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 [16] and in Alekhnovich et al. [2]. We explain a strategy of proving their hardness for Extended Frege systems via a conjecture about bounded arithmetic formulated in Krajíček [16]. Further we give a purely finitary statement, in the form of a hardness condition imposed 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 [5]. 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 fewer* means that the number can be bounded above by a polynomial in the size of the tautology (unless the size is exponential in the number of variables this is indeed smaller than the number of truth assignments).

The topic of this paper is a search for tautologies that make viable candidates for being hard for an Extended Frege proof system EF. Rather than

*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 03F30.

†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.

explaining what EF is now (see next section) 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. [7].

The tautologies considered are defined in a simple way from a pseudo-random number generator. I arrived at them in [16] as a consequence of work on forms of the weak pigeonhole principle in bounded arithmetic and their relations to various cryptographic primitives, searching also for a generalization of prime tautologies from [20] (cf. Section 3) that would be more generic and hopefully susceptible 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 [29] which was the first paper to bring cryptography into bounded arithmetic and propositional logic (via Razborov-Rudich's notion of natural proofs [30]; paper [20] grew from trying to use [15, Thm.9.2] in a concrete situation and that theorem originated from a remark in [29]).

The first aim of this note is to explain these tautologies to non-specialists, as well as the relation of the problem of proving their hardness for EF with the problem of constructing suitable models of the bounded arithmetic theory PV. In order to do this I recapitulate briefly the development of propositional proof complexity with an emphasis on the interplay between complexity proper and bounded arithmetic. This is in Section 2 after few basic definitions and facts are recalled in Section 1.

The rest of the paper is organized as follows. In Section 3 I recall two known candidates for tautologies that might be hard for EF. The definition of tautologies from a pseudo-random number generator is given in Section 4, together with the conjecture from [16], and the implication of the conjecture for the EF-hardness of the tautologies. A hardness condition on functions, called *free for EF*, is defined in Section 5. It is based on a notion of counter-example computation via a two player (Student/Teacher) communication. In Section 6 I give a statement that is purely finitary and equivalent to the main conjecture using the new hardness condition on functions. This is a necessary step towards showing that some usual hardness assumption (e.g. some cryptographic hardness) imposed on a function implies the conjecture and hence a lower bound to the size of EF proofs of concrete tautologies. The paper concludes with some examples and remarks on other proof systems.

Whenever paper [16] uses Buss's theory S^1_2 (cf. [3]) I use here Cook's PV (albeit in the formulation as PV_1 of [21, 14]). I also speak here about polynomial sizes rather than sub-exponential sizes. This is all in order not to exceed the self-imposed quota for new definitions and special notation. From the point of view of properties (1) - (3) in Section 2 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 6.2 would have a different form for S^1_2.) A few words about PV here for readers not familiar with the theory: the language has symbols for all polynomial time algorithms and the axioms are equations that codify how the algorithms use one another, together with a form of (binary search style) induction for polynomial time predicates. The reader only needs to know that it is a theory suitable for formalizing polynomial time constructions in the most natural way; a definition can be found in the next section, more details can be found in [14].

1 EF and PV

The DeMorgan language for propositional logic consists of 0, 1, $\neg$, $\vee$ and $\wedge$. A *Frege proof system* for propositional logic is given by finitely many axiom schemes and inference rules that are sound and implicationally complete (i.e., if ψ is true for all truth assignments making $\phi_1, \ldots, \phi_k$ true then ψ can be proved from the ϕ_i's). For example, systems based on a few axioms and modus ponens as the only rule are frequent text-book examples of so called Hilbert-style systems. (The name Frege system comes from [7] and was chosen mistakenly; however, [7] is an established taxonomy of propositional calculi and it is a custom to follow its terminology.)

