Constructive and Mechanised Meta-Theory of Intuitionistic Epistemic Logic

Christian Hagemeier and Dominik Kirst (✉)

Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
christian@hagemeier.ch kirst@cs.uni-saarland.de

Abstract. Artemov and Protopopescu proposed intuitionistic epistemic logic (IEL) to capture an intuitionistic conception of knowledge. By establishing completeness, they provided the base for a meta-theoretic investigation of IEL, which was continued by Krupski with a proof of cut-elimination, and Su and Sano establishing semantic cut-elimination and the finite model property. However, to the best of our knowledge, no analysis of these results in a constructive meta-logic has been conducted. We aim to close this gap and investigate IEL in the constructive type theory of the Coq proof assistant. Concretely, we present a constructive and mechanised completeness proof for IEL, employing a syntactic decidability proof based on cut-elimination to constructivise the ideas from the literature. Following Su and Sano, we then also give constructive versions of semantic cut-elimination and the finite model property. Given our constructive and mechanised setting, all these results now bear executable algorithms. We expect that our methods used for mechanising cut-elimination and decidability also extend to other modal logics (and have verified this observation for the classical modal logic K).

Keywords: Epistemic Logic, Completeness, Constructive Mathematics

1 Introduction

Intuitionistic epistemic logic (IEL), introduced by Artemov and Protopopescu [1], is a relatively recent formalism modelling an intuitionistic conception of knowledge. While classical epistemic logics [14,23] typically include the *reflection principle* $\mathsf{K}\, A \supset A$, read as "known propositions must be true", IEL is based on the *co-reflection principle* $A \supset \mathsf{K}\, A$, read as "from the existence of proofs we can gain knowledge by verification". This striking disagreement is explained by the divergent notions of truth: while a proposition is determined classically true by its binary truth value, it is considered intuitionistically true if an (intuitionistic) proof in the prevailing Brouwer-Heyting-Kolmogorov (BHK) interpretation has been constructed. While the sole addition of co-reflection to intuitionistic propositional logic results in the logic of intuitionistic belief (IEL$^-$), Artemov and Protopopescu propose the further addition of *intuitionistic reflection* $\mathsf{K}\, A \supset \neg\neg A$ for IEL. This principle reestablishes, up to a double negation, the factivity of truth classically expressed by reflection, and therefore places intuitionistic knowledge as a modality between intuitionistic and classical truth.

Complementing the philosophical arguments for (and against) IEL, the original paper [1] already contains several technical results such as soundness and completeness with respect to a suitable Kripke semantics, as well as derived observations concerning the disjunction property and admissibility of reflection. This formal investigation has been carried on for instance by Su and Sano [27] with proofs of the finite model property and semantic cut-elimination, and by Krupski [18] with proofs of syntactic cut-elimination and decidability. However, especially the arguments for completeness relying on the Lindenbaum construction manifestly employ classical logic, leaving the current state of the meta-theory of IEL unsatisfactory: while the formalism itself successfully embraces intuitionistic principles to tackle classical knowability paradoxes, no visible attempts are made to describe its semantics in constructive terms.

With this paper, we hope to contribute to a more uniform picture by developing all mentioned results in a purely constructive setting. Concretely, we illustrate that by preparing an argument for the finite model property along the lines of Su and Sano by a syntactic decidability proof inspired by Smolka, Brown, and Dang [26,6], completeness of IEL with respect to finite contexts can be obtained without appeal to classical logic. Moreover, in the fashion of *constructive reverse mathematics* [15,16], we show that completeness with respect to possibly infinite contexts as entailed by the development in [1] is equivalent to the law of excluded middle (LEM), while even the restriction of completeness to enumerable contexts is still strong enough to imply Markov's principle (MP), both observations following similar arguments as applicable to first-order logic [11].

As a framework, we employ the constructive type theory CIC [4,20] implemented in the *Coq proof assistant* [30]. We deem this choice valuable for three reasons: First, CIC embodies a rather modest system free of debatable choice principles diluting the analysis [24]. Secondly, CIC is based on the same principles justifying IEL by internalising the BHK interpretation in a proof-relevant way and in fact modelling K by a truncation operation from computational types to the impredicative universe $\mathbb{P}$ of propositions, obeying co-reflection and intuitionistic reflection. Thirdly, we use its implementation in Coq as a tool to verify all proofs, track the usage of assumptions, and exhibit the algorithmic content of the constructive meta-theory for instance in the form of executable algorithms for completeness, cut-elimination, and decidability. The resulting Coq development is systematically hyperlinked with the PDF version of this paper.[1]

Contributions. To the best of our knowledge, we are the first to explicitly develop the meta-theory of IEL in a fully constructive setting. Moreover, all our results are mechanised using the Coq proof assistant and accompanied by similar proof-theoretic results for the classical modal logic K.

Outline. In Section 2, we begin with some preliminary definitions concerning the constructive type theory we are working in. In Section 3, we introduce formulas and the natural deduction system of IEL and outline their encoding in

[1] See Appendix 2, also browsable at `https://www.ps.uni-saarland.de/extras/iel`.

constructive type theory. In Section 4, we introduce a sequent calculus suitable for mechanising cut-elimination which we use in Section 5 to prove decidability for IEL. Section 6 establishes constructive completeness and the finite model property. In Section 7, we report results about infinite theories and strong completeness. We close with a review of the literature and future work in Section 8.

2 Preliminaries

We work in the constructive type theory CIC [4,20] of the Coq proof assistant [30], with a predicative hierarchy of type universes $\mathbb{T}_i$ above a single impredicative universe $\mathbb{P}$. We will always omit the level and write $\mathbb{T}$ for any $\mathbb{T}_i$. On the type level, we have the unit type $\mathbb{1}$ with the single element $*$, the void type $\mathbb{0}$, function spaces $X \to Y$, products $X \times Y$, sums $X + Y$, dependent products $\forall x^X. F\,X$, and dependent sums $\Sigma x^X. F\,x$. On a propositional level, these types are denoted using by the usual logical notation $(\top, \bot, \to, \land, \lor, \exists, \forall)$. Elimination from $\mathbb{P}$ into $\mathbb{T}$ is restricted to hide the computational content of proofs.

Basic inductive types we use are natural numbers $\mathbb{N} ::= 0 \mid n+1\,(n \in \mathbb{N})$ and booleans $\mathbb{B} := \mathsf{tt} \mid \mathsf{ff}$. Furthermore given a type X, we define lists $\mathcal{L}(X) := \emptyset \mid x :: L$ for $x : X$ and $L : \mathcal{L}(X)$, and the option type $\mathcal{O}(X) := \emptyset \mid \ulcorner x \urcorner$. To ease notation we will oftentimes denote appending an element x to a list L by L, x.

Definition 1. Let X be a type and $p : X \to \mathbb{P}$ be a predicate. We call

- p enumerable, if there is $f : \mathbb{N} \to \mathcal{O}(X)$ with $\forall x^X. p\,x \leftrightarrow \exists n^{\mathbb{N}}. f\,n = \ulcorner x \urcorner$,
- p decidable, if there is some $f : X \to \mathbb{B}$ with $p\,x \leftrightarrow \forall x^X. f(x) = \mathsf{tt}$.

These notions generalise easily to predicates of higher arity. A type X is enumerable if the predicate $p : X \to \mathbb{P}$ defined by $p\,x := \top$ is enumerable. X is discrete if the predicate $\lambda xy. x = y$ is decidable.

One technique we will often use throughout this paper is reasoning classically locally whenever we prove a negative statement, captured by the following fact:

Lemma 2. *The statements* $\neg\neg(P \lor \neg P)$ *and* $((P \lor \neg P) \to \neg Q) \to \neg Q$ *hold for arbitrary propositions* $P, Q : \mathbb{P}$.

Non-classical-axioms. Especially important for our development is the law of excluded middle, $\mathsf{LEM} := \forall P : \mathbb{P}. P \lor \neg P$ and Markov's principle

$$\mathsf{MP} := \forall f : \mathbb{N} \to \mathbb{B}. \neg\neg(\exists n. f\,n = \mathsf{tt}) \to \exists n. f\,n = \mathsf{tt}.$$

It is well-known, that MP is weaker than LEM and has a computational justification based on linear search, which LEM completely lacks [5].

3 Basic Intuitionistic Epistemic Logic

This section introduces formulas of IEL, the natural deduction system, and its models closing with a statement of the classical completeness proof. We present nothing new, instead recapping material from Artemov and Protopopescu [1] adapted to the setting of constructive type theory.

