On Two Questions About Feasibly Constructive Arithmetic

Morteza Moniri

Institute for Studies in Theoretical Physics and Mathematics (IPM),

P.O. Box 19395-5746, Tehran, Iran

email: ezmoniri@ipm.ir

Abstract

IPV is the intuitionistic theory axiomatized by Cook's equational theory PV plus $PIND$ on NP-formulas. Two extensions of IPV were introduced by Buss and by Cook and Urquhart by adding $PIND$ for formulas of the form $A(x) \vee B$, respectively $\neg\neg A(x)$, where $A(x)$ is NP and x is not free in B. Cook and Urquhart posed the question of whether these extensions are proper. We show that in each of the two cases the extension is proper unless the polynomial hierarchy collapses.

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

Key words: First-Order Arithmetic; Feasibly Constructive Arithmetic; Kripke model; Polynomial Hierarchy; Polynomial Induction; NP-Formula; Negative Translation.

1 Introduction

The theory CPV is the conservative extension of Buss's theory S^1_2 obtained by adding function symbols for polynomial time functions and adding defining equations for the new function symbols. Equivalently, CPV is the theory axiomatized by Cook's theory PV plus $PIND$ on NP-formulas. Here, an NP-formula is a formula of the form $(\exists x \leqslant t)(r = s)$ with the usual restrictions on the variables. The theory IPV is the intuitionistic counterpart of CPV in the latter form.

An intuitionistic extension IPV^+ of IPV was defined in [B] which includes PV and has the $PIND$ axioms for formulas of the form $A(x) \vee B$, where $A(x)$ is an NP-formula and x is not free in B. Buss proved that this theory is sound and complete with respect to CPV-normal (i.e. locally CPV) Kripke structures, see [B, Th. 3 and 5].

Another extension of IPV was introduced by Cook and Urquhart which includes $PIND$ for formulas of the form $\neg\neg A(x)$, where $A(x)$ is an NP-formula, besides NP-$PIND$, see [CU]. Let us denote this theory IPV^*.

Cook and Urquhart argued that IPV is a good candidate for formalizing the notion of feasibly constructive proof for sentences expressed in first order arithmetic. On the

other hand, they mentioned that it is difficult philosophically to argue that these two more general induction schemes are not feasible.

They raised the question of whether these extensions are proper, see Chapter 0 of [CU]. Below, we show that in each of the two cases if the extension is not proper, then $CPV = PV_1$. The theory PV_1 can be considered as PV conservatively extended to first-order classical logic and so is a $\forall_1$-theory. This will be done by using Kripke models. We know that if $CPV = PV_1$, then the polynomial hierarchy collapses, by a result of Krajicek, Pudlak, and Takeuti (see [K, Th. 10.2.4]).

We refer to [B] and [CU] for more detailed versions of the definitions of the theories we use. We refer to [B] also for the definition of Kripke models and basic facts about them. The definition of the negative translation and basic facts about it can be found in [TD]. We will use this translation in the next section.

2 IPV^+ and IPV^* versus IPV

First we compare the theories IPV and IPV^+. The following easy Lemma shows that they are classically equivalent.

Lemma 2.1 The classical closure of IPV^+ is equivalent to CPV.

Proof This can be seen easily since one can classically decide any formula. More precisely, assume $M \vDash CPV$ and consider an instance of $PIND$ on a formula of the form $A(x) \vee B$, where $A(x)$ is an NP-formula and B is a sentence (both possibly with parameters from M). Now consider two cases $M \vDash B$ or $M \vDash \neg B$. It is easy to see that in each of the two cases $M \vDash (A(x) \vee B) - PIND$. $\square$

Theorem 2.2 If $IPV \vdash IPV^+$ then $CPV = PV_1$.

Proof Assume CPV is a proper extension of PV_1. Suppose $M \vDash PV_1$ and $M \nvDash CPV$. We can assume without loss of generality that M is countable. There is a Σ^b_1-elementary extension M^* of M such that $M^* \vDash CPV$, see [K, Th. 7.6.3]. Consider the two-node Kripke structure obtained by putting M^* above M. We show that this Kripke structure forces IPV. It forces PV since PV is $\forall_1$-axiomatized. Also, $M^* \Vdash IPV^+$ by the above Lemma. Suppose M forces the assumptions of an instance of $PIND$ on a formula $A(x, \overline{b})$ of the form $(\exists y \leqslant t)(r = s)$ where $\overline{b} \in M$. Suppose also that M does not force $\forall x A(x, \overline{b})$. Hence, by definition of forcing, $M \nvDash A(c, \overline{b})$ for some $c \in M$. Thus $M^* \nvDash A(c, \overline{b})$ since the extension is Σ^b_1-elementary. This is a contradiction since M^* clearly forces this formula.

