Model theory of bounded arithmetic with applications to independence results

Morteza Moniri

Abstract

In this paper we apply some new and some old methods in order to construct classical and intuitionistic models for theories of bounded arithmetic. We use these models to obtain proof theoretic consequences. In particular, we construct an ω-chain of models of BASIC such that the union of its worlds satisfies S^1_2 but none of its worlds satisfies the sentence $\forall x \exists y(x = 0 \vee x = y + 1)$. Interpreting this chain as a Kripke model shows that double negation of the above mentioned sentence is not provable in the intuitionistic theory of BASIC plus polynomial induction on coNP formulas.

2000 Mathematics Subject Classification: 03F30, 03F55, 03F50, 68Q15.

Key words and phrases:

Bounded Arithmetic, Intuitionistic Logic, Polynomial Hierarchy, Polynomial Induction, NP, coNP, Kripke Model.

1 Introduction and Some Backgrounds

In this paper we are concerned with some well known classical and intuitionistic theories of bounded arithmetic such as S^1_2 and IS^1_2 (see [B1] and [B3]). The language of these theories extends the usual language of arithmetic by adding the function symbols $\lfloor \frac{x}{2} \rfloor$ ($= \frac{x}{2}$ rounded down to the nearest integer), $|x|$ (= the length of binary representation for x) and $\#$ ($x\#y = 2^{|x||y|}$). These symbols have clear computational meanings (see [B1]). We also work with a richer language introduced by Stephen Cook containing function symbols for polynomial time computable functions, and with theories such as IPV in this language (see [CU]).

This paper can be considered as a companion to our earlier works [M1] and [M2], but can be read independently. In particular, our results were not based on [M2].

Below, we give some general information concerning the theories mentioned above.

BASIC is a finite set of quantifier-free formulas expressing basic properties of the relation and function symbols.

A *sharply bounded* formula is a bounded formula in which all quantifiers are sharply bounded, i.e. of the form $\exists x \leqslant |t|$ or $\forall x \leqslant |t|$ where t is a term which does not contain x.

The class $\Sigma_0^b = \Pi_0^b$ is the class of all sharply bounded formulas. The syntactic classes Σ_{i+1}^b and Π_{i+1}^b of bounded formulas are defined by counting alternations of bounded quantifiers, ignoring sharply bounded quantifiers (see [B1]).

The Σ_i^b formulas represent exactly the relations in the i^{th} level of the polynomial hierarchy. So, for example, the NP relations in the standard model are exactly the ones that can be defined via Σ_1^b formulas. The same is true for Π_1^b formulas and coNP relations.

The (classical) theory S_2^1 is axiomatized by adding the scheme PIND for Σ_1^b formulas to BASIC, i.e. $[A(0) \wedge \forall x(A(\llcorner \frac{x}{2} \lrcorner) \rightarrow A(x))] \rightarrow \forall x A(x)$, where $A(x)$ is a Σ_1^b formula. Here, $A(x)$ can have more free variables besides x. A function f is said to be Σ_1^b-*definable* in S_2^1 if and only if it is provably total in S_2^1 with a Σ_1^b formula defining the graph of f. Buss proved that a function is Σ_1^b-definable in S_2^1 if and only if it is polynomial time computable.

The theories S_2^i, $i > 1$, are similarly defined as the theories axiomatized by BASIC together with PIND on Σ_i^b formulas. S_2 is the union of all S_2^i, $i \geqslant 1$.

The theory IS_2^1 is the intuitionistic theory axiomatized by BASIC plus the scheme PIND on positive Σ_1^b formulas (denoted Σ_1^{b+}), i.e. Σ_1^b formulas which do not contain '$\neg$' and '$\rightarrow$'. This theory was introduced and studied by Cook and Urquhart and by Buss (see [CU] and [B3]). A function f is also defined to be Σ_1^{b+}-*definable* in IS_2^1 if it is provably total in IS_2^1 with a Σ_1^{b+} formula defining the graph of f. In [CU] it is proved that f is Σ_1^{b+}-definable in IS_2^1 if and only if it is polynomial time computable. Also, S_2^1 is $\forall\exists\Sigma_1^b$-conservative over IS_2^1, as it follows from 10.7 and 4.2 in [CU], see also [A] for a different proof.

