Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds

Jan Krajíček*

Mathematical Institute†
Academy of Sciences, Prague

Abstract

This article is a continuation of our search for tautologies that are hard even for strong propositional proof systems like EF, cf.[14, 15]. The particular tautologies we study, the τ-formulas, are obtained from any $\mathcal{P}/poly$ map g; they express that a string is outside of the range of g. Maps g considered here are particular pseudorandom generators. The ultimate goal is to deduce the hardness of the τ-formulas for at least EF from some general, plausible computational hardness hypothesis.

In this paper we introduce the notions of pseudo-surjective and iterable functions (related to free functions of [15]). These two properties imply the hardness of the τ-formulas from the function but unlike the hardness they are preserved under composition and iteration. We link the existence of maps with these two properties to the provability of circuit lower bounds, and we characterize maps g yielding hard τ-formulas in terms of a hitting set type property (all relative to a propositional proof system). We show that a proof system containing EF admits a pseudo-surjective function unless it simulates a proof system WF introduced by Jeřábek [11], an extension of EF.

We propose a concrete map g as a candidate function possibly pseudo-surjective or free for strong proof systems. The map is defined as a Nisan-Wigderson generator based on a random function and on a random sparse matrix. We prove that it is iterable in a particular way in resolution, yielding the output/input ratio $n^{3-\epsilon}$ (that improves upon a direct construction of Alekhnovich et.al. [2]).

*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.

†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.

Propositional proof complexity studies the lengths of proofs of tautologies in various proof systems. The ultimate goal is to show that no proof system can prove all tautologies by proofs of size polynomial in the size of the tautology. With a general definition of proof systems as non-deterministic algorithms accepting exactly the set of tautologies (cf. [7]) the problem is equivalent to the $\mathcal{NP}/co\mathcal{NP}$ problem.

Non-trivial lower bounds to the lengths of proofs have been proved for various particular proof systems and already these partial results have deep implications.[1] All these proof systems are demonstrably weaker than the usual text-book calculus based on modus ponens and a finite number of axiom schemes, a Frege system F in the terminology of [7]. It is generally thought that a pivotal case in this research is Extended Frege system EF. EF extends F by allowing to abbreviate (possibly large) formulas by new atoms. Equivalently, one may think of EF as a Frege system operating with circuits rather than with formulas.[2]

No non-trivial lower bounds are known for either F or EF. A reason often suggested as an explanation of this is that we do not have any lower bounds for general boolean formulas or circuits. However, I do not see any evidence that understanding the circuit class a proof system operates with is either sufficient or necessary for proving lower bounds for the proof system. In fact, from all proof complexity lower bounds it is only in the case of constant depth Frege systems where a particular knowledge about AC^0 circuits (namely the effect of random restrictions) was ever relevant to the proof complexity lower bound. In all other cases (resolution, cutting planes and its generalizations, algebraic proof systems, etc.) understanding the formulas the system operates with is secondary to proof theoretic properties of the system (allowing feasible interpolation or some global characterization of shortly provable formulas in algebraic systems, width or degree arguments, decision tree/branching program arguments, etc.). Of course, for example in feasible interpolation the proof complexity lower bound is ultimately deduced from a circuit lower bound - but for monotone circuits that have nothing to do with the formulas of the system. Moreover, any proof system can be polynomially simulated by an extension of EF by a polynomial time set of tautologies as extra axioms (and natural strong systems are equal to such a system), and all these system operate with the same class of (all) circuits.

I rather think that a reason why EF lower bounds appear distant at

[1] See [25] for a survey.

[2] See [11] for a formulation.

this time is that the research concentrated essentially only on getting lower bounds for weak systems and neglected a development of a general theory of strong systems. In this respect the success of the transfer of the random restriction method from boolean complexity to constant depth Frege systems (the most important system for which we can prove lower bounds) is the Danae gift.

Another reason is a lack of examples of concrete tautologies that would make plausible candidates as being hard for EF. Researchers have proposed numerous formulas over the years. However, the only supporting evidence of the hardness of all these examples has been simply the lack of an obvious short EF-proof (this "evidence" turned out to be false rather often). One would like some candidates whose hardness could be deduced from a general plausible computational complexity assumption. The conjecture $\mathcal{NP} \neq co\mathcal{NP}$ implies that no proof system P can admit polynomial size proofs of all tautologies but it does not seem to imply lower bounds for any particular tautologies. More precisely, it only yields that any $co\mathcal{NP}$-complete set of tautologies must contain a P-hard tautology while we would like more concrete examples; for example, produced by a (probabilistic) polynomial-time algorithm. See also [16].

