Gossip and Knowledge

Hans van Ditmarsch
Open University of the Netherlands

Malvin Gattinger
University of Amsterdam

- Complexity of termination

presentation for ESSLLI Galway

August 2022

Optimal successful call sequences

For $n \geq 4$ agents, all can become expert in $2n - 4$ calls.

Four agents a, b, c, d: call sequence $ab.cd.ac.bd$ of length 4.
$(2 \cdot 4 - 4 = 4)$

Six agents a, b, c, d, e, f: call sequence $ae.af.ab.cd.ac.bd.ae.af$
$(2 \cdot 6 - 4 = 8)$

Among all agents, select four, let us say a, b, c, d. Among those four, select one, let us say a. Let a call all $n - 4$ other agents (than a, b, c, d): $ae.af\dots$. Then execute $ab.cd.ac.bd$ (4 calls). Then a calls again all $n - 4$ other agents: $ae.af\dots$. Alltogether these are $(n - 4) + 4 + (n - 4) = 2n - 4$ calls. Then everybody is expert.

Proving that $2n - 4$ is minimal is not trivial [Tijdeman, 1971].

Optimal successful call sequences

The optimal $2n - 4$ is not much better than very naive schedules. Here is one:

Among all agents, select one, let us say a. Let a call all other agents ($n - 1$ calls). Let the last such call be ab. Let a call once more all other agents except b ($n - 2$ calls). Then everybody is expert. Alltogether $(n - 1) + (n - 2) = 2n - 3$ calls. Just one more!

For particular network topologies (not everybody is your neighbour), we can obtain $2n - 3$ but not $2n - 4$.

- n agents in a circle (try 5)
- $2^n - 1$ agents in a binary tree of depth n (try 3, i.e., 7 nodes)

Note that $2n - 4$ and $2n - 3$ are $O(n)$.

Maximal successful call sequences

Prolonging the pleasure of gossip is also fun.
As long as in each call someone hears a new secret.
The maximum number of (factually) informative calls is

$$\binom{n}{2} = n(n-1)/2$$

For 4 agents we get $\binom{4}{2} = 6$. For 6 agents we get $\binom{6}{2} = 15$.
We achieve this by making all calls in lexicographic order:

$$ab.ac.ad.bc.bd.cd$$

The same calls in different order may not be (all) informative:

$$ab.cd.ac.bd.ad.bc$$

Protocols LNS, CMO permit at most $\binom{n}{2}$ calls. Note $\binom{n}{2}$ is $O(n^2)$.
Protocols ANY, SPI, TOK, ... permit infinite call sequences.

$$ab.ab.ab. \ldots$$

Expectation of the length of successful call sequences

If I buy a coffee at McDonald's every day. I get a receipt with order number between 00 and 99. How many days before I got all order numbers? (Coupon Collector's Problem)

Probability of getting a different order number:

$$\frac{100}{100}, \frac{99}{100}, \frac{98}{100}, \ldots, \frac{1}{100}$$

Expected number of days before this happens:

$\frac{100}{100} + \frac{100}{99} + \frac{100}{98} + \cdots + \frac{100}{1}$ that is: $100 \cdot (\frac{1}{100} + \frac{1}{99} + \frac{1}{98} + \cdots + \frac{1}{1})$

Harmonic series (Nicole Oresme, Johann Bernoulli, A De Moivre):

$\Sigma_{i=1}^{n} \frac{1}{i}$ adds up to $\log n$ plus a bit, which is $O(\log n)$

So we get $O(n \log n)$ altogether. (About 450 coffees.)

Now gossip ...

Expectation of the length of successful call sequences

Given n agents, imagine agent a making random calls, as in ANY, until she called all other $n-1$ agents. Probability 1, $\frac{n-2}{n-1}$, $\frac{n-3}{n-1}$, ..., $\frac{1}{n-1}$, expectation 1, $\frac{n-1}{n-2}$, $\frac{n-1}{n-3}$, ..., $\frac{n-1}{1}$. Coupon Collector's Problem! One more or less does not matter. So $O(n \log n)$ calls.

In gossip, all agents have to know all secrets. Agent a has to call all other agents (but one) again so they become experts. This does not matter: $O(n \log n)$ calls plus $O(n \log n)$ is still $O(n \log n)$ calls.

Instead, imagine agent a not randomly calling agents, but randomly calling agents whose secret she does not know, as in LNS. Now $n-1$ calls are enough.

This does not mean that the expectation of LNS is of a lower order of magnitude than the expectation of ANY. The agent a who is chosen to call is also selected randomly.

Expectation of the length of successful call sequences

Complexity results for gossip protocols: almost all is $O(n \log n)$.

