2007

TR-2007016: Symmetric Logic of Proofs

Sergei Artemov

Symmetric Logic of Proofs*

Sergei Artemov

CUNY Graduate Center
365 Fifth Avenue, New York, NY 10016
sartemov@gc.cuny.edu

September 7, 2007

Abstract

The Logic of Proofs LP captures the invariant propositional properties of proof predicates *t is a proof of F* with a set of operations on proofs sufficient for realizing the whole modal logic S4 and hence the intuitionistic logic IPC. Some intuitive properties of proofs, however, are not invariant and hence not present in LP. For example, the choice function '+' in LP, which is specified by the condition $s{:}F \vee t{:}F \to (s+t){:}F$, is not necessarily symmetric. In this paper, we introduce an extension of the Logic of Proofs, SLP, which incorporates natural properties of the standard proof predicate in Peano Arithmetic:

t is a code of a derivation containing F,

including the symmetry of Choice. We show that SLP produces Brouwer-Heyting-Kolmogorov proofs with a rich structure, which can be useful for applications in epistemic logic and other areas.

1 Introduction

In [15], Gödel used the modal logic S4 to axiomatize classical provability and provide the formal provability semantics to the intuitionistic propositional logic IPC by reducing IPC to S4. The question of the provability semantics of S4 itself was left open and found its resolution in [1; 2] via the Logic of Proofs LP[1] which provided a complete axiomatization of the proof predicate

t is a proof of F

*Dedicated to B.A. Trakhtenbrot on the occasion of his 85'th birthday. To appear in the LNCS Festschrift series.

[1]The first (incomplete) sketch of the logic of proofs was given by Gödel in one of his lectures of 1938 [16]. This lecture was published only in 1995; by that time, the complete system LP for the Logic of Proofs had already been discovered and shown to provide a desired provability semantics for intuitionistic logic (cf. [1; 2]).

in a propositional language with a sufficiently rich system of operations on proofs. On the other hand, LP can realize every S4 derivation by recovering corresponding proof terms at every occurrence of the modality (the Realization Theorem from [1; 2], cf. Theorem 1). The combination of these two features renders LP a bridge between intuitionistic logic and the realm of formal mathematical proofs in the style of Brouwer-Heyting-Kolmogorov:

$$\mathsf{IPC} \hookrightarrow \mathsf{S4} \hookrightarrow \mathsf{LP} \hookrightarrow \textit{Gödelian proof predicates}.$$

In this diagram, $\mathsf{IPC} \hookrightarrow \mathsf{S4}$ denotes Gödel's faithful embedding of IPC into S4 [15], $\mathsf{S4} \hookrightarrow \mathsf{LP}$ signifies the Realization Theorem which faithfully embeds S4 into LP [1; 2], and $\mathsf{LP} \hookrightarrow$ *Gödelian proof predicates* refers to the arithmetical soundness (and completeness) theorem ([1; 2]) for the Logic of Proofs. We refer the reader to [2] and surveys [6; 7] for detailed discussion of these matters.

2 LP Basics

The Logic of Proofs has three basic operations on proofs: *Application* '$\cdot$' (binary), *Choice* '$+$' (binary), and *Proof Checker* '!'(unary). *Proof polynomials* are terms built by these operations from *proof variables* $x, y, z, \ldots$ and *proof constants* $a, b, c, \ldots$. The formulas of LP are defined by the grammar

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

where t stands for any proof polynomial and S for any sentence letter. As usual, we shorten $s \cdot t$ to st when convenient. The binding priority from strong to weak is $!,\ \cdot,\ +,\ :, \neg, \wedge, \vee, \to$. In particular, $t(u+v){:}F \to tu{:}F \vee tv{:}F$ denotes

$$\{[t \cdot (u+v)]{:}F\} \to \{[(t \cdot u){:}F] \vee [(t \cdot v){:}F]\}.$$

The postulates of the Logic of Proofs LP are

1. a fixed set of axioms for classical propositional logic with *Modus Ponens* as its only rule of inference, e.g., the set from [18];
2. $s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G)$ (*Application*);
3. $t{:}F \to !t{:}(t{:}F)$ (*Proof Checker*);
4. $s{:}F \to (s+t){:}F, \quad t{:}F \to (s+t){:}F$ (*Choice*);
5. $t{:}F \to F$ (*Reflection*);
6. *Constant Specification Rule: If c is a proof constant and A is an axiom from 1-5, then infer $c{:}A$.*

LP is closed under substitutions of proof polynomials for proof variables and formulas for propositional variables, and enjoys the deduction theorem.

Constant Specification CS is a set of formulas $\{c_1{:}A_1, c_2{:}A_2, \ldots\}$ where each A_i is an axiom and each c_i is a proof constant. Each derivation in LP naturally generates a (finite) constant specification CS introduced in this derivation by the Constant Specification Rule. By LP_{CS}, we mean a subsystem of LP where

the Constant Specification Rule is only allowed to produce formulas from a given constant specification CS. If CS contains all formulas $c{:}A$ where A is an axiom and c is a proof constant, then LP_{CS} is LP itself.

