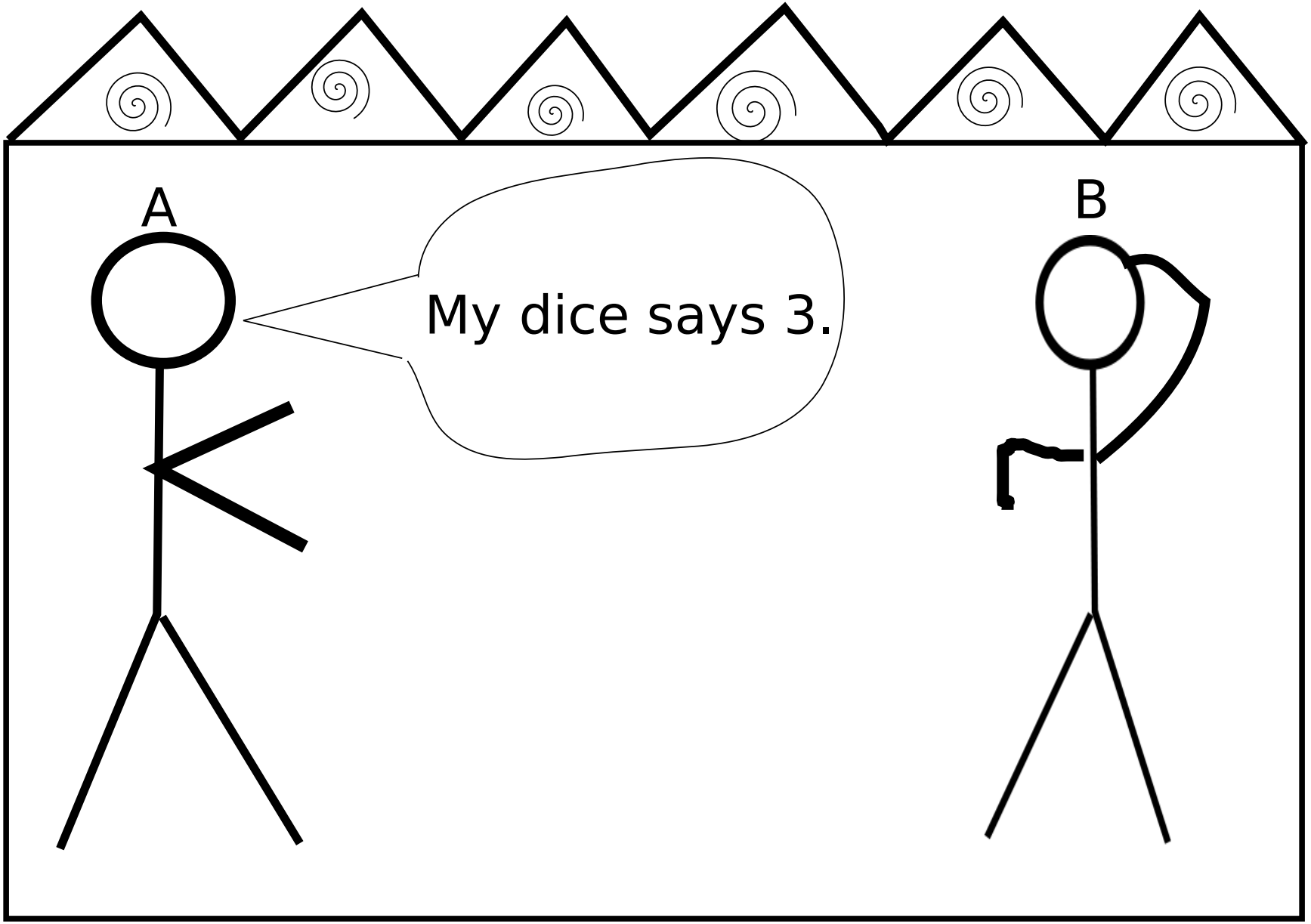
Disjunction Property and Finite Model Property For an Intuitionistic Epistemic Logic

