Modal Logics / Provability Logics

Weak Arithmetics / Bounded Arithmetics

Cut-Free Consistency / Herbrand Consistency

Saeed Salehi

http://staff.cs.utu.fi/staff/saeed/

Modal Logic

Philosophy – Logic – Computer Science

$$\Box\, A$$

Necessity – Provability – Program Execution

$$\Box A \to A$$

Philosophy:	necessity implies truth
Math. Logic:	provability implies validity
Comp. Sci.:	program is sound

$$A = \bot: \quad \neg\Box\bot$$

Falsity is not necessary.

Contradiction is not provable (consistent).

Program does not result in absurdity.

Other modalities

$$\Diamond\, A$$

Possibility – Consistency – Probable result

Define $\Diamond A = \neg\Box\neg A$ or $\Box A = \neg\Diamond\neg A$.

$$\Diamond\Diamond A \to \Diamond A \quad \text{or} \quad \Box A \to \Box\Box A$$

Philosophy: "necessity" is necessary

(If possibility of A is possible, then A is indeed possible.)

Math. Logic: "provability" is provable

(If consistency of A is consistent, then A is consistent.)

Comp. Sci.: "executability" is executable

Mathematical Logic:

$\Box A \Leftrightarrow$ 'A is provable' $\Leftrightarrow$ '$\neg A$ is not consistent'

$\Diamond A \Leftrightarrow$ 'A is consistent' $\Leftrightarrow$ '$\neg A$ is not provable'

Propositional Modal Logics

Classical Propositional Calculus +
Modality Axioms and Rules

Language: $\{\bot, \to, \Box\}$
Propositional Variables $\{p, q, r, \ldots\}$

Axioms of CPC:

- $A \to (B \to A)$
- $\Big(A \to (B \to C)\Big) \to \Big((A \to B) \to (A \to C)\Big)$
- $\Big((A \to \bot) \to \bot\Big) \to A$

Rule: (Modus Ponens)

$$\frac{A, \quad A \to B}{B}$$

Convention: $\top = \bot \to \bot$; $\neg A = A \to \bot$;
$A \vee B = \neg A \to B$; $A \wedge B = \neg(\neg A \vee \neg B)$;
$A \leftrightarrow B = (A \to B) \wedge (B \to A)$.

Normal Modal Logics

Axiom: $(\mathtt{K})\ \Box(A \to B) \to (\Box A \to \Box B)$

Rule:

$$(\mathtt{RN})\ \frac{A}{\Box A}$$

This base logic is denoted $\mathbf{K}$.

Add more axioms, get stronger modal logics.

$(\mathtt{4})\ \Box A \to \Box\Box A$; logic $\mathbf{K4}$.

$(\mathtt{L})\ \Box(\Box A \to A) \to \Box A$; Gödel-Löb logic $\mathbf{GL}$.

$$(\mathtt{K}) + (\mathtt{L}) + (\mathtt{RN}) = \ \mathbf{GL} \vdash (\mathtt{4}).$$

Semantics for Normal Modal Logics

Kripke Models: $\mathcal{K} = (W, R, \Vdash)$

$R \subseteq W \times W$; $\Vdash \subseteq W \times \{$Prop. Var.$\}$

$u, v, w \in W$: uRv; $u \Vdash p$.

Extend $\Vdash \subseteq W \times \{$Modal Fromulas$\}$:

$u \nVdash \bot$; $u \Vdash A \to B$ iff ($u \nVdash A$ or $u \Vdash B$);

$u \Vdash \Box A$ iff for any $v \in W$ (if uRv then $v \Vdash A$).

In every Kripke model the axiom

(K) $\Box(A \to B) \to (\Box A \to \Box B)$ is forced, and

the rule (RN) $\frac{A}{\Box A}$ is valid.

(4) $\Box A \to \Box\Box A$ is forced when R is transitive.

$\mathbf{GL}$ is sound and complete w.r.t transitive and reversely well-founded Kripke models.

Modal Logics Weaker than $\mathbf{K}$

When $\Box$ is interpreted as cut-free provability, (K) does not hold (in weak arithmetics).

Another semantics for modal logics:
Lindenbaum-Tarski (Boolean) Algebras
$\mathcal{B} = (B, \underset{\sim}{\wedge}, \underset{\sim}{\vee}, {}', \leqslant, 0, 1, \underset{\sim}{\Box}) \qquad \underset{\sim}{\Box} : B \to B$

Let T be a theory. $[\varphi]_T = \{\psi \mid T \vdash \varphi \leftrightarrow \psi\}$.
$[\varphi]_T \underset{\sim}{\wedge} [\psi]_T = [\varphi \wedge \psi]_T$; $[\varphi]_T \underset{\sim}{\vee} [\psi]_T = [\varphi \vee \psi]_T$;
$[\varphi]'_T = [\neg\varphi]_T$; $\qquad [\varphi]_T \leqslant [\psi]_T$ iff $T \vdash \varphi \to \psi$;
$0 = [\bot]_T$; $1 = [\top]_T$; $\qquad \underset{\sim}{\Box}[\varphi]_T = [\Box\varphi]_T$.

$$\text{Well–defined iff} \quad \frac{T \vdash \varphi \leftrightarrow \psi}{T \vdash \Box\varphi \leftrightarrow \Box\psi}.$$

Minimal Modal Logic $\mathbf{E}$

CPC + Rule of Inference

$$(\mathtt{RE})\ \frac{\varphi \leftrightarrow \psi}{\Box\varphi \leftrightarrow \Box\psi}.$$

Add more axioms or rules, get stronger logics.