There are two natural measures of complexity of proofs; the size, which is the total number of symbols in the proof, and the number of steps. The latter measure is perhaps more natural from a logical (or proof-theoretical) point of view but the former, the size, is the more important one in connection with computational complexity theory. The reason is that the length of a string encoding a proof (or a formula etc.) for a machine is proportional to the size of the proof but may be much bigger than the number of steps (even proofs with few steps may contain huge formulas). In particular, it is easy to see that there is an algorithm verifying that a string is a proof in a particular Frege system with polynomial (quadratic) running time relative to the size. Such a simple algorithm constitutes, in fact, the main link of lengths-of-proofs to the P/NP and NP/coNP problems. Namely, if there were always a proof π for any tautology τ of size polynomial in the size of τ then the coNP-complete set TAUT of tautologies would be in the class NP: simply guess a short proof and then verify its validity, and the class NP would be closed under complement (i.e., NP = coNP). If, moreover, one could find a suitable π in polynomial time, then similarly TAUT would be in class P and P would equal NP.

This relation of Frege systems to computational complexity was, in fact, taken by [7] as a definition of a general propositional proof system. A *propositional proof system* is a polynomial time relation $R(x, y)$ (on binary strings) such that the property of y: $\exists x \in \{0,1\}^*; R(x,y)$, defines exactly the set TAUT. Any string π such that $R(\pi, \tau)$ holds is called an R-proof of τ. Then, similarly to the case of Frege systems, NP = coNP iff there exists a proof system admitting polynomial size proofs for all tautologies.

The main method of comparison between different proof systems is *polynomial simulation*: P polynomially simulates Q iff there is a polynomial time algorithm A that, given a Q-proof π of τ, produces a P-proof $A(\pi, \tau)$ of τ. Proof systems that polynomially simulate each other are indistinguishable from the lengths-of-proofs point of view and in their relation to the P/NP and NP/coNP problems.

In this respect the definition of Frege systems is very robust. If we use any complete language instead of the DeMorgan language, any particular set of axioms and rules, and any usual format of proofs such as tree-like or sequence-like (or even writing proofs in sequent calculus or natural deduction formalisms) we always get a system that is equivalent by polynomial simulations to any other Frege system, cf. [7].

The idea of an *Extended Frege system*, EF, is to rectify one obvious defect of Frege systems: a Frege system cannot use abbreviations for formulas that are used several times in the proof (as sub-formulas of other formulas). Formally, the *extension rule* (which is not really a Hilbert-style schematic rule) allows one to extend a sequence of formulas $\phi_1, \ldots, \phi_k$ by a formula ϕ_{k+1} of the form $q \equiv \psi$, provided atom q occurs in none of $\phi_1, \ldots, \phi_k$, nor in ψ, nor in the last formula we aim at proving. The new atom can be, however, used in later steps $\phi_{k+2}, \ldots$ of the proof.

The definition of EF is equally robust as that of Frege systems and, moreover, the minimal size and the minimal number of steps of EF-proofs of a formula are proportional to each other. There is another extension of F that allows the *substitution rule*: from $\phi(p_1, \ldots, p_n)$ infer in one step any $\phi(\psi_1, \ldots, \psi_n)$. This *Substitution Frege* SF is, in fact, equivalent to EF by polynomial simulations, cf. [8, 17]. It is not known if F is also equivalent to them.

The main problem of propositional proof complexity, the NP/coNP problem, thus asks to demonstrate superpolynomial lower bounds to the lengths-of-proofs in all conceivable proof systems. At this point we do not have any lower bound for EF and only a simple quadratic one for F (cf. [11]). However, there are several interesting systems, all weaker than F, for which strong lower bounds are known. These systems naturally divide into three types. Proof systems of the first type are various subsystems of F in the DeMorgan language obtained by restricting the depth of formulas the system may use; examples include the depth d Frege system F_d or its extension by instances of counting principles like PHP_N or $Count_q^N$. Those of the second type are various linear geometric proof systems: the cutting planes system working with linear inequalities and its extensions. Those of the third type are algebraic proof systems: these are various proof systems for ideal-membership in polynomial rings over fields. They are subsystems of the equational logic in the language of polynomial rings, which is again just a particular Frege system. References can be found in the expository articles [27, 32].

