Notre Dame Journal of Formal Logic
Volume 46, Number 4, 2005

Polynomially Bounded Recursive Realizability

Saeed Salehi

Abstract A polynomially bounded recursive realizability, in which the recursive functions used in Kleene's realizability are restricted to polynomially bounded functions, is introduced. It is used to show that provably total functions of Ruitenburg's Basic Arithmetic are polynomially bounded (primitive) recursive functions. This sharpens our earlier result where those functions were proved to be primitive recursive. Also a polynomially bounded schema of Church's Thesis is shown to be polynomially bounded realizable. So the schema is consistent with Basic Arithmetic, whereas it is inconsistent with Heyting Arithmetic.

1 Introduction

One of the strongest tools for studying intuitionistic theories is realizability. Realizability was introduced by Kleene (see, e.g., Troelstra & van Dalen [15] for the history and definitions) and later was generalized to measure the strength of various subclassical theories. Here we are concerned about arithmetical realizability, that is, realizability by natural numbers, which serves as a Gödel coding of recursive functions. A common feature of all these generalizations is restricting the recursive functions in Kleene's "original" realizability to a certain class of recursive functions.

In López-Escobar's "Prim-realizability" for negationless arithmetic [7] and in Damnjanovic's "strictly primitive recursive realizability" ([1] and [4]) those recursive functions are restricted to primitive recursives. The other realizabilities introduced by Damnjanovic are realizability by $<\epsilon_0$-recursive functions in [2] and realizability by elementary functions in [3]. In Plisko's Σ_n-realizability [11] the recursive functions are restricted to those functions whose graphs are definable by Σ_n-formulas.

A new realizability by primitive recursive functions was introduced by Salehi [13]. It was applied to Basic Arithmetic **BA**, a theory built on Basic Logic, a subintuitionistic logic in which the modes ponens rule is not valid in its general form

Received January 30, 2004; accepted August 16, 2004; printed December 8, 2005
2000 Mathematics Subject Classification: Primary, 03F30; Secondary, 03F50
Keywords: provably total function, Basic Arithmetic, Basic Logic, realizability

(see Ruitenburg [12] where **BA** was introduced). This primitive recursive realizability was further studied by Viter ([16], [17], [18], and [19]), and some relations among the above mentioned realizabilities were recently investigated by Park ([8], [9], and [10]).

A well-known method of measuring the strength of a theory is characterizing its provably total functions. An application of the soundness of Heyting Arithmetic **HA** with respect to Kleene's recursive realizability is a specification of the provably total functions of **HA**: they are all recursive. This has been refined by an application of the soundness of **HA** to Damnjanovic's $<\epsilon_0$-recursive realizability [3]: all the provably total functions of **HA** are (exactly) $<\epsilon_0$-recursive functions.

In this paper, a result of [13], that provably total functions of **BA** are primitive recursive, is sharpened by applying a realizability by polynomially bounded recursive functions, abbreviated as P-realizability. Informally speaking, a formula is P-realizable if and only if it is efficiently verifiable, that is to say, its truth can be justified by polynomially computable functions. We note that a polynomially bounded recursive function is primitive recursive. So P-realizability is stronger than the other realizabilities mentioned above. This could be interesting from the Complexity Theory point of view since it deals with easily computable functions.

The essential facts about the applicability of P-realizability are

1. polynomially bounded recursive functions are definable by an arithmetical formula (denoted by $\mathcal{P}(x)$ in Section 3), and
2. all S-m-n functions can be chosen to be polynomially bounded in terms of the variables (the details are elaborated in Section 3).

Though **BA** is not sound with respect to P-realizability, a subtheory of **BA**, called weakened Basic Arithmetic $\mathbf{BA}^{\mathbf{w}}$ is sound with respect to this realizability. Since the provably total functions of **BA** and $\mathbf{BA}^{\mathbf{w}}$ coincide, it follows that the provably total functions of **BA** are polynomially bounded (primitive) recursive functions.

In Section 2, the axioms and rules of **BA** are listed, and some basic facts about **BA** and $\mathbf{BA}^{\mathbf{w}}$ are proved. In Section 3, P-realizability is introduced and the soundness of $\mathbf{BA}^{\mathbf{w}}$ with respect to it is proved. As a result it follows that the provably total functions of **BA** are polynomially bounded recursive functions. Finally, in Section 4, a polynomially bounded version of the arithmetical form of Church's Thesis is introduced and is proved to be P-realizable and consistent with **BA**, while it is intuitionistically (and classically) false.

2 Basic Arithmetic

Basic Arithmetic is built over Basic Logic in the same way that Heyting Arithmetic and Peano Arithmetic are built over intuitionistic logic and classical logic, respectively.

The nonlogical symbols of Basic Arithmetic are a constant '0', a unary function symbol 'S' for successor, and the binary function symbols '$\cdot$' and '$+$'. The language of Basic Logic contains two logical constants, $\bot$ (Falsehood) and $\top$ (Truth), and the logical connectives $\wedge$, $\vee$, $\exists$, and $\forall$. Terms, atomic formulas, and formulas are defined as usual, except that for universal quantification we have the more elaborate rule: if A and B are formulas and $\mathbf{x}$ is a finite (possibly empty) sequence of variables, then $\forall\mathbf{x}(A \to B)$ is also a formula. Free variables are defined in the obvious way. We may write $A \to B$ for $\forall(A \to B)$, that is, implication is universal quantification with

an empty sequence of variables. Given a sequence of variables $\mathbf{x}$ without repetitions, we write $A^{\mathbf{x}}_{\mathbf{t}}$ for the formulas that result from substituting the terms of $\mathbf{t}$ for all free occurrences of the variables of $\mathbf{x}$ in the formula A (see [12], Section 2).