The only examples of a different character were defined in [6]. The formulas express the soundness of a proof system Q w.r.t. proofs of size $n = 1, 2, \ldots$. One can show that if they have polynomial size EF-proofs then proofs in Q are at most polynomially shorter than proofs in EF. Thus if we take for Q a proof system we believe to be much stronger than EF (like the quantified propositional logic G or a proof system based on ZFC) then the formulas are hard for EF. However, here we derive one lengths-of-proofs lower bound from another one (which is, in fact, equivalent to the proved statement for $Q \supseteq EF$). There is also no known Q such that one can show that it has a superpolynomial speed-up over EF, assuming some general complexity conjecture. There are, however, interesting links to Gödel's second incompleteness theorem, cf.[17].

The present work hopes to contribute to the search for tautologies hard for strong proof systems and to the understanding of these systems in general. We continue in the research line of [14, 15] linking the problem with the provability of the dual weak pigeonhole principle (dWPHP) for polynomial-time computable functions. The principle says that $g : \{0,1\}^n \rightarrow \{0,1\}^m$ is not onto, if $n < m$. The qualification "weak" reflects the fact that the principle is weaker than the usual pigeonhole principle in which it is enough to consider $\{0,1\}^m \setminus \{\overline{0}\}$ instead of $\{0,1\}^n$. Reasons why there is a connection are explained in [14, 15] and further vindicated in [11] demonstrating a relation between theory BT (BT, defined in [14], is $S^1_2(PV)$ plus instances of dWPHP for all polynomial time functions g), probabilistic computations and derandomization techniques. Various relations between the provability of the (dual) weak pigeonhole principle and complexity theory are known for a long time, starting with [22] (linking WPHP with the Linear Time Hierarchy, cf. also [13, Chpt.15]). The relation we study here focuses on proof complexity.

The most important knowledge about EF (the only knowledge, really) and stronger proof systems P is their relation[3] to bounded arithmetic (a relation similar to the relation of Turing machines and boolean circuits). This relation motivates several notions and statements in the previous as well as in the present work. However, main definitions and statements about proof systems are formulated combinatorially. The only exception is Section 5 where the use of bounded arithmetic substantially simplifies the argument.

The tautologies we are interested in are called τ-formulas[4] and have been defined in [14]. The idea to investigate them has been discovered independently by Alekhnovich et.al. [2], although the motivation has been partially different. They are defined as follows[5]. Let $g : \{0,1\}^n \to \{0,1\}^m$, $n < m$, be a boolean map computed by a size s circuit C. The set of τ-formulas corresponding to C is parameterized by $b \in \{0,1\}^m \setminus Rng(g)$. Given such b we construct propositional formula $\tau(C)_b$, or simply τ_b when C is fixed, as follows. The atoms of τ_b are $x_1, \dots, x_n$ for bits of an input $x \in \{0,1\}^n$ and auxiliary atoms $y_1, \dots, y_s$ for bit values on subcircuits of C determined by the computation of C on x. The formula expresses in a DNF that if y_j's are correctly computed as in C with input x then the output $C(x)$ differs from b. The size of τ_b is proportional to $n + s$. The formula is a tautology as $b \notin Rng(g)$. For $P \supseteq EF$ operating with circuits we can use an easier definition of τ_b not involving y_j's: τ_b is simply the disjunction $\bigvee_{i \leq m} C_i(\overline{x}) \not\equiv b_i$, where $C_i(\overline{x})$ computes the ith bit of $C(\overline{x})$.

When C is canonically determined by g (and n) we may also speak of τ-formulas from g. This never leads to a confusion. Moreover, the maps g we consider should yield hard $\tau(C)$-formulas for *any* size $n^{O(1)}$ circuit C computing them.

The working conjecture is that for a randomly behaving g the τ-formulas

[3] The reader who is interested in the relation can find an elementary exposition in [15].

[4] By a coincidence the formulas in [2] are also denoted using the letter τ, so hopefully this is a generally acceptable notation.

[5] Note that this is a different formalization of a PHP-type principle than a formalization often considered in proof complexity with atoms p_{ij} representing the statement "i maps to j".

are indeed hard for many, if not all, propositional proof systems P and that the way how to show it is to prove that one can think consistently in P that g is onto. The phrase precisely means that there is a particular model of T, a bounded arithmetic theory corresponding to P, in which g is onto. Hence one replaces the proof complexity problem by a problem to construct a model. Fortunately this can be characterized in a finitary way using the notions of functions free resp. pseudo-surjective for P, defined in [15] and in Section 3 here (the characterization depends on the exact choice of T). The task to construct a suitable model is, in principle, harder than the original task to prove the hardness of the τ-formulas. We hope that this will be compensated for by the availability of methods of logic.

The precise meaning of the qualification "randomly" in the preceding paragraph is crucial and we shall discuss this in some detail in Sections 1 and 2. Briefly, the key property of g is akin to a hitting set generator w.r.t. $\mathcal{NP}/poly$-sets.

