Logic of proofs with complexity operators

Sergei Artëmov*
Steklov Mathematical Institute,
Vavilov str. 42,
Moscow 117966, RUSSIA
email:sergei@artemov.mian.su

Artëm Chuprina
Mathematical Logic Section
Department of Mathematics
Moscow State University
Moscow 119899, RUSSIA

1 Introduction.

In [1] the modal provability logic was enriched by new operators (labeled modalities) for individual proofs. The resulting *logic of proofs* was intended to meet some needs of the computer science, where not only provability is of interest but also proofs themselves. Decent algebraic models for the logic of proofs are still to be invented. Such models should probably provide a natural extension of the notion of Magari Algebras, which are also known as Diagonalizable Algebras [4].

In the current paper we add to the logic of proofs also new labeled modalities which stand for the complexity of proofs. The Kripke style completeness, decidability, and arithmetical completeness theorems are obtained.

The *complexity logics* introduced here correspond to two major classes of complexity measures: decidable and recursively enumerable ones; the completeness theorems thus relate either of these logics to the entire class of the relevant complexity measures.

A logic of a specific complexity measure may depend on particular details of proof coding; the logics from the current paper may turn out to be incomplete with respect to some individual complexity measure. However, the completeness theorems from this paper give us a clear idea about what axioms one should add to these logics in order to reach the completeness in a specific case, and what sort of models (Kripke, arithmetical) are relevant to complexity measures.

In what follows we assume, for short, the Peano Arithmetic $\mathtt{PA}$ to be the basic theory for proof and provability predicates. We denote the usual Gödel proof predicate "x is a gödelnumber of a proof of the formula with the gödelnumber y" as $Proof(x, y)$

*Supported by the grant # 93-011-16015 of the Russian Foundation for Fundamental Research and by the Netherlands Organization for Scientific Research (NWO).

and the usual provability predicate as $Provable(y)$, i.e. $Provable(y)$ coincides with $\exists x Proof(x,y)$.

1.1 Definition. An arithmetical formula $Prf(x,y)$ is called a **standard proof predicate** (cf.[2, 1]) iff

1. $Prf(x,y)$ is equivalent in $\mathtt{PA}$ to a recursive formula;
2. $Prf(x,y)$ numerates the theorems of $\mathtt{PA}$:

$$\mathtt{PA} \vdash \varphi \iff \text{for some } n \in \omega \ Prf(n, \ulcorner\varphi\urcorner) \text{ is true;}^1$$

3. the formula $Pr(y) := \exists x Prf(x,y)$ satisfies:

$$\mathtt{PA} \vdash (Pr(x) \& Pr(x \dot{\to} y)) \to Pr(y)^2$$

$$\mathtt{PA} \vdash \sigma \to Pr(\ulcorner\sigma\urcorner)$$

for every arithmetical Σ^0_1-sentence σ;

1.2 Definition. A standard proof predicate Prf is **functional** if for all $l, m, n \in \omega$

$$Prf(l,m),\ Prf(l,n) \implies m = n.$$

1.3 Definition. An arithmetical formula $Cpl(x,y)$ is called a **standard complexity predicate** iff

1. $Cpl(x,y)$ is equivalent in $\mathtt{PA}$ to a recursively enumerable formula;
2. $Cpl(x,y)$ numerates the theorems of $\mathtt{PA}$:

$$\mathtt{PA} \vdash \varphi \iff \text{for some } n \in \omega \ Cpl(n, \ulcorner\varphi\urcorner) \text{ is true,}$$

3. the formula $Prv(y) := \exists x Cpl(x,y)$ satisfies:

$$\mathtt{PA} \vdash (Prv(x) \& Prv(x \dot{\to} y)) \to Prv(y)$$

$$\mathtt{PA} \vdash \sigma \to Prv(\ulcorner\sigma\urcorner)$$

for every Σ^0_1 arithmetical sentence σ;

[1] In this paper we do not distinguish between the natural number n and its numeral $\overline{n}$. As usual, $\ulcorner\varphi\urcorner$ denotes the gödelnumber of φ.

[2] $\dot{\to}$ denotes the term with two free variables, such that for any arithmetical formulas B and C, $\ulcorner B\urcorner \dot{\to} \ulcorner C\urcorner = \ulcorner B \to C\urcorner$.

4. $Cpl(x, y)$ is (provably in $\mathtt{PA}$) monotone on the first argument, i.e.

$$\mathtt{PA} \vdash u \leq v \rightarrow [Cpl(u, y) \rightarrow Cpl(v, y)].$$

1.4 Definition. A standard complexity predicate is called **recursive** if it is equivalent in $\mathtt{PA}$ to a recursive formula.

1.5 Definition. Two predicates Prf and Cpl are called **provably compatible** if

$$\mathtt{PA} \vdash \forall y (Prv(y) \leftrightarrow Pr(y)).$$

Note that the complexity of proof and proof itself are of different character: complexity domain (the set of natural numbers) is linearly ordered, but proofs have no natural linear ordering. So for a modal description of this two notions we introduce two different sorts of variables, and assume that proof and complexity predicates are provably compatible. On the other hand, each standard decidable complexity predicate $Cpl(x, y)$ coincides with $\exists t \leq x Prf(t, y)$ for an appropriate standard proof predicate Prf. In this case we may identify proof variables and complexity variables in a natural way; while considering decidable complexity measures we will suppose that $Cpl(x, y) = \exists t \leq x Prf(t, y)$.

A labeled modal language $\mathcal{L}^{++}$ contains three sorts of variables, $p_0, p_1, \ldots$ (called *proof variables*), $\alpha_0, \alpha_1, \ldots$ (called *complexity variables*) and $S_0, S_1, \ldots$ (called *sentence variables*), symbol $\rightarrow$ for the classical implication, the truth value $\bot$ for absurdity (the usual Boolean connectives, and the truth value $\top$ for truth are defined as abbreviations), the usual modality $\Box$, for each proof variable p_i the unary modal operator $\Box_{p_i}$ and for each complexity variable α_i the unary modal operator $\triangle_{\alpha_i}$. The set of formulas of $\mathcal{L}^{++}$ is thus generated from the **atomic** formulas $\bot, S_0, S_1, \ldots$ by $\rightarrow$ as usual, and by the modal operators as follows: if A is an $\mathcal{L}^{++}$ formula, p is a proof variable and α is a complexity variable, then $\Box A$, $\Box_p A$ and $\triangle_\alpha A$ are $\mathcal{L}^{++}$ formulas; we call formulas of the form $\Box_p A$ and $\triangle_\alpha A$ **quasiatomic**, or **q-atomic** for short. We will also use the abbreviation $\Box^+ A$ for a formula $A \wedge \Box A$, and $\Diamond^+$ will stand for $\neg\Box^+\neg$. In the sequel under a modal formula we understand a formula in the language $\mathcal{L}^{++}$. We use small letters $p, q, r, \ldots$ for proof variables, greek letters $\alpha, \beta, \ldots$ for complexity variables, capital letters $S, T, \ldots$ for sentence variables and $A, B, C, \ldots$ for modal formulas. Let $\mathcal{L}$ denote the usual modal language over $\bot, S_0, S_1, \ldots$ with the only modality $\Box$, i.e. a labeled-modalities-free fragment of $\mathcal{L}^{++}$, $\mathcal{L}^{+}$ denote the $\triangle_{\alpha_i}$-free fragment of $\mathcal{L}^{++}$, $\mathcal{L}^{-+}$ – the $\Box_{p_i}$-free fragment, and $\mathcal{L}^{+-}$ – the fragment of $\mathcal{L}^{++}$, where we identify proof variable p_i with the correspondent complexity variable α_i.

We assume a reader to be familiar with the general unification technique (cf. [3, 1]). In particular, by τ_{AB} we denote the most general unifier (mgu) of A and B obtained by some fixed deterministic version of the Unification Algorithm.

1.6 Definition. (cf. [1]) Let $C = D \pmod{A = B}$ be an abbreviation for

$$\text{“for every substitution } \theta \ \ (A\theta \equiv B\theta \ \Rightarrow \ C\theta \equiv D\theta)\text{”}.$$

Apparently, if A, B are not unifiable, then $C = D \pmod{A = B}$ holds for all C and D.

