Notre Dame Journal of Formal Logic
Volume 60, Number 3, 2019

A Counterexample to Polynomially Bounded Realizability of Basic Arithmetic

Mohammad Ardeshir, Erfan Khaniki, and Mohsen Shahriari

Abstract We give a counterexample to the claim that every provably total function of Basic Arithmetic is a polynomially bounded primitive recursive function.

1 Introduction

We give a counterexample (Corollary 3.7) to the main result of Salehi [4, Corollary 3.7] which states that for a formula $A(\mathbf{x}, y)$ with the free variables $\mathbf{x}, y$, if Basic Arithmetic (**BA**) $\vdash\Rightarrow \exists y A(\mathbf{x}, y)$ or **BA** $\vdash\Rightarrow \forall \mathbf{x}(\top \to \exists y A(\mathbf{x}, y))$, then $\mathbb{N} \models \forall \mathbf{x} A(\mathbf{x}, f(\mathbf{x}))$, for a polynomially bounded primitive recursive function f.

As Salehi explains in [4], the above result is a sharpening of his previous result in [3], in which it is proved that every provably total function of **BA** is a primitive recursive function. Following [3], the notion of "polynomially bounded realizability," indicated by $\mathcal{P}$-realizability, is applied in [4] to obtain the above result. This notion of realizability is defined in Definition 3.8 of this article.

In this article, we give an explicit formula in the language of **BA** that *isn't* $\mathcal{P}$-realizable. Moreover, it shows that the induction axiom schema *isn't* $\mathcal{P}$-realizable, and hence the claim of soundness of the *weakened basic arithmetic* ($\mathbf{BA}^w$) with respect to $\mathcal{P}$-realizability (see [4, Theorem 3.3]) is wrong. The theory $\mathbf{BA}^w$ is defined in [4] to be the sequent theory axiomatized by all axioms and rules of **BA**, except the induction rule (rule 8 in 2.2).

2 Preliminaries to Basic Arithmetic

Basic Arithmetic is introduced by Ruitenburg in [2]. Basic Arithmetic is an arithmetical theory based on Basic Logic, as Heyting Arithmetic and Peano Arithmetic

Received March 16, 2016; accepted November 6, 2017
First published online July 4, 2019
2010 Mathematics Subject Classification: Primary 03F30; Secondary 03F50
Keywords: basic arithmetic, primitive recursive realizability, polynomially bounded realizability
 10.1215/00294527-2019-0013

are based on Intuitionistic Logic and Classical Logic, respectively. For motivations and basic properties of **BA**, see [2], Ardeshir [1], and [3].

2.1 Axioms and rules of Basic Predicate Calculus The language of Basic Predicate Calculus (**BQC**) is the same as of Intuitionistic Predicate Calculus (**IQC**). It was originally axiomatized in sequent notation, that is, using sequents like $A \Rightarrow B$, where A and B are formulas in the language $\{\vee, \wedge, \rightarrow, \bot, \top, \exists, \forall\}$ (see [2]). Since modus ponens is *not* a rule in **BQC**, a universally quantified formula like $\forall x \forall y\, A$ is different from $\forall xy\, A$. In **BQC**, when we write $\forall \mathbf{x}\,(A \rightarrow B)$, we mean $\mathbf{x}$ to be a finite sequence of variables *once* quantified. Besides a set of predicate and function symbols of possibly different finite arity, we also include the binary predicate "$=$" for equality. Terms, atomic formulas, and formulas are defined as usual except for universal quantification: if A and B are formulas, and $\mathbf{x}$ is a finite sequence of variables, then $\forall \mathbf{x}\,(A \rightarrow B)$ is a formula. The concepts of free and bound variables are defined as usual. A *sentence* is a formula with no free variable. An *implication* is a universal quantification $\forall \mathbf{x}\,(A \rightarrow B)$, where $\mathbf{x}$ is the empty sequence. Further, $\neg A$ means $A \rightarrow \bot$. Given a sequence of variables $\mathbf{x}$ without repetitions, $s[\mathbf{x}/\mathbf{t}]$ and $A[\mathbf{x}/\mathbf{t}]$ stand for, respectively, the term and formula that results from substituting the term $\mathbf{t}$ for all free occurrences of the variables of $\mathbf{x}$ in the term s and the formula A. For details, see [2] and Ardeshir [1]. We often write A for $\top \Rightarrow A$.

