Verification Logic: An Arithmetical Interpretation for Negative Introspection

Juan P. Aguilera [1]

Institut für diskrete Mathematik und Geometrie, Vienna University of Technology, Austria.

David Fernández-Duque [2]

Centre International de Mathématiques et d'Informatique, University of Toulouse, France;
Department of Mathematics, Instituto Tecnológico Autónomo de México, Mexico.

Abstract

We introduce *verification logic*, a variant of Artemov's logic of proofs with new terms of the form ¡φ! satisfying the axiom schema $\varphi \to$ ¡φ!:φ. The intention is for ¡φ! to denote a proof of φ in Peano arithmetic, whenever such a proof exists. By a suitable restriction of the domain of ¡·!, we obtain the verification logic VS5, which realizes the axioms of Lewis' system S5. Our main result is that VS5 is sound and complete for its arithmetical interpretation.

Keywords: verification logic, logic of proofs, negative introspection.

1 Introduction

Over twenty years ago, Artemov introduced the *logic of proofs* (LP) to give a provability interpretation of the modal logic S4 [1]. As opposed to the provability logic GL, which uses a single modal operator $\Box$ to represent provability [4], LP uses *proof terms,* meant to denote derivations in Peano arithmetic. If t is a proof term and φ a formula, $t{:}\varphi$ is interpreted as "t is a proof of φ." Complex terms may be built from simpler ones using a handful of operations; in particular, to every term t there corresponds a 'proof-checking' term $!t$, allowing us to realize the modal axiom 4—or *positive introspection,* $\Box\varphi \to \Box\Box\varphi$—by the LP axiom $t{:}\varphi \to !t{:}t{:}\varphi$ (see Section 7 for a definition of 'realization'). To be precise, Artemov proved that LP enjoyed two essential properties:

[1] Email: aguilera@logic.at. Partially supported by FWF grants P-26976-N25, I-1897-N25, I-2671-N35, and W1255-N23.

[2] Email: david.fernandez@irit.fr. Partially supported by ANR-11-LABX-0040-CIMI within the program ANR-11-IDEX-0002-02.

(i) every theorem of S4 can be realized by a theorem of LP, and

(ii) LP is sound and complete for its arithmetical interpretation.

Since then, LP has inspired a family of logics called *justification logics,* which use simlar constructions for 'justification terms' but are not necessarily motivated by mathematical proof (see [2] for an overview). In particular, for applications in epistemic or doxastic logics, one may wish to work with a justification logic realizing the axiom 5—or *negative introspection,* $\neg\Box\varphi \to \Box\neg\Box\varphi$—by some term refuting $t{:}\varphi$. Such a logic may be obtained by extending LP with 'proof-refuting' terms of the form $?t$, satisfying $\neg t{:}\varphi \to ?t{:}\neg t{:}\varphi$. Rubstova proved that the resulting logic, now known as JS5, indeed realizes all theorems of S5 [12]. Her proof was non-constructive, but constructive proofs of this result have since been found; see, for example, [6]. Moreover, there are relational semantics for LP due to Fitting [5], which may also be used to interpret JS5 as well as other justification logics realizing many well-known modal logics [11].

Unfortunately, terms of the form $?t$ satisfying $\neg t{:}\varphi \to ?t{:}\neg t{:}\varphi$ cannot be interpreted using standard PA proofs, since any standard PA derivation represented by t proves at most finitely many formulae, and therefore there are infinitely many formulae φ for which $t{:}\varphi$ fails. But this means that $?t$ would have to be a proof with *infinitely many conclusions* (one for every formula φ not proven by t), contrary to the nature of standard PA proofs (although Kuznets and Studer consider derivations having infinitely many conclusions in [10]).

In order to circumvent this issue, Artemov et. al. [3] instead consider a logic LP(S5), where the term $?t$ satisfies $t{:}(\psi \to \neg s{:}\varphi) \to (\psi \to ?t{:}\neg s{:}\varphi)$. This allows $?t$ to prove finitely many instances of $\neg s{:}\varphi$ (only those already appearing in t), which in turns makes it possible for us to realize any finite collection of instances of negative introspection—one introduces proof constants c such that $c{:}(\neg t{:}\varphi \to \neg t{:}\varphi)$, whence $\neg t{:}\varphi \to ?c{:}\neg t{:}\varphi$ holds. Alternately, Artemov et. al. propose a variant where one is allowed to introduce new proof constants c satisfying $\neg t{:}\varphi \to c{:}\neg t{:}\varphi$. However, either version of LP(S5) has the drawback that the constant specification may have to be extended each time we want a suitable term satisfying a new instance of negative introspection.

In this work, we use a different approach to justification logics, introducing a new family of systems where proof-checkers are replaced with *fact-verifiers* of the form $¡\varphi!$, similar to the *update terms* in [9]. We call such systems *verification logics,* and while we define a few natural examples, we focus our attention on a particular verification logic which we denote VS5. As we show, VS5 realizes both axioms 4 and 5, while enjoying a natural arithmetical interpretation similar to that of LP. It has the advantage that all instances of negative introspection are uniformly realized, while maintaining the finiteness of proofs.

Our main result is that VS5 is complete for this arithmetical interpretation. Our completeness proof follows the basic structure of Artemov's in [1], but a few additional subtleties arise when dealing with the 'negative introspection verifiers.'

Layout. The paper is structured as follows. In Section 2, we introduce proof-checking terms, the language $L_{¡!}$, and the logic VL, along with its natural sublogics, which include VT, $\mathsf{VS4}$ and $\mathsf{VS5}$. In Section 4, we introduce arithmetical interpretations. The arithmetical completeness proof is divided between Section 5, which provides a constructive Lindenbaum lemma, and Section 6, which constructs suitable proof predicates using the fixed point theorem. Finally, in section 7, we present some comments on the possible realizability of $\mathsf{S5}$ by $\mathsf{VS5}$.

2 The logics

In this section we introduce verification logics, and show that some natural verification logics enjoy the internalization property.

Definition 2.1 We define the *terms* and *formulae* of the *full language* $L_{¡!}$ of verification logic by simultaneous recursion as follows:

$$\begin{array}{l} t :: x \mid t \cdot s \mid \ t + s \ \mid ¡\varphi! \\ \varphi :: p \mid \neg\varphi \mid \varphi \to \psi \mid t{:}\varphi, \end{array} \tag{1}$$

where each of x and p is an element of a countably-infinite set of proof or propositional variables. We assume that the two sets of variables are disjoint.

An *expression* is either a term or a formula. We define the *subexpressions* $\mathrm{se}(\epsilon)$ of an expression ϵ by $\mathrm{se}(\epsilon) = \{\epsilon\}$ if ϵ is a variable, $\mathrm{se}(\epsilon) = \{\epsilon\} \cup \mathrm{se}(\varphi)$ if $\epsilon = ¡\varphi!$ or $\epsilon = \neg\varphi$, $\mathrm{se}(\epsilon) = \{\epsilon\} \cup \mathrm{se}(\eta) \cup \mathrm{se}(\rho)$ if $\epsilon = \eta + \rho$, $\eta \cdot \rho$, $\eta \to \rho$ or $\eta{:}\rho$. The *subformulae* are the subexpressions that are formulae, denoted $\mathrm{sf}(\epsilon)$, and the *subterms* are the subexpressions that are terms, denoted $\mathrm{st}(\epsilon)$. If $\eta \in \mathrm{se}(\epsilon)$ we may say that η *occurs* in ϵ, and if Γ is a set of expressions, we say that η *occurs* in Γ if η is a subexpression of some $\epsilon \in \Gamma$.

Next, let us introduce the axioms of full verification logic.

Definition 2.2 The logic VL is defined as the logic generated by modus ponens and the following sets of axioms:

(i) all propositional tautologies,

(ii) $t{:}\varphi \to \varphi$,

(iii) $t{:}(\varphi \to \psi) \to (s{:}\varphi \to s \cdot t{:}\psi)$,

(iv) $t{:}\varphi \to (t + s){:}\varphi$ and $s{:}\varphi \to (t + s){:}\varphi$,

(v) $\varphi \to ¡\varphi!{:}\varphi$.

We will not work with full verification logic, but with one of its natural sublogics, as defined below.

Definition 2.3 A *natural sublanguage* is one obtained by restricting the domain of ¡·! to specific choices of φ in (1). In particular, we define:

$L_{¡\mathsf{T}!}$, obtained by restricting the domain of ¡·! to all axioms (including tautologies);

$L_{¡4!}$, obtained by restricting the domain of ¡·! to axioms and formulae of the form $t{:}\varphi$; and

$L_{¡5!}$, obtained by restricting the domain of ¡·! to tautologies, formulae of the form $t{:}\varphi$, and formulae of the form $\neg t{:}\varphi$.

If L is a natural restriction of $L_{¡!}$, the *natural restriction of* VL *associated to* L is the logic $\mathsf{V}(L)$ obtained by restricting the axioms to L and closing under modus ponens. Any logic obtained in this way is a *natural verification logic.* We denote by $\mathsf{VS4}$, $\mathsf{VS5}$ the natural restrictions associated to $L_{¡4!}$ and $L_{¡5!}$, respectively.

If $\lambda = \mathsf{V}(L)$ is a natural verification logic, $\Gamma \subset L$ and $\varphi \in L$, we write $\Gamma \vdash_\lambda \varphi$ if φ belongs to the smallest set containing all axioms of λ, all formulae of Γ, and closed under modus ponens. When $\Gamma = \varnothing$, we write $\vdash_\lambda \varphi$. We say Γ is *consistent (over* λ*)* if $\Gamma \nvdash_\lambda \varphi \wedge \neg\varphi$ for any formula φ.

Observe that $L_{¡5!}$ is not a proper extension of the other two languages since it does not include formulae of the forms $t{:}\varphi \to \varphi$ or $\varphi \to ¡\varphi!{:}\varphi$. However, there is good reason for defining it in this way:

Lemma 2.4 *For any axiom* φ *of* $\mathsf{VS5}$ *of the forms* (ii)–(v)*, there exists an* $L_{¡5!}$*-term* s *such that* $\vdash_{\mathsf{VS5}} s{:}\varphi$.

Proof. If $\varphi = t{:}\psi \to \psi$ is an instance of (ii), set

$$s = ¡\psi \to \varphi! \cdot ¡t! + ¡\neg t{:}\psi \to \varphi! \cdot ¡\neg t{:}\psi!.$$

From the assumption that $t{:}\psi$, it is easy to derive $¡\psi \to \varphi! \cdot ¡t!{:}\varphi$, while from the assumption that $\neg t{:}\psi$, one obtains $¡\neg t{:}\psi \to \varphi! \cdot ¡\neg t{:}\psi!{:}\varphi$; in either case, we obtain $s{:}\varphi$, and this reasoning may be performed within $\mathsf{VS5}$ using the tautology $t{:}\psi \vee \neg t{:}\psi$.