The theory PV is Stephen Cook's equational theory for polynomial time functions and PV_1 is its (conservative) extension to classical first-order logic. PV_1 is a universal theory which proves the polynomial induction on quantifier-free formulas. PV^i denotes the intuitionistic deductive closure of PV. IPV is the intuitionistic theory of PV plus polynomial induction on NP formulas. Here, an NP formula is a quantifier free formula (in the language of PV) prefixed by a block of bounded existential quantifiers. IPV is a conservative extension of IS_2^1. CPV is the classical version of IPV.

It is known that the theory S_2^1 can be axiomatized over the base theory BASIC using either PIND(Π_1^b) or PIND(Σ_1^b). On the other hand, in [M1], we showed that the same is not true for the corresponding theories based on intuitionistic logic,

Fact 1.1

The intuitionistic theory axiomatized by BASIC + PIND(Π_1^{b+}) does not imply IS_2^1.

In Section 4, we give more exact results in this direction. The following related results are also proved in [M1].

Fact 1.2

(i) If IPV $\vdash$ PIND(coNP), then CPV = PV_1.

(ii) If $\mathrm{IS}_2^1 \vdash \mathrm{PIND}(\Pi_1^{b+})$, then $\mathrm{CPV} = \mathrm{PV}_1$.

Is is known that, $\mathrm{CPV} = \mathrm{PV}_1$ implies the collapse of the polynomial hierarchy (see [KPT]).

In the last section we will consider the question of whether $\mathrm{PV} + \mathrm{PIND}(\mathrm{coNP}) \vdash_{\mathrm{i}} \mathrm{PIND}(\mathrm{NP})$. We will give a negative answer to this question based on a plausible assumption.

2 Basic results on Kripke models of intuitionistic bounded arithmetic

In this section we briefly describe Kripke models. All theories we will study prove the principle of excluded middle PEM (that is, $\varphi \vee \neg\varphi$) for atomic formulas and so we can use a slightly simpler version of the definition of Kripke models as we have completeness with respect to this restricted class of models (see [B2]).

A Kripke structure K for a language L can be considered as a set of classical structures for L partially ordered by the relation substructure. We can assume, without loss of generality, that this partially ordered set is a rooted tree. For every node α, L_α denotes the expansion of L by adding constants for elements of M_α. The forcing relation $\Vdash$ is defined between nodes and L_α-sentences inductively as follows:

- For atomic φ, $M_\alpha \Vdash \varphi$ if and only if $M_\alpha \vDash \varphi$;
- $M_\alpha \Vdash \varphi \vee \psi$ if and only if $M_\alpha \Vdash \varphi$ or $M_\alpha \Vdash \psi$;
- $M_\alpha \Vdash \varphi \wedge \psi$ if and only if $M_\alpha \Vdash \varphi$ and $M_\alpha \Vdash \psi$;
- $M_\alpha \Vdash \varphi \to \psi$ if and only if for all $\beta \geq \alpha$, $M_\beta \Vdash \varphi$ implies $M_\beta \Vdash \psi$;
- $M_\alpha \Vdash \forall x\varphi(x)$ if and only if for all $\beta \geq \alpha$ and all $a \in M_\beta$, $M_\beta \Vdash \varphi(a)$; and
- $M_\alpha \Vdash \exists x\varphi(x)$ if and only if there exists $a \in M_\alpha$ such that $M_\alpha \Vdash \varphi(a)$.

A Kripke model K forces a formula $\varphi(\overline{x})$, if each of its nodes (equivalently its root) forces $\forall\overline{x}\varphi(\overline{x})$. A Kripke model is *T-normal*, where T is a set of sentences, if each node (world) of it satisfies T. It decides quantifier free formulas if it forces the axiom PEM restricted to quantifier free formulas. So, for example, any BASIC-normal Kripke model decides atomic formulas (see [B3]).

Below, we mention some facts about Kripke models of bounded arithmetic theories (see [M1]).

Proposition 2.1

(i) Kripke models of PV^{i} are exactly PV_1-normal Kripke models.

(ii) For a Kripke model of PV^{i} over the frame ω to force PIND(coNP) it is necessary and sufficient that the union of the worlds in it satisfies CPV.