Axioms and rules of **BQC** In the following list, the use of a double horizontal line in a rule means that the rule is reversible.

1. $A \Rightarrow A$,
2. $A \Rightarrow \top$,
3. $\bot \Rightarrow A$,
4. $A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)$,
5. $A \wedge \exists x\, B \Rightarrow \exists\, x(A \wedge B)$, where x is not free in A,
6. $\top \Rightarrow x = x$,
7. $x = y \wedge A \Rightarrow A[x/y]$, where A is atomic,
8. $\forall \mathbf{x}\,(A \rightarrow B) \wedge \forall \mathbf{x}\,(B \rightarrow C) \Rightarrow \forall \mathbf{x}\,(A \rightarrow C)$,
9. $\forall \mathbf{x}\,(A \rightarrow B) \wedge \forall \mathbf{x}\,(A \rightarrow C) \Rightarrow \forall \mathbf{x}\,(A \rightarrow B \wedge C)$,
10. $\forall \mathbf{x}\,(B \rightarrow A) \wedge \forall \mathbf{x}\,(C \rightarrow A) \Rightarrow \forall \mathbf{x}\,(B \vee C \rightarrow A)$,
11. $\forall \mathbf{x}\,(A \rightarrow B) \Rightarrow \forall \mathbf{x}\,(A[\mathbf{x}/\mathbf{t}] \rightarrow B[\mathbf{x}/\mathbf{t}])$, where no variable in the sequence of terms $\mathbf{t}$ is bound by a quantifier of A or B,
12. $\forall \mathbf{x}\,(A \rightarrow B) \Rightarrow \forall \mathbf{y}\,(A \rightarrow B)$, where no variable in $\mathbf{y}$ is free on the left-hand side,
13. $\forall \mathbf{y}x\,(B \rightarrow A) \Rightarrow \forall \mathbf{y}\,(\exists x\, B \rightarrow A)$, where x is not free in A,
14. $\dfrac{A \Rightarrow B \qquad B \Rightarrow C}{A \Rightarrow C}$,
15. $\dfrac{A \Rightarrow B \qquad A \Rightarrow C}{A \Rightarrow B \wedge C}$ (double line),
16. $\dfrac{B \Rightarrow A \qquad C \Rightarrow A}{B \vee C \Rightarrow A}$ (double line),
17. $\dfrac{A \Rightarrow B}{A[\mathbf{x}/\mathbf{t}] \Rightarrow B[\mathbf{x}/\mathbf{t}]}$, where no variable in the sequence of terms $\mathbf{t}$ is bound by a quantifier in the denominator,
18. $\dfrac{B \Rightarrow A}{\exists x\, B \Rightarrow A}$ (double line), where x is not free in A,

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

2.2 Axioms and rules of BA The nonlogical language $\mathcal{L}$ of **BA** is $\{0, S, +, \cdot\}$, where 0 is a constant symbol, S is a unary function symbol for successor, and $+$ and $\cdot$ are binary function symbols for addition and multiplication, respectively. Note that in the following list of axioms and rules, beside the *Rule of Induction* (8), we also have the *Induction Axiom Schema* (7).

