Computer Science in Russia 2008

Topological Semantics of Justification Logic

Sergei Artemov and *Elena Nogina*

City University of New York

Moscow, June 9, 2008

Brouwer-Heyting-Kolmogorov (BHK) semantics.

- a proof of $A \wedge B$ consists of a proof of proposition A and a proof of proposition B,

- a proof of $A \vee B$ is given by presenting either a proof of A or a proof of B

- a proof of $A \rightarrow B$ is a construction transforming proofs of A into proofs of B

Gödel's modal logic of provability.

Gödel (1933) introduced the modal logic S4 as the system axiomatizing provability in classical mathematics:

Axioms and rules of classical propositional logic

$\Box(F \to G) \to (\Box F \to \Box G)$ *Normality*

$\Box F \to F$ *Reflexivity*

$\Box F \to \Box\Box F$ *Transitivity*

Necessitation Rule: $\dfrac{\vdash F}{\vdash \Box F}$

Gödel's translation $tr(F)$ of the propositional formula F in the intuitionistic language into the language of classical modal logic:

tr*(F) was obtained by prefixing every subformula of F with the provability modality* $\Box$.

Provides a proper embedding of the intuitionistic logic IPC into S4

Theorem [Gödel, McKinsey, Tarski]

IPC *proves F* $\Leftrightarrow$ S4 *proves tr(F).*

Still, Gödel's original goal of defining IPC in terms of classical provability was not reached, since the connection of S4 to the usual mathematical notion of provability was not established.

The situation after Gödel's paper of 1933 can be described by the following figure where '$\hookrightarrow$' denotes a proper embedding:

$$\text{IPC} \hookrightarrow \text{S4} \hookrightarrow \, ? \, \hookrightarrow \textit{CLASSICAL PROOFS} \, .$$

Provability semantics for modality

Gödel also considered the interpretation of $\Box F$ as

F is provable in Peano Arithmetic PA

and noticed that this semantics is inconsistent with S4.

Indeed, $\Box(\Box F \rightarrow F)$ can be derived in S4. On the other hand, interpreting $\Box$ as the predicate *Provable* of formal provability in Peano Arithmetic PA and F as *falsum* $\bot$, converts this formula into the false statement that the consistency of PA is internally provable in PA:

Provable (*Consis PA*) .

Gödel's paper left open two questions

1. What is the logic of formal provability *Provable*?

'**a provability semantics without a calculus**'

Was answered by Solovay (1976), who found the logic of formal provability GL.

2. What is the precise provability semantics for S4?

'**a provability calculus without a semantics**'

Was answered by the first author (1995) whose Logic of Proofs LP provided a semantics of explicit proofs for S4 and hence formalization of *BHK*-semanics for IPC.

Gödel's "explicit" format for provability

In his lecture in Vienna in 1938 Gödel mentioned a possibility of building an explicit version of S4 with basic propositions "t is a proof of F":

$$\textit{Proof}\,(t, F)$$

This Gödel's lecture remained unpublished until 1995. By that time the full Logic of Proofs was already discovered by the first author.

Logic of Proofs LP**: the language**

Proof polynomials are terms built from *proof variables* $x, y, z, \ldots$ and *proof constants* $a, b, c, \ldots$ by means of two binary operations: *application* '$\cdot$' and *choice* '$+$', and one unary *proof checker* '!'.

Using t to stand for any proof polynomial and S for any sentence letter, the **formulas of the Logic of Proofs** are defined by the grammar

$$A = S \mid A \rightarrow A \mid A \wedge A \mid A \vee A \mid \neg A \mid t{:}A \ .$$

