Tautologies from pseudo-random generators

Jan Krajíček*

Mathematical Institute†
Academy of Sciences, Prague

Abstract

We consider tautologies formed from a pseudo-random number generator, defined in Krajíček [12] and in Alekhnovich et.al. [2]. We explain a strategy of proving their hardness for EF via a conjecture about bounded arithmetic formulated in Krajíček [12]. Further we give a purely finitary statement, in a form of a hardness condition posed on a function, equivalent to the conjecture.

This is accompanied by a brief explanation, aimed at non-specialists, of the relation between propositional proof complexity and bounded arithmetic.

It is a fundamental problem of mathematical logic to decide if tautologies can be inferred in propositional calculus in substantially fewer steps than it takes to check all possible truth assignments. This is closely related to the famous P/NP problem of Cook [3]. By propositional calculus I mean any text-book system based on a finite number of inference rules and axiom schemes that is sound and complete. The qualification *substantially less* means that the number can be bounded above by a poly-logarithm of the number of truth assignments.

*Partially supported by grant # A 101 99 01 of the Academy of Sciences of the Czech Republic and by project LN00A056 of The Ministry of Education of the Czech Republic.
Mathematics Subject Classification: Primary 03F20, 68Q15. Secondary 03530.

†Also member of the *Institute for Theoretical Computer Science* of the Charles University. A part of this work was done while visiting the Mathematical Institute at Oxford.

The topic of this paper is a search for tautologies that make viable candidates for being hard for Extended Frege proof system EF. Rather than explaining what EF is let me only say that the minimum size (i.e. the number of symbols) of EF proofs is proportional to the minimum number of inference steps in the usual calculus, cf.[5]. The tautologies considered are defined in a simple way from a pseudo-random number generator. I arrived at them in [12] as a consequence of a work on forms of weak pigeonhole principle in bounded arithmetic and their relations to various cryptographic primitives, searching also for a generalization of prime tautologies from [16] (cf. Section 2) that would be more generic and hopefully suspectable to forcing. The same tautologies were recently rediscovered in [2] in a purely combinatorial language as a framework in which one can think of certain known lower bound methods and try to generalize them to stronger systems. In a sense both lines of thought have a common origin in Razborov's [22] which was the first paper to bring cryptography into bounded arithmetic and propositional logic. The first aim of this note is to explain that the two lines of thought did not really diverge that much. In order to do that I recapitulate briefly the development of propositional proof complexity with emphasis on the interplay between complexity proper and bounded arithmetic. I keep logic notation to a minimum. This is in Section 1. The rest of the paper is organized as follows. In Section 2 I recall two known candidates for tautologies hard for EF. The definition of tautologies from a pseudo-random number generator is given in Section 3, together with the conjecture from [12], and the implication of the conjecture for the EF-hardness of the tautologies. In Section 4 I give a statement that is purely finitary and equivalent to the main conjecture. It is in a form of a new hardness condition posed on a function. This is a necessary step towards showing that some usual hardness assumption (e.g. some cryptographic hardness) posed on a function implies the conjecture and hence a lower bound to the size of EF proofs of concrete tautologies. The paper is concluded by an example and a remark on stronger proof systems. Whenever paper [12] uses Buss's theory S^1_2 I use here Cook's PV (albeit in the formulation as PV_1 of [17, 10]). I also speak here about polynomial sizes rather than subexponential sizes. This is all in order not to overflow the self-imposed quota for new definitions and special notation. From the point of view of properties (1) - (3) in Section 1 of the relation of arithmetic to propositional proof complexity, theories PV and S^1_2 are essentially indistinguishable and they both relate in the same way to the system EF. (This does not imply that all results transfer between PV and S^1_2; for example, Theorem 4.2 would have a different form for S^1_2.) I should say few words about PV: the language has symbols for all polynomial time algorithms and the axioms are equations that codify how the algorithms use one another. The reader only needs to know that it is a theory suitable for formalizing polynomial time constructions in the most natural way; details can be found in [10].

