of 6 calls the first two calls overlap.

Further research

- ~~Manuscript under submission~~ ~~Available on ArXiV~~ soon?
- Results for other distributed epistemic gossip protocols
- Prove minima and orders of magnitude