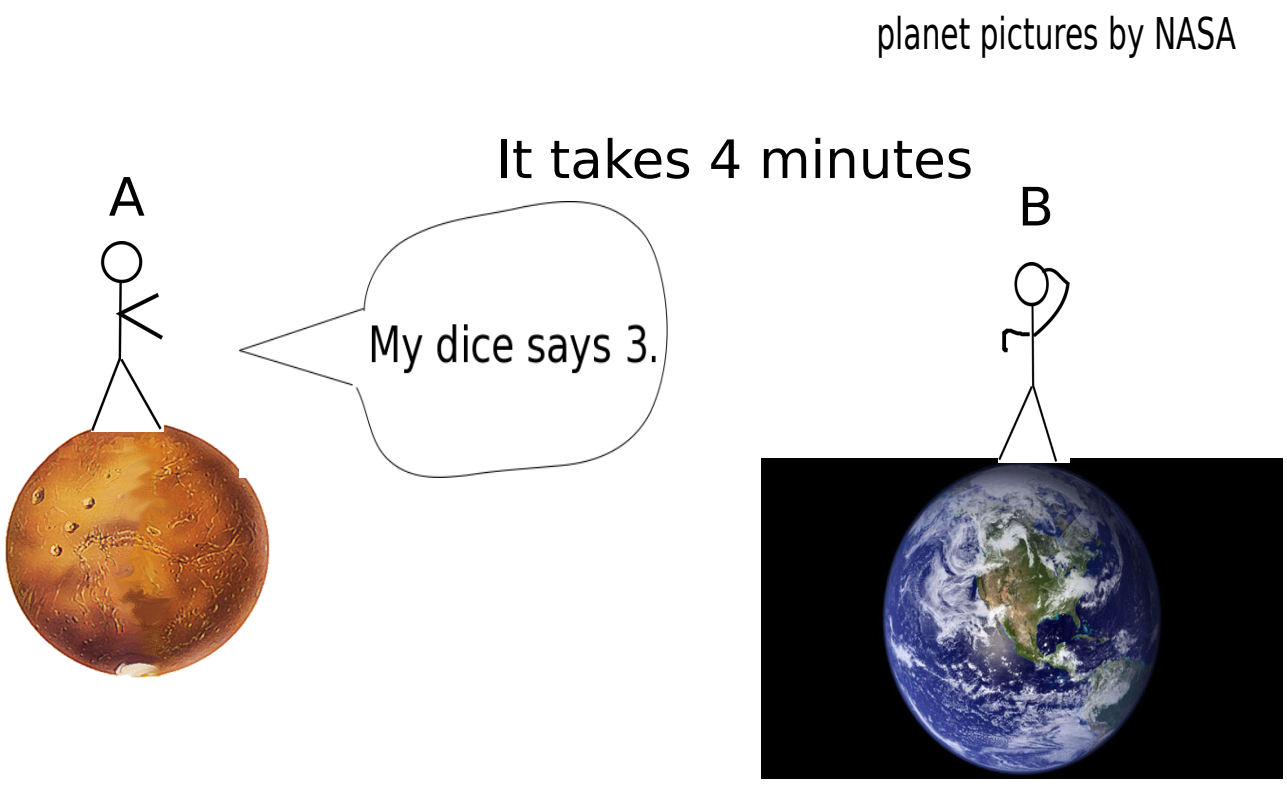
Yoichi Hirai
yh@is.s.u-tokyo.ac.jp

2010-06-26, Bloomington

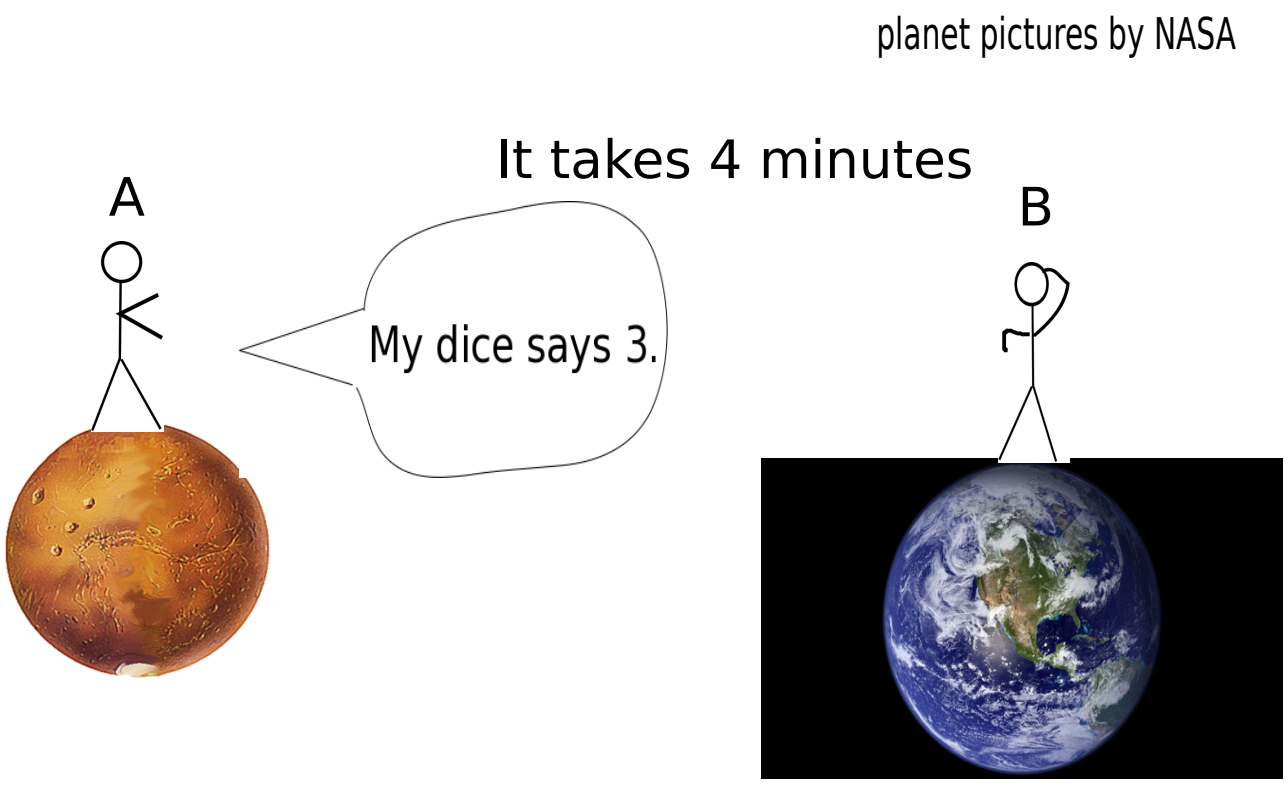
Common Knowledge



Common Knowledge?



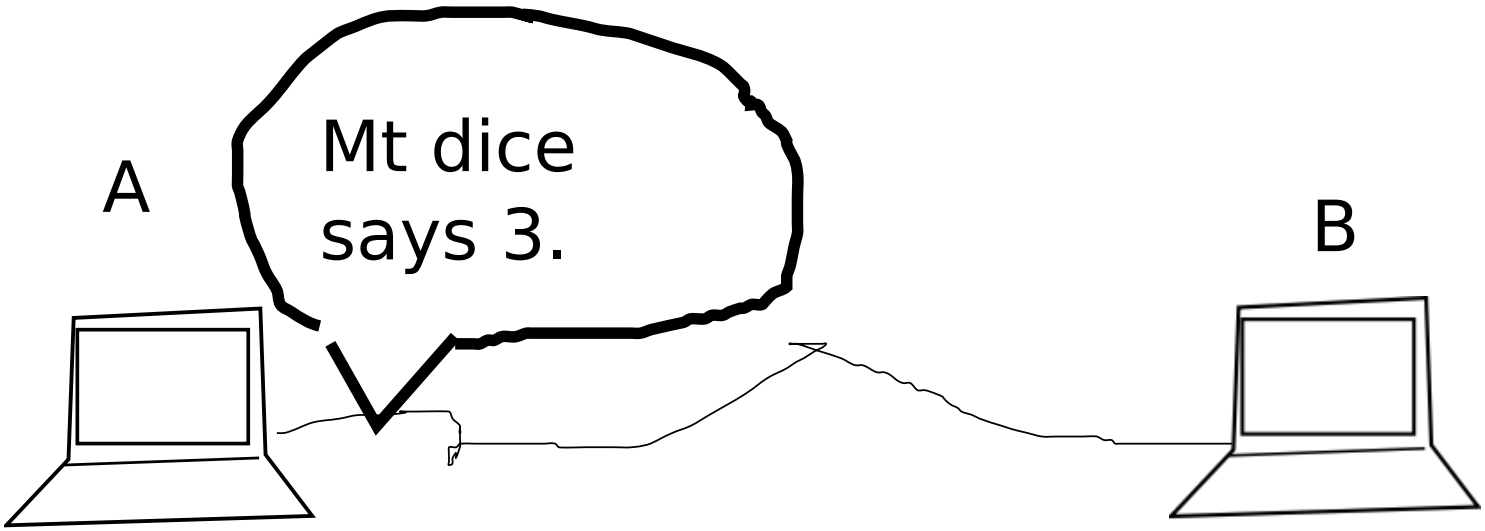
Common Knowledge?