If $\varphi = \psi \to ¡\psi!{:}\psi$ is an instance of (v), then there are three cases to consider; if ψ is a tautology, set $s = ¡\,(¡\psi!{:}\psi \to \varphi)\,! \cdot ¡\,(¡\psi!{:}\psi)\,!$. If $\psi = t{:}\theta$, we set $s = ¡\,(¡t{:}\theta!{:}t{:}\theta \to \varphi)\,! \cdot ¡(¡t{:}\theta!{:}t{:}\theta)! + ¡\neg t{:}\theta \to \varphi! \cdot ¡\neg t{:}\theta!$. Finally, if $\psi = \neg t{:}\theta$, set $s = ¡\,(¡\neg t{:}\theta!{:}\neg t{:}\theta \to \varphi)\,! \cdot ¡(¡\neg t{:}\theta!{:}\neg t{:}\theta)! + ¡t{:}\theta \to \varphi! \cdot ¡t{:}\theta!$.

In all cases, similar reasoning shows that $s{:}\varphi$ is derivable in $\mathsf{VS5}$. The axioms (iii) and (iv) may be treated similarly and are left to the reader. □

Henceforth we will write $¡\varphi! = s$ for the term s given by Lemma 2.4; we will use this notation in the following proof. Observe that verification logics are only a minor variation of justification logics, and as such we may expect them to share many of their basic properties, such as the following familiar 'lifting lemma'. Below, if $\boldsymbol{t} = (t_i)_{i<n}$ is a tuple of terms and $\Gamma = (\gamma_i)_{i<n}$ a tuple of formulas, then $\boldsymbol{t}{:}\Gamma$ denotes the tuple $(t_i{:}\gamma_i)_{i<n}$.

Lemma 2.5 *Let* $\lambda \in \{\mathsf{VT}, \mathsf{VS4}, \mathsf{VS5}\}$ *and* Γ, Δ, Ξ *be tuples of formulae such that* $\Gamma = \Delta = \varnothing$ *if* $\lambda = \mathsf{VT}$ *and* $\Delta = \varnothing$ *if* $\lambda = \mathsf{VS4}$*. Let* $\boldsymbol{t}$*,* $\boldsymbol{s}$ *be tuples of terms and* $\boldsymbol{x}$ *of variables with the same length as* Γ, Δ, Ξ*, respectively. Then, if* $\boldsymbol{t}{:}\Gamma, \neg\boldsymbol{s}{:}\Delta, \Xi \vdash_{\mathsf{VS5}} \varphi$*, there is a term* $u(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ *such that*

$$\boldsymbol{t}{:}\Gamma, \neg\boldsymbol{s}{:}\Delta, \boldsymbol{x}{:}\Xi \vdash_{\mathsf{VS5}} u(\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{s}){:}\varphi.$$

Proof. We proceed by induction on the derivation of φ. There are several base cases.

If φ is an axiom, we set $u = ¡\varphi!$, where in the case of $\lambda = \mathsf{VS5}$ this $¡\varphi!$ is given by Lemma 2.4. If $\varphi \in \boldsymbol{t}{:}\Gamma$ (so that $\lambda \neq \mathsf{VT}$) or $\varphi \in \neg\boldsymbol{s}{:}\Delta$ (so that $\lambda = \mathsf{VS5}$), set $u = ¡\varphi!$. Similarly, if $\varphi \in \Xi$, say $\varphi = \xi_i$, set $u = x_i$.

Otherwise, we obtain φ by modus ponens, say from formulae ψ and $\psi \to \varphi$. By the induction hypothesis, there are terms v, w such that $\boldsymbol{t}{:}\Gamma, \neg\boldsymbol{s}{:}\Delta, \boldsymbol{x}{:}\Xi \vdash_{\mathsf{VS5}} v(\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{s}){:}\psi$ and $\boldsymbol{t}{:}\Gamma, \neg\boldsymbol{s}{:}\Delta, \boldsymbol{x}{:}\Xi \vdash_{\mathsf{VS5}} w(\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{s}){:}(\psi \to \varphi)$, and we may set $u = w \cdot v$. □

As an immediate consequence, we obtain the internalization theorem for these three verification logics, which is an explicit version of the necessitation rule:

Corollary 2.6 *Let $\lambda \in \{\mathsf{VT}, \mathsf{VS4}, \mathsf{VS5}\}$ and suppose that $\vdash_\lambda \varphi$. Then, there is a λ-term t such that $\vdash_\lambda t{:}\varphi$.*

3 Theories of arithmetic

In this section we review some basic notions of first-order arithmetic and settle some notation and terminology. The material presented here is treated in detail, for example, in [8].

3.1 Conventions of syntax

We will consider arithmetical theories in languages extending that of first-order arithmetic with exponential, which includes the symbols $\mathsf{0}, \mathsf{1}, x+y, x\cdot y, \mathsf{2}^x$ and $=$, representing the standard constants, operations and relations on the natural numbers, along with the Booleans $\neg, \to$ and the quantifiers $\forall, \exists$; the language generated by these symbols will be denoted L_{PA}. We assume that L_{PA} has a countably infinite set of first-order variables $x, y, z, \ldots$. We may define $x \leq y$ by $\exists z(y = x + z)$ and $x < y$ by $x + \mathsf{1} \leq y$. We define inductively $\mathsf{2}^x_0 = \mathsf{2}^x$ and $\mathsf{2}^x_{l+1} = \mathsf{2}^{\mathsf{2}^x_l}$.

As is customary, we use Δ_0 to denote the set of all formulae where all quantifiers are *bounded*, that is, of the form $\forall x < t\ \varphi$ or $\exists x < t\ \varphi$. We will use pseudo-terms to simplify notation, where an expression $\varphi(t(\boldsymbol{x}))$ should be understood as a shorthand for $\exists y < s(\boldsymbol{x})\ \big(\psi(\boldsymbol{x}, y) \wedge \varphi(y)\big)$, with ψ a Δ_0 formula defining the graph of the intended interpretation of t and s a standard term bounding the values of $t(\boldsymbol{x})$. The domain of the functions defined by these pseudo-terms may be a proper subset of $\mathbb{N}$. Functions definable by pseudo-terms of this form are *elementary.*

We assume that every finite sequence $(s_1, \ldots, s_n)$ may be represented by a natural number $\boldsymbol{s}$, with the following properties:

(i) there is a Δ_0 formula $\mathtt{seq}(x)$ such that $\mathtt{seq}(\boldsymbol{s})$ is true if and only if $\boldsymbol{s}$ codes a sequence;

(ii) there is a pseudo-term $|x|$ such that $|\boldsymbol{s}|$ returns the length of $\boldsymbol{s}$, and we assume that $|\boldsymbol{s}| \leq \boldsymbol{s}$ for all sequences $\boldsymbol{s}$;

(iii) there is a pseudo-term $(x)_y$ such that $(\boldsymbol{s})_i$ returns the i^{th} element of s, also with the assumption that $(\boldsymbol{s})_i \leq \boldsymbol{s}$, and

(iv) there is a term $B(x, y)$ such that whenever $\boldsymbol{s}$ is a sequence of length at most N and with each s_i bounded by M, it follows that $\boldsymbol{s} < B(N, M)$.

Finite sets may also be represented using sequences (by ordering them arbitrarily), in which case we say that x belongs to $\boldsymbol{s}$ if $x = (\boldsymbol{s})_i$ for some i. Similarly, we can represent some functions using sequences. Call a function *small* if its domain is finite. Small functions can be coded by pairs $f = (\boldsymbol{d}, \boldsymbol{r})$, where $\boldsymbol{d}$, $\boldsymbol{r}$ are sequences of the same length, and we write $f(x) = y$ if there is some i such that $(\boldsymbol{d})_i = x$ and $(\boldsymbol{r})_i = y$. We call $\boldsymbol{d}$ the *domain* of f and denote it by $\mathrm{dom}(f)$.

3.2 Peano Arithmetic

For the sake of concreteness, we will be working in Peano arithmetic. PA is formed by adding the axiom schema of successor induction (equation (2) below for any formula φ of L_{PA}) to Robinson Arithmetic, e.g., as axiomatized by:

(i) $\forall x\ (x = x)$

(ii) $\forall x \forall y\ (x \neq y \vee \alpha \vee {\sim}\alpha[x/y])$

(iii) $\forall x \forall y\ (x \neq y \vee y = x)$

(iv) $\forall x \forall y \forall z\ \big(x \neq y \vee y \neq z \vee x = z\big)$

(v) $\forall x\ (\mathsf{0} \neq x + \mathsf{1})$

(vi) $\forall x\ (x = \mathsf{0} \vee \exists y\ x = y + \mathsf{1})$

(vii) $\forall x\ (x + \mathsf{0} = x)$

(viii) $\forall x \forall y\ \big(x + (y + \mathsf{1}) = (x + y) + \mathsf{1}\big)$

(ix) $\forall x\ (x \times \mathsf{0} = \mathsf{0})$

(x) $\forall x \forall y\ \big(x \times (y + \mathsf{1}) = (x \times y) + y\big)$

(xi) $\mathsf{2}^{\mathsf{0}} = \mathsf{1}$

(xii) $\forall x\ \big(\mathsf{2}^{x+\mathsf{1}} = \mathsf{2}^x + \mathsf{2}^x\big)$

(xiii) $\forall x \forall y\ (x + \mathsf{1} \neq y + \mathsf{1} \vee x = y)$

(in (ii) above, α is any atomic formula). The axiom schema of successor induction is given by

$$\varphi(\mathsf{0}) \wedge \forall x\ \big(\varphi(x) \to \varphi(x + \mathsf{1})\big)\ \to\ \forall x\ \varphi(x). \tag{2}$$

We remark, however, that our proof is fairly general and would readily work for many theories stronger (or weaker) than PA, or even theories in other languages, such as that of set theory.

3.3 Gödel numberings

Fix some Gödel numbering $\ulcorner\cdot\urcorner : L_{\mathrm{PA}} \cup L_{\text{¡5!}} \to \mathbb{N} \setminus \{0\}$, such that the set of codes from each language is elementary. Note that 0 is not the Gödel number of any expression. For a natural number n, define a term $\bar{n}$ recursively by $\bar{0} = \mathsf{0}$ and $\overline{n+1} = (\bar{n}) + \mathsf{1}$. As in the case of sequences, we will assume that if N, M are such that the expression ϵ has at most N symbols, each with code bounded by M, then $\ulcorner\epsilon\urcorner < B(N, M)$; that if η is a proper subexpression of ϵ, then $\ulcorner\eta\urcorner < \ulcorner\epsilon\urcorner$; and that if ϵ has n symbols, then $n < \ulcorner\epsilon\urcorner$.[3]

[3] These conditions are achieved, for example, if ϵ is coded by putting all of its symbols in a sequence and using our previous assumptions on the coding of sequences.