1.7 Lemma. If A and B are unifiable, then

$$C = D \pmod{A = B} \quad \Leftrightarrow \quad C\tau_{AB} \equiv D\tau_{AB}.$$

Proof. Direction ($\Rightarrow$) is obvious as τ_{AB} unifies A and B. Direction ($\Leftarrow$): let $C\tau_{AB} \equiv D\tau_{AB}$ and θ be an arbitrary unifier A and B. As τ_{AB} is an mgu of A, B for some λ we have $\theta = \tau_{AB} \circ \lambda$, then

$$C\theta \equiv C\tau_{AB} \circ \lambda \equiv D\tau_{AB} \circ \lambda \equiv D\theta.$$

■

1.8 Corollary. The relation $C = D \pmod{A = B}$ is decidable.

1.9 Definition. An **arithmetical interpretation** $*$ is a triple (Prf, Cpl, ϕ), where Prf and Cpl are provably compatible standard proof and complexity predicates and ϕ is a function which assigns:

- to each proof variable p some $n \in \omega$,
- to each complexity variable α_i some $m \in \omega$
- and to each sentence variable S a sentence of $\mathtt{PA}$.

The arithmetical translation A^* of a modal formula A under the interpretation $*$ is the extension of ϕ to all modal formulas by:

- $\bot^* := (0 = 1)$,
- $p^* := \phi(p)$ for a proof variable p,
- $\alpha^* := \phi(\alpha)$ for a complexity variable α,

- $S^* := \phi(S)$ for a sentence variable S,
- $(\cdot)^*$ commutes with the Boolean connectives,
- $(\Box A)^* := Pr(\ulcorner A^* \urcorner)$,
- $(\Box_p A)^* := Prf(p^*, \ulcorner A^* \urcorner)$.
- $(\triangle_\alpha A)^* := Cpl(\alpha^*, \ulcorner A^* \urcorner)$,

An arithmetical interpretation (Cpl, Prf, ϕ) is called functional iff Prf is a functional proof predicate.

We'll combine the formal systems for complexity logics from the following set of axioms:

(A0) Boolean tautologies in the language $\mathcal{L}^{++}$;

(A1) $\Box(A \to B) \to (\Box A \to \Box B)$ (distributivity)

(A2) $\Box(\Box A \to A) \to \Box A$ (Löb axiom)

(A3) $\Box_p A \to A$ (q-reflexivity)

(A4) $\Box_p A \to \Box\Box_p A$ (stability)

(A5) $\neg\Box_p A \to \Box(\neg\Box_p A)$ (stability)

(A6) $\Box_p A \& \Box_p B \to (C \to D) \quad \text{if } C = D \pmod{A = B}$ (functionality)

(A7) $\triangle_\alpha A \to A$ (q-reflexivity)

(A8) $\triangle_\alpha A \to \Box A$ (q-provability)

(A9) $\triangle_\alpha A \to \Box\triangle_\alpha A$ (stability)

(A10) $\neg\triangle_\alpha A \to \Box(\neg\triangle_\alpha A)$ (stability)

(A11) $\Box_p A \to \triangle_p A$ (in the language $\mathcal{L}^{+-}$) (correspondence)

(A12) $\neg[(\beta_0 <_{A_0} \beta_1)\&(\beta_1 <_{A_1} \beta_2)\&\ldots\&(\beta_n <_{A_n} \beta_0)]$ (irreflexivity)
where $\beta_0, \beta_1, \ldots$ are complexity variables, $A_0, A_1, \ldots$ are formulas and $\alpha <_A \beta$ means $\Diamond^+(\triangle_\beta A \& \neg\triangle_\alpha A)$

and inference rules

(R0) $$\frac{A \qquad A \to B}{B}$$

(R1) $\dfrac{A}{\Box A}$

(R2) $\dfrac{\Box A}{A}$

Axioms **A0**–**A2** and rules **R0** and **R1** axiomatize the provability logic $\mathtt{GL}$, the system $\mathcal{B}$ is $\mathtt{GL}$ (in the language $\mathcal{L}^+$) + (**A3**–**A5**) + **R2**, the system $\mathcal{F}$ is $\mathcal{B}$ + **A6** (cf. [1]).

1.10 Definition. (cf. [1]) A **frame** is a pair $\langle K, \prec\rangle$, where $K \neq \emptyset$ and K is finite, $\prec$ is an irreflexive tree-like ordering of K[3]. In the sequel we call elements of K *nodes*, and let $\succ$ stand for $(\prec)^{-1}$. A **model** is a triple $\langle K, \prec, \Vdash\rangle$, where $\langle K, \prec\rangle$ is a frame and $\Vdash$ is a forcing relation between nodes and $\mathcal{L}^+$ formulas satisfying the following **forcing conditions**:

1. $\Vdash$ respects Boolean operations nodewise,
2. $x \Vdash \Box\varphi$ iff $\forall y \succ x \; y \Vdash \varphi$,
3. for every q-atomic formula $\Box_p A$, and every $x \prec y$
   $x \Vdash \Box_p A$ iff $y \Vdash \Box_p A$,
   (stability)
4. for every q-atomic formula $\Box_p A$
   $x \Vdash \Box_p A \;\Rightarrow\; x \Vdash A$,
   (q-reflexivity)
5. for every q-atomic formula $\triangle_\alpha A$
   $x \Vdash \triangle_\alpha A \;\Rightarrow\; x \Vdash \Box A$ and $\forall y \succ x \; y \Vdash \triangle_\alpha A$,
6. $\Vdash$ satisfies the axiom **A12** in each node.

1.11 Definition. By r-**model** we mean the model, restricted to the language $\mathcal{L}^{+-}$ with three additional forcing conditions for q-atomic formulas:

1. $x \Vdash \triangle_p A \;\Rightarrow\; x \Vdash A$,
2. $\forall x, y \in K \; x \prec y \;\Rightarrow\; x \Vdash \triangle_p A$ iff $y \Vdash \triangle_p A$,
3. $x \Vdash \Box_p A \;\Rightarrow\; x \Vdash \triangle_p A$.

[3] In fact any $\mathtt{GL}$-frame (i.e. transitive reverse well-founded) would fit here.

(The two first items together are stronger, than the item 5 of the previous definition.) The r-models will serve as Kripke-like models for systems for recursive complexity measures.

1.12 Definition. We say that a modal formula A is **valid in a model** $\mathcal{K} = \langle K, \prec, \Vdash \rangle$ if A holds at every node; and $\mathcal{K}$ is a **countermodel to** A if A is not valid in $\mathcal{K}$, i.e. $\neg A$ holds at some node $x \in K$.

2 Logics for decidable complexity measures.

We formulate formal systems for decidable complexity measures in the language $\mathcal{L}^{+-}$.

2.1 Definition. System $\mathcal{BC}$ is the system $\mathcal{B}$ (in the language $\mathcal{L}^{+-}$) + **A7** + (**A9** – **A12**), and the system $\mathcal{FC}$ is the system $\mathcal{BC}$ + functionality axiom **A6**.

Note that **A8** also holds in $\mathcal{BC}$ and $\mathcal{FC}$, but it is easy to derive it from **A7** and **A9** by **R1**.

2.2 Definition. A set X of modal formulas is **adequate** if it is closed under subformulas; $\bot \in X$; if $B \in X$ and B is not of a form $\neg C$, then $\neg B \in X$; for all p, A if there exist q, B such that $\Box_q A$ (or $\triangle_q A$) and $\Box_p B$ (or $\triangle_p B$) belong to X, then $\Box_p A \in X$ ($\triangle_p A \in X$).

Let $Ad(A)$ be the least adequate set containing A (it is easy to see that $Ad(A)$ is finite) and let $H(A) = \bigwedge\{\Box B \to B | \Box B \in Ad(A)\}$

2.3 Definition. X-model is a triple $\mathcal{K} = \langle K, \prec, \Vdash \rangle$ where $\langle K, \prec \rangle$ is a frame and the forcing relation $\Vdash$ is defined only for formulas from X and their Boolean and $\Box$-combinations and satisfies all the forcing conditions. We call an X-model A-**sound** if $H(A)$ holds at its root.