In this paper we propose a concrete map g as a candidate function possibly pseudo-surjective or free for strong proof systems. The map is defined as a Nisan-Wigderson generator based on a random function and on a random sparse matrix. Then we introduce the notions of pseudo-surjective and iterable functions (related to free functions of [15]) and link it to the provability of circuit lower bounds, and we characterize maps g yielding hard τ-formulas in terms of a hitting set type property (all relative to a propositional proof system). This is in Sections 1, 2, 3 and 4. In Section 5 we show that a proof system containing EF admits a pseudo-surjective function unless it simulates a proof system WF introduced by Jeřábek [11], an extension of EF. Finally, in Section 6, we prove that the proposed g is iterable in a particular way in resolution, yielding the output/input ratio $n^{3-\epsilon}$, any $\epsilon > 0$.

The paper is self-contained but the reader can benefit from reading [15] for background in proof complexity and bounded arithmetic, motivations for some of the notions, and for some bibliographical information. Two particular pieces of the background we shall use are: First, any propositional proof system Q can be p-simulated by some $P \supseteq EF$. The symbol $P \supseteq EF$ means that P extends EF by a set of tautologies as extra axioms (no new rules are needed for the previous sentence to hold). Hence, when aiming at strong proof systems, the restriction to $P \supseteq EF$ is without a loss of generality (see [6, 17, 13]). All $P \supseteq EF$ prove their own soundness. Second, let $A(x) := \forall y(|y| \leq |x|^k), B(x, y)$ be a $co\mathcal{NP}$-property (i.e. a Π^b_1-formula), where $B(x, y)$ is a polynomial-time relation. For $n \geq 1$, the propositional formula $||A(x)||^n$ has n atoms for the bits of x, n^k atoms for bits of y and $n^{O(1)}$ atoms for bits of a computation by a (fixed) circuit of the relation

$B(x, y)$. The formula says that if the bits of the computation are correct then the relation $B(x, y)$ holds. Again, if we work with $P \supseteq EF$ manipulating directly with circuits we do not need the auxiliary $n^{O(1)}$ atoms encoding the computation and the translation is simply a circuit computing the relation $B(x, y)$ restricted to inputs of the right length. The issue how a circuit is associated to $B(x, y)$ is important and the reader should look in [13] for this. Note that $\tau(C)_b$ is just $||\forall x, C(x) \neq y||^m_{(\overline{y}/b)}$, where x is a priori bounded by the input size of C and $\overline{y}$ are the m bits associated to y in the translation.

We shall often consider functions $g : \{0,1\}^* \rightarrow \{0,1\}^*$ satisfying the following assumptions for some constant $c \geq 1$:

(A1) The length of the output $|g(x)| = m(n)$ depends only on the length of the input $|x| = n$, and $n < m(n) \leq n^c$, all $n \geq 1$.

(A2) Map g is in $\mathcal{P}/poly$: C_n is a size $\leq n^c$ circuit computing g on $\{0,1\}^n$ (hence it has n inputs and $m(n)$ outputs).

We shall call functions obeying condition (A1) *polynomially stretching* (or just p-stretching). Hence the statement that $g = \{C_n\}_n$ obey assumptions (A) is abbreviated by the phrase $g = \{C_n\}_n$ is a $\mathcal{P}/poly$ p-stretching function. We shall denote by g_n the function g restricted to $\{0,1\}^n$, i.e. computed by C_n.

Some notation and conventions: $[n]$ is the set $\{1, \ldots, n\}$, $\{0,1\}^{\leq \ell}$ is $\bigcup_{r \leq \ell} \{0,1\}^r$, all logarithms are base 2 and matrices and vectors are over field $\mathbf{F}_2$. dWPHP(g) denotes the instances of the dual weak pigeonhole principle for function g. $C^D(f)$ is the circuit complexity of boolean function f w.r.t. circuits querying an oracle D. For proof systems P and Q, $P \geq Q$ means that Q has at most polynomial-speed up over P. The symbols $P \vdash^s$ and $P \vdash_*$ stand for P-provable in size $\leq s$ and has poly-size P-proofs respectively. All other notions or facts not explained here can be found in [13].

1 A hitting set property

Let us note first a simple characterization of those $\mathcal{P}/poly$ p-stretching maps $g = \{C_n\}_n$ for which all corresponding $\tau(C_n)$-formulas are hard for a proof system P.

Definition 1.1 *Let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. The resultant of g with respect to P, denoted Res^P_g, is the class of all $\mathcal{NP}/poly$-sets $A \subseteq \{0,1\}^*$ such that for some definition of A:*

$$y \in A \textit{ iff } \exists z(|z| \leq |y|^k), B(y, z)$$

$B(y,z)$ a $\mathcal{P}/poly$ relation, the proof system P admits polynomial-size proofs of the propositional statements

$$||\forall x, z;\ B(y,z) \to C(x) \neq y||^{m(n)}$$

(with the bounds to the lengths of x and z implicitly polynomial in n).