Rule

$$(\mathtt{RM})\ \frac{\varphi \to \psi}{\Box\varphi \to \Box\psi}$$

(or equivalently) the Axiom

$$(\mathtt{M})\ \Box(A \wedge B) \to \Box A \wedge \Box B.$$

Semantically, $\underset{\sim}{\Box}$ is monotone:

$$a \leqslant b \Rightarrow \underset{\sim}{\Box}\, a \leqslant \underset{\sim}{\Box}\, b \ \ \dashv\vdash \ \ \underset{\sim}{\Box}(a \underset{\sim}{\wedge} b) \leqslant \underset{\sim}{\Box}\, a \underset{\sim}{\wedge} \underset{\sim}{\Box}\, b.$$

Rule

$$(\mathtt{RN})\ \frac{\varphi}{\Box\varphi}$$

(or equivalently) the Axiom

$$(\mathtt{N})\ \Box\top.$$

Semantically, $\underset{\sim}{\Box}\, 1 = 1$.

Axiom $(\mathtt{C})$ $\Box A \wedge \Box B \to \Box(A \wedge B)$;

In models: $\underset{\sim}{\Box}\, a \underset{\sim}{\wedge} \underset{\sim}{\Box}\, b \leqslant \underset{\sim}{\Box}\, (a \underset{\sim}{\wedge} b)$.

Axiom $(\mathtt{K})$ $\Box(A \to B) \wedge \Box A \to \Box B$;

In models: $\underset{\sim}{\Box}(a' \underset{\sim}{\vee} b) \underset{\sim}{\wedge} \underset{\sim}{\Box}\, a \ \leqslant\ \underset{\sim}{\Box}\, b$.

We note that

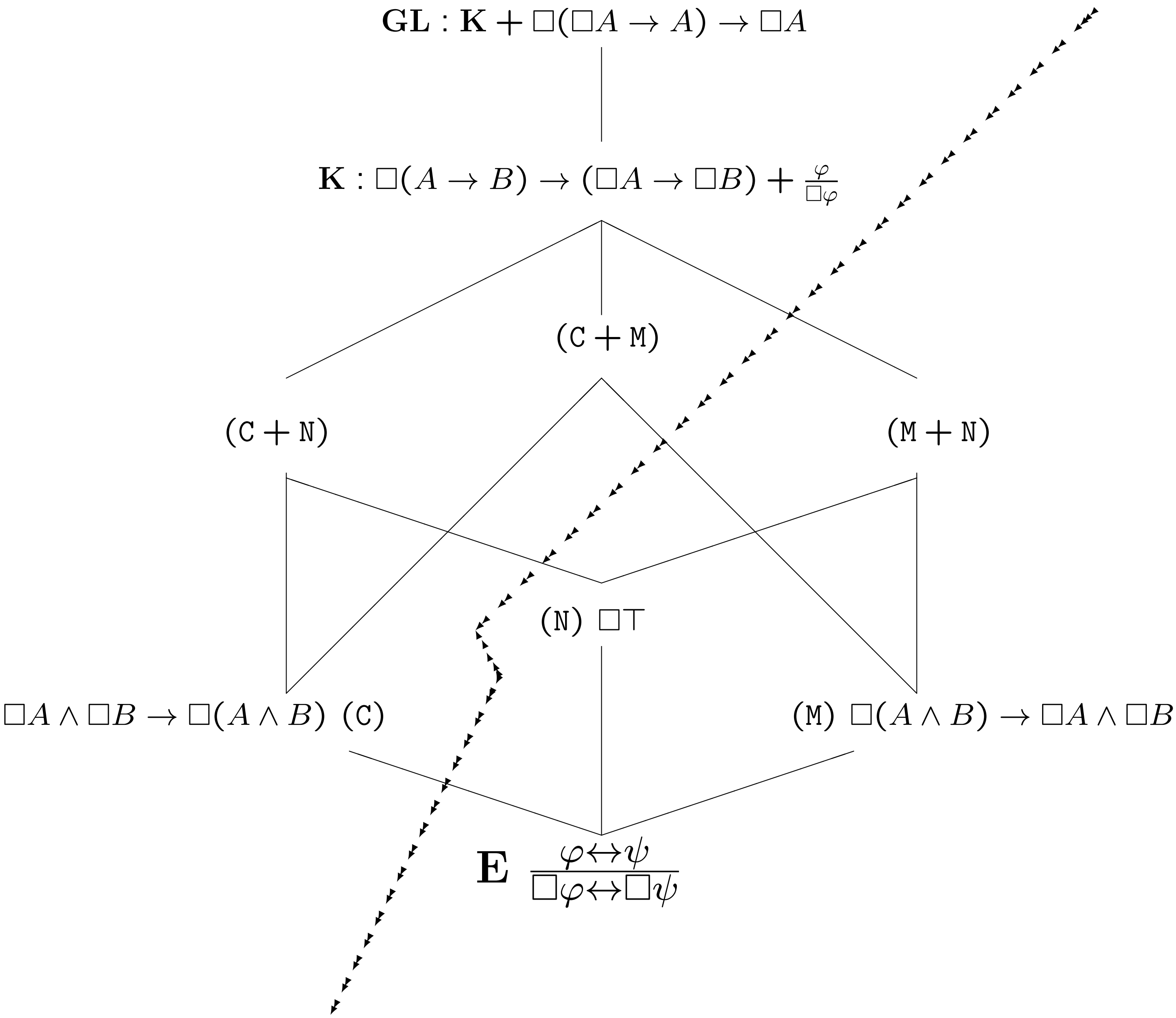
$$\mathbf{K} \vdash (\mathtt{N}) + (\mathtt{M}) + (\mathtt{C}),$$

and

$$(\mathtt{M}) + (\mathtt{C}) \vdash_{\mathbf{E}} (\mathtt{K}).$$

So,

$$\mathbf{K} = \mathbf{E} + (\mathtt{N}) + (\mathtt{M}) + (\mathtt{C}).$$



B. Chellas, *Modal logic: An introduction* (Cambridge University Press, 1980).

Minimal (Neighborhood) Models for $\mathbf{E}$

$\mathcal{M} = \langle W, N, \|\cdot\| \rangle$,

- W is a nonempty set (of worlds);
- N is a mapping $W \to \mathcal{P}\mathcal{P}(W)$

  $\mathcal{P}(\cdot)$ is the power set operation;
- $\|\cdot\|$: {Prop. Var.} $\to \mathcal{P}(W)$ mapping.