The reader may wonder why one should try to prove lower bounds for EF rather than aim first at the apparently weaker F. Well, some researchers do the latter. For me the reasons to aim at EF are perhaps more informal than strictly technical. First, all known lower bounds for subsystems of F (and for most of other systems too) actually apply directly to the number of steps, and the number of steps in F is, by the remark above, just the size in EF. A second reason is that I believe that the relation of proof systems to bounded arithmetic will continue to be instrumental in devising new lower bound methods, and EF corresponds to a much nicer and more transparent theory than F does.

As we shall see in the next section, a key property of proof systems is their relation to weak fragments of Peano Arithmetic, so called bounded arithmetic theories. A prototype of this relation is given by EF and Cook's theory PV. I shall explain the main idea of PV but I leave the somewhat tedious details of the definition for reader to read in [6] or [14], if desired.

Cobham [4] characterized the class of polynomial time functions operating on binary strings in a machine independent way. A function f is defined from functions g_0, g_1, g_2, g_3 by *limited recursion on notation* if:

(1) $f(\overline{x}, 0) = g_2(\overline{x})$,

(2) $f(\overline{x}, s_i(y)) = g_i(\overline{x}, y, f(\overline{x}, y))$, for $i = 0, 1$,

(3) $f(\overline{x}, y) \leq g_3(\overline{x}, y)$,

where $s_0(y)$ and $s_1(y)$ are the two functions adding 0 resp. 1 to the right of the binary representation of y. Cobham proved that the class of polynomial time functions is the smallest class of functions containing the constant 0, functions $s_0(y), s_1(y)$ and $x\#y$ ($|y|$ copies of x concatenated one after another), and closed under:

1. permutation and renaming of variables
2. composition of functions
3. limited recursion on notation

Building on this characterization Cook [6] defined an equational theory PV (for Polynomially Verifiable). I shall give a slightly modified definition of an equivalent universal theory. The theory has symbols for the initial functions and for a few other basic functions useful for manipulating strings (like truncation of the last bit Tr, concatenation $\frown$, and ordering $Less(x, y)$), and for all functions introduced consecutively by applying Cobham's operations arbitrarily many times. Axioms are universal formulas that for each function f produced by limited recursion on notation from functions $g_0, \ldots, g_3$ and all possible choices of functions f' and f^* for f and g'_i and g^*_i for g_i's say, that if all $g'_i = g^*_i$ and if conditions of the operation are satisfied for g'_i and g^*_i's respectively and if both f' and f^* were introduced by the operation, then $f' = f^*$. For example, let $E'_1, \ldots, E'_3$ and $E^*_1, \ldots, E^*_3$ be the equations $(1-3)$ from the definition of the limited recursion for on notation g'_i's and g^*_i's: three for f' and three for f^* in place of f. Then:

$$g'_0 = g^*_0 \wedge g'_1 = g^*_1 \wedge g'_2 = g^*_2 \wedge g'_3 = g^*_3 \wedge E'_1 \wedge E'_2 \wedge E'_3 \wedge E^*_1 \wedge E^*_2 \wedge E^*_3 \rightarrow f' = f^*$$

The theory also contains a form of induction. For any polynomial time predicate $P(x)$ (given by its characteristic function) there is a function symbol h (constructed by simulating binary search via limited recursion on notation) such that we have:

$$(P(0) \wedge \neg P(a)) \rightarrow (h(a) \subseteq_e a \wedge \neg P(h(a)) \wedge P(Tr(h(a))))$$

with $x \subseteq_e y$ denoting that x is an initial subword of y.

