Preservation theorems for bounded formulas

Morteza Moniri

Abstract

In this paper we naturally define when a theory has bounded quantifier elimination, or is bounded model complete. We give several equivalent conditions for a theory to have each of these properties. These results provide simple proofs for some known results in the model theory of the bounded arithmetic theories like CPV and PV_1. We use the mentioned results to obtain some independence results in the context of intuitionistic bounded arithmetic. We show that, if the intuitionistic theory of polynomial induction on strict Π^b_2 formulas proves decidability of Σ^b_1 formulas, then P = NP. We also prove that, if the mentioned intuitionistic theory proves LMIN(Σ^b_1), then P = NP.

2000 Mathematics Subject Classification: 03F30, 03C10, 03F50, 68Q15.

Key words: Bounded Arithmetic, Intuitionistic Logic, Kripke Model, Polynomial Hierarchy, Polynomial Induction, NP, Model Completeness, Quantifier Elimination, Universal Theory.

1 Preliminaries

Assume that any theory T we work with below contains $\leqslant$ in its language and that T proves the following basic properties of $\leqslant$. We assume that T proves that $\leqslant$ is reflexive and transitive. We also assume that for all r and s, there is a term t so that T proves that $r \leqslant t$ and $s \leqslant t$. We further suppose that, for all terms $t(\overline{x}, y)$ and $r(\overline{x})$, there is a term $s(\overline{x})$ such that T proves $y \leqslant r(\overline{x}) \rightarrow t(\overline{x}, y) \leqslant s(\overline{x})$. Bounded quantifiers and bounded formulas are defined in the usual way. By a Σ^b_1 formula we mean a quantifier-free formula prefixed by a bounded existential quantifier. We also call these formulas NP formulas, simultaneously. The reason is that, in this paper, we are mainly concerned with bounded arithmetic theories that use the language of Cook's equational theory PV and have PV as a subtheory. In these theories, the Σ^b_1 formulas are exactly the formulas that define the NP relations in the standard model of natural numbers. The Π^b_1 and coNP notations will be used in the same way.

A theory is said to be *bounded* if it is axiomatizable by a set of bounded formulas. To see a proof of the following fact, see e.g. [B2].

Fact 1.1 (Parikh's Theorem) Let T be a bounded Theory and $A(\overline{x}, y)$ be a bounded formula. Suppose that $T \vdash \forall \overline{x} \exists y A(x, y)$. Then there is a term t such that $T \vdash \forall \overline{x} \exists y \leqslant tA(\overline{x}, y)$.

The theories PV_1 and CPV of bounded arithmetic are the first-order versions of the equational theory theory PV, and Buss's theory S^1_2 conservatively extended to the language of PV, respectively. It is known that PV_1 is a universal theory, and CPV is $\forall\exists$-conservative over PV_1.

The theory IPV is defined as CPV but over intuitionistic logic. CPV is $\forall\exists$-conservative over IPV. For more on IPV, see [CU], [B3], [B4] and [A1]. For a semantical investigation of this theory, see [M1], where Kripke models of intuitionistic bounded arithmetic is studied.

2 Some model theory for bounded formulas

In this chapter, we define bounded versions of some well-known notions in model theory, and prove modifications of some well-known theorems of model theory in the context of bounded formulas. These theorems, in some sense, extend the corresponding theorems concerning bounded arithmetic theories which can be proved using the relations between bounded arithmetic and propositional proof complexity, see e.g. [K].

Definition 2.1 Let T be a theory. T has *bounded quantifier elimination* if any bounded formula is T-equivalent to a quantifier-free formula (with the same free variables).

The following proposition can be easily proved via induction on the quantifier complexity of the prenex bounded formulas.

Proposition 2.2 A theory T has bounded quantifier elimination if any Σ^b_1 formula is T-equivalent to a quantifier-free formula (with the same free variables).

As an example of a theory which has bounded quantifier elimination, one can consider the (first-order) theory PRA (Primitive Recursive Arithmetic). The language of PRA contains a function symbol for each primitive recursive function and the theory has defining axioms for these functions. For more on PRA, see e.g. [A2] and [TD].