$\|A\|$ is the set of worlds in which A holds;
$N : w \mapsto N_w$ the set of propositions that are necessary at w.

Extend $\|\cdot\|$: {Modal Formulas} $\to \mathcal{P}(W)$:
$\|\bot\| = \emptyset$; $\quad \|A \to B\| = \|A\|^{\complement} \cup \|B\|$;
$\|\Box A\| = \{w \in W \mid \|A\| \in N_w\}$.

(RE) $(A \leftrightarrow B)/(\Box A \leftrightarrow \Box B)$ is valid in any $\mathcal{M}$:
if $\|A\| = \|B\|$ then $\|\Box A\| = \|\Box B\|$.

Completeness:
$\mathbf{E} \vdash \varphi$ iff φ is valid ($\|\varphi\| = W$) in any $\mathcal{M}$.

($\mathtt{M}$) $\Box(A \wedge B) \rightarrow \Box A \wedge \Box B$ is valid in $\mathcal{M}$ if every N_w is closed under super-sets: if $X \subseteq Y$ and $X \in N_w$, then $Y \in N_w$.

$\mathbf{E} + (\mathtt{M}) \vdash \varphi$ iff φ is valid in any $\mathcal{M}$ closed under supersets.

($\mathtt{N}$) $\Box\top$ is valid in $\mathcal{M}$ if every N_w contains W: $W \in N_w$.

$\mathbf{E} + (\mathtt{N}) \vdash \varphi$ iff φ is valid in any $\mathcal{M}$ contains W.

($\mathtt{C}$) $\Box A \wedge \Box B \rightarrow \Box(A \wedge B)$ is valid in $\mathcal{M}$ if every N_w is closed under intersections: if $X, Y \in N_w$, then $X \cap Y \in N_w$.

$\mathbf{E} + (\mathtt{C}) \vdash \varphi$ iff φ is valid in any $\mathcal{M}$ closed under intersections.

$\mathbf{K}$ is sound and complete in any $\mathcal{M}$ in which each N_w is a non-empty (principal) filter.

Relations to Kripke Models

Given a Kripke model $\mathcal{K} = (W, R, \Vdash)$ define $\mathcal{M} = \langle W, N, \|\cdot\|\rangle$ by $\|p\| = \{w \in W \mid w \Vdash p\}$, $N_w = \Big\{X \subseteq W \mid X \supseteq \{v \in W \mid wRv\}\Big\}$ (principal) filter.

For any modal formula A, $w \in \|A\| \iff w \Vdash A$.

If in $\mathcal{M} = \langle W, N, \|\cdot\|\rangle$ each N_w is a principal filter, define Kripke model $\mathcal{K} = (W, R, \Vdash)$ by $wRv \iff v \in \bigcap N_w$, and $w \Vdash p \iff w \in \|p\|$.

For any modal formula A, $w \Vdash A \iff w \in \|A\|$.

Arithmetic

Language $\mathcal{L} = \{S, +, \times, =, \leq, 0\}$

Base Theory – Robinson's Arithmetic Q

▪$S(x) \neq 0$ ▪$S(x) = S(y) \to x = y$

▪$x + 0 = x$ ▪$x + S(y) = S(x + y)$

▪$x \times 0 = 0$ ▪$x \times S(y) = (x \times y) + x$

•$x \neq 0 \to \exists y(x = S(y))$ •$x \leq y \leftrightarrow \exists z(x + z = y)$

•-axioms replaced with some $\forall$-sentences

▪$x \leq x$ ▪$x \leq y \leq x \to x = y$ ▪$x \leq y \vee y \leq x$

▪$0 \leq x$ ▪$x \leq y \leq z \to x \leq z$ ▪$x \leq y \to S(x) \leq S(y)$

▪$x \leq S(y) \to x = S(y) \vee x \leq y$

This base $\forall$-theory $\mathbf{A}$ is useful.
No Skolem term is needed for $\forall$-theories.

Induction axiom (for $\varphi(x, \overline{y})$) Ind_φ

$$\varphi(0, \overline{y}) \wedge \forall x\{\varphi(x, \overline{y}) \to \varphi(S(x), \overline{y})\} \Rightarrow \forall x \varphi(x, \overline{y})$$

$\mathbf{PA} = \mathbf{A} + \{\mathrm{Ind}_\varphi\}_\varphi$ Peano's Arithmetic

Arithmetization

T arithmetical theory. $\ulcorner\varphi\urcorner$ Gödel code of φ

$\mathsf{Proof}_T(z, x) = z$ is a T-proof of x (Δ_0)

$\mathsf{Pr}_T(x) = \exists z \mathsf{Proof}_T(z, x)$ (Σ_1)

$\mathsf{Pr}_T(\ulcorner\varphi\urcorner)$ is true (in $\mathbb{N}$) iff $T \vdash \varphi$

Provability Logic

For sufficiently strong theories T:

- if $T \vdash \varphi$ then $T \vdash \mathsf{Pr}_T(\ulcorner\varphi\urcorner)$
- $T \vdash \mathsf{Pr}_T(\ulcorner\varphi \to \psi\urcorner) \to (\mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \mathsf{Pr}_T(\ulcorner\psi\urcorner))$
- $T \vdash \mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \mathsf{Pr}_T(\ulcorner\mathsf{Pr}_T(\ulcorner\varphi\urcorner)\urcorner)$
- $T \vdash \mathsf{Pr}_T(\ulcorner(\mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \varphi)\urcorner) \to \mathsf{Pr}_T(\ulcorner\varphi\urcorner)$

Weak Arithmetics

Bounded formula – all quantifiers are bounded

$\forall x \leq y \exists u \leq v \cdots$ Δ_0-formula; Ind_{Δ_0}
$\forall x(x \leq y \to \ldots)$; $\exists u(u \leq v \wedge \ldots)$

Σ_1-formula $= \exists \ldots \exists(\Delta_0)$; Ind_{Σ_1}
Π_1-formula $= \forall \ldots \forall(\Delta_0)$; Ind_{Π_1}

$I\Delta_0 = \mathbf{A} + \mathrm{Ind}_{\Delta_0}$ $I\Sigma_1 = \mathbf{A} + \mathrm{Ind}_{\Sigma_1}$
The two $\bullet$-axioms of Q are provable in $I\Delta_0$.