1 Proof complexity and bounded arithmetic

Propositional proof complexity starts with Cook's 1971 and 1975 papers [3, 4]. The former is the famous paper stating the P/NP problem and its relation to propositional logic, the later is another pioneering work uncovering a tight relation of proof complexity to formal arithmetic theories. That paper introduced Cook's theory PV, the translation of arithmetic formulas and proofs into propositional ones, and proves a relation of PV to Extended Frege system EF (the same relation was rediscovered by Paris and Wilkie [19] in the context of another but closely related systems). This was in my opinion the birth of proof complexity proper, although even earlier there were results and ideas about lengths of propositional proofs that are still very interesting and important. Most notable is work of Tseitin [23] about resolution that was inspired by problems about formal linguistic. Then came Cook and Reckhow's [5] systematic classification of various usual calculi for propositional logic and the definition of the right notion of reducibility (polynomial simulation). The beginning of contemporary research in lower bounds for propositional proof systems starts by Ajtai's lower bound for constant depth Frege proofs of pigeonhole principle PHP [1]. This is in my view the most important propositional lower boundpaper ever written as it opened the relation to boolean complexity and freed the research from a narrowly combinatorial approach. This is not to diminish other important achievements, notably Haken's exponential resolution lower bound [7]. The relation between proof systems and theories, present in the field from its beginning, can be summarized as follows. Let $A(x)$ be a coNP definition of a set of numbers. Assume $A(x)$ has the form $\forall y; |y| \leq |x|^k \rightarrow B(x,y)$ with $B(x,y)$ a polynomial time predicate. Fix length n to bound $|x|$'s and construct a propositional formula $||A(x)||^n$ as in the completeness of satisfiability: the formula has n atoms $p_1, \ldots, p_n$ for bits of an x, $m = n^k$ atoms $q_1, \ldots, q_m$ for bits of potential y, and also atoms

$r_1, \ldots, r_s$ for $s = n^{O(1)}$ bits of values on nodes of a fixed circuit C_n computing from $\overline{p}$, $\overline{q}$ the truth value of predicate $B(x,y)$. Formula $||A(x)||^n$ says, in a DNF form, that if $\overline{r}$ are correctly computed by circuit C_n from inputs $\overline{p}$, $\overline{q}$ then the output of the computation is 1. Having any b of length at most n with bits $b(1), \ldots, b(n)$ denote by $||A(x)||^n(b)$ the propositional formula with $b(i)$ substituted for p_i, and with remaining atoms $\overline{q}$ and $\overline{r}$ left unsubstituted. Clearly then b satisfies $A(x)$ iff $||A(x)||^n(b)$ is a tautology. The relation between proof systems and theories is as follows: The systems/theories come in pairs P/T such that:

(1) If T proves $\forall x; A(x)$ then tautologies $||A(x)||^n(B)$ have polynomial size proofs in P.

(2) T proves the soundness of P and for any another proof system Q, if T proves also the soundness of Q then P polynomially simulates Q.

One such prominent pair is formed by Extended Frege system EF and by Cook's PV.

