Polynomial Induction and Length Minimization in Intuitionistic Bounded Arithmetic

Morteza Moniri

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

Abstract

It is shown that the feasibly constructive arithmetic theory IPV does not prove (double negation of) LMIN(NP), unless the polynomial hierarchy CPV-provably collapses. It is proved that PV plus (double negation of) LMIN(NP) intuitionistically proves PIND(coNP). It is observed that PV+ PIND(NP∪coNP) does not intuitionistically prove NPB, a scheme which states that the extended Frege systems are not polynomially bounded.

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

Key words: Kripke model; Polynomial Induction; Length Minimization; IPV; Extended Frege System.

1 Introducing Classical and Intuitionistic Bounded Arithmetic

The theory PV is an equational theory of polynomial time functions introduced by Stephen Cook, $(PV)^i$ is its extension to intuitionistic first-order logic and IPV is the intuitionistic theory of PV plus polynomial induction on NP formulas. Here an NP formula is a formula equivalent to an atomic formula (in the language of PV) prefixed by a bounded existential quantifier (see [CU]). Also, the instance of the Polynomial Induction $PIND$ with respect to a distinguished free variable x on a formula $\varphi(x)$ is the sentence

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

.

The NP formulas represent precisely the NP relations in the standard model. coNP formulas are defined dually. The theory $(PV)^i$ proves the Principle of Excluded Middle for atomic formulas (of PV).

The classical deductive closure of PV is usually denoted PV_1. CPV is the classical version of IPV.

In the following, the notation $\equiv_i$ between two sets of formulas is used to show that they have the same intuitionistic consequences. Also, $\vdash_i$ denotes provability in intuitionistic (first-order) logic.

If Γ is a set (collection) of formulas, $\neg\Gamma$ denotes the set of formulas of the form $\neg\varphi$ with $\varphi \in \Gamma$.

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].

For a set T of sentences, a T-normal Kripke model is a Kripke model in which all the worlds (classically) satisfy T.

2 Polynomial induction versus length minimization

In this section we work in the language of PV. Also, $(PV)^i$ is the underlying theory for all intuitionistic theories we will mention.

The instance of the length minimization $LMIN$ with respect to a distinguished free variable x on a formula $\varphi(x)$ is the sentence

$\exists x\varphi(x) \to [\varphi(0) \vee \exists x(\varphi(x) \wedge (\forall z \leqslant \llcorner \frac{x}{2} \lrcorner)\neg\varphi(z))]$.

We will compare intuitionistic schemes of polynomial induction and length minimization on NP formulas. By $\neg\neg LMIN(\mathrm{NP})$, we denote the intuitionistic theory axiomatized by PV plus the set of all doubly negated instances of $LMIN$ on NP formulas.

Proposition 2.1 If $\mathcal{K} \Vdash \neg\neg LMIN(\mathrm{NP})$ is linear, then the union of the worlds in $\mathcal{K}$ satisfies CPV.

Proof First note that $(PV)^i$ is contained in the theory $\neg\neg LMIN(\mathrm{NP})$ by our assumption, so each of the nodes in $\mathcal{K}$ forces $(PV)^i$. But $(PV)^i$ is a universal theory, so each node satisfies the classical deductive closure of $(PV)^i$, i.e. PV_1. Therefore, the union of the worlds in $\mathcal{K}$ satisfies PV_1. Recall that $CPV \equiv_c PV + PIND(\mathrm{coNP})$. So, it is enough to show that $PIND(\mathrm{coNP})$ holds in the union. Assume that the union does not satisfy $PIND(A(x))$, for some coNP formula A. Here, it is possible that A has other free variables, besides the one explicitly shown. Let A be of the form $\forall y B(y,x)$, where B is a quantifier-free formula. Assume C to be the formula $\exists y\neg B(y,x)$, an NP formula. There would exist a node M_γ present in $\mathcal{K}$ and some $a \in M_\gamma$, such that (a) $M_\gamma \vDash \neg C(0) \wedge C(a)$ and (b) the union satisfies $\forall x(\neg C(\llcorner \frac{x}{2} \lrcorner) \to \neg C(x))$ (here we have replaced all other free variables of C with parameters from M_γ). We have $\gamma \Vdash C(a)$ (because forcing and truth of $C(a)$ are equivalent) and $\gamma \Vdash \neg C(0)$ (since the union satisfies $\forall y B(y,0)$). Therefore, by $\mathcal{K} \Vdash \neg\neg LMIN(\mathrm{NP})$, we get

$$\gamma \Vdash \neg\neg\exists x(C(x) \wedge \forall z \leq \llcorner \tfrac{x}{2} \lrcorner \neg C(z)).$$

In particular, for some $\delta \geq \gamma$ and some (necessarily nonzero) $d \in M_\delta$, $\delta \Vdash C(d) \wedge \forall z \leq \llcorner \frac{d}{2} \lrcorner \neg C(z)$.

