An Intuitionistic Epistemic Logic for Sequential Consistency on Shared Memory

Yoichi Hirai

2010-04-27, Dakar

Motivation

- Treating asynchronous communication using an "epistemic logic".
- Shared memory consistency is an example of asynchronous communication.

Informal reading of $K_p\varphi$

in epistemic logic [Hintikka, 1962]

$K_p\varphi$: p knows φ.
(What does "know" mean?)

In all p's possible worlds, φ is true.

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.

Extending Browuer–Heyting–Kolmogorov Interpretation with Communication

Browuer–Heyting–Kolmogorov interpretation taken from [Troelstra and van Dalen, 1988]

- (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

Extending Browuer–Heyting–Kolmogorov Interpretation with Communication

(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

New informal reading of $K_p\varphi$

$K_p\varphi$: p knows φ.
(What does "know" mean?)

p has received a proof of φ.

c.f. Plato: *Theaetetus*.

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.

Deduction System

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

$$(\text{necessitation})\ \frac{\Gamma \vdash \varphi}{K_p\Gamma \vdash K_p\varphi}$$

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

$$(\mathsf{ax})\ \frac{}{\varphi \vdash \varphi} \qquad (\mathsf{w})\ \frac{\Gamma \vdash \varphi}{\psi, \Gamma \vdash \varphi} \qquad (\mathsf{c})\ \frac{\varphi, \varphi, \Gamma \vdash \varphi'}{\varphi, \Gamma \vdash \varphi'} \qquad (\mathsf{e})\ \frac{\Gamma, \varphi, \psi, \Gamma' \vdash \varphi'}{\Gamma, \psi, \varphi, \Gamma' \vdash \varphi'}$$

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

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

$$(\Gamma) \qquad \Gamma \vdash \psi_0 \vee \psi_1 \qquad \Gamma, \psi_0 \vdash \varphi \qquad \Gamma, \psi_1 \vdash \varphi$$

Formal Semantics = Intuitionistic Logic (with Knowledge)

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

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

valuation $\rho \colon \mathrm{PVar} \to \mathcal{P}(W)$ $\rho(I)$: upward-closed

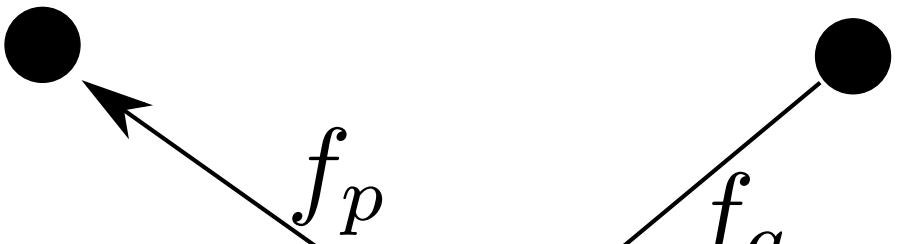
Define $w \models \varphi$ for a state $w \in W$ and

Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future

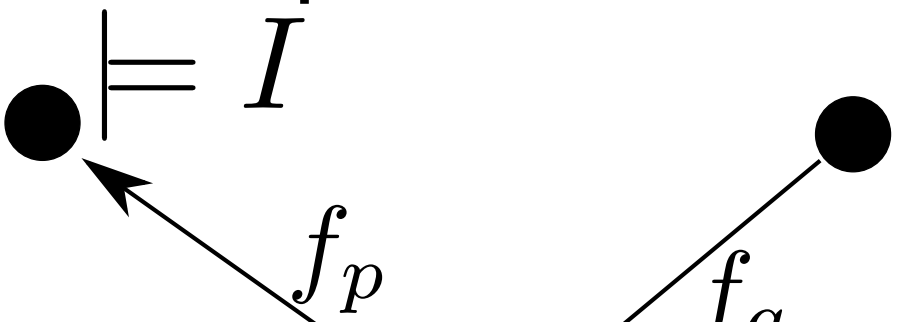


Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\leq$ future

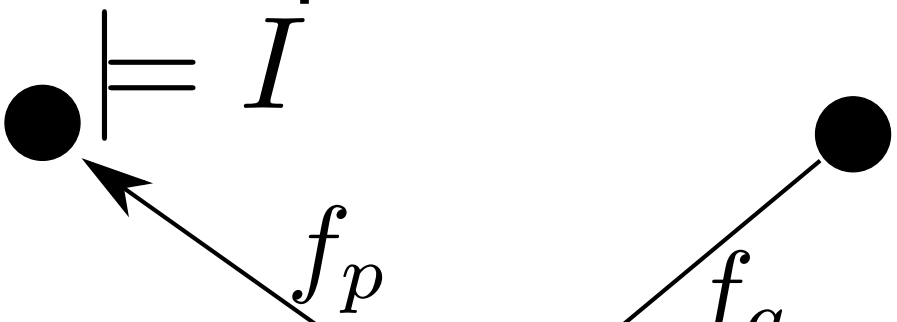


Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\leq$ future

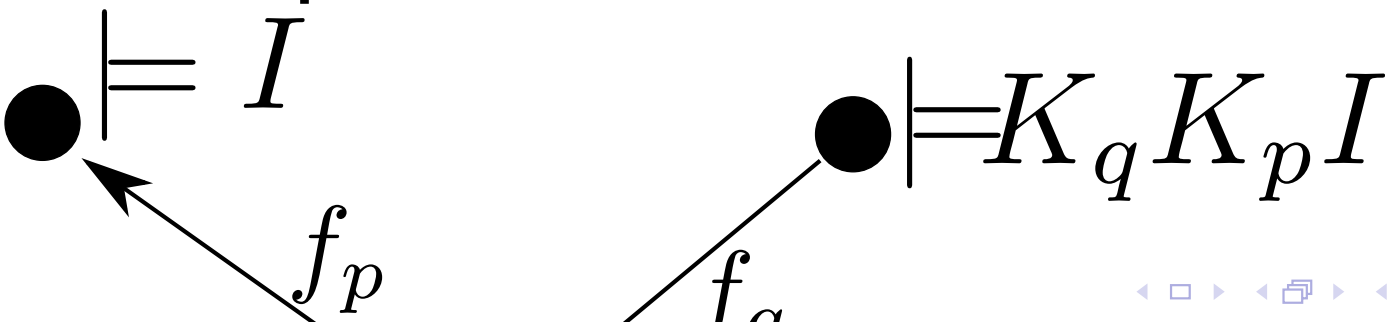


Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\leq$ future



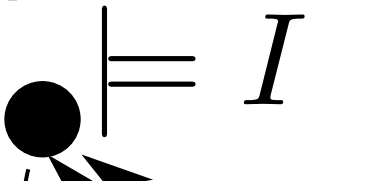
Formal Semantics = Intuitionistic Logic (+ Knowledge)

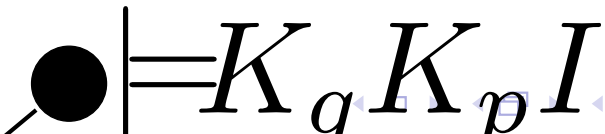
model $\langle W, \leq, (f_p)_{p \in P} \rangle$

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

past $\leq$ future

p's state.





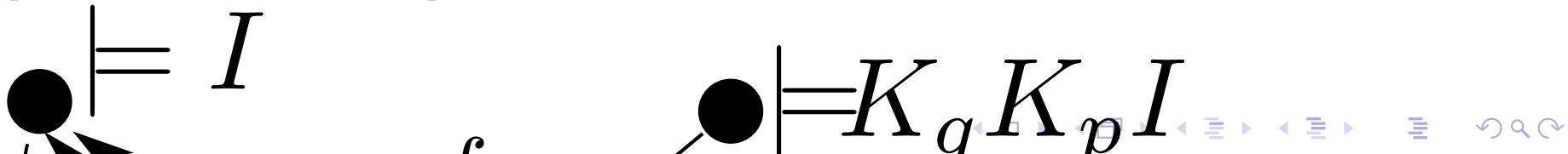
Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\leq$ future

p's state. q's state.