Axioms of BA (over the sequent calculus)

Ax1 $A \Rightarrow A$

Ax2 $A \Rightarrow \top$

Ax3 $\bot \Rightarrow A$

Ax4 $A \wedge \exists x B \Rightarrow \exists x(A \wedge B)$ where x is not free in A

Ax5 $A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)$

Ax6 $\forall \mathbf{x}(A \to B) \wedge \forall \mathbf{x}(B \to C) \Rightarrow \forall \mathbf{x}(A \to C)$

Ax7 $\forall \mathbf{x}(A \to B) \wedge \forall \mathbf{x}(A \to C) \Rightarrow \forall \mathbf{x}(A \to B \wedge C)$

Ax8 $\forall \mathbf{x}(B \to A) \wedge \forall \mathbf{x}(C \to A) \Rightarrow \forall \mathbf{x}(B \vee C \to A)$

Ax9 $\forall \mathbf{x}(A \to B) \Rightarrow \forall \mathbf{x}(A^{\mathbf{x}}_{\mathbf{t}} \to B^{\mathbf{x}}_{\mathbf{t}})$
where no variable in $\mathbf{t}$ is bounded by a quantifier of A or B

Ax10 $\forall \mathbf{x}(A \to B) \Rightarrow \forall \mathbf{y}(A \to B)$
where no variable in $\mathbf{y}$ is free in the left-hand side

Ax11 $\forall \mathbf{y} x(B \to A) \Rightarrow \forall \mathbf{y}(\exists x B \to A)$ where x is not free in A

Ax12 $\Rightarrow x = x$

Ax13 $x = y \wedge A \Rightarrow A^x_y$ for atomic A

Ax14 $S(x) = S(y) \Rightarrow x = y$

Ax15 $S(x) = 0 \Rightarrow \bot$

Ax16 $\Rightarrow x + 0 = x$

Ax17 $\Rightarrow x \cdot 0 = 0$

Ax18 $\Rightarrow x + S(y) = S(x + y)$

Ax19 $\Rightarrow x \cdot S(y) = (x \cdot y) + x$

Ax20 $\forall x \mathbf{y}(A \to A^x_{Sx}) \Rightarrow \forall x \mathbf{y}(A^x_0 \to A)$

Rules

Ru1 $$\frac{A \Rightarrow B \quad B \Rightarrow C}{A \Rightarrow C}$$

Ru2 $$\frac{A \Rightarrow B \quad A \Rightarrow C}{A \Rightarrow B \wedge C}$$

Ru3 $$\frac{A \Rightarrow B \wedge C}{A \Rightarrow B} \qquad \frac{A \Rightarrow B \wedge C}{A \Rightarrow C}$$

Ru4 $$\frac{B \Rightarrow A \quad C \Rightarrow A}{B \vee C \Rightarrow A}$$

Ru5 $$\frac{B \vee C \Rightarrow A}{B \Rightarrow A} \qquad \frac{B \vee C \Rightarrow A}{C \Rightarrow A}$$

Ru6 $\dfrac{A \Rightarrow B}{A^{\mathbf{x}}_{\mathbf{t}} \Rightarrow B^{\mathbf{x}}_{\mathbf{t}}}$ in which no variable in $\mathbf{t}$ is bounded in A or B

Ru7 $\dfrac{B \Rightarrow A}{\exists x B \Rightarrow A}$ where x is not free in A

Ru8 $\dfrac{\exists x B \Rightarrow A}{B \Rightarrow A}$ where x is not free in A

Ru9 $\dfrac{A \wedge B \Rightarrow C}{A \Rightarrow \forall \mathbf{x}(B \to C)}$ where no variable in $\mathbf{x}$ is free in A

Ru10 $\dfrac{A \Rightarrow A^x_{Sx}}{A^x_0 \Rightarrow A}$

The *Weakened Basic Arithmetic*, denoted by $\mathbf{BA^w}$, is defined to be the sequent theory axiomatized by the above axioms and rules except Ru10. However, $\mathbf{BA^w}$ is closed under a weaker version of Ru10.

Lemma 2.1 *The theory* $\mathbf{BA^w}$ *is closed under the rule*

$$\frac{A \Rightarrow A^x_{Sx}}{A^x_0 \Rightarrow \forall x(\top \to A)}\ .$$

Proof By Ru9, from $A \Rightarrow A^x_{Sx}$ the sequent $\Rightarrow \forall x(A \to A^x_{Sx})$ follows and this by Ax20 and Ru1 implies $\Rightarrow \forall x(A^x_0 \to A)$. On the other hand, by Ax1 and Ru9, $A^x_0 \Rightarrow \forall x(\top \to A^x_0)$ can be proved. Hence, from Ax8, Ru2, and Ru1, $A^x_0 \Rightarrow \forall x(\top \to A)$ follows. □

In fact, $\mathbf{BA^w}$ is not much weaker than **BA** and it proves the universal closure formulas of the **BA**-provable sequents.

Theorem 2.2 *For a sequent* $A \Rightarrow B$*, if* $\mathbf{BA} \vdash A \Rightarrow B$*, then there exists a sequence of variables* $\mathbf{x}$ *such that* $\mathbf{BA^w} \vdash\Rightarrow \forall \boldsymbol{x}(A \to B)$.

Proof This is essentially Proposition 6.1 of [12] whose proof is mainly based on Proposition 4.13 (of [12]). An easy examination of the proof shows that in deducing $\mathbf{BA} \vdash\Rightarrow \forall \mathbf{x}(A \to B)$ from $\mathbf{BA} \vdash A \Rightarrow B$, Ru10 is not used, so the proof immediately implies $\mathbf{BA^w} \vdash\Rightarrow \forall \mathbf{x}(A \to B)$ from $\mathbf{BA} \vdash A \Rightarrow B$. □

It follows that provably total functions of **BA** and of $\mathbf{BA^w}$ coincide.

Corollary 2.3 *Let* $A(\mathbf{x}, y)$ *be a formula with the shown free variables. If* $\Rightarrow \exists y A(\mathbf{x}, y)$ *is provable in* **BA***, then* $\mathbf{BA} \vdash\Rightarrow \forall \mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$*, and then* $\mathbf{BA^w} \vdash\Rightarrow \top \to \forall \mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$.

