An Independence Result For Intuitionistic Bounded Arithmetic

Morteza Moniri

Abstract

It is shown that the intuitionistic theory of polynomial induction on positive Π^b_1 (coNP) formulas does not prove the sentence $\neg\neg\forall x, y\exists z \leq y(x \leq |y| \to x = |z|)$. This implies the unprovability of the scheme $\neg\neg\mathrm{PIND}(\Sigma^{b+}_1)$ in the mentioned theory. However, this theory contains the sentence $\forall x, y\neg\neg\exists z \leq y(x \leq |y| \to x = |z|)$. The above independence result is proved by constructing an ω-chain of submodels of a countable model of $\mathrm{S}_2 + \Omega_3 + \neg\exp$ such that none of the worlds in the chain satisfies the sentence, and interpreting the chain as a Kripke model.

Key words: Bounded Arithmetic, Intuitionistic Logic, Kripke model, NP, Polynomial Hierarchy, Polynomial Induction.

1 Introducing Classical and Intuitionistic Bounded Arithmetic

We first briefly describe the first-order theories of bounded arithmetic introduced by Samuel Buss [B1]. The language of these theories extends the usual language of first-order arithmetic by adding function symbols $\llcorner \frac{x}{2} \lrcorner$ ($= \frac{x}{2}$ rounded down to the nearest integer), $|x|$ (=the number of digits in the binary expansion of x) and $\#$ ($x\#y = 2^{|x||y|}$).

The set BASIC of basic axioms for the theories of bounded arithmetic is a finite set of (universal closures of) quantifier-free formulas fixing the basic properties of the relations and functions of the language.

Below, we recall the exact syntactic definitions of the hierarchies of bounded formulas, since we work with weak theories of bounded arithmetic, it is necessary to be careful about the definitions. The set of sharply bounded formulas is the set of bounded formulas 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 that does not contain x.

Definition 1.1 (Buss's hierarchy of bounded formulas)

(1) $\Sigma^b_0 = \Pi^b_0$ is the set of all sharply bounded formulas.

(2) Σ^b_{i+1} is defined inductively by:

(a) $\Pi^b_i \subseteq \Sigma^b_{i+1}$;

(b) If $A \in \Sigma^b_{i+1}$, so are $(\exists x \leqslant t)A$ and $(\forall x \leqslant |t|)A$;

(c) If $A, B \in \Sigma^b_{i+1}$, so are $A \wedge B$ and $A \vee B$;

(d) If $A \in \Sigma^b_{i+1}$ and $B \in \Pi^b_{i+1}$, then $\neg B$ and $B \rightarrow A$ are in Σ^b_{i+1}.

(3) Π^b_{i+1} is defined dually.

(4) Σ^b_{i+1} and Π^b_{i+1} are the smallest sets which satisfy (1)-(3).

The Σ^b_1 formulas represent exactly the NP relations in the standard model.

The (classical) theory S^1_2 is axiomatized by adding the scheme PIND for Σ^b_1 formulas $A(x)$ to BASIC:

$[A(0) \wedge \forall x(A(\llcorner \frac{x}{2} \lrcorner) \rightarrow A(x))] \rightarrow \forall x A(x)$

A function f is said to be Σ^b_1-definable in S^1_2 if and only if it is provably total in S^1_2 with a Σ^b_1 formula defining the graph of f. Buss proved that a function is Σ^b_1-definable in S^1_2 if and only if it is polynomial time computable.

The theories $\mathrm{S}^{\mathrm{i}}_2$, $i \geqslant 0$, are similarly defined as the theories axiomatized by BASIC together with PIND on Σ^b_i formulas. S_2 is the union of all $\mathrm{S}^{\mathrm{i}}_2$, $i \geqslant 0$.