Proof. By induction on the complexity of formulas it is easy to see that for each $\exists$-free formula A, each node in such a Kripke model forces A if and only the union of the worlds above it satisfies A. Now apply the definition of forcing. $\Box$

3 Constructing models of bounded arithmetic

In this section we introduce some methods for constructing models for classical and intutionistic bounded arithmetic. First the classical one. This is indeed a variant of the construction given in Johannsen [J1-J2], where a model of the theory S_2^0 (the classical theory axiomatized by BASIC plus PIND on sharply bounded formulas) was constructed to witness a well-known independence result of Takeuti [Ta], i.e. $S_2^0 \nvdash \forall x \exists y(x = 0 \vee x = y + 1)$. Takeuti proved this result through the use of a proof-theoretic method.

Let M and N be two models of BASIC. Let $Log(M) = \{a \in M : (\exists b \in M)a \leq |b|\}$. N is called a *weak end-extension* of M and it is written that $M \subseteq_{w.e.} N$, if N extends M and $Log(N)$ is an end-extension of $Log(M)$, i.e. for all $a \in Log(M)$, $b \in Log(N)$ with $N \vDash b \leq a$, we have $b \in Log(M)$. It is known and easy to see that weak end-extensions are always Σ_0^b-elementary, i.e. if $M \subseteq_{w.e.} N$, then for any Σ_0^b-formula $A(\overline{x})$ and $\overline{a} \in M$, $M \vDash A(\overline{a})$ if and only if $N \vDash A(\overline{a})$. Elements of $Log(M)$ are called *small* elements of M. The others are *large* elements of M.

Recall that, the axiom *exp* states that the exponentiation function is total, and the axiom Ω_2 states that the function $x\#_3 y = 2^{|x|\#|y|}$ is total.

It is known that the function $Bit(x, i)$ which gives the value of the i^{th} bit in the binary expansion of x, and the operation of length bounded counting are definable in S_2^1. Hence the function $count(a) = \#i < |a|(Bit(a, i) = 1)$, which gives the number of 1's in the binary expansion of a, is well defined in S_2^1. Now, let M be a countable (nonstandard) model of $S_2^1 + \Omega_2 + \neg$exp. For a large element $a \in M$, structures of the form

$M' = \{x \in M : count(x) < ||a|| \text{ for some } a \in M\}$

were studied in [J2].

Next we need to modify the definition of M' (in order to prove our independence result).

Fix a large element $a \in M$ and define

$M^* = Log(M) \cup \{x \in M : count(x) < ||a||^n \text{ for some non-negative integer } n\}$.

Theorem 3.1 $M^* \vDash$ BASIC.

Proof. First, note that $Log(M)$ is a model of BASIC (note that since we have assumed M is closed under Ω_2, small elements are closed under $\#$).

Moreover, as it is mentioned in [J1], it can be proved in S_2^1 that

$count(a + b) \leqslant count(a) + count(b)$ and $count(a \cdot b) \leqslant count(a) \cdot count(b)$.

Furthermore, for any $a, b \in M$, $count(a\#b) = 1$. Therefore, M^* is closed under $+$, $\cdot$, and $\#$. Also, M^* is clearly closed under the function $|x|$ because each small element of M is in M^*. Closure of M^* under the function $\llcorner \frac{x}{2} \lrcorner$ can also be easily verified by a simple computation.

Now it should be clear that $M^* \models$ BASIC as BASIC is a universal theory. $\square$

In fact, since $M^* \subseteq_{w.e.} M$, we have $M^* \models \mathrm{L}_2^0$, where L_2^0 is the theory axiomatized by BASIC plus length induction on sharply bounded formulas (see [J1, Corollary 2]). The scheme of length induction is $[A(0) \wedge \forall x(A(x) \rightarrow A(x+1))] \rightarrow \forall x A(|x|)$.

Theorem 3.2 $M^* \nvDash \forall x \exists y(x = 0 \vee x = y + 1)$.

Proof. The proof is similar to the one given in [J2, Proposition 6].

Note that $count(2^{|a|}) = 1$ and so $2^{|a|} \in M^*$. Consider the element $b = 2^{|a|} - 1 \in M$. Then $count(b) = |a|$. If $b \in M^*$, then $|a| < ||a||^n$ for some $n \in \mathbb{N}$. As $M \models \Omega_2$, there is $a' \in M$ such that $|a| < ||a'||$ and so $a < 2|a'|$, in contradiction to a being large. $\square$

Inductively define $a^{\#0} = 1$, $a^{\#1} = a$, and $a^{\#(n+1)} = a^{\#n}\#a$, for each $a \in M$.