The lemma generalizes [19, Thm.5.1]. That theorem states that the canonical formulas expressing the primality of a number have polynomial size EF-proofs iff there is an $\mathcal{NP}$-definition of primes whose soundness is provable in S^1_2.

Lemma 1.2 *Let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. Let $P \supseteq EF$ be a proof system. Then the following two conditions are equivalent:*

1. *There exists $t \geq 0$ such that for infinitely many $n \geq 1$ and $b \in \{0,1\}^{m(n)}$ the formula $\tau(C_n)_b$ has a P-proof of size $\leq |\tau(C_n)_b|^t = |b|^{O(t)}$.*
2. *The resultant Res^P_g contains an infinite set.*

Proof :

Consider sets U_t for $t \geq 1$ defined by:

$$U_t \ := \ \{b \in \{0,1\}^* \mid P \vdash^{|b|^t} \tau_b\}$$

Clearly all U_t are in Res^P_g, as P proves its own soundness. So if the resultant contains no infinite set only finitely many $b \in \{0,1\}^* \setminus Rng(g)$ yield a τ-formula with a P-proof of size $\leq |b|^t$. This proves the if-part of the statement.

For the opposite implication assume that A is an infinite set in the resultant. Let A be defined by the condition $\exists z(|z| \leq |y|^k), B(y,z)$, B a $\mathcal{P}/poly$ relation. In particular, all formulas

$$||(|z| \leq |y|^k \wedge B(y,z)) \ \to \ (|x| = n \to C_n(x) \neq y)||^{m(n)}$$

have P-proofs of size $m^{O(1)}$.

For $b \in A \cap \{0,1\}^m$ pick c, $|c| \leq |b|^k$, such that $B(b,c)$ holds. The formula $||B(y,z)||^m(b,c)$, with the bits of b and c substituted for the bits corresponding to the variables y and z respectively, is just a true boolean circuit of size $m^{O(1)}$. Hence it has size $m^{O(1)}$ P-proof (the evaluation of the circuit). Modus ponens yields a P-proof of τ_b of size $m^{O(1)}$.

q.e.d.

Note that if g is uniform polynomial time then the resultant contains an infinite set iff it contains a uniform $\mathcal{NP}$ infinite set. This is because U_t's are define using C_n's only as advises. We could also consider "exponential" version of the resultants, replacing "polynomial size proof" with "sub-exponential size proofs" and $\mathcal{NP}$-sets with sets in $NTime(2^{n^{o(1)}})$.

The proof of the lemma utilizes the fact that the soundness of P has short P-proofs. As mentioned earlier, this is true for all $P \supseteq EF$ and also for all known natural systems simulating EF. However, the statement can be also viewed (and was originally) as a simple model theoretic fact.[6] Let K be any infinite first-order structure, $\Theta(y)$ an existential formula in the language of K, and $b \in K$. Then there is an extension of K to a model N of a theory S (in the language of K) in which $\Theta(b)$ holds iff b satisfies in K all universal consequences of $\Theta(y)$ provable in S. Taking $\Theta(y)$ to be $\exists x(|x| \leq |y|^{\ell}), g(x) = y$, and considering only cofinal extensions N of a canonical structure M_n (defined in Section 3) to a model of T corresponding to P yields the theorem too. In this way a variant of the lemma can be proved, for example, for resolution R which does not prove its own soundness, cf.[3].

Lemma 1.2 suggests that one should thus try to find $\mathcal{P}/poly$ p-stretching maps $g = \{C_n\}_n$ such that any $\mathcal{NP}/poly$-set disjoint with its range must be small, forgetting about the condition that the disjointness is P-provable.[7] This would imply, in particular, that resultants with respect to any P must contain only small $\mathcal{NP}$-sets and that there are P-hard $\tau(g)$-formulas. Here the qualification "small" cannot mean finite because as long as we drop the P-provability we can encode into advises of the $\mathcal{NP}/poly$ sets polynomially many elements from each $\{0,1\}^m \setminus Rng(g)$. It seems that the meaning of the qualification most natural and so most useful for further research is "small density". A chief reason is the connection with pseudo-random generators. We will define a modification of the NW-generators for this purpose in the next section.

Let us summarize this discussion by a simple formal statement. It follows from the fact that for any proof system P and any polynomial $p(n)$ the set of b's for which $\tau(g)_b$ has a P-proof of size at most $p(|\tau(g)_b|)$ is an $\mathcal{NP}/poly$-set in the complement of $Rng(g)$.

[6] The name "resultant" reflects a corresponding notion in model theory which itself generalizes the well-known notion of resultant in field theory.

[7] On the other hand, finding any P for which the resultant contains a set intersecting all $\{0,1\}^n$, $n \geq 1$, is also unlikely to be easy: Assume that A is an $\mathcal{NP}$-set in the complement of the truth table function (see Definition 4.1), such that $A \cap \{0,1\}^n \neq \emptyset$, for all $n \geq 1$. Then $BPP \subseteq \mathcal{NP}$: Guess $f \in A$. So f is a function with large $C(b)$. By [21, 10] such f can be used for derandomization of BPP. I learned this example from R. Impagliazzo.