The principal feature of the Logic of Proofs is the Internalization Principle[2] which states that

$$\textit{whenever} \vdash F\textit{, there is a proof polynomial } p \textit{ such that} \vdash p{:}F,$$

which is nothing more than the explicit version of the modal Necesitation Rule

$$\frac{\vdash F}{\vdash \Box F.}$$

The following Theorem 1 discloses a connection between the Logic of Proofs LP and Gödel's provability logic $\mathsf{S4}$; this result has been crucial for providing intuitionistic logic with the intended Brouwer-Heyting-Kolmogorov semantics of proofs. This theorem shows that the provability modality in $\mathsf{S4}$ can indeed be read as

$$\Box F \quad = \quad \textit{there is proof of } F$$

using the language of Skolem-style operations on proofs rather than quantifiers. For example, a sentence

$$\Box F \ \rightarrow \ \Box G$$

in the logic of formal provability[3] reads as

$$\exists x(\textit{`x is a proof of F'}) \ \rightarrow \ \exists y(\textit{`y is a proof of G'}),$$

whereas, by the Realization Theorem, this reads as an LP sentence

$$x{:}F \ \rightarrow \ t(x){:}G,$$

for an appropriate proof polynomial $t(x)$.

The usual Skolemization does not work for quantifiers on proofs, and a totally new technique has been invented here.

Theorem 1 [Realization Theorem for LP ([1; 2])] *There is an algorithm which, given* $\mathsf{S4} \vdash F$*, substitutes each occurrence of the modality in* F *by an appropriate proof polynomial such that the resulting formula* F^r *is derivable in* LP*. Moreover, such a realization can be made in a way that respects Skolem-style reading of* $\Box X$ *as 'there is a proof of X': each negative occurrence of* $\Box$ *can be realized by a proof variable, and each positive occurrence of* $\Box$ *is realized by a proof polynomial depending of those variables.*

The size of realizing proof polynomials can be limited by a quadratic function in the length of a cut-free derivation of F in $\mathsf{S4}$ ([12]). A semantical proof of the Realization theorem which is not based on cut-elimination in $\mathsf{S4}$ was suggested in [14]. R. Kuznets in [12] showed that $\mathsf{S4}$ cannot be realized in LP without using self-referential proof assertions of the sort $t{:}F(t)$.

[2] In his brief sketch of the logic of proofs in [16], Gödel cited the Internalization Principle as one of its features.

[3] This approach led to the well-known Provability Logic GL (cf. [11; 27]).

Corollary 1 S4 *is the forgetful projection of* LP.

Proof. It is straightforward that the forgetful projection of LP is S4-compliant; it suffices to notice that the forgetful projections of all axioms of LP are provable in S4 and the rules of LP are S4-sound. By Theorem 1, every theorem of S4 is a forgetful projection of some LP-theorem. □

3 Symmetric Provability Interpretation

The intended provability semantics of LP is given by interpreting $t{:}F$ as the arithmetical proof predicate

$$t \textit{ is a proof of } F,$$

where 'proofs' are understood in a multi-conclusional way, i.e., a proof can yield more than one theorem (think of a Hilbert-style proof sequence that proves all formulas occurring in this sequence).

A body of work in this area shows that proof realization of modality necessarily requires the multi-conclusion reading of proof predicates. What follows is a light informal argument which hints at what is going on. Imagine a variant $\mathcal{LP}$ of the logic of proofs capable of realizing S4. Then $\mathcal{LP}$ should be able to realize the modality in an easy S4 theorem $\Box A$ where A is a propositional modal-free axiom (e.g., $P \to (Q \to P)$ for propositional letters P and Q). Such a realization should be of the form $t{:}A$ for some proof term t and $\mathcal{LP} \vdash t{:}A$. Assume that $\mathcal{LP}$ is closed under the substitution of propositional formulas for propositional letters; all provability logics have this feature since they describe schemas valid under all arithmetical interpretations, and this property survives substitution. Let A' be a substitutional instance of A, syntactically different from the latter. By the substitution closure, $\mathcal{LP} \vdash t{:}A'$. Hence $\mathcal{LP} \vdash t{:}A \wedge t{:}A'$ and t represents a proof of two different theorems.

Moreover, the logic of single-conclusion proofs contains some principles which are inconsistent with modal logic. For example (cf. [2]), the principle $\neg(x{:}\top \wedge x{:}(\top \wedge \top))$ is valid for single-conclusion proofs whereas its natural modal language presentation via the 'forgetful projection,' $\neg(\Box\top \wedge \Box(\top \wedge \top))$, is false in any modal logic. The logic of single-conclusion proofs has been axiomatized in [10] (without operations) and in [20; 21] (with the operations Application and Proof Checker[4]). For further progress in this direction cf. [22].

In the context of the Logic of Proofs, one has to consider the whole class of proof predicates and axiomatize only invariant properties, i.e., those that hold for all proof predicates (from a given class). There is a good reason for this. The language of the Logic of Proofs is rather expressive and captures individual properties of proofs which should not count as general logic laws. For example, the formula $x : (\top \wedge \top) \to x : \top$ claims that any (multi-conclusion) proof of

[4]The operation Choice '+' is incompatible with single-conclusion proof semantics

the conjunction $\top \wedge \top$ should prove $\top$ as well. Apparently, this 'principle' is not invariant since by changing an axiom system, one can obtain two proof predicates in which this formula both holds and does not hold, respectively.

