# An Intuitionistic Epistemic Logic

Yoichi Hirai

2010-03-12, Kanazawa

# Motivation

Applying program extraction (modified realizability) to generating asynchronously communicating programs.

# A standard reference: *Reasoning about Knowledge* [Fagin et al., 2003]

Warning: for the speaker, the formalisation below is complicated.

Let us fix
$\Phi$: 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 $\mathcal{G}$.
- $\pi : \mathcal{G} \to \Phi \to \{\top, \bot\}$.

# 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 $m' \geqslant m$.
- $(r, m) \models K_i\varphi$
  iff $(\mathcal{I}, r', m') \models \varphi$ for any point $(r', m)$ such that
  $(r, m) \sim_i (r', m')$.
- $(r, m) \models \varphi \supset \psi$ iff $(r, m) \not\models \varphi$ or $(r, m) \models \psi$.

# Asynchronous communication in [Fagin et al., 2003]

A class $\mathcal{C}_n^{amp}$ of interpreted systems called asynchronous message-passing systems.

A history $h$ over $\Sigma_i, INT_i$ 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 $\varphi$ and a proof of $\psi$.

(H2) A proof of $\varphi \vee \psi$ is given by presenting either a proof of $\varphi$ or a proof of $\psi$ (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 $\varphi$ into a proof of $\psi$.

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

# 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 $\varphi$ and also contains the acknowledged proof.

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

(H2) A proof of $\varphi \vee \psi$ is given by presenting either a proof of $\varphi$ or a proof of $\psi$ (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 $\varphi$ into a proof of $\psi$.

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

# An Anonymous Refree's Comment

> this is at odds with real life applications, where an agent often has just disjunctive knowledge, So he can e.g. have a proof (evidence) that John works for either CIA or FBI, without having a prooof that he works for CIA or that he works for FBI.

- This is not consistent with the BHK-interpretation.
- The author should have explained BHK-interpretation in detail.

# An Anonymous Refree's Comment

> this is at odds with real life applications, where an agent often has just disjunctive knowledge, So he can e.g. have a proof (evidence) that John works for either CIA or FBI, without having a prooof that he works for CIA or that he works for FBI.

- This is not consistent with the BHK-interpretation.
- The author should have explained BHK-interpretation in detail.
- FBI and CIA have secrets so that they sometimes make non-constructive proofs?

# An Anonymous Refree's Comment

> this is at odds with real life applications, where an agent often has just disjunctive knowledge, So he can e.g. have a proof (evidence) that John works for either CIA or FBI, without having a prooof that he works for CIA or that he works for FBI.

- This is not consistent with the BHK-interpretation.
- The author should have explained BHK-interpretation in detail.
- FBI and CIA have secrets so that they sometimes make non-constructive proofs?
- Let us take a notion of proof satisfying BHK-interpretation.

# New informal reading of $K_p\varphi$

Formulae $\varphi ::= \bot \mid I \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \supset \varphi \mid K_p\varphi$.
all interpretable in classical epistemic logic
(widely attributed to [Hintikka, 1962], writes [Ditmarsch et al., 2007]).

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

**Classical** In all $p$'s possible worlds, $\varphi$ is true.

**This work** $p$ has received a proof of $\varphi$.

c.f. Plato: *Theaetetus*.

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

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

$K_q K_p \varphi$: $q$ knows that $p$ knows $\varphi$.

Classical In all $q$'s possible worlds, in all $p$'s possible worlds, $\varphi$ is true.
(Maybe useful for a philosopher defending conventionalism following David Lewis.)

This work $q$ has received a proof of the fact that $p$ has received a proof of $\varphi$.
Communication from $p$ to $q$

# Do we have this: $(K_p(\varphi \vee \psi)) \supset (K_p\varphi \vee K_p\psi)$

nnnn Analysis of the creative subject by [Dummett, 2000, p.237].

$$\forall n((\vdash_n A) \wedge (\vdash_n B) \rightarrow (\vdash_n (A \wedge B)))$$

is “less evident” than

$$\forall n((\vdash_n A) \vee (\vdash_n B) \leftrightarrow (\vdash_n (A \vee B))).$$

Analogously,

$$K_p(A \wedge B) \supset (K_p(A \wedge B))$$

is less evident than

$$K_p(A \vee B) \supset (K_p(A \vee B)).$$

# Deduction System

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

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

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

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

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

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

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

If we add the double negation elimination, we obtain $\varphi \supset K_p\varphi$.