Logic of Proofs LP

The standard axioms and rules of classical propositional logic

$t{:}(F \to G) \ \to\ (s{:}F \to (t\cdot s){:}G)$ *Application*

$t{:}F \ \to\ !t{:}(t{:}F)$ *Proof Checker*

$s{:}F \to (s+t){:}F, \quad t{:}F \to (s+t){:}F$ *Choice*

$t{:}F \to F$ *Reflexivity*

$\vdash c{:}A$, where A is an axiom and c is a proof constant

$-$ *Constant Specification Rule*

One of the basic properties of LP is its capability of internalizing its own derivations:
if

$$A_1, \ldots, A_n \vdash B \ ,$$

then for some proof polynomial $t(x_1, \ldots, x_n)$*,*

$$x_1{:}A_1, \ldots, x_n{:}A_n \vdash t(x_1, \ldots, x_n){:}B$$

Note that the Curry-Howard isomorphism covers only a simple instance of the proof internalization property where all of $A_1, \ldots, A_n, B$ are purely propositional formulas containing no proof terms.

Realization of S4 **in the Logic of Proofs** LP

S4 *is the forgetful projection of* LP, *i.e.,*

1. *The forgetful projection of* LP *is* S4*-compliant.*

2. *For each theorem* F *of* S4 *one can recover a witness (proof polynomial) for each occurrence of* $\Box$ *in* F *in such a way that the resulting formula* F^r *is derivable in* LP.

Realization gives a semantics of proofs for S4**.**

$$\mathsf{S4} \vdash F \quad \Leftrightarrow \quad \exists r\ \mathsf{LP} \vdash F^r$$

	Derivation in S4	Derivation in LP
1.	$\Box A \rightarrow \Box A \vee B$	$x{:}A \rightarrow x{:}A \vee B$
2.	$\Box(\Box A \rightarrow \Box A \vee B)$	$a{:}(x{:}A \rightarrow x{:}A \vee B)$
3.	$\Box\Box A \rightarrow \Box(\Box A \vee B)$	$!x{:}x{:}A \rightarrow (a \cdot !x){:}(x{:}A \vee B)$
4.	$\Box A \rightarrow \Box\Box A$	$x{:}A \rightarrow\ !x{:}x{:}A$
5.	$\Box A \rightarrow \Box(\Box A \vee B)$	$x{:}A \rightarrow (a \cdot !x){:}(x{:}A \vee B)$
6.	$B \rightarrow \Box A \vee B$	$B \rightarrow x{:}A \vee B$
7.	$\Box(B \rightarrow \Box A \vee B)$	$b{:}(B \rightarrow x{:}A \vee B)$
8.	$\Box B \rightarrow \Box(\Box A \vee B)$	$y{:}B \rightarrow (b \cdot y){:}(x{:}A \vee B)$
9.	$\Box A \vee \Box B \rightarrow \Box(\Box A \vee B)$	$x{:}A \vee y{:}B \rightarrow (???){:}(x{:}A \vee B)$

	Derivation in S4	Derivation in LP
1.	$\Box A \rightarrow \Box A \vee B$	$x{:}A \rightarrow x{:}A \vee B$
2.	$\Box(\Box A \rightarrow \Box A \vee B)$	$a{:}(x{:}A \rightarrow x{:}A \vee B)$
3.	$\Box\Box A \rightarrow \Box(\Box A \vee B)$	$!x{:}x{:}A \rightarrow (a\cdot !x){:}(x{:}A \vee B)$
4.	$\Box A \rightarrow \Box\Box A$	$x{:}A \rightarrow\ !x{:}x{:}A$
5.	$\Box A \rightarrow \Box(\Box A \vee B)$	$x{:}A \rightarrow (a\cdot !x){:}(x{:}A \vee B)$
5′.		$(a\cdot !x){:}(x{:}A \vee B) \rightarrow (a\cdot !x + b\cdot y){:}(x{:}A \vee B)$
5″.		$x{:}A \rightarrow (a\cdot !x + b\cdot y){:}(x{:}A \vee B)$
6.	$B \rightarrow \Box A \vee B$	$B \rightarrow x{:}A \vee B$
7.	$\Box(B \rightarrow \Box A \vee B)$	$b{:}(B \rightarrow x{:}A \vee B)$
8.	$\Box B \rightarrow \Box(\Box A \vee B)$	$y{:}B \rightarrow (b\cdot y){:}(x{:}A \vee B)$
8′.		$(b\cdot y){:}(x{:}A \vee B) \rightarrow (a\cdot !x + b\cdot y){:}(x{:}A \vee B)$
8″.		$y{:}B \rightarrow (a\cdot !x + b\cdot y){:}(x{:}A \vee B)$
9.	$\Box A \vee \Box B \rightarrow \Box(\Box A \vee B)$	$x{:}A \vee y{:}B \rightarrow (a\cdot !x + b\cdot y){:}(x{:}A \vee B)$