- ANY: $O(n \log n)$ (in fact $\frac{3}{2} n \log n$ plus a linear factor in n) [Moon 1972] [Boyd & Steele 1979]
- CMO: $O(n \log n)$ (lower and upper bounds, simulations suggest bit below ANY)
- SPI, TOK: $O(n \log n)$ (simulations suggest bit above ANY)
- LNS: $O(n \log n)$ not confirmed (simulations suggest $n \log n$)

Methods to obtain these results: [vD, Kokkinis, Stockmarr, 2017]

- combinatorial: Markov chains (few agents)
- computational: asymptotic behaviour of expectation (as ANY)
- simulations: $50,000$ runs for up to 50 agents

With special topologies (restricted neighbours) has been obtained:

- $O(n \log^2 n)$ [Haeupler, 2015]

Gossip and Knowledge

Hans van Ditmarsch
Open University of the Netherlands

Malvin Gattinger
University of Amsterdam

- Gossip protocols with higher-order epistemic goals

presentation for ESSLLI Galway

August 2022

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.

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 and 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. $\mathcal{O}(n)$
$3n-4$: a calls all $n-1$, then all but one $n-2$, then all $n-1$ call a.
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 — example of CMO

The maximum number of calls between n agents is $\binom{n}{2}$. All maximal CMO-permitted sequences are successful. Given agents a, b, c, d, a maximal CMO-permitted sequence is

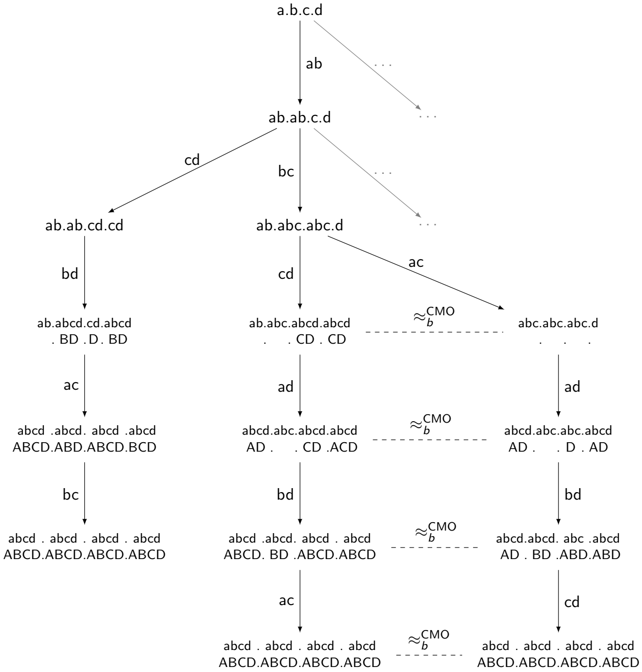
$$\sigma := ab; bc; cd; ad; bd; ac.$$

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. Let time not be known (but CMO known). Then $\sigma \sim_a \tau'$ for:

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


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
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
abcd.abcd. abc .abcd
AD . BD .ABD.ABD
ac
cd
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD

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 — informal introduction synchronous case

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 $\sigma \approx_a^{\mathsf{P}} \tau$, $I_b^\sigma = I_b^\tau$, $\sigma \models \neg K_a^{\mathsf{P}} \mathit{Exp}_A \wedge \mathsf{P}_{ab}$, $\tau \models \neg K_a^{\mathsf{P}} \mathit{Exp}_A \wedge \mathsf{P}_{ab}$, and ($\sigma \models K_b^{\mathsf{P}} \mathit{Exp}_A$ iff $\tau \models K_b^{\mathsf{P}} \mathit{Exp}_A$), 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. 2022]
https://arxiv.org/abs/2011.13203

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

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

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

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 $\sigma \approx_a^{\mathsf{P}} \tau$ by $\sigma \sim_a^{\mathsf{P}} \tau$ in clause $K_a^{\mathsf{P}}\varphi$.

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

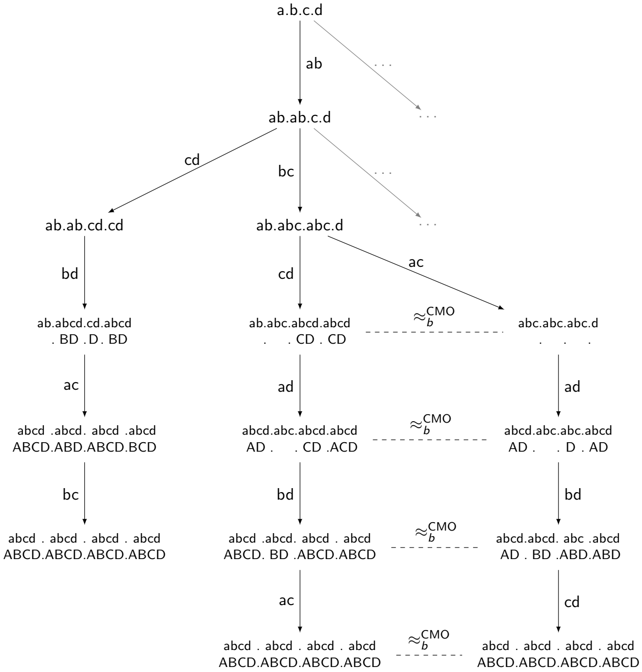
- Knowledge does not imply truth
  $K_a^{\mathrm{P}}\varphi \to \varphi$ is invalid. This is because a call sequence σ may contain a call bc that is not P-permitted (P_{bc} is false) or wherein b is a super expert. The epistemic relation is then empty: there is no τ with $\sigma \approx_a \tau$. Therefore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