Definition 3. The syntax of IEL is given by the following inductive datatype:

$$A, B : \mathcal{F} ::= A \vee B \mid A \wedge B \mid A \supset B \mid \mathsf{K}\,A \mid p_i \mid \bot \quad (i \in \mathbb{N})$$

Lemma 4. *The type $\mathcal{F}$ is discrete and enumerable.*

Proof. Both are established using standard techniques e.g. [10, Fact 3.19]. □

Since $\mathcal{F}$ is inhabited, we can even establish a stronger claim than enumerability, namely that a function $f : \mathbb{N} \to \mathcal{F}$ exists s.t. $\forall A^{\mathcal{F}}.\, \exists n^{\mathbb{N}}.\, f n = A$. In our formal setting, we model finite theories as lists of formulas. Throughout this paper, we refer to these as finite sets and use usual set-theoretic notation. Induction on a finite set, then, is just induction on the list representing the finite set. Infinite contexts, here called theories, are represented as predicates $\mathcal{T} : \mathcal{F} \to \mathbb{P}$, with the intended reading that $A \in \mathcal{T}$ iff $\mathcal{T}\,A$ holds.

The natural deduction calculus for IEL is encoded as an inductive predicate $\vdash : \mathcal{L}(\mathcal{F}) \to \mathcal{F} \to \mathbb{P}$. Natural deduction for IEL$^-$ was introduced by Rogozin [25], however our system is slightly different to ease the mechanisation. The idea is to extend a natural deduction calculus for intuitionistic propositional logic by rules for co-reflection *(KR)* and distribution *(KD)* to express IEL$^-$, and by a rule for intuitionistic reflection *(KF)* to express IEL. These rules are shown in Figure 1; the full system can be found in Appendix 1. The main difference between our system and that of Rogozin is the distribution rule, as Rogozin's formulation equivalently allows for multiple applications of our *KD*-rule in one step.

In this paper, we will always state and prove results for IEL, the proofs for IEL$^-$ can be obtained from the proofs for IEL by omitting certain parts. In fact, the mechanisation contains formal proofs for both systems, avoiding code duplication with tagged deduction systems (see Appendix 2).

We naturally extend derivability to theories $\mathcal{T} : \mathcal{F} \to \mathbb{P}$ by writing $\mathcal{T} \vdash A$ if there is a finite set $\Gamma \subseteq \mathcal{T}$ with $\Gamma \vdash A$.

$$\frac{\Gamma \vdash A}{\Gamma \vdash \mathsf{K}\,A}\ (KR) \qquad \frac{\Gamma \vdash \mathsf{K}\,(A \supset B)}{\Gamma \vdash \mathsf{K}\,A \supset \mathsf{K}\,B}\ (KD) \qquad \frac{\Gamma \vdash \mathsf{K}\,A}{\Gamma \vdash \neg\neg A}\ (KF)$$

Fig. 1. Selected natural deduction rules for IEL

Models for IEL extend standard Kripke semantics by a verification relation. We refer to the reader to Wolter and Zakharyaschev [33], whose paper contains general results in the model theory of intuitionistic modal logics.

Definition 5. (Kripke Models) A *Kripke Model* for IEL, IEL^- is a quadruple $(\mathcal{W}, \mathcal{V}, \leq, \leq_{\mathsf{K}})$ consisting of a type of worlds $\mathcal{W}$, and a valuation $\mathcal{V} : \mathcal{W} \to \mathbb{N} \to \mathbb{P}$, which must have the following properties:

1. $\leq$ is a preorder on $\mathcal{W}$,
2. If $w \leq v$ and $V(w, i)$ then $V(v, i)$ for any w, v, i,
3. $\leq \circ \leq_{\mathsf{K}} \subseteq \leq_{\mathsf{K}}$, i.e. if $w \leq u$ and $u \leq_{\mathsf{K}} v$ then $w \leq_{\mathsf{K}} v$ for any $w, u, v \in \mathcal{W}$,
4. $\leq_{\mathsf{K}} \subseteq \leq$, i.e. if $w \leq_{\mathsf{K}} v$ then $w \leq u$ for any $u, v \in \mathcal{W}$.

Property 2 in above definition is known as *persistence*. For IEL, additionally the models need to have a serial $\leq_{\mathsf{K}}$-relation, i.e. for all w there should be some v with $w \leq_{\mathsf{K}} v$.

Definition 6. (Forcing Relation) Let $\mathcal{M}$ be a Kripke model. We define the forcing relation by recursion on the formula:

$$\begin{aligned}
w \Vdash p_i &:\Leftrightarrow \mathcal{V}(w, i) \\
w \Vdash A_0 \wedge A_1 &:\Leftrightarrow w \Vdash A_0 \wedge w \Vdash A_1 \\
w \Vdash A_0 \vee A_1 &:\Leftrightarrow w \Vdash A_0 \vee w \Vdash A_1 \\
w \Vdash A_0 \supset A_1 &:\Leftrightarrow \forall w'. w \leq w' \to w' \Vdash A_0 \to w' \Vdash A_1 \\
w \Vdash \mathsf{K}\, A_0 &:\Leftrightarrow \forall w'.\, w \leq_{\mathsf{K}} w' \to w' \Vdash A_0
\end{aligned}$$

We can easily establish that the forcing relation is monotone.

Lemma 7. (Monotonicity) *Let $\mathcal{M}$ be an arbitrary model and A be any formula. If $w \leq v$ and $\mathcal{M}, w \Vdash A$ then $\mathcal{M}, v \Vdash A$.*

Proof. Induction on A utilising the persistence of $\mathcal{V}$. □

We use the standard notation $\Gamma \Vdash A$ to denote that any model forcing Γ forces A, too.[2] Note that this notation is monotone in the following sense: If $\Gamma \subseteq \Gamma'$ and $\Gamma \Vdash A$ then $\Gamma' \Vdash A$.

Soundness for Kripke models can be established by a simple induction.

Lemma 8. (Soundness) *If $\mathcal{T} \vdash A$ then $\mathcal{T} \Vdash A$.*

Proof. Assume $\mathcal{T} \vdash A$, thus there is a finite set $\Gamma \subseteq \mathcal{T}$ s.t. $\Gamma \vdash A$. Then by induction on $\Gamma \vdash A$ we show $\Gamma \Vdash A$, relying on Lemma 7. Thus also $\mathcal{T} \Vdash A$. □

With soundness, we can establish consistency of IEL.

Lemma 9. (Consistency) *IEL is consistent.*

Proof. For deriving a contradiction, assume $\vdash \bot$. Thus by soundness (Lemma 8) $\bot$ is entailed in any model at every world. But we can easily construct a model where $M, w \nVdash \bot$, contradicting the assumption. □

[2] Formally, define $\Gamma \Vdash A := \forall \mathcal{M} w.\, (\forall B \in \Gamma.\, \mathcal{M}, w \Vdash B) \to \mathcal{M}, w \Vdash A$.

Finally, we formulate a strong version of the classical completeness theorem, by composition of the Lindenbaum and Truth Lemma both established in [1]. Notably, the authors of [1] prove both lemmas using LEM to allow case distinctions whether a formula is contained in or provable from an infinite context.

Theorem 10. (Classical Completeness) *Let $\mathcal{T} : \mathcal{F} \to \mathbb{P}$ be an arbitrary predicate on formulas. Assuming* LEM*, if $\mathcal{T} \Vdash A$ then $\mathcal{T} \vdash A$.*

4 Cut-Free Sequent Calculus

Sequent calculus representations for IEL have been proposed by Krupski [18], Su and Sano [28], and more recently Fiorino [9].

A main challenge for us is to find an encoding suitable for proving termination of the proof search and structural properties in a proof assistant. We employ a sequent calculus similar to the GKI-calculus by Kleene [17] and extending it to cover IEL by using additional rules, similar to those used by Krupski [18]. Similar techniques have been used by Smolka, Brown, and Dang [26,6] to establish decidability of classical and intuitionistic propositional logic in Coq.

Let us highlight why this encoding is well-suited for mechanisation: In most textbooks [31] the GKI-calculus does not use membership but instead just keeps the principal formula in the premiss.

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

The left-hand side is the usual presentation, while the version on the right is the one we use. This change into using membership helps with automation.

The rules of the calculus are displayed in Figure 2, where for a finite set Γ we denote the downward K-projection by $\Gamma_{\mathsf{K}} := \{A \mid \mathsf{K}\, A \in \Gamma\}$.