If $\Gamma = (\epsilon_i)_{i<n}$ is a sequence of expressions, we define $\ulcorner\Gamma\urcorner$ to be the code of the sequence $(\ulcorner\epsilon_i\urcorner)_{i<n}$. We will sometimes abuse notation by identifying expressions with their Gödel numbers and sets or sequences with their codes.

4 Arithmetical interpretations

In this section we will define the arithmetical interpretation of verification logic. It requires the notion of a *normal proof system*:

Definition 4.1 A *normal proof system* is a triple $(\pi, \mathsf{m}, \mathsf{a})$ such that:

(i) $\pi = \pi(x, y)$ is a Δ_0 formula of L_{PA} and, for every $\varphi \in L_{\mathrm{PA}}$, $\mathrm{PA} \vdash \varphi$ if and only if $\exists x\, \pi(x, \ulcorner\varphi\urcorner)$ holds.

(ii) Say that y is a π-*conclusion* of x if $\pi(x, y)$ holds. Then, the set $[\![x]\!]_\pi$ of all π-conclusions of x is finite for all x and the function $x \mapsto [\![x]\!]_\pi$ is computable.

(iii) m is a computable function such that, for all n, k and formulae φ, ψ, if $\pi(n, \ulcorner\varphi \to \psi\urcorner)$ and $\pi(k, \ulcorner\varphi\urcorner)$, then $\pi(\mathsf{m}(n, k), \ulcorner\psi\urcorner)$.

(iv) a is a computable function such that, for all n, k and any formula φ, if $\pi(n, \ulcorner\varphi\urcorner)$ or $\pi(k, \ulcorner\varphi\urcorner)$, then $\pi(\mathsf{a}(n, k), \ulcorner\varphi\urcorner)$.

We assume that a canonical normal proof system $(\mathtt{Proof}, \mathsf{m}_{\mathrm{PA}}, \mathsf{a}_{\mathrm{PA}})$ is given, and $[\![x]\!] = [\![x]\!]_{\mathtt{Proof}}$. The existence of normal proof systems is well known; for example, we may use a multi-conclusion variant of Gödel's proof predicate. Observe that it is not necessary to work with Δ_0 proof predicates (Δ_1 is sufficient), but we follow [7] and work within bounded arithmetic when possible.

Definition 4.2 A *potential arithmetical interpretation* is a tuple $\mathfrak{S} = (f, \pi, \mathsf{m}, \mathsf{a}, \mathsf{v})$ such that f maps propositional variables to formulas of L_{PA} and term variables to natural numbers, $(\pi, \mathsf{m}, \mathsf{a})$ is a normal proof system, and $\mathsf{v}\colon L_{\mathrm{PA}} \to \mathbb{N}$ is a computable function. We define a function $\cdot^{\mathfrak{S}}\colon L_{¡5!} \to L_{\mathrm{PA}}$ by letting

(i) $v^{\mathfrak{S}} = f(v)$ for any variable v,

(ii) $\cdot^{\mathfrak{S}}$ commute with Booleans,

(iii) $(t{:}\varphi)^{\mathfrak{S}} = \pi(\overline{t^{\mathfrak{S}}}, \overline{\ulcorner\varphi^{\mathfrak{S}}\urcorner})$,

(iv) $(t \cdot s)^{\mathfrak{S}} = \mathsf{m}\big(t^{\mathfrak{S}}, s^{\mathfrak{S}}\big)$,

(v) $(t + s)^{\mathfrak{S}} = \mathsf{a}\big(t^{\mathfrak{S}}, s^{\mathfrak{S}}\big)$, and

(vi) $¡\varphi!^{\mathfrak{S}} = \mathsf{v}(\varphi^{\mathfrak{S}})$.

We say that $\mathfrak{S}$ is an *arithmetical interpretation of* $\mathsf{VS5}$ if whenever $\varphi \in L_{¡5!}$, then $\varphi^{\mathfrak{S}} \to \pi(\mathsf{v}(\varphi^{\mathfrak{S}}), \ulcorner\varphi^{\mathfrak{S}}\urcorner)$ holds. The arithmetical interpretation $\mathfrak{S}$ is *robust* if, whenever $\varphi \in \Delta_0$, then $\varphi^{\mathfrak{S}} \to \pi(\mathsf{v}(\varphi^{\mathfrak{S}}), \ulcorner\varphi^{\mathfrak{S}}\urcorner)$ also holds.

We remark that robustness is not necessary for our proofs to go through, but it is a desirable property since such interpretations automatically satisfy all expressions $\varphi \to ¡\varphi!{:}\varphi$ whenever $\varphi \in \Delta_0$, thus internalizing the completeness of Peano arithmetic for Δ_0 formulas [8].

Proposition 4.3 (Arithmetical soundness) *If* $\mathsf{VS5} \vdash \varphi$, *then* $\mathrm{PA} \vdash \varphi^{\mathfrak{S}}$ *for any arithmetical interpretation* $\mathfrak{S}$.

Proof. By a straightforward induction. Clearly, modus ponens preserves validity. We check the axiom $t{:}\varphi \to \varphi$, which translates as $\pi(\ulcorner t^{\mathfrak{S}} \urcorner, \ulcorner \varphi^{\mathfrak{S}} \urcorner) \to \varphi^{\mathfrak{S}}$. Either $\pi(\ulcorner t^{\mathfrak{S}} \urcorner, \ulcorner \varphi^{\mathfrak{S}} \urcorner)$ is true, whence $\mathrm{PA} \vdash \varphi^{\mathfrak{S}}$ (by the soundness of a normal proof predicate, i.e., condition (i)) and so $\mathrm{PA} \vdash \pi(\ulcorner t^{\mathfrak{S}} \urcorner, \ulcorner \varphi^{\mathfrak{S}} \urcorner) \to \varphi^{\mathfrak{S}}$, or $\pi(\ulcorner t^{\mathfrak{S}} \urcorner, \ulcorner \varphi^{\mathfrak{S}} \urcorner)$ is false, whence it is refutable in PA (as it is Δ_0), whereby again $\mathrm{PA} \vdash \pi(\ulcorner t^{\mathfrak{S}} \urcorner, \ulcorner \varphi^{\mathfrak{S}} \urcorner) \to \varphi^{\mathfrak{S}}$. The rest of the axioms are proved similarly. □

Our main objective is now to prove that VS5 is also complete. We will in fact prove a slightly strengthened version of completeness:

Theorem 4.4 (Arithmetical completeness) *If φ is consistent with* VS5*, then there is a robust arithmetical interpretation $\mathfrak{S}^*$ such that* $\mathrm{PA} \vdash \varphi^{\mathfrak{S}^*}$.

We defer the proof of this result to Section 6. Its general structure is similar to that of the arithmetical completeness proof in [1], although some additional care must be taken to deal with the 'negative information' conveyed by proof terms of the form $¡\neg t{:}\varphi!$. Among the technical difficulties is that many of the steps must be done constructively, including a version of the Lindenbaum lemma.

5 A constructive Lindenbaum's lemma

As in many familiar completeness proofs, the first step is to expand the consistent set $\{\varphi\}$ to a larger set that can be dealt with more easily. We do this by first expanding the set "downwards" and then "upwards." It will be convenient to introduce the notation $\sim\varphi$ defined by $\sim\varphi = \neg\varphi$ if φ does not begin with a negation, and $\sim\varphi = \psi$ if $\varphi = \neg\psi$.

Definition 5.1 A set of formulae Γ is *saturated* if:

(i) whenever ψ occurs in Γ, either $\psi \in \Gamma$ or $\sim\psi \in \Gamma$,

(ii) whenever $\neg(s + t){:}\varphi \in \Gamma$, then $\neg s{:}\varphi \in \Gamma$ and $\neg t{:}\varphi \in \Gamma$, and

(iii) whenever $\neg(s \cdot t){:}\varphi \in \Gamma$ and $\psi \to \varphi$ occurs in Γ, then either $\neg s{:}(\psi \to \varphi) \in \Gamma$, or $\neg t{:}\psi \in \Gamma$.

Lemma 5.2 *For any consistent formula φ there exists a finite, consistent, saturated set that contains φ.*

Proof. Choose a subformula of φ and either add it or its negation so as to maintain consistency, as well as the required formulae for $\neg(s \cdot t){:}\varphi$ and $\neg(s + t){:}\varphi$. Rinse and repeat. Note that either the formulae or the terms that we add are simpler than those previously appearing and thus the process terminates.□

As an immediate consequence of the definition, we note that saturated sets of formulae have some basic closure properties.

Lemma 5.3 *Suppose Γ is a saturated set of formulae.*

(i) *$\psi \to \varphi \in \Gamma$ implies that $\sim\psi \in \Gamma$ or $\varphi \in \Gamma$ and $\neg(\psi \to \varphi) \in \Gamma$ implies that $\psi, \sim\varphi \in \Gamma$;*

(ii) *$\neg ¡\varphi!{:}\varphi \in \Gamma$ implies that $\neg\,\varphi \in \Gamma$ for φ of the form $t{:}\psi$ or $\neg t{:}\psi$, and*

(iii) $t{:}\varphi \in \Gamma$ *implies* $\varphi \in \Gamma$.

These properties are easily verified and left to the reader. Once we have included a formula φ in a saturated, consistent set Γ, the next step would be to use a suitable variant of Lindenbaum's lemma to extend Γ to a maximal-consistent set of formulae. This amounts to selecting which instances of $t{:}\varphi$ must be true, as propositional variables not appearing in Γ may all be assigned the value 'false.' In fact, instances of $t{:}\varphi$ may also be assumed false, unless they are forced to be true by axiom (v) or are sufficiently witnessed by Γ. We make this notion precise below. Recall that an expression ϵ *occurs* in Γ if it is a subexpression of a formula in Γ.

Definition 5.4 Let Γ be a set of formulae A *verification instance of* $L_{\text{¡5!}}$ (or simply: a *verification*) is any formula of the form $t{:}\varphi \in L_{\text{¡5!}}$. We say that $t{:}\varphi$ is Γ-*balanced* (or simply 'balanced') if φ occurs in either t or Γ. The set of Γ-balanced verifications will be denoted by $[\Gamma]$.

Remark. If $\Gamma \subseteq L_{\text{¡5!}}$ is a (code for a) finite set of formulae and $t{:}\varphi \in \Gamma$, then $t{:}\varphi \in [\Gamma]$. Moreover, ¡φ!:$\varphi \in L_{\text{¡5!}}$ is always Γ-balanced, regardless of Γ or φ. Observe that if $t{:}\varphi$ is Γ-balanced then $\ulcorner\varphi\urcorner < \max(\ulcorner t\urcorner, \ulcorner\Gamma\urcorner)$ by our convention on Gödel numbering.