Soundness and Strong Completeness

$$\Gamma \models \varphi \iff \Gamma \vdash \varphi.$$

Proof strategy

Following
[Troelstra and van Dalen, 1988].

For a formula $\Gamma \nvdash \varphi$,
we construct a model M and a state $w \in M$

Disjunction Property

[not in LPAR-16 paper, accepted to NASSLLI student session.]

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

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

Finite model property

[not in LPAR-16 paper, accepted to NASSLLI student session.]

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

Proof strategy

For a formula $\not\vdash \varphi$,

we construct a finite model M and a state $w \in M$

so that $M, w \not\models \varphi$.

The same method does not work:

An example

Modelling Sequential Consistency

Need for shared memory consistency

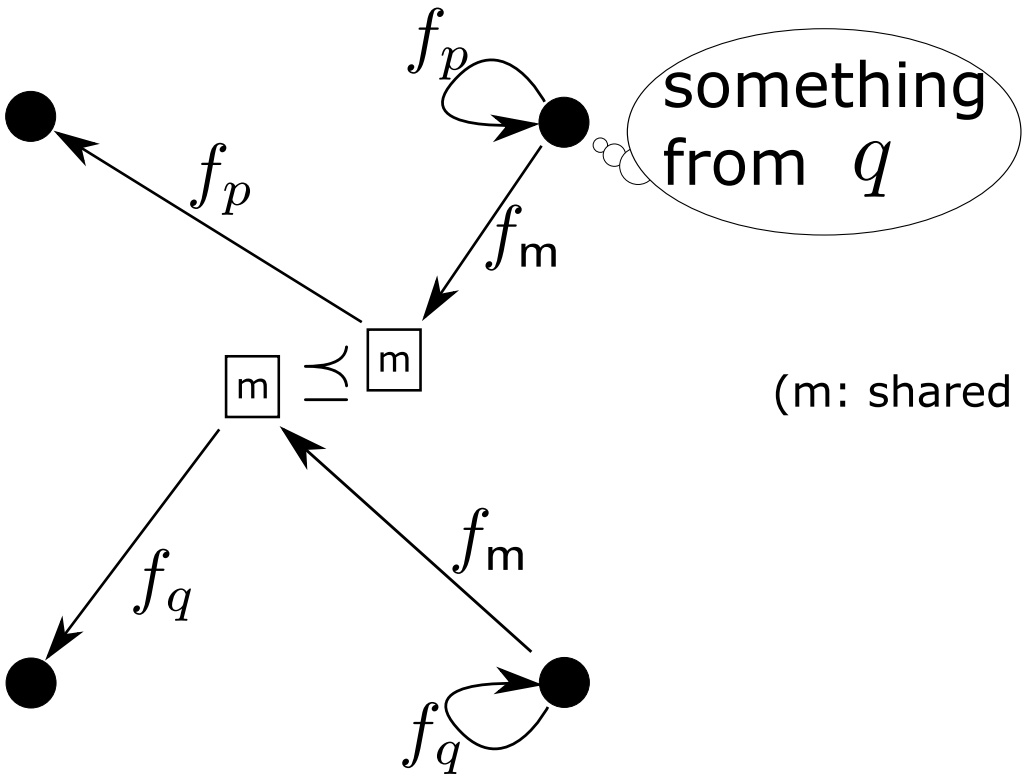
Assumption: full-information

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

Even under this assumption, no communication is guaranteed between processes.

