Constructive and Mechanised Meta-Theory of Intuitionistic Epistemic Logic

Christian Hagemeier and Dominik Kirst

LFCS'22
January 12th

SAARLAND UNIVERSITY
COMPUTER SCIENCE
SIC Saarland Informatics Campus

Intuitionistic Epistemic Logic (IEL)

Classical epistemic logic (Hintikka, 1962)

- Extend classical logic with modality K
- Add axioms for K capturing understanding of belief/knowledge
- Reflection principle $\mathsf{K}\,A \to A$: "Known propositions are true"

Intuitionistic Epistemic Logic (IEL)

Classical epistemic logic (Hintikka, 1962)

- Extend classical logic with modality K
- Add axioms for K capturing understanding of belief/knowledge
- Reflection principle $\mathsf{K}\,A \to A$: "Known propositions are true"

Intuitionistic epistemic logics (Artemov and Protopopescu, 2016)

- Understand truth as intuitionistic provability (BHK-interpretation)
- Co-reflection principle $A \to \mathsf{K}\,A$: "From proofs we gain knowledge by verification"
- Intuitionistic reflection $\mathsf{K}\,A \to \neg\neg A$: "Known propositions are potentially true"

$$\mathsf{IEL}^- := \mathsf{IPC} + \text{co-reflection} \qquad \mathsf{IEL} := \mathsf{IEL}^- + \text{int. reflection}$$

Meta-Theory of IEL

Artemov and Protopopescu (2016)

- Soundness and completeness with respect to suitable Kripke semantics
- Derived results: disjunction property, admissibility of reflection, etc.

Meta-Theory of IEL

Artemov and Protopopescu (2016)

- Soundness and completeness with respect to suitable Kripke semantics
- Derived results: disjunction property, admissibility of reflection, etc.

Su and Sano (2019)

Finite model property and semantic cut-elimination

Meta-Theory of IEL

Artemov and Protopopescu (2016)

- Soundness and completeness with respect to suitable Kripke semantics
- Derived results: disjunction property, admissibility of reflection, etc.

Su and Sano (2019)

Finite model property and semantic cut-elimination

Krupski (2020)

Syntactic cut-elimination and decidability

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction. Since we have $\neg\neg P$, on deriving a contradiction we may assume P.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction. Since we have $\neg\neg P$, on deriving a contradiction we may assume P. But then $\mathcal{M} \Vdash \bot$, contradiction. □

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction. Since we have $\neg\neg P$, on deriving a contradiction we may assume P. But then $\mathcal{M} \Vdash \bot$, contradiction. □

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for enumerable $\mathcal{T}$, then Markov's principle holds.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction. Since we have $\neg\neg P$, on deriving a contradiction we may assume P. But then $\mathcal{M} \Vdash \bot$, contradiction. □

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for enumerable $\mathcal{T}$, then Markov's principle holds.

Proof.

Let $f : \mathbb{N} \to \mathbb{B}$ with $\neg\neg(\exists n.\, f\, n = \text{true})$ be given.

Classical Meta-Theory of IEL

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for arbitrary $\mathcal{T}$, then double negation elimination holds.

Proof.

Given some proposition P and assuming $\neg\neg P$, consider $\mathcal{T} := \{A \in \mathcal{F} \mid P\}$. It is enough to show $\mathcal{T} \vdash \bot$, since then $\mathcal{T}$ must be non-empty and thus P holds. Apply completeness and show $\mathcal{T} \Vdash \bot$, so assume a model $\mathcal{M} \Vdash \mathcal{T}$ and derive a contradiction. Since we have $\neg\neg P$, on deriving a contradiction we may assume P. But then $\mathcal{M} \Vdash \bot$, contradiction. □

Fact

If $\mathcal{T} \Vdash A$ implies $\mathcal{T} \vdash A$ for enumerable $\mathcal{T}$, then Markov's principle holds.

Proof.

Let $f : \mathbb{N} \to \mathbb{B}$ with $\neg\neg(\exists n.\, f\ n = \text{true})$ be given. Using the enumerable set $\mathcal{T} := \{A_n \wedge \neg A_n \mid f\ n = \text{true}\}$ derive $\exists n.\, f\ n = \text{true}$ with an argument as above. □

Constructive Meta-Theory of IEL

Can IEL be meaningfully described in a constructive system?

Constructive Meta-Theory of IEL

Can IEL be meaningfully described in a constructive system?