For balanced verifications, the truth value of $t{:}\varphi$ will be decided recursively, according to an order determined by the Gödel number of each formula:

Definition 5.5 Fix a (code for a) set of formulae Γ. If $t{:}\varphi$, $s{:}\psi$ are verifications, we write $t{:}\varphi \lhd s{:}\psi$ whenever $(\ulcorner t\urcorner, \ulcorner\varphi\urcorner) <_{\texttt{lex}} (\ulcorner s\urcorner, \ulcorner\psi\urcorner)$; i.e., either $\ulcorner t\urcorner < \ulcorner s\urcorner$ or $t = s$ and $\ulcorner\varphi\urcorner < \ulcorner\psi\urcorner$. For any $\tau \in [\Gamma]$, we define $\downarrow\tau = \{\sigma \in [\Gamma] \colon \sigma \lhd \tau\}$.

In words, $\downarrow\tau$ is the set of balanced predecessors of τ. It will be convenient to give a simple bound on the size of this set:

Lemma 5.6 *Let* Γ *be saturated and* $t{:}\varphi \in [\Gamma]$. *Then,* $|\downarrow(t{:}\varphi)| < \ulcorner t\urcorner{\cdot}(\ulcorner t\urcorner + \ulcorner\Gamma\urcorner)$.

Proof. This follows from a straightforward counting argument: if $s{:}\psi \in \downarrow(t{:}\varphi)$, there are at most $\ulcorner t\urcorner$ choices for s, and $\ulcorner s\urcorner + \ulcorner\Gamma\urcorner \leq \ulcorner t\urcorner + \ulcorner\Gamma\urcorner$ choices for ψ, since $s{:}\psi$ must be balanced and, by our conventions, any subexpression ϵ of any formula in Γ must satisfy $\ulcorner\epsilon\urcorner < \ulcorner\Gamma\urcorner$. The inequality is strict because $t{:}\varphi$ is excluded. □

An immediate consequence of Lemma 5.6 is that $\lhd \restriction [\Gamma]$ is a well-order of order type ω.

Definition 5.7 Let Γ be any set of $L_{\text{¡5!}}$-formulae. We define a set $\widetilde{\Gamma} \subseteq [\Gamma]$ by recursion on $\lhd$ as follows.

Fix $\tau \in [\Gamma]$ and assume, inductively, that $\widetilde{\Gamma} \cap \downarrow\tau$ has been defined. Then, $\tau \in \widetilde{\Gamma}$ if and only if one of the following holds:

(i) $\tau \in \Gamma$,

(ii) $\tau =$ ¡φ!:φ and φ is a tautology;

(iii) $\tau = (s \cdot t){:}\varphi$, and there is a formula ψ such that both $s{:}(\psi \to \varphi)$ and $t{:}\psi$ belong to $\widetilde{\Gamma} \cap {\downarrow}\tau$;

(iv) $\tau = (t + s){:}\varphi$ and either $t{:}\varphi$ or $s{:}\varphi$ belongs to $\widetilde{\Gamma} \cap {\downarrow}\tau$;

(v) $\tau = {¡}t{:}\varphi{!}{:}(t{:}\varphi)$ and $t{:}\varphi \in \widetilde{\Gamma} \cap {\downarrow}\tau$, or

(vi) $\tau = {¡}{\neg}t{:}\varphi{!}{:}({\neg}t{:}\varphi)$ and $t{:}\varphi \notin \widetilde{\Gamma} \cap {\downarrow}\tau$.

Although we have only closed $\widetilde{\Gamma}$ under restricted versions of the clauses for the term operations, $\widetilde{\Gamma}$ is actualy closed under the unrestricted versions, as we show in the following lemma.

Lemma 5.8 *Given finite $\Gamma \subseteq L_{¡5!}$ and arbitrary terms t, s and arbitrary formulae φ, ψ,*

(i) *if φ is a tautology then ${¡}\varphi{!}{:}\varphi \in \widetilde{\Gamma}$;*

(ii) *if both $s{:}(\psi \to \varphi)$ and $t{:}\psi$ belong to $\widetilde{\Gamma}$ then $(s \cdot t){:}\varphi \in \widetilde{\Gamma}$;*

(iii) *if either $t{:}\varphi$ or $s{:}\varphi$ belongs to $\widetilde{\Gamma}$ then $(s + t){:}\varphi \in \widetilde{\Gamma}$;*

(iv) *if $t{:}\varphi \in \widetilde{\Gamma}$ then ${¡}t{:}\varphi{!}{:}(t{:}\varphi) \in \widetilde{\Gamma}$;*

(v) *if $t{:}\varphi \notin \widetilde{\Gamma}$ then ${¡}{\neg}t{:}\varphi{!}{:}{\neg}(t{:}\varphi) \in \widetilde{\Gamma}$.*

Proof. (i) As observed above, ${¡}\varphi{!}{:}\varphi$ is always balanced. If φ is a tautology, it follows that ${¡}\varphi{!}{:}\varphi \in [\Gamma]$ and thus ${¡}\varphi{!}{:}\varphi \in \widetilde{\Gamma}$ by definition.

(ii) If both $s{:}(\psi \to \varphi)$ and $t{:}\psi$ belong to $\widetilde{\Gamma}$ then by definition, $s{:}(\psi \to \varphi), t{:}\psi \in [\Gamma]$. Moreover, $\ulcorner s \urcorner, \ulcorner t \urcorner < \ulcorner s \cdot t \urcorner$, whence $s{:}(\psi \to \varphi), t{:}\psi \lhd (s \cdot t){:}\varphi$. Meanwhile, φ occurs in $\psi \to \varphi$, which occurs in s, which occurs in $s \cdot t$, hence $(s \cdot t){:}\varphi$ is balanced. It follows by definition that $(s \cdot t){:}\varphi \in \widetilde{\Gamma}$.

(iii) If $s{:}\varphi \in \widetilde{\Gamma}$, then it is balanced. Reasoning as above, $(s + t){:}\varphi$ is also balanced and $s{:}\varphi \lhd (s + t){:}\varphi$. It follows that $(s + t){:}\varphi \in \widetilde{\Gamma}$; the case for $t{:}\varphi \in \widetilde{\Gamma}$ is symmetric.

(iv) As before, ${¡}t{:}\varphi{!}{:}t{:}\varphi$ is balanced regardless of t, φ, and since $\ulcorner t \urcorner < \ulcorner t{:}\varphi \urcorner < \ulcorner {¡}t{:}\varphi{!} \urcorner$, we have that $t{:}\varphi \lhd {¡}t{:}\varphi{!}{:}t{:}\varphi$. Moreover, if $t{:}\varphi \in \widetilde{\Gamma}$, then it must be balanced, so $t{:}\varphi \in {\downarrow}\,({¡}t{:}\varphi{!}{:}t{:}\varphi)$, which by definition implies that ${¡}t{:}\varphi{!}{:}t{:}\varphi \in \widetilde{\Gamma}$.

(v) Assume that $t{:}\varphi \notin \widetilde{\Gamma}$. Then, $t{:}\varphi \notin \widetilde{\Gamma} \cap {\downarrow}({¡}{\neg}t{:}\varphi{!}{:}{\neg}t{:}\varphi)$, and we know that ${¡}{\neg}t{:}\varphi{!}{:}{\neg}t{:}\varphi \in [\Gamma]$, so by definition ${¡}{\neg}t{:}\varphi{!}{:}{\neg}t{:}\varphi \in \widetilde{\Gamma}$, as desired. □

Of course, $\widetilde{\Gamma}$ is not actually a maximal-consistent set, but the set of its consequences is.

Definition 5.9 Let Γ be a saturated, consistent set of $L_{¡5!}$-formulae. We define $\Gamma \mathrel{|\!\sim} \varphi$ by induction on φ as follows:

(i) For any propositional variable p, $\Gamma \mathrel{|\!\sim} p$ if and only if $p \in \Gamma$.

(ii) If $t{:}\varphi$ is a verification, then $\Gamma \mathrel{|\!\sim} t{:}\varphi$ if and only if $t{:}\varphi \in \widetilde{\Gamma}$.

(iii) $\Gamma \mathrel{|\!\sim} {\neg}\varphi$ if and only if $\Gamma \not\mathrel{|\!\sim} \varphi$, and

(iv) $\Gamma \mathrel{|\!\sim} \psi \to \varphi$ if and only if either $\Gamma \not\mathrel{|\!\sim} \psi$ or $\Gamma \mathrel{|\!\sim} \varphi$.

The following lemma shows that $\widetilde{\Gamma}$ is not that far away from Γ.

Lemma 5.10 *Let Γ be a consistent set of formulae.*

(i) *If $t{:}\varphi \in \widetilde{\Gamma}$ and t occurs in Γ, then φ also occurs in Γ, and*

(ii) *if $\neg t{:}\varphi \in \Gamma$ then $t{:}\varphi \notin \widetilde{\Gamma}$.*

Lemma 5.10 is proved by induction. We omit the details.

Lemma 5.11 *Let Γ be any finite, consistent, saturated set of formulae.*

(i) *If φ is a tautology, then $\Gamma \vdash\!\!\sim \varphi$.*

(ii) *If $\varphi \in \Gamma$ then $\Gamma \vdash\!\!\sim \varphi$.*

(iii) *Whenever $t{:}\varphi \in \widetilde{\Gamma}$, it follows that $\Gamma \vdash\!\!\sim \varphi$.*

Proof. We only sketch the proof. For the first item: proceed by a simple induction using clauses (iii) and (iv) of the definition, treating expressions of the form $t{:}\varphi$ as separate propositional variables. The second item follows by an easy induction on the length of φ using the fact that Γ is consistent and saturated.

For the last item: if $t{:}\varphi \in \Gamma$, then $\varphi \in \Gamma$ by Lemma 5.3(iii), and thus by the previous item, $\Gamma \vdash\!\!\sim \varphi$. Hence we may assume that $t{:}\varphi \notin \Gamma$. The result then follows by induction on t. □

Our goal in the remainder of this section is to prove the next lemma. It will be crucial for defining the arithmetical interpretations needed for the proof of Theorem 4.4, and implies that membership in $\widetilde{\Gamma}$ is elementary.

Lemma 5.12 *There is a Δ_0 formula $\mathtt{Comp}_\Gamma(x)$ such that, for all verifications τ, $\tau \in \widetilde{\Gamma}$ if and only if $\mathtt{Comp}_\Gamma(\ulcorner\tau\urcorner)$ holds.*

Towards a proof of Lemma 5.12, we define some auxiliary notions.

Definition 5.13 Given any finite set $\Gamma \subseteq L_{\text{¡5!}}$, we say that a sequence $(\sigma_0, \dots, \sigma_n)$ of Γ-balanced verifications is an *initial $\lhd$-segment* if, for all verifications τ and all $j \leq n$, $\tau \in {\downarrow}\sigma_j$ if and only if $\tau = \sigma_i$ for some $i \leq j$. We say that $(\sigma_0, \dots, \sigma_n)$ *contains* τ if $\tau = \sigma_i$ for some $i \leq n$.