2 Proof complexity and bounded arithmetic

Propositional proof complexity starts with Cook's 1971 and 1975 papers [5, 6]. The former is the famous paper stating the P/NP problem and its relation to propositional logic, and the latter is another pioneering work uncovering a tight relation of proof complexity to formal arithmetic theories. That paper introduced Cook's theory PV, gave the translation of arithmetic formulas and proofs into propositional ones, and proved a relation of PV to Extended Frege system EF (the same relation was rediscovered by Paris and Wilkie [24] in the context of different 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 [31] about resolution that was inspired by problems about formal linguistics. Then came Cook and Reckhow's [7] 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 with Ajtai's lower bound for constant depth Frege proofs of pigeonhole principle PHP [1]. This is in my view the most important propositional lower bound paper 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 [9].

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 proof of the NP-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 a 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 the 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 prominent such 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 [24] and also in Ajtai's famous 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 $b_1, b_2, \dots$ is a sequence of numbers of lengths $n_1 < n_2 < \dots$ 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 non-standard 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 the polynomial hierarchy (and thus expressible by a bounded formula in the language of PV) then 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 lengths 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) Consider M, 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 for bounded arithmetic the name of "uniform proof complexity", having a relation to boolean proof complexity analogous to the relation of Turing machines to circuit complexity. Here are some examples.

Property (1): Quasi-polynomial proofs of the weak pigeonhole principle (WPHP) in constant-depth Frege were obtained via (1) from Paris-Wilkie-Woods [25], or the construction of polynomial size EF-proofs of disjointness of two NP-sets related to the RSA cryptosystem from [20], 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 [23] 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. [12]) 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. [8, 17]. Property (2) is currently totally ignored, although various recent polynomial (non)simulation results between tree-like/non-tree-like systems, or between constant-depth subsystems of Frege 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 a super-polynomial lower bound for constant-depth Frege proofs of PHP. Another instance is Wilkie's proof of Cook's simulation results from [6] as generalized in [13].

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

3 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 $|u|$ and $|v|$ 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 [6].

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 [17] or [14] for details.

The second example is from [20], a part of a work showing that the method of feasible interpolation (cf. [15] 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 [20] 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 example of a number-theoretic statement which is unknown to be provable in PV. In fact, it is not provable assuming the RSA is secure, see [20].

Note that tautologies of this second sort are of the form $||x \notin Rng(f)||^n$ for a conjectured one-way function.

Let us also mention one non-example. It has been suggested repeatedly that various finitary combinatorial principles independent from PA or ZFC could yield tautologies hard for many ordinary proof systems. However, this suggestion is somewhat flawed, at least when it is interpreted in the straightforward way.

All such principles, be they the Paris-Harrington version of Ramsey theorem, Kruskal's theorem or some other, are (at least) Π^0_2 - statements of the form $\forall n \exists N, \phi(n, N)$, with ϕ bounded. Their unprovability stems solely from the enormously rapid growth of the function giving the minimal witness N for parameter n, but otherwise - once given N - the proofs of $\phi(n, N)$ are based on counting of or induction on substructures inside N. To turn such a principle into a propositional tautology one needs to take N itself as a parameter. The formula speaks about the finite structure with the universe $[0, N]$ (see e.g. formalization of Ramsey theorem by formulas RAM_n in [16]) which makes the formula huge and its proof, based on counting or induction that are both easily simulated in EF, short compared to its size.

4 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 [14, 16]) is the best result about the principle. A question about provability of the principle for a concrete polynomial time function was posed also in [28, Append.C]. It is explained in [16] 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 [16, 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. [14]. One may note here that the ordinary weak pigeonhole principle WPHP^{2a}_a, saying that f cannot injectively map $2a$ into a, is not provable in PV or S^1_2 for a particular polynomial time function (exponentiation modulo a prime) unless the cryptosystem RSA is insecure, cf. [20].

A strong pseudo-random generator (a concept introduced by Yao [33]) 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 $C(y_1, \ldots, y_{n+1})$ 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 is chosen uniformly at random from $\{0,1\}^n$ and y from $\{0,1\}^{n+1}$.