The theory IS^1_2 is the intuitionistic theory axiomatized by BASIC plus the scheme PIND on positive Σ^b_1 formulas (denoted Σ^{b+}_1), i.e. Σ^b_1 formulas that 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^{b+}_1-definable in IS^1_2 if it is provably total in IS^1_2 with a Σ^{b+}_1 formula defining the graph of f. They [CU] proved that f is Σ^{b+}_1-definable in IS^1_2 if and only if it is polynomial time computable.

An intuitionistic version for each of the theories $\mathrm{S}^{\mathrm{i}}_2$, $i > 1$, was defined and studied by V. Harnik [H].

A positive Π^b_1 formula (denoted Π^{b+}_1), is defined to be a Π^b_1 formula which does not contain $\neg$ and $\rightarrow$. The intuitionistic theory of BASIC + PIND(Π^{b+}_1) was also discussed in the literature on intuitionistic bounded arithmetic (see e.g. [B3] and [H]).

Fact 1.2 $\mathrm{S}^1_2 \equiv$ BASIC + PIND(Π^b_1).

Proof See [K, Lemma 5.2.5]. □

IBASIC is the usual notation for the intuitionistic deductive closure of BASIC.

Fact 1.3 IBASIC proves the Principle of Excluded Middle for atomic formulas of its language. IS^1_2 proves the same principle for sharply bounded formulas.

Proof See [B3] and [CU]. □

In the following, the notation $\vdash_i$ shows provability in intuitionistic first order logic.

For the definition of Kripke models of intuitionistic bounded arithmetic and basic results about them, see [M2] and [B2]. The general results on intuitionistic logic and arithmetic, and also Kripke models, can be found in [TD]. [MM] contains a study of weak fragments of first-order intuitionistic arithmetic (Heyting arithmetic) concerning closure properties via Kripke models. Here, we just mention that all intuitionistic theories we will study prove the principle of excluded middle for atomic formulas, and so we can use a slightly simpler version of the definition of Kripke model. So, a Kripke model in the language of bounded arithmetic is a set of (normal) classical structures in the same language partially ordered by the relation substructure. In these Kripke models, forcing and satisfaction of quantifier-free formulas in each node (world) are equivalent.

In [M2], it is shown that the intuitionistic theory axiomatized by BASIC + PIND(Π_1^{b+}) does not imply IS_2^1 by using Kripke models. The paper also proves the converse assuming the Polynomial Hierarchy S_2^1-provably does not collapse. Similar techniques are used in [M1] to show that certain apparently stronger extensions of S_2^1 are actually stronger assuming the above mentioned complexity assumption.

Here, we strengthen the first independence result mentioned above by showing that the sentence $\neg\neg\forall x, y\exists z \leq y(x \leq |y| \rightarrow x = |z|)$ is not provable in the intuitionistic theory of BASIC + PIND(Π_1^{b+}). This can be easily applied to prove that even the double negation of the scheme PIND(Σ_1^{b+}) is not deducible in this intuitionistic theory. In [M3], we showed the same for the sentence $\neg\neg\forall x\exists y < x(x = 0 \vee x = y + 1)$. The following fact shows a difference between the classical power of these two sentences.

Fact 1.4

i) $\mathrm{S}_2^0 \vdash \forall x, y\exists z \leq y(x \leq |y| \rightarrow x = |z|)$,

ii) $\mathrm{S}_2^0 \nvdash \forall x\exists y < x(x = 0 \vee x = y + 1)$.

Proof See [J1, Proposition 8] and [T]. □

2 A model theoretic construction and its application

In this section we work in the language of BASIC. Also, IBASIC is the underlying theory for all intuitionistic theories we will mention.