The soundness and completeness theorems from [1; 2] state that the Logic of Proofs LP captures exactly all invariant properties of multi-conclusion proof predicates with natural computable operations on proofs corresponding to Application, Proof Checker, and Choice[5]. We refer the reader to [3; 6; 7] for more details.

In the rest of this section, we introduce a symmetric version of the standard provability semantics for the Logic of Proofs which differs slightly from the one given in [2], § 6 and is more convenient for revealing the natural structure of proof operations.

Consider the proof predicate $PROOF(x, y)$ for Peano Arithmetic PA which is a natural arithmetical formalization of the usual Hilbert-style definition of proofs:

x is a number of a proof sequence which contains a formula with a number y .

An interpretation of the language of LP maps propositional letters to sentences of PA, and proof variables and constants to Gödel numbers of Hilbert-style proofs in PA. This is the only difference between the symmetric semantics and the standard provability semantics from [2], § 6, where proof variables and constants are mapped to arbitrary natural numbers, and not necessarily the codes of PA-derivations. Note that each proof sequence in PA is a complete proof of each sentence occurring within it.

For the proof predicate $PROOF(x, y)$, $s{\cdot}t$ can be interpreted as the operation which concatenates the codes of proofs corresponding to s and t and adds to the right all formulas G such that for some F, $F \to G$ and F occur in s and t respectively.

Here is a more formal description. Let s', t', ... denote arithmetical interpretations of s, t, etc., i.e., Gödel numbers of Hilbert-style proofs in PA. Let also $*$ denote the concatenation on Gödel numbers of finite sequences. Then we define

$$(s \cdot t)' = s' * t' * \ulcorner G_1 \urcorner * \ldots * \ulcorner G_n \urcorner \tag{1}$$

where $\ulcorner G_1 \urcorner, \ldots, \ulcorner G_n \urcorner$ are Gödel numbers of single-formula sequences for each G_i for which there exists F such that $F \to G_i$ and F are in the proofs with the numbers s' and t' respectively. For example, if $s' = \ulcorner F \to G \urcorner$ and $t' = \ulcorner F \urcorner$, then

$$(s \cdot t)' = \ulcorner F \to G \urcorner * \ulcorner F \urcorner * \ulcorner G \urcorner, \qquad (t \cdot s)' = \ulcorner F \urcorner * \ulcorner F \to G \urcorner.$$

The Choice operation $s{+}t$ can be interpreted as the concatenation of proof sequences corresponding to s and t respectively:

$$(s + t)' = s' * t'. \tag{2}$$

[5] E. Goris suggested in [17] a natural interpretation of LP in Bounded Arithmetic where all of these operations are PTIME-computable.

The Proof Checker is a primitive recursive operation that takes a proof t and, for each F such that $t{:}F$ holds, produces a proof of all such $t{:}F$'s; such an operation can be traced back to the proof of Gödel's Second Incompleteness Theorem (cf. [26]).

We call $PROOF(x, y)$ with operations (1), (2), and Proof Checker as above the *symmetric arithmetical semantics of the Logic of Proofs*.

We can see that within the standard semantics, the Choice function is symmetric:

$$(s{+}t){:}F \leftrightarrow (t{+}s){:}F;$$

moreover, it satisfies the principles

$$(s{+}t){:}F \leftrightarrow s{:}F \vee t{:}F,$$
$$u(s{+}t){:}F \leftrightarrow (us{+}ut){:}F,$$
$$(s{+}t)u{:}F \leftrightarrow (su{+}tu){:}F.$$

None of these principles is derivable in LP. The point is that these principles are not invariant! For example, one can easily devise an interpretation where $(s{+}t){:}F \to s{:}F \vee t{:}F$ does not hold. Indeed, interpret $s{+}t$ and $s \cdot t$ as follows:

$$(s \cdot t)^\sharp = s^\sharp * t^\sharp * {\ulcorner G_1 \urcorner} * \ldots * {\ulcorner G_n \urcorner},$$

as in (1), and

$$(s + t)^\sharp = (s \cdot t)^\sharp.$$

It is clear that $s{:}F \vee t{:}F \to (s{+}t){:}F$ holds, since $(s{+}t)^\sharp$ contains the concatenation of $s^\sharp$ and $t^\sharp$. However, $(s + t)^\sharp$ and $(t + s)^\sharp$ can very well prove different sets of theorems, cf. an example about $(s \cdot t)'$ and $(t \cdot s)'$ above. In this case, neither $(s + t){:}F \leftrightarrow (t + s){:}F$ nor $(s + t){:}F \leftrightarrow s{:}F \vee t{:}F$ holds.

Under yet another interpretation:

$$(s \cdot t)^\flat = s^\flat * t^\flat * {\ulcorner G_1 \urcorner} * \ldots * {\ulcorner G_n \urcorner},$$

as in (1), and

$$(s + t)^\flat = (s \cdot t)^\flat * (t \cdot s)^\flat.$$

Choice '+' becomes symmetric,

$$(s{+}t){:}F \leftrightarrow (t{+}s){:}F,$$

but $(s + t){:}F \to s{:}F \vee t{:}F$ generally does not hold.