Work in the constructive type theory CIC (Coquand and Huet, 1988; Paulin-Mohring, 1993):

- Expressive system implementing higher-order intuitionistic logic
- Clean analysis without obscuring choice principles (Richman, 2001; Forster, 2022)
- Obtain (variants of) main results without appeal to additional axioms

Constructive Meta-Theory of IEL

Can IEL be meaningfully described in a constructive system?

Work in the constructive type theory CIC (Coquand and Huet, 1988; Paulin-Mohring, 1993):

- Expressive system implementing higher-order intuitionistic logic
- Clean analysis without obscuring choice principles (Richman, 2001; Forster, 2022)
- Obtain (variants of) main results without appeal to additional axioms

Fact (CIC models IEL)

The truncation operation $||X||$ squashing a computational type X of CIC into the propositional universe $\mathbb{P}$ satisfies co-reflection $X \to ||X||$ and intuitionistic reflection $||X|| \to \neg\neg X$.

Mechanised Meta-Theory of IEL[1]

Can IEL be feasibly mechanised in a proof assistant?

[1] https://www.ps.uni-saarland.de/extras/iel/

Mechanised Meta-Theory of IEL[1]

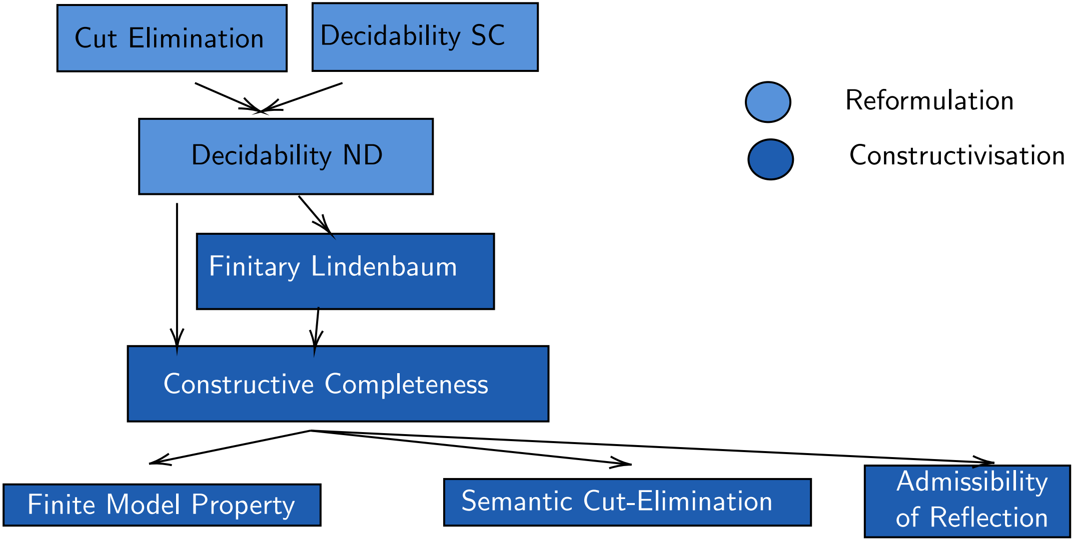
Can IEL be feasibly mechanised in a proof assistant?

Work with the Coq proof assistant:

- Implements CIC, used as tool to verify our proofs and track assumptions
- Executable algorithms via constructive completeness, cut-elimination, and decidability
- Synthetic computability as a shortcut (Richman, 1983; Bauer, 2006; Forster et al., 2019)
- Development systematically hyperlinked with the paper

[1] `https://www.ps.uni-saarland.de/extras/iel/`

Results Overview



Deduction Systems for IEL

Model deduction systems as inductive predicates of type $\mathcal{L}(\mathcal{F}) \to \mathcal{F} \to \mathbb{P}$.

Natural Deduction (ND)
Extends natural deduction for IPC by 3 rules (co-reflection, distribution and int. reflection)

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

$$\frac{\Gamma \vdash \mathsf{K}\, A}{\Gamma \vdash \neg\neg A}\ (KF)$$

Sequent Calculus (SC)
Extend G3I by 2 rules (Krupski, 2020); we use GKI as base (better for mechanisation)

$$\frac{\Gamma \cup \{A \mid \mathsf{K}\, A \in \Gamma\} \Rightarrow B}{\Gamma \Rightarrow \mathsf{K}\, B}\ (\mathsf{KI})$$

$$\frac{\Gamma \Rightarrow \mathsf{K}\,\bot}{\Gamma \Rightarrow A}\ (\mathsf{KF})$$

In contrast to ND, SC is analytic, i.e. (almost) has the subformula property.