The cumulative character of the rules makes it possible to encode this calculus easily in a proof assistant, utilising list membership. This calculus is encoded as a predicate $\Rightarrow : \mathcal{L}(\mathcal{F}) \to \mathcal{F} \to \mathbb{P}$, we also define a height-bounded variant and use $\Gamma \overset{h}{\Rightarrow} A$ to denote that a derivation of $\Gamma \Rightarrow A$ of height less or equal to h exists. Our height encoding is inspired by Michaelis and Nipkow [19]. We assume that the heights of all derivations in the premisses are equal and we include an additional rule to increase the height of any derivation (see Appendix 2).

From a high-level view, our cut-admissibility proof follows the same structure employed by many textbooks (e.g. [31]), using a double induction on the sum of heights in the derivation and the formula size. However the lower level structure is different since we cannot perform case distinctions on principality and instead can only use case analyses on the last rule applied in a derivation. Following the traditional presentation, we first show depth-preserving weakening.

Lemma 11. (Weakening) *If $\Gamma \subseteq \Delta$ and $\Gamma \overset{n}{\Rightarrow} A$ then $\Delta \overset{n}{\Rightarrow} A$.*

Proof. The proof is by induction on the derivation $\Gamma \overset{n}{\Rightarrow} A$ with Δ quantified. □

$$\frac{p_i \in \Gamma}{\Gamma \Rightarrow p_i}\ (V) \qquad \frac{\bot \in \Gamma}{\Gamma \Rightarrow S}\ (F)$$

$$\frac{F \supset G \in \Gamma \qquad \Gamma \Rightarrow F}{\Gamma \Rightarrow G}\ (IL) \qquad \frac{\Gamma, F \Rightarrow G}{\Gamma \Rightarrow F \supset G}\ (IR)$$

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

$$\frac{F \vee G \in \Gamma \qquad \Gamma, F \Rightarrow H \qquad \Gamma, G \Rightarrow H}{\Gamma \Rightarrow H}\ (OL) \qquad \frac{\Gamma \Rightarrow F_i}{\Gamma \Rightarrow F_1 \vee F_2}\ (\mathrm{OR}_i)$$

$$\frac{\Gamma \cup \Gamma_{\mathsf{K}} \Rightarrow F}{\Gamma \Rightarrow \mathsf{K}\, F}\ (\mathrm{KI}) \qquad \frac{\Gamma \Rightarrow \mathsf{K} \bot}{\Gamma \Rightarrow A}\ (\mathrm{KF})$$

Fig. 2. Sequent system for IEL (GKIEL)

Note that this result is stronger than what is usually referred as weakening e.g. $\Gamma \Rightarrow A \to \Gamma, B \Rightarrow A$, since our version does allow to remove duplicate occurrences of formulas. Thus we do not prove what is usually referred to as the contraction rule.

Lemma 12. (Inversion) *The rules for conjunction, disjunction and implication are height-preserving invertible in the following sense:*

- *If* $B \in \Gamma$ *and* $\Gamma, A \supset B \overset{n}{\Rightarrow} C$ *then* $\Gamma \overset{n}{\Rightarrow} C$.
- *If* $A \in \Gamma$ *and* $\Gamma, A \vee B \overset{n}{\Rightarrow} C$ *then* $\Gamma \overset{n}{\Rightarrow} C$.
- *If* $B \in \Gamma$ *and* $\Gamma, A \vee B \overset{n}{\Rightarrow} C$ *then* $\Gamma \overset{n}{\Rightarrow} C$.
- *If* $A \wedge B, \Gamma \Rightarrow C$ *and* $\Gamma, A, B \overset{n}{\Rightarrow} C$ *then* $\Gamma \overset{n}{\Rightarrow} C$.

Proof. The proofs are by induction on the height with the formulas quantified. Most cases are solved by applying the rule used to obtain the derivation and using the inductive hypothesis afterwards. Only when the rule we are showing invertible is used on the same formulas (e.g. same A and B), it suffices to use the inductive hypothesis directly. □

Theorem 13. (Cut-Admissibility) *If* $\Gamma \Rightarrow A$ *and* $A, \Gamma \Rightarrow B$ *then* $\Gamma \Rightarrow B$.

Proof. The proof uses a strong induction on pairs of numbers (r, s), representing the cut-rank (sum of the depths of the derivation) and the size of the cut-formula s. Thus we have one inductive hypothesis allowing us to delete cuts on smaller formulas (e.g. formulas with smaller size; this includes subformulas) with arbitrary depths and a second hypothesis, allowing us to eliminate cuts with a smaller rank on the same formula.

We first do a case analysis on $\Gamma \Rightarrow A$, in some cases, we also need to do a second case analysis on $A, \Gamma \Rightarrow B$. Some illustrative cases can be found in Appendix 3. □

With cut-elimination, we can prove the agreement between natural deduction and the sequent calculus directly.

Theorem 14. (Agreement) *For any Γ and A, we have $\Gamma \vdash A$ iff $\Gamma \Rightarrow A$.*

Proof. Both directions are proven by induction on the derivation. The direction from natural deduction to the sequent calculus prominently uses the cut-admissibility result (Theorem 13), the converse direction is straightforward and does not need this result. □

Lemma 15. (Disjunction Property) *If $\Rightarrow A \vee B$ then $\Rightarrow A$ or $\Rightarrow B$.*

Proof. By induction on the derivation $\Rightarrow A \vee B$. □

Combining both Theorem 14 and Lemma 15 yields a proof of the disjunction property for natural deduction.

Corollary 16. (ND Disjunction Property) *If $\vdash A \vee B$ then $\vdash A$ or $\vdash B$.*

5 Decidability via Proof Search

We establish decidability of the natural deduction system for IEL by proving decidability for the cut-free sequent calculus and combining this with our equivalence proof (Theorem 14). The algorithm is an instance of Kleene-style fixed-point iteration. Crucial to this endeavor is the subformula property, which states that for a sequent $\Gamma \Rightarrow A$ there is a finite universe of sequents such that any backwards application of the rules stays within the universe.

Definition 17. (Subformula) The finite set $\mathrm{Subs}(A)$, containing all subformulas of a formula A, is defined by recursion on A:

$$\begin{aligned}\mathrm{Subs}(A_1 \circ A_2) &:= \mathrm{Subs}(A_1) \cup \mathrm{Subs}(A_2) \cup \{A_1 \circ A_2\}\\ \mathrm{Subs}(\mathsf{K}\, A_1) &:= \mathrm{Subs}(A_1) \cup \{\mathsf{K}\, A_1\}\\ \mathrm{Subs}(p_i) &:= \{p_i\}\end{aligned}$$

In the above definition, the circle $\circ$ is a placeholder for any binary connective. For a set of formulas Γ we define its *subformula universe* $\mathrm{Subs}(\Gamma) := \bigcup_{F \in \Gamma} \mathrm{Subs}(F)$. We call Γ subformula-closed if $\mathrm{Subs}(\Gamma) \subseteq \Gamma$.

Formally, we represent the sequents used during the proof search, also called goals, by members of the type $\mathcal{G} := \mathcal{L}(\mathcal{F}) \times \mathcal{F}$, so pairs (Γ, A) of a context Γ and a formula A. IEL enjoys the subformula property, since all derivations of $\Gamma \Rightarrow A$ only use formulas from $S := \mathrm{Subs}(\Gamma, A, \mathsf{K}\perp)$ and thus we can identify a universe $\mathcal{U} := \{(\Gamma, A) \mid \Gamma \subseteq S \wedge A \in S\}$ and restrict our proof search to $\mathcal{U}$-goals.

Having identified this set, we compute the set of derivable goals by a fixed-point iteration starting from the empty set. We can envision this process as iteratively expanding a candidate set of derivable goals until the set no longer changes. We always add a goal when it is possible to derive it using the previous goals, for example, assume that $\Gamma \Rightarrow A$ and $\Gamma \Rightarrow B$ are both derivable, then in the next step of the iteration, it would be possible to add $\Gamma \Rightarrow A \wedge B$. To formalise this extension process we define a decidable step relation $\mathsf{step} : \mathcal{L}(\mathcal{G}) \to \mathcal{G} \to \mathbb{P}$. This relation holds if, using the derivations in the list, the goal can be derived in a single step.

The algorithm now works by, in every iteration, checking if there is a goal in $\mathcal{U}$ which is in step relation with the set of currently known derivable sequents. If there is such a goal, it is added and the step is repeated, otherwise the algorithm terminates. Such a procedure will reach a fixed-point after at most $|\mathcal{U}|$ iterations. We denote the resulting list of goals by Λ.