4 Justification and Epistemic Semantics

A formal justification semantics for LP was offered by Mkrtychev in [25]. This helped to establish the decidability of LP ([25]), find complexity bounds ([23; 24]), and establish the disjunctive property of LP ([19]).

A Mkrtychev model is a pair $M = (\mathcal{A}, \Vdash)$, where

- $\Vdash$ is the usual truth evaluation of propositional letters;
- $\mathcal{A}$ is an *admissible evidence* predicate $\mathcal{A}(t, F)$ defined on pairs *(term, formula)*. The intuition behind $\mathcal{A}$ is that $\mathcal{A}(t, F)$ means

  $$t \textit{ is an admissible evidence for } F.$$

  The admissible evidence predicate respects operations on proofs, i.e., $\mathcal{A}$ satisfies the natural closure conditions copied from the axioms of LP:

  Application: $\mathcal{A}(s, F \to G)$ and $\mathcal{A}(t, F)$ implies $\mathcal{A}(s \cdot t, G)$;

  Proof Checker: $\mathcal{A}(t, F)$ implies $\mathcal{A}(!t, t{:}F)$;

  Choice: $\mathcal{A}(s, F)$ or $\mathcal{A}(t, F)$ implies $\mathcal{A}(s + t, F)$.

Given a model, the truth relation $\Vdash$ is extended to all formulas by stipulating that

- $\Vdash$ respects classical Boolean connectives;
- $\Vdash t{:}F$ iff '$\Vdash F$ and $\mathcal{A}(t, F)$.'

For a given constant specification CS, a model $M = (\mathcal{A}, \Vdash)$ is a *CS-model* iff $\mathcal{A}(c, B)$ holds for any $c{:}B \in CS$. It is an easy exercise to check, by induction on derivations in LP_{CS}, the soundness of LP with respect to Mkrtychev semantics:

$$\textit{If } \mathsf{LP}_{CS} \vdash F\textit{, then } F \textit{ holds in each } CS\textit{-model.}$$

In particular, all formulas from CS are true in all CS-models.

We present here a different (from that shown in [25]) proof of the completeness theorem for LP with respect to Mkrtychev models by the standard maximal completeness sets construction. Let W be the collection of all maximal consistent sets over LP_{CS}. For each $\Gamma \in W$, we define the truth relation $\Vdash_\Gamma$ on propositional letters as

$$\Vdash_\Gamma p \quad \textit{iff} \quad p \in \Gamma$$

and the admissible evidence predicate as

$$\mathcal{A}_\Gamma(t, F) \quad \textit{iff} \quad t{:}F \in \Gamma \ .$$

The aforementioned closure conditions on $\mathcal{A}_\Gamma$ are obviously met. Let us check *Choice*. Suppose $\mathcal{A}_\Gamma(s, F)$ holds. Then $s{:}F \in \Gamma$. Since $s{:}F \to (s+t){:}F \in \Gamma$ (as an LP-axiom) and Γ is maximal consistent, $(s+t){:}F \in \Gamma$, too. Hence $\mathcal{A}_\Gamma(s+t, F)$. Moreover, $c{:}B \in \Gamma$ for all $c{:}B$ from CS, by maximality and consistency of Γ. Therefore, for each Γ, $M = (\mathcal{A}_\Gamma, \Vdash_\Gamma)$ is an LP_{CS}-model.

The next step is to establish the Truth Lemma: *for each formula F,*

$$\Vdash_\Gamma F \quad \textit{iff} \quad F \in \Gamma.$$

Induction on F. The base case is given by the definition of the model. The Boolean cases are straightforward. Consider the case when F is $t{:}G$. If $t{:}G \in \Gamma$,

then $G \in \Gamma$ as well, since $t{:}G \to G \in \Gamma$ and Γ is deductively closed. By the induction hypothesis, $\Vdash_\Gamma G$. Moreover, $\mathcal{A}_\Gamma(t, G)$ also holds, by the definition of $\mathcal{A}_\Gamma$. Hence $\Vdash_\Gamma t{:}G$.

Now let $t{:}G \notin \Gamma$. Then $\mathcal{A}_\Gamma(t, G)$ does not hold, by the definition. Hence $\not\Vdash_\Gamma t{:}G$.

To finish the completeness theorem, it suffices to note that if $\mathsf{LP}_{CS} \not\vdash F$, then $\{\neg F\}$ is a consistent set. By the standard Lindenbaum construction, find its maximal consistent extension Γ. Since $\neg F \in \Gamma$, $F \notin \Gamma$. By the Truth Lemma, for $\mathcal{A}_\Gamma$ and $\Vdash_\Gamma$, $\not\Vdash_\Gamma F$.