Corollary 1.3 *Let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. Let P be an arbitrary proof system and $p(n)$ any polynomial.*

Assume that there is a function $\epsilon : m \to \epsilon(m) < 1/2$ such that the density of any $\mathcal{NP}/poly$-set A in the complement of $Rng(g)$ is at most ϵ: $|A \cap \{0,1\}^m| \leq \epsilon(m) \cdot 2^m$.

Then the τ-formula $\tau(g)_b$ determined by a randomly chosen $b \in \{0,1\}^m$ requires with the probability at least

$$1 - 2^{n-m(n)} - \epsilon(m) \geq 1/2 - \epsilon(m) > 0$$

P-proofs of size bigger than $p(|\tau(g)_b|)$.

The question whether there are any $\mathcal{P}/poly$ p-stretching maps $g = \{C_n\}_n$ allowing only small density $\mathcal{NP}/poly$ sets in their complement has been considered by Rudich [29]. He defines a demi-hardness of such g_n as the minimum s such that there is a non-deterministic circuit of size $\leq s$ defining a set in the complement of $Rng(g_n)$ of size at least $s^{-1}2^{m(n)}$, and he conjectures (see the demi-bit Conjecture 5 in [29]) that there exists such g with $m(n) = n+1$ and the demi-bit hardness $2^{n^{\Omega(1)}}$. The conjecture implies that, for any P, with a probability exponentially close to 1 a random $b \notin Rng(g)$ yields the τ-formula $\tau(g)_b$ requiring an exponential size P-proof. In fact, he proposes a candidate g based on the subset-sum. There are no results in [29] supporting the conjecture.

2 Candidate τ-formulas

In this section we define a modification of the NW-generators as a candidate for g yielding hard τ-formulas. To motivate the changes we first need to briefly discuss how the NW-generators work.

Definition 2.1 ([21]) *Let $\ell \geq 1$. An ℓ-sparse matrix A is an $m \times n$ $0-1$ matrix having in each row i entry 1 in at most ℓ columns $S_i \subseteq [n]$.*

Let A be an ℓ-sparse matrix and $f : \{0,1\}^{\leq \ell} \to \{0,1\}$ be a boolean function defined on vectors of size at most ℓ. The map

$$NW_{A,f} \ : \ \{0,1\}^n \to \{0,1\}^m$$

computes from $x \in \{0,1\}^n$ vector $y \in \{0,1\}^m$ with i-th bit $y_i := f(x_{j_1}, \ldots, x_{j_u})$ for $S_i = \{j_1 < \ldots < j_u\}$, $u \leq \ell$.

Assume that we have a predicate D on $\{0,1\}^m$. We consider D as an oracle, and this oracle independence of the constructions around the NW-generators is one of the reasons for trying to adapt them for our purposes. One picks an ℓ-sparse $m \times n$ matrix A and a function $f : \{0,1\}^{\leq \ell} \rightarrow \{0,1\}$ with large hardness, and defines $g := NW_{A,f}$. If A has a suitable combinatorial property (being the so called $(\ell, \log(m))$-design, cf.[21]) then by [21, 10] the circuit complexity of f is $C^D(f) \leq O(m^2)$, assuming that D distinguishes the pseudo-random strings produced by g from truly random strings with the discrepancy at least $1/m$.

Now assume that D is computable in (non-uniform) time m^k. Then $C^D(f) = O(m^2)$ implies $C(f) = O(m^{2k})$ and to find any f of such complexity we need $\ell \geq c \cdot \log(m)$, where the parameter c grows with k. The same is true for D computable in a non-deterministic way (circuits querying D are then non-uniform analogy of the Δ_2^p level of the polynomial-time hierarchy). In other words, ℓ grows as the time complexity of D grows.

Let $C(f) = s$. So g is computed by a circuit of size $O(ms)$ and the $\tau(g)$-formulas will have size $O(ms)$ too. Hence an $\mathcal{NP}$-oracle D asking if there is a P-proof of $\tau(g)_b$ of size $\leq |\tau(g)_b|^t$ has the time complexity at least $(ms)^t >> s$. We cannot thus choose ℓ, f and s in order to have a "sufficiently" hard function for the predicates U_t from the proof of Lemma 1.2. Here it is irrelevant whether ℓ is small or large. The standard analysis of the NW-generators does not work and we cannot reduce the problem of the hardness of $\tau(g)$-formulas to the hardness of f in this way.

For the derandomization purposes it is important that one can construct (in uniform polynomial time even) suitable matrices A with $n = O(c^2 \log(m))$. This is irrelevant for our purposes and we relax these conditions as much as possible.