Cut-Elimination

Theorem (Cut-Elimination)

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

Proof.

Typical double induction on rank and size of a cut (cf. Troelstra/Schwichtenberg(2000)). □

Corollary (Agreement)

$\Gamma \vdash A$ *if and only if* $\Gamma \Rightarrow A$.

Proof.

Both directions are proven by induction on the given derivations; only direction from ND to SC needs Cut-Elimination. □

Decidability

Lemma

One can construct a function $f : \mathcal{F} \to \mathbb{B}$ *such that* $f\ A = \text{true}$ *if and only if* $\Rightarrow A$.

- Synthetic notion of decidability (no Turing-machines; f computable by construction)
- Utilise subformula property of sequent calculus for IEL
- Compute derivable sequents as a fixed point of stepwise derivation

Decidability

Lemma

One can construct a function $f : \mathcal{F} \to \mathbb{B}$ such that $f\ A = \mathrm{true}$ if and only if $\Rightarrow A$.

- Synthetic notion of decidability (no Turing-machines; f computable by construction)
- Utilise subformula property of sequent calculus for IEL
- Compute derivable sequents as a fixed point of stepwise derivation

Theorem (Decidability)

SC and ND are decidable.

Proof.

By the previous lemma and the agreement of ND and SC. □

Lindenbaum Construction

Let $\mathcal{U}$ be finite and subformula-closed.

Definition (Primeness)

A set of formulas Γ is $\mathcal{U}$-prime $A \vee B \in \Gamma$ implies that $A \in \Gamma$ or $B \in \Gamma$ for all $A, B \in \mathcal{U}$.

Lemma

For any context $\Gamma \subseteq \mathcal{U}$ and formula $A_\bot$, we can compute Δ extending Γ which is $\mathcal{U}$-prime, closed under derivability in $\mathcal{U}$, and preserves non-derivability of $A_\bot$.

Proof.

Iterate through the formulas A_i of $\mathcal{U}$ to obtain contexts Γ_i. In step i, add A_i, if non-derivability of $A_\bot$ is preserved by the addition (using decidability):

$$\Gamma_{i+1} := \begin{cases} \Gamma_i, A_i & \text{if } \Gamma_i, A_i \nvdash A_\bot \\ \Gamma_i & \text{otherwise} \end{cases}$$

□

Decidable Universal Model

Given $\mathcal{U}$, build a canonical Kripke model $\mathcal{M}_\mathcal{U} = (\mathcal{W}_\mathcal{U}, \mathcal{V}_\mathcal{U}, \leq, \leq_\mathsf{K})$:

- $\mathcal{W}_\mathcal{U}$ contains $\mathcal{U}$-prime, consistent $\mathcal{U}$-theories as worlds
- $\mathcal{V}_\mathcal{U}(\Gamma, i) := p_i \in \Gamma$
- $\Gamma \leq \Delta := \Gamma \subseteq \Delta$
- $\Gamma \leq_\mathsf{K} \Delta := \Gamma \cup \{A \mid \mathsf{K}\, A \in \Gamma\} \subseteq \Delta$ (same as in Su and Sano (2019b))

Lemma (Truth Lemma)

For $A \in \mathcal{U}$ and $\Gamma \in \mathcal{W}_\mathcal{U}$, we have $A \in \Gamma \iff \Gamma \Vdash A$.

Proof.

Induction on A. Using decidability of membership and the Lindenbaum Lemma. □

Decidable Universal Model

Given $\mathcal{U}$, build a canonical Kripke model $\mathcal{M}_\mathcal{U} = (\mathcal{W}_\mathcal{U}, \mathcal{V}_\mathcal{U}, \leq, \leq_\mathsf{K})$:

- $\mathcal{W}_\mathcal{U}$ contains $\mathcal{U}$-prime, consistent $\mathcal{U}$-theories as worlds
- $\mathcal{V}_\mathcal{U}(\Gamma, i) := p_i \in \Gamma$
- $\Gamma \leq \Delta := \Gamma \subseteq \Delta$
- $\Gamma \leq_\mathsf{K} \Delta := \Gamma \cup \{A \mid \mathsf{K}\, A \in \Gamma\} \subseteq \Delta$ (same as in Su and Sano (2019b))

Lemma (Truth Lemma)

For $A \in \mathcal{U}$ and $\Gamma \in \mathcal{W}_\mathcal{U}$, we have $A \in \Gamma \iff \Gamma \Vdash A$.

Theorem (Finitary Completeness)

If $\Vdash A$ then $\vdash A$, or equivalently, if $\Gamma \Vdash A$ then $\Gamma \vdash A$ for finite Γ.