There are several useful refinements of Mkrtychev semantics known:

1. Exact Evidence Model ([25]): *For every model $M = (\mathcal{A}, \Vdash)$, there is a model $M' = (\mathcal{A}', \Vdash')$ such that*
   - *M and M' are equivalent, i.e., for each F, $\Vdash F$ iff $\Vdash' F$;*
   - *$\mathcal{A}'$ is exact, i.e., $\mathcal{A}'(t, F)$ iff $\Vdash' t{:}F$.*
2. Minimal Model ([19]): *For each constant specification CS, there is an exact evidence model $M = (\mathcal{A}, \Vdash)$ such that for each $t{:}F$, $M \Vdash t{:}F$ iff $\mathsf{LP}_{CS} \vdash t{:}F$.*

The minimal model theorem yields the Disjunctive Property ([19]):

$$\mathsf{LP}_{CS} \vdash s{:}F \vee t{:}G \text{ iff } (\mathsf{LP}_{CS} \vdash s{:}F \text{ or } \mathsf{LP}_{CS} \vdash t{:}G).$$

An epistemic Kripke-style semantics for LP was offered by Fitting [13; 14]. A Fitting model may be regarded as a Kripke model, each node of which is a Mkrtychev model with a monotone admissible evidence function:

$$\text{if } uRv \text{ then } \mathcal{A}_u \subseteq \mathcal{A}_v.$$

The new condition which specifies the truth of proof assertions at a given node is as follows

$$u \Vdash t{:}F \quad \text{iff} \quad \mathcal{A}_u(t, F) \text{ holds and } v \Vdash F \text{ for every } v \text{ with } uRv.$$

Proper modifications of Fitting semantics can accommodate multiple modalities and proof assertions and are playing a key role connecting the Logic of Proofs with epistemic modal logics ([4; 5; 8; 9]).

5 Choice Function '+' in LP

The operation '+' which is called *Choice, Union, Sum,* or *Plus* indeed performs something which can be described as *choice*. The behavior of '+' is governed by the logical principle

$$s{:}F \vee t{:}F \to (s+t){:}F,$$

which states that '+' takes two proofs s and t, at least one of which is indeed a proof of F, and produces the output $s+t$, which is a proof of F. 'Under the hood,' this operation chooses a proof of F between s and t.

The following theorem was established in [19]; it showed that the Choice operation in LP is weakly symmetric and weakly equivalent to a disjunction.

Theorem 2 [19] *For any constant specification CS, the following are equivalent:*

1. $\mathsf{LP}_{CS} \vdash (s+t){:}F$
2. $\mathsf{LP}_{CS} \vdash (t+s){:}F$
3. $\mathsf{LP}_{CS} \vdash s{:}F \vee t{:}F$.

Theorem 3 below shows that none of these properties hold in LP in a strong sense, i.e., internally.

Theorem 3 *Let x,y be proof variables and P a propositional letter. Then*

1. $\mathsf{LP} \nvdash (x+y){:}P \to (y+x){:}P$
2. $\mathsf{LP} \nvdash (x+y){:}P \to x{:}P \vee y{:}P$
3. $\mathsf{LP} \nvdash x(y+z){:}P \to (xy+xz){:}P$
4. $\mathsf{LP} \nvdash (y+z)x{:}P \to (yx+zx){:}P$.

Proof. In principle, these statements could be proven by proper use of the arithmetical counterexamples. However, since not all details about the provability semantics of LP were given there, we present a proof based on Mrktychev models.

To establish (1), consider a Mkrtychev model $M = (\mathcal{A}, \Vdash)$ where $\Vdash P$ and $\mathcal{A}(t, F)$ holds iff t is different from x, y, and $y + x$. To verify that M is a legitimate model, it suffices to check the closure properties of $\mathcal{A}$. The only relevant case is *Choice* in a configuration when $\mathcal{A}(y+x, G)$ does not hold. In this situation, neither $\mathcal{A}(y, G)$ nor $\mathcal{A}(x, G)$ holds, which does not constitute a violation of the closure property of $\mathcal{A}$. It is easy to see that in this model, $\Vdash (x+y){:}P$ since both $\mathcal{A}(x+y, P)$ and $\Vdash P$ hold. On the other hand, $\nVdash (y+x){:}P$ since $\mathcal{A}(y+x, P)$ does not hold. Overall,

$$\nVdash (x+y){:}P \to (y+x){:}P.$$

Item (2) immediately follows from (1) since $\mathsf{LP} \vdash x{:}P \vee y{:}P \to (y+x){:}P$.

Item (3). Similar to 1. Consider a Mkrtychev model $M = (\mathcal{A}, \Vdash)$ where $\Vdash P$ and $\mathcal{A}(t, F)$ holds iff t is different from any subterm of $xy+xz$, i.e., $t \notin \{xy+xz,\ xy,\ xz,\ x,\ y,\ z\}$. The closure property holds since in all applicable clauses when $\mathcal{A}$ can be false in the conclusion, the assumptions are also false, by the definition of $\mathcal{A}$. In this model, $x(y+z){:}P$ is true since $x(y+z)$ is not a subterm of $xy+xz$, but $(xy+xz){:}P$ is false.

Item(4) can be treated similarly to (3). □

6 Symmetric Logic of Proofs

As we have already discussed, the Logic of Proofs LP has two prominent features which determine its foundational significance: it has a natural provability semantics[6], and it suffices for realizing S4, hence IPC, thus making LP a kind of Brouwer-Heyting-Kolmogorov semantics for intuitionistic logic.

In this chapter, we introduce the *Symmetric Logic of Proofs*, SLP, extending LP itself by postulating a property borrowed from the symmetric arithmetical interpretation.