Proof By Ru9, $\mathbf{BA} \vdash\Rightarrow \exists y A(\mathbf{x}, y)$ implies $\mathbf{BA} \vdash\Rightarrow \forall \mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$, and this, by Theorem 2.2 and Ax10, implies $\mathbf{BA^w} \vdash\Rightarrow \top \to \forall \mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$. □

3 Polynomially Bounded Recursive Realizability

The Gödel encoding described in Chapter V of Hájek and Pudlák [5] is used in the paper. It is called "Linear Compressed Encoding" by Willard [21]. This encoding enables us to have polynomially bounded S-m-n functions. The details are discussed below.

Let φ_x be the (unique) unary recursive function whose program has the (Gödel) code x (cf. Soare [14] and [13]).[1] Take $\langle\,,\,\rangle$ to be a fixed pairing function (such as $\langle x, y\rangle = \frac{1}{2}(x+y)(x+y+1)+y$ with the projections π_1 and π_2, that is, $\pi_1(\langle x, y\rangle) = x$ and $\pi_2(\langle x, y\rangle) = y$. For a sequence $\mathbf{x} = (x_1, x_2, \ldots, x_m)$, $\varphi_a(\mathbf{x})$ is understood as $\varphi_a(\langle x_1, \langle x_2, \ldots, \langle x_{m-1}, x_m\rangle\rangle\rangle)$. We note that any statement involving $\varphi_a(x)$ can be written in the language of arithmetic: a proposition such as $\mathcal{A}(\varphi_a(x))$ is $\exists z\big(\mathbf{T}(a, x, z)\wedge\mathcal{A}(\mathbf{U}(z))\big)$ where $\mathbf{T}$ is Kleene's T-predicate and $\mathbf{U}$ is a result-extracting function (see, e.g., [15]).

Throughout, we take the language of $\mathbb{N}$ to contain function symbols for all primitive recursive functions. Let $\mathcal{P}(x)$ be the formula $\forall z\big(\varphi_{\pi_1(x)}(z) \le z^{\pi_2(x)} + \pi_2(x)\big)$, or equivalently, $\forall z\exists t\big(\mathbf{T}(\pi_1(x), z, t)\wedge\mathbf{U}(t) \le z^{\pi_2(x)}+\pi_2(x)\big)$. Holding $\mathcal{P}(x)$ means that $x = \langle x_1, x_2\rangle$ where x_1 is the code of a polynomially bounded recursive function with the bound x_2, that is, $\varphi_{x_1}(z) \le z^{x_2} + x_2$ for all z. We note that a function $f : \mathbb{N} \to \mathbb{N}$ is polynomially bounded if and only if for a fixed $m \in \mathbb{N}$, $f(x) \le x^m + m$ holds for all x. If such a function f is recursive, then there is a natural n such that $f = \varphi_n$ and $\mathbb{N} \models \mathcal{P}(\langle n, m\rangle)$.

We define polynomially bounded recursive realizability, P-realizability for short.

Definition 3.1 $x\,\mathbf{r}^{\mathrm{P}}A$ is defined by induction on the complexity of A:

1. $x\,\mathbf{r}^{\mathrm{P}}p \equiv p$, for atomic p and $p = \top, \bot$;
2. $x\,\mathbf{r}^{\mathrm{P}}A \wedge B \equiv \big(\pi_1(x)\,\mathbf{r}^{\mathrm{P}}A\big) \wedge \big(\pi_2(x)\,\mathbf{r}^{\mathrm{P}}B\big)$;
3. $x\,\mathbf{r}^{\mathrm{P}}A \vee B \equiv \big(\pi_1(x) = 0 \wedge \pi_2(x)\,\mathbf{r}^{\mathrm{P}}A\big) \vee \big(\pi_1(x) \ne 0 \wedge \pi_2(x)\,\mathbf{r}^{\mathrm{P}}B\big)$;
4. $x\,\mathbf{r}^{\mathrm{P}}\exists z A(z) \equiv \pi_2(x)\,\mathbf{r}^{\mathrm{P}}A(\pi_1(x))$;
5. $x\,\mathbf{r}^{\mathrm{P}}\forall\mathbf{z}(A(\mathbf{z}) \to B(\mathbf{z})) \equiv \mathcal{P}(x) \wedge \forall y, \mathbf{z}\big(y\,\mathbf{r}^{\mathrm{P}}A(\mathbf{z}) \to \varphi_{\pi_1(x)}(y, \mathbf{z})\,\mathbf{r}^{\mathrm{P}}B(\mathbf{z})\big)$.

P-realizability can be extended to sequents as

6. $x\,\mathbf{r}^{\mathrm{P}}\Big(A \Rightarrow B\Big) \equiv \mathcal{P}(x) \wedge \forall y\big(y\,\mathbf{r}^{\mathrm{P}}A \to \varphi_{\pi_1(x)}(y)\,\mathbf{r}^{\mathrm{P}}B\big)$.

We say "the function f P-realizes $A \Rightarrow B$", if for a natural number n, $\mathcal{P}(n)$, $\varphi_n = f$, and $n\,\mathbf{r}^{\mathrm{P}}\Big(A \Rightarrow B\Big)$ hold.

A useful property of the Linear Compressed Encoding is providing an efficient upper bound on the substitution functions. For a term t, t_s^x is obtained from t by replacing all the occurrences of x in t with the term s. As stated in the explanation after Proposition 3.36 of [5] (see also Lemma 4.11 (1) of Wilkie & Paris [20]) $|t_s^x| \le \text{constant} \cdot |t| \cdot |s|$ where $|a| = \lceil\log_2(a+1)\rceil$. Moreover, this bound is essentially the best possible. As a result it follows that there is a fixed natural number $\mathbf{c}$ such that $t_s^x \le (s+1)^{\mathbf{c}\cdot\log_2(t+1)} + \mathbf{c}$.