Proof.

Assume $\Vdash A$ and $\nvdash A$ (by decidability of $\vdash$). Using the Lindenbaum Lemma there is a world Γ in the canonical model over the subformula universe of A s.t. $A \notin \Gamma$. Contradiction to $\Vdash A$. $\square$

Finite Model Property

Definition (FMP)

IEL has FMP, if $\vdash A$ whenever $\mathcal{M} \Vdash A$ for all (essentially) finite $\mathcal{M}$.

Theorem

IEL has the finite model property.

Proof.

Given the bound against $\mathcal{U}$, the canonical model is (essentially) finite. □

Semantic Cut-Elimination[2]

Lemma (Completeness SC)

If $\Gamma \Vdash A$ *then* $\Gamma \Rightarrow A$.

Proof.

Canonical model construction with respect to SC using saturated theories. □

Theorem (SCE)

If $\Gamma \vdash A$ *then* $\Gamma \Rightarrow A$.

Proof.

By composition of Soundness and Completeness. □

[2] Following Su and Sano (2019a)

Coq Mechanisation[3]

- Roughly 3k lines of code, structured in accordance with the paper
- Uses helpful features of Coq: e.g. can prove most results simultaneously for IEL and IEL^- using a type class flag
- Method for mechanising syntactic results (i.e. decidability and cut-elimination) generalises to other logics, we instantiated to classical modal logic K

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

Figure: Overview of the mechanisation components

[3] https://www.ps.uni-saarland.de/extras/iel/

Conclusion

- Background: IEL is a convincing rendering of knowledge in intuitionistic framework
- Contribution: IEL has a well-behaved meta-theory in intuitionistic framework
- Method: Proof assistant helps ensuring correctness and exhibits algorithms
- Future Work: Investigate if similar method applies to other logics (i.e. GL)

Conclusion

- Background: IEL is a convincing rendering of knowledge in intuitionistic framework
- Contribution: IEL has a well-behaved meta-theory in intuitionistic framework
- Method: Proof assistant helps ensuring correctness and exhibits algorithms
- Future Work: Investigate if similar method applies to other logics (i.e. GL)

Thank You!

Bibliography I

Artemov, S. and Protopopescu, T. (2016). Intuitionistic epistemic logic. *Review of Symbolic Logic*, 9(2):266–298.

Bauer, A. (2006). First steps in synthetic computability theory. *Electronic Notes in Theoretical Computer Science*, 155:5–31.

Coquand, T. and Huet, G. (1988). The calculus of constructions. *Information and Computation*, 76(2):95–120.

Forster, Y. (2022). Parametric church's thesis: Synthetic computability without choice. In *International Symposium on Logical Foundations of Computer Science*, pages 70–89. Springer.

Forster, Y., Kirst, D., and Smolka, G. (2019). 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*.

Hintikka, J. (1962). Knowledge and belief: An introduction to the logic of the two notions. *Studia Logica*, 16.

Krupski, V. N. (2020). Cut elimination and complexity bounds for intuitionistic epistemic logic. *Journal of Logic and Computation*, 30(1):281–294.

Paulin-Mohring, C. (1993). Inductive definitions in the system Coq rules and properties BT - Typed Lambda Calculi and Applications. pages 328–345, Berlin, Heidelberg. Springer Berlin Heidelberg.

Richman, F. (1983). Church's thesis without tears. *The Journal of symbolic logic*, 48(3):797–803.

Bibliography II

Richman, F. (2001). *Constructive Mathematics without Choice*, pages 199–205. Springer Netherlands, Dordrecht.

Su, Y. and Sano, K. (2019a). Cut-free and Analytic Sequent Calculus of Intuitionistic Epistemic Logic. In Sedlár, I. and Blicha, M., editors, *The Logica Yearbook 2019*, pages 179–193. College Publications.

Su, Y. and Sano, K. (2019b). First-Order Intuitionistic Epistemic Logic. In Blackburn, P., Lorini, E., and Guo, M., editors, *Logic, Rationality, and Interaction*, pages 326–339, Berlin, Heidelberg. Springer Berlin Heidelberg.

Troelstra, A. S. and Schwichtenberg, H. (2000). *Basic Proof Theory*.

Cut Elimination

Decidability

SC

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

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

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

ND

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

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

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \mathrm{DIL} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \mathrm{DIR} \quad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}\ \mathrm{DE} \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \mathrm{CI}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \mathrm{CEL} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \mathrm{CER}$$

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