Basic Proof Theory of Intuitionistic Epistemic Logic in Coq

2nd Bachelor Seminar Talk

Christian Hagemeier

Advisors: Dominik Kirst, Prof. Holger Sturm
Supervisor: Prof. Gert Smolka

April 8, 2021

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Recap

- **I**ntuitionistic **E**pistemic **L**ogic (Artemov and Protopopescu, 2016)
- Intuitionistic propositional logic + modal K operator modelling intuitionistic knowledge (= provability)
  1. $A \to \mathbf{K}A$ (co-reflection)
  2. $\mathbf{K}\,(A \to B) \to \mathbf{K}\,A \to \mathbf{K}\,B$ (distribution)
  3. $\mathbf{K}\,A \to \neg\neg A$ (intuitionistic reflection)
- Two logics: IEL and IEL^{-} (intuitionistic belief)
- IEL Axioms are valid when K is interpreted as propositional truncation ($\| \cdot \| \colon \mathbb{T} \to \mathbb{P}$)
- This talk: Decidability, Cut-Elimination, (Constructive) Completeness

Recap II

- Quick reminder: Natural deduction $\vdash$, Kripke-style semantics $\Vdash$
- Completeness proof using canonical model construction with worlds built from consistent prime theories
- $\mathcal{T} \vdash A \implies \mathcal{T} \vDash A$ (Soundness)
- $\mathcal{T} \vDash A \implies \mathcal{T} \vdash A$ (Completeness)
  Using LEM trice: Lindenbaum lemma, truth lemma and top-level

Recap II

- Quick reminder: Natural deduction $\vdash$, Kripke-style semantics $\Vdash$
- Completeness proof using canonical model construction with worlds built from consistent prime theories
- $\mathcal{T} \vdash A \implies \mathcal{T} \vDash A$ (Soundness)
- $\mathcal{T} \vDash A \implies \mathcal{T} \vdash A$ (Completeness)
  Using LEM trice: Lindenbaum lemma, truth lemma and top-level

Today

- $(\Gamma \vdash A) + (\Gamma \nvdash A)$ (Decidability)
- $\mathcal{T} \Vdash' A \implies \neg\neg(\mathcal{T} \vdash A)$ (Quasi-completeness)
- $\mathcal{T} \vdash A \implies \mathcal{T} \Vdash' A$ (Soundness using LEM)

Decidability via proof-search

- Without constructive finite model property[1] need syntactic method for proof search
- Standard approach: Cut-free sequent calculus (with subformula property) yields decidability
- 2 step proof
    1. Cut-elimination (for IEL proven by Krupski and Yatmanov (2016), similar to textbook Troelstra and Schwichtenberg (2000) for propositional logic)
    2. Proof search based on fixed-point iteration (Dang, 2015; Smolka and Brown, 2012)

[1] IEL enjoys the finite model property Wolter and Zakharyaschev (1999) per Rogozin (2020)

Representing derivations

$$\frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C}$$

- Explicit permutation rule:
  sc A::B::Γ C -> sc (A $\wedge$ B)::Γ C
  sc Γ A -> $\Gamma \equiv_P \Gamma'$ -> sc Γ' A
- Structural encoding:
  sc Γ++A::Γ'++B::Γ'' C -> sc Γ++(A $\wedge$ B)::Γ'++Γ'' C
- Membership encoding:
  (A $\wedge$ B) $\in \Gamma$ -> sc A::B::Γ C -> sc Γ C
- Inlined permutations
  $\Gamma' \equiv_P (A \wedge B) :: \Gamma$ -> $\Gamma'' \equiv_P A :: B :: \Gamma$ -> sc Γ'' C -> sc $\Gamma' C$

Representing derivations

$$\frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C}$$

- Explicit permutation rule:
  `sc A::B::`Γ `C -> sc (A` $\wedge$ `B)::`Γ `C`
  `sc` Γ `A ->` $\Gamma \equiv_P \Gamma'$ `-> sc` Γ' `A`
  Used in: Hara, 2013
- Structural encoding:
  `sc` Γ`++A::`Γ'`++B::`Γ'' `C -> sc` Γ`++(A` $\wedge$ `B)::`Γ'`++`Γ'' `C`
  Used in: Penington, 2018; Doorn, 2015; Park, 2013
- Membership encoding:
  `(A` $\wedge$ `B)` $\in \Gamma$ `-> sc A::B::`Γ `C -> sc` Γ `C`
  Used in: Dang, 2015; Smolka and Brown, 2012
- Inlined permutations
  $\Gamma' \equiv_P (A \wedge B) :: \Gamma$ `->` $\Gamma'' \equiv_P A :: B :: \Gamma$ `-> sc` Γ'' `C -> sc` $\Gamma' C$
  Used in: Michaelis and Nipkow, 2017; Chaudhuri et al., 2017; Tews, 2013

