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 Δ_1^b-elementary, non-Σ_1^b-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_2^1 is the fragment of bounded arithmetic introduced in [1]. The language of this theory contains symbols 0, $s(x)$, $x + y$, $x \cdot y$, $|x|$, $\lfloor \frac{x}{2} \rfloor$, $x \# y$ and $=$, $\leq$, where the meaning of $|x|$ is $\lceil \log_2(x + 1) \rceil$ and $x \# y$ is $2^{|x|\cdot|y|}$. The theory is axiomatized by 32 open axioms BASIC and the induction scheme PIND:

$$\phi(0) \;\&\; \forall x(\phi(\lfloor \tfrac{x}{2} \rfloor) \rightarrow \phi(x)) \rightarrow \forall x \phi x,$$

where $\phi(x)$ is a Σ_1^b-formula.

Σ_1^b-formulas define in the standard model ω 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_2^1 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 $\forall\Sigma_1^b$-sentence is provable in S_2^1 iff the corresponding equation (containing the witnessing function) is provable in PV. Thus S_2^1 is in a sense partially conservative over PV.

In [1, 4] it was demonstrated that PV and S_2^1 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_2^1 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 <u>Cook</u> [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].

Via the simulation described above <u>Cook's</u> result transfers to S_2^1. Note that <u>Wilkie</u> [13] proved this result for S_2^1 directly, cf. [10] for a discussion.

This result can also be stated more sharply as follows: If S_2^1 (or PV) proves that an NP-set X is contained in TAUT then there is a polynomial bound to the length of a shortest EF-proof of each τ in X. This means that it is not possible to prove in S_2^1 a super-polynomial lower bound to the length of EF-proofs for any simply defined sequence of tautologies. For details and discussion see [10].

The second result, due to <u>Buss</u> [1], states that P = NP $\cap$ coNP is in a sense consistent with S_2^1: If $S_2^1 \vdash \phi(x) \longleftrightarrow \neg\psi(x)$, where both $\phi(x)$ and $\psi(x)$ are Σ_1^b-formulas, then $\phi(x)$ actually defines a PTime-predicate. However, this does not seem to imply the consistency in the classical sense as we do not have any model of S_2^1 in which P = NP $\cap$ coNP is true. In an earlier paper <u>DeMillo</u> and <u>Lipton</u> [7] showed that Herbrand's theorem gives such a result for theory PT, which is the set of true universal statements about PTime-predicates. However, this is rather weak result as in their model induction fails very badly: standard numbers are PTime-definable.

This paper attempts to pinpoint which consistency results are possible with the present means. We are not able to show that S_2^1 is consistent with NP = coNP but we shall show that in a theory slightly weaker (extending PV) no superpolynomial bounds to the length of EF-proofs are possible.

§2. Results

We shall describe a natural construction which produces a propositional formula (= proposition) $[\varphi]^m$ from a Π_1^b-formula $\varphi(x_1,\dots,x_n)$ and an integer $m \geq 1$. This construction is, essentially, only an extension of the construction of Cook [4] and it is used in [10], where it is denoted by $^*[\ ]^m$ As the construction and its properties have been treated in [10] we shall concentrate on details which are important for this paper.

(1) The translation $[\varphi]^m$ for φ atomic is given by natural boolean circuits computing the corresponding predicate for integers at length $\leq m$; thus $[\varphi]^m$ has a string of length m of propositional variables for each variable of φ, moreover it has propositional variables which code the value of the gates during the computation, hence once we substitute propositional constants 0, 1 (False and True) for the former ones the values of the latter ones are uniquely determined.

(2) If φ is $\alpha \rightarrow \beta$, $\neg\alpha$ etc. then

$$[\varphi]^m \text{ is } [\alpha]^m \rightarrow [\beta]^m,\ \neg[\alpha]^m$$

etc.; further we assume that in case of binary connectives the translations are chosen in such a way that the common propositional variables of $[\alpha]^m$ and $[\beta]^m$ are only those which correspond to common free first order variables of α and β.