2.4 Remark. Note that every X-model can be extended to a model by defining $x \nVdash \varphi$ for each node $a \in K$ and for each atomic and q-atomic formula $\varphi \notin X$. Indeed, the stability and q-reflexivity forcing conditions are clearly preserved. We also address a reader to the remark 3.3.

2.5 Theorem. $\mathcal{BC}$ is complete with respect to the class of r-models, and thus is decidable.

Proof. The part "$\mathcal{BC} \nvdash A \Rightarrow$ there is a countermodel" goes exactly along the lines of that for $\mathcal{BE}$ (3.5 and 3.6), but the set Y should include items corresponding to **A7** instead of **A8** and to **A10** and **A11**. The other part "$\Rightarrow$" can be easily derived from 2.6 and 2.7.
■

2.6 Lemma. $\mathcal{BC} \vdash A \Rightarrow$ for every interpretation $*$ $\mathtt{PA} \vdash A^*$.

Proof. By induction on a proof of A in $\mathcal{BC}$. The cases of axioms **A0** – **A2** are treated in [2], **A4**, **A5**, **A9** and **A10** hold because *Prf* and *Cpl* are recursive. Let us consider the axiom **A3**. If $Prf(p^*, \ulcorner B^* \urcorner)$ is true, then B^* is in fact provable and $\mathtt{PA} \vdash (\Box_p B \to B)^*$; If $Prf(p^*, \ulcorner B^* \urcorner)$ is false, then $(\Box_p B)^*$ is a false recursive formula, thus $\mathtt{PA} \vdash (\neg \Box_p B)^*$ and again $\mathtt{PA} \vdash (\Box_p B \to B)^*$. Now **A7** is trivial because $Cpl(x, y) = \exists t \leq x Prf(x, y)$. Let us consider **A12**. We have

$$\mathtt{PA} \vdash u \leq v \to [Cpl(u, y) \to Cpl(v, y)].$$

As $u \leq v \in \Sigma_1^0$, then $\mathtt{PA} \vdash u \leq v \to \Box(u \leq v)$[4]. Hence

$$\mathtt{PA} \vdash u \leq v \to \Box^+[Cpl(u, y) \to Cpl(v, y)].$$

An interpretation of any example of $q <_A r$ is some substitution of free variabled by terms in the formula $\Diamond^+[\neg Cpl(u, y) \wedge Cpl(v, y)]$; also

$$\begin{aligned} \Diamond^+[\neg Cpl(u, y) \wedge Cpl(v, y)] &\leftrightarrow \neg \Box^+[Cpl(v, y) \to Cpl(u, y)] \\ &\to \neg(v \leq u) \\ &\to u < v. \end{aligned}$$

An arithmetical interpretation of an example of irreflexivity axiom is thus equivalent in $\mathtt{PA}$ to

$$(q_0 <_{A_0} q_1)^* \& (q_1 <_{A_1} q_2)^* \& \ldots \& (q_{n-1} <_{A_{n-1}} q_n)^* \to \neg(q_n <_{A_n} q_0)^*,$$

which is provable in $\mathtt{PA}$ because

$$\begin{aligned} &(q_0 <_{A_0} q_1)^* \& (q_1 <_{A_1} q_2)^* \& \ldots \& (q_{n-1} <_{A_{n-1}} q_n)^* \\ &\to u_0 < u_1 \& u_1 < u_2 \& \ldots \& u_{n-1} < u_n \\ &\to \neg(u_n < u_0) \\ &\to \neg(q_n <_{A_n} q_0)^*. \end{aligned}$$

Note that the proof of **A12*** does not use the fact, that *Cpl* is recursive, so this proof is valid for a recursively enumerable *Cpl* too.

[4] We understand here $\Box$ as $Pr(\ulcorner \cdot^* \urcorner)$.

■

2.7 Theorem. $\mathcal{BC} \nVdash A \Rightarrow$ for some interpretation $*$ $\mathtt{PA} \nVdash A^*$.

Proof. Let $\mathcal{BC} \nVdash A$, and let $\mathcal{K} = (K, \prec, \Vdash)$ be an A-sound $Ad(A)$-r-model. We assume that $K = \{1, \ldots, n\}$ and 1 is the root node and define a new model $\mathcal{K}'$ by adding a node 0 to K, putting $0 \prec i$ $(1 \le i \le n)$, and defining $0 \Vdash B$ iff $1 \Vdash B$ for every atomic and q-atomic formula $B \in Ad(A)$. An easy induction proves that $\mathcal{K}'$ is an A-sound $Ad(A)$-r-model.

We proceed with the Solovay construction and define the Solovay function $h(t)$ and the arithmetical formulas "$l = j$" for the model $\mathcal{K}'$ and for the usual Gödel proof predicate $\mathit{Proof}(x, y)$, and put

$$\varphi(S_i) := [\bigvee_{j S_i} \text{“}l = j\text{”}] \wedge i = i.$$

The following *Solovay Lemma* holds:

2.8 Lemma. [5]

1. $\mathtt{PA} \vdash$ "$0 \le l \le n$";
2. "$l = 0$" is true, but each of the theories $\mathtt{PA}+$"$l = i$" is consistent for $i = 0, 1 \ldots, n$;
3. $\mathtt{PA} +$ "$l = i$" $\vdash \mathit{Provable}(\ulcorner \text{“}l \neq i\text{”} \urcorner)$, $i = 1, 2, \ldots, n$;
4. $\mathtt{PA} +$ "$l = i$" $\vdash \neg\mathit{Provable}(\ulcorner \text{“}l \neq j\text{”} \urcorner)$, $i = 0, 2, \ldots, n$, $i \prec j$;
5. $\mathtt{PA} +$ "$l = i$" $\vdash \mathit{Provable}(\ulcorner \text{“}l \neq j\text{”} \urcorner)$, $i = 1, 2, \ldots, n$, $i \not\prec j$.

2.9 Definition. We define now a relation **prec** on the set *Var* of all proof variables occurring in $Ad(A)$: p **prec** q iff there are

$$\triangle_p A_1, \triangle_{q_1} A_1, \triangle_{q_1} A_2, \ldots, \triangle_{q_{n-1}} A_n, \triangle_q A_n \in X$$

such that

$$(p <_{A_1} q_1) \& (q_1 <_{A_2} q_2) \& \ldots \& (q_{n-1} <_{A_n} q)$$

holds in $\mathcal{K}'$.

The relation **prec** is obviously transitive and the axiom **A12** guarantees that it is also irreflexive.

2.10 Lemma. There is an injective homomorphism f of the order (Var, **prec**) to the natural ordering of rationals such that

$$p \textbf{ prec } q \quad \Rightarrow \quad f(p) < f(q).$$

Proof. Without loss of generality we assume that $Var = \{p_0, \dots, p_m\}$. We define f by induction on the cardinality of Var; $f(p_0)$ is mapped arbitrarily. Suppose $f(p_0), \dots, f(p_{k-1})$ are defined. Let

$$H := \min\{f(p_i) \mid p_k \textbf{ prec } p_i,\ i < k\}, \quad \min \emptyset = +\infty$$

and

$$h := \max\{f(p_j) \mid p_j \textbf{ prec } p_k,\ j < k\}, \quad \max \emptyset = -\infty.$$

We claim that $h < H$. Indeed, $h = H$ is impossible because of the injectivity of f. If $H < h$, then there are $i, j < k$ such that $f(p_i) < f(p_j)$, but p_j **prec** p_k and p_k **prec** p_i. By the transitivity of **prec** we have p_j **prec** p_i which contradicts the homomorphic property of f. So $h < H$ and put $f(p_k)$ to be $h < f(p_k) < H$. The desired inequalities are obvious: if p_i **prec** p_k, then $f(p_i) \leq h$ by the definition of h, and thus $f(p_i) < f(p_k)$, etc.
■

Again, without loss of generality we assume that

$$f(p_0) < f(p_1) < \ldots < f(p_m),$$

put

$$Q_i \;=\; \{B \mid \triangle_{p_i} B \in Ad(A) \text{ and } \triangle_{p_i} B \text{ holds in } \mathcal{K}'\}, (0 \leq i \leq m),$$

$$Q = \bigcup_{0 \leq i \leq m} Q_i,$$

and

$$P_i \;=\; \{B \mid \Box_{p_i} B \in Ad(A) \text{ and } \Box_{p_i} B \text{ holds in } \mathcal{K}'\}, (0 \leq i \leq m),$$

and observe that $Q_i \subseteq Q_j$, whenever $i < j$, and $P_i \subseteq Q_i$ with $0 \leq i \leq m$. Indeed, suppose $i < j$ but there is B such that $\triangle_{p_i} B, \triangle_{p_j} B \in X$, $\triangle_{p_i} B$ holds in $\mathcal{K}'$, but $\triangle_{p_j} B$ does not. Then $\neg \triangle_{p_j} B$ is valid in $\mathcal{K}'$ and thus $p_j <_B p_i$ holds in $\mathcal{K}'$: contradiction with $i < j$. The property $P_i \subseteq Q_i$ with $0 \leq i \leq m$ is guaranteed by **A12**.