We propose to study maps g of the form $g := NW_{A,f}$, where $n < m < n^{O(1)}$, $\ell = O(\log(m))$, A is a random ℓ-sparse $m \times n$ matrix, and f is a random function on $\{0,1\}^{\leq \ell}$. A suitable random process yielding an ℓ-sparse matrix A is the following. For every $i \leq m$ and $u \leq \ell$ let $\mathbf{j}_{i,u}$ be chosen independently and uniformly at random from $[n]$. Let $S_i \subseteq [n]$ be the set of these values for fixed i, and define $A_{i,j} = 1$ iff $j \in S_i$. Similarly, random f on $\{0,1\}^{\leq \ell}$ is constructed by filling its truth table by random bits, independently and uniformly. Note that any such g is computed by a circuit of size $n^{O(1)}$ (as each bit is expressible by a DNF for at most $O(\log n)$ variables).

Our working conjecture is that all τ-formulas from such a g with parameters $m = n + 1$ and $\ell = c \cdot \log(n)$, $c \geq 1$ a sufficiently large constant, are hard for EF and possibly even for some stronger systems, if not for all.

In fact, we think that such a g may have a stronger property (defined in the next section) of being pseudo-surjective for EF and free even for some stronger proof systems (with m getting smaller as the proof system gets stronger).

The intuition why this should be so is that a proof system P trying to prove the unsolvability of the system of m equations $g(x) = b$ (one for each bit of b) is forced to operate with functions akin to f but defined on many large sets of inputs (that differ a lot among themselves too) and these functions are hard and thus inexpressible in P by small circuits. This should happen if sets S_i of ones in rows $i \leq m$ are interconnected in a random way or sharing a suitable expansion property of a random collection of such sets.

The first step towards establishing the conjecture could be the following question.

Problem 2.2 *Let g_n be of the form $g_n := NW_{A,f}$ with parameters $m := n+1$ and $\ell := c \cdot \log(n)$, $c \geq 1$ a sufficiently large constant, and random A and f.*

Prove under some plausible hardness assumption that g_n are hitting set generators of super-polynomial hardness. That is, the minimal s such that there is a circuit of size at most s defining a subset of $\{0,1\}^{n+1} \setminus Rng(g_n)$ of size at least $s^{-1}2^{n+1}$ is not polynomial in n.

The τ-formulas of the form $NW_{A,f}$ were studied already by Alekhnovich et.al.[2]. However, there are important differences from our set-up. In [2] bigger ℓ are allowed and, in order to express the formulas succinctly, extension variables for various boolean functions are used. In particular, they consider f that cannot be computed by small circuits from a circuit class with which the proof system operates. More important, however, seems to me be the differences in intuition why the τ-formulas for $NW_{A,f}$ should be hard: According to [2] (see the 3rd paragraph on p.5 there) a key source of the proof complexity of the τ-formulas should be the computational complexity of f. In our case the f's are computationally easy (as they depend only on logarithmically many inputs) and the presumed hardness of the τ-formulas should depend on combinatorial properties of A, taking f random.

Allowing n of size close to m brigs us to the realm of strong pseudorandom generators and one-way functions. Goldreich [8] has made an independent[8] suggestion to consider functions $NW_{A,f}$ with $n = m$, same ℓ

[8] I lectured about the candidate g and the motivation behind at the *Workshop on Complexity of Proofs and Computations* at the IAS in Princeton in December 2000. I am indebted to A. A. Razborov for pointing out reference [8] to me.

and f as above, and an explicit A having a suitable "expansion" property, as candidates for one-way functions. [8] does not contain any result supporting the conjecture.

Let me conclude with another motivation to look at the modification of the NW-generator with the proposed change in parameters. Ajtai [1] has proved a form of independence of the pigeonhole principle for bounded arithmetic $I\Delta_0(F)$ (or V_1^0 in other notation, cf. [13]). In particular, one can construct suitable models of the theory containing a bijection $F : [n+1] \rightarrow [n]$ (the map F is represented by a symbol in the language, an oracle, not by a circuit). So the $(n+1) \times n$ matrix A in which $A_{ij} = 1$ iff $F(i) = j$ defines a linear isomorphism between $\{0,1\}^{n+1}$ and $\{0,1\}^n$. It is an ideal NW-generator: From n independent bits produces $n+1$ independent bits. Hence for finite n we should try to construct matrices A simulating this property and it makes sense to start with matrices with analogous features (genericity/randomness of the entries and sparsity).

3 Pseudo-surjective functions

For the next definition we do not explicitly show all variables of the τ-formulas. Namely, the notation $\tau(C)_b(x_1, \dots, x_n)$ means that $x_1, \dots, x_n$ are the variables of $\tau(C)_b$ corresponding to the bits of an $x \in \{0,1\}^n$; the auxiliary variables y's corresponding to the bits of the computation of the circuit C will not be shown. The symbol $Var(\overline{q})$ denotes the set of circuits using variables from $\overline{q}$.