Representing derivations

- Choosing the correct representation is a trade-off (e.g. more high level is less suited for constructing concrete derivations)
- Need both $\Rightarrow$ and $\overset{h}{\Rightarrow}$ (e.g. for contraction), height bounded encoding similar to Michaelis and Nipkow, 2017
- KI-Rule

$$\frac{\Gamma, \mathbf{K}\,\Delta, \Delta \Rightarrow A}{\Gamma, \mathbf{K}\,\Delta \Rightarrow \mathbf{K}\,A}$$

  cannot be expressed with structural encoding
- Final pick for cut-elimination: inlined permutations
- Permutations are manageable[2]

[2] `https://github.com/foreverbell/permutation-solver`

Cut-elimination proof (Krupski and Yatmanov, 2016)

Theorem (Cut is admissible)

$$\frac{\Gamma_1 \Rightarrow A \qquad A, \Gamma_2 \Rightarrow B}{\Gamma_1, \Gamma_2 \Rightarrow B}$$

Proof.

Strong Induction on pairs (s, r) of **cut-rank** r and **formula size** s. Inversion on left derivation, in some cases another inversion on right derivation. Most cases use depth preserving inversion, weakening. (Structure similar to Plato, 2001) □

Different from Troelstra and Schwichtenberg, 2000 Principal vs. non-principal derivations

Cut-elimination proof (Krupski and Yatmanov, 2016)

Theorem (Cut is admissible)

$$\frac{\Gamma_1 \overset{h_1}{\Rightarrow} A \qquad A, \Gamma_2 \overset{h_2}{\Rightarrow} B}{\Gamma_1, \Gamma_2 \Rightarrow B}$$

Proof.

Strong Induction on pairs (s, r) of **cut-rank** $r := (h_1 + h_2)$ and **formula size** s.
Inversion on left derivation, in some cases another inversion on right derivation. Most cases use depth preserving inversion, weakening. (Structure similar to Plato, 2001) □

Different from Troelstra and Schwichtenberg, 2000 Principal vs. non-principal derivations

Cut-elimination proof (Krupski and Yatmanov, 2016)

Theorem (Cut is admissible)

$$\dfrac{\Gamma_1 \overset{h_1}{\Rightarrow} A \qquad A, \Gamma_2 \overset{h_2}{\Rightarrow} B}{\Gamma_1, \Gamma_2 \Rightarrow B}$$

Proof.

Strong Induction on pairs (s, r) of **cut-rank** $r := (h_1 + h_2)$ and **formula size** s.
Inversion on left derivation, in some cases another inversion on right derivation. Most cases use depth preserving inversion, weakening. (Structure similar to Plato, 2001) □

Corollary (Equivalence of natural deduction and sequent calculus)

$\Gamma \Rightarrow A \iff \Gamma \vdash A$

Proof search (Dang, 2015)

- **Want:** $\forall \Gamma\, A.\, (\Gamma \Rightarrow A) + (\Gamma \not\Rightarrow A)$
- Consider subformulas of Γ, A ($=:$ subformula universe $\mathcal{U}$)
- **Idea:** Compute

$$\left\{(\Gamma_1, A') \middle| \Gamma_1 \Rightarrow A', \Gamma_1 \subseteq \mathcal{U}, A' \in \mathcal{U}\right\}$$

  by using a fixed point iteration
- Obtain decider as a membership test
- Step function deciding to add a sequent

$$s : \mathcal{L}(\mathbf{G}) \to \mathbf{G} \to \mathbb{B}$$

  if one of the rules is applicable

Preparing for proof search

- Implementation of the step function depends on the formalization of sequent-calculus, in particular