# 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

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

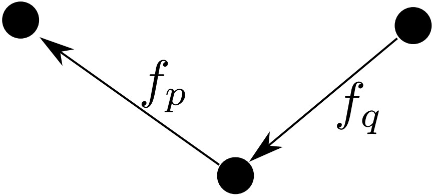
Define $w \models \varphi$ for a state $w \in W$ and a formula $\varphi$:

$$\begin{aligned}
w \models \bot \quad &\Leftrightarrow \quad \text{never} \\
w \models I \quad &\Leftrightarrow \quad w \in \rho(I) \\
w \models K_p\psi \quad &\Leftrightarrow \quad f_p(w) \models \psi \\
w \models \psi_0 \wedge \psi_1 \quad &\Leftrightarrow \quad \text{both } w \models \psi_0 \text{ and } w \models \psi_1 \text{ hold} \\
w \models \psi_0 \vee \psi_1 \quad &\Leftrightarrow \quad \text{either } w \models \psi_0 \text{ or } w \models \psi_1 \text{ holds} \\
w \models \psi_0 \supset \psi_1 \quad &\Leftrightarrow \quad v \models \psi_0 \text{ implies } v \models \psi_1 \text{ for any } v \succeq w.
\end{aligned}$$

# 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

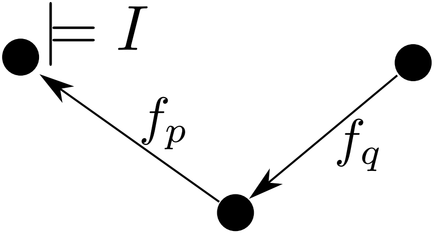


# Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future

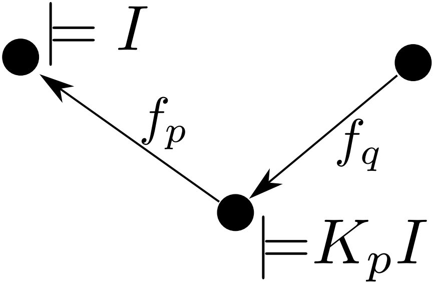


# Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future

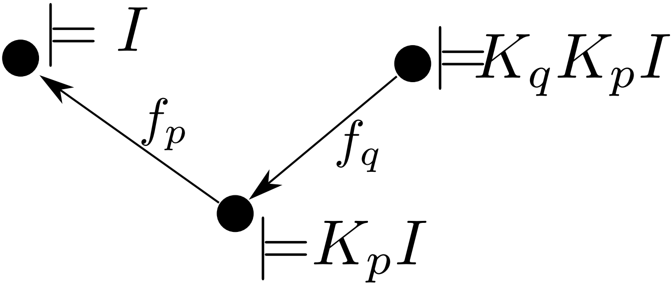


# Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future



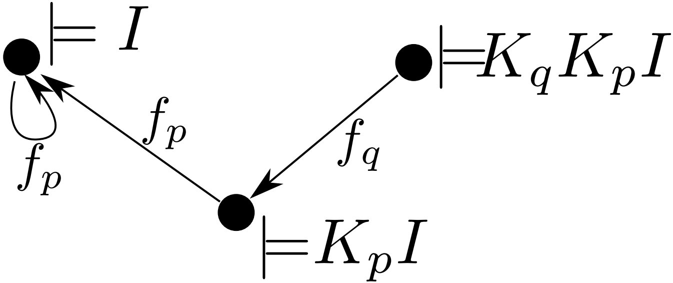
# Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future

$p$'s state.



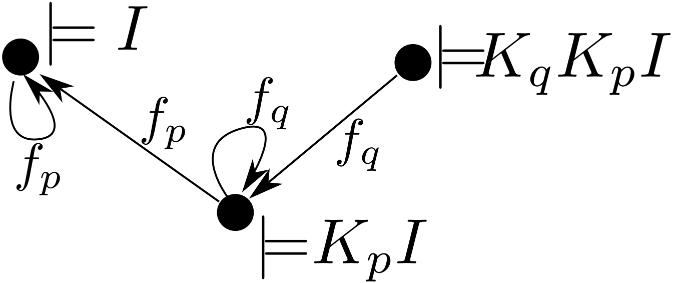
# Formal Semantics = Intuitionistic Logic (+ Knowledge)

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

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

past $\preceq$ future

$p$'s state. $q$'s state.



# 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 $M, w \models \varphi$.

By
$W$ is the set of saturated sets of formulae.
$f_p(\Gamma) = \{\varphi \mid K_p\varphi \in \Gamma\}$.
Checking $f_p$ is actually $W \to W$ requires the rule $(\vee K)$.

# Disjunction Property

$\vdash \varphi \vee \psi \quad \Longrightarrow \quad \vdash \varphi$ 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 $\Gamma$) defined as

$$\begin{aligned} g_p(\Gamma) &= \{\varphi \in \mathrm{Fml} \mid (K_p)^+\varphi \in \Gamma \text{ and } \varphi \text{ does not begin with } K_p\}, \\ f_p(\Gamma) &= g_p(\Gamma) \cup K_p g_p(\Gamma) \cup \{\varphi \in \mathrm{Fml} \mid \Gamma \vdash \bot\}. \end{aligned}$$

# Finite model property

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

## Proof strategy

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

### It does not work:

only looking at the formulae in a subformula-closed set $\Omega$ and using one of the previous $f_p$'s.
Reason: $f_p \colon W \to W$ does not hold.

## Instead

$W$ to be the set of pairs $(\Omega, \Gamma)$ where $\Gamma$ is $\Omega$-saturated.
($\Omega$ is closed for taking a subformula and replacing $K_pK_p$ with $K_p$).