1. $Sx = 0 \Rightarrow \bot$,
2. $Sx = Sy \Rightarrow x = y$,
3. $x + 0 = x$,
4. $x + Sy = S(x + y)$,
5. $x \cdot 0 = 0$,
6. $x \cdot Sy = x \cdot y + x$,
7. $\forall \mathbf{y}x\,(A \to A[x/Sx]) \Rightarrow \forall \mathbf{y}x\,(A[x/0] \to A)$,
8. $\dfrac{A \Rightarrow A[x/Sx]}{A[x/0] \Rightarrow A}$.

2.3 Some properties of BA In this section, we collect some elementary properties of **BA** that we may need later in this article.

Lemma 2.1 *The following rules are derivable in* **BQC***:*

1. $\dfrac{A \Rightarrow B}{C \vee A \Rightarrow C \vee B}$,
2. $\dfrac{A \Rightarrow B \qquad \top \Rightarrow C}{A \Rightarrow B \wedge C}$,
3. $\dfrac{A \Rightarrow B \qquad C \Rightarrow D}{A \wedge C \Rightarrow B \wedge D}$,
4. $\dfrac{\exists x A(x) \Rightarrow B}{\exists y A(y) \Rightarrow B}$, *where y is not bound by any quantifier in $A(y)$ and y is not free in B.*

Proof All items are easy. We show the last one by the following tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x A(x) \Rightarrow \exists x A(x)}}{A(x) \Rightarrow \exists x A(x)}}{A(y) \Rightarrow \exists x A(x)}}{\exists y A(y) \Rightarrow \exists x A(x)} \qquad \exists x A(x) \Rightarrow B}{\exists y A(y) \Rightarrow B}$$

□

Definition 2.2

1. $x < y \equiv \exists z(x + Sz = y)$,
2. $x \leq y \equiv x < y \vee x = y$,
3. $x \mid y \equiv \exists z(x \cdot z = y)$.

Lemma 2.3 *The following are derivable in* **BA***:*

1. $(x + y) + z = x + (y + z)$,
2. $x + y = y + x$,
3. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
4. $x \cdot y = y \cdot x$,
5. $x \cdot (y + z) = x \cdot y + x \cdot z$,

6. $x > 0 \Rightarrow \exists y(x = Sy)$,
7. $x < 0 \Rightarrow \bot$,
8. $x \geq 0$,
9. $x > 0 \Rightarrow x + y > 0$,
10. $x + y = 0 \Rightarrow x = 0 \wedge y = 0$,
11. $x < Sy \Rightarrow x = y \vee x < y$,
12. $x < n \Rightarrow x = 0 \vee x = 1 \vee \cdots \vee x = n - 1$,
13. $x > 0 \wedge y > 0 \Rightarrow x \cdot y > 0$,
14. $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$,
15. $x < y \Rightarrow Sx < Sy$,
16. $y < x \Rightarrow x = Sy \vee Sy < x$,
17. $x > y \Rightarrow x + z > y + z$,
18. $x > y \wedge z > 0 \Rightarrow x \cdot z > y \cdot z$,
19. $x + y = 1 \Rightarrow x = 0 \vee y = 0$,
20. $x \cdot y = 1 \Rightarrow x = 1 \wedge y = 1$.

Proof See [1, Lemma 2.5]. □

Definition 2.4 Let $\mathbf{BA}^Q$ be a subtheory of **BA** including:

1. All axioms and rules of **BQC**,
2. All axioms and rules of **BA**, except the induction axiom (7) and rule (8),
3. All sequents listed in Lemma 2.3.

Lemma 2.5 *For terms s, t, and u,*

1. $\mathbf{BA}^Q \vdash s = t \Rightarrow t = s$,
2. $\mathbf{BA}^Q \vdash s = t \wedge t = u \Rightarrow s = u$,
3. $\mathbf{BA}^Q \vdash s = t \Rightarrow u[x/s] = u[x/t]$.

Proof All items are easily proved. The last one can be proved by induction on u. □

Lemma 2.6 $\mathbf{BA}^Q \vdash x = y \Rightarrow x \mid y \cdot z$.