The first property has also a converse (used first explicitly by Paris and Wilkie [19] and also by famous Ajtai's paper [1]) that is slightly more complex to state (and cannot be done in a logic-free combinatorial set-up only). It is a simple instance of compactness of first order logic though. Assume that $b_1, b_2, \ldots$ is a sequence of numbers of lengths $n_1 < n_2 < \ldots$ such that the formulas $||A(x)||^{n_i}(b_i)$ are tautologies and have P-proofs of size $\leq {n_i}^k$. Let M be any countable model of true arithmetic. Then there will be a non-standard $n^* \in M$ and an element $b^* \in M$ of length n^* such that the formula (in M) $||A(x)||^{n^*}(b^*)$ is a tautology and has (in M) a P-proof π^* of size $\leq n^{*k}$. Moreover, if all original elements b_i satisfy some property $U(x)$ from polynomial hierarchy (and thus expressible by a bounded formula in the language of PV) also b^* will satisfy in M the same property. Now comes the idea from item (1) above. Take an initial substructure M_{b^*} of M consisting of all elements that have the length bounded by some $n^{*\ell}$, ℓ a standard natural number. In particular, b^* as well as π^* are in M_{b^*}, and both $A(b^*)$ and $U(b^*)$ hold in M_{b^*}. Let $N \supseteq M_{b^*}$ be any extension of M_{b^*} that is a model of theory T and preserves polynomial time predicates (in particular, the predicate "to be a P-proof"). Then the element b^* must have property $A(x)$ also in N: Otherwise take any $c \in N$ witnessing the existential quantifier in $\neg A(b^*) = \exists y; |y| \leq n^{*k} \wedge \neg B(b^*, y)$. The bits of c

define a truth evaluation (in N) of the atoms $\overline{q}$ of $||A(x)||^{n^*}(b^*)$ that together with evaluation of atoms $\overline{r}$ by the actual bits that occur in the computation of C_{n^*} on b, c yield a truth assignment falsifying the formula $||A(x)||^{n^*}(b^*)$. However, the formula has a P proof π^* in N (as π^* was already in M_{b^*}) and the system P is sound in N (as the soundness is provable in T and N is a model of T); hence the existence of such a truth assignment and of c is impossible and consequently b^* must satisfy $A(x)$ also in N. Thus we have the suitable inverse to the first property:

(3) Let M be an arbitrary countable model of true arithmetic and $b^* \in M$ an arbitrary non-standard element satisfying a property $U(x)$. Assume that for any such M and b^* we can find an extension of the substructure M_{b^*} to a model N of T that preserves polynomial time predicates and in which $\neg A(b^*)$ holds. Then there are no $k < \omega$ and infinite sequence $b_1, b_2, \ldots$ of numbers of lengths $n_1 < n_2 < \ldots$ having all property $U(x)$ such that all formulas $||A(x)||^{n_i}(b_i)$, $i = 1, 2, \ldots$ are tautologies with P - proofs of size $\leq {n_i}^k$.

(In fact, the opposite implication also holds.)

All these three properties are very well established and fruitfully used, and they earned to bounded arithmetic the adjective of "uniform proof complexity", having a relation to boolean proof complexity analogous to the relation of Turing machines to circuit complexity. To give some examples: quasi-polynomial proofs of WPHP in constant-depth Frege were obtained via (1) from Paris-Wilkie-Woods [20], or the construction of polynomial size EF-proofs of disjointness of two NP-sets related to RSA from [16], an important link of proof complexity and cryptography. There are many such examples and I regret that the beautiful new proof of WPHP by Maciel-Pitassi-Woods [18] is not presented in this way as the combinatorics used is the same as the one used in establishing the appropriate correspondence P/T (cf.[8]) and the presentation may be done on one page[1].

Property (2): the polynomial simulation of system SF (Frege system with the substitution rule) by EF was first proved in this way, while the explicit construction is quite involved, cf. [6, 13]. Property (2) is currently totally ignored, although various recent polynomial (non)simulation between tree-like/non-tree-like systems, or between constant-depth subsystems of Frege

[1] Cf. seminar notes `http://www.math.cas.cz/~krajicek/mpw.ps`

system and algebraic systems are immediate corollaries of (2), often even stated in print as the corresponding soundness properties or explicitly as lower bound criteria. Property (3): the most famous instance is Ajtai's proof of super-polynomial lower bound for constant-depth Frege proofs of PHP. Or Wilkie's proof of Cook's simulation results from [4] as generalized in [9].