(3) If φ is $(\forall x \leq t)\alpha(x)$ resp $(\exists x \leq t)\alpha(x)$ and it is not sharply bounded quantification then $[\varphi]^m$ is

$$[x \leq t \rightarrow \alpha(x)]^{m'} \quad \text{resp.} \quad [x \leq t \,\&\, \alpha(x)]^{m'}$$

where m' is sufficiently large to code numbers less than or equal t evaluated on numbers of length $\leq m$.

(4) If φ is $(\forall x \leq |t|)\alpha(x)$ resp. $(\exists x \leq |t|)\alpha(x)$ then $[\varphi]^m$ is

$$[(\underset{\sim}{0} \leq |t| \rightarrow \alpha(\underset{\sim}{0})) \wedge \cdots \wedge (\underset{\sim}{m'} \leq |t| \rightarrow \alpha(\underset{\sim}{m'}))]^{m'}$$

resp

$$[(\underset{\sim}{0} \leq |t| \,\&\, \alpha(\underset{\sim}{0})) \vee \cdots \vee (\underset{\sim}{m'} \leq |t| \,\&\, \alpha(\underset{\sim}{m'}))]^{m'},$$

where m' is the maximum of m and $|t|$ evaluated on numbers of length $\leq m$, $\underset{\sim}{n}$ denotes the dyadic numeral.

The main property of $[\varphi]^m$ is that it expresses the validity of $\varphi(k_1,\dots,k_n)$ for all $k_1,\dots,k_n$ such that $|k_1|,\dots,|k_n| \leq m$, where we assume that, φ has no other free variables than $x_1,\dots,x_n$. We assume that 0, 1 are constants of our propositional calculus, so instead of taking, say, $[\psi(\underset{\sim}{k})]^m$ we can take $[\psi(x)]^m$ and substitute in it the sequence of 0's and 1's which codes k (i.e. which represents the dyadic numeral $\underset{\sim}{k}$). There is a short proof in EF that these two formulas are equivalent and this is provable in S_2^1. We shall need the following facts about this translation.

Lemma 1 Suppose $\psi(x_1,\dots,x_n) \in \Sigma_1^b$, $\varphi \in \Pi_1^b$ and φ does not contain any free variables of ψ. Then S_2^1 proves:

$$\psi(b_1, \dots, b_n) \ \& \ (EF \vdash [\psi(x_1,\dots,x_n) \rightarrow \varphi]^c) \ \&$$

$$\& \ c \geq \max(|b_1|,\dots,|b_m|) \rightarrow (EF \vdash [\varphi]^c).$$

Proof: First assume that provably in S_2^1, if we have an EF-proof of proposition $\alpha(p_1,\dots,p_k) \rightarrow \beta$, where $p_1,\dots,p_k$ are all free variables of α and do not occur in β, and another EF proof of $\alpha(c_1,\dots,c_k)$ for $c_1,\dots,c_k$ propositional constants, then we have also a proof of β. This follows, for instance, from the substitution rule, which EF simulates (see [10]), and Modus Ponens.

Also provably in S_2^1, if $\alpha(c_1,\dots,c_k)$ is true, then it is provable in EF. This is because $\alpha(c_1,\dots,c_k)$ does not have free variables, hence its truth value can be simply computed and this computation can be presented as a proof in EF.

We reduce the lemma to the above situation, i.e. let $\alpha(p_1,\dots,p_k)$ be $[\psi(x_1,\dots,x_n)]^c$ and β be $[\varphi]^c$. Suppose we work in S_2^1 and let $b_1,\dots,b_n$ be given such that $\psi(b_1,\dots,b_n)$, $|b_1|,\dots,|b_n| \leq c$. As in the definition of [..], part (4), we can replace sharply bounded quantifiers of $\psi(b_1,\dots,b_n)$ by conjunctions and disjunctions. Then there remain only bounded quantifiers which are essentially existential. Thus we can take witnesses for these quantifiers, say $d_1,\dots,d_m$. We substitute 0-1 codes (i.e. bits of dyadic numerals) of $b_1,\dots,b_n$, $d_1,\dots,d_m$ into $\alpha(p_1,\dots,p_k)$. The remaining free

variables are those which correspond to the values of gates of the circuits which compute the atomic formulas, so they are determined easily too. The resulting variable free proposition must have the same truth value as $\psi(b_1,\dots b_n)$, hence it is true and we can apply the above argument to get the proof of $[\varphi]^c$. □

