On provability logic of Heyting Arithmetic

Mojtaba Mojtahedi (Ghent University)

October 19, 2023

Sections

Modal Logic

- Modal logic, extends the language of logic with a unary operator $\Box$.
- Intuitively, $\Box A$ means *necessarily* A.
- Its dual operator, $\Diamond$, usually defined as $\Diamond A := \neg\Box\neg A$.
- $\Diamond A$ means *possibly* A.
- Expressibility increased.
- Used for various purposes in various disciplines.
- Necessity, Knowledge, Obligation, Belief, Provability.

Provability Logic

- $\Box$ as provability.

Provability Logic

- $\Box$ as provability.
- Gödel 1933: Based on BHK, interpreted IL in $\mathsf{S4}$.

Provability Logic

- $\Box$ as provability.
- Gödel 1933: Based on BHK, interpreted IL in $\mathsf{S4}$.
- IL is Heyting's formalization of a logic based on BHK interpretation.
- Simply, IL is CL without PEM $(A \vee \neg A)$.
- BHK:
  - A proof of $A \vee B$ is a pair $\langle i, x\rangle$, either $i = 0$ and x is a proof of A or $i \neq 0$ and x is a proof of B.
  - A proof of $A \to B$ is a function which returns a proof of B, given a proof of A.

Why it is interesting?

From a philosophical point of view, provability logic is interesting because:

- The concept of provability in a fixed theory of arithmetic has a unique and non-problematic meaning, other than concepts like necessity and knowledge studied in modal and epistemic logic. Quine was a proponent of syntactical approach to the modal logic.
- Provability logic provides tools to study the notion of self-reference.
- The ideal balance between *simplicity* and *expressiveness*.

Provability Logic: more precise

$\mathsf{PL}(T)$:=Provability logic of $T := \{A \in \mathcal{L}_\Box : \forall\sigma\ T \vdash \sigma_{_T} A\}$

Provability Logic: more precise

$\mathsf{PL}(T)$:=Provability logic of $T := \{A \in \mathcal{L}_\Box : \forall\sigma\ T \vdash \sigma_T A\}$

- $\sigma_T(p) := \sigma(p)$ for atomics.
- σ_T commutes with boolean connectives.
- $\sigma_T(\Box A) := \mathsf{Pr}_T(\ulcorner \sigma_T A \urcorner)$.

Gödel's Incompleteness Theorem

A consistent theory is incapable of proving its own consistency

Gödel's Incompleteness Theorem

A consistent theory is incapable of proving its own consistency

If T is consistent then it can not prove its own consistency

Gödel's Incompleteness Theorem

A consistent theory is incapable of proving its own consistency

If T is consistent then it can not prove its own consistency

$$\neg\Box\bot \to \neg\Box(\neg\Box\bot) \in \mathsf{PL}(T)$$

Gödel's Incompleteness Theorem

A consistent theory is incapable of proving its own consistency

If T is consistent then it can not prove its own consistency

$$\neg\Box\bot \to \neg\Box(\neg\Box\bot) \in \mathsf{PL}(T)$$

$$\Box(\neg\Box\bot) \to \Box\bot$$

Gödel's Incompleteness Theorem

A consistent theory is incapable of proving its own consistency

If T is consistent then it can not prove its own consistency

$$\neg\Box\bot \to \neg\Box(\neg\Box\bot) \in \mathsf{PL}(T)$$

$$\Box(\neg\Box\bot) \to \Box\bot$$

$$\Box(\Box\bot \to \bot) \to \Box\bot \quad \text{(Löb's Axiom)}$$

Solovay 1976

The Provability logic of PA is GL

- All theorems of classical propositional logic.
- K $:= \Box(A \to B) \to (\Box A \to \Box B)$.
- Löb $:= \Box(\Box A \to A) \to \Box A$. Implies $\Box A \to \Box\Box A$.
- modus ponens: $A, A \to B / B$.
- Necessitation: $A / \Box A$.