Essence of Sequential Consistency

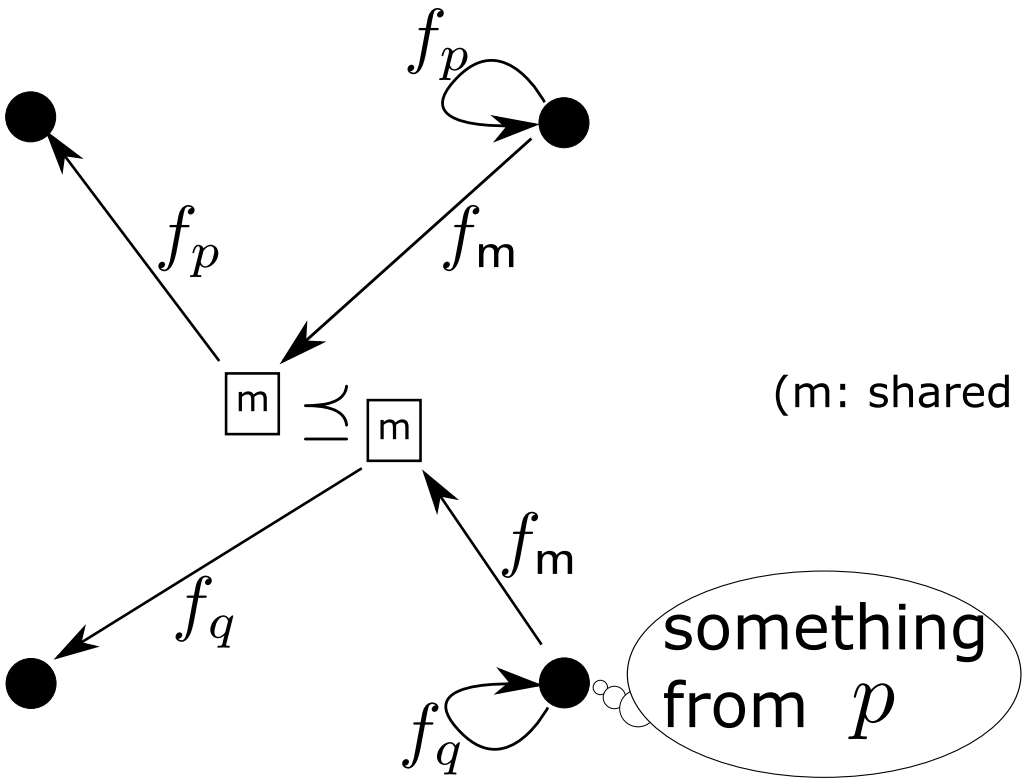
For two memory states, either $\preceq$ or $\succeq$ holds.



(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 logic + $(\varphi \supset \psi) \vee (\psi \supset \varphi)$:

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

Well-known property:

Lin $\vdash \theta \Longleftrightarrow M \models \theta$ for all linear Kripke model M

(Linear model: for any two states,

A logic **SC** for Sequential Consistency

SC = Int. Epistemic logic + $(K_m\varphi \supset K_m\psi) \vee (K_m\psi \supset K_m\varphi)$:

Intuitionistic epistemic logic $\subsetneq$ **SC** $\subsetneq$ Classical logic

A result:

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

for all sequential model M

(Sequential model: for any two

An example theorem under sequential consistency

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

Informal reading

- p sends a proof of I to m, then m replies to p.
- q sends a proof of J to m, then m replies to q.