SLP has all the postulates of LP and one additional principle:

Symmetry Principle:

$$t(u{+}v){:}F \leftrightarrow tu{:}F \vee tv{:}F, \tag{3}$$

$$(u{+}v)t{:}F \leftrightarrow ut{:}F \vee vt{:}F. \tag{4}$$

Notational conventions: we assume that this principle also covers the case when there is no multiplication by t at all, i.e.

$$(u{+}v){:}F \leftrightarrow u{:}F \vee v{:}F. \tag{5}$$

With this convention, the Symmetry Principle subsumes the Choice Axiom of LP and hence may be considered a generalization of the latter.

Clearly,

$$\mathsf{LP} \quad \subset \quad \mathsf{SLP}.$$

Theorem 4 SLP *is sound with respect to the symmetric provability interpretation.*

Proof. We have to establish soundness of the Symmetry Principle.

Let us start with $tu{:}F \vee tv{:}F \to t(u{+}v){:}F$. Fix the (symmetric arithmetical) interpretation t', u', v', F' of s, u, v, and F respectively and suppose that $(tu{:}F)'$ holds. By the definition of the symmetric arithmetical interpretation, at least one of the following cases holds:

1. $F' \in t'$;
2. $F' \in u'$;
3. there is X such that $X \to F' \in t'$ and $X \in u'$.

In cases (1) and (2), $F' \in [t(u{+}v)]'$, by the definition of the symmetric arithmetical interpretation. In case (3), $X \in u' * v'$, hence $X \in (u+v)'$, hence $F' \in [t(u{+}v)]'$ as well. The case when $[tv{:}F]'$ holds is symmetric.

Let us examine $t(u+v) : F \to tu : F \vee tv : F$. Suppose $F' \in [t(u+v)]'$. By the definition of the symmetric arithmetical interpretation, at least one of the following cases holds:

[6] Moreover, LP provides a complete axiomatization of the class of all multi-conclusion proof predicates.

1. $F' \in t'$;

2. $F' \in (u+v)'$, i.e., $F' \in u' * v'$;

3. there is X such that $X \to F' \in t'$ and $X \in u' * v'$.

In case (1), both $(tu{:}F)'$ and $(tv{:}F)'$ hold. In case (2), either $F' \in u'$, and then $(tu{:}F)'$, or $F' \in v'$, and then $(tv{:}F)'$. In case (3), either $X \in u'$, hence $(tu{:}F)'$; or $X \in v'$, hence $(tv{:}F)'$. In any case, $(tu{:}F \vee tv{:}F)'$ holds.

The cases $ut{:}F \vee vt{:}F \leftrightarrow (u+v)t{:}F$ and $u{:}F \vee v{:}F \leftrightarrow (u+v){:}F$ are treated similarly. □

Theorem 5 SLP *is closed under substitution and enjoys the Internalization Property.*

Proof. Trivial from the definition of SLP and the fact that no new rules of inference were added to SLP as compared to LP. □

Theorem 6 SLP *enjoys the Realization Theorem with respect to* S4*.*

Proof. Indeed, suppose F is derivable in S4. By the Realization Theorem for LP (Theorem 1), there is a realization of F, F^r by proof polynomials in the basis $\{\cdot, +, !\}$ which is derivable in LP. Since SLP extends LP, SLP $\vdash F^r$. □

Theorem 7 S4 *is the forgetful projection of* SLP*.*

Proof. It suffices to note that the Symmetry Principle has forgetful projections of the sort $\Box X \leftrightarrow \Box X \vee \Box X$, trivially provable in S4. By Theorem 6, every theorem of S4 is a forgetful projection of some SLP-theorem. □

These results, along with the provability semantics for SLP, show that the latter gives a Brouwer-Heyting-Kolmogorov-style semantics for S4 and IPC as well.

$$\text{IPC} \hookrightarrow \text{S4} \hookrightarrow \text{SLP} \hookrightarrow \textit{Gödelian proof predicates.}$$

Theorem 8 *Let CS be a constant specification. Let $s \sim t$ mean that for any formula F, $s{:}F \leftrightarrow t{:}F$ is provable in* SLP *with this CS. Then the following holds:*

1. $s + t \sim t + s$ *(commutativity of Choice);*

2. $s + (t + u) \sim (s + t) + u$ *(associativity of Choice);*

3. $s + s \sim s$ *(idempotency of Choice);*

4. $t(u + v) \sim tu + tv$ *(left distributivity);*

5. $(u + v)t \sim ut + vt$ *(right distributivity).*

Proof. All the derivations are in SLP.

1. $(s+t){:}F \;\rightarrow\; s{:}F \vee t{:}F \;\rightarrow\; t{:}F \vee s{:}F \;\rightarrow\; (t+s){:}F$
2. $[s+(t+u)]{:}F \;\leftrightarrow\; s{:}F \vee t{:}F \vee u{:}F \;\leftrightarrow\; [(s+t)+u]{:}F$
3. $(s+s){:}F \;\leftrightarrow\; s{:}F \vee s{:}F \;\leftrightarrow\; s{:}F$
4. $t(u+v){:}F \;\leftrightarrow\; tu{:}F \vee tv{:}F \;\leftrightarrow\; tu+tv{:}F$
5. $(u+v)t{:}F \;\leftrightarrow\; ut{:}F \vee vt{:}F \;\leftrightarrow\; ut+vt{:}F$