Kripke semantics GL

GL is sound and complete for

finite transitive irreflexive Kripke models.

$$\mathcal{K} := (W, \sqsubset, \models)$$

$$\mathcal{K}, w \models \Box A \quad \Leftrightarrow \quad \forall u \sqsupset w \, \mathcal{K}, u \models A$$

Σ_1-substitutions

$$\mathsf{PL}_{\Sigma}(T) := \Sigma_1\text{-Provability logic of } T := \{A \in \mathcal{L}_\Box : \forall \sigma \in \Sigma_1 \; T \vdash \sigma_T A\}$$

Theorem (Visser)

$\mathsf{PL}_{\Sigma}(\mathsf{PA}) = \mathsf{GLC_a} := \mathsf{GL} + p \to \Box p$ *for atomic* p*'s.*

Reduction of provability logics

Theorem (Ardeshir & M. 2015)

One may reduce the arithmetical completeness of GL *to the one for* GLCa.

Proof.

Let $\mathsf{GL} \nvdash A$. Then find a Kripke counter model of A. Then transform it to a Kripke model of $\mathsf{GLC_a}$ which refutes $\alpha(A)$ for some propositional substitution α. Thus $\mathsf{GLC_a} \nvdash \alpha(A)$. Finally use arithmetical completeness of $\mathsf{GLC_a}$ and obtain σ such that $\mathsf{PA} \nvdash \sigma\alpha(A)$. ❑

Intuitionistic Provability Logic

Question.

What is the provability logic of Intuitionistic Arithmetic (HA)?

Provability logic of HA

- A. Visser 1980 first considered this.
- Since then many partial related results where obtained.
- Main source for difficulty: HA-verifiable admissible rules.

$$\frac{\neg A \to (B \vee C)}{(\neg A \to B) \vee (\neg A \to C)}$$

Theorem (Visser 2002)

Decidability of the letterless fragment of PL(HA).

Admissible rules

- $A \mathrel{|\!\!\sim_{\mathsf{T}}} B$ iff $\forall \alpha\ (\mathsf{T} \vdash \alpha(A) \Rightarrow \mathsf{T} \vdash \alpha(B))$.
- Example: $\neg A \to (B \vee C) \mathrel{|\!\!\sim_{\mathsf{IPC}}} (\neg A \to B) \vee (\neg A \to C)$.
- In the provability logic of HA, the above rule reflected as:

$$\Box(\neg A \to (B \vee C)) \to \Box((\neg A \to B) \vee (\neg A \to C)).$$

- Why not classically interesting?

$$A \mathrel{|\!\!\sim_{\mathsf{CPC}}} B \quad \text{iff} \quad \mathsf{CPC} \vdash A \to B.$$

Admissible rules of IPC

- For every $A \mathrel{|\!\!\sim_{\mathsf{IPC}}} B$ we have $\Box A \to \Box B$ in $\mathsf{PL}(\mathsf{HA})$.
- What are the admissible rules of IPC? Decidable? (H. Friedman 1975)

Admissible rules of IPC

- For every $A \mathrel{|\!\!\sim_{\mathsf{IPC}}} B$ we have $\Box A \to \Box B$ in PL(HA).
- What are the admissible rules of IPC? Decidable? (H. Friedman 1975)
  Decidability: Rybakov 1997.
  Axiomatization: Visser and de Jongh.
  Completeness proof: Iemhoff 2001.

The system $[\![\mathsf{T},\Delta]\!]$

Axioms: Define $A \xrightarrow{\Delta} E := \begin{cases} E & : E \in \Delta \\ A \to E & : \text{otherwise} \end{cases}$

$$\frac{\mathsf{T} \vdash A \to B}{A \rhd B}\ [\mathsf{T}]$$

$$\frac{A = \bigwedge_{i=1}^{n}(E_i \to F_i) \qquad B = \bigvee_{i=n+1}^{n+m}(F_i)}{(A \to B) \rhd \bigvee_{i=1}^{n+m} A \xrightarrow{\Delta} E_i}\ \mathsf{V}(\Delta)$$

Rules:

$$\frac{A \rhd B \qquad A \rhd C}{A \rhd (B \wedge C)}\ \text{Conj} \qquad \frac{A \rhd B \qquad B \rhd C}{A \rhd C}\ \text{Cut}$$

$$\frac{A \rhd C \qquad B \rhd C}{(A \vee B) \rhd C}\ \text{Disj} \qquad \frac{A \rhd B \qquad (D \in \Delta)}{(D \to A) \rhd (D \to B)}\ \text{Mont}(\Delta)$$

Admissible Rules of IPC

Theorem (Iemhoff 2001)

$A \mathrel{|\!\!\sim}_{\mathsf{IPC}} B$ *iff* $[\![\mathsf{IPC}, \{\top, \bot\}]\!] \vdash A \rhd B$.