Yes, (with enough prior common knowledge)
in 4 minutes, "A knows B knows A knows ... the message *now*"
for any number of iteration.

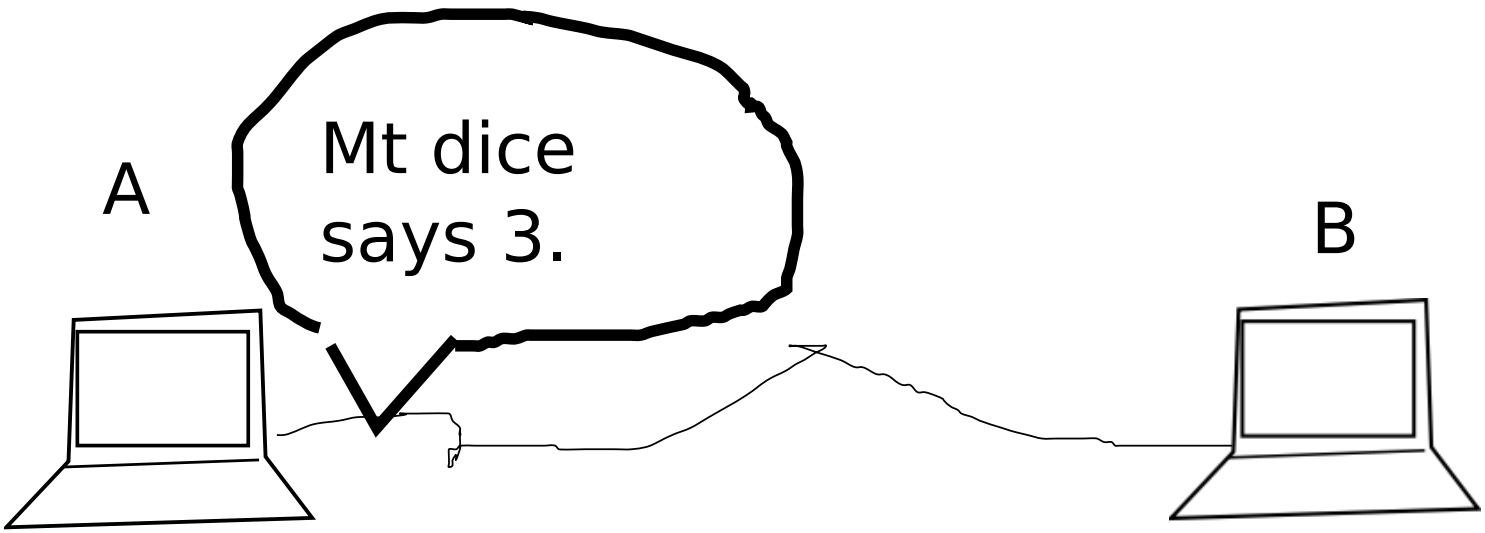
Common Knowledge?

Amount of delay is indefinite according to the internet protocol.



Common Knowledge?

Amount of delay is indefinite according to the internet protocol.



No. "A knows B knows A knows ... the message *now* ~~eventually~~" never holds for all number of iteration.

Asynchrony = Lack of Global Common Clock

Asynchrony poses difficulty even if

- every agent's knowledge increases over time, and
- every message contains sender's whole knowledge

There is no waitfree algorithm over

before execution two agents each know their numbers.

after execution both agents know the sum of their initial numbers.

(Waitfree: cannot wait until your mate reads your message.
You can wait for the shared memory. Details later.)

Herlihy and Shavit's "Topological Structure of Asynchronous Computability" [Herlihy and Shavit, 1999]
(ACM/ETAPS Gödel Prize, 2004).

Their work:

Asynchronous Communication in Classical Epistemic S5 Logic

Asynchrony in Epistemic Logic with Time (1)

from: *Reasoning about Knowledge* [Fagin et al., 2003]
Warning: for the speaker, the formalisation below is complicated.

Let us fix
Φ: a set (of propositional variables).
L_i: a set (of local states) for $1 \leqslant i \leqslant n$.

$\mathcal{G} = L_1 \times \cdots \times L_n$ (global states).
A run over $\mathcal{G}$ is a function $\mathbb{N} \to \mathcal{G}$.
A system $\mathcal{R}$ over $\mathcal{G}$ is a set of runs $\mathcal{R} \subseteq \mathcal{G}^{\mathbb{N}}$.

An interpreted system $\mathcal{I}$ is a pair $(\mathcal{R}, \pi)$

- $\mathcal{R}$: a system over $\mathcal{G}$.
- $\pi : \mathcal{G} \to \Phi \to \{\top, \bot\}$.

Asynchrony in Epistemic Logic with Time (2)

An interpreted system interprets the formulae
(still from [Fagin et al., 2003])

With the natural projection $f_i = \mathcal{G} \to L_i$,
$s \sim_i s'$ iff $f_i(s) = f_i(s')$.
A point: $(r, m) \in \mathcal{R} \times \mathbb{N}$.

- $(r, m) \models l$ iff $\pi(r, m)(l) = \top$ for $l \in \Phi$.
- $(r, m) \models \bot$ never holds.
- $(r, m) \models K_i\varphi$
  iff $(r', m') \models \varphi$ for any point (r', m) such that
  $(r, m) \sim_i (r', m')$.
- $(r, m) \models \Box\varphi$ iff $(r, m') \models \varphi$ for all $m' \geqslant m$.
- $(r, m) \models \Diamond\varphi$ iff $(r, m') \models \varphi$ for some $m' \geqslant m$.
- $(r, m) \models \varphi \supset \psi$ iff $(r, m) \not\models \varphi$ or $(r, m) \models \psi$.

Asynchrony in Epistemic Logic with Time (3)

A class $\mathcal{C}_n^{amp}$ of interpreted systems called asynchronous message-passing systems [Fagin et al., 2003]

A history h over Σ_i, INT_i and MSG is a nonempty finite sequence with

- $h_0 \in \Sigma_i$
- $h_k \in \{send(\mu, j, i), receive(\mu, j, i) \mid \mu \in MSG, 1 \leqslant j \leqslant n\}$ $\cup \{int(a, i) \mid a \in INT_i\}$ for $k > 0$.