The theory PRA is not bounded. There is also a simple way to construct a theory which is bounded and at the same time has bounded quantifier elimination. This method is similar to the way that in the basic model theory one can extend a theory to a theory in a extended language and with quantifier elimination. Let T be a bounded theory in a language L. For each bounded L-formula $\varphi(\overline{x})$, add a new predicate symbol $R_\varphi(\overline{x})$ to L to obtain a language L'. Also, for each such φ, add a new axiom $\forall \overline{x}(\varphi(\overline{x}) \leftrightarrow R_\varphi(\overline{x}))$ to T to obtain a new (bounded) theory T' in the language L'. It is easy to see that T' has bounded quantifier elimination.

Definition 2.3 Let T be a theory. A model M of T is called *bounded existentially closed* if whenever N is a model of T such that $M \subseteq N$, then $M \subseteq_1^b N$, i.e. for any Σ_1^b formula $\varphi(\overline{x})$ with parameters from M, if $N \vDash \varphi(\overline{a})$, then $M \vDash \varphi(\overline{a})$, where $\overline{a} \in M$.

By a well-known result in model theory, any model of a universal theory can be embedded in an existentially closed model of that theory (see e.g. [CK, Lemma 3.5.7]). As a consequence, any model of PV can be embedded in a bounded existentially closed model of PV. In such a model, the extended Frege propositional proof system EF is complete, see [K, Corollary 15.3.10 and Theorem 15.3.12].

Definition 2.4 A theory T is called *bounded model complete* if whenever $M \subseteq N$ are models of T, then $M \subseteq_1^b N$.

As an example of a theory which is bounded model complete, one can consider the theory PA (Peano Arithmetic). By the famous MRDP theorem, any bounded formula in PA is equivalent to a $\exists$-formula, and so, if $M \subseteq N$ are models of PA, then N is a bounded elementary extension of M (see e.g. [HP]).

The following theorem is similar to a famous result in model theory characterizing model complete theories (see e.g [CK, Theorem 3.5.1]).

Theorem 2.5 Let T be a bounded theory. The following are equivalent.

(1) T is bounded model complete.

(2) Every model of T is a b.e.c. model of T.

(3) For any Σ_1^b formula there is a T-equivalent Π_1^b formula.

(4) For any bounded formula there is a T-equivalent Π_1^b formula.

Proof We only give the proof for the case (1) implies (3). The other parts are straightforward and similar to the ones for the unbounded version of this theorem. Let $\exists x \leqslant t\varphi(x, \overline{w})$ be a Σ_1^b formula. By the assumption and a basic result in model theory characterizing universal formulas (see e.g. [Ho, Theorem 5.4.4]), there is a universal formula $\forall y\psi(y, \overline{w})$ such that $T \vdash \forall y\psi(y, \overline{w}) \leftrightarrow \exists x \leqslant t\varphi(x, \overline{w})$. From $T \vdash \forall y\psi(y, \overline{w}) \rightarrow \exists x \leqslant t\varphi(x, \overline{w})$, we have $T \vdash \exists y \exists x \leqslant t(\psi(y, \overline{w}) \rightarrow \varphi(x, \overline{w}))$. Now, using the fact that T is a bounded theory, by Parikh's theorem (Fact 1.1), there is a term s such that $T \vdash \exists y \leqslant s \exists x \leqslant t(\psi(y, \overline{w}) \rightarrow \varphi(x, \overline{w}))$. So $T \vdash \forall y \leqslant s\psi(y, \overline{w}) \rightarrow \exists x \leqslant t\varphi(x, \overline{w})$. Therefore, $T \vdash \forall y \leqslant s\psi(y, \overline{w}) \leftrightarrow \exists x \leqslant t\varphi(x, \overline{w})$. ■

Corollary 2.6 Let T be a bounded theory which is bounded model complete. Then T is $\forall\Sigma_1^b$-axiomatizable.

Proof Using the fact that T is a bounded theory and Theorem 2.5 (4), one can see that the class of models of T is closed under union of chains. So, by a well-known result

in model theory, T is $\forall\exists$-axiomatizable. Now Parikh's theorem guarantees that T is $\forall\Sigma^b_1$-axiomatizable. ■

Corollary 2.7 If PV_1 is not equal to CPV, then there exist models M and N of CPV such that $M \subseteq N$ but not $M \subseteq^b_1 N$.