2 Earlier tautologies possibly hard for EF

Let me recall two types of tautologies possibly hard for EF. The first type is simply the property (2) of the relation of soundness to polynomial simulation. Let P and T be a pair as earlier and take a proof system Q that you believe to be impossible to polynomially simulate by P. The soundness of Q can be expressed as $Con_Q := \forall x, Con_Q(x)$ where $Con_Q(x)$ says that there is no Q-proof w of size $|w| \leq |x|$ of a formula v, and a truth assignment u satisfying the negation of v (clearly $|u|$ an $|v|$ are also bounded by $|x|$). Then one expects that tautologies $||Con_Q(x)||^n$ do not have polynomial size P-proofs. This is because by (1) the existence of polynomial P-proofs is close to provability in T and provability of the soundness of Q in T would imply the polynomial simulation. These candidates go back to [4]. In fact, a bit stronger assumption about P and Q is equivalent to the non-existence of polynomial size P-proofs of $||Con_Q(x)||^n$. The assumption is that the minimal size of P-proofs cannot be bounded by a polynomial in minimal sizes of Q-proofs. See [13] or [10] for details. The second example is from [16], a part of a work showing that the method of feasible interpolation (cf. [11] for explanation) cannot be applied to EF. The tautologies express that a number is a prime. Namely, take formula $A(x)$ of the form $\forall y, z < x; y \cdot z \neq x$. Then for a prime p of length n the formula $||A(x)||^n(p)$ is a tautology. The question what is the minimum size of EF-proofs of these tautologies was posed in [16] and it was proved there that the tautologies do have polynomial EF-proofs iff there is an NP-definition $E(x)$ of primes such that PV proves that the definition is sound: $\forall x, E(x) \rightarrow A(x)$. All such definitions seem to use at some point or another the Little Fermat theorem that is a notorious number-theoretic statement which is unknown to be provable in PV. In fact, it is not provable assuming the RSA is secure, see [16]. Note that these second tautologies are of the form $||x \notin Rng(f)||^n$ for a conjectured one-way function.

3 Tautologies from pseudo-random generators

Denote by WPHP^a_{2a} the statement that $f : a \to 2a$ cannot be onto. I shall call it *dual* WPHP, similarly as [2]. This has been first considered by Wilkie and his witnessing theorem (see [10, 12]) is the best result about the principle. A question about provability of the principle for a concrete polynomial time function was posed also in [21, Append.C]. It is explained in [12] that proof-theoretic properties of (dual) WPHP are related to the existence of strong pseudo-random number generators and other cryptographic primitives in several ways. The problem whether PV proves WPHP^a_{2a} for all polynomial time functions [12, Sec.7] seems to me to be the right avenue towards other main problems; it has bigger quantifier complexity (Σ^b_2) than ordinary (W)PHP while still having implications for propositional proof complexity, and it also relates to the famous problem on finite axiomatizability of bounded arithmetic, cf.[10].

A strong pseudo-random generator is a polynomial time function G that stretches the inputs by (at least) one bit and has exponential hardness. That is: there is $\epsilon > 0$ such that for any n and any circuit $C(y_1, \dots, y_{n+1})$ of size less than 2^{n^ϵ} it holds that

$$\mathrm{Prob}_x[C(G(x)) = 1] \;-\; \mathrm{Prob}_y[C(y) = 1] < 2^{n^\epsilon}$$

where x are chosen uniformly at random from $\{0,1\}^n$ and y from $\{0,1\}^{n+1}$.

For explaining Conjecture [12, 7.9] I shall use the same set-up as for property (3) in Section 1. Denote by f_n the restriction of a function f to inputs of length n.

Conjecture 3.1 ([12, 7.9]) *Assume that a strong pseudo-random generator G exists. Then there is a polynomial time computable function f such that any countable model M_{a^*} of the form as earlier, $a^* = 2^{n^*}$ in M, has an extension to a model N of PV that violates $WPHP^{a^*}_{2a^*}(f)$. In particular, if strong pseudo-random number generators exist then PV does not prove $WPHP^a_{2a}$ for all polynomial time functions.*

The reference to G seems redundant. However, I conjectured in [12] that there is a construction of f from G uniform in G and that there are even G for which one can take $f := G$. (This cannot be true for all G; e.g. G can have the form $1 + H$. For another example see Section 4.) The qualification *uniform* is used informally; for example, precomposing G with a simple polynomial time function depending on G.