Two crucial properties of Λ we need later are the closure property and induction principle.

Lemma 18. *The following hold for the list Λ obtained as fixed-point of* step*:*

- *Λ-Closure: $\mathsf{step}\,\Lambda \subseteq \Lambda$*
- *Λ-Induction: Let $\mathsf{step}\,A \cap \mathcal{U} \subseteq p$ for all $A \subseteq p$ and an arbitrary predicate p. Then $\Lambda \subseteq p$.*

Proof. See Lemma 12.4.2 in [26]. □

Lemma 19. *If $(\Gamma, A) \in \Lambda$ then $\Gamma \Rightarrow A$.*

Proof. By Λ-induction. Thus fix any set $\mathcal{U}'$ s.t. $(\Gamma, A) \in U' \to \Gamma \Rightarrow A$ and assume that the step relation holds for U' and $\Gamma' \Rightarrow A'$. We need to show $\Gamma' \Rightarrow A'$. We can analyse which rule caused the step relation to be fulfilled and the assumptions about $\mathcal{U}'$ to create the derivation. □

Lemma 20. *If $\Gamma, A \in \mathcal{U}$ and $\Gamma \Rightarrow A$ then $(\Gamma, A) \in \Lambda$.*

Proof. The proof is by induction on $\Gamma \Rightarrow A$. We use Λ-closure in every step and thus only need to prove that $\mathsf{step}\,\Lambda\,(\Gamma, A)$ holds.

Case AR: Assume $\Gamma \Rightarrow A_1$ and $\Gamma \Rightarrow A_2$, thus $(\Gamma, A_1) \in \Lambda$ and $(\Gamma, A_2) \in \Lambda$ by the inductive hypothesis. Thus the step relation holds between Λ and $(\Gamma, A_1 \wedge A_2)$. Since Λ is closed under the step relation, we are done.

Case AL: Assume there is $B \wedge C \in \Gamma$ and $B, C, \Gamma \Rightarrow A$. Thus by the inductive hypothesis $((B, C, \Gamma), A) \in \Lambda$. Thus the step relation holds between Λ and $((B \wedge C, \Gamma), A)$, since we can derive the goal in one step using AL.

□

Theorem 21. *The sequent calculus $\Gamma \Rightarrow A$ is decidable.*

Proof. Decide $(\Gamma, A) \in \Lambda$ and, depending on the outcome, apply Lemma 20 or Lemma 19 to obtain either $\Gamma \Rightarrow A$ or $\Gamma \not\Rightarrow A$. □

Corollary 22. *The natural deduction system $\Gamma \vdash A$ is decidable.*

Proof. A consequence of Theorem 21 and Theorem 14. □

6 Constructive Completeness

In this section, we detail the constructive proof of both the finite model property and completeness. Both properties are proven by constructing a finite canonical model, whose worlds consist of finite, prime, and consistent sets of formulas that are deductively closed with respect to a subformula-universe.

We begin by carrying out the Lindenbaum construction constructively. The key insight here is that due to decidability, we can actually represent the extension process as a computable function operating on finite contexts.

6.1 Lindenbaum Extension

We start by defining a function that extends a (finite) set of formulas Γ by a formula B, if non-derivability of $A_\bot$ is preserved.

$$\Gamma \oplus_{A_\bot} B \coloneqq \begin{cases} \Gamma, B & \text{if } \Gamma, B \nvdash A_\bot \\ \Gamma & \text{otherwise} \end{cases}$$

Note that due to the decidability, we can actually compute this function for any finite set of formulas Γ. For a finite set $\mathcal{U}$ we use $\Gamma \oplus_{A_\bot} \mathcal{U}$ as notation for applying the extension procedure iteratively to every element from $\mathcal{U}$.

Definition 23. (Context Properties) Let $\mathcal{U}$ be a finite set of formulas. A set of formulas Γ is a $\mathcal{U}$-theory iff for any formula $A \in U$ derivability implies membership, i.e. $\Gamma \vdash A \to A \in \Gamma$.

Γ is $\mathcal{U}$-prime if for any $A \vee B \in \Gamma$ we have $A \in \Gamma \vee B \in \Gamma$ for any $A, B \in \mathcal{U}$.

We can now establish properties of the extension.

Lemma 24. *If $\Gamma \nvdash A_\bot$ then $\Gamma \oplus_{A_\bot} \mathcal{U} \nvdash A_\bot$ for any $\mathcal{U}$.*

Proof. The proof is by induction on $\mathcal{U}$. The case $\mathcal{U} = \emptyset$ is trivial. In the case where $\mathcal{U} = \mathcal{U}' \cup \{u\}$, we can decide $\Gamma \oplus_{A_\bot} \mathcal{U}', u \vdash A_\bot$. If $\Gamma \oplus_{A_\bot} \mathcal{U}', u \vdash A_\bot$, we know that $\Gamma \oplus_{A_\bot} \mathcal{U}'$ is extensionally equivalent to $\Gamma \oplus_{A_\bot} \mathcal{U}$ and thus can use the inductive hypothesis; in the other case we have $\Gamma \oplus_{A_\bot} \mathcal{U}' \nvdash A_\bot$ as a hypothesis. □

Lemma 25. *If $\Gamma \nvdash A_\bot$, $B \in \mathcal{U}$ and $\Gamma \oplus_{A_\bot} \mathcal{U} \nvdash B$ then $\Gamma \oplus_{A_\bot} \mathcal{U} \vdash B \supset A_\bot$.*

Lemma 26. *The extension is a $\mathcal{U}$-theory.*

Next, we can establish that the extension is $\mathcal{U}$-prime.

Lemma 27. (Primeness) *For any $\Gamma, \mathcal{U}$: If $\Gamma \nvdash A_\bot$ then $\Gamma \oplus_{A_\bot} \mathcal{U}$ is $\mathcal{U}$-prime.*

Proof. Let $A \vee B \in \Gamma \oplus_{A_\bot} \mathcal{U}$, furthermore assume $A \in \mathcal{U} \vee B \in \mathcal{U}$. Since we can compute the extension, we can decide wether A or B are contained in the extension. The cases where either are contained are easy. In the other case, we have both $A \notin \Gamma \oplus_{A_\bot} \mathcal{U}$ and $B \notin \Gamma \oplus_{A_\bot} \mathcal{U}$, thus by Lemma 25 we have both $\Gamma \oplus_{A_\bot} \mathcal{U} \vdash A \supset A_\bot$ and $\Gamma \oplus_{A_\bot} \mathcal{U} \vdash B \supset A_\bot$. Since $A \vee B \in \Gamma \oplus_{A_\bot} \mathcal{U}$ we can derive $A_\bot$ contradicting Lemma 24. □

So essentially, constructive primeness follows from decidable membership.

Lemma 28. (Lindenbaum) *Let Γ be a list of formulas s.t. $\Gamma \nvdash A$ and $\mathcal{U}$ arbitrary. We can compute a $\mathcal{U}$-prime $\mathcal{U}$-theory extending Γ not deriving A.*

Proof. Can be achieved by combining Lemmas 24, 25 and 27. □

6.2 Canonical Models

In this section, we construct a canonical model with respect to a finite formula universe $\mathcal{U}$. This universe will be instantiated to a concrete subformula universe in the proof of Theorem 32. The construction is inspired by both [1] and [27].

Definition 29. (Canonical Model) We define $\mathcal{M}_C = (\mathcal{W}_C, \mathcal{V}_C, \leq, \leq_{\mathsf{K}})$ by

- $\mathcal{W}_C := \{\Gamma \subseteq \mathcal{U} \mid \Gamma \text{ is a } \mathcal{U}\text{-prime, consistent } \mathcal{U}\text{-theory}\}$
- $\mathcal{V}_C(\Gamma, i) := p_i \in \Gamma$
- $\Gamma \leq \Delta := \Gamma \subseteq \Delta$
- $\Gamma \leq_{\mathsf{K}} \Delta := \Gamma \cup \Gamma_{\mathsf{K}} \subseteq \Delta$

We can easily establish that the defined model is actually a model for IEL, by showing that the $\leq_{\mathsf{K}}$-relation is serial (e.g. every world w has a $\leq_{\mathsf{K}}$-successor):

Lemma 30. *Every world has a $\leq_{\mathsf{K}}$-successor.*

Proof. The proof works by Lindenbaum-extending $\Gamma \cup \Gamma_{\mathsf{K}}$ to not derive $\bot$. This yields a world in the model, which is a $\leq_{\mathsf{K}}$-successor to Γ. □

Now we can show the following version of the Truth Lemma constructively.