$$\frac{\Gamma, \mathbf{K}\,\Delta, \Delta \Rightarrow A}{\Gamma, \mathbf{K}\,\Delta \Rightarrow \mathbf{K}\,A}$$

  is complicated to check
- Can find better encoding for IEL, using modified KI-rule:

$$\frac{\Gamma, K^{-}(\Gamma) \Rightarrow s}{\Gamma \Rightarrow \mathbf{K}\,s}$$

  where $\mathbf{K}^{-}(\Gamma) := \{A | \mathbf{K}\,A \in \Gamma\}$
- With this formulation of KI-rule (present in Krupski et al., 2016), membership-based representation for IEL can be used for proof search
- The proof itself is a straightforward adaption of Dang (2015)

Completeness revisited

Define forcing relation $\Vdash$:

$$
\begin{aligned}
w \vDash \mathbf{K}\, s &:\Leftrightarrow \forall w'. w \leq_{\mathbf{K}} w' \to w' \Vdash s \\
w \Vdash s \vee t &:\Leftrightarrow w \Vdash s \vee w \Vdash t \\
w \Vdash p_i &:\Leftrightarrow V_w(i)
\end{aligned}
$$

Completeness revisited

Define forcing relation $\Vdash'$:

$$w \vDash' \mathbf{K}\, s :\Leftrightarrow \forall w'. w \leq_{\mathbf{K}} w' \to w' \Vdash s$$

$$w \Vdash' s \lor t :\Leftrightarrow \neg\neg(w \Vdash' s \lor w \Vdash' t)$$

$$w \Vdash p_i :\Leftrightarrow \neg\neg(V_w(i))$$

Changes

- A theory $\mathcal{T}$ is quasi-prime iff.
  $\mathcal{T} \vdash A \lor B \implies \neg\neg(\mathcal{T} \vdash A \lor \mathcal{T} \vdash B)$
- Lindenbaum lemma: Any set $\mathcal{T}$ not deriving A can be extended to a consistent quasi-prime theory not deriving A
- Use consistent quasi-prime theories as worlds in canonical model
- Truth lemma: In the canonical model for any world w, formula A

$$w \Vdash A \iff \neg\neg(A \in w)$$

Completeness revisited

Define forcing relation $\Vdash'$:

$$w \vDash' \mathbf{K}\, s :\Leftrightarrow \forall w'. w \leq_{\mathbf{K}} w' \rightarrow w' \Vdash s$$

$$w \Vdash' s \vee t :\Leftrightarrow \neg\neg(w \Vdash' s \vee w \Vdash' t)$$

$$w \Vdash p_i :\Leftrightarrow \neg\neg(V_w(i))$$

Theorem (Quasi-completeness)

$\mathcal{T} \Vdash' A \implies \neg\neg\mathcal{T} \vdash A$

Corollary (Finitary completeness)

$\Gamma \Vdash' A \implies \Gamma \vdash A$

Summary

- Flexibility of representations important, two needed
- Constructive completeness still open (maybe provable via finite topological models (Coquand and Smith, 1996; Krupksi, 2016) or similar to IPC)
- Complete development $\approx$ 3.3 k LoC (1.5 k Cut Elimination, 1.5k ND + completeness, 300 decidability)
- Results apply to both IEL and IEL^{-}
- Results will probably transfer to similar intuitionistic modal logics, maybe even to classical ones (e.g. Logic K (Ono, 1998; Lellmann and Ramanayake, 2017))
- 2 perspectives: IEL as an interesting logic / IEL as a case-study
- Thesis will include philosophical discussion of IEL / co-reflection principle (cf. Murzi, 2010; Florio and Murzi, 2009)

Bibliography I

- Sergei Artemov and Tudor Protopopescu. "Intuitionistic epistemic logic". In: Review of Symbolic Logic 9.2 (2016), pp. 266–298. ISSN: 17550211. DOI: 10.1017/S1755020315000374. arXiv: 1406.1582.
- Kaustuv Chaudhuri, Leonardo Lima, and Giselle Reis. "Formalized Meta-Theory of Sequent Calculi for Substructural Logics". In: Electronic Notes in Theoretical Computer Science 332 (2017), pp. 57–73. ISSN: 15710661. DOI: 10.1016/j.entcs.2017.04.005. URL: http://dx.doi.org/10.1016/j.entcs.2017.04.005.
- Thierry Coquand and Jan M. Smith. "An application of constructive completeness". In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 1996. ISBN: 3540617809. DOI: 10.1007/3-540-61780-9_63.