A sequence $(x_0, \dots, x_n)$ *codes an initial $\lhd$-segment* if there is an initial $\lhd$-segment $(\sigma_0, \dots, \sigma_n)$ such that $x_i = \ulcorner\sigma_i\urcorner$ for all $i \leq n$.

An initial $\lhd$-segment is simply an initial segment of the well-ordering $\lhd \restriction [\Gamma]$, so that it is uniquely determined by its last element.

Lemma 5.14 *There is an elementary function $K(x)$ such that if $\tau \in [\Gamma]$, then there is some $y < K(\ulcorner\tau\urcorner)$ coding an initial $\lhd$-segment containing τ.*

Proof. For each x that does not code some $\tau \in [\Gamma]$, we set $K(x) = 0$. If x does code such a τ, we will give a value for $K(x)$ such that for some $y < K(x)$, y codes the initial $\lhd$-segment whose last element is τ.

By definition, if $t{:}\varphi \lhd s{:}\psi$, then either $\ulcorner t\urcorner < \ulcorner s\urcorner$ or $t = s$ and $\ulcorner\varphi\urcorner < \ulcorner\psi\urcorner$. By the remark following Definition 5.4, if $\tau = s{:}\psi$ is Γ-balanced then $\ulcorner\psi\urcorner < \max(\ulcorner s\urcorner, \ulcorner\Gamma\urcorner)$. By our conventions on the Gödel numbering, $\ulcorner t{:}\varphi\urcorner$ is

elementarily bounded in $\ulcorner t \urcorner + \ulcorner \varphi \urcorner$, for any verification $t{:}\varphi$. Hence, the Gödel numbers of τ and all of its $\lhd \restriction [\Gamma]$-predecessors are bounded by some M that is elementary in $\ulcorner s \urcorner + \ulcorner \Gamma \urcorner$. It is also clear that the cardinality of the set of $\lhd \restriction [\Gamma]$-predecessors of τ is bounded by M, so that we may set, for example, $K(\ulcorner \tau \urcorner) = B\,(M, M)$. □

Below, recall that a function on the natural numbers is *small* if its domain is finite.

Definition 5.15 Fix a finite set Γ of $L_{¡5!}$-formulae. We say that a small function e is an *initial evaluation* if $\mathrm{dom}(e)$ is an initial $\lhd$-segment, e takes values in $\{0, 1\}$, and for all $\tau \in \mathrm{dom}(e)$ we have that $e(\tau) = 1$ if and only if one of the following occurs:

(i) $\tau \in \Gamma$,

(ii) $\tau = ¡\varphi!{:}\varphi$ and φ is a tautology;

(iii) $\tau = (s \cdot t){:}\varphi$, and $e(s{:}(\psi \to \varphi)) = e(t{:}\psi) = 1$;

(iv) $\tau = (t + s){:}\varphi$ and either $e(t{:}\varphi) = 1$ or $e(s{:}\varphi) = 1$;

(v) $\tau = ¡t{:}\varphi!{:}(t{:}\varphi)$ and $e(t{:}\varphi) = 1$, or

(vi) $\tau = ¡\neg t{:}\varphi!{:}(\neg t{:}\varphi)$ and $e(t{:}\varphi) \neq 1$ (i.e., it is 0 or undefined).

Given any verification τ, define $E(\tau) = 1$ if and only if there exists an initial evaluation e which assigns 1 to τ, and set $E(\tau) = 0$ otherwise.

Observe that if τ is not Γ-balanced, then $E(\tau) = 0$. Otherwise, the value of $E(\tau)$ may be computed in any of several equivalent ways:

Lemma 5.16 *Let $\tau \in [\Gamma]$, $b \in \{0, 1\}$. Then, there is an elementary function $C(x)$ such that the following are equivalent:*

(i) *$E(\tau) = b$,*

(ii) *$e(\tau) = b$ for every initial evaluation e,*

(iii) *$e(\tau) = b$ for some initial evaluation e,*

(iv) *$e(\tau) = b$ for some initial evaluation $e = (\boldsymbol{d}, \boldsymbol{r})$ such that $\ulcorner \boldsymbol{d} \urcorner, \ulcorner \boldsymbol{r} \urcorner < C(\ulcorner \tau \urcorner)$.*

Proof. The lemma is proven by checking that if e, e' are two initial evaluations, then $e(\tau) = e'(\tau)$ whenever the two are defined; this is straightforward and we omit the details. Thus to evaluate $E(\tau)$, it suffices to consider *any* such initial evaluation. The function C bounding the smallest witness can be constructed using the funcion K from Lemma 5.14 and the function B from Section 3.1. □

The function $E(\cdot)$ is useful because it gives us an elementary method to determine whether $\tau \in \widetilde{\Gamma}$.

Lemma 5.17 *For any finite set of formulas $\Gamma \subseteq L$ and any verification τ, $E(\tau) = 1$ if and only if $\tau \in \widetilde{\Gamma}$.*

Proof. If τ is not Γ-balanced, then it is not included in any initial $\lhd$-segment, so $E(\tau) = 0$; on the other hand, $\tau \notin \widetilde{\Gamma}$, so the equivalence holds trivially.

Otherwise, we proceed by induction on τ along $\lhd \restriction [\Gamma]$. In view of Lemma 5.16, it suffices to consider an arbitrary initial evaluation e such that $e(\tau)$ is defined, and prove that $e(\tau) = 1$ if and only if $\tau \in \widetilde{\Gamma}$. If $\tau \in \Gamma$, then $e(\tau) = 1$ and $\tau \in \widetilde{\Gamma}$, so we may assume otherwise. We must then consider several cases depending on τ; we work out only a few as examples.

If, for example, $\tau = (s \cdot t){:}\varphi$ and $e(\tau) = 1$, then $e(s{:}(\psi \to \varphi)) = e(t{:}\psi) = 1$ for some ψ, which by the induction hypothesis means that $s{:}(\psi \to \varphi), t{:}\psi \in \widetilde{\Gamma}$, so that by Lemma 5.8, $\tau \in \widetilde{\Gamma}$. Conversely, if $\tau \in \widetilde{\Gamma}$, then by definition $s{:}(\psi \to \varphi), t{:}\psi \in \widetilde{\Gamma} \cap {\downarrow}\tau$ for some ψ. But since the domain of e is an initial $\lhd$-segment and $e(\tau)$ is defined, we must also have that $s{:}(\psi \to \varphi), t{:}\psi \in \mathrm{dom}(e)$ and thus by the induction hypothesis, $e(s{:}(\psi \to \varphi)) = e(t{:}\psi) = 1$, which means that $e(\tau) = 1$.

Next, we consider the case when τ is of the form ¡$\neg t{:}\varphi$!:$\neg t{:}\varphi$. If $t{:}\varphi$ is not Γ-balanced, then $e(t{:}\varphi)$ is undefined, whence $e(\tau) = 1$; similarly, $t{:}\varphi \notin \widetilde{\Gamma}$, so $\tau \in \widetilde{\Gamma}$. If, instead, $t{:}\varphi$ is Γ-balanced, then again we have that $t{:}\varphi \in \mathrm{dom}(e)$ and thus $e(\tau) = 1 \Leftrightarrow e(t{:}\varphi) = 0 \overset{\text{IH}}{\Leftrightarrow} t{:}\varphi \notin \widetilde{\Gamma} \Leftrightarrow \tau \in \widetilde{\Gamma}$.

Each of the remaining cases is similar to one of the above and is left to the reader. □

Proof of Lemma 5.12. Let $C(\cdot)$ be the bound given by Lemma 5.16. We use $C(\cdot)$ to define $\mathtt{Comp}_\Gamma(x)$ by a natural translation into L_{PA} of:

> *x codes a verification τ and there is a number $y < C(x)$ such that y codes an initial evaluation e with $e(\tau) = 1$.*

The only thing that needs to be verified is that the property 'y codes an initial evaluation' is Δ_0. This is straightforward from Definitions 5.13 and 5.15 and our conventions on coding of sequences, as all quantifiers involved are bounded by x and $\ulcorner\Gamma\urcorner$. □

6 Fixed-point proof predicates

The construction of $\widetilde{\Gamma}$ allows us to constructively extend any saturated, consistent set Γ to a maximal-consistent set of formulas $\{\varphi \in L : \Gamma \nvdash \varphi\}$. Next, we construct an arithmetical interpretation for L tailored specifically for this extended set. This construction relies on a fixed-point argument that we detail in this subsection, very similar to that of [1]. For this completeness proof, it is sufficient to consider simple propositional assignments, in the following sense:

Definition 6.1 A propositional assignment f is *simple* if f is elementary and, for every variable p, either $f(p) = (\ulcorner p \urcorner = \ulcorner p \urcorner)$ or $f(p) = (\ulcorner p \urcorner = 0)$.

Moreover, the arithmetical interpretations resulting from the proof will coincide with the function f given below, for a particular choice of π:

Definition 6.2 Given a formula $\pi = \pi(x, y)$ and a propositional assignment f, we extend f to an auxiliary function $f_\pi \colon L_{\text{¡5!}} \to L_{\mathrm{PA}}$ by letting

- $f_\pi(p) = f(p)$ for any propositional variable p,
- f_π commute with Booleans, and
- $f_\pi(t{:}\varphi) = \pi(\overline{\ulcorner t \urcorner}, \overline{\ulcorner f_\pi(\varphi) \urcorner})$.

Lemma 6.3 *If f is a simple propositional assignment and $\pi(x, y)$ is Δ_0, then $f_\pi(\varphi)$ is Δ_0 for all $\varphi \in L_{\mathsf{j5!}}$. Moreover, if π contains quantifiers and each of x and y appears free in π at least once, then f_π is injective.*

Proof. We prove by induction on $\ulcorner \varphi \urcorner + \ulcorner \psi \urcorner$ that if $f_\pi(\varphi) = f_\pi(\psi)$, then $\varphi = \psi$. If $\varphi = p$ is a propositional variable, then $f_\pi(\varphi)$ does not contain quantifiers or Booleans, and hence neither does $f_\pi(\psi)$. It follows that ψ must also be a propositional variable, which by the injectivity of the Gödel numbering yields $\psi = p$ as well.

Next, consider the case where neither φ nor ψ is of the form $t{:}\theta$. If $\varphi = \varphi_0 \to \varphi_1$, then we must also have that ψ is of the form $\psi_0 \to \psi_1$, since otherwise the outermost connective of $f_\pi(\psi)$ could not be an implication. Then, by the induction hypothesis, $\varphi_0 = \psi_0$ and $\varphi_1 = \psi_1$, so $\varphi = \psi$. The case where $\varphi = \neg\varphi_0$ is analogous.