Put $R_i = Q_i - P_i$, define

$$p_i := 2i + 1$$

and consider the following arithmetical fixed point equation (FPE):

$$
\begin{array}{llllll}
Prf(u,v) & \leftrightarrow & [& u=0 & \rightarrow & \Gamma_0 & \& \\
& & & u=1 & \rightarrow & \Delta_0 & \& \\
& & & u=2 & \rightarrow & \Gamma_1 & \& \\
& & & u=3 & \rightarrow & \Delta_1 & \& \\
& & & & & \vdots & \\
& & & u=2m & \rightarrow & \Gamma_m & \& \\
& & & u=2m+1 & \rightarrow & \Delta_m & \& \\
& & & u>2m+1 & \rightarrow & Proof(u-2m-2,v) &]
\end{array}
$$

where

$$
\Gamma_i \equiv \begin{cases} \bigvee_{B\in R_i}(v = \ulcorner B^* \urcorner) & \text{if } R_i \neq \emptyset \\ \\ v = \ulcorner \forall x_0(x_0 = x_0)\urcorner & \text{otherwise,} \end{cases}
$$

$$
\Delta_i \equiv \begin{cases} \bigvee_{B\in P_i}(v = \ulcorner B^* \urcorner) & \text{if } P_i \neq \emptyset \\ \\ v = \ulcorner \forall x_0(x_0 = x_0)\urcorner & \text{otherwise.} \end{cases}
$$

One can easily see that Prf is recursive and $*$ is injective. Moreover,

$$
\mathtt{PA} \vdash Pr(y) \;\leftrightarrow\; [Provable(y) \vee \bigvee_{B\in Q} (y = \ulcorner B^* \urcorner)].
$$

We have to prove now the usual Solovay lemma:

2.11 Lemma. For every $B \in Ad(A)$ and every node j from $\mathcal{K}'$

$$
j \Vdash B \;\Rightarrow\; \mathtt{PA} \vdash \text{“}l = j\text{”} \rightarrow B^*
$$

$$
j \nVdash B \;\Rightarrow\; \mathtt{PA} \vdash \text{“}l = j\text{”} \rightarrow \neg B^*.
$$

Proof. By induction on formulas. Basis in case when B is a sentence variable, or a constant $\bot$ is trivial.

Let $B \equiv \Box_{p_i} D \in X$. If $j \Vdash \Box_{p_i} D$ then $D \in P_i$ and because of the FPE, $Prf(2i+1, \ulcorner D^* \urcorner)$ is true, $\mathtt{PA} \vdash Prf(2i+1, \ulcorner D^* \urcorner)$ and $\mathtt{PA} \vdash$ “$l = j$” $\rightarrow B^*$. If $j \nVdash \Box_{p_i} D$, then $D \notin P_i$ and because of the FPE and the injectivity of $*$, $Prf(2i+1, \ulcorner D^* \urcorner)$ is false. In this case $\mathtt{PA} \vdash$ “$l = j$” $\rightarrow \neg B^*$.

Let $B \equiv \triangle_{p_i} D \in X$. If $j \Vdash \triangle_{p_i} D$ then $D \in Q_i$ and, according to the FPE, either $Prf(2i, \ulcorner D^* \urcorner)$ is true or $Prf(2i+1, \ulcorner D^* \urcorner)$ is true. In either case

$$\mathtt{PA} \vdash \exists x \leq {p_i}^* \; Prf(x, \ulcorner D^* \urcorner)$$

and thus $\mathtt{PA} \vdash$ "$l = j$" $\rightarrow B^*$.

If $j \nVdash \triangle_{p_i} D$, then $D \notin Q_i$, moreover $D \notin Q_k$ for all $k \leq i$ (thus $D \notin P_k$ and $D \notin R_k$ for all $k \leq i$). Also $D^* \not\equiv \forall x_0 (x_0 = x_0)$ and, by the FPE and because of the injectivity of $*$ $Prf(k, \ulcorner D^* \urcorner)$ is false for all $k \leq 2i+1$. Thus

$$\mathtt{PA} \vdash \neg \exists x \leq {p_i}^* \; Prf(x, \ulcorner D^* \urcorner),$$

and $\mathtt{PA} \vdash$ "$l = j$" $\rightarrow \neg B^*$.

Now we proceed with different inductions on formulas, first for $k > 0$, and then for $k = 0$.

Let $1 \leq k \leq n$. The induction step in case of "$\rightarrow$" is straightforward (cf.[5]). The induction step in case $B \equiv \Box H$: we proceed with the standard Solovay argument.

If $k \Vdash \Box H$, then

$$\text{for all } \; j \succ k \;\; j \Vdash H,$$

$$\text{for all } \; j \succ k \;\; \mathtt{PA} \vdash \text{“}l = j\text{”} \rightarrow H^*,$$

$$\mathtt{PA} \vdash \bigvee_{k \prec j} \text{“}l = k\text{”} \rightarrow H^*,$$

$$\mathtt{PA} \vdash Provable(\ulcorner \bigvee_{k \prec j} \text{“}l = k\text{”} \urcorner) \rightarrow Provable(\ulcorner H^* \urcorner), \qquad \dagger$$

$$\text{by 2.8 (4)} \;\; \mathtt{PA} \vdash \text{“}l = k\text{”} \rightarrow \bigwedge_{k \not\prec j} Provable(\ulcorner \text{“}l \neq j\text{”} \urcorner),$$

$$\mathtt{PA} \vdash \text{“}l = k\text{”} \rightarrow Provable(\ulcorner \bigwedge_{k \not\prec j} \text{“}l \neq j\text{”} \urcorner) \text{ (by commutting } Provable(\cdot) \text{ and } \textstyle\bigwedge),$$

$$\text{by 2.8 (1)} \;\; \mathtt{PA} \vdash Provable(\ulcorner \bigvee_{0 \leq j \leq n} \text{“}l = j\text{”} \urcorner),$$

$$\mathtt{PA} \vdash Provable(\ulcorner \bigwedge_{k \neq j} \text{“}l \neq j\text{”} \rightarrow \bigvee_{k = j, k \prec j} \text{“}l = j\text{”} \urcorner),$$

$$\text{by 2.8 (3)} \;\; \mathtt{PA} \vdash \text{“}l = k\text{”} \rightarrow Provable(\ulcorner \text{“}l \neq k\text{”} \urcorner),$$

$$\text{finally, } \; \mathtt{PA} \vdash \text{“}l = k\text{”} \rightarrow Provable(\ulcorner \bigvee_{k \prec j} \text{“}l = j\text{”} \urcorner),$$

$$\text{and by } \dagger \; \mathtt{PA} \vdash \; \text{“}l = k\text{”} \rightarrow Provable(\ulcorner H^* \urcorner),$$

$$\text{and since } \mathtt{PA} \vdash \forall y (Provable(y) \rightarrow Pr(y)) \text{ we are done:}$$

$$\mathtt{PA} \vdash \; \text{“}l = k\text{”} \rightarrow B^*.$$

If $k \not\Vdash \Box H$, then

$$\text{for some } \; j \succ k \;\; j \not\Vdash H,$$

$$\text{by the induction hypothesis } \mathbf{PA} \vdash \text{``}l = k\text{''} \rightarrow \neg H^*,$$

$$\mathbf{PA} \vdash H^* \rightarrow \text{``}l \neq j\text{''},$$

$$\mathbf{PA} \vdash \mathit{Provable}(\ulcorner H^* \urcorner) \rightarrow \mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner),$$

$$\mathbf{PA} \vdash \neg\mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner) \rightarrow \neg\mathit{Provable}(\ulcorner H^* \urcorner),$$

$$\text{but by 2.8 (4) } \; \mathbf{PA} \vdash \text{``}l = k\text{''} \rightarrow \neg\mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner),$$

$$\text{thus } \mathbf{PA} \vdash \; \text{``}l = k\text{''} \rightarrow \neg\mathit{Provable}(\ulcorner H^* \urcorner).$$