Gödel's Second Incompleteness Theorem can be worked out in $I\Sigma_1$
($\supseteq$ Primitive Recursive Arithmetic).

$I\Delta_0$ is very weak:
If $I\Delta_0 \vdash \forall x \exists y\, \psi(x, y)$ for bounded ψ, then for some polynomial p, $I\Delta_0 \vdash \forall x \exists y \leq p(x)\, \psi(x, y)$.

So, exp ($y = 2^x$) is not provably total in $I\Delta_0$ (but is in $I\Sigma_1$). We note that exp can be defined by a bounded formula.

Bounded Arithmetics

$\omega_1(x) = x^{\log x}$ $(> x^n + n)$ $\Omega_1 = \forall x \exists y (\underbrace{y = \omega_1(x)}_{\Delta_0})$

$I\Delta_0 + \Omega_1$ is just right for treating syntax; e.g. substitution (of terms in formulas) is possible.

$\omega_2(x) = 2^{(\log x)^{\log\log x}} \quad \Omega_2 = \forall x \exists y (y = \omega_2(x))$

$I\Delta_0 \subsetneqq I\Delta_0 + \Omega_1 \subsetneqq I\Delta_0 + \Omega_2 \subsetneqq \ldots \subsetneqq I\Delta_0 + \mathrm{exp}$

Arithmetization

T arithmetical theory. $\ulcorner\varphi\urcorner$ Gödel code of φ

$\mathrm{Proof}_T(z, x) = z$ is a T-proof of x (Δ_0)

$\mathrm{Pr}_T(x) = \exists z \mathrm{Proof}_T(z, x)$ (Σ_1)

$\mathrm{Pr}_T(\ulcorner\varphi\urcorner)$ is true (in $\mathbb{N}$) iff $T \vdash \varphi$

Σ_1-completeness and Diagonalization in $\mathbf{A}$

Every true (in $\mathbb{N}$) Σ_1-formula is provable in $\mathbf{A}$. In particular, if $T \vdash \varphi$ then $\mathbf{A} \vdash \mathsf{Pr}_T(\ulcorner\varphi\urcorner)$.

For any formula $\Phi(x)$ there exists a (fixed-point) formula φ such that $\mathbf{A} \vdash \varphi \leftrightarrow \Phi(\ulcorner\varphi\urcorner)$

Provability Logic

Suppose $T \supseteq I\Delta_0 + \Omega_1$:

- if $T \vdash \varphi$ then $T \vdash \mathsf{Pr}_T(\ulcorner\varphi\urcorner)$
- $T \vdash \mathsf{Pr}_T(\ulcorner\varphi \to \psi\urcorner) \to (\mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \mathsf{Pr}_T(\ulcorner\psi\urcorner))$
- $T \vdash \mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \mathsf{Pr}_T(\ulcorner\mathsf{Pr}_T(\ulcorner\varphi\urcorner)\urcorner)$
- $T \vdash \mathsf{Pr}_T(\ulcorner(\mathsf{Pr}_T(\ulcorner\varphi\urcorner) \to \varphi)\urcorner) \to \mathsf{Pr}_T(\ulcorner\varphi\urcorner)$

Gödel's Second Incompleteness Theorem

$T \nvdash \neg\mathsf{Pr}_T(\ulcorner 0 = 1 \urcorner)$.

Write $\mathsf{Con}(T) = \neg\mathsf{Pr}_T(\ulcorner \bot \urcorner)$: $T \nvdash \mathsf{Con}(T)$.

For T which satisfies above,

$T \vdash \mathsf{Pr}_T(\ulcorner (\mathsf{Pr}_T(\ulcorner \bot \urcorner) \to \bot) \urcorner) \to \mathsf{Pr}_T(\ulcorner \bot \urcorner)$

$T \vdash \mathsf{Pr}_T(\ulcorner \mathsf{Con}(T) \urcorner) \to \neg\mathsf{Con}(T)$

$T \vdash \mathsf{Con}(T) \to \neg\mathsf{Pr}_T(\ulcorner \mathsf{Con}(T) \urcorner)$

If $T \vdash \mathsf{Con}(T)$, $T \vdash \mathsf{Pr}_T(\ulcorner \mathsf{Con}(T) \urcorner)$ and

$T \vdash \neg\mathsf{Pr}_T(\ulcorner \mathsf{Con}(T) \urcorner)$,

so $T \vdash \bot$ #

▶▶▶ With other methods

$T \nvdash \mathsf{Con}(T)$ also for theories as weak as $T \supseteq Q$

Interpretation

Mapping:

$\{$Modal Formulas$\} \to \{$Arithmetical Formulas$\}$

T – an arithmetical theory

Atomic $p \mapsto p^*$ - arbitrary; $\perp \mapsto \perp^* = (0 = 1)$

$(A \to B)^* = A^* \to B^*, \quad (\Box A)^* = \mathsf{Pr}_T(\ulcorner A^* \urcorner)$

Provability Logic of T at U: modal axioms and rules valid in U when $\Box$ is interpreted as Pr_T.

$\mathbf{PL}_T$ Provability Logic of T at T.

Theorem. For suff. strong T, $\mathbf{PL}_T = \mathbf{GL}$.