Proof We have the following sequence of derivations in $\mathbf{BA}^Q$:

1. $x = y \Rightarrow x \cdot z = y \cdot z$, by Lemma 2.5(3),
2. $x = y \Rightarrow \exists w(x \cdot w = y \cdot z)$, by axiom 1 and rules 14, 17, and 18. □

Lemma 2.7 $\mathbf{BA}^Q \vdash x \mid y \Rightarrow x \mid z \cdot y$.

Proof We have the following sequence of derivations in $\mathbf{BA}^Q$:

1. $x \cdot w = y \Rightarrow z \cdot (x \cdot w) = z \cdot y$, by Lemma 2.5(3),
2. $x \cdot w = y \Rightarrow (z \cdot x) \cdot w = z \cdot y$, by Lemmas 2.3(3), 2.1(2), 2.5(2), and rule 14,
3. $x \cdot w = y \Rightarrow (x \cdot z) \cdot w = z \cdot y$, by Lemmas 2.3(4), 2.5, 2.1(2), 2.5(2), and rule 14,
4. $x \cdot w = y \Rightarrow x \cdot (z \cdot w) = z \cdot y$, by Lemmas 2.3(3), 2.1(2), 2.5(1 and 2), and rule 14,
5. $x \cdot w = y \Rightarrow \exists u(x \cdot u = z \cdot y)$, by axiom 1 and rules 18, 17, and 14,
6. $\exists w(x \cdot w = y) \Rightarrow \exists u(x \cdot u = z \cdot y)$, by rule 18. □

3 A Counterexample

Let us define the following formula that is our main concern:

$$\mathcal{E}(x, y) \equiv y > 0 \wedge \forall z(z \leq x \rightarrow z = 0 \vee z \mid y).$$

We note that for $m, n \in \mathbb{N}$ and $m, n \geq 1$ that if $\mathbb{N} \models \mathcal{E}(m, n)$, then the least common multiple (LCM) of $1, 2, \ldots, m$ divides n. We indicate this by $\operatorname{lcm}\{1, 2, \ldots, m\} \mid n$.

We need a well known classical fact in number theory called *the prime number theorem*. Let $\pi(x)$ indicate the number of prime numbers less than or equal to natural number $x > 1$.

Theorem 3.1 (Prime number theorem) $\lim_{x\rightarrow\infty} \pi(x) \cdot \frac{\ln x}{x} = 1$.

Proof See, for example, Zagier [5]. □

Corollary 3.2 *For large enough natural number m, we have* $\operatorname{lcm}\{1, \ldots, m\} \geq 2^{\frac{m}{2 \ln m}}$.

Proof By Theorem 3.1, there exists $n_0 \in \mathbb{N}$ such that for any $m > n_0$, $|\pi(x) \cdot \frac{\ln x}{x} - 1| < 0.5$. Then for any $m > n_0$, $\frac{0.5m}{\ln m} < \pi(m) < \frac{1.5m}{\ln m}$. This implies that for any $m > n_0$,

$$\operatorname{lcm}\{1, \ldots, m\} \geq \prod_{i=1}^{\pi(m)} p_i \geq \prod_{i=1}^{\pi(m)} 2 = 2^{\pi(m)} \geq 2^{\frac{m}{2 \ln m}}.$$

□

Now we want to show that the formula $\exists y \mathcal{E}(x, y)$ is derivable in **BA**.

Lemma 3.3 $\mathbf{BA}^{\mathcal{Q}} \vdash \mathcal{E}(x, y) \Rightarrow \mathcal{E}(Sx, Sx \cdot y)$.

