Intuitionistic Distributed Knowledge

Completeness by a Canonical Model Construction

Michel Marti
Joint work with Gerhard Jäger

Institute of Computer Science
University of Bern

AiML 2016

Overview

1. Syntax of Intuitionistic Distributed Knowledge
2. Semantics: Intuitionistic Kripke structures
3. The Deductive System IDK
4. The Canonical Model

Intuitionistic Epistemic Logics

Intuitionistic Epistemic Logics

Intuitionistic Epistemic Logics: Reasoning about the knowledge of intuitionistic agents

Intuitionistic Epistemic Logics

Intuitionistic Epistemic Logics: Reasoning about the knowledge of intuitionistic agents

Intuition: $K_i\alpha \approx$ the (intuitionistic) agent i knows / the agent i intuitionistically knows that α

Intuitionistic Epistemic Logics

Intuitionistic Epistemic Logics: Reasoning about the knowledge of intuitionistic agents

Intuition: $K_i\alpha \approx$ the (intuitionistic) agent i knows / the agent i intuitionistically knows that α

$\approx$ the agent i has constructive evidence for α

What is distributed knowledge?

Distributed knowledge: Knowledge that "is distributed across a community of agents".

What is distributed knowledge?

Distributed knowledge: Knowledge that "is distributed across a community of agents".

α is distributed knowledge in a group of agents $a_1, \ldots, a_n$ means (roughly) that the agents would know α if they could combine what they individually know.

What is distributed knowledge?

Distributed knowledge: Knowledge that "is distributed across a community of agents".

α is distributed knowledge in a group of agents $a_1, \ldots, a_n$ means (roughly) that the agents would know α if they could combine what they individually know.

Equivalently, it is the knowledge of an agent $a^\star$ who knows everything that the agents $a_1, \ldots, a_n$ know.

The Language $\mathcal{L}_{\mathcal{DK}}$

We want to talk about n agents $a_1, \ldots, a_n$ and formally represent what they know, what they don't know and what is distributed knowledge in this group of agents.

Definition (Language $\mathcal{L}_{\mathcal{DK}}$)

The language $\mathcal{L}_{\mathcal{DK}}$ of intuitionistic distributed knowledge consists of

- Countably many propositional letters, denoted by $p, q, r, \ldots$ (possibly with subscripts). The set of propositional letters is called *PROP*.
- the constant symbol $\bot$
- binary connectives $\wedge, \vee, \rightarrow$
- unary modal operators K_i for each $i = 1, \ldots, n$
- a unary modal operator D

Formulas

Definition

The formulas of $\mathcal{L}_{\mathcal{DK}}$ are defined by the grammar

$$\alpha ::= \bot \mid p \mid (\alpha \vee \alpha) \mid (\alpha \wedge \alpha) \mid (\alpha \to \alpha) \mid K_i(\alpha) \mid D(\alpha)$$

We use the standard abbreviation

$$\neg\alpha := \alpha \to \bot$$

Intended Reading

The intended epistemic readings are:

Intended Reading

The intended epistemic readings are:

$$K_i(\alpha) \approx \text{ agent } a_i \text{ knows / believes } \alpha$$

Intended Reading

The intended epistemic readings are:

$$K_i(\alpha) \approx \text{ agent } a_i \text{ knows / believes } \alpha$$

$D(\alpha) \approx \alpha$ is distributed knowledge /belief among the agents $a_1, \ldots, a_n$.

The intuition that distributed knowledge arises from the combined knowledge of the agents is captured by the axioms

The intuition that distributed knowledge arises from the combined knowledge of the agents is captured by the axioms

$$K_i(\alpha) \to D(\alpha)$$

The intuition that distributed knowledge arises from the combined knowledge of the agents is captured by the axioms

$$K_i(\alpha) \to D(\alpha)$$

$$D(\alpha \to \beta) \to (D(\alpha) \to D(\beta))$$

Semantics of Intuitionistic Distributed Knowledge

Definition

An epistemic Kripke structure (EK-structure) is an $(n+3)$ tuple

$$\mathfrak{M} = (W, \preceq, R_1, \dots, R_n, V)$$

Semantics of Intuitionistic Distributed Knowledge

Definition

An epistemic Kripke structure (EK-structure) is an $(n+3)$ tuple

$$\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$$

such that

- W is a nonempty set and $\preceq$ is a preorder on W.