(Generalized) Solovay's Completeness Thm

Interpretation

Mapping:

{Modal Formulas} $\to$ {Arithmetical Formulas}

T – an arithmetical theory

Atomic $p \mapsto p^*$ - arbitrary; $\perp \mapsto \perp^* = (0 = 1)$

$(A \to B)^* = A^* \to B^*, \quad (\Box A)^* = \mathrm{Pr}_T(\ulcorner A^* \urcorner)$

Provability Logic of T at U: modal axioms and rules valid in U when $\Box$ is interpreted as Pr_T.

$\mathbf{PL}_T$ Provability Logic of T at T.

Theorem. For $T \supseteq I\Delta_0 + \mathrm{exp}$, $\mathbf{PL}_T = \mathbf{GL}$.

(Generalized) Solovay's Completeness Thm

We also know $\mathbf{PL}_{I\Delta_0+\Omega_1} \supseteq \mathbf{GL}$.

Open Question. $\mathbf{PL}_{I\Delta_0+\Omega_1} = \mathbf{GL}$?

Weakening a theory does not weaken its provability logic. E.g., intuitionistic $\mathbf{HA}$:

(†) $\Box(A \vee B) \to \Box(\Box A \vee \Box B)$ is in $\mathbf{PL_{HA}}$, indeed by the disjunction property

$\mathbf{HA} \vdash \varphi \vee \psi \;\Rightarrow\; \mathbf{HA} \vdash \varphi$ or $\mathbf{HA} \vdash \psi$.

(†) does not hold for $\mathbf{PA}$: take $\mathsf{C} = \mathsf{Con}(\mathbf{PA})$. Then $\mathbf{PA} \vdash \mathsf{Pr}_{\mathbf{PA}}(\ulcorner \mathsf{C} \vee \neg \mathsf{C} \urcorner)$, but

$\mathbf{PA} \nvdash \mathsf{Pr}_{\mathbf{PA}}\Big(\ulcorner \mathsf{Pr}_{\mathbf{PA}}(\ulcorner \mathsf{C} \urcorner) \vee \mathsf{Pr}_{\mathbf{PA}}(\ulcorner \neg \mathsf{C} \urcorner)\urcorner\Big)$

Though $\mathbf{PL_{HA}} \supsetneqq \mathbf{GL}$; open question $\mathbf{PL_{HA}} =$?.

For *classical* theories we do not know if $U \subseteq V$ implies $\mathbf{PL}_U \subseteq \mathbf{PL}_V$.

$\mathbf{GL}$ is the only provability logic known so far.

Π_1-conservativity

PROVABILITY $\subseteq$ TRUTH;

Truth is not Π_1-conservative over Provaility:

$\mathbb{N} \models \mathrm{Con}(\mathbf{PA})$
$\mathrm{ZFC} \vdash \mathrm{Con}(\mathbf{PA})$ $\quad \mathbf{PA} \nvdash \mathrm{Con}(\mathbf{PA})$

$\mathbf{PA} \vdash \mathrm{Con}(I\Sigma_1) \qquad I\Sigma_1 \nvdash \mathrm{Con}(I\Sigma_1)$

But $I\Delta_0 + \exp \nvdash \mathrm{Con}(I\Delta_0) \quad I\Delta_0 \nvdash \mathrm{Con}(I\Delta_0)$

For weak arithmetics the predicate of Cut-Free consistency seemed to be a good alternative for consistency predicate.

Paris & Wilkie 1981:

$I\Delta_0 + \exp \vdash \mathrm{CFCon}(I\Delta_0) \not\prec$

$I\Delta_0 \nvdash \mathrm{CFCon}(I\Delta_0)$ (? - took 20 years)

$I\Sigma_1 \vdash \mathsf{CFCon}(T) \leftrightarrow \mathsf{Con}(T)$

$$\begin{aligned} I\Delta_0 + \mathsf{exp} \ &\nvdash \mathsf{Con}(I\Delta_0),\ \mathsf{Con}(Q) \\ &\vdash \mathsf{CFCon}(I\Delta_0) \end{aligned}$$

For weak theories:

Initial segment (definable cut): $J(x)$,

$J(0) \wedge \{J(x) \rightarrow J(Sx)\} \wedge \{J(x) \wedge y \leq x \rightarrow J(y)\}$

for any cut J, $\quad T \nvdash \mathsf{Con}^J(T)$

for some cut J, $\quad T \vdash \mathsf{CFCon}^J(T)$

Π_1-conservativity of $I\Delta_0 + \Omega_2$ over $I\Delta_0 + \Omega_1$, and of $I\Delta_0 + \Omega_1$ over $I\Delta_0$ is still open.

Also $I\Delta_0 + \Omega_2 \nvdash \mathsf{CFCon}(I\Delta_0)$.

A good candidate: CFCon^I for some I ?

(Kolodziejczyk 2006)

Herbrand Consistency

Skolemization: For any $\exists$ put a new function symbol whose arity is the number of $\forall$'s that appears before it(s scope).

$$\exists x\, \psi(x, \ldots) \xrightarrow{\text{Sk}} \psi(\mathfrak{c}, \ldots) \text{ constant symbol}$$

$$\forall x \exists y\, \psi(x, y) \xrightarrow{\text{Sk}} \psi(x, \mathfrak{f}(x)) \text{ unary function}$$

Herbrand-Skolem:

A theory is consistent iff its Skolemized form is consistent (in the expanded language).

Herbrand model:

(add) Skolem constants, make it closed

under Skolem functions, satisfying the resulted Skolemized $\forall$-theory.

Example: Let T be axiomatized by

1. $\forall x \exists y\ \alpha(x, y)$ 2. $\forall x \exists y\ \beta(x, y)$

3. $\forall x, y(\alpha(x, y) \to \gamma(x) \vee \delta(y))$

4. $\forall x, y(\beta(x, y) \to \neg\delta(x))$

Skolemized T^{Sk}:

1. $\alpha(x, \mathfrak{f}(x))$ 2. $\beta(x, \mathfrak{g}(x))$ 3. 4.