Therefore, the union satisfies $\neg C(\llcorner \frac{d}{2} \lrcorner)$. On the other hand, by $\delta \Vdash C(d)$, $M_\delta \vDash C(d)$. Hence, the union satisfies $C(d)$. The combination of these two leads to a contradiction to (b).□

It is known that CPV proves $LMIN(\mathrm{NP})$. Here, we show that even $\neg\neg LMIN(\mathrm{NP})$ is not provable in IPV under some plausible complexity-theoretic assumption.

Theorem 2.2 $IPV \nvdash \neg\neg LMIN(\mathrm{NP})$, unless $CPV = PV_1$.

Proof Assume $IPV \vdash \neg\neg LMIN(\mathrm{NP})$. Any ω-chain of (classical) models of CPV can be considered as a Kripke model of IPV whose underlying accessibility relation has order type ω (the proof is straightforward, see [M2]). Now, by the assumption, this model forces $\neg\neg LMIN(\mathrm{NP})$ as well, hence by 2.1, the union of its worlds should satisfy CPV. This shows that CPV is an inductive theory. Hence, using the well-known characterization of the inductive theories (see e.g. [CK, Th. 3.2.3]), CPV should be $\forall_2$. Now, using $\forall_2$-conservativity of CPV over PV_1 (see [B1, Th. 5.3.6 and Coro. 6.4.8]), we get $CPV \equiv PV_1$ which is what we wanted. □

It is known that, under the assumption $CPV = PV_1$, the polynomial hierarchy CPV-provably collapses, see [K, Theorem 10.2.4].

Here we state a small result which is a converse to Proposition 2.1.

Proposition 2.3 If $\mathcal{K} \Vdash (PV)^i$ and the union of the worlds in any path of $\mathcal{K}$ satisfies CPV, then $\mathcal{K} \Vdash PIND(\mathrm{coNP})$.

Proof Note that a coNP formula is forced at a node α of a Kripke model of PV if and only if it is satisfied in the union of the worlds in any path above α. □

Theorem 2.4 $PV + LMIN(\mathrm{NP}) \vdash_i PIND(\mathrm{coNP})$.

Proof The proof is similar to the one for Proposition 2.1. Let $\mathcal{K} \Vdash PV + LMIN(\mathrm{NP})$. Consider an arbitrary coNP formula $A(x, \overline{y})$. Assume α is an arbitrary node in $\mathcal{K}$ and $\overline{b} \in M_\alpha$. Suppose also that $\alpha \Vdash A(0, \overline{b}) \wedge \forall x(A(\llcorner \frac{x}{2} \lrcorner, \overline{b}) \rightarrow A(x, \overline{b}))$. We shall show that $\alpha \Vdash \forall x A(x, \overline{b})$. If for every $\beta \geqslant \alpha$, $M_\beta \vDash A(x, \overline{b})$, then we have $\alpha \Vdash \forall x A(x, \overline{b})$. Suppose not. Assume $\eta \geqslant \alpha$ does not have the mentioned property. Let $A(x, \overline{b})$ be of the form $\forall z B(x, z)$, where B is a quantifier-free formula. Assume $C(x)$ to be the formula $\exists z \neg B(x, z)$, an NP formula.

We have $M_\eta \nVdash C(0)$ and $M_\eta \Vdash C(a)$ for some $a \in M_\eta$. Hence, by $\mathcal{K} \Vdash LMIN(\mathrm{NP})$, we get $\eta \Vdash \exists x(C(x) \wedge \forall z \leq \llcorner \frac{x}{2} \lrcorner \neg C(z))$. Clearly, such a node η forces $PIND(A(x, \overline{b}))$.□

Corollary 2.5 $\neg\neg LMIN(\mathrm{NP}) \vdash_i PIND(\mathrm{coNP})$.