Lemma 31. (Truth Lemma) *For any $\Gamma \in \mathcal{W}_C$ and $A \in \mathcal{U}$ we have*

$$A \in \Gamma \iff \mathcal{M}_C, \Gamma \Vdash A.$$

Proof. The proof is by induction on A. We only consider selected cases here.

$A = A_1 \vee A_2$: Assume $\mathcal{M}_C, \Gamma \Vdash A$ thus by definition, we have either $\mathcal{M}_C, \Gamma \Vdash A_1$ or $\mathcal{M}_C, \Gamma \Vdash A_2$, thus by the inductive hypothesis; we either have $A_1 \in \Gamma$ or $A_2 \in \Gamma$. Using that Γ is a $\mathcal{U}$-theory and $A_1 \vee A_2 \in \mathcal{U}$ we can arrive at the conclusion.
For the other direction, we assume $A_1 \vee A_2 \in \Gamma$. Since Γ is $\mathcal{U}$-prime, we have either $A_1 \in \Gamma$ or $A_2 \in \Gamma$. In both cases, we can establish $\Gamma \Vdash A$ using the inductive hypothesis and the definition of entailment.

$A = \mathsf{K}\, A_1$: Assume $\mathsf{K}\, A \in \Gamma$. Let Δ be an arbitrary $\leq_{\mathsf{K}}$-successor to Γ. We need to establish $\Delta \vdash A$, by the inductive hypothesis it suffices to establish $A \in \Delta$, which is simple using the definition of $\leq_{\mathsf{K}}$.
Assume $M_C, \Gamma \Vdash \mathsf{K}\, A$. Again using stability of membership, furthermore assume $\mathsf{K}\, A \notin \Gamma$. Now we can Lindenbaum-extend $\Gamma, \Gamma_{\mathsf{K}}$ to a world in the model that does not derive A. But this world is a $\leq_{\mathsf{K}}$-successor, contradicting $M_C, \Gamma \Vdash \mathsf{K}\, A$. □

This allows us to prove completeness constructively, which can be interpreted as an algorithm reifying a proof term of the formal type-theoretic meta-logic into a derivation in natural deduction.

Theorem 32. (Constructive Completeness) *If $\Gamma \Vdash A$ then $\Gamma \vdash A$.*

Proof. Since $\vdash$ is stable under double negation (consequence of decidability, Corollary 22), we can assume both $\Gamma \Vdash A$ and $\Gamma \nvdash A$ and need to derive a contradiction. Using the Lindenbaum lemma (Lemma 28) Γ can be extended to a world $\Gamma'$with $A \notin \Gamma'$ of the canonical model for the subformula universe of (Γ, A) and therefore by Lemma 31, $\mathcal{M}_C, \Gamma' \nVdash A$. But this contradicts $\Gamma' \Vdash A$, which is easily obtained from $\Gamma \Vdash A$ using monotonicity. □

With the constructive completeness proof it is now possible to constructively derive admissibility results from [1], e.g. the admissibility of reflection (we don't repeat the proof from [1] here but refer to the Coq development).

6.3 Finite Model Property

Intuitively, the finite model property is a trivial consequence of the fact that the canonical model is finite, which is simple to observe since the worlds are subsets of a finite set and thus only finitely many of them exist. This has also been established by Su and Sano [27]. For IEL$^-$ the finite model property has already been established by Wolter and Zakharyaschev [32]. We first define entailment restricted to finite models:[3]

$$\Gamma \Vdash_{\text{fin}} A \;:=\; \forall \mathcal{M}.\, \mathsf{fin}(\mathcal{M}) \to \mathcal{M} \Vdash \Gamma \to \mathcal{M} \Vdash A.$$

A logic now has the finite model property, if any formula entailed in all finite models is a theorem.[4]

Definition 33. A logic $\mathcal{L}$ has the finite model property if $\Gamma \Vdash_{\text{fin}} A \to \Gamma \vdash A$.

To complete this definition, a suitable notion of *finite model* needs to be made. A straightforward choice would be to define that a model is finite if the type of worlds is finite. But since the world-type of the canonical model does not just contain the formulas, but also proofs about them (e.g. a proof that the finite set of formulas is consistent), an additional axiom, namely proof irrelevance, is needed. To avoid, the additional axiom, we introduce the property of being essentially finite.

Definition 34. A model $\mathcal{M} = (\mathcal{W}, \mathcal{V}, \leq, \leq_{\mathsf{K}})$ with world type $\mathcal{W}$ is essentially finite, if there is a list of worlds L s.t.

$$\forall w \exists v \in L.\, w \leq v \land v \leq w.$$

Theorem 35. *The canonical model is essentially finite.*

[3] The notation $\mathcal{M} \Vdash \Gamma$ is a short-hand for $\forall A \in \Gamma.\, \mathcal{M} \Vdash A$.

[4] Or, classically equivalent, if any formula valid in some model also has a finite model.

Proof. We can compute a list containing all finite, prime, consistent, $\mathcal{U}$-theories, which is possible since all aforementioned properties are decidable. From these we obtain a list of worlds which satisfies the essential finiteness property. □

Corollary 36. *IEL has the finite model property.*

Proof. Analogous to Theorem 32, utilising Theorem 35. □

There are different versions of the finite model property in the literature. One commonly used version is that any non-theorem must have a finite countermodel:

$$\mathsf{FMP} := \forall A.\ \nvdash A \to \exists \mathcal{M}.\ \mathcal{M} \nVdash A \land \mathrm{fin}(\mathcal{M})$$

We can actually establish this result, too, as the canonical model can be employed as the countermodel.

6.4 Semantic Cut-Elimination

Su and Sanno [27] use a slightly different construction to prove completeness of the cut-free sequent calculus. We can adapt their argument to be constructive by using the decidability of the cut-free sequent calculus.

Theorem 37. (Completeness for GKIEL) *If $\Gamma \Vdash A$ then $\Gamma \Rightarrow A$.*

Proof. We construct a canonical model with finite saturated theories as worlds as in [27] and then we proceed as in Theorem 32. □

Theorem 38. (Semantic Cut-Elimination) *If $\Gamma \vdash A$ then $\Gamma \Rightarrow A$.*

Proof. By composing Lemma 8 and Theorem 37. □

Corollary 39. *If $\Gamma \Rightarrow A$ and $A, \Gamma \Rightarrow B$ then $\Gamma \Rightarrow B$.*

Proof. Since the two premises can be replayed in the natural deduction system, they trivially entail $\Gamma \vdash B$ and thus $\Gamma \Rightarrow B$ by Theorem 38. □

Since completeness is constructive, this procedure bears an executable algorithm. Note that the presented semantic cut-elimination proof does not rely on the syntactic cut-elimination proof given in Section 4; thus in principle, we could as well obtain all main results without it. However, we view both proofs of cut-elimination as valuable, especially since the syntactic one does not rely on completeness and is overall shorter.

7 Completeness for Infinite Theories

In this section, we analyse the connections between *strong completeness*, i.e. completeness for infinite theories as stated in Theorem 10 based on [1], and non-constructive axioms. This is similar to the analysis by Forster et al. [11] for first-order logic and relies on the stability of semantic inconsistencies:

Lemma 40. *If $\neg\neg\,(\mathcal{T} \Vdash \bot)$ then $\mathcal{T} \Vdash \bot$.*

Proof. Assume $\neg\neg\,(\mathcal{T} \Vdash \bot)$ and let w be a world in an arbitrary model $\mathcal{M}$, that forces $\mathcal{T}$. We need to show $\mathcal{M}, w \vDash \bot$ which is by definition $\bot$. Using Lemma 2 we can reason classically and thus strip the double negation off $\neg\neg\,(\mathcal{T} \Vdash \bot)$. Now we can obtain the proof of $\mathcal{M}, w \Vdash \bot$ from $\mathcal{T} \vDash \bot$ since $\mathcal{M}$ forces $\mathcal{T}$. □

7.1 Arbitrary Theories

Our first result is the equivalence between strong completeness for arbitrary theories and the law of excluded middle, adding the converse of Theorem 10.