Herbrand model: $\{\mathfrak{c}, \mathfrak{f}(\mathfrak{c}), \mathfrak{g}(\mathfrak{c}), \mathfrak{f}\mathfrak{f}(\mathfrak{c}), \mathfrak{f}\mathfrak{g}(\mathfrak{c}), \ldots\}$

Let $\varphi = \forall x\ \gamma(x)$. We want to show $T \vdash \varphi$.
Suffices to show $T + \neg\varphi$ is not consistent.
Skolemize $\neg\varphi = \exists x \neg\gamma(x)$ as $\neg\gamma(\mathfrak{c})$.
Show $T^{\mathsf{Sk}} + \neg\gamma(\mathfrak{c})$ cannot be realized in the above Herbrand set (of Skolem terms).

We have $\alpha(\mathfrak{c}, \mathfrak{f}(\mathfrak{c}))$ and $\beta(\mathfrak{f}(\mathfrak{c}), \mathfrak{g}\mathfrak{f}(\mathfrak{c}))$ by 1.,2.; so $\gamma(\mathfrak{c}) \vee \delta(\mathfrak{f}(\mathfrak{c}))$ by 3., and $\neg\delta(\mathfrak{f}(\mathfrak{c}))$ by 4. Thus $\gamma(\mathfrak{c})$ contradicting the assumption $\neg\gamma(\mathfrak{c})$.

Actually the finite set $\{\mathfrak{c}, \mathfrak{f}(\mathfrak{c}), \mathfrak{g}\mathfrak{f}(\mathfrak{c})\}$ of Skolem terms was sufficient for the proof.

Herbrand's Theorem: $T \vdash \varphi$ iff there is a *finite* set of Skolem terms (of $(T + \neg\varphi)^{\mathsf{Sk}}$) such that $T + \neg\varphi$ cannot be realized in it.

So, Herbrand's proof of $T \vdash \varphi$ is a finite set of Skolem terms.

Evaluation p on a set of terms Λ is a mapping $p : \Lambda \to \{0, 1\}$ such that $p[x = x] = 1$ and $p[x = y] = 1 \Rightarrow p[\phi(x)] = p[\phi(y)]$.
T-evaluation: $p[T^{\mathsf{Sk}}] = 1$.

Herbrand's Theorem: T is consistent iff for every finite set of Skolem terms there exists an T-evaluation on it.

Herbrand Consistency Predicate $\mathsf{HCon}_T(\ulcorner\varphi\urcorner)$:
$\forall$ set of terms, $\exists$ $(T+\varphi)-$evaluation on it
$\mathsf{HPr}_T(\ulcorner\varphi\urcorner) = \neg\, \mathsf{HCon}_T(\ulcorner\neg\varphi\urcorner)$

Weak Arithmetics:

Treat $\{S,+,\times\}$ as predicates. For a set of terms Λ there are $3|\Lambda|^2+2|\Lambda|^3$ atomic formulas with terms in Λ;
(number of evaluations on Λ) $= 2^{3|\Lambda|^2+2|\Lambda|^3}$
code of evaluations $\leq \Lambda^{|\Lambda|^4}$

For $I\Delta_0$, $\mathsf{HCon}_T(\ulcorner\varphi\urcorner)$:
$\forall\Lambda$ { $\Lambda^{|\Lambda|^4}\downarrow \Rightarrow \exists(T+\varphi)-$evaluation on Λ }
$\mathsf{HPr}_T(\ulcorner\varphi\urcorner)$:
$\exists\Lambda$ { $\Lambda^{|\Lambda|^4}\downarrow$ & $\nexists(T+\neg\varphi)-$evaluation on Λ }

Define $I(x)$: there exists a sequence $\langle 2, 2^2, \ldots, a_n, a_{n+1}, \ldots, 2^{2^x} \rangle$ of length $x+1$ s.t. $a_0 = 2$, $a_{n+1} = a_n \times a_n$. In particular $2^{2^x}\downarrow$.

$\mathsf{HCon}^I_T(\ulcorner \varphi \urcorner)$:
$\forall \Lambda \, \{ \, I(\Lambda^{|\Lambda|^4}) \ \Rightarrow \exists (T + \varphi)-$evaluation on $\Lambda \, \}$

$\mathsf{HPr}^I_T(\ulcorner \varphi \urcorner)$:
$\exists \Lambda \, \{ \, I(\Lambda^{|\Lambda|^4}) \,\&\, \ \nexists (T + \neg\varphi)-$evaluation on $\Lambda \, \}$

$T = I\Delta_0 +$ two $I\Delta_0$-provable sentences

$$T \vdash \mathsf{HCon}(T) \rightarrow \Big(\exists x \in I\ \theta(x) \rightarrow$$

"$\theta \in \Delta_0$"

$$\mathsf{HCon}^I_T(\ulcorner \exists x \in I\ \theta(x) \urcorner)\Big)$$

$$T \vdash \mathsf{HCon}(T) \rightarrow \Big(\mathsf{HPr}^I_T(\ulcorner \varphi \urcorner) \rightarrow$$

$$\mathsf{HCon}^I_T(\ulcorner \mathsf{HPr}^I_T(\ulcorner \varphi \urcorner) \urcorner)\Big)$$

$\mathsf{HPr}_T = \Box^0 \quad \mathsf{HCon}_T = \Diamond^0$

$\mathsf{HPr}^I_T = \Box \quad \mathsf{HCon}^I_T = \Diamond$

★ $T \vdash \Diamond^0 \top \rightarrow (\Box \varphi \rightarrow \Diamond \Box \varphi)$

★ $T \vdash \mathbb{F} \leftrightarrow \neg \Box\, \mathbb{F}$

★ $T \vdash \varphi \ \Rightarrow\ T \vdash \Box \varphi$

★ $T \vdash \varphi \leftrightarrow \psi \ \Rightarrow\ T \vdash \Box \varphi \leftrightarrow \Box \psi$

$T \nvdash \mathsf{HCon}(T) = \Diamond^0 \top$:

If $T \vdash \Diamond^0 \top$, $T \vdash \Box\, \mathbb{F} \to \Diamond \Box\, \mathbb{F}$.