Let $L_i (1 \leqslant i \leqslant n)$ be a prefix-closed set of histories.

Let $\mathcal{R}$ be the set of runs r satisfying

- $f_i(r(0))$ is a history of length one.
- $f_i(r(m+1))$ is identical to $f_i(r(m))$ or a history obtained by appending one element to $f_i(r(m))$
- for every $receive(\mu, j, i)$ appearing in $f_i(r(m))$, there exists an event $send(\mu, i, j)$ appearing in $f_j(r(m))$.

$\mathcal{I} = (\mathcal{R}, \pi)$ is a.m.p. iff $\mathcal{R}$ can be constructed in this way.

Axiomatisable?

"At this point, we do not even have a candidate for a sound and complete axiomatization of $\mathcal{C}_n^{amp}$".
[Fagin et al., 2003, Notes, Ch. 8]

An important observation in [Fagin et al., 2003]

> The processes can gain or lose knowledge only by sending and receiving messages.

This (ignoring "sending and") seemed intuitionistic to the speaker.

Asynchronous Communication in an Intuitionistic Epistemic Logic

Extending Browuer–Heyting–Kolmogorov Interpretation with Knowledge

Browuer–Heyting–Kolmogorov interpretation taken from [Troelstra and van Dalen, 1988]
Intuitionistic connective interpretation explained (for non-intuitionists).

- (H1) A proof of $\varphi \wedge \psi$ is given by presenting a proof of φ and a proof of ψ.
- (H2) A proof of $\varphi \vee \psi$ is given by presenting either a proof of φ or a proof of ψ (plus the stipulation that we want to regard the proof presented as evidence for $\varphi \vee \psi$ [plus left or right information]).
- (H3) A proof of $\varphi \supset \psi$ is a construction which permits us to transform any proof of φ into a proof of ψ.
- (H4) Absurdity $\perp$ (contradiction) has no proof; a proof of $\neg\varphi$ is a construction which transforms any hypothetical proof of φ into a proof of a contradiction.

Extending Browuer–Heyting–Kolmogorov Interpretation with Knowledge

(HK) A proof of $K_p\varphi$ is a construction that witnesses agent p's acknowledgement of a proof of φ and also contains the acknowledged proof.

(H1) A proof of $\varphi \wedge \psi$ is given by presenting a proof of φ and a proof of ψ.

(H2) A proof of $\varphi \vee \psi$ is given by presenting either a proof of φ or a proof of ψ (plus the stipulation that we want to regard the proof presented as evidence for $\varphi \vee \psi$ [plus left or right information]).

(H3) A proof of $\varphi \supset \psi$ is a construction which permits us to transform any proof of φ into a proof of ψ.

(H4) Absurdity $\perp$ (contradiction) has no proof; a proof of $\neg\varphi$ is a construction which transforms any hypothetical proof of φ into a proof of a contradiction.

New informal reading of $K_p\varphi$

The single most important slide.
$K_p\varphi$: p knows φ.
(What does "know" mean?)

p has acknowledged a proof of φ.

c.f. Plato: *Theaetetus*. Knowledge is ...

1. perception
2. a true opinion
3. a true opinion with explanation

New informal reading of $K_p\varphi$

The single most important slide.
$K_p\varphi$: p knows φ.
(What does "know" mean?)

p has acknowledged a proof of φ.

c.f. Plato: *Theaetetus*. Knowledge is ...

1. perception
2. a true opinion
3. a true opinion with explanation

All refuted by Socrates.

New informal reading of $K_q K_p \varphi$: COMMUNICATION

$K_q K_p \varphi$: q knows p knows φ.

Classical	In all q's possible worlds, in all p's possible worlds, φ is true.
This work	q has received a proof of the fact that p has received a proof of φ. communication from p to q

Deduction System

$$(\mathsf{T})\ \frac{\Gamma \vdash K_p\varphi}{\Gamma \vdash \varphi} \qquad (\text{introspection})\ \frac{\Gamma \vdash K_p\varphi}{\Gamma \vdash K_pK_p\varphi}$$

$$(\text{nec})\ \frac{\Gamma \vdash \varphi}{K_p\Gamma \vdash K_p\varphi} \qquad (\vee K)\ \frac{\Gamma \vdash K_p(\varphi \vee \psi)}{\Gamma \vdash K_p\varphi \vee K_p\psi}$$

$$(\wedge\text{-E}_0)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} \qquad (\wedge\text{-I})\ \frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \varphi \wedge \psi} \qquad (\wedge\text{-E}_1)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$(\vee\text{-I}_0)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \qquad (\text{ax})\ \frac{}{\varphi \vdash \varphi} \qquad (\vee\text{-I}_1)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi}$$

$$(\vee\text{-E})\ \frac{\Gamma \vdash \psi_0 \vee \psi_1 \qquad \Gamma, \psi_0 \vdash \varphi \qquad \Gamma, \psi_1 \vdash \varphi}{\Gamma \vdash \varphi}$$

$$(\supset\text{-I})\ \frac{\varphi, \Gamma \vdash \psi}{\Gamma \vdash \varphi \supset \psi} \qquad (\supset\text{-E})\ \frac{\Gamma \vdash \psi_0 \supset \psi_1 \qquad \Gamma \vdash \psi_0}{\Gamma \vdash \psi_1} \qquad (\bot\text{-E})\ \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}$$

Double negation elimination would make φ and $K_p\varphi$ equivalent.