As noted in [12] the conjecture has also implications for Extended Frege system EF. This is via property (3) from Section 1. To simplify notation denote by τ_b the propositional formula $\|y \notin Rng(f_n)\|^{n+1}(b)$, $b \in \{0,1\}^{n+1}$, and $n \in \mathbf{N}$. The following statement is an obvious instance of property (3).

Corollary 3.2 *Assume that G is a strong pseudo-random generator and f is a function with properties guaranteed by the conjecture. Then tautologies τ_b for $b \notin Rng(f_n)$, $n = 1, 2, \ldots$, require superpolynomial EF-proofs.*

Alekhnovich et.al. [2] consider various propositional encodings of the statement $b \notin Rng(G_n)$ and prove several lower bounds for systems like resolution, polynomial calculus and their combination, and for concrete pseudo-random generators inspired by the Nissan-Wigderson generator. They also offer a view of Tseitin's tautologies [23] that sees them as tautologies of the same form.

4 An equivalent form of the conjecture

We continue using the abbreviation τ_b defined before Corollary 3.2 but as we shall substitute into the formulas we shall use a notation showing explicitly occurrences of atoms. The formula $\|y \notin Rng(f_n)\|^{n+1}$ has atoms $p_1, \ldots, p_{n+1}$ for bits of y, atoms $q_1, \ldots, q_n$ for bits of possible x, and atoms $r_1, r_2, \ldots$ for bits of computation of $f(x)$. We shall neglect atoms r_i as they are unique for any particular $\overline{q}$. (One may also think of EF as operating with circuits in which case atoms r_i can be replaced by the corresponding circuits.)

For $b \in \{0,1\}^{n+1}$ the formula $\tau_b(\overline{q})$ is $\|y \notin Rng(f_n)\|^{n+1}(\overline{p}/b)$. However, assume that b is not a string of bits but a string of single output circuits with inputs (atoms) $\overline{u} = (u_1, \ldots, u_\ell)$. The formula $\tau_b(\overline{q}, \overline{u})$ makes a perfect sense and it is a tautology iff the range of the function $b : \{0,1\}^\ell \to \{0,1\}^{n+1}$ is disjoint with $Rng(f_n)$.

Our hardness condition on f will have a similar form. We shall denote by $\text{Circuit}^{n+1}(\overline{u})$ the set of circuits computing $n+1$ output bits from atoms $\overline{u}$. In particular, $\text{Circuit}^{n+1}(\emptyset)$ is a circuit without inputs computing $n+1$ constants.

Definition 4.1 *Let $k \geq 1$. Function f is k-restricted for EF iff there is a polynomial $p(n)$ such that there are arbitrarily large n and circuits $b_1, \ldots, b_k$, $b_1 \in Circuit^{n+1}(\emptyset)$, $b_2 \in Circuit^{n+1}(\overline{q}^1)$, $b_3 \in Circuit^{n+1}(\overline{q}^1, \overline{q}^2)$, $\ldots$, $b_k \in Circuit^{n+1}(\overline{q}^1, \ldots, \overline{q}^{k-1})$, $\overline{q}^i$ disjoint n-tuples of atoms, of size at most $p(n)$ such that the formula*

$$(*) \qquad \tau_{b_1}(\overline{q}^1) \vee \ldots \vee \tau_{b_k}(\overline{q}^1, \ldots, \overline{q}^k)$$

has an EF-proof of size at most $p(n)$. Function f is k-free for EF iff it is not k-restricted, and it is free for EF iff it is k-free for all $k \geq 1$.