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

- $f_p(\Gamma) = g_p(\Gamma) \cup K_p g_p(\Gamma) \cup \{\varphi \in \mathsf{Fml} \mid \Gamma \vdash \bot\}$.
- $f'_p(\Omega) = g_p(\Omega) \cup K_p g_p(\Omega)$.

meanwhile

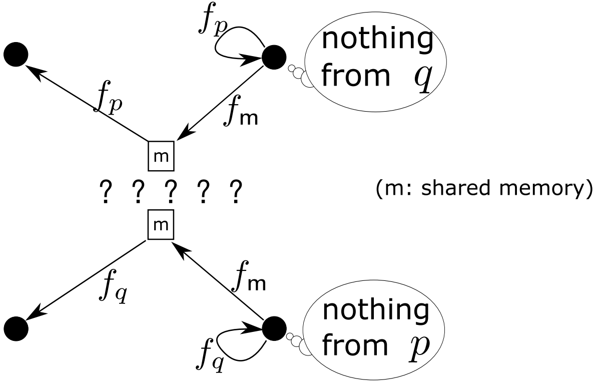
# Modelling Sequential Consistency

# Need for shared memory consistency

Assumption: full-information

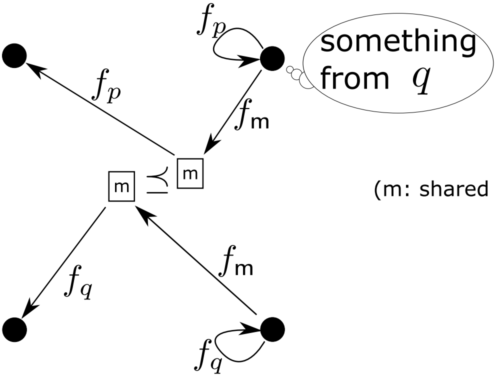
- A message contains all knowledge of its sender.
- Nothing is ever forgotten.

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



# Essence of Sequential Consistency

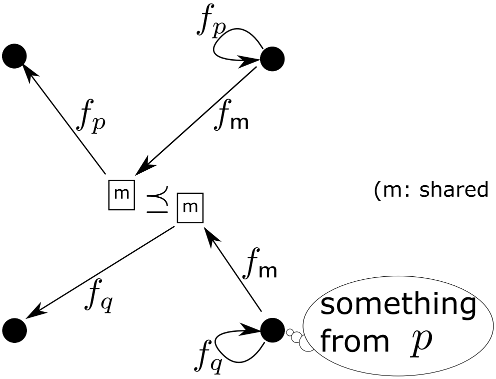
For two memory states, either $\preceq$ or $\succeq$ holds.



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

$$\text{Intuitionistic logic} \subsetneq \textbf{Lin} \subsetneq \text{Classical logic}$$

Well-known property:

$$\textbf{Lin} \vdash \theta \iff M \models \theta \text{ for all linear model } M$$

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

# A logic **SC** for Sequential Consistency

**SC** = Int. Epistemic logic + $(K_{\mathrm{m}}\varphi \supset K_{\mathrm{m}}\psi) \vee (K_{\mathrm{m}}\psi \supset K_{\mathrm{m}}\varphi)$:

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

A result:

$$\mathbf{SC} \vdash \theta \iff M \models \theta \text{ for all sequential model } M$$

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

# An example theorem under sequential consistency

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

## 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 $q$.
- then, $p$'s knowledge $I$ has been transmitted to $q$, or $q$'s knowledge $J$ has been transmitted to $p$.

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

Trying to avoid

- logically possible but computationally impossible schedules like

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

- finite but non-sequential schedules.

Revising a proof until the speaker finds a gap.
(Similar construction using $f_p(\Gamma) = \{\varphi \mid \Gamma \nvdash (K_p\varphi) \supset \bot\}$).

If succeeds, a similar method would give an axiomatization for Halpern's $\mathcal{C}_n^{amp}$ limited to the class of formulae whose every subformula

- begins with $\Box$, or
- is immediately after $\Box$.

Def. **AMP** = Int. Epis. logic + $(K_p\varphi \supset K_p\psi) \vee (K_p\psi \supset K_p\varphi)$.
Speculation. **AMP** $\vdash \varphi \iff \mathcal{C}_n^{amp} \models (\varphi)^\circ$
where $(\varphi)^\circ$ is obtained by putting $\Box$ before every subformula of $\varphi$.

# 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
  - Type-safe Paxos [Lamport, 1997] implimentation
- Quantify agents $\exists x K_x \varphi$ for program extraction with mobility.
  - Knowledge of $\pi$-calculus terms
- Knowledge of forking and merging agents (forking creates common knowledge).

A part (soundness, strong completeness and modelling sequential consistency) of this work has been accepted to LPAR-16 that will be held in Dakar, Senegal.

Ditmarsch, H., Hoek, W., and Kooi, B. (2007).
Dynamic Epistemic Logic.

Dummett, M. (2000).
Elements of intuitionism.
Oxford University Press, USA.

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.