Formal Semantics = Intuitionistic Logic (with Knowledge)

model $\langle W, \preceq, (f_p)_{p \in P} \rangle$

$f_p \colon W \to W$: idempotent, decreasing, monotonic

1. $f_p(f_p(w)) = f_p(w)$
2. $f_p(w) \preceq w$
3. $v \preceq w \Rightarrow f_p(v) \preceq f_p(w)$

valuation $\rho \colon \mathrm{PVar} \to \mathcal{P}(W)$

$\rho(I)$: upward-closed

Formal Semantics

We define $w \models \varphi$ for $w \in W$ and a formula φ:

$$w \models K_p\psi \quad \Leftrightarrow \quad f_p(w) \models \psi$$

$$w \models \bot \quad \Leftrightarrow \quad \text{never}$$

$$w \models I \quad \Leftrightarrow \quad w \in \rho(I)$$

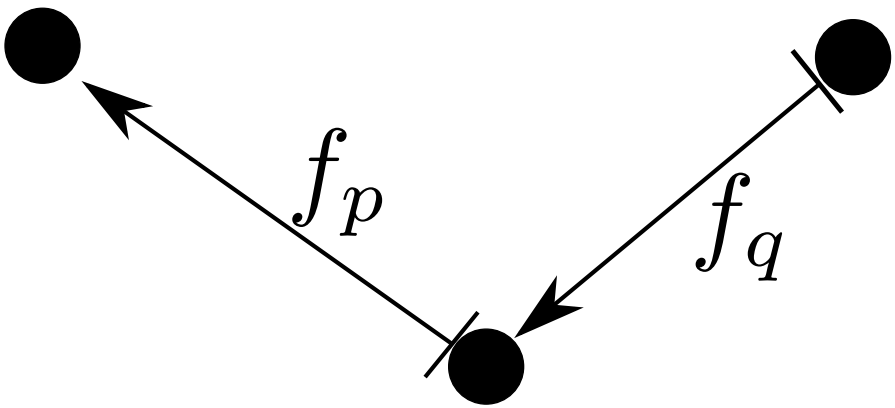
$$w \models \psi_0 \wedge \psi_1 \quad \Leftrightarrow w \models \psi_0 \text{ and } w \models \psi_1 \text{ hold}$$

$$w \models \psi_0 \vee \psi_1 \quad \Leftrightarrow w \models \psi_0 \text{ or } w \models \psi_1 \text{ holds}$$

$$w \models \psi_0 \supset \psi_1 \quad \Leftrightarrow v \models \psi_0 \text{ implies } v \models \psi_1 \text{ for any } v \succeq w.$$