Semantics of Intuitionistic Distributed Knowledge

Definition

An epistemic Kripke structure (EK-structure) is an $(n+3)$ tuple

$$\mathfrak{M} = (W, \preceq, R_1, \dots, R_n, V)$$

such that

- W is a nonempty set and $\preceq$ is a preorder on W.
- for any $1 \leq i \leq n$: $R_i \subseteq W \times W$ s.t. for any $v, w \in W$: $v \preceq w \Rightarrow R_i[w] \subseteq R_i[v]$

Semantics of Intuitionistic Distributed Knowledge

Definition

An epistemic Kripke structure (EK-structure) is an $(n+3)$ tuple

$$\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$$

such that

- W is a nonempty set and $\preceq$ is a preorder on W.
- for any $1 \leq i \leq n$: $R_i \subseteq W \times W$ s.t. for any $v, w \in W$: $v \preceq w \Rightarrow R_i[w] \subseteq R_i[v]$
- $V : W \to \mathcal{P}(PROP)$ s.t. for any $v, w \in W$: $v \preceq w \Rightarrow V(v) \subseteq V(w)$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

(3) $\|\alpha \wedge \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cap \|\beta\|_{\mathfrak{M}}$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

(3) $\|\alpha \wedge \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cap \|\beta\|_{\mathfrak{M}}$

(4) $\|\alpha \to \beta\|_{\mathfrak{M}} := \{v \in W : \{w \in W : v \preceq w\} \cap \|\alpha\|_{\mathfrak{M}} \subseteq \|\beta\|_{\mathfrak{M}}\}$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

(3) $\|\alpha \wedge \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cap \|\beta\|_{\mathfrak{M}}$

(4) $\|\alpha \to \beta\|_{\mathfrak{M}} := \{v \in W : \{w \in W : v \preceq w\} \cap \|\alpha\|_{\mathfrak{M}} \subseteq \|\beta\|_{\mathfrak{M}}\}$

(5) $\|K_i(\alpha)\|_{\mathfrak{M}} := \{v \in W : R_i[v] \subseteq \|\alpha\|_{\mathfrak{M}}\}$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \dots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

(3) $\|\alpha \wedge \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cap \|\beta\|_{\mathfrak{M}}$

(4) $\|\alpha \to \beta\|_{\mathfrak{M}} := \{v \in W : \{w \in W : v \preceq w\} \cap \|\alpha\|_{\mathfrak{M}} \subseteq \|\beta\|_{\mathfrak{M}}\}$

(5) $\|K_i(\alpha)\|_{\mathfrak{M}} := \{v \in W : R_i[v] \subseteq \|\alpha\|_{\mathfrak{M}}\}$

(6) $\|D(\alpha)\|_{\mathfrak{M}} := \{v \in W : \bigcap_{i=1}^{n} R_i[v] \subseteq \|\alpha\|_{\mathfrak{M}}\}$

Semantics of Intuitionistic Distributed Knowledge (cont.)

Definition

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ be an EK-structure. Then the set $\|\alpha\|_{\mathfrak{M}} \subseteq W$ is inductively defined for every formula α as follows:

(1) $\|\bot\|_{\mathfrak{M}} := \varnothing$ and $\|p\|_{\mathfrak{M}} := V(p)$ for any atomic proposition p

(2) $\|\alpha \vee \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cup \|\beta\|_{\mathfrak{M}}$

(3) $\|\alpha \wedge \beta\|_{\mathfrak{M}} := \|\alpha\|_{\mathfrak{M}} \cap \|\beta\|_{\mathfrak{M}}$

(4) $\|\alpha \rightarrow \beta\|_{\mathfrak{M}} := \{v \in W : \{w \in W : v \preceq w\} \cap \|\alpha\|_{\mathfrak{M}} \subseteq \|\beta\|_{\mathfrak{M}}\}$

(5) $\|K_i(\alpha)\|_{\mathfrak{M}} := \{v \in W : R_i[v] \subseteq \|\alpha\|_{\mathfrak{M}}\}$

(6) $\|D(\alpha)\|_{\mathfrak{M}} := \{v \in W : \bigcap_{i=1}^{n} R_i[v] \subseteq \|\alpha\|_{\mathfrak{M}}\}$

IDK

The system IDK is a Hilbert system with the following axioms and rules:

IDK

The system IDK is a Hilbert system with the following axioms and rules:

- Axioms for intuitionistic propositional logic

IDK

The system IDK is a Hilbert system with the following axioms and rules:

- Axioms for intuitionistic propositional logic
- K-axioms

$$K_i(\alpha \to \beta) \to (K_i(\alpha) \to K_i(\beta))$$

IDK

The system IDK is a Hilbert system with the following axioms and rules:

- Axioms for intuitionistic propositional logic
- K-axioms

$$K_i(\alpha \to \beta) \to (K_i(\alpha) \to K_i(\beta))$$

- A corresponding axiom for D

$$D(\alpha \to \beta) \to (D(\alpha) \to D(\beta))$$

IDK

The system IDK is a Hilbert system with the following axioms and rules:

- Axioms for intuitionistic propositional logic
- K-axioms

$$K_i(\alpha \to \beta) \to (K_i(\alpha) \to K_i(\beta))$$

- A corresponding axiom for D

$$D(\alpha \to \beta) \to (D(\alpha) \to D(\beta))$$

- individual knowledge implies distributed knowledge

$$K_i(\alpha) \to D(\alpha)$$

IDK, (cont.)