Definition 3.1 *Let P be any proof system.*

Part 1.

Let $s \geq 1$, and let C be a circuit computing a map $g : \{0,1\}^n \rightarrow \{0,1\}^m$, $m = m(n) > n$.

C is s-pseudo-surjective for P iff all disjunctions of the form

$$\tau(C)_{B_1}(\overline{q}^1) \vee \ldots \vee \tau(C)_{B_k}(\overline{q}^1, \dots, \overline{q}^k)$$

require P-proof of size $\geq s$. Here $k \geq 1$ is arbitrary, and $B_1, \dots, B_k$ are circuits such that $B_1 \in Var(\emptyset)$, $B_2 \in Var(\overline{q}^1)$, $\dots$, $B_k \in Var(\overline{q}^1, \dots, \overline{q}^{k-1})$, $\overline{q}^i$ disjoint m-tuples of atoms.

Part 2. *Let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. Let $s(n) \geq 1$ be a function.*

Then we say that g is $s(n)$-pseudo-surjective for P iff for all but finitely many $n \geq 1$ the circuit C_n is $s(n)$-pseudo-surjective for P.

Map g is (exponentially) pseudo-surjective for P iff it is $s(n)-pseudo-surjective$ for some $s(n) \geq n^{\omega(1)}$ (resp. for $s(n) \geq 2^{n^{\Omega(1)}}$).

Note that, in particular, the parameter k in Definition 3.1 may change with n and is bounded a priori only by the size of the whole proof, i.e. by $s(n)$. **Free functions**, defined in [14], are functions obeying this definition but with any constant k only[9].

The disjunction in the definition of the pseudo-surjectivity can be interpreted as an interactive protocol for computing an element outside of the range of g. The interaction goes on between an all-powerful Teacher (supplying x_i's) and $\mathcal{P}/poly$ Student (suggesting B_i's). See [15] for details of this interpretation and [20] for more information about the interactive computation model.

The pseudo-surjectivity of g is also equivalent to a model-theoretic property of g. First a little terminology. Let M be any countable non-standard model of true arithmetic in the language having symbols for all polynomial-time algorithms, computing either a function or deciding a relation. Let $n \in M \setminus \mathbf{N}$ be a non-standard element. Structures M_n and M_n^* are substructures of M with the universes $\{u \in M \mid \exists k \in \mathbf{N}, |u| \leq n^k\}$ and $\{u \in M \mid \forall k \in \mathbf{N}, |u| \leq 2^{n^{1/k}}\}$ respectively. Any structure of the form M_n will be called a **small canonical structure**, and of the form M_n^* a **large canonical structure**.

The following is proved analogously as [15, Thm.6.2], replacing PV by S^1_2 and Herbrand theorem for (Σ^b_2-consequences of) PV by a KPT-style witnessing theorem for S^1_2 where the number of disjuncts is unbounded (besides implicit polynomial upper bound); see [24, 12] or [13, Sec.7.3]. That corresponds exactly to the disjunctions in the definition of pseudo-surjectivity.

Theorem 3.2 *Let $P \supseteq EF$ and let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. Then g is pseudo-surjective (resp. exponentially pseudo-surjective) for P iff any small canonical structure M_n (resp. large canonical structure M_n^*) can be extended to a model of S^1_2 in which P is sound and where $g_n : \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ is onto.*

If g is only free for P then the extension can be guaranteed to satisfy only theory PV, cf.[15, Thm.6.2]. If we only knew that all $\tau(g)$-formulas

[9] Pseudo-surjective functions as well as iterable ones (to be defined in Def. 3.6) are variants of the concept of free functions and thus could be named by adding some adjectives to the term "free". However, we fear that this would lead to a confusion as there are enough adjectives already, and so we decided to use two new names.

are hard for P then for any $b \in M_n$ outside of the range of g we can find an extension in which b belongs to $Rng(g)$ but we may not be able to do it for two b's at the same time.

For the next definition let $C(x_1, \ldots, x_n)$ be a circuit with $m > n$ outputs.

Definition 3.3 *An iteration protocol Θ for C is a sequence of conditions*

$$C(u^1) = v^1, C(u^2) = v^2, \ldots, C(u^t) = v^t$$

where

1. *Each u^i is an n-tuple of distinct variables, each v^i is an m-tuple of distinct variables.*

2. *Every variable occurs in at most one u^i and in at most one v^i.*

3. *If a variable occurs in u^i, $i > 1$, then it also occurs in some v^j, $j < i$.*

The variables in u^1 are the input variables of Θ, the variables v^i_j that occur in no u^r are the output variables of Θ.

The size of Θ is t. The iteration protocol naturally defines a circuit (whose input/output variables are the input/output variables of Θ). It will be denoted $Iter(C/\Theta)$.