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 $Log(M)$. This means that, for all $a \in Log(M)$ and $b \in Log(N)$ with $N \vDash b \leq a$, we have $b \in Log(M)$. It is known and easy to check that weak end extensions are always Σ_0^b-elementary. 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. Here we express two well known weak forms of *exp*: the axiom Ω_2 states that the function

$x\#_3 y = 2^{|x|\#|y|}$ is total and the axiom Ω_3 states that the function $x\#_4 y = 2^{|x|\#_3|y|}$ is total. For more on these axioms, see e.g. [HP], pages 272-274. The functions $\#_3$ and $\#_4$ mentioned above have the same growth rates as the functions ω_3 and ω_4 mentioned in [HP], respectively. The axioms Ω_2 and Ω_3 are consistent with $\neg exp$ by Parikh's theorem, see [HP].

Theorem 2.1 There is a weak end extension ω-chain of classical structures such that the union of its worlds satisfies S_2 but none of its worlds satisfies the sentence $\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

Proof Let M be a countable (nonstandard) model of $S_2 + \Omega_3 + \neg$exp. Assume that $a \in M$ is large.

Inductively define $a^{\#_3(0)} = 1$ and $a^{\#_3(n+1)} = a^{\#_3(n)}\#_3 a$ for each $n \geq 1$. Also define,

$I = \{x \in M : x < a^{\#_3(n)}$ for some non-negative integer n$\}$.

One can easily see that I is closed under $\#_3$, and so under $+$, $\cdot$ and $\#$. Note that, I is a proper cut in M, since for example $a\#_4 a \in M - I$ as obviously $a^{\#_3(n)} < a\#_4 a$ for any n.

Suppose that $a_0, a_1, a_2, \cdots$ is a cofinal sequence of large elements of I such that $a_i^{\#n} < a_{i+1}$ for all $n \geq 0$. Here $a_i^{\#n}$ is defined similar to $a_i^{\#_3(n)}$ by changing $\#_3$ to $\#$. One should choose $a_{i+1} \geqslant a_i \#_3 a_i$.

Also, for each i, define

$a_i^{\#\frac{1}{\mathbb{N}}} = \{x \in M : x^{\#n} < a_i$ for all non-negative integers n$\}$.

Define, $M_i = a_i^{\#\frac{1}{\mathbb{N}}} \cup (M - I)$ for each i. It is easy to see that M_i is closed under $+$, $\cdot$, $\llcorner \frac{x}{2} \lrcorner$, and $\#$. Moreover, M_i is closed under the function $|x|$ because each small element of M is in $a_i^{\#\frac{1}{\mathbb{N}}}$ (note that a_i is large).

Now it should be clear that $M_i \vDash$ BASIC as BASIC is a universal theory. Also, clearly, the union of the M_i's is M. So, to complete the proof of the Theorem, it is enough to show the following.

Claim: $M_i \vDash \exists x, y(x < |y| \wedge \forall z \leq y\ x \neq |z|)$.

Proof of Claim: One can consider $|a_i|$ as x and any fixed element $c \in (M - I)$ as y. The proof is as follows. For each $x \in a_i^{\#\frac{1}{\mathbb{N}}}$ we have $|x| < |a_i|$. To see it suppose $|b| \geq |a_i|$ for some $b \in a_i^{\#\frac{1}{\mathbb{N}}}$. We have $b\#b < a_i$. So $|b\#b| \leq |a_i|$. But, in this case, we would have $|b\#b| = |b|^2 + 1 \leq |a_i| \leq |b|$, contradiction. Moreover, for each $y \in (M - I)$, we have $y > 2a_i$. Therefore, $|y| > |a_i|$. $\square$

The structures of the form $a_i^{\#\frac{1}{\mathbb{N}}}$ used in the proof above were first applied in Johannsen [J, Proposition 6-7].

Now we use the above classical result to prove a strong independence result for the theories of intuitionistic bounded arithmetic. We shall give a model theoretic argument.

Proposition 2.2 Suppose $\mathcal{K}$ is a weak end extension Kripke model whose accessibility relation is ω and decides atomic formulas. Then for any node α in $\mathcal{K}$ and any Π_1^{b+} L_α-sentence A we have, $M_\alpha \Vdash A$ if and only if the union of the worlds in $\mathcal{K}$ satisfies A.