Lemma 2 Let $\varphi(x_1,\dots,x_n) \in \Pi_1^b$ and suppose that:

$$S_2^1 \vdash \varphi(a_1,\dots,a_n)$$

Then:

$$S_2^1 \vdash (EF \vdash [\varphi(x_1,\dots,x_n)]^{|z|})$$

Proof: This follows from the simulation of PV, Cook [4], using the fact that S_2^1 is $\forall\Pi_1^b$-conservative over PV, cf. Buss [1, Thm. 6.7]. The translation of arithmetical formulas obtained in this way is slightly different than the one described above, however EF is not sensitive to such modifications. ■

The following theorem is our main tool

Theorem 1: Assume $\mathbf{M} \models S^1_2$, $a \in \mathbf{M}$ and $\phi(x) \in \Sigma^b_1$ Then (i) and (ii) are equivalent:

(i) There is an extension N of $\mathbf{M}$ which preserves Σ^b_1–formulas and satisfies:

$$N \models S^1_2 + \phi(a).$$

(ii) $\mathbf{M}$ satisfies:

$$\mathbf{M} \models \text{"EF} \not\vdash [\neg\phi(\underset{\sim}{a})]^{|a|}\text{"}$$

Remark: The condition on the extension N in (i) means precisely that if $\psi(x)$ is any Σ^b_1–formula and $b \in \mathbf{M}$ then $\mathbf{M} \models \psi(b)$ implies that $N \models \psi(b)$. It follows that N is Δ^b_1–elementary extension of $\mathbf{M}$ then. Recall also that each PTime set is Δ^b_1–definable in S^1_2, thus PTime predicates are absolute. (Δ^b_1 means equivalent to Σ^b_1 and Π^b_1 in S^1_2.)

Proof: Suppose (i) holds true. The fact that $[\neg\phi(\underset{\sim}{a})]^{|a|}$ expresses the truth of $\neg\phi(a)$ is provable in S^1_2, cf. Lemma 3.2 of [11]. Further the reflection principle for EF proofs (denoted 0–RFN(EF) in [11]) is also provable in S^1_2, see Theorem 5.1 in [11]. If there were an EF–proof of $[\neg\phi(\underset{\sim}{a})]^{|a|}$ in $\mathbf{M}$, then it would also be an EF–proof in N and thus we would get a contradiction.

Now assume that there is no such an extension, i.e.

$$(*) \qquad S^1_2 \quad \mathrm{Diag}_{\Sigma^b_1}(\mathbf{M}) \vdash \neg\phi(a).$$

This means that there are Σ^b_1–formulas $\psi_1(x, y_1, \dots, y_k), \dots, \psi_n(x, y_1, \dots, y_k)$ and $b_1, \dots, b_k \in \mathbf{M}$ such that

$$(1) \qquad \mathbf{M} \models \psi_1(a, b_1, \dots, b_k) \ \& \cdots \& \ \psi_n(a, b_1, \dots, b_k),$$

and

$$(2) \qquad S^1_2 \vdash (\bigwedge_i \psi_i(x, y_1, \dots, y_k)) \quad \neg\phi(x)$$

By Lemma 2, (2) implies that it is provable in S^1_2 that formula

$$[(\bigwedge_i \psi_i(x, y_1, \dots, y_k)) \to \neg\phi(x)]^{|z|}$$

has an EF–proof for every z.

By Lemma 1, in $\mathbf{M}$ there is an EF–proof of

$$[\neg\phi(\underset{\sim}{a})]^c.$$

Finally, as $|a| \le c$, the implication:

$$[\neg\phi(\underset{\sim}{a})]^c \to [\neg\phi(\underset{\sim}{a})]^{|a|}$$

holds in $\mathbf{M}$ and we get a contradiction with (ii)

Let Taut(x) be a Π_1^b formula which formalizes: "x is a propositional tautology".