Theorem 3.3 There is an ω-chain of models of BASIC such that the union of its worlds satisfies S_2^1 but none of its worlds satisfies the sentence $\forall x \exists y(x = 0 \vee x = y + 1)$. Moreover, for each i, M_{i+1} is a proper weak end-extension of M_i.

Proof. As above, let M be a countable (nonstandard) model of $\mathrm{S}_2^1 + \Omega_2 + \neg\exp$. Consider a cofinal sequence (a_i) of large elements of M such that $a_{i+1} \geqslant (a_i \#_3 a_i)$, for all $i \geq 0$.

Now define a sequence of substructures of M as follows:

1) $M_0 = M^*$ (as defined above, with a_0 as a),

2) M_{i+1} is defined as the set

$\{x \in M : x < a_i^{\#n} \text{ for some } n \in \mathbb{N}\} \cup \{x \in M : count(x) < ||a_{i+1}||^n \text{ for some } n \in \mathbb{N}\}$.

Similar proofs as the ones given for M^* above can be applied to show that $M_i \models$ BASIC $+ \neg\forall x \exists y(x = 0 \vee x = y + 1)$. Also, clearly, $\bigcup M_i = M \models \mathrm{S}_2^1$ as $a_i \in M_{i+1}$.

Note that each world contains $Log(M)$, and so clearly M_{i+1} is a weak end-extension of M_i. Moreover the extension is proper, since for example, $(a_i \# a_i) - 1 \in M_{i+1} \setminus M_i$. $\square$

Next we mention an easy fact about Kripke models (see [M1]). Its proof is similar to the one for Proposition 2.1. A Kripke model is a weak end-extension Kripke model if its accessibly relation is a weak end-extension.

Proposition 3.4 For a weak end-extension Kripke model whose accessibility relation is ω and decides atomic formulas to force PIND(Π_1^{b+}) it is necessary and sufficient that the union of the worlds in it satisfies PIND(Π_1^{b+}).

Proof. Note that any such Kripke model is Σ_0^b-elementary. $\square$

The last two results suggest a way to construct a special Kripke model. Below, we will explicitly define and use it.

4 PIND on NP and coNP formulas

In this section our aim is to apply the models constructed above to show that the sentence $\neg\neg\forall x\exists y(x = 0\vee x = y+1)$ is not intuitionistically provable in BASIC + PIND(Π_1^{b+}). A similar method is used in [M2] to show that

BASIC + PIND(Π_1^{b+}) $\nvdash_i \neg\neg\forall x, y\exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

Each of these results, using $\forall\exists$ conservatively of S_2^1 over IS_2^1, can be easily applied to show that

BASIC + PIND(Π_1^{b+}) $\nvdash_i \neg\neg$PIND(Σ_1^{b+}).

Theorem 4.1 BASIC + PIND(Π_1^{b+}) $\nvdash_i \neg\neg\forall x\exists y(x = 0 \vee x = y + 1)$.

Proof. Consider the ω-chain $M_0 \subset_{w.e.} M_1 \subset_{w.e.} M_2 \subset_{w.e.} \cdots$ of Theorem 3.3, and interpret it as an ω-framed Kripke model K. For each i, $M_i \not\models \forall x\exists y(x = 0 \vee x = y + 1)$.

Therefore, by the definition of forcing, $K \Vdash \neg\forall x\exists y(x = 0 \vee x = y + 1)$. Hence, $K \nVdash \neg\neg\forall x\exists y(x = 0 \vee x = y + 1)$.

On the other hand, since the union of the worlds in this Kripke model is equal to $M \models S_2^1$, by Proposition 3.4, we have $K \Vdash$ PIND(Π_1^{b+}). □

Now, we are interested in the question of whether results analogous to the above hold if we work in the language of PV (recall that, by [M1], IPV $\nvdash$ PIND(coNP) unless CPV = PV_1). This question is not easy. The following proposition gives a reason for this claim. By IS_2(PV) we mean the intuitionistic version of S_2 conservatively extended to the language of PV.

Proposition 4.2 If $PV^i \vdash$ P = NP, i.e. any NP formula in PV^i is equivalent to a quantifier free formula, then $PV^i \equiv IS_2(PV)$.