The intuition behind the definition is that although G cannot be onto $\{0,1\}^{n+1}$, it's range is hard to distinguish from $\{0,1\}^{n+1}$ in the sense that any sub-exponential size circuit does not distinguish a random element y of $\{0,1\}^{n+1}$ from a pseudo-random element $G(x)$ of $Rng(G)$ with more than a negligible probability.

For explaining Conjecture 7.9 of [16] I shall use the same set-up as for property (3) in Section 2. Denote by f_n the restriction of a function f to inputs of length n.

Conjecture 4.1 ([16, 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 [16] 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 other examples see Section 7.) The qualification *uniform* is used informally; it could mean, for example, pre-composing G with a simple polynomial time function depending on G.

As noted in [16] the conjecture has also implications for Extended Frege system EF. This is via property (3) from Section 2. 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 4.2 *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 Nisan-Wigderson generator. They also offer a view of Tseitin's tautologies [31] that sees them as tautologies of the same form.

5 Counter-example computations

In the next section we link the conjecture with a new notion of hardness of a function, so that the conjecture holds with a function f iff f is hard in this new sense. To illustrate the definition of the hardness notion we shall discuss first in this section the notion of counter-example computation, stemming from [21, 26] and studied in [22].

Let $\Phi(x) := \exists y(|y| \leq |x|^k)\forall z(|z| \leq |x|^\ell); \phi(x, y, z)$ be a property of x with ϕ polynomial time decidable, and with x the only free parameter. A general computational task is to, given x, find y witnessing the property. The particular computation of y is performed by Student, a polynomial time algorithm, and by all-powerful Teacher.

Student first computes some y_1 (tacitly of the appropriate length) knowing only x. If it is not a valid witness Teacher provides him with a counter-example: some z_1 (again tacitly of the appropriate length) such that $\phi(x, y_1, z_1)$ fails. In the second round Student computes another candidate y_2 but now using not only x but also z_1. If it is not a witness then he gets a counter-example from Teacher, and so on.

An example of interesting properties Φ are various optimization problems. For example, a property may say that a graph x has a maximal clique y. Important results in bounded arithmetic follow from proving that, unless the polynomial time hierarchy collapses, Student cannot find a maximal clique in a constant number of rounds, cf.[21].

What we shall consider is $\Phi(x) := \mathrm{WPHP}^x_{2x}$, the dual weak pigeonhole principle (for a fixed f). Witnesses to it are exactly elements of $\{0,1\}^{|x|+1}$ outside of the range of $f_{|x|}$. In the previous example an important restriction on Student's capabilities comes from the fact that it is a polynomial time algorithm that should work for all x's. We shall abolish this restriction and we allow Student to compute with (non-uniform) polynomial size circuits. This means, equivalently, that Student can use a different polynomial time algorithm for each length n of x's. However, this itself would trivialise things: a circuit can simply output directly some fixed witness without computing anything. But we shall restrict Student in another way: we will require that he can solve the problem in constantly many rounds and that it can be proved by polynomial size EF proofs that his strategy works. This is a non-trivial restriction because if you simply have a witness y you may still not be able to prove that it is a witness as the proof may, in principle, have to go through exponentially many (in the length of x) possible counter-examples z. We define this formally in the next section.

6 Functions free for EF

We continue using the abbreviation τ_b defined before Corollary 4.2 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 6.1 *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, Student's strategy given by circuits $b_1, \ldots, b_k$ leads him in at most k steps to an element outside $Rng(f_n)$; in particular, such an element exists in a model of PV if $(*)$ has an EF-proof there, as then it is a tautology by property (2) of Section 2.

Note that 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 (this is proved analogously as the next theorem).