But $Pr(y)$ may differ from $\mathit{Provable}(y)$ only on the gödelnumbers of $*$-interpretations of the q-atomic formulas from the fixed finite set T; every formula from T is valid in each node of the model $\mathcal{K}'$, thus $H \notin T$, and

$$\mathbf{PA} \vdash \; Pr(\ulcorner H^* \urcorner) \rightarrow \mathit{Provable}(\ulcorner H^* \urcorner).$$

Finally, we have got the desired $\mathbf{PA} \vdash \; \text{``}l = k\text{''} \rightarrow \neg Pr(\ulcorner H^* \urcorner)$, i.e.

$$\mathbf{PA} \vdash \; \text{``}l = k\text{''} \rightarrow \neg B^*.$$

Let now $k = 0$. Again, the basis of the induction on formulas is done, the case of $\rightarrow$ is trivial. Let $B = \Box H$. If $0 \Vdash \Box H$, then for all $j = 1, \ldots, n \;\; j \Vdash H$, by the previous induction

$$\text{for all } \; j = 1, \ldots, n \;\; \mathbf{PA} \vdash \text{``}l = j\text{''} \rightarrow H^*,$$

$$\mathbf{PA} \vdash \bigvee_{1 \leq j \leq n} \text{``}l = j\text{''} \rightarrow H^*.$$

Also $1 \Vdash H \;\Rightarrow\; 0 \Vdash H$, and by the induction hypothesis $\mathbf{PA} \vdash \text{``}l = 0\text{''} \rightarrow H^*$. By 2.8 (1) $\mathbf{PA} \vdash \text{``}0 \leq j \leq n\text{''}$, and thus $\mathbf{PA} \vdash H^*$, $\mathbf{PA} \vdash \mathit{Provable}(\ulcorner H^* \urcorner)$, and $\mathbf{PA} \vdash \text{``}l = 0\text{''} \rightarrow B^*$. If $0 \not\Vdash \Box H$, then for some $j > 0 \;\; j \not\Vdash H$, by the previous induction $\mathbf{PA} \vdash \text{``}l = j\text{''} \rightarrow \neg H^*$, $\mathbf{PA} \vdash H^* \rightarrow \text{``}l \neq j\text{''}$,

$$\mathbf{PA} \vdash \mathit{Provable}(\ulcorner H^* \urcorner) \rightarrow \mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner),$$

$$\mathbf{PA} \vdash \neg\mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner) \rightarrow \neg\mathit{Provable}(\ulcorner H^* \urcorner),$$

$$\text{but by 2.8 (4) } \; \mathbf{PA} \vdash \text{``}l = 0\text{''} \rightarrow \neg\mathit{Provable}(\ulcorner \text{``}l \neq j\text{''} \urcorner),$$

$$\text{thus } \mathbf{PA} \vdash \; \text{``}l = 0\text{''} \rightarrow \neg\mathit{Provable}(\ulcorner H^* \urcorner).$$

The same argument as above shows that

$$\mathtt{PA} \vdash \ Pr(\ulcorner H^{*}\urcorner) \to Provable(\ulcorner H^{*}\urcorner),$$

and we again have

$$\mathtt{PA} \vdash \ \text{“}l = 0\text{”} \to \neg B^{*}.$$

■

2.12 Definition. A model is called **functional** if it satisfies an extra forcing condition:

$$x \Vdash \neg(\Box_p B \& \Box_p C) \quad \text{if} \quad B, C \text{ are not unifiable, else}$$
$$x \Vdash \Box_p B \& \Box_p C \Rightarrow \ x \Vdash D \to E \ \ \text{for every } D, E \text{ s.t. } \ D = E \pmod{B = C}$$

Kripke models for $\mathcal{FC}$ are functional r-models. We skip the proof, addressing the reader to [1], Theorem 3.2 and to Lemmas 3.4 and 3.5.

2.13 Theorem.

$$\mathcal{FC} \vdash A \quad \Leftrightarrow \quad \text{for every interpretation } * \ \ \mathtt{PA} \vdash A^{*}.$$

Proof. Correctness, i.e. the case ($\Rightarrow$). Induction on a proof of A in $\mathcal{F}$. After Theorem 2.6 it only remains to check the correctness of the functionality axiom **A6**, which is done *de facto* in [1], theorem 3.14.

($\Leftarrow$).The proof is an easy combination of the proofs of Theorem 3.14 from [1] and 2.7. In the notations of the Theorem 2.7 let

$$Q_{i+1} - Q_i = \{A_{i,2},\ A_{i,3}, \ldots, A_{i,n_i}\}\ (0 \le i \le m).$$

Pay attention that here $n_i = 1+$ the cardinality of R_i, so if $n_i = 1$, then $R_i = \emptyset$. Because of the functional property of the model with respect to q-atomic formulas $\Box_{p_i} A$, there is not more than one formula among $A_{i,j}$, for which $\Box_{p_i} A_{i,j}$ holds in the model; without loss of generality we may assume that it is A_{i,n_i}. Let also $M = n_0 + \ldots + n_m$. We define

$$p_i{}^{*} := n_0 + \ldots + n_i - 1$$

and consider the following fixed point equation:

$$
\begin{array}{llllll}
Prf(u,v) & \leftrightarrow & [& u=0 & \to & v=\ulcorner \forall x_0(x_0=x_0)\urcorner \ \& \\
 & & & u=1 & \to & v=\ulcorner {A_{0,2}}^{\sharp}\urcorner \ \& \\
 & & & u=2 & \to & v=\ulcorner {A_{0,3}}^{\sharp}\urcorner \ \& \\
 & & & & & \vdots \\
 & & & u=n_1-1 & \to & v=\ulcorner {A_{0,n_0}}^{\sharp}\urcorner \ \& \\
 & & & u=n_1 & \to & v=\ulcorner \forall x_0(x_0=x_0)\urcorner \ \& \\
 & & & u=n_1+1 & \to & v=\ulcorner {A_{1,2}}^{\sharp}\urcorner \ \& \\
 & & & & & \vdots \\
 & & & u=M-1 & \to & v=\ulcorner {A_{m,n_m}}^{\sharp}\urcorner \ \& \\
 & & & u\geq M & \to & Proof(u-M,v) \ ]
\end{array}
$$

Now we have just to repeat the steps of the proof of Theorem 2.7 and then 3.14 from [1].

■

2.1 Comments

1. Uniform completeness of $\mathcal{BC}$ and for $\mathcal{FC}$ takes place, namely, in theorems 2.7 and 2.13 one can choose a proof predicate uniformly for all A's.

2. The case of logics of all formulas true in the standard model of arithmetic for $\mathcal{BC}$ and for $\mathcal{FC}$ can be treated exactly as that for $\mathcal{B}$ and $\mathcal{F}$ in [1]. The truth cases for $\mathcal{BC}$ and $\mathcal{FC}$ are the logics $\mathcal{BC}^{\omega}$ and $\mathcal{FC}^{\omega}$ whose axioms are all the theorems of $\mathcal{BC}$ and $\mathcal{FC}$, the axiom scheme $\Box A \to A$ and the only rule is **R0**.

3. How $\mathcal{BC}$ and $\mathcal{FC}$ are related to specific complexity measures? Let us take the one determined by the usual Gödel proof predicate $Proof(x,y)$. Clearly, the logic of $Proof(x,y)$ extends $\mathcal{FC}$, but this logic itself essentially depends on some occasional details of the coding of formulas and proofs. For example, the scheme

$$\triangle_p \neg\neg A \to \triangle_p A$$

expresses the conjecture that the least proof code of any formula A is less then any proof code of $\neg\neg A$. One can easily define numerations of proofs with or without this property; the question whether it holds for a "usual" coding of proofs doesn't look relevant to real problems of the complexity of proofs. It is the main reason why unlike the paper [1] we skip the usual Gödel proof predicate case. However, for some natural complexity measures the question of their individual complexity logics might have sence; such a logic would extend $\mathcal{BC}$ or even $\mathcal{FC}$ (for a decidable complexity predicate), or $\mathcal{BE}$ from the next chapter (for a recursively enumerable complexity predicate).