Proof We have the following sequence of derivations in $\mathbf{BA}^{\mathcal{Q}}$:

1. $\forall z(z = 0 \vee z \mid y \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by Lemmas 2.7, 2.1, and rule 19,
2. $\forall z(z \leq x \rightarrow z = 0 \vee z \mid y) \Rightarrow \forall z(z \leq x \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by axioms 1 and 6, Lemma 2.1(2), and rule 14,
3. $\forall z(z \leq x \rightarrow z = 0 \vee z \mid y) \Rightarrow \forall z(z < Sx \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by Lemmas 2.3(11) and 2.1(2), rules 19 and 14, and axiom 6,
4. $\forall z(z = Sx \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by axiom 1, rules 16, 14, and 19, and Lemma 2.6,
5. $\forall z(z \leq x \rightarrow z = 0 \vee z \mid y) \Rightarrow \forall z(z \leq Sx \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by Lemma 2.1(2), axiom 6, and rule 14,
6. $y > 0 \Rightarrow Sx \cdot y > 0$, by Lemmas 2.1(2) and 2.3(13), rules 17 and 14, and the fact that $\mathbf{BA}^{\mathcal{Q}} \vdash Sx > 0$. The following proof tree justifies this fact:

$$\dfrac{\dfrac{\dfrac{}{x \geq 0}}{Sx \geq 0} \qquad \dfrac{\dfrac{\dfrac{}{Sx = 0 \Rightarrow \bot} \qquad \dfrac{}{\bot \Rightarrow Sx > 0}}{Sx = 0 \Rightarrow Sx > 0} \qquad \dfrac{}{Sx > 0 \Rightarrow Sx > 0}}{Sx \geq 0 \Rightarrow Sx > 0}}{Sx > 0}$$

7. $y > 0 \wedge \forall z(z \leq x \rightarrow z = 0 \vee z \mid y) \Rightarrow Sx \cdot y > 0 \wedge \forall z(z \leq Sx \rightarrow z = 0 \vee z \mid Sx \cdot y)$, by Lemma 2.1(3). □

Lemma 3.4 $\mathbf{BA}^{\mathcal{Q}} \vdash \exists y \mathcal{E}(x, y) \Rightarrow \exists y \mathcal{E}(Sx, y)$.

Proof We have the following proof tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{E}(x,w)\Rightarrow\mathcal{E}(Sx,Sx\cdot w)}\qquad \dfrac{\dfrac{\dfrac{}{\exists y\mathcal{E}(Sx,y)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\mathcal{E}(Sx,y)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\mathcal{E}(Sx,Sx\cdot w)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\mathcal{E}(x,w)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\exists w\mathcal{E}(x,w)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\exists y\mathcal{E}(x,y)\Rightarrow\exists y\mathcal{E}(Sx,y)}$$

□

Lemma 3.5 $\mathbf{BA}^{Q}\vdash\mathcal{E}(0,1)$.

Proof We have the following proof tree:

$$\dfrac{\dfrac{}{1>0}\qquad \dfrac{\dfrac{\dfrac{\dfrac{}{z<0\Rightarrow\bot}\qquad\dfrac{}{\bot\Rightarrow z=0\vee z\mid 1}}{z<0\Rightarrow z=0\vee z\mid 1}\qquad \dfrac{\dfrac{}{z=0\vee z\mid 1\Rightarrow z=0\vee z\mid 1}}{z=0\Rightarrow z=0\vee z\mid 1}}{z\leq 0\Rightarrow z=0\vee z\mid 1}}{\forall z(z\leq 0\rightarrow z=0\vee z\mid 1)}}{1>0\wedge\forall z(z\leq 0\rightarrow z=0\vee z\mid 1)}$$

□

Theorem 3.6 $\mathbf{BA}\vdash\exists y\mathcal{E}(x,y)$.