We have two rules of inference:

IDK, (cont.)

We have two rules of inference:

- Modus Ponens

$$\frac{\alpha \to \beta \qquad \alpha}{\beta}\ \text{(MP)}$$

IDK, (cont.)

We have two rules of inference:

- Modus Ponens

$$\frac{\alpha \to \beta \qquad \alpha}{\beta}\ (\mathrm{MP})$$

- Necessitation rules

$$\frac{\alpha}{K_i(\alpha)}\ (\mathrm{nec_i})$$

IDK, (cont.)

Remark

We have as a derived rule

$$\frac{\alpha}{D(\alpha)}\ (\mathrm{nec_D})$$

Truth Axiom

If we want our system to reflect that only truths can be known, we can add the axioms

$$(T) \quad K_i(\alpha) \to \alpha$$

The Deductive System **IDK**, (cont.)

Definition

- We write
$$\mathbf{IDK} \vdash \alpha$$
iff there is a derivation of α in **IDK**.
- Given a finite set Φ of $\mathcal{L}_{\mathcal{DK}}$ formulas, we write
$$c(\Phi) \quad \text{for the conjuction of the elements of } \Phi.$$
- If M is a any set of $\mathcal{L}_{\mathcal{DK}}$ formulas, we write
$$M \vdash_{\mathbf{IDK}} \alpha$$
iff there exists a finite subset $\Phi \subseteq M$ such that $\mathbf{IDK} \vdash c(\Phi) \to \alpha$.

Soundness of **IDK**

Lemma (Soundness of IDK)

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, V)$ *be an EK-structure. Then we have that*

$$\Phi \vdash_{\mathbf{IDK}} \alpha \Rightarrow W \subseteq \|c(\Phi) \to \alpha\|_{\mathfrak{M}}$$

Pseudo Models

Definition (Pseudo-model)

A **pseudo-model** for intuitionistic distributed knowledge is a structure

$$(W, \preceq, R_1, \ldots, R_n, R_{n+1} = R_D, V)$$

such that

$$(W, \preceq, R_1, \ldots, R_n, V)$$

is a model for intuitionistic modal logic, and

$$w \vDash D\varphi \quad :\Longleftrightarrow \quad v \vDash \varphi \text{ for all } v \in R_D[w]$$

Strict Pseudo Model

Definition (Strict Pseudo Model)

Given a pseudo-model

$$\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, , R_{n+1} = R_D, V)$$

We define the **strict pseudo model** $\mathfrak{M}'$ of $\mathfrak{M}$ by

$$W' := W \times \{1, \ldots, n+1\}$$

Strict Pseudo Model

Definition (Strict Pseudo Model)

Given a pseudo-model

$$\mathfrak{M} = (W, \preceq, R_1, \dots, R_n, , R_{n+1} = R_D, V)$$

We define the **strict pseudo model** $\mathfrak{M}'$ of $\mathfrak{M}$ by

$$W' := W \times \{1, \dots, n+1\}$$

$$(w, i) \preceq' (v, j) :\Leftrightarrow w \preceq v \quad \text{and} \quad V'((w, i)) := V(w)$$

Strict Pseudo Model

Definition (Strict Pseudo Model)

Given a pseudo-model

$$\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, , R_{n+1} = R_D, V)$$

We define the **strict pseudo model** $\mathfrak{M}'$ of $\mathfrak{M}$ by

$$W' := W \times \{1, \ldots, n+1\}$$

$$(w, i) \preceq' (v, j) :\Leftrightarrow w \preceq v \quad \text{and} \quad V'((w, i)) := V(w)$$

For $i = 1, \ldots, n+1$ we define

$$(w, j) R'_i (v, k) \quad :\Leftrightarrow \quad w R_i v \text{ and } i = k$$

Strict Pseudo Model

Remark

Let $\mathfrak{M}$ be a pseudo-model and $\mathfrak{M}$' its strict pseudo-model. Then we have the following facts, where the first holds by definition and the latter following immediately from the former:

1. $wR_iv \Leftrightarrow (w, j)R'_i(v, i)$ for all $j = 1, \ldots, n$
2. $wR_iw \Rightarrow (w, i)R'_i(w, i)$
3. If R_i is reflexive, so is R'_i.
4. If $\mathfrak{M}$ is reflexive, so is $\mathfrak{M}$'.

