Propositional Provability and Models of Weak Arithmetic

Jan Krajíček and Pavel Pudlák
Mathematical Institute at Prague

We connect a propositional provability in models of weak arithmetics with the existence of $\Delta^b_1$-elementary, non-$\Sigma^b_1$-elementary extensions. This is applied to demonstrate that certain lower bounds to the length of propositional proofs are not provable in weak systems of arithmetic (Corollary 4).

§1. Introduction

$S^1_2$ is the fragment of bounded arithmetic introduced in [1]. The language of this theory contains symbols 0, $s(x)$, $x + y$, $x \cdot y$, $|x|$, $x \frac{1}{2^y}$, $x \neq y$ and $=$, $\leq$, where the meaning of $|x|$ is $\lceil \log_2(x + 1) \rceil$ and $x \neq y$ is $2^{\lfloor x \rfloor} \cdot |y|$. The theory is axiomatized by 32 open axioms BASIC and the induction scheme PIND:

$$\phi(0) \& \forall x(\phi(\frac{x}{2^j}) \rightarrow \phi(x)) \rightarrow \forall x\phi,$$

where $\phi(x)$ is a $\Sigma^b_1$-formula.

$\Sigma^b_1$-formulas define in the standard model $\omega$ exactly NP-predicates. Scheme PIND is slightly weaker than the usual scheme of induction.

*The work was performed while the first author was visiting Department of Mathematics, University of Illinois at Urbana.*
Theory $S^1_2$ is closely related to the equational theory $PV$ introduced in [4]. Using the scheme of limited recursion on notation one can define in $PV$ a function symbol for every $PTIME$–function. Since predicates can be represented by their characteristic functions, all universal statements about $PTIME$–predicates are represented in $PV$. In fact, using witnessing functions, one can represent statements of higher quantifier complexity too. In [1] it is shown that a $\forall \Sigma^b_1$–sentence is provable in $S^1_2$ iff the corresponding equation (containing the witnessing function) is provable in $PV$. Thus $S^1_2$ is in a sense partially conservative over $PV$.

In [1, 4] it was demonstrated that $PV$ and $S^1_2$ are rather powerful theories, e.g. one can formalize syntax and the notion of Turing machine and prove their basic properties there. Note also that $PV_1$ from [12] is fully conservative over $PV$.

Our aim here is to investigate what can be proved about the problem $NP = coNP$? in theories like $PV$ and $S^1_2$ and, in particular, how strong scheme of induction is consistent with $NP = coNP$. There are two important results which should be mentioned here.

The first one is a result of Cook [4] which can be roughly stated as follows: If $PV$ proves $NP = coNP$ then propositional tautologies $TAUT$ have polynomially long proofs in the extended Frege system $EF$. This means that we know in advance which $NP$–algorithm would accept the $coNP$–complete set $TAUT$, if $NP = coNP$ would be provable in $PV$. The system $EF$ is the usual textbook axiomatic propositional calculus augmented by the extension rule allowing to abbreviate long propositions by new atoms, for details see [5].