If the formula $(*)$ is a tautology then either $b_1 \in \{0,1\}^{n+1}$ is outside $Rng(f_n)$, or if $f(a_1) = b_1$ for some $a_1 \in \{0,1\}^n$ then $b_2(\overline{q}^1/a_1) \in \{0,1\}^{n+1}$ is outside $Rng(f_n)$ etc. So, in at most k steps one finds in this way an element outside $Rng(f_n)$; in particular, such element exists in a model of PV if $(*)$ has an EF-proof there, as then it is a tautology by property (2) of Section 1.

The formula implies that the range of the map $b : \{0,1\}^{(k-1)n} \to \{0,1\}^{k(n+1)}$ given by $b_1, \ldots, b_k$ is not included in the range of $\bigoplus_{i=1}^k f_n$ (k-fold direct sum). In fact, provability of any similar non-inclusion in PV yields an analogous interactive computation.

Theorem 4.2 *Conjecture 3.1 is satisfied with function f iff f is free for EF.*

Proof : The conjecture obviously implies that f must be free. Otherwise, by compactness, there would model M_{a^*} of the form as earlier containing circuits $b_1, \ldots, b_k$ for some non-standard n^* (with appropriate inputs as in Definition 4.1) and an EF-proof of the formula $(*)$. Hence the formula $(*)$ is a tautology in any extension N of M_{a^*}, $b_1, \ldots, b_k$ determine an element of N outside $Rng(f_{n^*})$ and N cannot violate $\mathrm{WPHP}^a_{2a}(f)$.

For the opposite direction assume that in all extensions of M_{a^*} $\mathrm{WPHP}^a_{2a}(f)$ holds. This means that PV together with the open diagram $Diag(M_{a^*})$ proves the following formula: $\exists y \in \{0,1\}^{n^*+1} \forall x \in \{0,1\}^{n^*}; f_{n^*}(x) \neq y$.

By the KPT witnessing theorem [17] there are $k \geq 1$ and polynomial time functions $h_1(z, \overline{u})$, $h_2(z, x_1, \overline{u})$, $\ldots$, $h_k(z, x_1, \ldots, x_{k-1}, \overline{u})$ such that the following universal formula

$$f_{n^*}(x_1) \neq h_1(a^*, \overline{w}) \vee f_{n^*}(x_2) \neq h_2(a^*, x_1, \overline{w}) \vee$$

$$\ldots \vee f_{n^*}(x_k) \neq h_k(a^*, x_1, \ldots, x_{k-1}, \overline{w})$$

with $\overline{w}$ some parameters from M_{a^*}, is provable in PV + $Diag(M_{a^*})$. Hence in M_{a^*} the propositional translation of this formula has an EF proof (propositional translations of all sentences in $Diag(M_{a^*})$ have polynomial size EF proofs in M_{a^*}, cf. [14, 10]). The propositional translation is the formula (*) with circuits b_i computing $h_i(a^*, x_1, \ldots, x_{i-1}, \overline{w})$

q.e.d.

Let us consider an example: Let g be a one way permutation such that PV proves that it is injective. Let G be a pseudo-random generator constructed from g by adding to the value $g(x)$ a hard bit of x. Then clearly PV proves that for any $y \in \{0,1\}^n$ at least one of $b_0 := (y, 0)$, $b_1 := (y, 1)$ is outside $Rng(G_n)$. So for formulas τ_b constructed from $f := G$, by property (1) , EF admits polynomial size proofs of disjunctions $\tau_{b_0} \vee \tau_{b_1}$. Hence G is 2-restricted. (This example was noticed by P. Pudlák and by A. Wigderson.) Note that we can dispose of the disjunction by precomposing G with a suitable polynomial time function (depending on the particular hard bit).