Proof If PV_1 is not equal to CPV, then CPV is not $\forall\Sigma^b_1$-axiomatizable. ■

NOTE The above result can also be proved via some known results in bounded arithmetic as follows. We refer to [K] for the proofs of all mentioned facts. If PV_1 is not equal to CPV, then PV_1 does not prove $\mathrm{P} = \mathrm{NP}$, since PV_1 proves polynomial induction on the quantifier-free formulas. So, $\mathrm{CPV} \nvdash \mathrm{P} = \mathrm{NP}$ as CPV is a $\forall\exists\Delta^b_1$-conservative extension of PV_1 and $\mathrm{P} = \mathrm{NP}$ is a $\forall\exists\Delta^b_1$ sentence. Therefore, $\mathrm{CPV} \nvdash \mathrm{NP} = \mathrm{coNP}$ because $\mathrm{CPV} \vdash \mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$. So, there is a model of CPV in which the extended Frege system is not complete. Hence, it is not the case that any extension of the mentioned model is Σ^b_1 elementary.

3 Some intuitionistic consequences

In this section we prove some independence results in the context of intuitionistic bounded arithmetic using the results proved in Chapter 2. Our proofs are based on Kripke model theory for these theories. In the context of intuitionistic bounded arithmetic, where quantifier-free formulas are decidable, Kripke models are normal, i.e. the interpretation of $=$ in each world is true equality, and the accessability relation is substructure. For more on Kripke models of intuitionistic bounded arithmetic, we refer the reader to [B3] and [M1].

Cook and Urquhart [CU] proved that if the theory IPV proves the principe PEM of excluded middle for Σ^b_1 formulas, then $\mathrm{P} = \mathrm{NP}$. Below, we prove a similar result for a stronger theory.

Recall that the instance of the *length-minimization* LMIN with respect to a distinguished free variable x on a formula $\varphi(x)$ (which may have more free variables) is the universal closure of the formula

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

By a *strict* Π^b_2 formula, denoted $s\Pi^b_2$, we mean a formula of the form

$\forall x \leqslant t \exists y \leqslant s\varphi(x, y)$, where φ is a quantifier-free formula.

Recall that the theory S^2_2 proves polynomial induction on all Π^b_2 formulas, see [B1] for the definition of the hierarchy of bounded arithmetic formulas and the mentioned result.

Theorem 3.1 If the intuitionistic theory of BASIC + PIND($s\Pi^b_2$) proves PEM(Σ^b_1), then $S^2_2 \vdash P = NP$.

Proof First we show that if $M \subseteq N$ are models of S^2_2, then the two node tower can be considered as a Kripke model of BASIC + PIND($s\Pi^b_2$). For this, assume that $\psi(x)$ is a $s\Pi^b_2$ formula with possible parameters from M (and with x as the only free variable). Using the definition of forcing, one can easily see that $\psi(a)$, for $a \in M$, is forced in M if and only if $\psi(a)$ is satisfied in M and N. Assume for the purpose of a contradiction, that PIND($\psi(x)$) is not forced in M. So $\psi(0)$ and $\forall x(\psi(\llcorner \frac{x}{2} \lrcorner) \rightarrow \psi(x))$ are forced in M, but $\forall x \psi(x)$ is not forced in M. So $\forall x \psi(x)$ is not satisfied in M since it should be satisfied in N as forcing and satisfaction are equivalent in N. Now, using LMIN on the Σ^b_2 formula $\neg\psi(x)$ which is available by [B1, Theorem 2.8.17], there exists an $a \in M$ such that $M \nVdash \psi(a)$ and for any $b \in M$ with the condition $b \leqslant \llcorner \frac{a}{2} \lrcorner$, $M \vDash \psi(b)$. In particular, $M \vDash \psi(\llcorner \frac{a}{2} \lrcorner)$. So, $M \Vdash \psi(\llcorner \frac{a}{2} \lrcorner)$. Therefore, by $M \Vdash \forall x(\psi(\llcorner \frac{x}{2} \lrcorner) \rightarrow \psi(x))$, we have $M \Vdash \psi(a)$, contradiction.