Proof Using the general equivalence $\neg\neg(A \to B) \equiv_i (A \to \neg\neg B)$, it is easy to see that in $(PV)^i$, $\neg\neg PIND(A(x)) \equiv_i PIND(A(x))$ for any coNP formula A. Now, Theorem 2.4 immediately implies what we want. □

3 Unprovability of NPB in $PV + PIND(\mathrm{NP}\cup\mathbf{co}\mathrm{NP})$

Let f be a one-place function symbol of IPV. Suppose f is provably an increasing function and provably dominates any polynomial growth rate function. Let $NPB(f)$ be the formula

$\forall x \exists y (x \leqslant y \wedge TAUT(y) \wedge \forall z (z \leqslant f(y) \to \neg z \vdash_{e\mathcal{F}} y))$.

Here $TAUT(y)$ states that y is the Godel number of a propositional tautology and $z \vdash_{e\mathcal{F}} y$ states that z is the Godel number of an extended Frege proof of the formula coded by y, see [K] for the definitions. In the sequel, we fix f and write NPB instead of NPB_f.

Cook and Urquhart [CU, Th. 10.16] proved that, $IPV \nvdash NPB$ using their characterization of provably total functions of IPV. Krajicek and Pudlak proved that $PV_1 \nvdash NPB$ by constructing a chain of models of PV_1 such that the union of its worlds does not satisfy NPB, see [K]. Buss [B2] used the model theoretic method of Krajicek and Pudlak and also used Kripke models to show that $IPV^+ \nvdash \neg\neg NPB$. The theory IPV^+ which was introduced by Buss [B2] apparently is stronger than IPV and is sound and complete with respect to CPV-normal Kripke structures. Here, we use a simple model theoretic proof to show $PV + PIND(NP\cup coNP) \nvdash_i NPB$. This theory is actually equivalent to the theory IPV^*, which is by definition the intuitionistic theory axiomatized by $PV + PIND(NP \cup \neg\neg NP)$, originally mentioned in [CU] and studied in [M1]. The reason is that, by [M2, Theorem 2.3], $PV + PIND(\mathrm{coNP}) \equiv_i PV + PIND(\neg\neg\mathrm{NP})$. The proof of [M1, Theorem 2.5] actually shows that $IPV^+ \nvdash IPV^*$ unless $CPV = PV_1$.

NPB is intuitionistically equivalent to $\forall x \exists y \forall z \mathrm{NPB_M}$. Here NPB_{M} is an atomic formula formalizing "$x \leqslant y$, and z is a satisfying assignment of y, and if $z \leqslant f(y)$ then z is not an extended Frege proof of y". Below, we work with this form of NPB.

Theorem 3.1 $PV + PIND(NP\cup\mathrm{coNP}) \nvdash_{\mathrm{i}} \mathrm{NPB}$

Proof Let $M \vDash PV_1 + \neg NPB$ be countable. Such a model exists by the above mentioned result of Krajicek and Pudlak. Extend M Σ_1^b-elementarily to a model of CPV, for existence of such a model see [K, Theorem 7.6.3]. Now, consider the obvious two-node Kripke model. It is easy to see that this Kripke model forces $PV + PIND(\mathrm{NP}\cup\mathrm{coNP})$. On the other hand this model does not force the prenex sentence NPB since otherwise its root-model would satisfy this sentence, which is a contradiction. □

Note that the Kripke model constructed in the above Theorem forces IPV^+ if and only if $M \vDash CPV$, see [M1, Theorem 2.2].

Here we just mention that, by the following theorem, which is the main result of [CU], all prenex consequences of IPV are already provable in $(PV)^i$:

Theorem 3.2 (Cook and Urquhart, [CU])

(i) If f is a polynomial time computable function then f is Σ_1^{b+}-definable in IS_2^1.

(ii) If $IS_2^1 \vdash \forall \overline{x} \exists y \phi(\overline{x}, y)$ then there is a polynomial time computable function f such that $IS_2^1 \vdash \forall \overline{x} \phi(\overline{x}, f(\overline{x}))$.

Note that, in part (ii) above, the function symbol f does not belong to the language of IS_2^1; however by part (i), it can be expressed in the language.

Acknowledgements

My thanks to Shahid Beheshti university, Tehran, Iran, for financial support.

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.

[CK] C.C. Chang and J. Keisler, Model theory, North-Holland, 1990.

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

[K] J. Krajicek, 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.

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