Finally, suppose that one of φ, ψ is of the form $t{:}\theta$ (say, φ). Then, since $f_\pi(\varphi) = \pi(\overline{\ulcorner t \urcorner}, \overline{\ulcorner f_\pi(\theta) \urcorner})$ contains quantifiers (by our assumption on π), so does $f_\pi(\psi)$, which implies that ψ contains some occurrence of a subformula $\psi' = s{:}\gamma$. But then, if we let $\#\xi$ denote the total number of logical symbols in ξ (Booleans and quantifiers), we see that $\#f_\pi(\varphi) = \#f_\pi(\psi) \geq \#f_\pi(\psi') = \#f_\pi(\varphi)$, where the last equality holds because both formulas are instances of π. Thus $\#f_\pi(\psi) = \#f_\pi(\psi')$, which imples that $\psi = \psi'$. It follows by the injectivity of the Gödel numbering that $t = s$ and $f_\pi(\theta) = f_\pi(\gamma)$, and by the induction hypothesis that $\gamma = \theta$, so that $\varphi = \psi$, as needed. □

Note that if π does not contain quantifiers then f_π may fail to be injective, but proof predicates may always be assumed to contain quantifiers (if they don't, dummy quantifiers can always be introduced).

Lemma 6.4 *Given a simple propositional assignment f, there are elementary functions $f^+ \colon \mathbb{N}^2 \to \mathbb{N}$ and $f^- \colon \mathbb{N}^2 \to \mathbb{N}$ such that, whenever $\pi = \pi(x, y)$ is a predicate that contains quantifiers and has both variables free, and $\varphi \in L_{\mathsf{j5!}}$, then*

- $f^+(\ulcorner \varphi \urcorner, \ulcorner \pi \urcorner) = \ulcorner f_\pi(\varphi) \urcorner$,
- $f^-(\ulcorner f_\pi(\varphi) \urcorner, \ulcorner \pi \urcorner) = \ulcorner \varphi \urcorner$, *and*
- $f^-(\ulcorner \psi \urcorner, \ulcorner \pi \urcorner) = 0$ *for any $\psi \in L_{\mathrm{PA}}$ not lying in the range of f_π.*

Proof. By our assumptions on Gödel numbers, we have that, if n is the number of symbols in $\varphi \in L_{\mathsf{j5!}}$ and the greatest Gödel numbers of a symbol appearing in φ is m, then $n, m \leq \ulcorner \varphi \urcorner$. Meanwhile, for any number k, the length of $\overline{k}$ is $2k{+}1$, so the number of symbols in $f_\pi(\varphi)$ is bounded by $(2(2\ulcorner \varphi \urcorner + 1) + 3)\ulcorner \varphi \urcorner \cdot \ulcorner \pi \urcorner$. Similarly, $\ulcorner v \urcorner < \ulcorner \pi \urcorner$ if v is any variable appearing in π. If we let c be a bound for the Gödel codes of all constants and logical symbols of L_{PA}, we thus see

that every symbol in $f_\pi(\varphi)$ is bounded by $\ulcorner\pi\urcorner + c$. It follows that

$$\ulcorner f_\pi(\varphi)\urcorner < B'(\ulcorner\varphi\urcorner, \ulcorner\pi\urcorner) := B((2(2\ulcorner\varphi\urcorner + 1) + 3)\ulcorner\varphi\urcorner \cdot \ulcorner\pi\urcorner, \ulcorner\pi\urcorner + c),$$

whenever $\varphi \in L_{\text{¡5!}}$ and $\pi(x, y) \in L_{\mathrm{PA}}$. Moreover, $f_\pi(\varphi)$ can be defined recursively on the complexity of φ, and thus we may set $z = f^+(x, y)$ if $z < B'(x, y)$ and there are φ, π such that $x = \ulcorner\varphi\urcorner$, $y = \ulcorner\pi\urcorner$ and $z = \ulcorner f_\pi(\varphi)\urcorner$, and $f^+(x, y) = 0$ if there is no such z. The function f^+ thus defined is clearly elementary.

To define f^-, note that $\ulcorner\varphi\urcorner$ can also be bounded elementarily by some elementary function $B''(\ulcorner f_\pi(\varphi)\urcorner, \ulcorner\pi\urcorner)$ (the actual function may be computed analogously to B' and is inessential). Thus we may set $f^-(x, y) = z$ if $x = f^+(z, x)$ with $z < B''(x, y)$, and otherwise, set $f^-(x, y) = 0$. □

Now that we have studied simple propositional assignments in general, let us relate them to our previous results on saturated sets of formulae. Given a saturated set Γ, we will define a propositional assignment designed to 'agree' with Γ.

Definition 6.5 Fix a set of formulae $\Gamma \subseteq L_{\text{¡5!}}$. Define a propositional assignment f^Γ given by $f^\Gamma(p) = (\ulcorner p\urcorner = \ulcorner p\urcorner)$ if $p \in \widetilde{\Gamma}$, and $f^\Gamma(p) = (\ulcorner p\urcorner = 0)$ if not.

Clearly, if Γ is finite, then f^Γ is simple. Next, we tailor our proof predicates so that they, too, match well with Γ (and f^Γ):

Definition 6.6 Given a formula π and a finite set of formulae $\Gamma \subseteq L_{\text{¡5!}}$, define a new formula

$$\begin{aligned}\mathtt{NewProof}_\pi(x, y) = {} & \mathtt{Proof}(x, y) \\ & \vee \exists t\, \exists \varphi\ (x = \ulcorner t\urcorner \wedge \mathtt{Comp}_\Gamma(\ulcorner t{:}\varphi\urcorner) \wedge y = (f^\Gamma)^+(\ulcorner\varphi\urcorner, \ulcorner\pi\urcorner)).\end{aligned} \tag{3}$$

Lemma 6.7 *If Γ is any finite set of $L_{\text{¡5!}}$ formulae, there is a Δ_0 formula π^Γ containing at least one quantifier, with free variables $\{x, y\}$, and such that*

$$\mathrm{PA} \vdash \forall x \forall y \left(\pi^\Gamma(x, y) \leftrightarrow \mathtt{NewProof}_{\pi^\Gamma}(x, y)\right). \tag{4}$$

Proof. Apply the usual fixed-point theorem. □

The reason why we want the formula π^Γ in Lemma 6.7 to contain at least one quantifier is so that it satisfy the hypotheses of Lemma 6.3. Lemma 6.8 below shows that the valuations given by Lemma 6.10 behave just like we would like them to.

Lemma 6.8 *If Γ is a finite, consistent, saturated set of $L_{\text{¡5!}}$-formulae, then for every formula φ, $\Gamma \mathrel{|\!\sim} \varphi$ if and only if $\mathrm{PA} \vdash f^\Gamma_{\pi^\Gamma}(\varphi)$.*

Proof. In view of Lemma 6.3, $f^\Gamma_{\pi^\Gamma}(\varphi)$ is always Δ_0, so $\mathrm{PA} \vdash f^\Gamma_{\pi^\Gamma}(\varphi)$ is equivalent to $f^\Gamma_{\pi^\Gamma}(\varphi)$. Thus we will only prove that $\Gamma \mathrel{|\!\sim} \varphi$ is equivalent to $f^\Gamma_{\pi^\Gamma}(\varphi)$. We proceed by induction on the complexity of φ, considering several cases.

If $\varphi = p$ for some propositional variable p, then PA $\vdash f^{\Gamma}_{\pi^{\Gamma}}(\varphi)$ exactly when $f^{\Gamma}_{\pi^{\Gamma}}(\varphi) = \ulcorner p \urcorner = \ulcorner p \urcorner$, which is the case if and only if $p \in \Gamma$. But this is equivalent, by definition, to $\Gamma \mid\!\sim \varphi$.

If $\varphi = \psi \to \theta$, we have that $f^{\Gamma}_{\pi^{\Gamma}}(\varphi) = f^{\Gamma}_{\pi^{\Gamma}}(\psi) \to f^{\Gamma}_{\pi^{\Gamma}}(\theta)$. By definition, $\Gamma \mid\!\sim \varphi$ if and only if either $\Gamma \not\mid\!\sim \psi$ or $\Gamma \mid\!\sim \theta$. But this is equivalent, by induction hypothesis, to having that either $\neg f^{\Gamma}_{\pi^{\Gamma}}(\psi)$ or $f^{\Gamma}_{\pi^{\Gamma}}(\theta)$ holds, i.e., that $f^{\Gamma}_{\pi^{\Gamma}}(\psi) \to f^{\Gamma}_{\pi^{\Gamma}}(\theta)$ holds. The case where $\varphi = \neg\psi$ for some formula ψ is similar.

Finally, consider $\varphi = t{:}\psi$. Suppose that $\Gamma \mid\!\sim \varphi$, so that $t{:}\psi \in \widetilde{\Gamma}$ by definition. This is equivalent, by Lemma 5.12, to $\mathtt{Comp}_{\Gamma}(\ulcorner t{:}\psi \urcorner)$ holding, which by (3) yields $\mathtt{NewProof}_{\pi^{\Gamma}}(\ulcorner t \urcorner, \ulcorner \psi \urcorner)$, as well as $\pi^{\Gamma}(\ulcorner t \urcorner, \ulcorner f^{\Gamma}_{\pi^{\Gamma}}(\psi) \urcorner)$ by (4). But the latter is just $f^{\Gamma}_{\pi^{\Gamma}}(\varphi)$, and since this is a Δ_0 formula it follows that PA $\vdash f^{\Gamma}_{\pi^{\Gamma}}(\varphi)$, as needed.

Conversely, suppose that $\Gamma \not\mid\!\sim \varphi$, so that $t{:}\psi \notin \widetilde{\Gamma}$, i.e., $\mathtt{Comp}_{\Gamma}(\ulcorner t{:}\psi \urcorner)$ is false. Since by assumption, $\mathtt{Proof}(\ulcorner t \urcorner, k)$ is false for all k, it follows that $\mathtt{NewProof}_{\pi^{\Gamma}}(\ulcorner t \urcorner, \ulcorner \psi \urcorner)$ is false and hence so is $\pi^{\Gamma}(\ulcorner t \urcorner, \ulcorner f^{\Gamma}_{\pi^{\Gamma}}(\psi) \urcorner)$, i.e., $\neg\pi^{\Gamma}(\ulcorner t \urcorner, \ulcorner f^{\Gamma}_{\pi^{\Gamma}}(\psi) \urcorner)$ is true. But this formula is Δ_0, whence PA $\vdash \neg\pi^{\Gamma}(\ulcorner t \urcorner, \ulcorner f^{\Gamma}_{\pi^{\Gamma}}(\psi) \urcorner) = f^{\Gamma}_{\pi^{\Gamma}}(\varphi)$.

Since we have considered all cases, the lemma follows. □

The following lemma shows that the predicate π^{Γ} is extensionally correct.