Provability semantics of LP

Interpretations respect Boolean connectives and

$$(p{:}F)^* \quad = \quad \mathit{Proof}(p^*, F^*).$$

Completeness theorem:
LP *derives all valid logical principles in its language*

The situation now can be described as

$$\mathrm{IPC} \hookrightarrow \mathrm{S4} \hookrightarrow \mathrm{LP} \hookrightarrow \mathit{CLASSICAL\ PROOFS}\ .$$

From Proofs to Justifications

Plato: **Knowledge $\sim$ Justified True Belief**

Hintikka, et al:

F **is known $\sim$ F holds in all possible situations.**

Simplified approach leaves Justification off the picture. It allowed to built an applicable formal theory of knowledge, but has had a number of deficiencies, e.g., the Logical Omniscience Problem.

Justification Logic (grows from LP):

F **is known** $\sim$ F **holds in all possible situations**
and there is an adequate evidence for F.

Joining Implicit and evidence-based knowledge.

A. & N., 2004:

$$\mathsf{S4LP} = \mathsf{S4} \quad + \quad \mathsf{LP} \quad + \quad (t{:}F \rightarrow \Box F) \qquad (\text{or } t{:}F \rightarrow \Box t{:}F).$$

Multiple systems combining implicit knowledge '$\Box F$' and evidence-based knowledge '$t{:}F$'. A mathematical definition of Logical Omniscience via proof complexity and a series of results showing that in Justification Logic implicit knowledge is logically omniscient whereas evidence-based knowledge is not logically omniscient.

Epistemic models for justifications (Fitting)

Model is $(W, R, \mathcal{E}, \Vdash)$, where

• (W, R) is an S4-frame;

• $\mathcal{E}$ is an evidence function: for each term t and formula F, $\mathcal{E}(t, F)$ is a set of $u \in W$ where t is a possible evidence for F. An evidence function is monotonic

$$uRv \text{ and } u \in \mathcal{E}(t, F) \text{ yield } v \in \mathcal{E}(t, F)$$

and has natural closure properties that agree with operations of LP.

• $u \Vdash t{:}F$ iff $u \Vdash \Box F$ and $u \in \mathcal{E}(t, F)$.

Topological models for S4 (Tarski)

Naturally extends the set-theoretical interpretation of classical propositional logic. Given a topological space $\mathcal{T} = \langle \mathbf{X}, \mathit{Interior} \rangle$ and a valuation (mapping) $*$ of propositional letters to subsets of $\mathbf{X}$, we can extend $*$ to all modal formulas as follows:

$$\neg A = \mathbf{X} \setminus A^*; \qquad (A \wedge B)^* = A^* \cap B^*;$$

$$(A \vee B)^* = A^* \cup B^*; \qquad (\Box A)^* = \mathit{Interior}(A)^*.$$

A is valid in $\mathcal{T}$ (notation: $\mathcal{T} \Vdash A$) if $A^* = \mathbf{X}$ for any valuation $*$.
The set $\mathbf{L}(\mathcal{T}) := \{A \mid \mathcal{F} \Vdash A\}$ is called the modal logic of $\mathcal{T}$.

McKinsey and Tarski Theorem:
Let $\mathcal{S}$ be a separable dense-in-itself metric space. Then $\mathbf{L}(\mathcal{S}) =$ S4.