Now we show that the Kripke model does not force IPV^+. By $M \nvDash CPV$, there is an NP-formula $A(x)$, possibly with parameters from M, such that M does not satisfy the $PIND$ axiom for $A(x)$. So $M \vDash A(0)$, $M \vDash \forall x(A(\llcorner \frac{x}{2} \lrcorner) \rightarrow A(x))$, but $M \nvDash \forall x A(x)$. Hence $M^* \nvDash \forall x A(x)$. Define $C = \exists x(A(\llcorner \frac{x}{2} \lrcorner) \wedge \neg A(x))$. We show that $M \nVdash (A(x) \vee C) - PIND$.

Claim 1 We have $M \nVdash C$ but $M^* \Vdash C$.

Proof of Claim 1 $M \nVdash C$ since $M \nvDash C$ (note that $M \Vdash A(d)$ if and only if $M \vDash A(d)$, for any $d \in M$).

To show that $M^* \Vdash C$, recall that $M^* \nvDash \forall x A(x)$ but $M^* \vDash A(0)$ and $M^* \vDash A(x) - PIND$. So $M^* \vDash C$. Therefore, $M^* \Vdash C$.

Claim 2 We have $M \nVdash (A(x) \vee C) - PIND$.

Proof of Claim 2 $M \Vdash (A(0) \vee C)$ because $M \Vdash A(0)$. $M \nVdash \forall x(A(x) \vee C)$ because $M \nvDash \forall x A(x)$ and $M \nVdash C$. So, to prove the claim, it is enough to show that $M \Vdash \forall x((A(\llcorner \frac{x}{2} \lrcorner) \vee C) \rightarrow (A(x) \vee C))$. We must show that

(i) $\forall d \in M$, $M \Vdash ((A(\llcorner \frac{d}{2} \lrcorner) \vee C) \rightarrow (A(d) \vee C))$ and

(ii) $\forall e \in M^*$, $M^* \Vdash ((A(\llcorner \frac{e}{2} \lrcorner) \vee C) \rightarrow (A(e) \vee C))$.

By Claim 1, $M^* \Vdash C$ so we get (ii). To prove (i), assume $M \Vdash ((A(\llcorner \frac{d}{2} \lrcorner) \vee C)$ for some $d \in M$. Then $M \vDash A(\llcorner \frac{d}{2} \lrcorner)$ because $M \nVdash C$. Thus by $M \vDash \forall x(A(\llcorner \frac{x}{2} \lrcorner) \rightarrow A(x))$, we get $M \vDash A(d)$. Hence, $M \Vdash A(d) \vee C$. $\square$

Now we compare the theories IPV and IPV^*. First we express two useful results.

Proposition 2.3 The theory IPV^* is closed under the negative translation.

Proof To see this note that atomic formulas are decidable in IPV and so clearly the negative translation of each axiom of PV is equivalent to the same axiom. Moreover, the negative translation of each NP-formula A, in IPV is equivalent to $\neg\neg A$. $\square$

Corollary 2.4 The union of the worlds in any linear Kripke model of IPV^* satisfies CPV.

Proof Let $\mathcal{K}$ be a linear Kripke model of IPV^*. By induction on the complexity of formulas it is easy to see that for each $\exists$-free formula A, $\mathcal{K}$ forces A if and only if some node in $\mathcal{K}$ forces A if and only if the union of the worlds in $\mathcal{K}$ satisfies A. Now to prove the corollary it is enough to note that the negative translation of each formula is classically equivalent to the same formula and is $\exists$-free. $\square$

We next establish the second main result of this paper, concerning the relation between IPV and IPV^*.

Theorem 2.5 If $IPV \vdash IPV^*$ then $CPV = PV_1$.

Proof Suppose $IPV = IPV^*$. Thus each chain of models of CPV produces a linear Kripke model of IPV^* because IPV is sound with respect to CPV-normal Kripke structures. Therefore, by the above corollary, the union of the worlds in the chain must satisfy CPV. Thus, using the well-known model theoretic characterization of $\forall_2$-theories (see [CK, Th. 3.2.3]), we obtain that CPV must be $\forall_2$-axiomatizable. Thus it must be equivalent to PV_1 because CPV is $\forall_2$-conservative over PV_1, see [K, Coro. 7.2.4 and 7.2.6]. This implies that $CPV = PV_1$. $\square$

Acknowledgements I would like to thank the referee for useful suggestions. The present proof of the fact that the Kripke model constructed in Theorem 2.2 does not force IPV^+ belongs to the referee. The original proof of this fact was based on two small lemmas which were deleted in the final version of the paper. This research is supported by Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran.

References

[B] 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, Ann. Pure and Appl. Logic 63 (1993), 103-200.

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

[TD] A. S. Troelstra and D. Van Dalen, Constructivism in Mathematics, An Introduction, Vol. 1, North-Holland, Amsterdam, 1988.