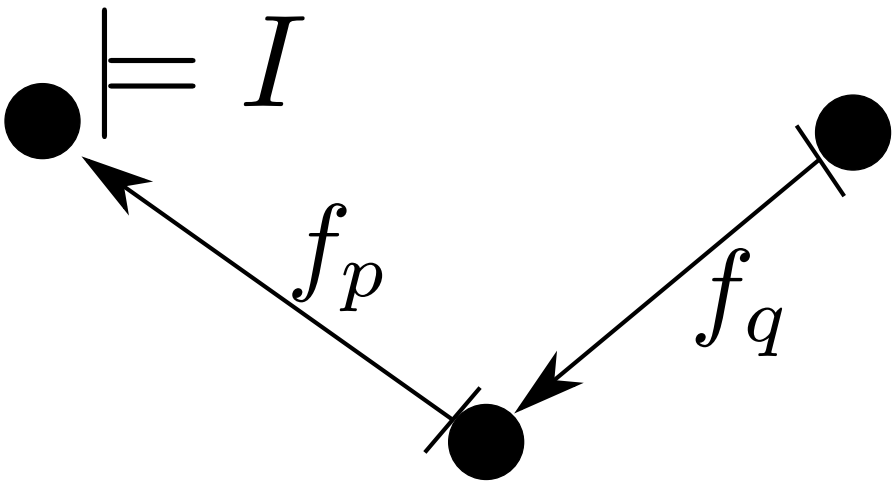
Formal Semantics

past $\preceq$ future



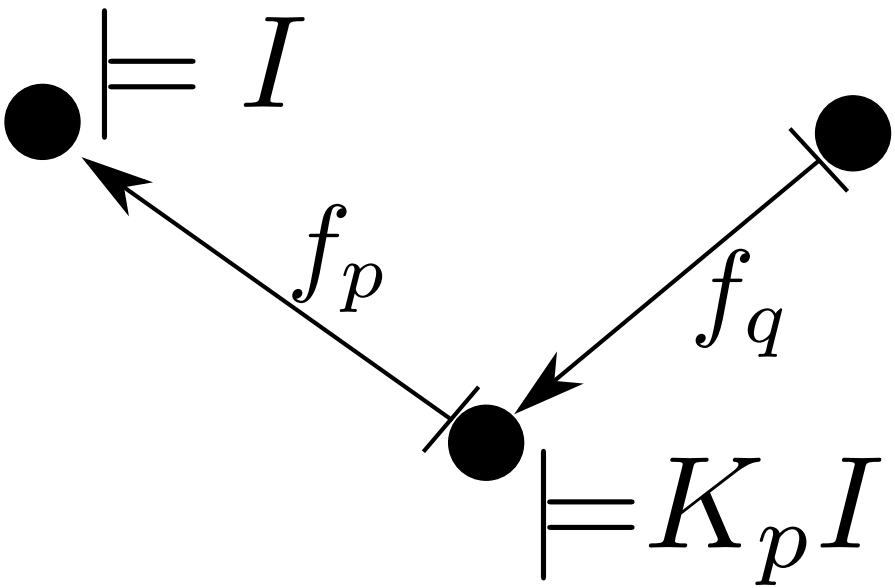
Formal Semantics

past $\preceq$ future



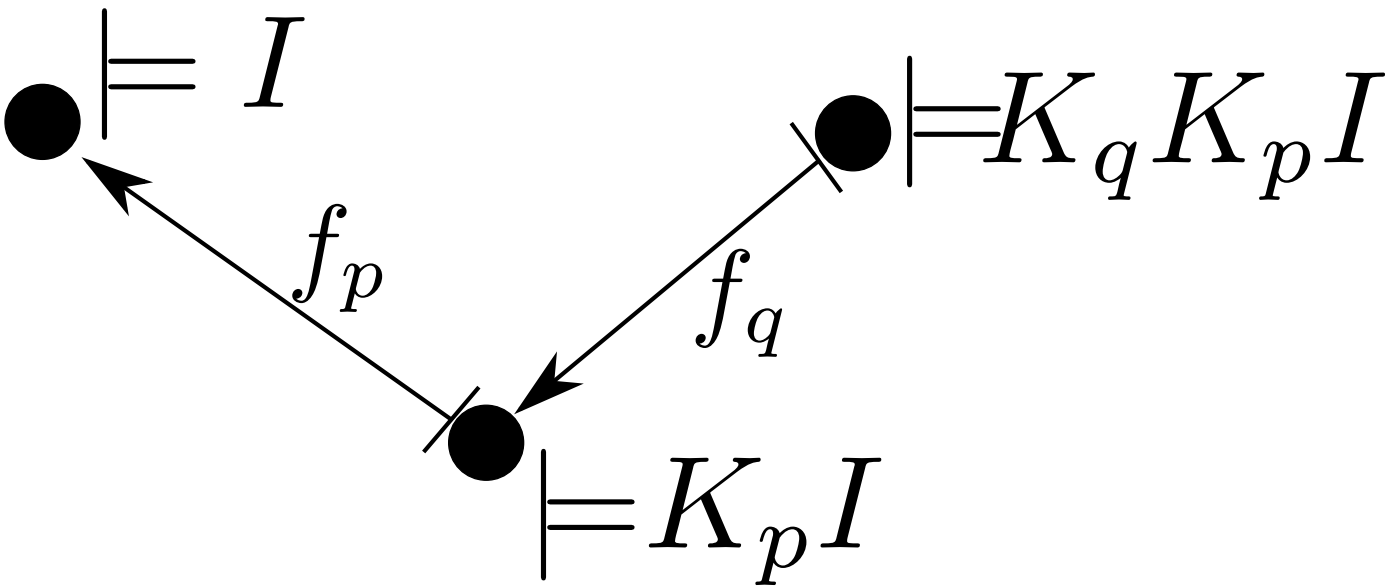
Formal Semantics

past $\preceq$ future



Formal Semantics

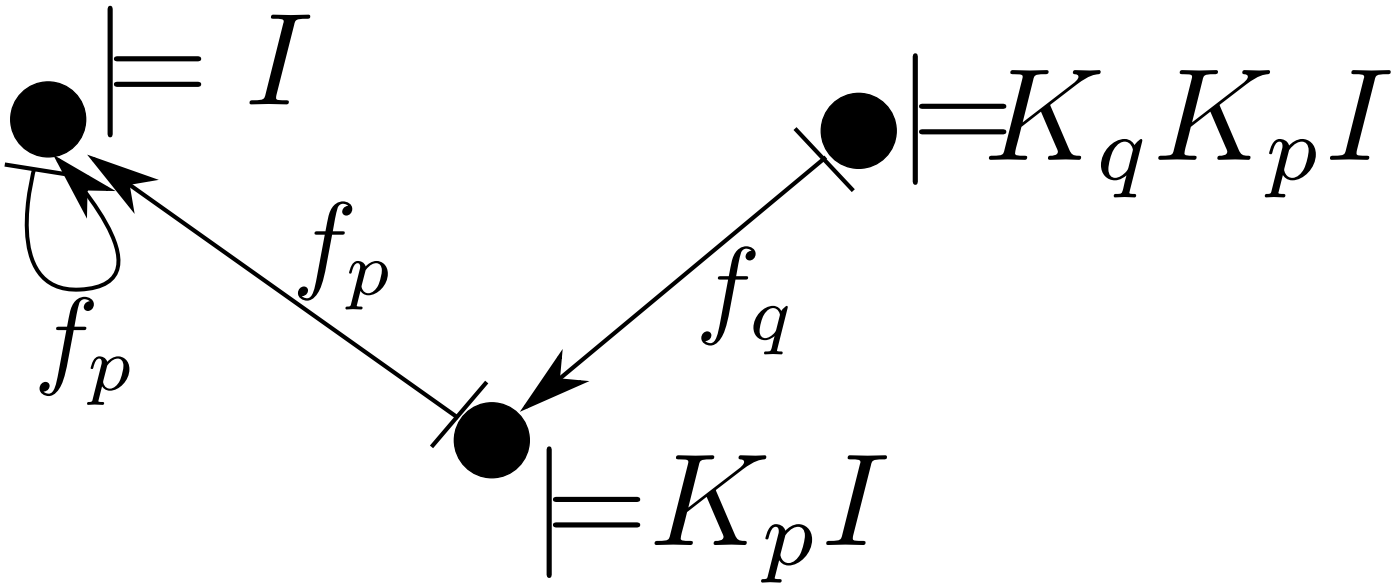
past $\preceq$ future



Formal Semantics

past $\preceq$ future

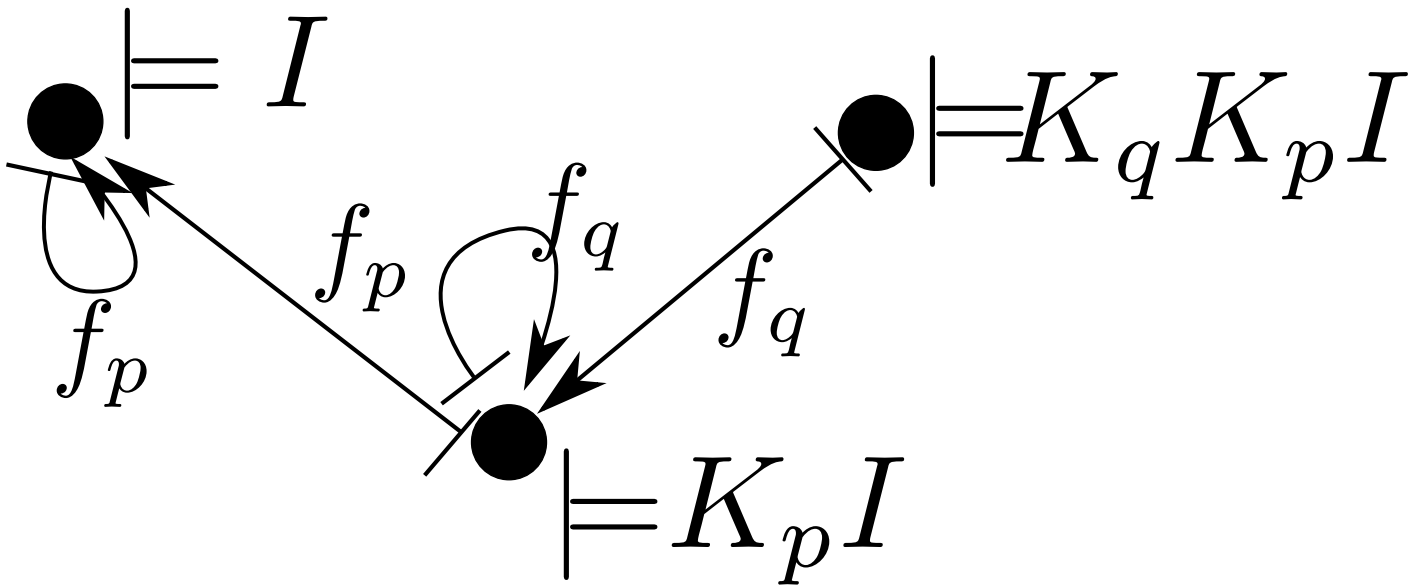
p's state.