- 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.
- Optimality conjectures: $3n - 4$ / $\mathcal{O}(n)$ for ANY with engaged agents versus $n - 2 + \binom{n}{2}$ / $\mathcal{O}(n^2)$ for ANY (asynchronous)
  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
- *EEExp*$_A$ is unsatisfiable [vD & G, The Limits to Gossip, 2022]


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
$\approx_b^{CMO}$
abc.abc.abc.d
. . .
ac
ad
ad
abcd .abcd. abcd .abcd
ABCD.ABD.ABCD.BCD
abcd.abc.abcd.abcd
AD . . CD .ACD
$\approx_b^{CMO}$
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
$\approx_b^{CMO}$
abcd.abcd. abc .abcd
AD . BD .ABD.ABD
ac
cd
abcd . abcd . abcd . abcd
ABCD.ABCD.ABCD.ABCD
$\approx_b^{CMO}$
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'.
But *b* would become super expert 'noticing' absence of a next call.

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'.
But *b* would become super expert 'noticing' absence of a next call.

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.

Second-order shared knowledge is unsatisfiable

success: Exp_A ! Yes.
super success: $EExp_A$! Yes.
mega super success: $EEExp_A$? No !

For this a simplified setting is sufficient: an epistemic language only, and instead of calls and protocols in the language, we investigate truth of epistemic formulas given call sequences. So, $\sigma \models \varphi$ where φ contains K_a modalities, and atoms for agents knowing secrets. It is like doing asynchronous ANY but off-line (semantically) only.

Then, instead of the question whether a protocol asynchronous ANY can reach a higher-order epistemic goal $EEExp_A$, given a PDL-like language, we investigate whether (epistemic!) formula $EEExp_A$ is satisfiable in the simplified language and semantics.

Second-order shared knowledge is unsatisfiable

Epistemic language

$\varphi ::= b_a \mid \neg\varphi \mid \varphi\wedge\varphi \mid K_a\varphi$ for Sab or $S_a = \{b\}$ we now write b_a

Epistemic (observation) relation

- $\epsilon \sim_a \epsilon$
- if $\sigma \sim_a \tau$ and $a \notin \{b, c\}$, then $\sigma.bc \sim_a \tau$
- if $\sigma \sim_a \tau$, and for all c, $\sigma \models c_b$ iff $\tau \models c_b$, then $\sigma.ab \sim_a \tau.ab$

Semantics

$\epsilon \models a_b$	iff	$a = b$	
$\sigma.ab \models c_a$	iff	$\sigma \models c_a$ or $\sigma \models c_b$	for all $c \in A$
$\sigma.ab \models c_b$	iff	$\sigma \models c_a$ or $\sigma \models c_b$	for all $c \in A$
$\sigma.ab \models c_d$	iff	$\sigma \models c_d$	for all $c, d \in A$ with $d \notin \{a, b\}$
$\sigma \models \neg\varphi$	iff	$\sigma \not\models \varphi$	
$\sigma \models \varphi \wedge \psi$	iff	$\sigma \models \varphi$ and $\sigma \models \psi$	
$\sigma \models K_a\varphi$	iff	$\tau \models \varphi$ for all τ such that $\sigma \sim_a \tau$	

Second-order shared knowledge is unsatisfiable

Lucky Calls

Given four agents $\{a, b, c, d\}$ consider the call sequence $ac.ad.ac.bc.ac$. Agent a learns in the final call ac that a, b, c are experts. Because b is not involved in this call we say that this a lucky call and say that a is lucky about b.

	a	b	c	d
$\xrightarrow{ac}$	a c	b	a c	d
$\xrightarrow{ad}$	a cd	b	a c	a cd
$\xrightarrow{ac}$	a cd	b	a cd	a cd
$\xrightarrow{bc}$	a cd	abcd BC	abcd BC	a cd
$\xrightarrow{ac}$	abcd ABC	abcd BC	abcd ABC	a cd

After $ac.ad.ac$, agent a knows that a, b, c know the secrets of a, b, c. Agent a is a super expert of the subset $\{a, b, c\}$ of all.

Second-order shared knowledge is unsatisfiable

Definition: a is lucky about c if $\sigma \not\models K_a Exp_c$ and $\sigma.ab \models K_a Exp_c$.

- When two agents become experts they cannot be lucky.
- When two agents become experts they do not become super experts.
- An agent becoming an expert can only be lucky if she is a super expert for all agents but one: $\sigma \not\models Exp_a$ & $\sigma.ac \models Exp_a$ implies: $\sigma.ac \models K_a Exp_b$ iff $\sigma \models K_a Exp_{A-b}(A - b)$.
- An agent cannot become an expert and a super expert in the same call.
- An agent becoming a super expert considers possible that the other agent involved in the call did not become a super expert.

Theorem: $EEExp_A$ is unsatisfiable. (As $K_a K_b Exp_A$ is unsat.)

Optimality questions: $2n - 3$ calls to reach $K_a Exp_A$, $n - 2 + \binom{n}{2}$ calls to reach $EExp_A$? Problematic, as experts can also be lucky.