Also $T \vdash \Box\, \mathbb{F} \leftrightarrow \Box \neg \Box\, \mathbb{F} = \neg \Diamond \Box\, \mathbb{F}$, so $T \vdash \neg \Box\, \mathbb{F}$.

From $T \vdash \mathbb{F}$: $T \vdash \Box\, \mathbb{F}$, $T \vdash \neg \Box\, \mathbb{F}$, $T \vdash \bot$ #

Also from $T \vdash T \leftrightarrow I\Delta_0$: $I\Delta_0 \vdash \Diamond T \leftrightarrow \Diamond I\Delta_0$

So, $I\Delta_0 \nvdash \mathsf{HCon}(I\Delta_0)$. (Salehi 2002,2006)

(Adamowicz 2001)

$I\Delta_0 + \Omega_2 \nvdash \mathsf{HCon}(I\Delta_0 + \Omega_2)$ [& Zbierski]

$I\Delta_0 + \Omega_1 \nvdash \mathsf{TabCon}(I\Delta_0 + \Omega_1)$

(Willard 2002)

$Q + V \nvdash \mathsf{TabCon}(Q + V)$, $\Pi_1, I\Delta_0$−provable

also, $I\Delta_0 \nvdash \mathsf{TabCon}(I\Delta_0)$

Herbrand Provability Logic of $I\Delta_0$

$\mathcal{H}$: CPC$\{\mathbb{F}, \mathbb{C}\}$ +

$$(\mathtt{RE})\ \frac{\varphi \leftrightarrow \psi}{\Box\varphi \leftrightarrow \Box\psi}$$

(N) $\Box\top$

(M) $\Box(A \wedge B) \to \Box A \wedge \Box B$

(F) $\mathbb{F} \leftrightarrow \neg\Box\,\mathbb{F}$

(S) $\mathbb{C} \to (\Box A \to \Diamond\Box A)$

By the above proof $\mathcal{H} \nvdash \mathbb{C}$.
If $\mathcal{H} \vdash \mathbb{C}$, then $\mathcal{H} \vdash \Box\,\mathbb{F} \to \Diamond\Box\,\mathbb{F}$,
also $\mathcal{H} \vdash \Box\,\mathbb{F} \leftrightarrow \Box\neg\Box\,\mathbb{F} = \neg\Diamond\Box\,\mathbb{F}$, so $\vdash\neg\Box\,\mathbb{F}$ or $\mathcal{H} \vdash \mathbb{F}$. Thus $\mathcal{H} \vdash \Box\,\mathbb{F}\ \&\ \neg\Box\,\mathbb{F}$, or $\mathcal{H} \vdash \bot$ #

Interpretation.

- $\bot^* =$ "$0 = 1$" • $\mathbf{A} \vdash \mathbb{F}^* \leftrightarrow \neg\,\mathsf{HPr}^I_T(\ulcorner\mathbb{F}^*\urcorner)$
- $\mathbb{C}^* =$ "$\mathsf{HCon}(T)$" • $(\Box A)^* = \mathsf{HPr}^I_T(\ulcorner A^*\urcorner)$

$\mathcal{H} \vdash A \ \Rightarrow\ I\Delta_0 \vdash A^*$ for any modal A

¿$\Leftarrow$?

$\mathcal{H} \hookrightarrow \mathbf{GL}$: $\quad \mathbb{F}, \mathbb{C} \mapsto \Diamond\top$

$\mathbf{GL} \vdash \Diamond\top \leftrightarrow \neg\Box\Diamond\top$; $\;\mathbf{GL} \vdash \Diamond\top \to (\Box A \to \Diamond\Box A)$.

$\mathbf{GL} \vdash \Box(\Box\varphi \to \varphi) \leftrightarrow \Box\varphi \qquad\qquad \varphi = \bot$;

$\mathbf{K} \vdash \Diamond\top \wedge \Box B \to \Diamond B$:

$\mathbf{K} \vdash \Box B \wedge \neg\Diamond B \to \Box B \wedge \Box\neg B \to \Box\bot \to \neg\Diamond\top$.

$\mathbf{K4} \vdash \Diamond\top \wedge \Box A \to \Diamond\top \wedge \Box\Box A \to \Diamond\Box A$.

Open Question. $\mathbf{HPL}_{I\Delta_0} =?$ $\;\mathbf{HPL}_{I\Delta_0+\Omega_1} =?$

$(\mathtt{C})$ $\Box A \wedge \Box B \to \Box(A \wedge B)$ and

$(\mathtt{K})$ $\Box(A \to B) \wedge \Box A \to \Box B$

are not in $\mathbf{HPL}_{I\Delta_0}, \mathbf{HPL}_{I\Delta_0+\Omega_1}$.

Conjecture. $\quad \mathbf{HPL}_{I\Delta_0}, \mathbf{HPL}_{I\Delta_0+\Omega_1} \subsetneqq \mathbf{GL}$

There is an arithmetical formula $\mathbb{F}$ such that for weak arithmetics T:

★ $T \vdash \mathbb{C} \to (\Box\varphi \to \Diamond\Box\varphi)$

★ $T \vdash \mathbb{F} \leftrightarrow \neg\Box\,\mathbb{F}$

★ $T \vdash \varphi \;\Rightarrow\; T \vdash \Box\varphi$ (or $T \vdash \Box\top$)

★ $T \vdash \varphi \leftrightarrow \psi \;\Rightarrow\; T \vdash \Box\varphi \leftrightarrow \Box\psi$

where $\mathbb{C}$ denotes Cut-Free Consistency of T.