□

Mkrtychev models for SLP are the usual Mkrtychev LP-models with admissible evidence predicates which respect the Symmetry Principle:

$$\mathcal{A}(t(u+v),F) \quad \textit{iff} \quad \text{`}\mathcal{A}(tu,F) \textit{ or } \mathcal{A}(tv,F)\text{'} \tag{6}$$

$$\mathcal{A}((u+v)t,F) \quad \textit{iff} \quad \text{`}\mathcal{A}(ut,F) \textit{ or } \mathcal{A}(vt,F)\text{'} \tag{7}$$

$$\mathcal{A}(u+v,F) \quad \textit{iff} \quad \text{`}\mathcal{A}(u,F) \textit{ or } \mathcal{A}(v,F).\text{'} \tag{8}$$

Theorem 9 *For each constant specification CS,* SLP *is sound and complete for* SLP *Mkrtychev models.*

Proof. Soundness of SLP is straightforward. We have only to check that Symmetry holds in each SLP-model. Let us consider (3). Let $\Vdash t(u{+}v){:}F$. Then $\Vdash F$ and $\mathcal{A}(t(u{+}v),F)$. By (6), $\mathcal{A}(tu,F)$ holds or $\mathcal{A}(tv,F)$ holds, hence $\Vdash tu{:}F$ or $\Vdash tv{:}F$. In either case, $\Vdash tu{:}F \vee tv{:}F$. The remaining clauses for soundness are checked in the same manner.

Completeness can be established by a maximal consistent set construction as in Section 4. One need only check that the canonical model (the set of maximal consistent sets with $\mathcal{A}$ and $\Vdash$ as in Section 4) is indeed an SLP-model. For this, is suffices to check that for each maximal consistent set Γ, conditions (6), (7), and (8) hold. Let us check (6).

Suppose $\mathcal{A}(t(u+v),F)$ holds for this Γ. This means that $t(u{+}v){:}F \in \Gamma$. Since $t(u{+}v){:}F \rightarrow tu{:}F \vee tv{:}F \in \Gamma$, by maximality of Γ, either $tu{:}F \in \Gamma$ or $tv{:}F \in \Gamma$, hence '$\mathcal{A}(tu,F)$ *or* $\mathcal{A}(tv,F)$' holds for this Γ.

Now let '$\mathcal{A}(tu,F)$ *or* $\mathcal{A}(tv,F)$' hold in Γ. Then either $tu{:}F \in \Gamma$ or $tv{:}F \in \Gamma$. By the Symmetry Principle (3), since Γ is deductively closed, $t(u{+}v){:}F \in \Gamma$, which yields that $\mathcal{A}(t(u+v),F)$ holds for this Γ.

The remaining clauses are checked similarly. □

Fitting models for SLP are obtained from those for LP by adding conditions (6), (7), and (8), respectively. The following theorem can be easily established along the lines of Theorem 9:

Theorem 10 *For each constant specification CS,* SLP *is sound and complete for* SLP *Fitting models.*

7 Discussion

Note that Application in SLP is neither associative nor commutative since neither of these properties hold for the symmetric arithmetical interpretation (Section 3).

A natural attempt to add more ring structure to SLP by introducing a constant 0 for the empty derivation does not work well with the symmetric provability interpretation. In particular, $t + 0 = t$, but $t \cdot 0$ is t rather than 0 here[7]. This could be fixed to $t \cdot 0 = 0$ by bending the provability semantics a little. However, under any modification of semantics, the identity $\neg 0{:}\top$ holds, which spoils the connection to modal logic. Indeed, the forgetful projection of the latter formula is $\neg\Box\top$, which is false in any normal modal logic. This observation alone should not discourage us from considering the addition of 0 to a version of SLP, though. The language of proof polynomials should then be extended by a special constant 0 which cannot be used as 'c' in the Constant Specification Rule (Section 2). A new axiom schema $\neg 0{:}F$ should also be added.

Note that the relation '$\sim$' from Theorem 8 is an equivalence relation on proof polynomials. However, '$\sim$' is not a congruence, e.g., $s \sim t$ does not generally yield $!s \sim !t$. For example, $x \sim x + x$ (Theorem 8.3), but not $!x \sim !(x + x)$. Indeed, in the symmetric provability interpretation, $!x$ should contain proofs of $x{:}F$ for all $F \in x$, whereas $!(x + x)$ contains proofs of $(x + x){:}F$ for all such F's. This observation still leaves an opportunity for '$\sim$' to be a congruence in some !-free variant of SLP. It is easy to check that in SLP, $s \sim t$ and $u \sim v$ yield $s+u \sim t+v$. It is not known whether the same holds for '$\cdot$', i.e., $su \sim tv$ as well. Such a rule for '$\cdot$' is sound for the standard symmetric provability interpretation, which suggests that a proper version of this rule either holds in, or can be safely added to, SLP. Answers to these questions could lead to an adequate notion of the *equality of proofs* in Justification Logic in general. We leave this, however, for future studies.

Other natural steps in this direction would be to clarify the questions of decidability and complexity for SLP, to check the disjunctive property, and to describe adequate Gentzen and tableaux proof systems.