■

3 Logics for recursively enumerable measures.

The system $\mathcal{E}$ is formulated in the language $\mathcal{L}^{-+}$, i.e. without modalities $\Box_p$, and its axioms are **A0** – **A2** (the system GL) + **A8** + **A9** + **A12** and inference rules **R0** – **R2**. The system $\mathcal{BE}$ (formulated in $\mathcal{L}^{++}$) is $\mathcal{B} + \mathcal{E}$. For technical reasons we introduce an auxiliary system $\mathcal{E}^-$ that is $\mathcal{E}$ without **R2**. In the sequel "$\vdash$" without the left argument means "$\mathtt{PA} \vdash$". Also under modal formula we understand an $\mathcal{L}^{-+}$-formula for $\mathcal{E}$ and an $\mathcal{L}^{++}$ one for $\mathcal{BE}$. As for $\mathcal{BC}$ and $\mathcal{FC}$ we prove the following

3.1 Lemma. For an arithmetical interpretation $*$ and a modal formula F

$$\mathcal{E} \vdash F \;\Rightarrow\; \mathtt{PA} \vdash F^*$$
$$\mathcal{BE} \vdash F \;\Rightarrow\; \mathtt{PA} \vdash F^*$$

Proof.
The proof is essentially done in Lemma 2.6. We have to prove only that $\vdash (\triangle_\alpha A \to \Box A)^*$, i.e. $\vdash Cpl(t, \ulcorner A^* \urcorner) \to \exists x\, Cpl(x, \ulcorner A^* \urcorner)$ which is obvious, and $\vdash (\triangle_\alpha A \to \Box\triangle_\alpha A)^*$, which follows from Σ^0_1-completeness of $\mathtt{PA}$.
■

3.2 Definition. A set X of modal formulas is **adequate** if it is closed under subformulas; $\bot \in X$; if $B \in X$ and B is not of a form $\neg C$, then $\neg B \in X$; for all α, A if there exist β, B such that $\triangle_\beta A$ and $\triangle_\alpha B$ belong to X, then $\triangle_\alpha A \in X$ and $\Box A \in X$.

The definition of an X-model $\mathcal{K}$ is the same as that for $\mathcal{BC}$ and $\mathcal{FC}$ (definition 2.3).

3.3 Remark. Every X-model can be extended to a model by defining $x \not\Vdash \varphi$ for each node $x \in K$ and for each atomic and q-atomic formula $\varphi \notin X$. The forcing conditions 1.-5. are clearly respected, we only need to verify the condition 6. **A12**. Suppose

$$x \Vdash \Diamond^+(\triangle_{\beta_1} A_0 \& \neg\triangle_{\beta_0} A_0) \& \ldots \& \Diamond^+(\triangle_{\beta_0} A_n \& \neg\triangle_{\beta_n} A_n),$$

and also suppose that there is an q-atomic formula among those mentioned explicitly here that does not belong to X; w.l.g. assume that $\triangle_{\beta_1} A_1 \notin X$. However, $x \Vdash \triangle_{\beta_1} A_0$ and $x \Vdash \triangle_{\beta_2} A_1$, thus $\triangle_{\beta_1} A_0, \triangle_{\beta_2} A_1 \in X$, hence $\triangle_{\beta_1} A_1 \in X$. It demonstrates that all q-formulas from the example of **A12** above are from X, which is impossible since we consider an X-model.

3.4 Lemma. $\mathcal{E}^- \not\vdash A \Rightarrow$ there is an $Ad(A)$-model $\mathcal{K}$ with the root $\mathbf{r}$ such that $\mathbf{r} \not\Vdash A$.

Proof. Let $\{\triangle_{\alpha_i} A_j\}_{i=0}^{n}{}_{j=0}^{m}$ be all the $\triangle_\alpha$-formulas in $Ad(A)$, and let $\{T_{ij}\}_{i=0}^{n}{}_{j=0}^{m}$ be sentence variables not occurring in $Ad(A)$. In every $B \in X$ we replace all occurrences of $\triangle_{\alpha_i} A_j$, that are not in the scope of any labeled modality, by T_{ij}. The resulting formula B^t is in the language $\mathcal{L}$. Let Y be a set of $\mathcal{L}$-formulas, containing

1. $\Box^{+}(T_{ij} \to \Box {A_j}^t)$,

2. $\Box^{+}(T_{ij} \to \Box T_{ij})$,

3. $\Box^{+}(\neg(\Diamond^{+}(\neg T_{kr} \wedge T_{lr}) \wedge \Diamond^{+}(\neg T_{ls} \wedge T_{.s}) \wedge \ldots \wedge \Diamond^{+}(\neg T_{k't} \wedge T_{kt})$ for all $(k, l \ldots k') \subset \{0 \ldots n\}^*$ and $(r, s \ldots t) \subset \{0 \ldots m\}^*$.

Thus the substitution of $\triangle_{\alpha_i} A_j$ for T_{ij} makes Y the set of theorems of $\mathcal{E}^-$, so if $\mathtt{GL} \vdash \bigwedge Y \to B^t$, then $\mathcal{E}^- \vdash B$, whenever $B \in Ad(A)$ (easy induction on a proof). But $\mathcal{E}^-$ does not prove A, so we can (cf. [5]) construct a $\mathtt{GL}$-countermodel $\mathcal{K}' = \langle K, \prec, \Vdash' \rangle$, which is a finite tree with the root $\mathbf{r}$ such that $\mathbf{r} \nVdash' \bigwedge Y \to A^t$, hence $\mathbf{r} \Vdash' \bigwedge Y$ and $\mathbf{r} \nVdash' A^t$. By the definition of Y and $\mathbf{r} \Vdash' \bigwedge Y$ we can define an $Ad(A)$-model $\mathcal{K} = \langle K, \prec, \Vdash \rangle$ putting

$$a \Vdash F \stackrel{\text{def}}{\Longleftrightarrow} a \Vdash' F^t.$$

Then $\mathbf{r} \nVdash A$.

■

3.5 Lemma. $\mathcal{E} \nvdash A \Rightarrow$ there is an A-sound $Ad(A)$-countermodel $\mathcal{K}$ for A

Proof. If $\mathcal{E} \nvdash A$, then for any $N \in \omega$ $\mathcal{E}^- \nvdash \Box^N A$. Take $N = Card\{\Box B \in Ad(A)\}$. By Lemma 3.4 there is an $Ad(A)$-model $\mathcal{K}'$ with the root $\mathbf{r}$ such that $\mathbf{r} \nVdash \Box^N A$. By the forcing condition for $\Box$ there is a chain $i_N \prec \ldots \prec i_0$ such that $i_k \nVdash \Box^k A$, but the formula $\Box B \to B$ can fail at one node of the chain at the most. So, by the pigeonhole principle, there is k such that $i_k \Vdash H(A)$. Since $i_N \preceq i_k$ the restriction of $\mathcal{K}'$ to the set $\{j \mid j \succ i_k \text{ or } j = i_k\}$ is a desired $Ad(A)$-model.

■

3.6 Lemma. $\mathcal{BE} \nvdash A \Rightarrow$ there is an A-sound $Ad(A)$-countermodel for A.

Proof. The proof is nearly the same as in Lemmas 3.4 and 3.5. We only need to replace $\mathtt{GL}$ by $\mathcal{B}^-$ and $\mathcal{E}^{(-)}$ by $\mathcal{BE}^{(-)}$. The Kripke model completeness for $\mathcal{B}^-$ is proved in [1].

■

3.7 Theorem. The systems $\mathcal{E}$ and $\mathcal{BE}$ are complete with respect to the intended classes of finite Kripke models and thus are both decidable.

Proof. An easy combination of Lemmas 3.5 and 3.6, Theorem 3.1 and Theorem 3.8 proved below.