Theorem 6.2 *Conjecture 4.1 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 6.1) and an EF-proof of the formula **(*)**. Hence the formula **(*)** is a tautology in any model N of PV extending 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 [21] 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 $\mathrm{PV} + Diag(M_{a^*})$. 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. [18, 14]). 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.

7 Examples and remarks

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 appending 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 $\tau_{b_0} \vee \tau_{b_1}$. (This example was noticed by P. Pudlák and by A. Wigderson.) However, clearly one of b_0 or b_1 is in the range of G; say $G(a_0) = b_0$. Then substituting bits of a_0 together with bits of the computation of $G(a_0)$ into the proof of $\tau_{b_0} \vee \tau_{b_1}$ collapses τ_{b_0} to 0 and yields a proof of τ_{b_1}. Hence G is 1-restricted. Note that we can rectify this by pre-composing G with a suitable polynomial time function (depending on the particular hard bit).

Let us modify the example a bit. Assume that we have two (provably in PV) one-to-one functions g_1, g_2 for which the corresponding τ-formulas are hard to prove. Define $f(x)$ to be $(g_1(x), 0)$ if x contains an even number of ones, and $(g_2(x), 1)$ otherwise. The τ-formulas for f are hard to prove unless the restriction to inputs with even or odd number of ones respectively helps to prove the τ-formulas for g_1 or g_2 respectively. But f is 2-restricted; namely, let b_1 have the form $(b, 0)$ for $b \notin Rng(g_1)$ and $b_2(\overline{x}_1)$, a circuit, have the form $(g_2(\overline{x}_1), 1)$. Then $\tau_{b_1}(\overline{q}_1) \ \vee \ \tau_{b_2}(\overline{q}_1, \overline{q}_2)$ is easily provable.

The notion of a function free for a general proof system Q makes perfect sense and Theorem 6.2 holds for any Q that polynomially simulates EF, with PV replaced by PV $+ Con_Q$ (Con_Q is the $\forall\Pi^b_1$ sentence from Section 3). The choice of the particular theory for Q (it is unique only up to $\forall\Pi^b_1$ consequences) is important. For example, system G_2, a subsystem of quantified propositional logic G, corresponds to theory T^2_2 (cf. [3, 19, 14]). That theory proves WPHP^a_{2a} for all polynomial time functions. However, that does not imply that every such function is k-restricted for G_2, some $k \geq 1$. The proof of Theorem 6.2 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.

One may also look at proof systems for which we already have good lower bounds and some lower bound methods. For example, very interesting is the case of constant depth Frege systems. A depth d Frege system F_d operates with formulas of the depth at most d in the DeMorgan language with unbounded arity $\vee, \wedge$. In this case we would look for an AC^0 function (i.e., computable by polynomial size, constant depth formulas) that would be free for all F_d, meaning that no strategy of Student given itself by AC^0 circuits can be proved to be winning by polynomial size F_d proofs.

A simpler problem, to prove that it is consistent with PV or S^1_2 that a concrete polynomial time function f violates WPHP^a_{2a}, leads to the task to show that EF has no short proof that a uniform polynomial time Student (one algorithm for all input lengths) finds an element outside the range of the function in constantly many (for PV) or polynomially many (for S^1_2) rounds.

The EF provability is now important (for the S^1_2 case) even if we have a uniform Student instead of a circuit Student. Namely, it follows from results of Impagliazzo and Wigderson [10] (proved under a plausible complexity-theoretic assumption) that there is a polynomial time Student winning in polynomially many rounds. Let f be computable in time n^k. Impagliazzo and Wigderson [10] construct a polynomial time function g that takes $O(\log(n))$ input bits and computes $n+1$ bits, and such that no NP algorithm running in time $O(n^k)$ can distinguish a random element of $\{0,1\}^{n+1}$ from a pseudo-random element $g(x)$. This implies that $Rng(g) \not\subseteq Rng(f)$ as otherwise the property to belong into $Rng(f)$ would distinguish the random and pseudo-random strings with probability at least 1/2. Hence Student can simply consecutively list as candidates all $n^{O(1)}$ elements of $Rng(g)$, not using Teacher's counter-examples at all. The assumption their construction uses is, in this case, that there is an exponential time function that cannot be computed by a sub-exponential size circuit querying an NP property. This is true if, for example, the sub-exponential time hierarchy is properly included in EXP.