Lemma 41. *Assuming strong completeness, derivation of falsity is stable, i.e. $\neg\neg\,(\mathcal{T} \vdash \bot)$ implies $\mathcal{T} \vdash \bot$ for arbitrary $\mathcal{T}$.*

Proof. Assume $\neg\neg\,(\mathcal{T} \vdash \bot)$. By soundness we have $\neg\neg(\mathcal{T} \vDash \bot)$, by Lemma 40 we thus have $\mathcal{T} \vDash \bot$. Using strong completeness concludes the proof. □

Theorem 42. *Strong completeness implies* LEM.

Proof. Assume strong completeness and let P be arbitrary. We have to show $P \vee \neg P$. Consider the theory $\mathcal{T} := \{A | P \vee \neg P\}$. Let us first show $\mathcal{T} \vdash \bot$. For this, we can use stability of deriving falsity (Lemma 40) and are left with proving $\neg\neg(\mathcal{T} \vdash \bot)$. Since our goal is negated, we can assume $P \vee \neg P$ by Lemma 2. Now we can show $\mathcal{T} \vdash \bot$ using the assumption rule.

Having established that $\mathcal{T} \vdash \bot$, by definition a list $\Gamma \subseteq \mathcal{T}$ exists s.t. $\Gamma \vdash \bot$. We either have $\Gamma = \emptyset$ or $\Gamma = A, \Gamma'$. In the first case we thus have a derivation $\vdash \bot$, we can derive a contradiction using consistency (Lemma 9)). In the second case we know that $A \in \mathcal{T}$ is proven, but this yields a proof of $P \vee \neg P$. □

7.2 Enumerable Theories

Even if we restrict strong completeness to enumerable theories, we can still derive MP. Here we will need the fact that the type of formulas is enumerable (Lemma 4), we will denote the n-th formula in this enumeration by A_n. We can first adapt Lemma 41 to strong enumerable completeness.

Lemma 43. *Assuming strong enumerable completeness, derivation of falsity is stable for any enumerable theory $\mathcal{T}$, i.e. $\neg\neg\,(\mathcal{T} \vdash \bot)$ implies $\mathcal{T} \vdash \bot$.*

Proof. The proof is analogous to the proof of Lemma 41. □

Theorem 44. *Strong enumerable completeness implies* MP.

Proof. To show MP, let $f : \mathbb{N} \to \mathbb{B}$ be a boolean function s.t. $\neg\neg\exists n.\, f\, n = \mathsf{tt}$. We construct the enumerable theory $\{A_n \wedge \neg A_n | f\, n = \mathsf{tt}\}$. It is easy to verify that this theory is enumerable. In constructive type theory, we can encode this theory as $\lambda(F : \mathcal{F}).\, \exists n\, fn = \mathsf{tt} \wedge F = (A_n \wedge \neg A_n)$.

Assume that $\mathcal{T} \vdash \bot$, we will establish this fact shortly. Now we have that a finite subset $\Gamma \subseteq \mathcal{T}$ derives $\bot$. As before, this subset cannot be empty since otherwise consistency would be violated. But then we can derive that there is an n s.t. $f\,n = \mathsf{tt}$.

To conclude the proof, we need to establish $\mathcal{T} \vdash \bot$. Since $\mathcal{T}$ is enumerable, we can use Lemma 43 and use $\neg\mathcal{T} \vdash \bot$ as an additional hypothesis and need to derive a contradiction. Therefore we can strip the double-negation and know that there is a j s.t. $f\,j = \mathsf{tt}$, thus $F_j \wedge \neg F_j \in \mathcal{T}$. We can now show $\mathcal{T} \vdash \bot$ using the implication elimination rule with F_j and $\neg F_j$. □

Thus, having observed Theorems 42 and 44, we can conclude that the approach to completeness of IEL pursued e.g. by Artemov and Protopopescu [1] inherently relies on a classical meta-theory. Also, let us remark that for these observations we only used a modest propositional fragment of IEL, therefore they generalise to strong completeness of many other logical formalisms.

8 Conclusion

8.1 Related Work

Of course the main reference for IEL is the paper introducing the logic by Artemov and Protopoescu [1]. Protopopescu [21] furthermore proves soundness and completeness of embeddings from IEL to S4. His dissertation [22] consists of two more papers on IEL, one investigating the connection between IEL and modal logics of verifications and one about fallible knowledge.

Proof theory of IEL has been studied by Krupski [18], Su and Sano [27,28], and more recently Fiorino [9]. Su and Sano propose a cut-free sequent calculus for IEL (and an extension of IEL with quantifiers). Their calculus for IEL uses sets of formulas with at most 1 element in the succedent of some rules, which will probably makes it less convenient to mechanise in a proof assistant. Fiorino proposes a sequent calculus for IEL with linear depth.

Tarau [29] develops a theorem prover for IEL using Prolog and presents embeddings from IEL into IPC (intuitionistic propositional calculus), however soundness or completeness proofs about the embeddings are not given. We tried to investigate those, however in our setting, we were unable to come up with a completeness proof.

There is a lot of existing work on mechanising decidability and cut-elimination in Coq and other proof assistants. For instance, Bentzen [2] mechanises a completeness proof for S5 in the Lean proof assistant, which uses classical logic. Doczkal and Smolka present axiom-free Coq mechanisations of completeness with respect to Kripke semantics and decidability of the forcing relation for K*, an extension of the classical modal logic K [7], as well as for various temporal logics (e.g. CTL) [8]. There are many mechanisations of cut-elimination proofs, many use G3K-style calculi and embed these using permutations in a proof assistant. Michaelis and Nipkow [19] establish (among other results, such as completeness) cut-elimination of IPC using Isabelle/HOL formalising the rules using multisets.

A somewhat similar approach (using permutations to express multisets) is also used by Chaudhuri and Lima [3]. Goré et al. [12] mechanise cut-elimination for the provability logic GL in multiset representation using Coq and discuss how their work benefits from using a proof assistant.

8.2 Future Work

There are several possible lines of future work. For one, it would be worthwhile to investigate whether, as the converse to Theorem 44, MP implies completeness for enumerable theories, or whether a stronger assumption is required. As indication for the latter, it seems not clear how MP would help with for instance establishing the Lindenbaum lemma constructively for infinite enumerable theories.

Secondly, it is certainly interesting to see if this general method for proving the finite model property and completeness in a constructive setting will also generalise to other modal logics. Here, we currently only have partial results: We verified that the cut-elimination and decidability proofs extend to the modal logic K (using an encoding based on a sequent calculus by Hakli and Negri [13]).

Lastly, our current decidability and cut-elimination proofs are not very efficient. Mechanising more efficient decidability procedures might be an interesting challenge (for example basing on Krupski's [18] decidability proof or Fiorino's [9] refutation calculus).

Acknowledgments. The authors would like to thank thank Yannick Forster, Marc Hermes, Jannik Kudla, Dominik Wehr and the anonymous reviewers for their helpful comments and suggestions on drafts of this paper.

Appendix 1 Natural Deduction System for IEL

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ \text{A} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \text{E}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \text{II} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \supset B}{\Gamma \vdash B}\ \text{IE}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \text{DIL} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \text{DIR} \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}\ \text{DE}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \text{CI} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \text{CEL} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \text{CER}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \mathsf{K}\, A}\ \text{KR} \qquad \frac{\Gamma \vdash \mathsf{K}\,(A \supset B)}{\Gamma \vdash \mathsf{K}\, A \supset \mathsf{K}\, B}\ \text{KD} \qquad \frac{\Gamma \vdash \mathsf{K}\, A}{\Gamma \vdash \neg\neg A}\ \text{KF}$$

Appendix 2 Coq Mechanisation

Component	Spec	Proof
preliminaries	121	93
natural deduction + lindenbaum	183	418
models	43	23
completeness	75	325
semantic cut-elimination	49	214
cut-elimination + decidability IEL	193	399
classical completeness / infinite theories	90	261
cut-elimination + decidability K	116	362
$\sum$	737	2194

Fig. 3. Overview of the mechanisation components

Our mechanisation compiles using Coq 8.13.2. It takes roughly 4 minutes to compile on a 2.6 GHz machine. An overview of the development with line counts can be found in Figure 3.

We use a *parametrised deduction system* to represent natural deduction (and the sequent calculus) for both IEL and IEL$^-$. That is, formally our deduction system has type $\vdash$: $\mathbb{F} \to \mathcal{L}(\mathcal{F}) \to \mathcal{F} \to \mathbb{P}$, where $\mathbb{F}$ is a two-element type class, which is responsible for flagging whether IEL$^-$ or IEL shall be used. This allows us to prove most results simultaneously for IEL and IEL$^-$ as the lemmas are parametrised in the flag of the deduction system.