Ongoing work: finite sequential model property of **SC**

Trying to avoid

- logically possible but computationally impossible schedules like

$$\overbrace{t_0 \precneqq t_1 \precneqq t_2 \precneqq \cdots \precneqq t_n \precneqq \cdots}^{\text{infinite}} \precneqq t'$$

An example of the example

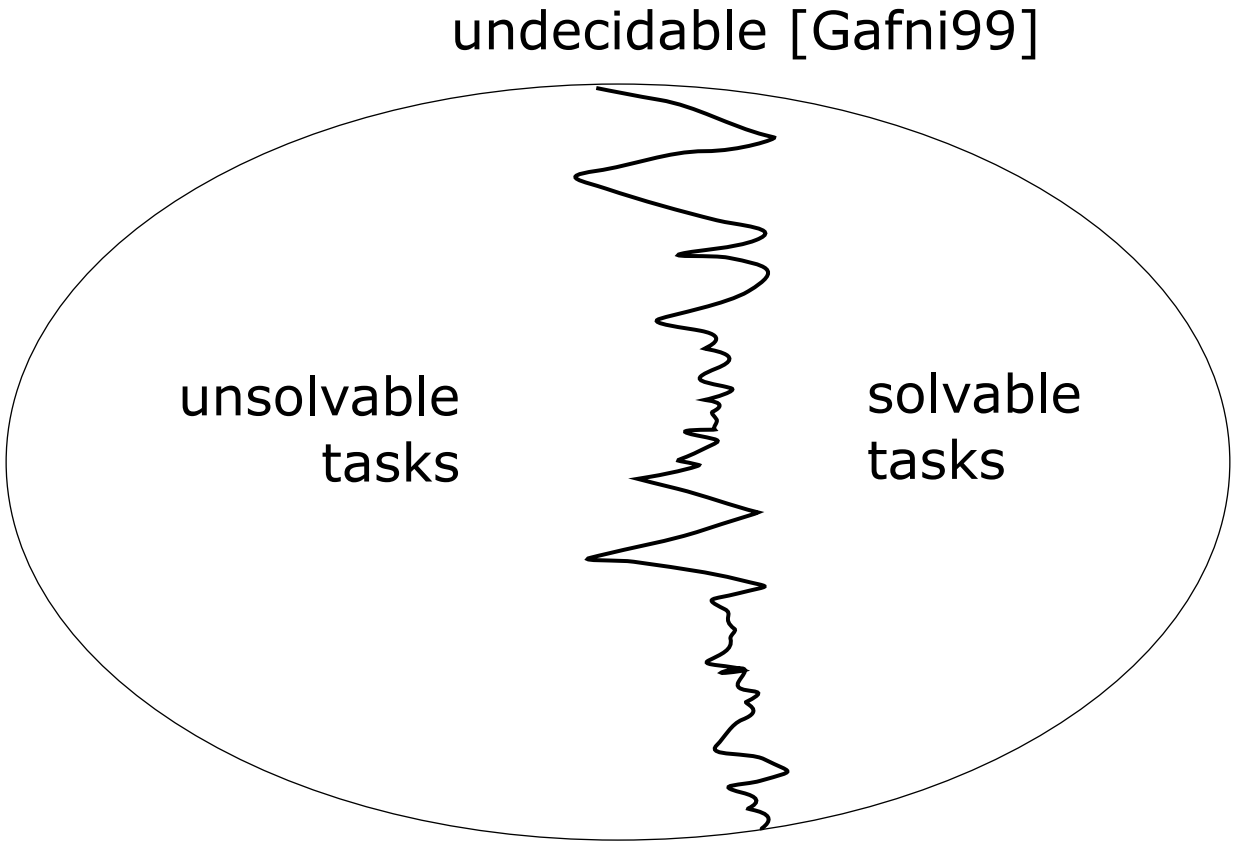
Decidable Abstraction of Waitfreely Solvable Tasks

Is a task waitfreely solvable or not?