Bibliography II

Hai Dang. Systems for Propositional Logics. Tech. rep. Saarland University, 2015, pp. 1–12. URL: https://www.ps.uni-saarland.de/{~}dang/ri-lab/propsystems/systems.pdf.

Floris van Doorn. "Propositional Calculus in Coq". In: (2015), pp. 1–11. arXiv: 1503.08744. URL: http://arxiv.org/abs/1503.08744.

S. Florio and J. Murzi. "The Paradox of Idealization". In: Analysis (2009). ISSN: 0003-2638. DOI: 10.1093/analys/anp069.

Masaki Hara. Proving decidability of Intuitionistic Propositional Calculus on Coq. 2013. URL: https://de.slideshare.net/qnighy/proving-decidability-of-intuitionistic-propositional-calculus-on-coqhttps://github.com/qnighy/IPC-Coq/tree/master/IPC.

Bibliography III

Vladimir N. Krupksi. On Some Formal Systems for Intuitionistic Epistemic Logic. 2016. URL: http://lpcs.math.msu.su/{~}krupski/IEL{_}abstract{_}slides.pdf (visited on 01/01/2021).

Vladimir N. Krupski and Alexey Yatmanov. “Sequent calculus for intuitionistic epistemic logic IEL”. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. 9537. Springer Verlag, 2016, pp. 187–201. ISBN: 9783319276823. DOI: 10.1007/978-3-319-27683-0_14. URL: https://link.springer.com/chapter/10.1007/978-3-319-27683-0{_}14.

Bibliography IV

- Björn Lellmann and Revantha Ramanayake. General methods in proof theory for modal logic. 2017. URL: https://www.logic.at/staffpages/revantha/Tutorial-lectures-1-3.pdf.
- Julius Michaelis and Tobias Nipkow. "Formalized Proof Systems for Propositional Logic". In: 5 (2017), pp. 1–5.
- Julien Murzi. "Knowability and bivalence: Intuitionistic solutions to the Paradox of Knowability". In: Philosophical Studies (2010). ISSN: 00318116. DOI: 10.1007/s11098-009-9349-y.
- Hiroakira Ono. "Proof-theoretic methods in nonclassical logic. An Introduction". In: M. Takahashi, M. Okada, and M. Dezani-Ciancaglini (eds.) Theories of Types and Proofs 2 (1998), pp. 207–254. DOI: 10.2969/msjmemoirs/00201c060.

Bibliography V

Hyungchul Park. "Bidirectional Proof Search Procedure for Intuitionistic Modal Logic IS5". Bachelors Thesis. Pohang University of Science and Technology (POSTECH), 2013. URL: http://pl.postech.ac.kr/IS5/thesis1.pdf.

Joseph Penington. Classical Propositional Proof Theory Proving in Coq Joseph Penington. Tech. rep. May. 2018, pp. 1–14.

Jan Von Plato. "A proof of Gentzen ' s Hauptsatz without multicut". In: 24 (2001), pp. 9–18.

Daniel Rogozin. Categorical and Algebraic Aspects of the Intuitionistic Modal Logic IEL´ and its predicate extensions. 2020. DOI: 10.1093/logcom/exaa082.

Gert Smolka and Chad E. Brown. Introduction to Computational Logic. 2012, p. 195. URL: http://www.ps.uni-saarland.de/courses/cl-ss12/script/icl.pdf.

Bibliography VI

- Hendrik Tews. "Formalizing cut elimination of coalgebraic logics in Coq". In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2013. ISBN: 9783642405365. DOI: 10.1007/978-3-642-40537-2_22.
- A. S. Troelstra and H. Schwichtenberg. Basic Proof Theory. 2000. DOI: 10.1017/cbo9781139168717.
- F Wolter and M Zakharyaschev. "Intuitionistic modal logics as fragments of classical bimodal logics". In: Logic at Work (1999).