Theorem (Visser 2002)

$A \mathrel{|\!\!\sim}_{\mathsf{IPC}} B$ *iff* $[\![\mathsf{IPC}, \{\top, \bot\}]\!] \vdash A \rhd B$ *iff* $\Box A \to \Box B \in \mathsf{PL}(\mathsf{HA})$.

What else in PL(HA)? (Disjunction property)

- DP means that if a disjunction is derivable, then either of them are derivable.
- IPC, IQC and HA has DP.
- CPC $\vdash p \vee \neg p$ while CPC $\nvdash p$ and CPC $\nvdash \neg p$.
- $\Box(A \vee B) \to (\Box A \vee \Box B) \in$ PL(HA)?
- H. Friedman 1975: No!
- D. Leivant 1975: $\Box(A \vee B) \to \Box(\boxdot A \vee \boxdot B) \in$ PL(HA).

PL(HA): the axiomatization

Let us define the Leivant's axiom schema as follows:

$$(\mathsf{Le}):\ A \rhd \Box A \text{ for every } A.$$

Theorem (M. 2022)

$\mathsf{iGLH} := \mathsf{iGL} + \{\Box A \to \Box B : [\![\mathsf{iGL}, \Box]\!]\mathsf{Le} \vdash A \rhd B\} = \mathsf{PL}(\mathsf{HA})$.

PL(HA): the axiomatization

Let us define the Leivant's axiom schema as follows:

$$(\mathsf{Le}):\ A \rhd \Box A \text{ for every } A.$$

Theorem (M. 2022)

$\mathsf{iGLH} := \mathsf{iGL} + \{\Box A \to \Box B : [\![\mathsf{iGL}, \Box]\!]\mathsf{Le} \vdash A \rhd B\} = \mathsf{PL}(\mathsf{HA})$.

Theorem (Ardeshir & M. 2018)

$\mathsf{iGLC_aH}_\sigma := \mathsf{iGLC_a} + \{\Box A \to \Box B : [\![\mathsf{iGLC_a}, \mathsf{atomb}]\!]\mathsf{Le} \vdash A \rhd B\} = \mathsf{PL}_\Sigma(\mathsf{HA})$

Arithmetical soundness

The arithmetical soundness of this system in a more general setting, namely Σ_1-preservativity, was already known by Visser, de Jongh and Iemhoff (2001).

Arithmetical Completeness of iGLH

1. Let $\mathsf{iGLH} \nvdash A$.
2. find some α s.t. $\mathsf{iGLC_aH_\sigma} \nvdash \alpha(A)$.
3. use arithmetical completeness of $\mathsf{iGLC_aH_\sigma}$ to find σ s.t. $\mathsf{HA} \nvdash \sigma\alpha(A)$.

Step 2

- We first need a finite, or at least well-behaved Kripke semantics.
- Iemhoff already provided a semantic for an extension of iGLH in the language with binary modal operator.
- Iemhoff's semantics are not finite.
- At least we failed to use it for the purpose of reduction.
- We provided a finite *mixed* semantic which is a combination of derivability and Kripke-style validity.
- It well fits for preservativity.

Preservativity

$A \mathrel{|\!\!\approx^{\Gamma}_{\mathsf{T}}} B$ iff for every $E \in \Gamma$ ($\mathsf{T} \vdash E \to A$ implies $\mathsf{T} \vdash E \to B$)

Preservativity

$$A \mathrel{|\!\!\approx^{\Gamma}_{\mathsf{T}}} B \text{ iff for every } E \in \Gamma \; (\mathsf{T} \vdash E \to A \text{ implies } \mathsf{T} \vdash E \to B)$$

Theorem (M. 2022)

$[\![\mathsf{iGL}, \Box]\!]\mathsf{Le} \vdash A \rhd B$ *iff* $A \mathrel{|\!\!\approx^{\Gamma}_{\mathsf{iGL}}} B$.