$T \nvdash \mathbb{C}$:

If $T \vdash \mathbb{C}$, then $T \vdash \Box\,\mathbb{F} \to \Diamond\Box\,\mathbb{F}$.

Also $T \vdash \Box\,\mathbb{F} \leftrightarrow \Box\neg\Box\,\mathbb{F} = \neg\Diamond\Box\,\mathbb{F}$, so $T \vdash \neg\Box\,\mathbb{F}$.

From $T \vdash \mathbb{F}$: $T \vdash \Box\,\mathbb{F}$, $T \vdash \neg\Box\,\mathbb{F}$, $T \vdash \bot$ $\#$

$\mathcal{H}$: CPC$\{\mathbb{F},\mathbb{C}\}$ +

$$(\mathtt{RE})\ \frac{\varphi \leftrightarrow \psi}{\Box\varphi \leftrightarrow \Box\psi}$$

$(\mathtt{N})\ \Box\top$ $\qquad$ $(\mathtt{M})\ \Box(A \wedge B) \to \Box A \wedge \Box B$

$(\mathtt{F})\ \mathbb{F} \leftrightarrow \neg\Box\,\mathbb{F}$ $\qquad$ $(\mathtt{S})\ \mathbb{C} \to (\Box A \to \Diamond\Box A)$

This modal logic $\mathcal{H}$ is an approximation of Cut-Free provability logic of bounded arithmetics.

By the above proof $\mathcal{H} \nvdash \mathbb{C}$.

We note that $\mathcal{H} \hookrightarrow \mathbf{GL}$: $\quad \mathbb{F}, \mathbb{C} \mapsto \Diamond\top$

$\mathbf{GL} \vdash \Diamond\top \leftrightarrow \neg\Box\Diamond\top$; $\ \mathbf{GL} \vdash \Diamond\top \to (\Box A \to \Diamond\Box A)$.

$\mathbf{GL} \vdash \Box(\Box\varphi \to \varphi) \leftrightarrow \Box\varphi$

let $\varphi = \bot$, so $\mathbf{GL} \vdash \Diamond\top \leftrightarrow \neg\Box\Diamond\top$.

$\mathbf{K} \vdash \Diamond\top \wedge \Box B \to \Diamond B$:

$\mathbf{K} \vdash \Box B \wedge \neg\Diamond B \to \Box B \wedge \Box\neg B \to \Box\bot \to \neg\Diamond\top$.

$\mathbf{K4} \vdash \Diamond\top \wedge \Box A \to \Diamond\top \wedge \Box\Box A \to \Diamond\Box A$.

Interpretation

Mapping:
{Modal Formulas} $\to$ {Arithmetical Formulas}

T – an arithmetical theory

Atomic $p \mapsto p^*$ - arbitrary; $\perp \mapsto \perp^* = (0 = 1)$
$(A \to B)^* = A^* \to B^*$, $(\Box A)^* = \mathrm{Pr}_T(\ulcorner A^* \urcorner)$

$\mathbf{PL}_T$ Provability Logic of T at T.

Theorem. For $T \supseteq I\Delta_0 + \exp$, $\mathbf{PL}_T = \mathbf{GL}$.
(Generalized) Solovay's Completeness Thm

We also know $\mathbf{PL}_{I\Delta_0+\Omega_1} \supseteq \mathbf{GL}$.
Open Question. $\mathbf{PL}_{I\Delta_0+\Omega_1} = \mathbf{GL}$?

For *classical* theories we do not know if $U \subseteq V$ implies $\mathbf{PL}_U \subseteq \mathbf{PL}_V$.

$\mathbf{GL}$ is the only provability logic known so far.
(for sound theories)

Π_1-conservativity

PROVABILITY $\subseteq$ TRUTH;

Truth is not Π_1-conservative over Provaility:

$\mathbb{N} \models \mathrm{Con}(\mathbf{PA})$
$\mathrm{ZFC} \vdash \mathrm{Con}(\mathbf{PA})$ $\quad \mathbf{PA} \nvdash \mathrm{Con}(\mathbf{PA})$

$\mathbf{PA} \vdash \mathrm{Con}(I\Sigma_1)$ $\qquad I\Sigma_1 \nvdash \mathrm{Con}(I\Sigma_1)$

But $I\Delta_0 + \exp \nvdash \mathrm{Con}(I\Delta_0)$ $\quad I\Delta_0 \nvdash \mathrm{Con}(I\Delta_0)$

For weak arithmetics the predicate of Cut-Free consistency seemed to be a good alternative for consistency predicate.

Paris & Wilkie 1981:

$I\Delta_0 + \exp \vdash \mathrm{CFCon}(I\Delta_0)$ $\quad \checkmark$

$I\Delta_0 \nvdash \mathrm{CFCon}(I\Delta_0)$ (? - took 20 years)

$I =$ a suitable initial segment / cut

$T = I\Delta_0 +$ two $I\Delta_0$-provable sentences

$$T \vdash \mathsf{HCon}(T) \to \Big(\mathsf{HPr}^I_T(\ulcorner\varphi\urcorner) \to \mathsf{HCon}^I_T(\ulcorner\mathsf{HPr}^I_T(\ulcorner\varphi\urcorner)\urcorner)\Big)$$

$\mathsf{HPr}_T = \Box^0 \quad \mathsf{HCon}_T = \Diamond^0$
$\mathsf{HPr}^I_T = \Box \quad \mathsf{HCon}^I_T = \Diamond$

★ $T \vdash \Diamond^0\top \to (\Box\varphi \to \Diamond\Box\varphi)$

★ $T \vdash \mathbb{F} \leftrightarrow \neg\Box\,\mathbb{F}$

★ $T \vdash \varphi \;\Rightarrow\; T \vdash \Box\varphi$

★ $T \vdash \varphi \leftrightarrow \psi \;\Rightarrow\; T \vdash \Box\varphi \leftrightarrow \Box\psi$