Strict Pseudo Model

Lemma

The strict pseudo model satisfies the following properties:

(a) *If $\mathfrak{M}$ is finite, then $\mathfrak{M}'$ is finite too.*

(b) *for each state $w' = (w, k) \in W'$ and all $i, j \in \{1, \ldots, n, n+1 = D\}$:*

$$R'_i[(w,k)] \cap R'_j[(w,k)] = \varnothing \text{ if } i \neq j$$

Strict Pseudo Model

Lemma

If $\mathfrak{M}$ is a pseudo model and $\mathfrak{M}'$ its strict pseudo model, then

$$(\mathfrak{M}, w) \models \varphi \Leftrightarrow (\mathfrak{M}', (w, i)) \models \varphi$$

for each formula φ, each $w \in W$ and $i = 1, \ldots, n, n+1$.

Associated Model

Definition (Associated Model)

Given a strict pseudo model $\mathfrak{M} = (W, \preceq, R_1, \dots, R_n, R_D, V)$, we define its **associated model** $\mathfrak{M}^\star = (W^\star, \preceq^\star, R_1^\star, \dots, R_n^\star, V^\star)$ by

$$W^\star := W$$

$$\preceq^\star := \preceq$$

$$V^\star := V$$

$$R_i^\star := R_i \cup R_D \quad \text{for } i = 1, \dots, n$$

Associated Model

Lemma

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, R_D, V)$ *be a strict pseudo model, and* $\mathfrak{M}^\star = (W^\star, \preceq^\star, R_1^\star, \ldots, R_n^\star, V^\star)$ *its associated model and* $w \in W$ *a state. Then we have:*

$$\bigcap_{i=1}^{n} R_i^\star[w] = R_D[w]$$

Associated Model

Proof.

$$\bigcap_{i=1}^{n} R_i^\star[w] = \bigcap_{i=1}^{n}(R_i[w] \cup R_D[w]) = \bigcap_{i=1}^{n} R_i[w] \cup R_D[w] = R_D[w]$$

$\square$

Associated Model

Lemma

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, R_D, V)$ *be a strict pseudo model, and* $\mathfrak{M}^\star = (W^\star, \preceq^\star, R_1^\star, \ldots, R_n^\star, V^\star)$ *its associated model and* φ *a formula. Then*

$$(\mathfrak{M}, w) \vDash \varphi \quad \Longleftrightarrow \quad (\mathfrak{M}^\star, w) \vDash \varphi \qquad \text{for all } w \in W$$

Associated Model

Proof.

Lets consider the case $\varphi = D\psi$:

$(\mathfrak{M}, w) \models D\psi \Leftrightarrow (\mathfrak{M}, v) \models \psi$ for all $v \in R_D[w]$

Associated Model

Proof.

Lets consider the case $\varphi = D\psi$:

$(\mathfrak{M}, w) \models D\psi \Leftrightarrow (\mathfrak{M}, v) \models \psi$ for all $v \in R_D[w]$
by the lemma above, we have that
$\bigcap_{i=1}^{n} R_i^\star[w] = R_D[w]$
so

Associated Model

Proof.

Lets consider the case $\varphi = D\psi$:

$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in R_D[w]$
by the lemma above, we have that
$\bigcap_{i=1}^{n} R_i^\star[w] = R_D[w]$
so
$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in \bigcap_{i=1}^{n} R_i^\star[w]$

Associated Model

Proof.

Lets consider the case $\varphi = D\psi$:

$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in R_D[w]$
by the lemma above, we have that
$\bigcap_{i=1}^{n} R_i^\star[w] = R_D[w]$
so
$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in \bigcap_{i=1}^{n} R_i^\star[w]$
By the I.H. we have that $(\mathfrak{M}, v) \vDash \psi \Leftrightarrow (\mathfrak{M}^\star, v) \vDash \psi$

Associated Model

Proof.

Lets consider the case $\varphi = D\psi$:

$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in R_D[w]$
by the lemma above, we have that
$\bigcap_{i=1}^{n} R_i^\star[w] = R_D[w]$
so
$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}, v) \vDash \psi$ for all $v \in \bigcap_{i=1}^{n} R_i^\star[w]$
By the I.H. we have that $(\mathfrak{M}, v) \vDash \psi \Leftrightarrow (\mathfrak{M}^\star, v) \vDash \psi$
and therefore
$(\mathfrak{M}, w) \vDash D\psi \Leftrightarrow (\mathfrak{M}^\star, w) \vDash D\psi$.