$\Gamma := \mathsf{C{\downarrow}SN}(\Box)$

Roughly, Γ is the set of modal propositions which could be projected to a NNIL-proposition.

Preservativity

$$A \mathrel{|\!\!\approx^{\Gamma}_{\mathsf{T}}} B \text{ iff for every } E \in \Gamma \ (\mathsf{T} \vdash E \to A \text{ implies } \mathsf{T} \vdash E \to B)$$

Theorem (M. 2022)

$[\![\mathsf{iGL}, \Box]\!]\mathsf{Le} \vdash A \rhd B$ *iff* $A \mathrel{|\!\!\approx^{\Gamma}_{\mathsf{iGL}}} B$.

$\Gamma := \mathsf{C}{\downarrow}\mathsf{SN}(\Box)$

Roughly, Γ is the set of modal propositions which could be projected to a NNIL-proposition.

NNIL:

No Nested Implications in the Left.

NNIL-fication

It is a relativised version of Ghilardi's unification for IPC. (1999)

Projectivity: standard definition

A is projective iff there is some θ s.t. $\vdash \theta(A)$ and $A \vdash \theta(x) \leftrightarrow x$ for every variable x.

Theorem

Projective unifier is a most general unifier.

Proof.

Consider some α s.t. $\mathsf{IPC} \vdash \alpha(A)$. Then $\alpha(A) \vdash \alpha\theta(x) \leftrightarrow \alpha(x)$. This means that $\alpha\theta = \theta$, hence θ is more general than α. ❑

Theorem (Ghilardi 1999)

For every A there is a best approximation of A by finite disjunctions of projective propositions $\bigvee \Pi(A)$. Moreover

$$A \mathrel{|\!\!\sim_{\mathsf{IPC}}} \bigvee \Pi(A)$$

NNIL(par)-projectivity

A is NNIL(par)-projective if there is some θ and $B \in \mathsf{NNIL}(\mathsf{par})$ s.t. $\mathsf{IPC} \vdash \theta(A) \leftrightarrow B$ and $A \vdash_{\mathsf{IPC}} \theta(x) \leftrightarrow x$ for every var x.

Theorem (M. 2022)

For every A there is a best approximation of A by finite disjunctions of projective propositions $\bigvee \Pi(A)$. Moreover

$$A \mathrel{|\!\!\sim^{\mathsf{N(par)}}_{\mathsf{IPC}}} \bigvee \Pi(A)$$

Theorem (M. 2022)

$A \mathrel{|\!\!\sim^{\mathsf{N(par)}}_{\mathsf{IPC}}} B$ *iff* $[\![\mathsf{IPC}, \mathsf{NNIL}(\mathsf{par})]\!] \vdash A \rhd B$.

$\mathsf{iGLH}(\Gamma, \mathsf{T})$

$$\mathsf{iGLH}(\Gamma, \mathsf{T}) := \mathsf{iGL} + \{\Box A \to \Box B : A \mathrel{\substack{\Gamma \\ \mid\!\approx \\ \mathsf{T}}} B\}$$

Mixed semantic for $\mathsf{iGLH}(\Gamma, \mathsf{T})$

Mixed semantic for $\mathsf{iGLH}(\Gamma, \mathsf{T})$

- Roughly speaking, a mixed semantic is a usual Kripke model for intuitionistic modal logic, which is augmented by a family of propositions $\{\varphi_w\}_{w\in W}$ with
  - $\varphi_w \in \Gamma$,
  - $\mathcal{K}, w \Vdash \phi_w$,
  - $\mathcal{K}, w \Vdash \Box A$ iff for every $u \sqsupset w$ we have $\mathsf{T}, \Delta_w, \varphi_u \vdash A$.

Thanks For Your Attention