Formal Semantics

past $\preceq$ future

p's state. q's state.



An example

Modelling Sequential Consistency

[LPAR-16, Hirai]

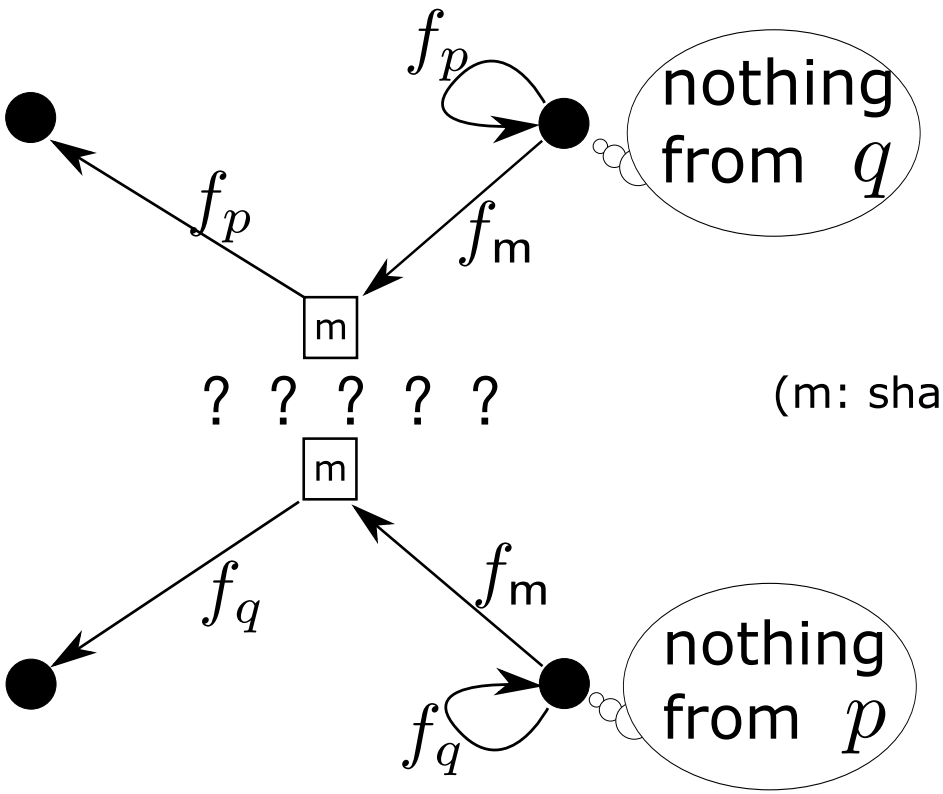
Need for shared memory consistency

Assumption: full-information

- A message contains all knowledge of its sender.
- Nothing is ever forgotten.

Even under this assumption, no communication is guaranteed between processes (or CPU's).

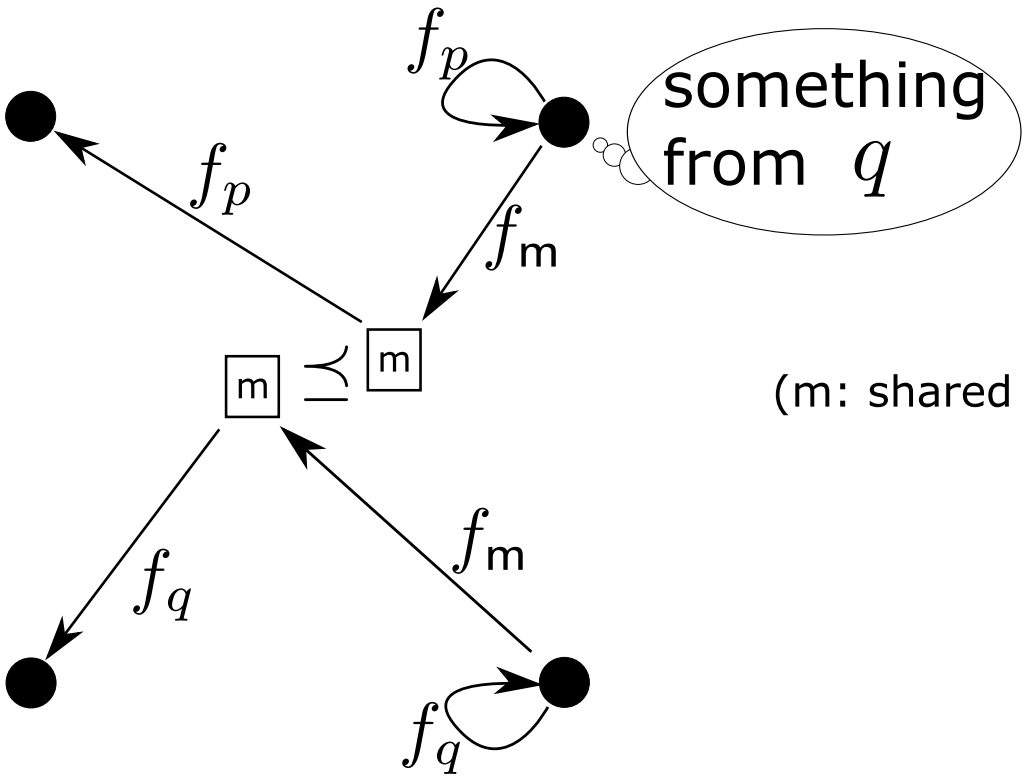
Need for shared memory consistency



(m: shared memory)