$\square$

Associated Model

Remark

Let $\mathfrak{M}$ be a strict pseudo-model, and $\mathfrak{M}^\star$ its associated model.

1. $R_i \subseteq R_i^\star$ for $i = 1, \ldots, n$
2. $wR_iw \Rightarrow wR_i^\star w$ for $i = 1, \ldots, n$
3. R_i is reflexive $\Rightarrow R_i^\star$ is reflexive for $i = 1, \ldots, n$

Reflexivity

Remark

Let $\mathfrak{M} = (W, \preceq, R_1, \ldots, R_n, R_{n+1} = R_D, V)$ be a pseudo-model, $\mathfrak{M}'$ its strict pseudo-model and $\mathfrak{M}^\star$ the associated model of $\mathfrak{M}'$. From the previous two remarks it follows immediately that

$$R_i \text{ is reflexive } \Rightarrow R_i' \text{ is reflexive } \Rightarrow R_i^\star \text{ is reflexive}$$

The Canonical Model

We fix an arbitrary $\mathcal{L}_{KD}$ formula α. Everything in the following section is relative to this particular α.

Definition

The fragment $M(\alpha)$ is defined by

$$M(\alpha) := \mathrm{Subf}(\alpha) \cup \{\perp\}$$

The Canonical Model

We fix an arbitrary $\mathcal{L}_{KD}$ formula α. Everything in the following section is relative to this particular α.

Definition

The fragment $M(\alpha)$ is defined by

$$M(\alpha) := \mathrm{Subf}(\alpha) \cup \{\bot\}$$

Lemma

$M(\alpha)$ is a finite set.

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

(3) $\beta \vee \gamma \in \Phi \Rightarrow \beta \in \Phi$ or $\gamma \in \Phi$ (disjunction property)

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

(3) $\beta \vee \gamma \in \Phi \Rightarrow \beta \in \Phi$ or $\gamma \in \Phi$ (disjunction property)

(4) $\Phi \nvdash \perp$ (consistent)

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

(3) $\beta \vee \gamma \in \Phi \Rightarrow \beta \in \Phi$ or $\gamma \in \Phi$ (disjunction property)

(4) $\Phi \nvdash \perp$ (consistent)

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

(3) $\beta \vee \gamma \in \Phi \Rightarrow \beta \in \Phi$ or $\gamma \in \Phi$ (disjunction property)

(4) $\Phi \nvdash \bot$ (consistent)

In the following, the Greek letters $\Gamma, \Delta, \Lambda, \Pi, \Sigma$ (possibly with subscripts) range over α-prime sets of formulas. Furthermore,

The Canonical Model (cont.)

Definition

A set Φ of $\mathcal{L}_{KD}$ formulas is called α-**prime** iff the following conditions are satisfied for all $\mathcal{L}_{KD}$ formulas:

(1) $\Phi \subseteq M(\alpha)$

(2) $\Phi \vdash \beta$ and $\beta \in M(\alpha) \Rightarrow \beta \in \Phi$ (deductively closed)

(3) $\beta \vee \gamma \in \Phi \Rightarrow \beta \in \Phi$ or $\gamma \in \Phi$ (disjunction property)

(4) $\Phi \nvdash \bot$ (consistent)

In the following, the Greek letters $\Gamma, \Delta, \Lambda, \Pi, \Sigma$ (possibly with subscripts) range over α-prime sets of formulas. Furthermore,

$$\Gamma^c := M(\alpha) \setminus \Gamma$$

The Canonical Model (cont.)

Lemma (Prime Lemma)

Suppose that $\Phi \subseteq M(\alpha)$ and $\Phi \nvdash \beta$ for some $\mathcal{L}_{KD}$ formula β; it is not required that $\beta \in M(\alpha)$. Then there exists an α-prime set Γ such that $\Phi \subseteq \Gamma$ and $\Gamma \nvdash \beta$.

The Canonical Model (cont.)

Proof.

Let $\gamma_0, \dots, \gamma_k$ be an enumeration of $M(\alpha)$.
Now we define $\Gamma_0 := \Phi$

$$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{\gamma_n\} & \text{, if } \Gamma_n \cup \{\gamma_n\} \nvdash \beta \\ \Gamma_n & \text{, otherwise} \end{cases}$$

Then we have

(i) $\Phi \subseteq \Gamma_i$ and $\Gamma_i \nvdash \beta$ for $i = 0, \dots, k+1$

(ii) $\Gamma := \Gamma_{k+1}$ is α-prime.