The following corollary extends a lemma from [13].

Corollary 1 Let $M \models S_2^1$ and $\tau \in M$ such that:

$$M \models \text{"}\tau \text{ is a propositional formula"} \ \& \ EF \not\vdash \tau.$$

Then there is a Δ_1^b-elementary, cofinal extension N of satisfying

$$N \models S_2^1 + \neg\, \mathrm{Taut}(\tau)$$

Proof: Take $\phi(x) := \neg\, \mathrm{Taut}(x)$ and apply Theorem 1 together with the following fact:

$$S_2^1 \vdash ((EF \vdash [\mathrm{Taut}(\underset{\sim}{\tau})]) \longrightarrow EF \vdash \tau),$$

see Lemma 3.4 (ii) in [11] The cofinality of M in N is achieved by possible shortening of N. □

Corollary 2. Let M be a countable model of S_2^1. Then there is a Δ_1^b-elementary, cofinal extension N of M satisfying

(i) $N \models \forall\Sigma_1^b(S_2^1)$,

(ii) $N \models \forall x((EF \vdash x) \equiv \mathrm{Taut}(x))$.

Proof: Under suitable enumeration of all elements of M and newly arrising elements we can construct—via Corollary 1—a chain of Δ_1^b-elementary, cofinal models of S_2^1:

$$M = M_0 \underset{\Delta_1^b,cf}{\prec} M_1 \underset{\Delta_1^b,cf}{\prec} M_2 \prec$$

having the following property: if $\tau \in M_i$ is a propositional formula then for some $j > i$, M_j contains either an EF-proof of τ or a truth assignment satisfying $\neg\tau$.

Thus $N := \bigcup_i M_i$ will satisfy (ii). Condition (i) follows from obvious

$M_i \underset{\Delta_1^b}{\prec} N$ □

Remark: By $\forall\Sigma_1^b(S_2^1)$ we denote the set of all sentences of the form $\forall x\phi(x)$, ϕ a Σ_1^b-formula. Because of the Buss's Theorem [1] these sentences are equivalent with $\forall\exists\Sigma_1^b(S_2^1)$. PV_1 of [12] is fully conservative over $\forall\Sigma_1^b(S_2^1)$.

Since the proof that EF is complete for propositional tautologies can be easily formalized in S_2^1 + Exp, any model of this theory satisfies (ii) above too. ("Exp" is an axiom saying that the exponentiation is a total function, one can take as Exp e.g. the formula $\forall x \exists y,\ x = |y|$.) Thus interesting applications of this Corollary are only in the case when Exp fails in N.

Corollary 3: There is nonstandard model N satisfying (i) and (ii) of Corollary 2 and moreover:

(iii) There is $a \in N$ such that for any $b \in N$ there is $k < \omega$ and it holds:

$N \vdash |b| \leq |a|^k$.

Proof: Apply Corollary 2 with M nonstandard countable model of S_2^1 satisfying (iii). □

In such a model N, in particular, the length of each EF-proof is bounded by some standard polynomial in $|a|$. However, we cannot claim that this shows NP = coNP in N since for different proofs we must take different polynomials. To obtain a uniform bound we have to take a function $f(x)$ which is (provably in S_2^1) superpolynomial. Then, of course, $2^{f(|x|)}$ is not provably total in S_2^1, which diminishes the importance of such a result.

More appropriate interpretation is given in terms of the unprovability of certain lower bounds to the length of EF-proofs in $\forall\Sigma_1^b(S_2^1)$. In order to compare it with a former result of Cook and Urquhart [6] we use similar terminology.