The notion of a function free for a general proof system Q makes a perfect sense and Theorem 4.2 holds for any Q that polynomially simulates EF, with PV replaced by PV $+Con_Q$ (Con_Q is the $\forall\Pi_1^b$ sentence from Section 2). The choice of the particular theory for Q (it is unique only up to $\forall\Pi_1^b$ consequences) is important. For example, system G_2, a subsystem of quantified propositional logic G, corresponds to theory T_2^2 (cf. [15, 10]). That theory proves WPHP_{2a}^a for all polynomial time functions. However, that does not imply that every such functions is k-restricted for G_2, some $k \geq 1$. The proof of Theorem 4.2 needs that the theory has a Skolemization by polynomial time functions as apparently only then do sentences from the open diagram have Q-proofs in the model.

References

[1] M. Ajtai: The complexity of the pigeonhole principle, in: *Proc. IEEE 29th Annual Symp. on Foundation of Computer Science*, (1988), pp. 346-355.

[2] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson, Pseudorandom generators in propositional proof complexity, preprint, (March 2000).

[3] Cook, S A., The complexity of theorem proving procedures, in: *Proc. 3^{rd} Annual ACM Symp. on Theory of Computing*, (1971), pp. 151-158. ACM Press.

[4] Cook, S A., Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, (1975), pp. 83-97. ACM Press.

[5] Cook, S. A. and Reckhow, A. R., The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**, (1979), pp.36-50.

[6] Dowd, M., Propositional representations of arithmetic proofs, *PhD Thesis*, *University of Toronto*, (1979).

[7] Haken, A., The intractability of resolution, *Theoretical Computer Science*, **39**, (1985), pp.297-308.

[8] J. Krajíček, Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**, (1994), pp.73-86.

[9] J. Krajíček, On Frege and Extended Frege Proof Systems, in: "Feasible Mathematics II", eds. P. Clote and J. Remmel, Birkhauser, (1995), pp. 284-319.

[10] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[11] J. Krajíček, Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. of Symbolic Logic*, **62(2)**, (1997), pp.457-486.

[12] J. Krajíček, On the weak pigeonhole principle, *Fundamenta Mathematicae*, to appear (preprint on web August 9 '99).

[13] J. Krajíček and P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, *J. Symbolic Logic*, **54(3)**, (1989), pp.1063-1079.

[14] J. Krajíček and P. Pudlák, Propositional provability in models of weak arithmetic, in: *Computer Science Logic (Kaiserlautern, Oct. '89)*, eds.E.Boerger, H.Kleine-Bunning and M.M. Richter, LNCS 440, (1990), pp.193-210. Springer-Verlag.

[15] J. Krajíček and P. Pudlák, Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**, (1990), pp.29-46.

[16] J. Krajíček and P. Pudlák, Some consequences of cryptographical conjectures for S_2^1 and EF", *Information and Computation*, Vol. **140 (1)**, (January 10, 1998), pp.82-94.

[17] Krajíček, J., Pudlák, P., and Takeuti, G., Bounded arithmetic and the polynomial hierarchy, *Annals of Pure and Applied Logic*, **52**, (1991), pp.143–153.

[18] A. Maciel, T. Pitassi, and A. Woods, A new proof of the weak pigeonhole principle, preprint (1999).

[19] Paris, J. and Wilkie, A. J., Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic*, LNM 1130, (1985), pp.317-340. Springer-Verlag.

[20] J. B. Paris, A. J. Wilkie, and A. R. Woods, Provability of the pigeonhole principle and the existence of infinitely many primes, *Journal of Symbolic Logic*, **53**, (1988), pp.1235–1244.

[21] A. A. Razborov, Bounded arithmetic and lower bounds in Boolean complexity, in: *Feasible Mathematics*, eds. P.Clote and J.Remmel, *Progress in Comp.Sci. and Applied Logic*, Vol. **13**, (1995), pp.344-386. Birkhauser.

[22] A. A. Razborov, Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**, (1995), pp.201-224.

[23] Tseitin, G. C., On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic, Part II*, ed. A.O.Slisenko, (1968), pp.115-125.