Proof We have the following proof tree:

$$\dfrac{\dfrac{\dfrac{}{\mathcal{E}(0,1)}\qquad \dfrac{\dfrac{\dfrac{}{\exists y\mathcal{E}(0,y)\Rightarrow\exists y\mathcal{E}(0,y)}}{\mathcal{E}(0,y)\Rightarrow\exists y\mathcal{E}(0,y)}}{\mathcal{E}(0,1)\Rightarrow\exists y\mathcal{E}(0,y)}}{\exists y\mathcal{E}(0,y)}\qquad \dfrac{\dfrac{}{\exists y\mathcal{E}(x,y)\Rightarrow\exists y\mathcal{E}(Sx,y)}}{\exists y\mathcal{E}(0,y)\Rightarrow\exists y\mathcal{E}(x,y)}}{\exists y\mathcal{E}(x,y)}$$

□

Corollary 3.7 *There is a formula $\mathcal{E}(x,y)$ with presented free variables, such that $\mathbf{BA}\vdash\exists y\mathcal{E}(x,y)$ (and thus $\mathbf{BA}\vdash\forall x(\top\rightarrow\exists y\mathcal{E}(x,y))$), but there is no polynomially bounded function f with $\mathbb{N}\models\forall x\mathcal{E}(x,f(x))$.*

Proof Combine Theorem 3.6 and Corollary 3.2. □

Corollary 3.7 provides a counterexample to [4, Corollary 3.7]. In the rest of the article, we want to show that [4, Corollary 3.7] is wrong because it is based on [4, Theorem 3.3]. In fact, the portion of [4] that makes the other results incorrect is the proof of Theorem 3.3, where it is claimed that the induction axiom (Ax20) is realizable. There, the function f may not be a P-function. That is repeated as the argument to prove Theorem 3.5 as well.

In [4], the author defines $\mathbf{q}^{P}$-realizability by the usual changes of the $\mathbf{r}^{P}$-realizability. By using this notion of realizability, the main result (Corollary 3.7) is stated. In the following definition, π_1 and π_2 are the projection functions, that is, $\pi_1(\langle m,n\rangle)=m$ and $\pi_2(\langle m,n\rangle)=n$, where $\langle,\rangle$ is a fixed pairing function such as $\langle m,n\rangle=\frac{1}{2}(m+n)(m+n+1)+n$. Moreover, φ_n is the unique unary recursive function whose program has code n. For a sequence $\mathbf{x}=(x_1,\ldots,x_m)$, the expression $\varphi_n(\mathbf{x})$ means $\varphi_n(\langle x_1,\langle x_2,\ldots,\langle x_{m-1},x_m\rangle\rangle\rangle)$. If the formula $\mathcal{P}(x)$ is true, then $\forall z(\varphi_{\pi_1(x)}(z)\leq z^{\pi_2(x)}+\pi_2(x))$ holds. This is what is meant by *polynomially bounded*. For more details, see [4].

Definition 3.8 (Polynomially bounded realizability) Now $x\ \mathbf{q}^P A$ is defined by induction on the complexity of A:

- $x\ \mathbf{q}^P A \equiv A$, for atomic A, $\top$, and $\bot$.
- $x\ \mathbf{q}^P B \wedge C \equiv (\pi_1(x)\mathbf{q}^P B) \wedge (\pi_2(x)\mathbf{q}^P C)$.
- $x\ \mathbf{q}^P B \vee C \equiv (\pi_1(x) = 0 \wedge \pi_2(x)\ \mathbf{q}^P B) \vee (\pi_1(x) \neq 0 \wedge \pi_2(x)\ \mathbf{q}^P C)$.
- $x\ \mathbf{q}^P\ \exists y B(y) \equiv \pi_2(x)\ \mathbf{q}^P B(\pi_1(x))$.
- $x\mathbf{q}^P \forall \mathbf{z}(B(\mathbf{z}) \to C(\mathbf{z})) \equiv \mathcal{P}(x) \wedge \forall y, \mathbf{z}(y\mathbf{q}^P B(\mathbf{z}) \to \varphi_{\pi_1(x)}(y, \mathbf{z})\mathbf{q}^P C(\mathbf{z})) \wedge \forall \mathbf{z}(B(\mathbf{z}) \to C(\mathbf{z}))$.