Recall that S-m-n function S_n^m is a primitive recursive function satisfying $\varphi_{S_n^m(e,\mathbf{a})}(\mathbf{b}) = \varphi_e(\mathbf{a}, \mathbf{b})$ for all (program code) e, m-tuple $\mathbf{a}$, and n-tuple $\mathbf{b}$. In this paper we need the special case of $m = n = 1$. Suppose the program $\mathcal{P}$ has the code e and its input symbols are x and y. For a natural number a, let the program $\mathcal{Q}$ be constructed from $\mathcal{P}$ by putting a in all the places of x and restricting its input to y. The output of the program $\mathcal{Q}$ for an input b (in the place of y) is $\varphi_e(a, b)$. Hence, the code of the program $\mathcal{Q}$ can be a candidate for the value of S_1^1 function, noting that $\varphi_{S_1^1(e,a)}(b) = \varphi_e(a, b)$. The code of $\mathcal{Q}$ is roughly e_a^x (the input x is replaced with a), or informally speaking, $e_a^x \approx S_1^1(e, a)$. Thus from $e_a^x \le (a+1)^{\mathbf{c}\cdot\log_2(e+1)} + \mathbf{c}$, we get a polynomially bounded version of S_1^1 theorem (see also Jones [6]).

Theorem 3.2 *For any unary recursive function g, there is a unary polynomially bounded recursive function f such that $\varphi_{f(a)}(b) = g(\langle a, b\rangle)$ for all a, b.*

This will be used in our soundness theorem of $\mathbf{BA}^{\mathbf{w}}$ to P-realizability.

Theorem 3.3 *For all sequents $A \Rightarrow B$, if $\mathbf{BA}^{\mathbf{w}} \vdash A \Rightarrow B$, then for a natural n, $\mathbb{N} \models n\, \boldsymbol{r}^{\mathrm{P}}\big(A \Rightarrow B\big)$.*

Proof The proof is by induction on the length of the proof of the sequent: we show that for each axiom of $\mathbf{BA}^{\mathbf{w}}$ there is a natural number P-realizing it, and for any P-realizer of the hypothesis of the rules of $\mathbf{BA}^{\mathbf{w}}$ there is a natural number P-realizing its conclusion. Throughout the proof we suppose that the assumptions about the variables (e.g., in Ax4 and Ru6) hold.

Axioms

For realizing a sequent $A \Rightarrow B$ it is enough to find a *polynomially bounded recursive* function (P-function, for short) f such that '$m\ \mathbf{r}^{\mathrm{P}} A \Longrightarrow f(m)\ \mathbf{r}^{\mathrm{P}} B$' for every m.

For Ax1 ($A \Rightarrow A$), Ax2 ($A \Rightarrow \top$), Ax3 ($\bot \Rightarrow A$), Ax14 ($S(x) = S(y) \Rightarrow x = y$), Ax18 ($\Rightarrow x + S(y) = S(x + y)$), Ax19 ($\Rightarrow x \cdot S(y) = (x \cdot y) + x$), and Ax9 ($\forall \mathbf{x}(A \to B) \Rightarrow \forall \mathbf{x}(A^{\mathbf{x}}_{\mathbf{t}} \to B^{\mathbf{x}}_{\mathbf{t}})$), let $f(u) = u$.

For Ax12 ($\Rightarrow x = x$), Ax15 ($S(x) = 0 \Rightarrow \bot$), Ax16 ($\Rightarrow x + 0 = x$), and Ax17 ($\Rightarrow x \cdot 0 = 0$), let $f(u) = 0$.

For Ax4 ($A \wedge \exists x B \Rightarrow \exists x(A \wedge B)$) and Ax5 ($A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)$), let $f(u) = \langle \pi_1\pi_2(u), \langle \pi_1(u), \pi_2\pi_2(u)\rangle\rangle$.

For Ax6 ($\forall \mathbf{x}(A \to B) \wedge \forall \mathbf{x}(B \to C) \Rightarrow \forall \mathbf{x}(A \to C)$), let f be a P-function (by Theorem 3.2) such that $\varphi_{f(u)}(v, \mathbf{x}) = \varphi_{\pi_2(u)}(\varphi_{\pi_1(u)}(v, \mathbf{x}), \mathbf{x})$.

For Ax7 ($\forall \mathbf{x}(A \to B) \wedge \forall \mathbf{x}(A \to C) \Rightarrow \forall \mathbf{x}(A \to B \wedge C)$), again by Theorem 3.2, let f be a P-function satisfying $\varphi_{f(u)}(v, \mathbf{x}) = \langle \varphi_{\pi_1(u)}(v, \mathbf{x}), \varphi_{\pi_2(u)}(a, \mathbf{x})\rangle$.

For Ax8 ($\forall \mathbf{x}(B \to A) \wedge \forall \mathbf{x}(C \to A) \Rightarrow \forall \mathbf{x}(B \vee C \to A)$), similar to the above cases, take a P-function f such that

$$\varphi_{f(u)}(v, \mathbf{x}) = \begin{cases} \varphi_{\pi_1(u)}(\pi_2(v), \mathbf{x}) & \text{if } \pi_1(v) = 0 \\ \varphi_{\pi_2(u)}(\pi_2(v), \mathbf{x}) & \text{if } \pi_1(v) \neq 0. \end{cases}$$

For Ax10 ($\forall \mathbf{x}(A \to B) \Rightarrow \forall \mathbf{y}(A \to B)$) we can assume $\mathbf{x} = (\mathbf{y}, \mathbf{z})$ for some $\mathbf{z}$. Take a P-function f satisfying $\varphi_{f(u)}(\mathbf{y}) = \varphi_u(\mathbf{y}, \mathbf{0})$.

For Ax11 ($\forall \mathbf{y} x(B \to A) \Rightarrow \forall \mathbf{y}(\exists x B \to A)$), take a P-function f satisfying $\varphi_{f(u)}(v, \mathbf{y}) = \varphi_u(\pi_2(v), \mathbf{y}, \pi_1(v))$.

For Ax13 ($x = y \wedge A \Rightarrow A^x_y$), put $f(u) = \pi_2(u)$.

And finally for Ax20 ($\forall x \mathbf{y}(A \to A^x_{Sx}) \Rightarrow \forall x \mathbf{y}(A^x_0 \to A)$), take a P-function f by $\varphi_{f(u)}(v, 0, \mathbf{y}) = v$ and $\varphi_{f(u)}(v, x + 1, \mathbf{y}) = \varphi_u(\varphi_{f(u)}(v, x, \mathbf{y}), x, \mathbf{y})$.