$\square$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

$$p \in V_\alpha(\Gamma) \quad :\Longleftrightarrow \quad p \in \Gamma$$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

$$p \in V_\alpha(\Gamma) \quad :\Longleftrightarrow \quad p \in \Gamma$$

$$\Gamma R_i \Delta \quad :\Longleftrightarrow \quad K_i^{-1}\Gamma \subseteq \Delta$$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

$$p \in V_\alpha(\Gamma) \quad :\Longleftrightarrow \quad p \in \Gamma$$

$$\Gamma R_i \Delta \quad :\Longleftrightarrow \quad K_i^{-1}\Gamma \subseteq \Delta$$

$$\Gamma R_D \Delta \quad :\Longleftrightarrow \quad D^{-1}\Gamma \subseteq \Delta$$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

$$p \in V_\alpha(\Gamma) \quad :\Longleftrightarrow \quad p \in \Gamma$$

$$\Gamma R_i \Delta \quad :\Longleftrightarrow \quad K_i^{-1}\Gamma \subseteq \Delta$$

$$\Gamma R_D \Delta \quad :\Longleftrightarrow \quad D^{-1}\Gamma \subseteq \Delta$$

$$\mathfrak{M}^{\text{pseudo}}_{\text{can}} \quad := \quad (W_\alpha, \subseteq, R_1, \ldots, R_n, R_D, V_\alpha)$$

The Canonical Model (cont.)

Definition (Canonical pseudo model)

$$W_\alpha \quad := \quad \{\Gamma \subseteq M(\alpha) : \Gamma \text{ is } \alpha\text{-prime}\}$$

$$p \in V_\alpha(\Gamma) \quad :\Longleftrightarrow \quad p \in \Gamma$$

$$\Gamma R_i \Delta \quad :\Longleftrightarrow \quad K_i^{-1}\Gamma \subseteq \Delta$$

$$\Gamma R_D \Delta \quad :\Longleftrightarrow \quad D^{-1}\Gamma \subseteq \Delta$$

$$\mathfrak{M}_{\mathrm{can}}^{\mathrm{pseudo}} \quad := \quad (W_\alpha, \subseteq, R_1, \ldots, R_n, R_D, V_\alpha)$$

Claim: $\mathfrak{M}_{\mathrm{can}}$ is a pseudo model.

A Truth Lemma

Lemma (Truth Lemma for the canonical pseudo model)

For all formulas $\beta \in M(\alpha)$ and α-prime Γ:

$$\beta \in \Gamma \quad \iff \quad (\mathfrak{M}_{\text{can}}^{\text{pseudo}}, \Gamma) \models \beta$$

Truth Lemma, (ctd.)

Proof.

$\beta = D\gamma$: Assume that $D\gamma \in \Gamma$. This means that $\gamma \in D^{-1}\Gamma$, so by the definition of the accessibility relation R_D in the canonical pseudo model:

Truth Lemma, (ctd.)

Proof.

$\beta = D\gamma$: Assume that $D\gamma \in \Gamma$. This means that $\gamma \in D^{-1}\Gamma$, so by the definition of the accessibility relation R_D in the canonical pseudo model:

$$\gamma \in \Delta \text{ for each } \Delta \in R_D[\Gamma]$$

Truth Lemma, (ctd.)

Proof.

$\beta = D\gamma$: Assume that $D\gamma \in \Gamma$. This means that $\gamma \in D^{-1}\Gamma$, so by the definition of the accessibility relation R_D in the canonical pseudo model:

$$\gamma \in \Delta \text{ for each } \Delta \in R_D[\Gamma]$$

It follows by the I.H. that

$$\Delta \models \gamma \text{ for each } \Delta \in R_D[\Gamma]$$

Truth Lemma, (ctd.)

Proof.

$\beta = D\gamma$: Assume that $D\gamma \in \Gamma$. This means that $\gamma \in D^{-1}\Gamma$, so by the definition of the accessibility relation R_D in the canonical pseudo model:

$$\gamma \in \Delta \text{ for each } \Delta \in R_D[\Gamma]$$

It follows by the I.H. that

$$\Delta \models \gamma \text{ for each } \Delta \in R_D[\Gamma]$$

so by the definition of the satisfaction relation in pseudo-models we have that

$$\Gamma \models D\gamma.$$

Truth Lemma, (ctd.)

Proof.

For the other direction, assume that $(\mathfrak{M}_{\mathrm{can}}^{\mathrm{pseudo}}, \Gamma) \vDash D\gamma$.
First, we show that

$$D^{-1}\Gamma \vdash \gamma$$

Truth Lemma, (ctd.)

Proof.