2.1 The Classical Modal Logic K

For the classical modal logic K, we prove cut-elimination and decidability by using a similar strategy as we used for IEL. Hakli and Negri [13] propose a G3C-style calculus for K; as in the case of IEL, we instead adopt a mechanisation-friendly variant of a G3I-calculus and introduce a single modal rule. A similar system for classical propositional logic was presented by Dang [6]. For the full system, we refer the reader to the Coq mechanisation. Here, we only present the modal rule and compare it with the one used by Hakli and Negri. Hakli and Negri use the following rule:[5]

$$\frac{\Gamma \Rightarrow A}{\Box\Gamma, \Theta \Rightarrow \Delta, \Box A}$$

In a similar spirit, as our modal rule, for IEL, we adopt the following rule for our system:

[5] In the following rules, we use a box instead of K as the modal operator, as this is standard for the classical modal logic K.

$$\frac{\Box A \in \Delta \qquad \Gamma_{\Box} \Rightarrow A}{\Gamma \Rightarrow \Delta}$$

This is easier to formalise as we use membership prominently and no longer split-up a context. The proofs for decidability and cut-elimination are similar as for IEL, we use the same induction on pairs of cut-rank and size of the cut-formula for the proof of cut-elimination. However the proofs are slightly more compact (due to more symmetric rules in the system).

2.2 Height-Encoding

To better illustrate the height-encoding, we consider how the right rule for conjunction is encoded.

$$\frac{\Gamma \overset{h}{\Rightarrow} A \qquad \Gamma \overset{h}{\Rightarrow} B}{\Gamma \overset{h+1}{\Rightarrow} A \wedge B} \qquad \frac{\Gamma \overset{h}{\Rightarrow} A}{\Gamma \overset{h+1}{\Rightarrow} A}$$

On the left side, we see how the conjunction rule is encoded, while on the right side, the step rule is given, which allows us to boost the height of any derivation.

One alternative would be to use a height-encoding using maximum on both sides, e.g.:

$$\frac{\Gamma \overset{h_1}{\Rightarrow} A \qquad \Gamma \overset{h_2}{\Rightarrow} B}{\Gamma \overset{\max(h_1,h_2)+1}{\Rightarrow} A \wedge B}$$

The encoding we used leads to easier proofs and inductions (since less arithmetical reasoning about maximum or minimum is needed).

Appendix 3 Cut-Elimination: Selected Cases

We shall showcase some cases of our cut-elimination proof.

Theorem 45. (Cut is admissible) *The cut rule is admissible.*

$$\frac{\begin{array}{c}[\delta_1] \\ \Gamma \overset{h_1}{\Rightarrow} B\end{array} \qquad \begin{array}{c}[\delta_2] \\ \Gamma, B \overset{h_2}{\Rightarrow} A\end{array}}{\Gamma \Rightarrow A}\ Cut$$

Proof. The proof is by induction on pairs (s, r) of formula-size s and cut-rank r. Here formula size is the size of the cut-formula B, and the cut-rank is the sum of the heights i.e. $r := h_1 + h_2$.

The induction principle gives us two inductive hypotheses, one which allows us to eliminate cuts of arbitrary height but with a cut formula of smaller size (s-cut) and another one, allowing us to eliminate cuts on formulas of the same size but with a smaller cut-rank (r-cut).

We now analyse which rule was used to derive δ_1. In two cases, namely the K introduction and right implication introduction rule we will need an additional case analysis (i.e. inversion) on δ_2.

AL-Rule: Assume δ_1 was derived using the left-rule for conjunction. Our derivation has the following form.

$$\dfrac{\dfrac{C_1 \wedge C_2 \in \Gamma \qquad \Gamma, C_1, C_2 \overset{h_1-1}{\Rightarrow} F}{\Gamma \overset{h_1}{\Rightarrow} B} \qquad \Gamma, B \overset{h_2}{\Rightarrow} A}{\Gamma \Rightarrow A}\ \text{r-cut}$$

We can permute the application of the left rule for conjunction downwards and use weakening on the derivation $C_1, C_2, \Gamma \overset{m}{\Rightarrow} \Delta$:

$$\dfrac{C_1 \wedge C_2 \in \Gamma \qquad \dfrac{\Gamma, C_1, C_2 \overset{n-1}{\Rightarrow} B \qquad B, \Gamma \overset{m}{\Rightarrow} A}{\Gamma, C_1, C_2 \Rightarrow A}}{\Gamma \Rightarrow A}$$

Note that the new cut is a cut on the same formula but of a smaller rank, thus we can eliminate it by the inductive hypothesis.

IR-Rule: Assume last rule used in the derivation of δ_1 was the right introduction rule for implication. Thus we know, that $B = B_1 \supset B_2$. We need to do a second case analysis on the derivation δ_2.

1. If δ_2 is an axiom, either $p_i = B$ or $p_i \in \Gamma$ and we know that $A = p_i$. The first case contradicts our assumption that $B = B_1 \supset B_2$ and in the second case we can directly use the variable rule.
2. Similarly, if the second premiss is derived using the falsity rule, either $F = \bot$ or $\bot \in \Gamma$.
3. An interesting case arises when the right premiss is proved using the left introduction rule for implication.

$$\dfrac{\dfrac{B_0, \Gamma \overset{h_1-1}{\Rightarrow} B_1}{\Gamma \overset{h_1}{\Rightarrow} B_0 \supset B_1} \qquad \dfrac{C_0 \supset C_1 \in \Gamma, B \qquad \Gamma, B \overset{h_2-1}{\Rightarrow} C_0 \qquad \Gamma, C_1, B \Rightarrow A}{\Gamma, B_0 \supset B_1 \overset{h_2}{\Rightarrow} A}}{\Gamma \Rightarrow A}$$

We have two cases: either $B = C_0 \supset C_1$ or $C_0 \supset C_1 \in \Gamma$.

(a) In the first case, we can build the following derivation:

$$\dfrac{\dfrac{\dfrac{\Gamma \overset{h_1}{\Rightarrow} B \qquad B, \Gamma \overset{h_2-1}{\Rightarrow} B_0}{\Gamma \Rightarrow B_0}\ \text{r-cut} \qquad \Gamma, B_0 \Rightarrow B_1}{\Gamma \Rightarrow B_1} \qquad \dfrac{B_1 \in B_1, \Gamma \qquad \Gamma, B_1, B \Rightarrow A}{\Gamma, B_1 \Rightarrow A}\ \text{IL-inv}}{\Gamma \Rightarrow A}$$

(b) In the second case, we can apply the left rule for implication first and do two cuts afterwards.

$$\dfrac{C_0 \supset C_1 \in \mathit{\Gamma} \qquad \dfrac{\mathit{\Gamma} \overset{h_1}{\Rightarrow} B \qquad \mathit{\Gamma}, B \overset{h_2-1}{\Rightarrow} C_0}{\mathit{\Gamma} \Rightarrow C_0}\,\text{r-cut} \qquad \dfrac{\dfrac{\mathit{\Gamma} \overset{h_1}{\Rightarrow} B}{\mathit{\Gamma}, C_1 \overset{h_1}{\Rightarrow} B}\,\text{weak.} \qquad \mathit{\Gamma}, B, C_1 \overset{h_2-1}{\Rightarrow} C_0}{\mathit{\Gamma}, C_1 \Rightarrow A}\,\text{r-cut}}{\mathit{\Gamma} \Rightarrow A}\,\text{IL}$$

KI-Rule: Assume the premiss was derived using the K-introduction rule. We need to make a second case distinction on the derivation of the right deduction. Most cases are similar to those obtained in the right rule for implication subcases, and we will not go into too much detail here.

$$\dfrac{\dfrac{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}} \Rightarrow B_0}{\mathit{\Gamma} \Rightarrow \mathsf{K}\, B_0} \qquad \mathit{\Gamma}, \mathsf{K}\, B_0 \Rightarrow A}{\mathit{\Gamma} \Rightarrow A}$$

1. The right premise is an axiom. Either $p_i = \mathsf{K}\, B_0$ which is impossible (since the constructors of an inductive datatype are disjoint) or $A \in \mathit{\Gamma}$ in which case we can directly construct the derivation.
2. The most interesting case occurs when the KI-rule is used on both sides. We have the following derivation:

$$\dfrac{\dfrac{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}} \overset{h_1-1}{\Rightarrow} B_0}{\mathit{\Gamma} \overset{h_1}{\Rightarrow} \mathsf{K}\, B_0} \qquad \dfrac{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}}, \mathsf{K}\, B_0, B_0 \overset{h_2-1}{\Rightarrow} A_0}{\mathit{\Gamma}, \mathsf{K}\, B_0 \overset{h_2}{\Rightarrow} \mathsf{K}\, A_0}}{\mathit{\Gamma} \Rightarrow \mathsf{K}\, A_0}$$