Essence of Sequential Consistency

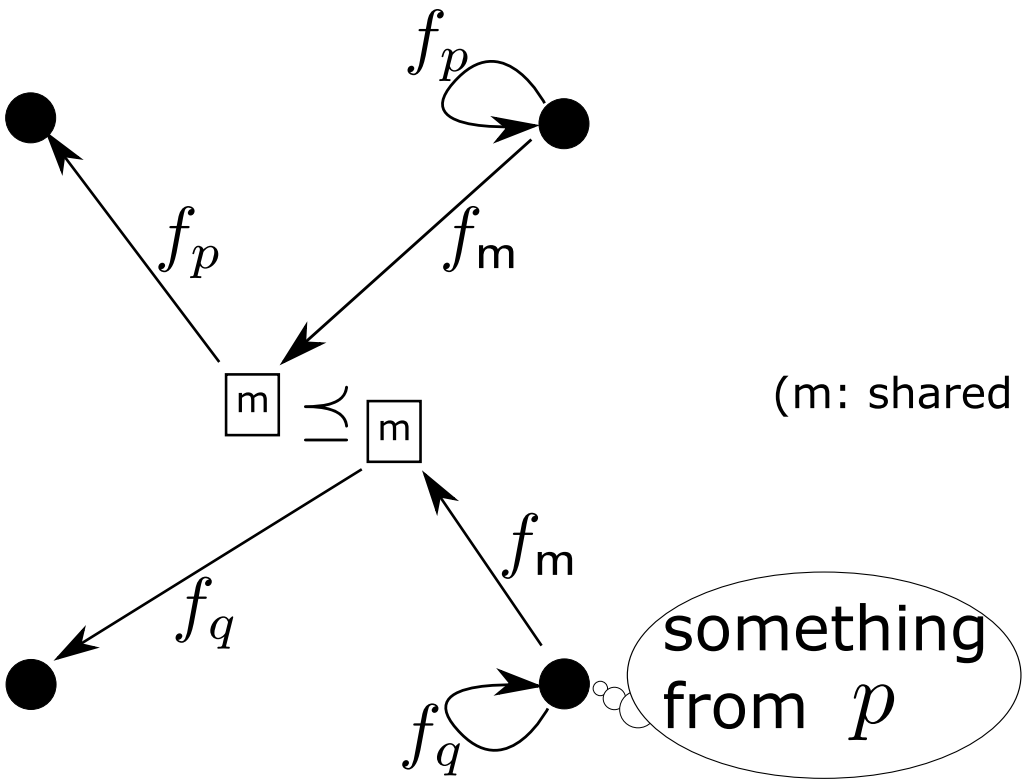
For two memory states, either $\preceq$ or $\succeq$ holds.



(m: shared memory)

Essence of Sequential Consistency

For two memory states, either $\preceq$ or $\succeq$ holds.



(m: shared memory)

Logical Background: logic **Lin** for linear models

Lin = Intuitionistic + $(\varphi \supset \psi) \vee (\psi \supset \varphi)$:

Intuitionistic $\subsetneq$ **Lin** $\subsetneq$ Classical

Well-known property:

$$\textbf{Lin} \vdash \theta \Longleftrightarrow M \models \theta$$

for all linear Kripke model M.

(Linear model: for any two states, $\preceq$ or $\succeq$.)

SC for Sequential Consistency

$$\textbf{SC} = \text{Int. Epistemic} + (K_m\varphi \supset K_m\psi) \vee (K_m\psi \supset K_m\varphi)$$

$$\text{Int. epistemic} \subsetneq \textbf{SC} \subsetneq \text{Epistemic}$$

A result:

$$\textbf{SC} \vdash \theta \Longleftrightarrow M \models \theta$$

for all sequential model M.

(Sequential model: for any two memory states, $\preceq$ or $\succeq$ holds.)

An example theorem under sequential consistency

$$\vdash ((K_p K_m K_p I) \wedge K_q K_m K_q J) \supset ((K_q K_p I) \vee K_p K_q J)$$

1. p sends a proof of I to m, then m replies to p.
2. q sends a proof of J to m, then m replies to q.
3. then, p's knowledge I has been transmitted to q, or q's knowledge J has been transmitted to p.

Theoretical Results

Soundness and Strong Completeness

$$\Gamma \models \varphi \quad \Longleftrightarrow \quad \Gamma \vdash \varphi.$$

Proof strategy

Following [Troelstra and van Dalen, 1988].

For a formula $\Gamma \not\vdash \varphi$,
we construct a model M and a state $w \in M$
so that $M, w \models \Gamma$ but not $M, w \models \varphi$.

Disjunction Property

[in the NASSLLI student session paper.]

$$\vdash \varphi \vee \psi \quad \Longrightarrow \quad \vdash \varphi \text{ or } \vdash \psi$$

Proof strategy

By extending Aczel's slash relation [Troelstra and van Dalen, 1988] by

$$\Gamma \mid K_p\varphi \Longleftrightarrow f_p(\Gamma) \mid \varphi$$

where $f_p(\Gamma)$ (agent p's view on a set of formulae Γ) defined as ...

where $f_p(\Gamma)$ (agent p's view on a set of formulae Γ) defined as

- $g_p(\Gamma) = \{\varphi \in \mathsf{Fml} \mid (K_p)^+\varphi \in \Gamma$ and φ does not begin with $K_p\}$,
- $f_p(\Gamma) = g_p(\Gamma) \cup K_p g_p(\Gamma) \cup \{\varphi \in \mathsf{Fml} \mid \Gamma \vdash \bot\}$.

Finite model property

[in the NASSLLI student session paper.]

$M \models \varphi$ for all finite $M \Longleftrightarrow \vdash \varphi$.

Proof strategy

For a formula $\nvdash \varphi$,
we construct a finite model M and a state $w \in M$
so that $M, w \not\models \varphi$.

However ...

The traditional method does not work only looking at the formulae in a subformula-closed set Ω. Reason: $f_p \colon W \to W$ does not hold.

Instead

W to be the set of pairs (Ω, Γ) where Γ is Ω-saturated.
(Ω is closed for taking a subformula and replacing K_pK_p with K_p).
(Ω does not contain a longer formula).

$F_p((\Omega, \Gamma)) = (f'_p(\Omega), f'_p(\Gamma))$ where

- $f'_p(\Omega) = g_p(\Omega) \cup K_p g_p(\Omega)$.

Trying to find a simpler proof while I'm in Bloomington.

What follows

- Typed lambda calculus [submitted to APLAS 2010]
  - Types as protocol.
  - supports asynchronous RPC facility “future” [Walker et al., 1990]
- Quantify agents $\exists x K_x \varphi$
- Knowledge of forking and merging agents (forking creates common knowledge).


Fagin, R., Halpern, J., Moses, Y., and Vardi, M. (2003).
Reasoning about knowledge.
The MIT Press.


Herlihy, M. and Shavit, N. (1999).
The topological structure of asynchronous computability.
Journal of the ACM (JACM), 46(6):858–923.


Troelstra, A. and van Dalen, D. (1988).
Constructivism in Mathematics: An Introduction: Vol.: 1.
North-Holland.


Walker, E., Floyd, R., and Neves, P. (1990).
Asynchronous remote operation execution in distributed systems.
In Distributed Computing Systems, 1990. Proceedings., 10th International Conference on, pages 253–259.