For all cases it can be proven that the function f P-realizes the corresponding axiom (cf. [13]).

Rules—The induction step

Similar to the axiom cases, assuming that $\langle n, k\rangle$ (and $\langle m, k'\rangle$) P-realize(s) the hypothesis of the rule, it is enough to find a polynomially bounded function (denoted by f and g) which P-realizes the conclusion of the rule. Note that if $\langle n, k\rangle$ and $\langle m, k'\rangle$ are P-realizers, then φ_n and φ_m are polynomially bounded.

Ru1: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A \Rightarrow B)$ and $\langle m, k'\rangle\, \mathbf{r}^{\mathrm{P}}(B \Rightarrow C)$, then the function f defined by $f(u) = \varphi_m(\varphi_n(u))$ P-realizes $A \Rightarrow C$.

Ru2: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A \Rightarrow B)$ and $\langle m, k'\rangle\, \mathbf{r}^{\mathrm{P}}(A \Rightarrow C)$, then the function f defined by $f(u) = \langle \varphi_n(u), \varphi_m(u)\rangle$ P-realizes $A \Rightarrow B \wedge C$.

Ru3: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A \Rightarrow B \wedge C)$, then f and g defined by $f(u) = \pi_1\varphi_n(u)$ and $g(u) = \pi_2\varphi_n(u)$ P-realize $A \Rightarrow B$ and $A \Rightarrow C$, respectively.

Ru4: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(B \Rightarrow A)$ and $\langle m, k'\rangle\, \mathbf{r}^{\mathrm{P}}(C \Rightarrow A)$, then f defined by

$$f(u) = \begin{cases} \varphi_n(\pi_2(u)) & \text{if } \pi_1(u) = 0 \\ \varphi_m(\pi_2(u)) & \text{if } \pi_1(u) \neq 0 \end{cases}$$

P-realizes $B \vee C \Rightarrow A$.

Ru5: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(B \vee C \Rightarrow A)$, then f and g defined by $f(u) = \varphi_n(0, u)$ and $g(u) = \varphi_n(1, u)$ P-realize $B \Rightarrow A$ and $C \Rightarrow A$, respectively.

Ru6: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A \Rightarrow B)$, then $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A^{\mathbf{x}}_{\mathbf{t}} \Rightarrow B^{\mathbf{x}}_{\mathbf{t}})$.

Ru7: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(B \Rightarrow A)$, and x is free in B, then the function f defined by $f(u) = \varphi_n(\pi_2(u))$ P-realizes $\exists x\, B \Rightarrow A$.

Ru8: If $\langle n, k\rangle \mathbf{r}^{\mathrm{P}}(\exists x\, B \Rightarrow A)$ and if x is free in B, then f defined by $f(u) = \varphi_n(0, u)$ P-realizes $B \Rightarrow A$.

Ru9: If $\langle n, k\rangle\, \mathbf{r}^{\mathrm{P}}(A \wedge B \Rightarrow C)$ and all the variables in $\mathbf{x}$ are free in $B \to C$, then a P-function f satisfying $\varphi_{f(u)}(v, \mathbf{x}) = \varphi_n(\langle u, v\rangle)$ P-realizes $A \Rightarrow \forall \mathbf{x}(B \to C)$.

It can be shown that if $\langle n, k\rangle$ (and $\langle m, k'\rangle$) P-realize(s) the hypothesis (hypotheses) of the above rules, then the function f (and g) P-realize(s) the conclusion of the rule (cf. [13]). □

Polynomially bounded $\mathbf{q}$-realizability is defined by applying the well-known changes to $\mathbf{r}^{\mathrm{P}}$-realizability.

Definition 3.4 $x\, \mathbf{q}^{\mathrm{P}} A$ is defined by induction on A:

1. $x\, \mathbf{q}^{\mathrm{P}} p \equiv p$, for atomic p, and $p = \top, \bot$;
2. $x\, \mathbf{q}^{\mathrm{P}} A \wedge B \equiv (\pi_1(x)\, \mathbf{q}^{\mathrm{P}} A) \wedge (\pi_2(x)\, \mathbf{q}^{\mathrm{P}} B)$;
3. $x\, \mathbf{q}^{\mathrm{P}} A \vee B \equiv (\pi_1(x) = 0 \wedge \pi_2(x)\, \mathbf{q}^{\mathrm{P}} A) \vee (\pi_1(x) \neq 0 \wedge \pi_2(x)\, \mathbf{q}^{\mathrm{P}} B)$;
4. $x\, \mathbf{q}^{\mathrm{P}} \exists z A(z) \equiv \pi_2(x)\, \mathbf{q}^{\mathrm{P}} A(\pi_1(x))$;
5. $x\, \mathbf{q}^{\mathrm{P}} \forall \mathbf{z}(A(\mathbf{z}) \to B(\mathbf{z})) \equiv \mathcal{P}(x) \wedge$
$\forall y, \mathbf{z}(y\, \mathbf{q}^{\mathrm{P}} A(\mathbf{z}) \to \varphi_{\pi_1(x)}(y, \mathbf{z})\, \mathbf{q}^{\mathrm{P}} B(\mathbf{z})) \wedge \forall \mathbf{z}(A(\mathbf{z}) \to B(\mathbf{z}))$.

And similarly for the sequents, $x\, \mathbf{q}^{\mathrm{P}}(A \Rightarrow B)$ is

6. $\mathcal{P}(x) \wedge \forall y\big(y\, \mathbf{q}^{\mathrm{P}} A \to \varphi_{\pi_1(x)}(y)\, \mathbf{q}^{\mathrm{P}} B\big) \wedge (A \to B)$.

The obvious property of **q**-realizability is $\mathbb{N} \models (n\ \mathbf{q}^{\mathrm{P}} A) \to A$ for any A.

The proof of soundness of $\mathbf{BA}^{\mathbf{w}}$ to $\mathbf{r}^{\mathrm{P}}$ works as usual for $\mathbf{q}^{\mathrm{P}}$-realizability.