Topological semantics for justifications - basic ideas

- based on Tarski's topological semantics $(\Box F)^* = \textit{Interior}(F)^*$

- t's denote **tests (measurements)**; there is a test function $\mathcal{M}$ that for each t and F specifies a set $\mathcal{M}(t,F)$ of 'possible outcomes' (not necessarily from F^*);

- $t{:}F$ $\sim$ '*a set where test t confirms F*'. This reading is supported by the definition
$$(t{:}F)^* \ = \ F^* \cap \mathcal{M}(t,F) \quad \text{or} \quad (t{:}F)^* \ = \ \textit{Interior}(F^*) \cap \mathcal{M}(t,F)$$
depending on a system

- first consider systems w/o operations on tests.

Basic Testing System $\mathsf{S4B}_0$

$$\mathsf{S4B}_0 \;=\; \mathsf{S4} \;+\; (x{:}F \rightarrow F).$$

In this system there are no any assumptions about tests; they don't even necessarily produce open sets of outcomes. The definition of the test assertion is

$$(x{:}F)^* \;=\; F^* \cap \mathcal{M}(x, F)$$

Robust Testing System $\mathsf{S4B}_1$

$$\mathsf{S4B}_1 \;=\; \mathsf{S4} \;+\; (x{:}F \rightarrow \Box F).$$

In this system, the test sets are still arbitrary (not necessarily open); however, the test assertions are interpreted as

$$(x{:}F)^* \;=\; \textit{Interior}(F^*) \cap \mathcal{M}(x, F)$$

Robust Testing System $\mathsf{S4B}_1$

$$\mathsf{S4B}_2 \;=\; \mathsf{S4} \;+\; (x{:}F \rightarrow F) \;+\; (x{:}F \rightarrow \Box x{:}F).$$

This system corresponds to the full operation-free version of S4LP. The test sets are open, the test assertions are interpreted as

$$(x{:}F)^* \;=\; \textit{Interior}(F^*) \cap \mathcal{M}(x, F)$$

Soundness and Completeness

All three systems $S4B_0$, $S4B_1$, and $S4B_2$ are sound and complete with respect to the corresponding classes of topological models. The soundness proofs are straightforward. Completeness proofs go via epistemic models which are then converted into topological spaces with cone topology.

Soundness and Completeness

Theorem. $\mathsf{S4B}_0$, $\mathsf{S4B}_1$, $\mathsf{S4B}_2$ *are complete with respect to the real topology* $\mathbb{R}^n$, *for each* $n = 1, 2, 3, ...$

Main lemma (Slavnov, Bezhanishvili, Gehrke, Mints, Zhang)
There is an open and continuous map π *from* $(0, 1)$ *onto the Kripke topological space corresponding to a finite rooted Kripke frame.*

Such a map π preserves truth values of modal formulas at the corresponding points. It now suffices to produce a finite rooted Fitting counter-model for a given formula F and define the test function $\mathcal{M}'(t, G)$ on $(0, 1)$ as

$$\mathcal{M}'(t, G) = \pi^{-1}\mathcal{M}(t, G).$$

The resulted topological model is a $(0, 1)$-countermodel for F. This construction yields completeness with respect to the real topology $\mathbb{R}^n$, for each $n = 1, 2, 3, ...$

Introducing operations

A natural topological interpretation for the whole of S4LP.

Operation	Test Function
$t{:}(F \rightarrow G) \;\rightarrow\; (s{:}F \rightarrow (t\cdot s){:}G)$	$\mathcal{M}(s, F \rightarrow G) \cap \mathcal{M}(t, F) \subseteq \mathcal{M}(s\cdot t, G)$
$t{:}F \;\rightarrow\, !t{:}(t{:}F)$	$\mathcal{M}(t, F) \subseteq \mathcal{M}(!t, t{:}F)$
$s{:}F \vee t{:}F \rightarrow (s+t){:}F$	$\mathcal{M}(s, F) \cup \mathcal{M}(t, F) \subseteq \mathcal{M}(s+t, F)$

Conclusions

Justification logics can be provided with a topological semantics which reads justification assertions $t{:}F$ as

test t supports F.

This semantics is a natural extension of the Tarski topological semantics for the modal logic S4.