Definition 3.9 $x\ \mathbf{q}^P (B \Rightarrow C) \equiv \mathcal{P}(x) \wedge \forall y(y\ \mathbf{q}^P B \to \varphi_{\pi_1(x)}(y)\ \mathbf{q}^P C) \wedge (B \to C)$.

Theorem 3.10 *For all sequents $A \Rightarrow B$, if $\mathbf{BA}^Q \vdash A \Rightarrow B$, then for a natural number n, $\mathbb{N} \models n\ \mathbf{q}^P (A \Rightarrow B)$.*

Proof The proof is by induction on the length of the proof of the sequent. It is easy to see that sequents of Lemma 2.3 are $\mathcal{P}$-realizable. The rest of proof is like the proof of Theorem 3.5 in [4]. □

Lemma 3.11 *There exists a natural number m such that $\mathbb{N} \models m\mathbf{q}^P (\forall x(\exists y\ \mathcal{E}(x, y) \to \exists y\ \mathcal{E}(Sx, y)))$.*

Proof By Lemma 3.4, $\mathbf{BA}^Q \vdash \exists y\ \mathcal{E}(x, y) \Rightarrow \exists y\ \mathcal{E}(Sx, y)$. Then $\mathbf{BA}^Q \vdash \forall x(\exists y\ \mathcal{E}(x, y) \to \exists y\ \mathcal{E}(Sx, y))$. Theorem 3.10 implies the result. □

Lemma 3.12 *There exists a natural number k such that $\mathbb{N} \models k\mathbf{q}^P (\exists y\ \mathcal{E}(0, y))$.*

Proof By Lemma 3.5, $\mathbf{BA}^Q \vdash \exists y\ \mathcal{E}(0, y)$. Then Theorem 3.10 implies the result. □

Theorem 3.13 *The induction axiom schema $\forall x\, \mathbf{y}(A(x, \mathbf{y}) \to A(Sx, \mathbf{y})) \Rightarrow \forall x\, \mathbf{y}(A(0, \mathbf{y}) \to A(x, \mathbf{y}))$ is not $\mathcal{P}$-realizable.*

Proof We consider an instance $\mathcal{E}(x, y)$ of the induction axiom schema. Suppose that there exists a natural number n such that

$$\mathbb{N} \models n\ \mathbf{q}^P \big(\forall x\big(\exists y\ \mathcal{E}(x, y) \to \exists y\ \mathcal{E}(Sx, y)\big) \Rightarrow \forall x\big(\exists y\ \mathcal{E}(0, y) \to \exists y\ \mathcal{E}(x, y)\big)\big).$$

Then

$$\mathbb{N} \models \forall a\big(a\mathbf{q}^P \big(\forall x\big(\exists y\ \mathcal{E}(x, y) \to \exists y\ \mathcal{E}(Sx, y)\big)\big) \to \varphi_{\pi_1(n)}(a)\mathbf{q}^P \big(\forall x\big(\exists y\ \mathcal{E}(0, y) \to \exists y\ \mathcal{E}(x, y)\big)\big)\big) \wedge \mathcal{P}(n).$$

In particular,

$$\mathbb{N} \models m\mathbf{q}^P \big(\forall x\big(\exists y\ \mathcal{E}(x, y) \to \exists y\ \mathcal{E}(Sx, y)\big)\big) \to \varphi_{\pi_1(n)}(m)\mathbf{q}^P (\forall x\big(\exists y\ \mathcal{E}(0, y) \to \exists y\ \mathcal{E}(x, y)\big).$$

Then by Lemma 3.11,

$$\mathbb{N} \models \varphi_{\pi_1(n)}(m)\mathbf{q}^P \big(\forall x\big(\exists y\ \mathcal{E}(0, y) \to \exists y\ \mathcal{E}(x, y)\big)\big).$$