Theorem 3.5 *For all sequents $A \Rightarrow B$, if $\mathbf{BA}^{\mathbf{w}} \vdash A \Rightarrow B$, then for some n, $\mathbb{N} \models n\ \mathbf{q}^{\mathrm{P}}\big(A \Rightarrow B\big)$.*

The theorem provides a specification of the provably total functions of $\mathbf{BA}^{\mathbf{w}}$.

Lemma 3.6 *For every formula $A(\mathbf{x}, y)$ with the presented free variables, there is a (unary) polynomially bounded primitive recursive function f such that if $\mathbf{BA}^{\mathbf{w}} \vdash\!\Rightarrow \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$ then $\mathbb{N} \models \forall\mathbf{x} A(\mathbf{x}, f(\mathbf{x}))$.*

Proof Suppose $\mathbf{BA}^{\mathbf{w}} \vdash\!\Rightarrow \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$. By Theorem 3.5, there is an $n \in \mathbb{N}$ such that $\mathbb{N} \models n\ \mathbf{q}^{\mathrm{P}}\big(\ \Rightarrow \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))\big)$. Since $0\ \mathbf{q}^{\mathrm{P}}\top$, then $\mathbb{N} \models \varphi_{\pi_1(n)}(0)\ \mathbf{q}^{\mathrm{P}}\forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$, hence $\mathbb{N} \models \mathcal{P}(\varphi_{\pi_1(n)}(0))$ and $\mathbb{N} \models \forall\mathbf{x}\big(\varphi_{\pi_1\varphi_{\pi_1(n)}(0)}(0, \mathbf{x})\ \mathbf{q}^{\mathrm{P}}\exists y A(\mathbf{x}, y)\big)$. Put $m = \pi_1\varphi_{\pi_1(n)}(0)$ and define f by $f(\mathbf{x}) = \pi_1\varphi_m(0, \mathbf{x})$. Then $\mathbb{N} \models \forall\mathbf{x}\big(\pi_2\varphi_m(0, \mathbf{x})\ \mathbf{q}^{\mathrm{P}} A(\mathbf{x}, \pi_1\varphi_m(0, \mathbf{x}))\big)$, and hence $\mathbb{N} \models \forall\mathbf{x} A(\mathbf{x}, f(\mathbf{x}))$. By $\mathbb{N} \models \mathcal{P}(\varphi_{\pi_1(n)}(0))$ and $m = \pi_1\varphi_{\pi_1(n)}(0)$, f is polynomially bounded primitive recursive. □

And finally our main theorem is a characterization of provably total functions of **BA** (cf. Corollary 4.5 of [13]).

Corollary 3.7 *Let $A(\mathbf{x}, y)$ be a formula with the free variables $\mathbf{x}, y$. If $\mathbf{BA} \vdash\!\Rightarrow \exists y A(\mathbf{x}, y)$ or $\mathbf{BA} \vdash\!\Rightarrow \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$, then $\mathbb{N} \models \forall\mathbf{x}(\mathbf{x}, f(\mathbf{x}))$ for a polynomially bounded primitive recursive function f.*

Proof From $\mathbf{BA} \vdash\!\Rightarrow \exists y A(\mathbf{x}, y)$ or $\mathbf{BA} \vdash\!\Rightarrow \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$, by Corollary 2.3, it follows that $\mathbf{BA}^{\mathbf{w}} \vdash\!\Rightarrow \top \to \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$. Then by Theorem 3.5, there is a natural k such that $\mathbb{N} \models k\ \mathbf{q}^{\mathrm{P}}\big(\top \to \forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))\big)$ which implies that $\mathbb{N} \models \varphi_{\pi_1(k)}(0)\ \mathbf{q}^{\mathrm{P}}\forall\mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$. By putting $n = \varphi_{\pi_1(k)}(0)$ and mimicking the lines of the proof of Lemma 3.6, the existence of a polynomially bounded recursive function f such that $\mathbb{N} \models \forall\mathbf{x} A(\mathbf{x}, f(\mathbf{x}))$ follows. □

4 Polynomially Bounded Church's Thesis

The arithmetical form of Church's Thesis,

CT_0 $\qquad \forall x \exists y A(x, y) \to \exists k \forall x \exists z[\mathbf{T}(k, x, z) \wedge A(x, \mathbf{U}(z))]$,

is known to be recursively realizable in Heyting Arithmetic **HA** (see, for example, [15]). In this section, we introduce a polynomially bounded counterpart of the arithmetical schema of Church's Thesis and prove it to be P-realizable.

Definition 4.1 Let CT^{P} be the schema

$$\forall x(\top \to \exists y A(x, y)) \to \exists u\big(\mathcal{P}(u) \wedge \forall x(\top \to \exists z[\mathbf{T}(\pi_1(u), x, z) \wedge A(x, \mathbf{U}(z))])\big).$$

Theorem 4.2 *All instances of the schema $\Rightarrow \mathrm{CT}^{\mathrm{P}}$ are P-realizable in $\mathbb{N}$.*

Proof Let $A(x, y)$ be a formula with the free variables x, y. We define a P-function f such that for all n, if $n\ \mathbf{r}^{\mathrm{P}}\forall x(\top \to \exists y A(x, y))$ then

$(\star)$ $\qquad f(n)\ \mathbf{r}^{\mathrm{P}}\exists u\big(\mathcal{P}(u) \wedge \forall x(\top \to \exists z[\mathbf{T}(\pi_1(u), x, z) \wedge A(x, \mathbf{U}(z))])\big)$.

Let k_1 and k_2 be unary P-functions satisfying $\varphi_{k_1(n)}(x) = \pi_1\varphi_{\pi_1(n)}(0,x)$ and $k_2(n) = \pi_2(n)$. Define the recursive functions $\jmath$ and ι by

$$\jmath(n,x,w) = \pi_2\varphi_{\pi_1(n)}(0,x) \text{ and } \iota(n,x) = \mu t\,(\mathbf{T}(k_1(n),x,t)),$$

where μ is the minimization operation. That is to say, $\iota(n,x)$ is the minimum t such that $\mathbf{T}(k_1(n),x,t)$ holds, if such a t exists (if there is no such a t for some n,x, then $\iota(n,x)$ is not defined).