Lemma 6.9 *Let Γ be any finite, consistent, and saturated set of $L_{\mathsf{j5!}}$-formulae. Then, for any $\varphi \in L_{\mathrm{PA}}$,* PA $\vdash \varphi$ *if and only if* $\exists x\, \pi^{\Gamma}(x, \ulcorner \varphi \urcorner)$ *holds.*

Proof. One direction is obvious from (3), since $\mathtt{Proof}(k, \ulcorner \varphi \urcorner)$ implies that $\mathtt{NewProof}_{\pi^{\Gamma}}(k, \ulcorner \varphi \urcorner)$, and thus that $\pi^{\Gamma}(k, \ulcorner \varphi \urcorner)$.

For the other, we note that if $\pi^{\Gamma}(k, \ulcorner \varphi \urcorner)$ holds, either we already have that $\mathtt{Proof}(k, \ulcorner \varphi \urcorner)$, or else $k = \ulcorner t \urcorner$ for some term t and $\varphi = f^{\Gamma}_{\pi^{\Gamma}}(\theta)$ for some $\theta \in L_{\mathsf{j5!}}$ such that $t{:}\theta \in \widetilde{\Gamma}$, which by definition means that $\Gamma \mid\!\sim t{:}\theta$. By Lemma 5.11, $\Gamma \mid\!\sim \theta$, and thus PA $\vdash \varphi$ by Lemma 6.8. □

The following is the main technical lemma:

Lemma 6.10 *Given a finite, consistent, saturated set of formulae Γ, there are elementary functions $\mathsf{m}^*, \mathsf{a}^*, \mathsf{v}^*$ such that $\mathfrak{S}^* = (f^{\Gamma}, \pi^{\Gamma}, \mathsf{m}^*, \mathsf{a}^*, \mathsf{v}^*)$ is a robust arithmetical interpretation and satisfies $\varphi^{\mathfrak{S}} = f^{\Gamma}_{\pi^{\Gamma}}(\varphi)$ for all $\varphi \in L_{\mathsf{j5!}}$.*

Theorem 4.4 readily follows from Lemma 6.10:

Proof of Theorem 4.4. By Lemma 5.2, if φ is consistent, then it can be included in a finite, consistent, saturated set Γ. By Lemma 6.8, if $\Gamma \mid\!\sim \gamma$, then PA $\vdash f^{\Gamma}_{\pi_{\Gamma}}(\gamma)$; in particular, PA $\vdash f^{\Gamma}_{\pi_{\Gamma}}(\varphi)$. By Lemma 6.10, there is a robust arithmetical interpretation $\mathfrak{S}^*$ which satisfies $\psi^{\mathfrak{S}^*} = f^{\Gamma}_{\pi^{\Gamma}}(\psi)$ for all $\psi \in L_{\mathsf{j5!}}$. It follows that PA $\vdash \varphi^{\mathfrak{S}^*}$, as needed. □

Hence, it remains to prove Lemma 6.10. The proof uses the following fact:

Lemma 6.11 *If φ is Δ_0, then there is an elementary function $b(\cdot)$ such that then* PA $\vdash \varphi(x) \wedge x < u \to \exists z \leq b(u)\ \pi_f(z, \ulcorner \varphi(x) \urcorner)$.

Proof. If φ is Δ_0, then PA proves that for all $x \in \mathbb{N}$ such that $\varphi(x)$ holds, there is some $z \leq 2_l^u$ with $\mathtt{Proof}(z, \ulcorner \varphi(x) \urcorner)$, where l is some constant that depends only on φ (see, for example, [8]). But then, once we have $\mathtt{Proof}(z, \ulcorner \varphi(x) \urcorner)$, we also have $\pi_f(z, \ulcorner \varphi(x) \urcorner)$ using Lemma 6.7 and the definition of $\mathtt{NewProof}$, so we may take $b(u) = 2_l^u$. □

Proof of Lemma 6.10. Let a_{PA} and m_{PA} be the computable functions introduced immediately after Definition 4.1, and $\mu x.\varphi(x)$ denote the least x satisfying φ, if it exists. We define $\mathsf{a}^*(n,k) = \ulcorner t + s \urcorner$ if both $n = \ulcorner t \urcorner$ and $k = \ulcorner s \urcorner$ for some proof terms s and t. If neither n nor k code proof terms, set $\mathsf{a}^*(n,k) = \mathsf{a}_{\mathrm{PA}}(n,k)$. Otherwise if, say, only n codes a proof term, define $\mathsf{a}^*(n,k) = \mathsf{a}_{\mathrm{PA}}(y,k)$, where $y = \mu x. \forall \varphi \in [\![n]\!]_{\pi^\Gamma} \mathtt{Proof}(x, \ulcorner f^\Gamma_{\pi^\Gamma}(\varphi) \urcorner)$. As we show, the existence of such a y follows from the fact that by Lemma 6.9, $\mathrm{PA} \vdash f^\Gamma_{\pi^\Gamma}(\varphi)$ for each $\varphi \in [\![n]\!]_{\pi^\Gamma}$. Indeed, this implies that for each $\varphi_i \in [\![n]\!]_{\pi^\Gamma} =: \{\varphi_0, \dots, \varphi_n\}$, we can find some z_i such that $\mathtt{Proof}(z_i, \ulcorner f^\Gamma_{\pi^\Gamma}(\varphi_i) \urcorner)$. Define $x_0 = z_0$ and $x_{i+1} = \mathsf{a}_{\mathrm{PA}}(x_i, z_{i+1})$. Hence, $x = x_n$ witnesses that y above is well-defined. If only k codes a proof term, define $\mathsf{a}^*(n,k)$ symmetrically.

Analogously, set $\mathsf{m}^*(n,k) = \ulcorner t \cdot s \urcorner$ if both $n = \ulcorner t \urcorner$, and $k = \ulcorner s \urcorner$ for some proof terms s, t; $\mathsf{m}^*(n,k) = \mathsf{m}_{\mathrm{PA}}(n,k)$ if n and k do not code proof terms; $\mathsf{m}^*(n,k) = \mathsf{m}_{\mathrm{PA}}(y,k)$ if only n codes a proof term, where $y = \mu x. \forall \varphi \in [\![n]\!]_{\pi^\Gamma} \mathtt{Proof}(x, \ulcorner f^\Gamma_{\pi^\Gamma}(\varphi) \urcorner)$. The existence of such a y is proved as before. The remaining case is defined symmetrically.

We want to show that a^* and m^* are computable. From Lemma 5.12 and Lemma 6.7 follows that π^Γ is computable. By assumption, the set of codes of proof terms is elementary. Thus, it suffices to show that $x \mapsto [\![x]\!]_{\pi^\Gamma}$ is computable.

Claim 1 *For all x, $[\![x]\!]_{\pi^\Gamma}$ is finite, and the function $x \mapsto [\![x]\!]_{\pi^\Gamma}$ is computable.*

Proof. By Lemma 6.7, $y \in [\![x]\!]_{\pi^\Gamma}$ if and only if either $\mathtt{Proof}(x,y)$ or x and y respectively code expressions t and $f^\Gamma_{\pi^\Gamma}(\varphi)$ such that $t{:}\varphi \in \widetilde{\Gamma}$. By our conventions on Gödel numbering, at most one of these alternatives occurs, and which one does—if any—is determined by whether x codes a proof term. If it does not, then the desired result is immediate, as $[\![\cdot]\!]_{\mathtt{Proof}}$ is finite-valued and computable by assumption. Otherwise, $x = \ulcorner t \urcorner$ for some proof term t and $\pi^\Gamma(x,y)$ holds. Then y codes some formula $f^\Gamma_{\pi^\Gamma}(\varphi)$ with $\varphi \in \widetilde{\Gamma}$. Recovering φ from y is elementary by Lemma 6.4, and so too is deciding whether $\varphi \in \widetilde{\Gamma}$, by Lemma 5.12. The expression $t{:}\varphi$ is Γ-balanced, whence φ either occurs in t or in Γ. Hence, the Gödel number of any π^Γ-conclusion of x is bounded by $x + \ulcorner \Gamma \urcorner$, and we can computably enumerate all of them. □

Claim 2 $(\pi^\Gamma, \mathsf{m}^*, \mathsf{a}^*)$ *is a normal proof system.*

Proof. Note that the formula π^Γ is Δ_0 by Lemma 6.7, and each $x \in \mathbb{N}$ has only finitely-many π^Γ-conclusions by Claim 1. Moreover, a^* and m^* satisfy the required conditions—we prove this for m^*. Clearly, whenever k and n do not code proof terms, then $\pi^\Gamma(\mathsf{m}^*(n,k), \ulcorner \psi \urcorner)$ is true if so too are $\pi^\Gamma(n, \ulcorner \varphi \to \psi \urcorner)$ and $\pi^\Gamma(k, \ulcorner \varphi \urcorner)$, as π^Γ is essentially the predicate $\mathtt{Proof}$ in this case. Meanwhile,

$\mathsf{m}^*(n,k) = \mathsf{m}_{\mathrm{PA}}(n,k)$ in this case, which is computable by assumption.

If only k codes a proof term s and $\varphi = f^{\Gamma}_{\pi^\Gamma}(\theta)$ for some $\theta \in L_{\text{¡5!}}$, then by (3), $\pi^\Gamma(n, \ulcorner\varphi \to \psi\urcorner)$ and $\pi^\Gamma(k, \ulcorner\varphi\urcorner)$ yield $\mathtt{Proof}(n, \ulcorner\varphi \to \psi\urcorner)$ and $\mathtt{Comp}_\Gamma(\ulcorner s{:}\theta\urcorner)$. In this case, $\mathsf{m}^*(n,k)$ is defined as $\mathsf{m}_{\mathrm{PA}}(n,y)$, where y is least such that $\forall \phi \in [\![k]\!]_{\pi^\Gamma}\, \mathtt{Proof}(y, \ulcorner f^{\Gamma}_{\pi^\Gamma}(\phi)\urcorner)$. Moreover, y can be computed from k, since $[\![\cdot]\!]_{\pi^\Gamma}$ and $\mathtt{Proof}$ are computable, and hence so is $\mathsf{m}_{\mathrm{PA}}(n,k)$. The case where only n codes a proof term is symmetric, and if n and k respectively code proof terms t and s, so that, say, $\varphi = f^{\Gamma}_{\pi^\Gamma}(\theta)$ and $\psi = f^{\Gamma}_{\pi^\Gamma}(\chi)$, then we obtain $\mathtt{Comp}_\Gamma(\ulcorner s{:}\theta\urcorner)$, as well as $\mathtt{Comp}_\Gamma(\ulcorner t{:}\theta \to \chi\urcorner)$, which together imply $\mathtt{Comp}_\Gamma(\ulcorner t \cdot s{:}\chi\urcorner)$ and thus $\pi^\Gamma(\mathsf{m}^*(n,k), \ulcorner\psi\urcorner)$. Clearly, the map $t, s \mapsto \ulcorner t \cdot s\urcorner$ is computable.