■

3.8 Theorem.

$$\begin{array}{c}\mathcal{E} \vdash A \\ \mathcal{BE} \vdash A\end{array} \iff \text{for any interpretation } * \ \mathtt{PA} \vdash A^*.$$

Proof. We prove the theorem for $\mathcal{BE}$ only. The proof for $\mathcal{E}$ is a straightforward restriction of that for $\mathcal{BE}$ to the language $\mathcal{L}^{-+}$.

Direction "$\Leftarrow$" by contraposition. If $\mathcal{BE} \nvdash A$, then by Lemma 3.6 there is an A-sound $Ad(A)$-countermodel $\mathcal{K}'$ for A; we can assume that $\mathcal{K}'$ is already extended to the (total) $Ad(A)$-countermodel for A. Let $\mathcal{K}'$ be $\langle K', \prec, \Vdash\rangle$. Again w.l.g. we assume, that $K' = \{1, \ldots, n\}$ and 1 is the root node, add to K' a new node 0 and define $0 \prec i$, $i \in K'$. For every atomic or q-atomic formula $F \in Ad(A)$ we define $0 \Vdash F \Leftrightarrow 1 \Vdash F$. Let K denote $\{0\} \cup K'$ and $\mathcal{K} = \langle K, \prec, \Vdash\rangle$. Again we define the Solovay function h and arithmetical formulas "$l = j$" for the model $\mathcal{K}$.

3.9 Definition.

$$\alpha < \beta \overset{\text{def}}{\iff} \exists B(0 \Vdash \alpha <_B \beta)$$

$$\alpha = \beta \overset{\text{def}}{\iff} \forall B \forall i \in M(i \Vdash \triangle_\alpha B \Leftrightarrow i \Vdash \triangle_\beta B)$$

$$\alpha \leq \beta \overset{\text{def}}{\iff} \alpha < \beta \text{ or } \alpha = \beta$$

It is easy to see that $\leq$ is a linear quasi-ordering of the set of complexity variables. Let $\{\alpha_i\}_{i=1}^N$ be all complexity variables occurring in $Ad(A)$ and enumerated in such a way that $i \leq j \Rightarrow \alpha_i \leq \alpha_j$; let also $\{p_i\}_{i=0}^{N'}$ be all proof variables occurring in $Ad(A)$, and $I_i = \{l : \mathcal{M} \Vdash \Box_{p_i} C_l\}$. We define

$$\phi(S_i) = \begin{cases} (i \neq i) & \text{if } S_i \notin Ad(A) \\ \bigvee_{w S_i} \ \text{“}l = w\text{”} \wedge i = i & \text{if } S_i \in Ad(A), \end{cases}$$

$$\phi(p_i) = \begin{cases} i & \text{if } i < N' \\ N' & \text{otherwise,} \end{cases}$$

$$\phi(\alpha_i) = \begin{cases} 0 & \text{if } \alpha_i \text{ does not occur in } Ad(A) \\ i & \text{otherwise.} \end{cases}$$

The predicates *Cpl* and *Prf* are defined as solutions of the following fixed point equations system

$$\begin{aligned} \vdash Cpl(x, y) \ \leftrightarrow \ & \textstyle\bigwedge_{k=1}^N \{x = k \rightarrow \exists m \exists B \in Ad(A)\, [y = \ulcorner B^* \urcorner \wedge h(m) \Vdash \triangle_{\alpha_k} B]\} \\ & \wedge \{x > N \rightarrow [Provable(y) \wedge \forall \Box B \in Ad(A)(y \neq \ulcorner B^* \urcorner)] \\ & \vee \exists m \exists B \in Ad(A)\, [y = \ulcorner B^* \urcorner \wedge h(m) \Vdash \Box B]\} \end{aligned}$$

$$\begin{aligned} \vdash Prf(x, y) \ \leftrightarrow \ & \textstyle\bigwedge_{k=0}^{N'-1} \left\{x = k \rightarrow \bigvee_{j \in I_k} (y = \ulcorner C_j{}^* \urcorner)\right\} \\ & \wedge \{x > N' \rightarrow Proof(x - N' - 1, y)\}. \end{aligned}$$

Note that the defined interpretation $*$ is injective on $Ad(A)$. We will base the interpretation of $\Box$ on Prv instead of Pr ; later we prove that both are equivalent to $Provable$.

3.10 Lemma. For all $F \in Ad(A)$ and $w \in K$

$$\vdash \text{“}l = w\text{”} \rightarrow (\text{“}w \Vdash F\text{”} \leftrightarrow F^*)^5.$$

Proof. We proceed with the induction on construction of F. The cases $F = S_i$, $F = \bot$ and $F = B \rightarrow C$ are treated as usual (cf. [5]).

Let F be $\Box_{p_k} C_l$. If $w \Vdash F$, then $l \in I_k$, hence $Prf(p_k{}^*, \ulcorner C_l{}^{*}\urcorner)$ is true, so it is provable in $\mathtt{PA}$. Then $\vdash \text{“}l = w\text{”} \rightarrow (\text{“}w \Vdash F\text{”} \rightarrow F^*$. If $w \not\Vdash F$, then $l \notin I_k$, hence $Prf(p_k{}^*, \ulcorner C_l{}^{*}\urcorner)$ is false, then $\vdash \neg F^*$, so $\vdash \text{“}l = w\text{”} \rightarrow (\text{“}w \not\Vdash F\text{”} \rightarrow \neg F^*)$.

Let F be $\triangle_{\alpha_k} B$. We argue in $\mathtt{PA}$. Suppose "$l = w$". Then there exists m such that $h(m) = w$. If "$w \Vdash F$", then "$h(m) \Vdash \triangle_{\alpha_k} B$" and as $\alpha_k{}^* = k$, then $Cpl(\alpha_k{}^*, \ulcorner B^{*}\urcorner)$. If "$w \not\Vdash F$", then $\forall v \prec w(\text{“}v \not\Vdash F\text{”})$. But $\forall m' \leq m[h(m') \preceq h(m)]$, hence "$h(m') \not\Vdash \triangle_{\alpha_k} B$". From the other side, "$l = w$" and "$w \not\Vdash F$" provide that $\forall m' \geq m[\text{“}h(m') \not\Vdash \triangle_{\alpha_k} B\text{”}]$. Now $\forall m \text{“}h(m) \not\Vdash \triangle_{\alpha_k} B\text{”}$, thus $\neg Cpl(\alpha_k{}^*, \ulcorner B^{*}\urcorner)$.

The case $F = \Box B$ is similar: "$w \Vdash F$" implies $Cpl(N+1, \ulcorner B^{*}\urcorner)$, hence $Pr(\ulcorner B^{*}\urcorner)$. If "$w \not\Vdash F$", then as above one can prove $\forall m \text{“}h(m) \not\Vdash \Box B\text{”}$. But $\Box B \in Ad(A)$, hence $Provable(y) \wedge \forall \Box B \in Ad(A)(y \neq \ulcorner B^{*}\urcorner)$ is false for $y = \ulcorner B^{*}\urcorner$, then

$$\forall x > N \neg Cpl(x, \ulcorner B^{*}\urcorner) \tag{1}$$

Now, "$w \not\Vdash \Box B$" $\Rightarrow \forall \alpha(\text{“}w \not\Vdash \triangle_\alpha B\text{”})$, hence

$$\forall x \leq N \neg Cpl(x, \ulcorner B^{*}\urcorner); \tag{2}$$

finally, (1) and (2) imply $\neg Pr(\ulcorner B^{*}\urcorner)$

■

3.11 Lemma. For all $\Box B \in Ad(A)$ and $w \in K$

$$\vdash \text{“}l = w\text{”} \rightarrow [\text{“}w \Vdash \Box B\text{”} \leftrightarrow Provable(\ulcorner B^{*}\urcorner)]$$

Proof. If $w \not\Vdash \Box B$, then there is $v \succ w$ such that $v \not\Vdash B$. By the Lemma 3.10[6]

$\vdash \text{“}l = v\text{”} \rightarrow \neg B^*$
$\vdash B^* \rightarrow \text{“}l \neq v\text{”}$
$\vdash Provable(\ulcorner B^{*}\urcorner) \rightarrow Provable(\ulcorner \text{“}l \neq v\text{”}\urcorner)$
$\vdash \text{“}l = w\text{”} \rightarrow \neg Provable(\ulcorner \text{“}l \neq v\text{”}\urcorner)$ by the Solovay lemma, 2.8(4)
$\vdash \text{“}l = w\text{”} \rightarrow \neg Provable(\ulcorner B^{*}\urcorner)$
$\vdash \text{“}l = w\text{”} \rightarrow [\text{“}w \not\Vdash \Box B\text{”} \rightarrow \neg Provable(\ulcorner B^{*}\urcorner)]$

[5]Here and below "$w \Vdash F$" means a natural recursive formalization of $w \Vdash F$ in $\mathtt{PA}$.
[6]We use the fact that the model is described in $\mathtt{PA}$ by natural recursive formulas.