We conjecture that SLP is arithmetically complete with respect to the class of proof predicates for which the Symmetry Principle holds. An intriguing question remains open about the logic of proofs for the standard symmetric provability interpretation.

8 Acknowledgements

This paper was inspired by discussions with Joan and Yiannis Moschovakis at the 6th Panhellenic Logic Symposium, Volos, Greece, 5-8 July 2007. The author is very grateful to Mel Fitting, Evan Goris, Vladimir Krupski, Roman Kuznets, and Elena Nogina whose advice helped with this paper. Many thanks to Karen Kletter for editing this text.

[7] This observation is due to V.N. Krupski.

References

[1] S. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, 1995.

[2] S. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, 2001.

[3] S. Artemov. Operations on proofs that can be specified by means of modal logic. In *Advances in Modal Logic. Volume 2*, pages 59–72. CSLI Publications, Stanford University, 2001.

[4] S. Artemov. Evidence-based common knowledge. Technical Report TR-2004018, CUNY Ph.D. Program in Computer Science, 2005.

[5] S. Artemov. Justified common knowledge. *Theoretical Computer Science*, 357(1-3):4–22, 2006.

[6] S. Artemov. On two models of provability. In Michael Zakharyaschev Dov M. Gabbay and Sergei S Goncharov, editors, *Mathematical Problems from Applied Logic II*, pages 1–52. Springer New York, 2007.

[7] S. Artemov and L. Beklemishev. Provability logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic, 2nd ed.*, volume 13, pages 229–403. Kluwer, Dordrecht, 2004.

[8] S. Artemov and E. Nogina. Introducing justification into epistemic logic. *Journal of Logic and Computation*, 15(6):1059–1073, 2005.

[9] S. Artemov and E. Nogina. On epistemic logic with justification. In R. van der Meyden, editor, *Theoretical Aspects of Rationality and Knowledge. Proceedings of the Tenth Conference (TARK 2005), June 10-12, 2005, Singapore.*, pages 279–294. National University of Singapore, 2005.

[10] S. Artemov and T. Strassen. Functionality in the basic logic of proofs. Technical Report IAM 93-004, Department of Computer Science, University of Bern, Switzerland, 1993.

[11] G. Boolos. *The Logic of Provability.* Cambridge University Press, Cambridge, 1993.

[12] V. Brezhnev and R. Kuznets. Making knowledge explicit: How hard it is. *Theoretical Computer Science*, 357(1-3):23–34, 2006.

[13] M. Fitting. A semantics for the logic of proofs. Technical Report TR-2003012, CUNY Ph.D. Program in Computer Science, 2003.

[14] M. Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132(1):1–25, 2005.

[15] K. Gödel. Eine Interpretation des intuitionistischen Aussagenkalkuls. *Ergebnisse Math. Kolloq.*, 4:39–40, 1933. English translation in: S. Feferman et al., editors, *Kurt Gödel Collected Works, Vol. 1*, pages 301–303. Oxford University Press, Oxford, Clarendon Press, New York, 1986.

[16] K. Gödel. Vortrag bei Zilsel, 1938. In S. Feferman, editor, *Kurt Gödel Collected Works. Volume III*, pages 86–113. Oxford University Press, 1995.

[17] E. Goris. Logic of proofs for bounded arithmetic. In J. Harrison D. Grigoriev and E.A. Hirsch, editors, *Computer Science - Theory and Applications. CSR 2006*, volume 3967 of *Lecture Notes in Computer Science*, pages 191–201. Springer, 2006.

[18] S. Kleene. *Introduction to Metamathematics*. Van Norstrand, 1952.

[19] N.V. Krupski. On the complexity of the reflected logic of proofs. *Theoretical Computer Science*, 357(1):136–142, 2006.

[20] V.N. Krupski. Operational logic of proofs with functionality condition on proof predicate. In S. Adian and A. Nerode, editors, *Logical Foundations of Computer Science '97, Yaroslavl'*, volume 1234 of *Lecture Notes in Computer Science*, pages 167–177. Springer, 1997.

[21] V.N. Krupski. The single-conclusion proof logic and inference rules specification. *Annals of Pure and Applied Logic*, 113(1-3):181–206, 2001.

[22] V.N. Krupski. Referential logic of proofs. *Theoretical Computer Science*, 357(1):143–166, 2006.

[23] R. Kuznets. On the complexity of explicit modal logics. In *Computer Science Logic 2000*, volume 1862 of *Lecture Notes in Computer Science*, pages 371–383. Springer-Verlag, 2000.

[24] R. Milnikel. Derivability in certain subsystems of the Logic of Proofs is Π_2^p-complete. *Annals of Pure and Applied Logic*, 145(3):223–239, 2007.

[25] A. Mkrtychev. Models for the logic of proofs. In S. Adian and A. Nerode, editors, *Logical Foundations of Computer Science '97, Yaroslavl'*, volume 1234 of *Lecture Notes in Computer Science*, pages 266–275. Springer, 1997.

[26] C. Smoryński. The incompleteness theorems. In J. Barwise, editor, *Handbook of Mathematical Logic*, pages 821–865. North Holland, Amsterdam, 1977.

[27] R.M. Solovay. Provability interpretations of modal logic. *Israel Journal of Mathematics*, 28:33–71, 1976.