Proof. Let $PV^i \vdash$P=NP. Then, using induction on the complexity of formulas, one can see that, any bounded formula in PV^i would be equivalent to a quantifier free formula. We only examine the $\forall$ case:

Let $PV^i \vdash \varphi(x, \overline{y}) \leftrightarrow \psi(x, \overline{y})$, where ψ is quantifier-free. So, $PV^i \vdash \forall x \leqslant t\varphi(x, \overline{y}) \leftrightarrow \forall x \leqslant t\psi(x, \overline{y})$. Using decidability of atomic formulas, we get the following intuitionistic equivalences:

$$\forall x \leqslant t\psi(x, \overline{y}) \equiv_i \forall x \leqslant t\neg\neg\psi(x, \overline{y}) \equiv_i \neg\exists x \leqslant t\neg\psi(x, \overline{y}).$$

Now, using the assumption, we obtain that $\forall x \leqslant t\psi(x, \overline{y})$ is equivalent to a quantifier free formula. To see $PV^i \equiv IS_2(PV)$, note that PV_1 proves the polynomial induction on quantifier free formulas and so one can see that PV^i does the same, using the negative translation.□

So proving $\mathrm{PV} + \mathrm{PIND(coNP)} \nvdash_{\mathrm{i}} \mathrm{PIND(NP)}$ would require proving that $\mathrm{PV}^{\mathrm{i}} \nvdash \mathrm{P} = \mathrm{NP}$.

In the theorem below, we give an answer to the above mentioned question under a plausible assumption.

Recall that, the (sharply bounded) replacement (or collection) scheme $\mathrm{BB}(\Sigma^{\mathrm{b}}_0)$ is

$\forall i < |a| \exists x < a A(i,x) \rightarrow \exists \omega \forall i < |a| A(i, [\omega]_i)$,

where A is a Σ^b_0 formula and $[x]_i$ is the ith element of the sequence coded by x. It is known that CPV proves this scheme but, if integer factoring is not possible in probabilistic polynomial time, then PV_1 does not prove the scheme (see [CT]). Also, if $\mathrm{PV}_1 + \mathrm{BB}(\Sigma^{\mathrm{b}}_0)$ proves CPV, then PV_1 proves CPV (see [Z] and [CT]).

Also, let EF denote an extended Frege proof system. Recall that a Frege proof system is just an ordinary propositional proof system containing finitely many axiom schemes and inference rules, and an extended Frege proof system is a Frege system allowing abbreviations of the form $p_A \equiv A$, where A is a propositional formula and p_A is a new propositional variable. The system EF can be formalized in PV_1 and related results about it can be stated and proved in this theory (see [C] or [K]). For example, it is known that provability of NP = coNP and that of the statement "EF is a complete proof system" in PV_1 are equivalent (see [K, Theorem 15.3.7]).

Theorem 4.3 If there exists a model M of $\mathrm{PV} + \mathrm{BB}(\Sigma^{\mathrm{b}}_0)$ that does not satisfy CPV and in which EF is not a complete proof system, then we have $\mathrm{PV} + \mathrm{PIND(coNP)} \nvdash_i \mathrm{PIND(NP)}$.

Proof. Let M be as above. There exists $M' \vDash \mathrm{PV}$ such that M embeds in M' and the embedding is not Σ^b_1-elementary (see [K, Corollary 15.3.10]). Now embed M' Σ^b_1-elementarily in a model $M^* \vDash \mathrm{CPV}$, see [K, Theorem 7.6.3] for the existence of such a model. Note that the induced embedding between M and M^* is not Σ^b_1-elementary. Putting M^* above M produces a Kripke model which forces $\mathrm{PV} + \mathrm{PIND(coNP)}$, see Proposition 2.1. We show that it does not force PIND(NP). Suppose the Kripke model forces PIND(NP). We will show that, in this case, the root, i.e. M, (classically) would satisfy PIND(NP) which is a contradiction.

We heavily rely on the easily verifiable fact that forcing and satisfaction of NP formulas in each node of a Kripke model of PV^{i} are equivalent.

Suppose that $A(y)$ is an NP formula (possibly with parameters from M) such that $M \nvDash A$ but $M^* \vDash A$. Such a formula exists because, modulo $\mathrm{PV}_1 + \mathrm{BB}(\Sigma^{\mathrm{b}}_0)$, each Σ^b_1 formula is equivalent to an NP formula, see [Th] for more detail on this theory.

Let $B(x)$ be an arbitrary NP formula. We are going to show that M satisfies the instance of polynomial induction on $B(x)$. So, let $M \vDash B(0)$ and

$M \vDash B(\llcorner \frac{x}{2} \lrcorner) \rightarrow B(x)$.