We can build the following derivation:

$$\dfrac{\dfrac{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}} \Rightarrow B_0 \qquad \dfrac{\dfrac{\mathit{\Gamma} \overset{h_1}{\Rightarrow} \mathsf{K}\, B_0}{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}} \overset{h_1}{\Rightarrow} \mathsf{K}\, B_0}\,\text{weak.} \qquad \mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}}, \mathsf{K}\, B_0, B_0 \overset{h_2-1}{\Rightarrow} A_0}{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}}, B_0 \Rightarrow A_0}\,\text{r-cut}}{\mathit{\Gamma} \cup \mathit{\Gamma}_{\mathsf{K}} \Rightarrow A_0}\,\text{s-cut}}{\mathit{\Gamma} \Rightarrow \mathsf{K}\, A_0}\,\text{KI}$$

References

1. Artemov, S., Protopopescu, T.: Intuitionistic epistemic logic. Review of Symbolic Logic **9**(2), 266–298 (2016). https://doi.org/10.1017/S1755020315000374
2. Bentzen, B.: A henkin-style completeness proof for the modal logic s5. In: Baroni, P., Benzmüller, C., Wáng, Y.N. (eds.) Logic and Argumentation. pp. 459–467. Springer International Publishing, Cham (2021). https://doi.org/https://doi.org/10.1007/978-3-030-89391-0_25
3. Chaudhuri, K., Lima, L., Reis, G.: Formalized Meta-Theory of Sequent Calculi for Substructural Logics. Electronic Notes in Theoretical Computer Science **332**, 57–73 (2017). https://doi.org/10.1016/j.entcs.2017.04.005, `http://dx.doi.org/10.1016/j.entcs.2017.04.005`

4. Coquand, T., Huet, G.: The calculus of constructions. Information and Computation **76**(2), 95–120 (1988). https://doi.org/https://doi.org/10.1016/0890-5401(88)90005-3, https://www.sciencedirect.com/science/article/pii/0890540188900053
5. Coquand, T., Mannaa, B.: The independence of markov's principle in type theory. arXiv preprint arXiv:1602.04530 (2016)
6. Dang, H.: Systems for Propositional Logics. Tech. rep., Saarland University (2015), https://www.ps.uni-saarland.de/{~}dang/ri-lab/propsystems/systems.pdf
7. Doczkal, C., Smolka, G.: Constructive completeness for modal logic with transitive closure. In: Hawblitzel, C., Miller, D. (eds.) Certified Programs and Proofs. pp. 224–239. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
8. Doczkal, C., Smolka, G.: Completeness and Decidability Results for CTL in Constructive Type Theory. Journal of Automated Reasoning (2016). https://doi.org/10.1007/s10817-016-9361-9
9. Fiorino, G.: Linear depth deduction with subformula property for intuitionistic epistemic logic (2021)
10. Forster, Y., Kirst, D., Smolka, G.: On synthetic undecidability in Coq, with an application to the Entscheidungsproblem. In: CPP 2019 - Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs, Co-located with POPL 2019 (2019). https://doi.org/10.1145/3293880.3294091
11. Forster, Y., Kirst, D., Wehr, D.: Completeness theorems for first-order logic analysed in constructive type theory. Journal of Logic and Computation (2021). https://doi.org/10.1093/logcom/exaa073
12. Goré, R., Ramanayake, R., Shillito, I.: Cut-elimination for provability logic by terminating proof-search: Formalised and deconstructed using coq. In: Das, A., Negri, S. (eds.) Automated Reasoning with Analytic Tableaux and Related Methods. pp. 299–313. Springer International Publishing, Cham (2021)
13. Hakli, R., Negri, S.: Does the deduction theorem fail for modal logic? Synthese (2012). https://doi.org/10.1007/s11229-011-9905-9
14. Hintikka, J.: Knowledge and belief: An introduction to the logic of the two notions. Studia Logica **16** (1962)
15. Ishihara, H.: Constructive reverse mathematics: compactness properties. From Sets and Types to Topology and Analysis. Oxford Logic Guides **48**, 245–267 (2005). https://doi.org/http://www.doi.org/10.1093/acprof:oso/9780198566519.001.0001
16. Ishihara, H.: Reverse mathematics in bishop's constructive mathematics. Philosophia Scientiæ. Travaux d'histoire et de philosophie des sciences (CS 6), 43–59 (2006). https://doi.org/http://dx.doi.org/10.4000/philosophiascientiae.406
17. Kleene, S.C.: Introduction to Metamathematics, vol. 19. North Holland (1952)
18. Krupski, V.N.: Cut elimination and complexity bounds for intuitionistic epistemic logic. Journal of Logic and Computation **30**(1), 281–294 (02 2020). https://doi.org/10.1093/logcom/exaa012, https://doi.org/10.1093/logcom/exaa012
19. Michaelis, J., Nipkow, T.: Formalized Proof Systems for Propositional Logic. In: Abel, A., Forsberg, F.N., Kaposi, A. (eds.) 23rd International Conference on Types for Proofs and Programs (TYPES 2017). Leibniz International Proceedings in Informatics (LIPIcs), vol. 104, pp. 5:1–5:16. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany (2018). https://doi.org/10.4230/LIPIcs.TYPES.2017.5, http://drops.dagstuhl.de/opus/volltexte/2018/10053

20. Paulin-Mohring, C.: Inductive definitions in the system Coq rules and properties BT - Typed Lambda Calculi and Applications. pp. 328–345. Springer Berlin Heidelberg, Berlin, Heidelberg (1993)
21. Protopopescu, T.: An arithmetical interpretation of verification and intuitionistic knowledge. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **9537**, 317–330 (2016). https://doi.org/10.1007/978-3-319-27683-0_22
22. Protopopescu, T.: Three Essays in Intuitionistic Epistemology. Ph.D. thesis, CUNY (2016), ttps://academicworks.cuny.edu/gc{_}etds/1391
23. Rescher, N.: Epistemic Logic: A Survey of the Logic of Knowledge. University of Pittsburgh Press (2005)
24. Richman, F.: Constructive Mathematics without Choice, pp. 199–205. Springer Netherlands, Dordrecht (2001). https://doi.org/10.1007/978-94-015-9757-9_17, https://doi.org/10.1007/978-94-015-9757-9_17
25. Rogozin, D.: Categorical and algebraic aspects of the intuitionistic modal logic IEL— and its predicate extensions. Journal of Logic and Computation **31**(1), 347–374 (jan 2021). https://doi.org/10.1093/logcom/exaa082, https://academic.oup.com/logcom/article/31/1/347/6049830
26. Smolka, G., Brown, C.E.: Introduction to Computational Logic (2012), http://www.ps.uni-saarland.de/courses/cl-ss12/script/icl.pdf
27. Su, Y., Sano, K.: Cut-free and Analytic Sequent Calculus of Intuitionistic Epistemic Logic. In: Sedlár, I., Blicha, M. (eds.) The Logica Yearbook 2019, pp. 179–193. College Publications (2019)
28. Su, Y., Sano, K.: First-Order Intuitionistic Epistemic Logic. In: Blackburn, P., Lorini, E., Guo, M. (eds.) Logic, Rationality, and Interaction. pp. 326–339. Springer Berlin Heidelberg, Berlin, Heidelberg (2019). https://doi.org/https://doi.org/10.1007/978-3-662-60292-8_24
29. Tarau, P.: Modality Definition Synthesis for Epistemic Intuitionistic Logic via a Theorem Prover (2019)
30. The Coq Development Team: The Coq proof assistant (Jan 2021). https://doi.org/10.5281/zenodo.4501022, https://doi.org/10.5281/zenodo.4501022
31. Troelstra, A.S., Schwichtenberg, H.: Basic Proof Theory (2000). https://doi.org/10.1017/cbo9781139168717
32. Wolter, F., Zakharyaschev, M.: Intuitionistic modal logics as fragments of classical bimodal logics. Logic at Work (1999)
33. Wolter, F., Zakharyaschev, M.: Intuitionistic Modal Logic, pp. 227–238. Springer Netherlands, Dordrecht (1999). https://doi.org/10.1007/978-94-017-2109-7_17, https://doi.org/10.1007/978-94-017-2109-7_17