IELGM calculus

$$\frac{\bot \in \Gamma}{\Gamma \Rightarrow s} \qquad \frac{p_i \in \Gamma}{\Gamma \Rightarrow p_i} \qquad \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C}$$

$$\frac{\Gamma \Rightarrow F \qquad \Gamma \Rightarrow G}{\Gamma \Rightarrow F \wedge G} \ \text{(AR)} \qquad \frac{F, \Gamma \Rightarrow U \qquad G, \Gamma \Rightarrow U}{(F \wedge G), \Gamma \Rightarrow U} \ \text{(AL)}$$

$$\frac{\Gamma \Rightarrow F_i}{\Gamma \Rightarrow F_1 \vee F_2} \ (\text{OR}_i) \qquad \frac{S, \Gamma \Rightarrow F \qquad T, \Gamma \Rightarrow F}{S \vee T, \Gamma \Rightarrow F} \ \text{(OL)}$$

$$\frac{F, \Gamma \Rightarrow G}{\Gamma \Rightarrow F_1 \supset F_2} \ \text{(IR)} \qquad \frac{S \supset T, \Gamma \Rightarrow S \qquad T, \Gamma \Rightarrow F}{S \supset T, \Gamma \Rightarrow F} \ \text{(IL)}$$

$$\frac{\mathbf{K}(\Delta), \Delta, \Gamma \Rightarrow \phi}{\Gamma, \mathbf{K}(\Delta) \Rightarrow \mathbf{K}\phi} \ \text{(KI)} \qquad \frac{\Gamma \Rightarrow \mathbf{K}\bot}{\Gamma \Rightarrow F} \ \text{(KB)}$$

Calculus for proof search

$$\frac{p_i \in \Gamma}{\Gamma \Rightarrow p_i} \qquad \frac{\bot \in \Gamma}{\Gamma \Rightarrow S} \qquad \frac{F, \Gamma \Rightarrow G}{\Gamma \Rightarrow F \supset G} \qquad \frac{F \supset G \in \Gamma \qquad \Gamma \Rightarrow F}{\Gamma \Rightarrow G}$$

$$\frac{F \wedge G \in \Gamma \qquad F, G, \Gamma \Rightarrow H}{\Gamma \Rightarrow H} \qquad \frac{\Gamma \Rightarrow F \qquad \Gamma \Rightarrow G}{\Gamma \Rightarrow F \wedge G}$$

$$\frac{F \vee G \in \Gamma \qquad F, \Gamma \Rightarrow H \qquad G, \Gamma \Rightarrow H}{\Gamma \Rightarrow H} \qquad \frac{\Gamma \Rightarrow F_i}{\Gamma \Rightarrow F_1 \vee F_2}$$

$$\frac{\Gamma, \mathbf{K}^{-}(\Gamma) \Rightarrow F}{\Gamma \Rightarrow \mathbf{K}\, F}$$

How does the permutation solver work?

1. $A \equiv_P B \iff \forall a, \text{countOcc}(A, a) = \text{countOcc}(B, a)$
2. Use that

   $$\text{countOcc}(A++B, a) = \text{countOcc}(A, a) + \text{countOcc}(B, a)$$

   and

   $$\text{countOcc}(b :: B, a) = \text{countOcc}([b], a) + \text{countOcc}(B, a)$$

   repeatedly
3. `intro ; lia`

Sample case from cut-elimination

Assume first premiss of cut was derived using right introduction rule for $\wedge$:

$$\dfrac{\dfrac{\Gamma 1 \overset{n-1}{\Rightarrow} A_1 \qquad \Gamma 1 \overset{n-1}{\Rightarrow} A_2}{\Gamma_1 \overset{n}{\Rightarrow} A_1 \wedge A_2} \qquad A_1 \wedge A_2, \Gamma_2 \overset{n}{\Rightarrow} \Delta}{\Gamma_1, \Gamma_2 \overset{S(n)}{\Rightarrow} \Delta}$$

Transformed into:

$$\dfrac{\Gamma_1 \overset{n-1}{\Rightarrow} A_1 \qquad \dfrac{\Gamma_1 \overset{n-1}{\Rightarrow} A_2 \qquad A_1, A_2, G, \Gamma_2 \overset{n-1}{\Rightarrow} \Delta}{A_1, \Gamma_1, \Gamma_2 \overset{n}{\Rightarrow} \Delta}}{\Gamma_1, (\Gamma_1, \Gamma_2) \Rightarrow \Delta}$$