Let g and h be some P-functions satisfying

$$\varphi_{g(n)}(w,x) = \langle \iota(n,x), \langle 0, \jmath(n,w,x)\rangle\rangle \text{ and } \varphi_{h(n)}(w,x) = \langle \iota(n,x), \langle 0,0\rangle\rangle,$$

and define f by $f(n) = \langle\langle k_1(n), k_2(n)\rangle, \langle h(n), g(n)\rangle\rangle$. Note that f is a polynomially bounded recursive function.

Suppose $n\,\mathbf{r}^{\mathrm{P}}\forall x(\top \to \exists y A(x,y))$. We show that $(\star)$ holds. For simplicity let $n_1 = \pi_1(n)$ and $\pi_2(n) = n_2$, so $n = \langle n_1, n_2\rangle$, and $\varphi_{n_1}(x) \le x^{n_2} + n_2$ and $\pi_2\varphi_{n_1}(w,x)\,\mathbf{r}^{\mathrm{P}}A(x,\pi_1\varphi_{n_1}(w,x))$ hold for every w,x. The statement $(\star)$ is equivalent to the two statements,

(1) $h(n)\,\mathbf{r}^{\mathrm{P}}\mathcal{P}(\langle k_1(n), k_2(n)\rangle)$, and
(2) $g(n)\,\mathbf{r}^{\mathrm{P}}\forall x(\top \to \exists z[\mathbf{T}(k_1(n),x,z) \wedge A(x,\mathbf{U}(z))])$,

which in turn are equivalent to

(1-1) $\pi_1\pi_2\varphi_{h(n)}(w,x)\,\mathbf{r}^{\mathrm{P}}\mathbf{T}(k_1(n),x,\pi_1\varphi_{h(n)}(w,x))$,
(1-2) $\pi_2\pi_2\varphi_{h(n)}(w,x)\,\mathbf{r}^{\mathrm{P}}\mathbf{U}\pi_1\varphi_{h(n)}(w,x) \le x^{k_2(n)} + k_2(n)$,
(2-1) $\pi_1\pi_2\varphi_{g(n)}(w,x)\,\mathbf{r}^{\mathrm{P}}\mathbf{T}(k_1(n),x,\pi_1\varphi_{g(n)}(w,x))$, and
(2-2) $\pi_2\pi_2\varphi_{g(n)}(w,x)\,\mathbf{r}^{\mathrm{P}}A(x,\mathbf{U}\pi_1\varphi_{g(n)}(w,x))$.

Since $\varphi_{k_1(n)}$ is a P-function, then the function $x \mapsto \iota(n,x)$ is total. Moreover, $\mathbf{T}(k_1(n),x,\iota(n,x))$ holds and $\mathbf{U}\iota(n,x) = \varphi_{k_1(n)}(w,x) = \pi_1\varphi_{n_1}(0,x)$.

Let us recall that

$$\pi_1\pi_2\varphi_{h(n)}(w,x) = \pi_1\pi_2\varphi_{g(n)}(w,x) = 0, \text{ and}$$
$$\pi_1\varphi_{h(n)}(w,x) = \pi_1\varphi_{g(n)}(w,x) = \iota(n,x).$$

Hence (1-1) and (2-1) hold by $\mathbf{T}(k_1(n),x,\iota(n,x))$. For (1-2) we note that by $\varphi_{n_1}(z) \le z^{n_2} + n_2$, $\mathbf{U}\pi_1\varphi_{h(n)}(w,x) = \pi_1\varphi_{n_1}(0,x) \le x^{n_2} + n_2$. Finally, (2-2) follows from the identities $\pi_2\pi_2\varphi_{g(n)}(w,x) = \pi_2\varphi_{n_1}(0,x)$ and $\mathbf{U}\pi_1\varphi_{g(n)}(w,x) = \mathbf{U}\iota(n,x) = \pi_1\varphi_{n_1}(0,x)$, and the instance of the assumption $\pi_2\varphi_{n_1}(w,x)\,\mathbf{r}^{\mathrm{P}}A(x,\pi_1\varphi_{n_1}(w,x))$ for $w = 0$. □

Since by Theorem 3.3, all theorems of $\mathbf{BA}^{\mathbf{w}}$ are P-realizable and the contradiction $\top \Rightarrow \bot$ is not P-realizable, then $\Rightarrow \mathrm{CT}^{\mathrm{P}}$ is consistent with $\mathbf{BA}^{\mathbf{w}}$. We show that it is consistent with **BA** too.

Theorem 4.3 *The schema* $\Rightarrow \mathrm{CT}^{\mathrm{P}}$ *is consistent with* **BA**.

Proof Assume not. So there are formulas $A_1(x,y),\ldots,A_n(x,y)$ such that the instances of CT^{P} for those formulas lead to contradiction with **BA**. Denote the instance of CT^{P} for the formula $B(x,y)$ by $\mathrm{CT}^{\mathrm{P}}_B$. So,

$$\mathbf{BA} + \{\Rightarrow \mathrm{CT}^{\mathrm{P}}_{A_1},\ldots,\Rightarrow \mathrm{CT}^{\mathrm{P}}_{A_n}\} \vdash \top \Rightarrow \bot.$$

By Proposition 6.1 of [12] and an argument similar to that of the Proof of Theorem 2.2, it follows that

$$\mathbf{BA}^{\mathbf{w}} \vdash (\top \to \mathrm{CT}^{\mathrm{P}}_{A_1}) \wedge \cdots \wedge (\top \to \mathrm{CT}^{\mathrm{P}}_{A_n}) \Rightarrow (\top \to \bot).$$

Since $\mathrm{CT}^{\mathrm{P}}_{A_i}$ is P-realizable by Theorem 4.2, then so is $\top \to \mathrm{CT}^{\mathrm{P}}_{A_i}$. Hence $\mathbf{BA^w} + (\top \to \mathrm{CT}^{\mathrm{P}}_{A_1}) \wedge \cdots \wedge (\top \to \mathrm{CT}^{\mathrm{P}}_{A_n})$ is P-realizable, whereas obviously $\top \to \bot$ is not. Contradiction. □

The arithmetical form of Church's Thesis CT_0 is consistent with **HA** whereas it is inconsistent with Peano Arithmetic **PA**. Likewise, the polynomially bounded counterpart of Church's Thesis CT^{P} is consistent with **BA**, whereas it can be easily shown to be inconsistent with **HA** and **PA**, noting that the exponential function $f(x) = 2^x$ is provably total in **HA** and **PA**.

