Extensions of Models of *PV*

Jan Krajíček*

Mathematical Institute and Institute of Computer Science
Academy of Sciences of the Czech Republic
Zitná 25, 115 67 Praha 1, Czech Rep
krajicek@cesnet.cz

Abstract. We prove that certain models of PV in which $NP \not\subseteq P/poly$ have a Π^b_1-elementary extension to a model of (PV and) $NP \not\subseteq coNP/poly$. If S_2 proves a particular fact about bipartite graphs then, in fact, all models of PV in which $NP \not\subseteq P/poly$ have a Π^b_1-elementary extension to a model of $NP \not\subseteq coNP/poly$.

Introduction

PV is a bounded arithmetic theory with function symbols for all polynomial time algorithms, and axiomatized by a particular set of universal formulas, cf. [3]. Models of PV are a natural environment for notions of computational complexity theory around deterministic and non-deterministic polynomial time. Major open problems in this part of complexity theory have their counterparts in bounded arithmetic and propositional logic. We are interested in proving some notorious open conjectures for a model of bounded arithmetic, and not so much in showing that some of these conjectures might be unprovable in bounded arithmetic. For a general motivation (for this author, at least) for research in this area see the preface to [4].

In a model M of the theory PV the class P of the polynomial-time sets is the class of subsets of M definable by an atomic PV-formula with parameters from M (in S^1_2 this would be provably Δ^b_1-formulas with parameters), equivalently: recognizable by a *standard* DTM with an extra input (the parameter) which may be non-standard, equivalently: recognizable by a DTM possibly with a non-standard description but whose time is bounded by a standard degree polynomial.

The class $P/poly$ is defined in the same way except that the parameters may vary with the length of the inputs, and the classes $NP, NP/poly$ and $coNP, coNP/poly$ are defined analogously using $NDTM$'s. In particular, NP-subsets of M (resp. $coNP$) are those definable by Σ^b_1-formulas (resp. by Π^b_1-formulas) with parameters, that may vary with the length in case of $NP/poly$ and $coNP/poly$.

* Partially supported by the *US - Czechoslovak Science and Technology Program* grant # 93025, and by grant #A1019602 of the *AVČR*.