Assume for a contradiction that

$$D^{-1}\Gamma \nvdash \gamma$$

Truth Lemma, (ctd.)

Proof.

Assume for a contradiction that

$$D^{-1}\Gamma \nvdash \gamma$$

Then by the Prime Lemma, there exists an α-prime set Π such that

$$D^{-1}\Gamma \subseteq \Pi \text{ and } \Pi \nvdash \gamma.$$

Truth Lemma, (ctd.)

Proof.

Assume for a contradiction that

$$D^{-1}\Gamma \nvdash \gamma$$

Then by the Prime Lemma, there exists an α-prime set Π such that

$$D^{-1}\Gamma \subseteq \Pi \text{ and } \Pi \nvdash \gamma.$$

so in particular, $\gamma \notin \Pi$, so by the I.H.

Truth Lemma, (ctd.)

Proof.

Assume for a contradiction that

$$D^{-1}\Gamma \nvdash \gamma$$

Then by the Prime Lemma, there exists an α-prime set Π such that

$$D^{-1}\Gamma \subseteq \Pi \text{ and } \Pi \nvdash \gamma.$$

so in particular, $\gamma \notin \Pi$, so by the I.H.

$$(\mathfrak{M}_{can}^{\text{pseudo}}, \Pi) \nvDash \gamma$$

Truth Lemma, (ctd.)

Proof.

$$(\mathfrak{M}_{can}^{\text{pseudo}}, \Pi) \not\models \gamma$$

but $D^{-1}\Gamma \subseteq \Pi$, so by definition of the accessibility relation R_D in the canonical pseudo model:

Truth Lemma, (ctd.)

Proof.

$$(\mathfrak{M}_{can}^{\text{pseudo}}, \Pi) \not\models \gamma$$

but $D^{-1}\Gamma \subseteq \Pi$, so by definition of the accessibility relation R_D in the canonical pseudo model:

$$\Pi \in R_D[\Gamma]$$

Truth Lemma, (ctd.)

Proof.

$$(\mathfrak{M}_{can}^{\text{pseudo}}, \Pi) \not\models \gamma$$

but $D^{-1}\Gamma \subseteq \Pi$, so by definition of the accessibility relation R_D in the canonical pseudo model:

$$\Pi \in R_D[\Gamma]$$

which contradicts our assumption that $(\mathfrak{M}_{\text{can}}, \Gamma) \models D\gamma$.

Truth Lemma, (ctd.)

Proof.

So we have shown that

$$D^{-1}\Gamma \vdash \gamma.$$

This means that there are formulas $\gamma_1, \dots, \gamma_n \in D^{-1}\Gamma$ such that

Truth Lemma, (ctd.)

Proof.

So we have shown that

$$D^{-1}\Gamma \vdash \gamma.$$

This means that there are formulas $\gamma_1, \ldots, \gamma_n \in D^{-1}\Gamma$ such that

$$\gamma_1, \ldots, \gamma_n \vdash \gamma$$

Truth Lemma, (ctd.)

Proof.

So we have shown that

$$D^{-1}\Gamma \vdash \gamma.$$

This means that there are formulas $\gamma_1, \ldots, \gamma_n \in D^{-1}\Gamma$ such that

$$\gamma_1, \ldots, \gamma_n \vdash \gamma$$

By propositional reasoning we get that

$$\vdash (\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Truth Lemma, (ctd.)

Proof.

So we have shown that

$$D^{-1}\Gamma \vdash \gamma.$$

This means that there are formulas $\gamma_1, \dots, \gamma_n \in D^{-1}\Gamma$ such that

$$\gamma_1, \dots, \gamma_n \vdash \gamma$$

By propositional reasoning we get that

$$\vdash (\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

so by necessitation

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Truth Lemma, (ctd.)

Proof.

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Truth Lemma, (ctd.)

Proof.

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Now we apply the axiom $K_i\varphi \to D\varphi$ for distributed knowledge and we continue with

Truth Lemma, (ctd.)

Proof.

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Now we apply the axiom $K_i\varphi \to D\varphi$ for distributed knowledge and we continue with

$$\vdash D(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Truth Lemma, (ctd.)

Proof.

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Now we apply the axiom $K_i\varphi \to D\varphi$ for distributed knowledge and we continue with

$$\vdash D(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Using the axiom $D(\alpha \to \beta) \to (D\alpha \to D\beta)$ and propositional reasoning, we get

Truth Lemma, (ctd.)