Proof Use induction on formulas and Fact 1.3. □

Corollary 2.3 Suppose $\mathcal{K}$ is a weak end extension Kripke model whose accessibility relation is ω and decides atomic formulas. $\mathcal{K}$ forces $\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+})$ if and only if the union of the worlds in $\mathcal{K}$ satisfies $\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+})$.

Proof By the definition of forcing and the above Proposition. Recall that BASIC is a universal theory. □

The scheme $\neg\neg\mathrm{PIND}(\Sigma_1^{b+})$ is double negation of the scheme $\mathrm{PIND}(\Sigma_1^{b+})$.

Corollary 2.4 $\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+}) \nvdash_i \neg\neg\mathrm{PIND}(\Sigma_1^{b+})$.

Proof Consider the ω-chain $M_0 \subset_{w.e.} M_1 \subset_{w.e.} M_2 \subset_{w.e.} \cdots$ constructed in Theorem 2.1. Interpret the chain as an ω-framed Kripke model $\mathcal{K}$. Since the union of the worlds in this Kripke model is clearly equal to $M \vDash \mathrm{S}_2^1$, by the above Corollary, it forces $\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+})$. Also, none of the models in $\mathcal{K}$ satisfies

$\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

Therefore, by the definition of forcing, one can easily see that $\mathcal{K}$ forces

$\neg\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

Hence, this Kripke model does not force

$\neg\neg\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

On the other hand, S_2^1 is $\forall\Sigma_1^b$-conservative over IS_2^1 (that is the intuitionistic theory of $\mathrm{BASIC} + \mathrm{PIND}(\Sigma_1^{b+})$, see e.g. [A]), and so

$\mathrm{IS}_2^1 \vdash_i \forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

Therefore,

$\mathrm{BASIC} + \neg\neg\mathrm{PIND}(\Sigma_1^{b+}) \vdash_i \neg\neg\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$. □

It is interesting to see that, however,

$\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+}) \vdash_i \forall x, y \neg\neg\exists z \leq y(x \leq |y| \rightarrow x = |z|)$.

The reason for this last result is that, the intuitionistic theory of $\mathrm{BASIC} + \mathrm{PIND}(\Pi_1^{b+})$ is obviously closed under the negative translation, and its classical counterpart proves the sentence $\forall x, y \exists z \leq y(x \leq |y| \rightarrow x = |z|)$ (in fact, polynomial induction on a simple atomic formula is sufficient for this provability, see [J. Proposition 8]). For the definition

of the negative translation and basic results about it, see e.g. [TD].

Acknowledgement

This research was in part supported by a grant from IPM (No. CS1383-4-07).

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.

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

[H] V. Harnik, Provably Total Functions of Intuitionistic Bounded Arithmetic, Journal of Symbolic Logic, 57 (1992) 466-477.

[HP] P. Hájek and P. Pudlák, Metamathematics of First-Order Arithmetic, Springer-Verlag, 1993.

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

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

[M1] Morteza Moniri, On Two Questions About Feasibly Constructive Arithmetic, Mathematical Logic Quarterly, 49 (2003) 425-427.

[M2] Morteza Moniri, Comparing Constructive Arithmetical Theories Based on NP-PIND and coNP-PIND, Journal of Logic and Computation, 13 (2003) 881-888.

[M3] Morteza Moniri, Model theory of Bounded Arithmetic With Applications to Independence Results, Submitted.

[MM] Morteza Moniri and Mojtaba Moniri, Some Weak Fragments of HA and Certain Closure Properties, Journal of Symbolic Logic, 67 (2002) 91-103.

[T] 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.

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

ADDRESS:

Department of Mathematics,

Shahid Beheshti University, Evin,

Tehran, Iran.

AND: Institute for Studies in

Theoretical Physics and Mathematics (IPM),

P.O. Box 19395-5746,

Tehran, Iran.

email: ezmoniri@ipm.ir