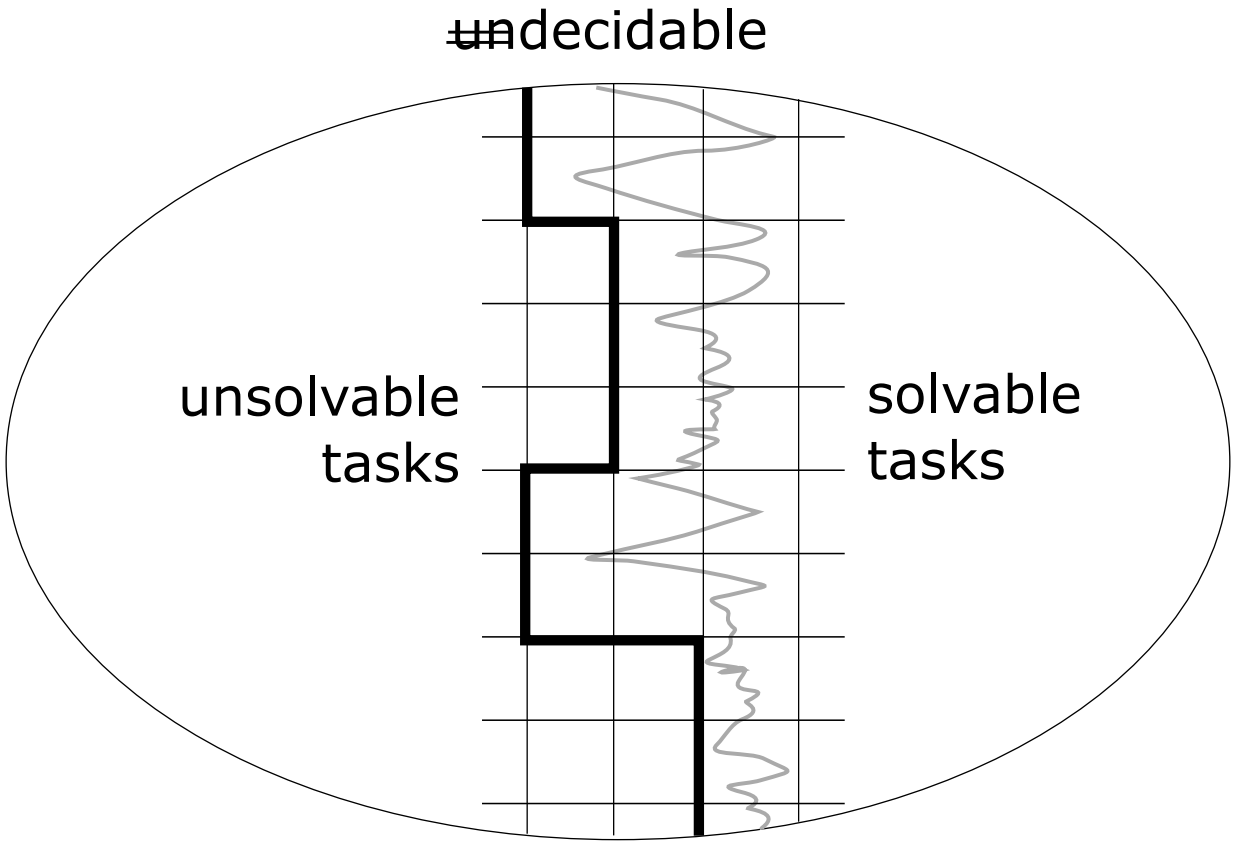
Original task: undecidable

Abstract task: decidableq

Contribution 2: Decidable abstraction of waitfreely solvable tasks



Contribution 2: Decidable abstraction of waitfreely solvable tasks



Future Work

Extending program extraction to concurrent/distributed computation.

- Making proofs constructive.
- Modelling other memory consistencies: especially PRAM consistency, cache consistency and processor consistency
- Typed lambda calculus


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


Hintikka, J. (1962).
Knowledge and belief: an introduction to the logic of the two notions.

Cornell University Press.


Lamport, L. (1997).
How to make a correct multiprocess program execute correctly on a multiprocessor.
IEEE Transactions on Computers, 46(7):779–782.


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

Today, I got 25 years old.