For a function $f(x)$ (with PTime graph definable in S_2^1) take the following formula:

$$\mathrm{Bound}(f) \leftrightarrows [\forall x \exists \tau \geq x;\ \mathrm{Taut}(\tau) \wedge (\forall d,\ |d| \leq f(|\tau|) \rightarrow$$

$$\rightarrow \text{"}d \text{ is not an EF-proof of } \tau\text{"})].$$

Thus Bound(f) formalizes that f is a lower-bound to the length of EF-proofs. Below, function f is S_2^1-provably superpolynomial iff for any $k < \omega$, $S_2^1 \vdash \forall u \exists y > u \exists x \leq y;\ f(x) = y \wedge x^k < y$. Corollary 3 immediately gives:

Corollary 4 Let f be S_2^1-provably superpolynomial. Then

$$\forall\Sigma_1^b(S_2^1) \nvdash \mathrm{Bound}(f). \quad □$$

Similarly $\forall\Sigma_1^b(S_2^1)$ cannot prove the formula:

$$[\forall x \exists \tau \geq x,\ \mathrm{Taut}(\tau) \wedge (\forall d,\ |d| \leq |\tau|^{|x|} \quad \text{"}d \text{ is not an EF-proof of}$$

(Note that the relation "$|d| \leq |\tau|^{|x|}$" is M-definable even if $2^{|\tau|^{|x|}}$ doe not exist in M.) This formula was in [6] shown to be unprovable in an intuitionistic version of S_2^1.

Now we turn our attention to the question how strong induction is available in $\forall\Sigma_1^b(S_2^1)$, (the axiomatization of this system IS_2^1 is different from S_2^1, for details see [6]).

Theorem 2: The usual scheme of induction for Δ_1^b-formulas (w.r.t. S_2^1) is derivable is $\forall\Sigma_1^b(S_2^1)$.

Proof: Buss [1] has shown that such a scheme is derivable in S_2^1 To see that it is equivalent to a $\forall\Sigma_1^b$ formula write it in the form:

$$\forall x \exists y < x((\varphi(0) \wedge (\varphi(y) \rightarrow \varphi(y+1))) \quad \varphi(x))$$

Finally, a formula Δ_1^b w.r.t. S_2^1 is also Δ_1^b w.r.t. $\forall\Sigma_1^b(S_2^1)$ □

Remark: As all PTime predicates are Δ_1^b-definable in S_2^1 we have in ou models induction for them.

§3. Some generalizations

We wish to extend the results from S_2^1 to a stronger theory T. Then we must also take a stronger proof system P for propositional calculus. The following conditions on T and P are sufficient for the derivation of Theorem 1 and its corollaries.

(a) T is a consistent theory in the language of S_2^1 (more generally we may allow any PTime-computable functions in the language of T) and $T \supseteq S_2^1$,

(b) T has a $\prod_1^0$-axiomatization,

(c) T proves the reflection principle for P,

(d) for every $\varphi(x)$ in $\prod_1^b$, if $T \vdash \forall x \varphi(x)$ then $T \vdash \forall y(P \vdash [\varphi]^{|y|})$,

(e) $T \vdash \forall x((EF \vdash x) \rightarrow (P \vdash x))$.

Such a proof system P can be constructed for any true, finitely axiomatizable, T satisfying (a) and (b), see [10]. This covers the fragments S_2^i of bounded arithmetic for which the proof systems are naturally defined fragments of the quantified propositional calculus, see [10, 8]. Moreover, for any true, recursively axiomatizable theory T_0 we can find T and P fulfilling the conditions such that T proves all $\forall \prod_1^b$-consequences of T_0: take $T := S_2^1 + Con_{T_0}$.

On the other hand these generalizations also show the weakness of our results. A significant independence result must depend essentially on the

theory, while here we can take for instance S_2^1 plus the consistency of Zermelo-Fraenkel set theory and still get a result of the same kind.

§4. Open questions

The model N constructed in Corollary 2 has a property which is interesting from the point of view of model theory.

Theorem 3: Let N be a model of $\forall\Sigma_1^b(S_2^1)$ satisfying:

$$(\dagger) \qquad N \vDash \forall x(EF \vdash x \equiv Taut(x)).$$

Then any Δ_1^b-elementary extension of N is already Σ_1^b-elementary.

Proof: In S_2^1 we have, for $\varphi(x)$ a $\prod_1^b$-formula:

$$(*) \qquad \forall x,\ Taut([\varphi(\underset{\sim}{x})]^{|x|}) \equiv \varphi(x)$$

As this equivalence can be written in $\forall\Sigma_1^b$-form, it holds in N. Hence we hav an EF-proof of $[\varphi(\underset{\sim}{a})]^{|a|}$ in N whenever $\varphi(a)$ is true in N. This proof will be in any Δ_1^b-elementary extension of N. As the reflection principle fo EF is also provable in $\forall\Sigma_1^b(S_2^1)$, the validity of $\varphi(a)$ will be preserved to (by (*)).