5 Conclusions

The next task to be done in the research line of the paper is investigating whether or not every polynomially bounded primitive recursive function is provably total in **BA**. In the affirmative case, **BA** will be the first arithmetical theory with full induction (having an induction axiom and rule for all formulas) which captures the polynomially bounded recursive functions. Some bounded arithmetics (based on classical or intuitionistic logic) are known to have the polynomially bounded recursive functions as their provably total (or provably recursive) functions, though the induction axiom/rule in those theories are restricted to a certain class of formulas.

Note

1. In the case that for a natural n there is no program with the code n, take φ_n to be the zero constant function.

References

[1] Damnjanovic, Z., "Strictly primitive recursive realizability. I," *The Journal of Symbolic Logic*, vol. 59 (1994), pp. 1210–27. Zbl 0816.03029. MR 1312305. 407

[2] Damnjanovic, Z., "Minimal realizability of intuitionistic arithmetic and elementary analysis," *The Journal of Symbolic Logic*, vol. 60 (1995), pp. 1208–41. Zbl 0854.03054. MR 1367206. 407

[3] Damnjanovic, Z., "Elementary realizability," *Journal of Philosophical Logic*, vol. 26 (1997), pp. 311–39. Zbl 0874.03067. MR 1456614. 407, 408

[4] Damnjanovic, Z., "Strictly primitive recursive realizability. II. Completeness with respect to iterated reflection and a primitive recursive Ω-rule," *Notre Dame Journal of Formal Logic*, vol. 39 (1998), pp. 363–88. Zbl 0971.03060. MR 1741544. 407

[5] Hájek, P., and P. Pudlák, *Metamathematics of First-order Arithmetic*, Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1998. Zbl 0889.03053. MR 1748522. 410, 411

[6] Jones, N. D., "Computer implementation and applications of Kleene's *S-m-n* and recursion theorems," pp. 243–63 in *Logic from Computer Science (Berkeley CA, 1989)*, vol. 21 of *Mathematical Sciences Research Institute Publications*, Springer, New York, 1992. Zbl 0754.03034. 411

[7] López-Escobar, E. G. K., "Elementary interpretations of negationless arithmetic," *Fundamenta Mathematicae*, vol. 82 (1974/75), pp. 25–38. Zbl 0307.02022. MR 0360223. 407

[8] Park, B. H., "Minimal realizability and predicate logic," Manuscript at VINITI (Russian) 1896-B2002, 2002. 408

[9] Park, B. H., "Strictly primitive recursive realizability and predicate logic," Manuscript at VINITI (Russian) 218-B2003, 2003. 408

[10] Park, B. H., *Subrecursive Realizability and Predicate Logi*, Ph.D. thesis, Moscow State University, 2003. 408

[11] Plisko, V., "Arithmetic complexity of the predicate logics of certain complete arithmetic theories," *Annals of Pure and Applied Logic*, vol. 113 (2002), pp. 243–59. First St. Petersburg Conference on Days of Logic and Computability (1999). Zbl 0992.03074. MR 1875746. 407

[12] Ruitenburg, W., "Basic predicate calculus," *Notre Dame Journal of Formal Logic*, vol. 39 (1998), pp. 18–46. Zbl 0967.03005. MR 1671797. 408, 409, 410, 415

[13] Salehi, S., "Provably total functions of Basic Arithmetic," *Mathematical Logic Quarterly*, vol. 49 (2003), pp. 316–22. Zbl 1026.03045. MR 1979138. 407, 408, 411, 412, 413, 414

[14] Soare, R. I., *Recursively Enumerable Sets and Degrees. A Study of Computable Functions and Computably Generated Sets*, Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1987. Zbl 0995.03031. MR 882921. 411

[15] Troelstra, A. S., and D. van Dalen, *Constructivism in Mathematics. Vol. I. An Introduction*, vol. 121 of *Studies in Logic and the Foundations of Mathematics*, North-Holland Publishing Co., Amsterdam, 1988. Zbl 0653.03040. MR 966421. 407, 411, 414

[16] Viter, D. A., "Base logic and primitive recursive realizability," pp. 90–102 in *Logical Investigations, No. 9 (Russian)*, Nauka, Moscow, 2002. Zbl 1036.03007. MR 1981315. 408

[17] Viter, D., "Primitive recursive realizability and predicate logic," Manuscript at VINITI (Russian), N. 1830, 2001. 408

[18] Viter, D., "Basic logic and primitive-recursive realizability," *Logical Studies*, vol. 8 (2002). Online Journal (Russian) http://www.logic.ru/LogStud/08/No8-02.html. 408

[19] Viter, D., *Primitive Recursive Realizability and Constructive Theory of Models*, Ph.D. thesis, Moscow State University, 2002. 408

[20] Wilkie, A. J., and J. B. Paris, "On the scheme of induction for bounded arithmetic formulas," *Annals of Pure and Applied Logic*, vol. 35 (1987), pp. 261–302. Zbl 0647.03046. MR 904326. 411

[21] Willard, D. E., "How to extend the semantic tableaux and cut-free versions of the second incompleteness theorem almost to Robinson's Arithmetic Q," *The Journal of Symbolic Logic*, vol. 67 (2002), pp. 465–96. Zbl 1004.03050. MR 1889562. 410

Turku Center for Computer Science
Lemminkäisenkatu 14 A
FIN-20520 Turku
FINLAND
saeed@cs.utu.fi