We will show that $M \vDash \forall x B(x)$. Clearly we have $M \vDash B(0) \vee A$ and

$M \vDash \forall x[(B(\llcorner \frac{x}{2} \lrcorner) \vee A) \rightarrow (B(x) \vee A)]$.

Therefore, $M \Vdash B(0) \vee A$ and, using the assumption $M^* \vDash A$,

$M \Vdash \forall x[(B(\llcorner \frac{x}{2} \lrcorner) \vee A) \rightarrow (B(x) \vee A)]$.

So, we get $M \Vdash \forall x(B(x) \vee A)$ since the Kripke model forces PIND(NP) by our assumption. Hence, $M \vDash \forall x(B(x) \vee A)$. So, $M \vDash \forall x B(x)$. Therefore, $M \vDash$ PIND(NP), which is a contradiction. $\square$

Acknowledgements

I would like to thank two anonymous referees for useful comments on earlier versions of this paper. I would also like to thank the editor responsible for this paper Iraj Kalantari for his comments improving presentation of the paper, and Chris Pollett for drawing my attention to [CT]. This research was in part supported by a grant from IPM (No. 83030118).

References

[A] J. Avigad, Interpreting Classical Theories in Constructive Ones, Journal of Symbolic Logic, 65 (2000), 1785-1812.

[B1] S. R. Buss, Bounded Arithmetic, Bibliopolis, 1986.

[B2] S. R. Buss, On Model Theory for Intuitionistic Bounded Arithmetic with Applications to Independence Results, in: Feasible mathematics, eds S. R. Buss and P. J. Scott, 1990, 27-47, Birkhauser.

[B3] S. R. Buss, A Note on Bootstrapping Intuitionistic Bounded Arithmetic, Proof theory (Leeds, 1990), 149-169, Cambridge University Press, Cambridge, 1992.

[C] S. A. Cook, Feasibly Constructive Proofs and the Propositional Calculus, in Proceedings of the Seventh Annual Symposium on Theory of Computing, 1975, 83-97.

[CT] S. A. Cook and N. Thapen, The Strength of Replacement in Weak Arithmetic, Nineteenth Annual IEEE Symposium on Logic in Computer Science (LICS 2004), pp 256-264.

[CU] S. A. Cook and A. Urquhart, Functional Interpretations of Feasibly Constructive Arithmetic, Annals of Pure and Applied Logic, 63 (1993), 103-200.

[J1] J. Johannsen, A Model-Theoretic Property of Sharply Bounded Formulae, With Some Applications, Mathematical Logic Quarterly, 44 (1998), 205–215.

[J2] J. Johannsen, A Remark on Independence Results for Sharply Bounded Arithmetic, Mathematical Logic Quarterly, 44 (1998), 569-570.

[K] J. Krajíček, Bounded Arithmetic, Propositional Logic, and Complexity Theory, Cambridge University Press, 1995.

[KPT] J. Krajíček, P. Pudlák, G. Takeuti, Bounded Arithmetic and the Polynomial Hierarchy, Annals of Pure and Applied Logic, 52 (1991), 143-153.

[M1] Morteza Moniri, Comparing Constructive Arithmetical Theories Based on NP-PIND and coNP-PIND, Journal of Logic and Computation, 13 (2003), 881-888.

[M2] Morteza Moniri, An Independence Result For Intuitionistic Bounded Arithmetic,Submitted.

[Ta] G. Takeuti, Sharply Bounded Arithmetic and the Function $a\dot{-}1$, Logic and computation (Pittsburgh, PA, 1987), 281-288, Contemp. Math., 106, Amer. Math. Soc., Providence, RI, 1990.

[Th] N. Thapen, The Weak Pigeonhole Principle in Models of Bounded Arithmetic, DPhil Thesis, University of Oxford, 2002.

[TD] A. S. Troelstra and D. van Dalen, Constructivism in Mathematics, v.I, North-Holland, 1988.

[Z] D. Zambella, Notes on Polynomially Bounded Arithmetic, Journal of Symbolic Logic 61 (1996), 942-966.

ADDRESS:

Institute for Studies in

Theoretical Physics and Mathematics (IPM), P.O. Box 19395-5746,

Tehran, Iran. **AND**:

Department of Mathematics, Shahid Beheshti University,

P.O. Box 19839, Tehran, Iran.

Email: ezmoniri@ipm.ir