So, if the intuitionistic theory of BASIC + PIND($s\Pi^b_2$) proves PEM(Σ^b_1), then the two-node Kripke model forces PEM(Σ^b_1), and so one can easily see that $M \subseteq^b_1 N$. Hence, we proved that the relation between any two models $M \subseteq N$ of S^2_2 is Σ^b_1-elementary extension. Now use Theorem 2.5 and the fact CPV $\vdash$ P = NP $\cap$ coNP. ■

The above result implies that, if P $\neq$ NP, then BASIC + PIND($s\Pi^b_2$) $\nvdash_i$ PIND(Π^{b+}_2). The reason is that, as mentioned in [Ha], Cook proved that the intuitionistic theory of BASIC + PIND(Π^{b+}_2) proves decidability of Σ^b_1 formulas. Here, Π^{b+}_2 denotes the class of positive Π^b_2 formulas. A formula is positive if it does not contain $\neg$ and $\rightarrow$.

It is known that S^2_2 proves the scheme length-minimization for Σ^b_2 formulas (see [B1, Theorem 2.8.17]). Here we show that even LMIN(Σ^b_1) is not derivable in the intuitionistic theory of BASIC + PIND($s\Pi^b_2$), unless P = NP. In [M2], it is proved that a weak form of LMIN(Σ^b_1) is not derivable in IPV under the assumption that PV_1 is not equal to CPV (and so, unless the polynomial hierarchy collapses by [KPT]).

Theorem 3.2 If the intuitionistic theory of BASIC + PIND($s\Pi^b_2$) proves LMIN(Σ^b_1), then $S^2_2 \vdash P = NP$.

Proof Assume that $S^2_2 \nvdash P = NP$. So, there exist models M and N of S^2_2 such that $M \subseteq N$ but not $M \subseteq^b_1 N$. Let σ be an $L(M)$-sentence which is Σ^b_1 and satisfied in N but not in M. Let K be the Kripke model of BASIC + PIND($s\Pi^b_2$) obtained by putting N above M (see prove of the above Theorem) . Let $\varphi(x)$ be the Σ^b_1 formula $x = 2 \vee \sigma$. We show that K does not force the instance of LMIN on $\varphi(x)$. It is easy to see that M (resp. N) forces $\varphi(a)$, for $a \in M$, if and only if M (resp. N) satisfies $\varphi(a)$.

So we have $M \nVdash \varphi(0)$, $M \nVdash \varphi(1)$, and $M \Vdash \varphi(2)$. Moreover, $M \nVdash \neg\varphi(0)$ and

$M \nVdash \neg\varphi(1)$. Therefore $K \nVdash \mathrm{LMIN}(\varphi(\mathrm{x}))$. ■

Acknowledgements I would like to thank the referee for useful suggestions. This research was in part supported by a grant from IPM (No. 84030114).

References

[A1] J. Avigad, Interpreting Classical Theories in Constructive Ones, Journal of Symbolic Logic, 65 (2000) 1785-1812.

[A2] J. Avigad, Saturated Models of Universal Theories, Annals of Pure and Applied Logic 118 (2002), 219-234.

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

[B2] S. R. Buss, First-Order Proof Theory of Arithmetic, Handbook of proof theory, 79–147, Stud. Logic Found. Math., 137, North-Holland, Amsterdam, 1998.

[B3] 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.

[B4] S. R. Buss, A Note on Bootstrapping Intuitionistic Bounded Arithmetic, Proof theory (Leeds, 1990), 149-169, Cambridge University Press, Cambridge, 1992.

[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.

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

[Ho] W. Hodges, A Shorter Model Theory, Cambridge University Press, Cambridge, 1997.

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

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

[KPT] J. Krajíček, P. Pudlák and G. Takeuti, Bounded Arithmetic and the Polynomial Hierarchy, International Symposium on Mathematical Logic and its Applications (Nagoya, 1988), 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, Polynomial Induction and Length Minimization in Intuitionistic Bounded Arithmetic, Mathematical Logic Quarterly, 51 (2005) 73-76.

[TD] A. S. Troelstra and D. van Dalen, Constructivism in Mathematics, vol. 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 **AND** m-moniri@cc.sbu.ac.ir