However, EF provability of the fact that such Student wins depends on formalizability of the construction in S^1_2. That is unlikely as its many counting arguments seem to presuppose some form of pigeonhole principle.

Finally, note that if f is itself a pseudo-random generator then PV does not disprove the statement that for an a and some $b < 2a$ not in the range of f, the tautology τ_b has no EF proof. Otherwise, by Herbrand's theorem as PV is a universal theory, there would be a polynomial time algorithm deciding the membership in the range of f, contradicting the pseudo-randomness of f.

Acknowledgement: I am very much indebted to the editor Andreas Blass for making numerous and detailed suggestions how to improve the paper.

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] Buss, S. R., Bounded Arithmetic. Naples, (1986), Bibliopolis. (Revision of 1985 Princeton University Ph.D. thesis.)

[4] Cobham, A, The intrinsic computational difficulty of functions, in : *Proc. Logic, Methodology and Philosophy of Science*, ed. Y. Bar-Hillel, North-Holland, (1965), pp. 24-30.

[5] 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.

[6] 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.

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

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

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

[10] R. Impagliazzo and A. Wigderson, $P = BPP$ unless E has subexponential circuits: derandomizing the XOR lemma, in: *Proc. of the 29^{th} Annual ACM Symposium on Theory of Computing*, (1997), pp. 220-229.

[11] J. Krajíček, Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universitatis Carolinae*, **30(1)**, (1989), pp. 137-140.

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

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

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

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

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

[17] 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.

[18] 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, Lecture Notes in Computer Science 440, (1990), pp. 193-210. Springer-Verlag.

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

[20] J. Krajíček and P. Pudlák, Some consequences of cryptographical conjectures for S^1_2 and EF, *Information and Computation*, Vol. **140 (1)**, (January 10, 1998), pp. 82-94.

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

[22] J. Krajíček, P. Pudlák and J. Sgall, Interactive Computations of Optimal Solutions, in: B. Rovan (ed.): Mathematical Foundations of Computer Science (B. Bystrica, August '90), Lecture Notes in Computer Science 452, Springer-Verlag, (1990), pp. 48-60.

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

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

[25] J. B. PARIS, A. J. WILKIE, and A. R. WOODS, Provability of the pigeonhole principle and the existence of infinitely many primes, *J. Symbolic Logic*, **53**, (1988), pp. 1235–1244.

[26] P. PUDLÁK, Some relations between subsystems of arithmetic and the complexity of computations, in: *Logic From Computer Science*, Proceedings of a Workshop held November 13-17, 1989 in Berkeley, ed. Y.N. Moschovakis, *Mathematical Sciences Research Institute Publication*, **21**, (1992), pp. 499-519. Springer-Verlag.

[27] P. PUDLÁK, The lengths of proofs, in: *Handbook of Proof Theory*, Ed. S. Buss, (1997).

[28] 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.

[29] A. A. RAZBOROV, Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izv. Ross. Akad. Nauk Ser. Mat.*, **59(1)**, (1995), pp. 201-224.

[30] A. A. RAZBOROV and S. RUDICH, Natural proofs, *J. of Computer and Systems Sciences*, **55(1)**, (1997), pp. 24-35.

[31] 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.

[32] URQUHART, A., The complexity of propositional proofs, *Bulletin of Symbolic Logic*, **1(4)**, (1995), pp. 425-467.

[33] YAO, A., Theory and applications of trapdoor functions, in: *Proc. of the 23^{rd} Annual Symp. on Foundation of Computer Science*, (1982), pp. 92-99.