Proof.

$$\vdash K_i(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Now we apply the axiom $K_i\varphi \to D\varphi$ for distributed knowledge and we continue with

$$\vdash D(\gamma_1 \wedge \cdots \wedge \gamma_n \to \gamma)$$

Using the axiom $D(\alpha \to \beta) \to (D\alpha \to D\beta)$ and propositional reasoning, we get

$$\vdash D\gamma_1 \wedge \cdots \wedge D\gamma_n \to D\gamma$$

Truth Lemma, (ctd.)

Proof.

$$\vdash D\gamma_1 \wedge \cdots \wedge D\gamma_n \to D\gamma$$

Truth Lemma, (ctd.)

Proof.

$$\vdash D\gamma_1 \land \cdots \land D\gamma_n \to D\gamma$$

so

Truth Lemma, (ctd.)

Proof.

$$\vdash D\gamma_1 \wedge \cdots \wedge D\gamma_n \to D\gamma$$

so

$$D\gamma_1, \ldots, D\gamma_n \vdash D\gamma$$

Truth Lemma, (ctd.)

Proof.

$$\vdash D\gamma_1 \wedge \cdots \wedge D\gamma_n \to D\gamma$$

so

$$D\gamma_1, \ldots, D\gamma_n \vdash D\gamma$$

since $D\gamma_i \in \Gamma$ for $i = 1, \ldots, n$, this means that

$$\Gamma \vdash D\gamma$$

Truth Lemma, (ctd.)

Proof.

$$\vdash D\gamma_1 \wedge \cdots \wedge D\gamma_n \to D\gamma$$

so

$$D\gamma_1, \ldots, D\gamma_n \vdash D\gamma$$

since $D\gamma_i \in \Gamma$ for $i = 1, \ldots, n$, this means that

$$\Gamma \vdash D\gamma$$

Since $D\gamma$ is in $M(\alpha)$ and Γ is deductively closed with respect to $M(\alpha)$, it follows that

$$D\gamma \in \Gamma.$$

Theorem (Completeness for Intuitionistic Distributed Knowledge)

For each formula α we have that

$$\models \alpha \quad \Longrightarrow \quad \vdash \alpha$$

Proof.

Assume that $\nvdash \alpha$. By the Prime Lemma, there is an α-prime set Π such that

$$\Pi \nvdash \alpha$$

Proof.

Assume that $\nvdash \alpha$. By the Prime Lemma, there is an α-prime set Π such that

$$\Pi \nvdash \alpha$$

By the Truth Lemma, it follows that

$$(\mathfrak{M}_{\text{can}}^{\text{pseudo}}, \Pi) \nvDash \alpha$$

Proof.

Assume that $\nvdash \alpha$. By the Prime Lemma, there is an α-prime set Π such that

$$\Pi \nvdash \alpha$$

By the Truth Lemma, it follows that

$$(\mathfrak{M}_{\text{can}}^{\text{pseudo}}, \Pi) \nvDash \alpha$$

Now let $\mathfrak{M}_{\text{strict}}$ be the strict pseudo model of $\mathfrak{M}_{\text{can}}^{\text{pseudo}}$, and let $\mathfrak{M}_{\text{can}}$ be the associated model of $\mathfrak{M}_{\text{strict}}$. By the lemmas above we have that

Proof.

Assume that $\nvdash \alpha$. By the Prime Lemma, there is an α-prime set Π such that

$$\Pi \nvdash \alpha$$

By the Truth Lemma, it follows that

$$(\mathfrak{M}_{\mathrm{can}}^{\mathrm{pseudo}}, \Pi) \nvDash \alpha$$

Now let $\mathfrak{M}_{\mathrm{strict}}$ be the strict pseudo model of $\mathfrak{M}_{\mathrm{can}}^{\mathrm{pseudo}}$, and let $\mathfrak{M}_{\mathrm{can}}$ be the associated model of $\mathfrak{M}_{\mathrm{strict}}$. By the lemmas above we have that

$$(\mathfrak{M}_{\mathrm{can}}^{\mathrm{pseudo}}, \Pi) \nvDash \alpha \Leftrightarrow (\mathfrak{M}_{\mathrm{strict}}, \Pi) \nvDash \alpha \Leftrightarrow (\mathfrak{M}_{\mathrm{can}}, \Pi) \nvDash \alpha.$$

$\square$

Corollary (Finite Model Property)

The logic of intuitionistic distributed knowledge has the finite model property (fmp), i.e.

$$\not\models \alpha \Rightarrow \text{ there exists a finite model } \mathfrak{M}_{\text{fin}} \text{ such that } \mathfrak{M}_{\text{fin}} \not\models \alpha$$

Open Questions

- What is / should be the meaning of an intuitionistic epistemic $\Diamond$?
- Stronger intuitionistic modal logics?
- Corresponding Justification Logics?
- Curry-Howard?

Thank you for your attention!