A similar argument shows that a^* also has the required properties, and thus $(\pi^\Gamma, \mathsf{m}^*, \mathsf{a}^*)$ is a normal proof system, as claimed. □

To define v^*, we need an auxiliary function. Let $b_t(x)$ be an elementary function such that whenever x codes a tautology, then $\mathtt{Proof}(k,z)$ holds for some $k < b_t(x)$; such a function can easily be computed for any reasonable proof system and is typically exponential. Whenever x codes a Δ_0 formula ϕ, define $b_x(\cdot)$ to be the function obtained by applying Lemma 6.11 to ϕ, so that $\phi(k)$ and $k < u$ imply $\pi^\Gamma(z, \ulcorner\phi(k)\urcorner)$ for some $z < b_x(u)$. Set $\mathsf{v}_{\mathrm{PA}}(x) = \mu y < b_x(x) + b_t(x).\, \pi^\Gamma(y,x)$ if such a y exists, and $\mathsf{v}_{\mathrm{PA}}(x) = 0$ otherwise. The function b_x is computable, whence so too is v_{PA}.

If $\pi^\Gamma(k,\, \varphi)$ holds, then, as it is a true Δ_0 sentence and $k < \ulcorner\pi^\Gamma(k,\, \varphi)\urcorner$, it follows that $\mathsf{v}_{\mathrm{PA}}(\ulcorner\pi^\Gamma(k,\, \varphi)\urcorner)$ is nonzero (here, we take $\phi(\cdot) = \pi^\Gamma(\cdot,\, \varphi)$). Hence,

$$\pi^\Gamma(k,\, \varphi) \to \pi^\Gamma(\mathsf{v}_{\mathrm{PA}}(\ulcorner\pi^\Gamma(k,\varphi)\urcorner),\, \ulcorner\pi^\Gamma(k,\varphi)\urcorner)$$

is valid. More generally, for any Δ_0-formula ϕ— in particular, for $\phi = \neg\pi^\Gamma(\cdot,\, \varphi)$— we have

$$\phi \to \pi^\Gamma(\mathsf{v}_{\mathrm{PA}}(\ulcorner\phi\urcorner),\, \ulcorner\phi\urcorner). \tag{5}$$

We also have $\varphi \to \pi^\Gamma(\mathsf{v}_{\mathrm{PA}}(\ulcorner\varphi\urcorner), \varphi)$, whenever φ is a tautology. Given this, define $\mathsf{v}^*(x) = \ulcorner\text{¡}\varphi\text{!}\urcorner$ if $x = \ulcorner f^{\Gamma}_{\pi^\Gamma}(\varphi)\urcorner$ for some φ in the domain of $\text{¡}\cdot\text{!}$, and $\mathsf{v}^*(x) = \mathsf{v}_{\mathrm{PA}}(x)$ if no such φ exists. We may now define $\mathfrak{S}^* = (f^\Gamma, \pi^\Gamma, \mathsf{m}^*, \mathsf{a}^*, \mathsf{v}^*)$.

Claim 3 *If t is any term of $L_{\text{¡5!}}$, then $t^{\mathfrak{S}^*} = \ulcorner t\urcorner$, and if φ is any formula, $\varphi^{\mathfrak{S}^*} = f^{\Gamma}_{\pi^\Gamma}(\varphi)$.*

Proof. We prove both claims simultaneously by induction on any expression ϵ of $L_{\text{¡5!}}$. Consider first the case where ϵ is a formula. We have that $p^{\mathfrak{S}^*} = f^\Gamma(p) = f^{\Gamma}_{\pi^\Gamma}(p)$ is true for atomic p and, by definition, $f^{\Gamma}_{\pi^\Gamma}$ and $\cdot^{\mathfrak{S}^*}$ both commute with Booleans. For a formula $t{:}\theta$, we use the identity $t^{\mathfrak{S}^*} = \ulcorner t\urcorner$ to see that $f^{\Gamma}_{\pi^\Gamma}(t{:}\theta) = \pi^\Gamma(\overline{\ulcorner t\urcorner}, \overline{\ulcorner f^{\Gamma}_{\pi^\Gamma}(\theta)\urcorner}) \overset{\text{IH}}{=} \pi^\Gamma(\overline{t^{\mathfrak{S}^*}}, \overline{\ulcorner\theta^{\mathfrak{S}}\urcorner}) = (t{:}\theta)^{\mathfrak{S}}$.

Now assume that ϵ is a term. We must consider several cases, depending on the form of ϵ, and use the definitions of a^*, m^*, and v^* to show that $\epsilon^{\mathfrak{S}^*} = \ulcorner\epsilon\urcorner$. We only consider two cases as examples. If $\epsilon = \text{¡}\varphi\text{!}$, $\text{¡}\varphi\text{!}^{\mathfrak{S}^*} = \mathsf{v}^*(\varphi^{\mathfrak{S}^*}) \overset{\text{IH}}{=}$

$\mathsf{v}^*(f^{\Gamma}_{\pi^\Gamma}(\varphi)) = \ulcorner ¡\varphi!\urcorner$; similarly, $(t \cdot s)^{\mathfrak{S}^*} = \mathsf{m}^*(t^{\mathfrak{S}^*}, s^{\mathfrak{S}^*}) \overset{\text{IH}}{=} \mathsf{m}^*(\ulcorner t\urcorner, \ulcorner s\urcorner) = \ulcorner t \cdot s\urcorner$. Considering $\epsilon = t + s$ and $\epsilon = x$ concludes the proof. □

Finally, note that $x = \ulcorner f^{\Gamma}_{\pi^\Gamma}(\varphi)\urcorner$ for some φ in the domain of $¡\cdot!$ iff x codes a formula in the range of $f^{\Gamma}_{\pi^\Gamma}$, iff $f^-(x, \ulcorner \pi^\Gamma \urcorner) > 0$, and the function f^- is elementary by Lemma 6.4. Therefore, v^* is computable. It follows that $\mathfrak{S}^*$ is an arithmetical interpretation, and by (5), it is robust.

This finishes the proof of Lemma 6.10. □

7 An afterword on realizability

Recall that $\mathsf{S5}$ is the normal modal logic generated by positive and negative introspections, and the reflection axiom T: $\Box p \to p$. The purpose of introducing $\mathsf{VS5}$ is to obtain a justification logic which combines two properties:

(i) it realizes $\mathsf{S5}$, and

(ii) it is sound and complete for its arithmetical interpretation.

In this article we have proven the second point and we leave the first for future work. However, in this section we will say a few words about it.

Let us use $(\cdot)^\Box$ to denote the "forgetful projection," which recursively replaces instances of $t{:}\varphi$ by $\Box(\varphi)^\Box$, commutes with Booleans and fixes propositional variables. Then, the following can be easily verified by induction on the length of a derivation:

Theorem 7.1 *For $\varphi \in L_{¡5!}$, if φ is derivable in $\mathsf{VS5}$ then $(\varphi)^\Box$ is derivable in $\mathsf{S5}$.*

A more interesting property would be the converse of this result; if we are given φ in the modal language such that $\mathsf{S5} \vdash \varphi$, can we find a formula φ^r in $L_{¡5!}$ such that $(\varphi^r)^\Box = \varphi$ and $\mathsf{VS5} \vdash \varphi$? Such a φ^r is a *realization* of φ. Let us see that all axioms of the respective modal logics have realizations.

Theorem 7.2 *If φ is an axiom of $\mathsf{S5}$, then there is $\varphi^r \in L_{¡5!}$ such that $(\varphi^r)^\Box = \varphi$ and $\mathsf{VS5} \vdash \varphi$.*

Proof. Let x, y be arbitrary term variables.

- $\Box(p \to q) \to (\Box p \to \Box q)$ is realized by $x{:}(p \to q) \to (y{:}p \to (x \cdot y){:}q)$;
- $\Box p \to p$ is realized by $x{:}p \to p$;
- $\Box p \to \Box\Box p$ is realized by $x{:}p \to ¡x{:}p!{:}(x{:}p)$, and
- $\neg\Box p \to \Box\neg\Box p$ is realized by $\neg x{:}p \to ¡\neg x{:}p!{:}(\neg x{:}p)$.

□

Thus we see that it is relatively straightforward to realize axioms of $\mathsf{S5}$. One would then expect to be able to 'cobble together' such realizations so as to realize more complex theorems, and while doing so is not trivial, it is possible for $\mathsf{JS5}$. We believe this to also be the case for $\mathsf{VS5}$, but leave it for future work. Thus we conclude our discussion on realizations with the following conjecture:

Conjecture 7.3 *If* $\mathsf{S5} \vdash \varphi$*, then there is* $\varphi^r \in L_{\text{¡5!}}$ *such that* $(\varphi^r)^\Box = \varphi$ *and* $\mathsf{VS5} \vdash \varphi^r$*.*

Acknowledgements. This work was inspired by discussions with Sergei Artemov and Melvin Fitting at the Second International Wormshop in Mexico City, 2014. Specifically, the issues with modeling negative introspection were brought to our attention by Fitting, and both later provided helpful comments for preparing this paper. We are also indebted to Lev Beklemishev, Eric Pacuit and Fernando Velázquez-Quesada for kindly answering our questions about justification logics.

References

[1] Artemov, S. N., *Explicit provability and constructive semantics*, Bulletin of Symbolic Logic **7** (2001), pp. 1–36.
[2] Artemov, S. N. and M. Fitting, *Justification logic*, in: E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*, 2012, fall 2012 edition .
URL
`http://plato.stanford.edu/archives/fall2012/entries/logic-justification/`
[3] Artemov, S. N., E. Kazakov and D. Shapiro, *On logic of knowledge with justifications*, Technical Report CFIS **99-12** (1999).
[4] Boolos, G. S., "The Logic of Provability," Cambridge University Press, Cambridge, 1993.
[5] Fitting, M., *The logic of proofs, semantically*, Annals of Pure and Applied Logic **132** (2004), pp. 1–25.
[6] Fitting, M., *The realization theorem for* S5*: a simple, constructive proof*, in: *Games, Norms and Reasons*, Synthese Library **353**, Springer Science+Business Media B.V., 2011 pp. 61–76.
[7] Goris, E., *Feasible operations on proofs: the logic of proofs for bounded arithmetic*, Theory of Computing Systems **43** (2008), p. 185203.
[8] Hájek, P. and P. Pudlák, "Metamathematics of First Order Arithmetic," Springer-Verlag, Berlin, Heidelberg, New York, 1993.
[9] Kuznets, R. and T. Studer, *Update as evidence: Belief expansion*, in: S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science: International Symposium, LFCS 2013, San Diego, CA, USA, January 6-8, 2013. Proceedings*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013 pp. 266–279.
[10] Kuznets, R. and T. Studer, *Weak arithmetical interpretations for the logic of proofs*, Logic Journal of IGPL (2016).
[11] Pacuit, E., *A note on some explicit modal logics*, ILLC tech report (2006).
[12] Rubtsova, N., *On realization of* S5*-modality by evidence terms*, J. Log. Comput. **16** (2006), pp. 671–684.