To simplify notations, let us assume $l = \varphi_{\pi_1(n)}(m)$. Then we have

$$\mathbb{N} \models \forall b, c\big(b\ \mathbf{q}^P \exists y\ \mathcal{E}(0, y) \to \varphi_l(b, c)\mathbf{q}^P\ \exists y\ \mathcal{E}(c, y)\big) \wedge \mathcal{P}(l).$$

By choosing the natural number k for b, we have

$$\mathbb{N} \models \forall c\big(k\ \mathbf{q}^P \exists y\ \mathcal{E}(0,y) \to \varphi_l(k,c)\mathbf{q}^P\ \exists y\ \mathcal{E}(c,y)\big) \wedge \mathcal{P}(l).$$

Then by Lemma 3.12,

$$\mathbb{N} \models \forall c\big(\varphi_l(k,c)\mathbf{q}^P\ \exists y\ \mathcal{E}(c,y)\big) \wedge \mathcal{P}(l).$$

Then

$$\mathbb{N} \models \forall c(\pi_2\varphi_l(k,c)\mathbf{q}^P\ \mathcal{E}\big(c,\pi_1\varphi_l(k,c)\big) \wedge \mathcal{P}(l).$$

Now by explanation before [4, Theorem 3.5], we have

$$\mathbb{N} \models \forall c\ \mathcal{E}\big(c,\pi_1\varphi_l(k,c)\big) \wedge \mathcal{P}(l).$$

By the definition of $\mathcal{E}(x,y)$, we can see that for all natural numbers e and r that if $\mathbb{N} \models \mathcal{E}(e,r)$, then $\mathrm{lcm}\{1,\ldots,e\} \mid r$. Then there exists a natural number i such that for all natural numbers $c > i$, $\pi_1\varphi_l(k,c) \geq \mathrm{lcm}\{1,\ldots,c\} \geq 2^{\frac{c}{2\ln c}}$. This contradicts $\mathbb{N} \models \mathcal{P}(l)$. □

The following result is in contrast with [4, Theorem 3.3].

Corollary 3.14 $\mathbf{BA}^w$ *is not sound with respect to* $\mathcal{P}$*-realizability.*

Proof See Theorems 3.13 and 3.6. □

References

[1] Ardeshir, M. and B. Hesaam, "An introduction to basic arithmetic," *Logic Journal of the IGPL*, vol. 16 (2008), pp. 1–13. Zbl 1168.03045. MR 2387433. DOI 10.1093/jigpal/jzm013. 482, 484

[2] Ruitenburg, W., "Basic predicate calculus," *Notre Dame Journal of Formal Logic*, vol. 39 (1998), pp. 18–46. Zbl 0967.03005. MR 1671797. DOI 10.1305/ndjfl/1039293019. 481, 482

[3] Salehi, S., "Provably total functions of Basic Arithmetic," *Mathematical Logic Quarterly (MLQ)*, vol. 49 (2003), pp. 316–22. Zbl 1026.03045. MR 1979138. DOI 10.1002/malq.200310032. 481, 482

[4] Salehi, S., "Polynomially bounded recursive realizability," *Notre Dame Journal of Formal Logic*, vol. 46 (2005), pp. 407–17. Zbl 1097.03051. MR 2183051. DOI 10.1305/ndjfl/1134397659. 481, 486, 487, 488

[5] Zagier, D., "Newman's short proof of the prime number theorem," *American Mathematical Monthly*, vol. 104 (1997), pp. 705–08. Zbl 0887.11039. MR 1476753. DOI 10.2307/2975232. 485

Ardeshir
Department of Mathematical Sciences
Sharif University of Technology
Tehran
Iran
mardeshir@sharif.edu

Khaniki
Department of Mathematical Sciences
Sharif University of Technology
Tehran
Iran
e.khaniki@gmail.com

Shahriari
Department of Mathematical Sciences
Sharif University of Technology
Tehran
Iran
shirik.shirik@gmail.com