If $w \Vdash \Box B$, then for every $v \succ w$ we have $v \Vdash B$. Thus by the Lemma 3.10 for all $v \succ w$ we have $\vdash$ "$l = v$" $\rightarrow B^*$,

$$\vdash \bigvee_{v \succ w} \text{“}l = v\text{”} \rightarrow B^*$$

If $w \succ 0$, then

$$\begin{array}{l} \vdash Provable(\ulcorner \bigvee_{v \succ w} \text{“}l = v\text{”}\urcorner) \rightarrow Provable(\ulcorner B^* \urcorner) \\ \vdash Provable(\ulcorner \bigvee_{v \in K} \text{“}l = v\text{”}\urcorner) \\ \vdash \text{“}l = w\text{”} \rightarrow Provable(\ulcorner \bigwedge_{w \not\prec v} \text{“}l \neq v\text{”}\urcorner) \\ \vdash \text{“}l = w\text{”} \rightarrow Provable(\ulcorner \bigvee_{w \prec v} \text{“}l = v\text{”}\urcorner) \\ \vdash \text{“}l = w\text{”} \rightarrow Provable(\ulcorner B^* \urcorner). \end{array}$$

If $w = 0$, then $1 \Vdash B$, hence $0 \Vdash B$, hence $\forall v \in K \; v \Vdash B$.

$$\begin{array}{l} \vdash \bigvee_{v \in K} \text{“}l = v\text{”} \rightarrow B^* \\ \vdash \bigvee_{v \in K} \text{“}l = v\text{”} \\ \vdash B^* \\ \vdash Provable(\ulcorner B^* \urcorner) \\ \vdash \text{“}l = 0\text{”} \rightarrow Provable(\ulcorner B^* \urcorner). \end{array}$$

In any case $\vdash$ "$l = 0$" $\rightarrow Provable(\ulcorner B^* \urcorner)$, thus

$$\vdash \text{“}l = 0\text{”} \rightarrow [\text{“}w \Vdash \Box B\text{”} \rightarrow Provable(\ulcorner B^* \urcorner)],$$

and we are done.
■

3.12 Lemma. $\vdash Prv(y) \leftrightarrow Provable(y)$

Proof. Since $w \Vdash \triangle_\alpha B \Rightarrow w \Vdash \Box B$, one can demonstrate in $\mathtt{PA}$ that *Prv* and *Provable* can differ only on gödelnumbers of some B^*'s such that $\Box B \in Ad(A)$. For such B^* by Lemma 3.10

$$\vdash \text{“}l = w\text{”} \rightarrow [\text{“}w \Vdash \Box B\text{”} \leftrightarrow Pr(\ulcorner B^* \urcorner)].$$

By Lemma 3.11 we get

$$\vdash \text{“}l = w\text{”} \rightarrow [Provable(\ulcorner B^* \urcorner) \leftrightarrow Pr(\ulcorner B^* \urcorner)]$$
$$\vdash \bigvee_{w \in K} \text{“}l = w\text{”} \rightarrow [Provable(\ulcorner B^* \urcorner) \leftrightarrow Pr(\ulcorner B^* \urcorner)]$$

and as

$$\vdash \bigvee_{w \in K} \text{“}l = w\text{”},$$

and we are done.
■

3.13 Lemma. $Cpl(x, y)$ is a standard complexity predicate.

Proof. By FPE $Cpl \in \Sigma^0_1$. Let us prove

$$\vdash u \leq v \rightarrow [Cpl(u, y) \rightarrow Cpl(v, y)].$$

All the following reasonings are formalizable in $\mathtt{PA}$.

1. $u = 0 \Rightarrow \neg Cpl(u, y)$;
2. If $0 < u \leq v \leq N$, then two cases are possible:
   - y is not equal to any B^* such that $\triangle_{\alpha_u} B \in Ad(A)$, hence $\neg Cpl(u, y)$;
   - $y = \ulcorner B^* \urcorner$ for some such B^*. Then
     $$u \leq v \Rightarrow \forall w (w \Vdash \triangle_{\alpha_u} B \Rightarrow w \Vdash \triangle_{\alpha_v} B),$$
     hence $Cpl(u, y) \rightarrow Cpl(v, y)$;
3. $u \leq N < v$. This case is similar to 2. but here we have $\forall w (w \Vdash \triangle_{\alpha_u} B \Rightarrow w \Vdash \Box B)$;
4. If $u > N$, then $v > N$ and by the definition of Cpl we get $Cpl(u, y) \leftrightarrow Cpl(v, y)$.

The other conditions on a standard complexity predicate follow from Lemma 3.12 and from the properties of *Provable* .

■

3.14 Lemma. *Prf* is a standard proof predicate and *Prf* and *Cpl* are provably compatible.

Proof. The recursiveness follows from the definition. We'll prove $\vdash Pr(y) \leftrightarrow Provable(y)$, what will imply all other conditions required. From the definition

$$\vdash Pr(y) \leftrightarrow Provable(y) \vee \bigvee_{i=0}^{N'} \bigvee_{j \in I_i} (y = \ulcorner C_j{}^* \urcorner).$$

But for all i, $j \in I_i$ and $w \in K$ $w \Vdash \Box_{p_i} C_j$, hence $w \Vdash C_j$, then by Lemma 3.10

$$\vdash \textstyle\bigvee_{w \in K} \text{“}l = w\text{”} \rightarrow C_j{}^*$$
$$\vdash C_j{}^*$$
$$\vdash Provable(\ulcorner C_j{}^* \urcorner)$$

■

Let us now complete the proof of the Theorem 3.8. Lemmas 3.13 and 3.14 provide that the interpretation $*$ is defined correctly. If $\mathcal{K}$ is a countermodel for A, then there is w such that $w \nVdash A$. Thus $\vdash$ “$l = w$” $\rightarrow \neg A^*$. Now if $\mathtt{PA} \vdash A^*$, then $\mathtt{PA} \vdash$ “$l \neq w$”, that contradicts the Solovay lemma.

■

Comment

As usual, the truth cases for $\mathcal{E}$ and $\mathcal{BE}$ called $\mathcal{E}^\omega$ and $\mathcal{BE}^\omega$ whose axioms are all the theorems of $\mathcal{E}$ and $\mathcal{BE}$, the axiom scheme $\Box A \rightarrow A$ and the only rule is **R0**, are complete with respect to all arithmetical interpretations:

3.15 Theorem.

$$\begin{array}{l} \mathcal{E}^\omega \vdash A \\ \mathcal{BE}^\omega \vdash A \end{array} \iff \text{for every interpretation } * \quad A^* \text{ is true.}$$

The proof goes like that in [2].

It looks now a routine exercise to incorporate the functionality property into the logic of recursively enumerable complexity predicates by combining the technique from chapters 2 and 3.

References

[1] S. Artëmov, "Logic of Proofs," *Annals of Pure and Applied Logic*,vol. 67, pp. 29-59, 1994.

[2] D. Guaspari and R. M. Solovay, "Rosser sentences," *Annals of Mathematical Logic*, vol. 16, pp. 81–99, 1979.

[3] J. Lassez, M. Maher, and K. Marriott, "Unification revisited," in *Foundations of Deductive Databases and Logic Programming* (J. Minker, ed.), ch. 15, pp. 587–625, Morgan Kaufmann Publishers, Inc., 1987.

[4] R. Magari, "The diagonalizable algebras (the algebraization of the theories which express Theor.:II)." *Bolletino della Unione Matematica Italiana. Serie IV* 12 (1975) Supplimento al fasc. 3, pp. 117-125, 1975.

[5] R. M. Solovay, "Provability interpretations of modal logic," *Israel Journal of Mathematics*, vol. 25, pp. 287–304, 1976.