The validity of Σ_1^b-formulas is preserved automatically. □

It would be very interesting to find a model N of S_2^1 having the above "saturation property" (†) and not satisfying Exp. This would entail the unprovability of exponential lower bounds to EF-proofs in S_2^1.

Problem 1: Is theory

$$S_2^1 + \forall x((EF \vdash x) \equiv Taut(x)) + \neg\, Exp$$

consistent?

Note that in the construction we can arrange model N to be a "weak end-extension" of M in the sense of [3], i.e. for any $a \in N$ there is $b \in M$ such that:

$$N \models |a| = |b|.$$

In other words: N does not introduce new lengths. However, we are not able to use this property for guaranteeing Σ_1^b-LIND in N.

Problem 2: Does every countable model M of S_2^1 have a Δ_1^b-elementary extension N satisfying $S_2^1 + \forall x((EF \vdash x) \equiv Taut(x))$?

The positive answer to Problem 2 implies the positive answer to Problem 1 as we may take M satisfying a Σ_1^b-formula which is refutable in S_2^1 + Exp.

The last problem proposes an improvement in another direction

Problem 3: Is theory

$$\forall\Sigma_1^b(S_2^1) + \forall x((EF \vdash x) \equiv Taut(x)) + \neg\, Exp + B\Sigma_0$$

consistent?

Above we have shown that without $B\Sigma_0$ this theory is consistent. But it may happen that in each model N of it, for some $a \in N$, the shortest EF-proofs of tautologies $\tau \leq a$ are cofinal in N. Thus there is not function total in N which bounds the length of the shortest proofs of tautologies. If the collection scheme $B\Sigma_0$ were satisfied in N, we would have such a function (and it would be subexponential).

References

[1] S. Buss: Bounded Arithmetic, Bibliopolis, Naples, (1986).

[2] S. Buss: Axiomatization and Conservation Results for Fragments of Bounded Arithmetic, in: Workshop in Logic and Computation, AMS Contemporary Mathematics, to appear.

[3] S. Buss: Weak End Extensions of Models of Bounded Arithmetic, unpublished manuscript.

[4] S. Cook: Feasibly Constructive Propositional Calculus, in: Proc. 7th A.C.M. Symp. on Th. of Comp., (1975), pp. 83–97.

[5] S. Cook, A. R. Reckhow: The Relative Efficiency of Propositional Proof Systems, J. Symbolic Logic 44(1), (1979), pp. 36–50.

[6] S. Cook, A. Urquhart: Fuctional Interpretation of Feasibly constructive Arithmetic, Univ. of Toronto, Rep. 210/88, (1988).

[7] R. A. DeMillo, R. J. Lipton: Some Connections Between Mathematical Logic and Complexity Theory, in: Proc. 11th A.C.M. Symp. on Th. of Comp., (1979), pp. 153–158.

[8] M. Dowd: Propositional Representation of Arithmetic Proofs, Ph.D. Thesis, Univ. of Toronto, (1979).

[9] A. Haken: The Intractability of Resolution, Theor. Comp. Sci. 39, (1985), pp. 297–308.

[10] J. Krajíček, P. Pudlák: Propositional Proof Systems, the Consistency of First Order Theories and the Complexity of Computations, J. Symbolic Logic, to appear.

[11] J. Krajíček, P. Pudlák: Quantified Propositional Calculi and Fragments of Bounded Arithmetic, Zeitschrift f. Math. Logik, to appear.

[12] J. Krajíček, P. Pudlák, G. Takeuti: Bounded Arithmetic and the Polynomial Hierarchy, Annals of Pure and Applied Logic, submitted.

[13] A. Wilkie: Subsystems of Arithmetic and Complexity Theory, an invited talk at 8th Int. Congress LMPS' 87, Moscow, (1987).