Theorem 3.4 *Let P simulates resolution. Let $C(x_1, \ldots, x_n)$ be a circuit with $m > n$ outputs. Let $\Theta := (C(u^1) = v^1, C(u^2) = v^2, \ldots, C(u^t) = v^t)$ be an iteration protocol for C of size t. Let $D(u^1_1, \ldots, u^1_n)$ be the circuit $Iter(C/\Theta)$.*

Assume that C is s-pseudo-surjective for P. Then D is $\Omega(s/t)$-pseudo-surjective for P.

Proof :

Let us start with an evident observation.

Claim: *The formula $\neg\tau(D)_y$ follows by a size $O(t)$ P-proof from formulas*

$$\neg\tau(C)_{v^1}(u^1), \ldots, \neg\tau(C)_{v^t}(u^t)$$

where the x-variables are substituted for by the variables in u^1, and the y-variables are substituted by the output variables of D (i.e. of Θ).

Assume that some disjunction of the form

$$\tau(D)_{B_1} \vee \ldots \vee \tau(D)_{B_k}$$

with the properties as in Definition 3.1 has a P-proof of size u. Hence the set $\neg\tau(D)_{B_1}, \ldots, \neg\tau(D)_{B_k}$ has a P-refutation of size $O(u)$.

By Claim, each formula $\neg\tau(D)_{B_i}$ has a size $O(t|B_i|)$ P-derivation from formulas $\neg\tau(C)_{v^1}(u^1), \ldots, \neg\tau(C)_{v^t}(u^t)$ with the output variables being substituted for by the outputs of B_i (the factor $|B_i|$ estimates the increase in the size due to the substitution).

Hence all formulas $\neg\tau(D)_{B_1}, \ldots, \neg\tau(D)_{B_k}$ can be derived in P from instances of formulas $\neg\tau(C)$ as above in the total size at most $\sum_{i \leq t} O(t|B_i|) = O(tu)$. This means that the disjunction of these instances of the $\tau(C)$-formulas have a P-proof of size at most $O(tu) + u = O(tu)$. As this $O(tu)$ must be at least s, $u = \Omega(s/t)$ follows.

It remains to verify that the disjunction so constructed obeys the condition on variables posed in Definition 3.1, which is straightforward.

q.e.d.

Assume we have a circuit $C : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ and we want to boost its output to $4n$ bits by defining $D(x_1, \ldots, x_n) = (z_1, \ldots, z_{4n})$ as follows: apply C again to the first resp. to the second n bits of the output of $C(x_1, \ldots, x_n)$. Assume that the $\tau(C)$-formulas are hard. However, this does not imply that the $\tau(D)$-formulas are also hard. For example, it can happen that for some $b_1, b_2 \in \{0,1\}^n$ the disjunction $\tau(C)_{b_1} \vee \tau(C)_{b_2}$ has a short P-proof (see [15] for other examples) and hence $\tau(D)_{(b_1,b_2)}$ has a short P-proof too.

The moral of the pseudo-surjectivity is that by establishing this stronger property for C we allow constructions of circuits by iterations, and the resulting circuits will still be pseudo-surjective and so still yield hard τ-formulas. This will be important in the next section, in the relation of the hardness of τ-formulas and the provability of circuit lower bounds.

Corollary 3.5 *Let P simulates resolution. Let $g = \{C_n\}_n$ be a $\mathcal{P}/poly$ p-stretching map. Assume that g is pseudo-surjective (resp. exponentially pseudo-surjective) for P. Let Θ_n, $n \geq 1$, be iteration protocols for C_n of size $n^{O(1)}$ (resp. of size $2^{n^{o(1)}}$). Let $D_n := Iter(C_n/\Theta_n)$.*

Then the function computed by $\{D_n\}_n$ is pseudo-surjective (resp. exponentially pseudo-surjective) for P as well.

Let $\Theta := (C(u^1) = v^1, C(u^2) = v^2, \ldots, C(u^t) = v^t)$ be an iteration protocol. As we noted in the proof of Theorem 3.4, the disjunction $\neg\tau(C)_{v^1}(u^1) \vee \ldots$ obeys, in particular, the restrictions from Definition 3.1. Moreover, if D is the circuit obtained by iterating C along Θ, and there is a P-proof of size u of a disjunction $\neg\tau(D)_{q^1}(p^1) \vee \ldots$ corresponding to an iteration protocol $\Psi := (D(p^1) = q^1, \ldots, D(p^r) = q^r)$ for D then the proof of the theorem constructs a P-proof of size $O(tr)$ of a disjunction coming from another iteration protocol for C, a "composition" of Θ and Ψ. Hence we can get by in Theorem 3.4 with a little weaker notion than pseudo-surjectivity and still preserve the iterability. It makes sense to formalize it as it may be, in principle, easier to establish that property for C in a given proof system. Indeed, this is what we do in Section 6 for resolution.

This weak notion is formalized in the next definition and theorem.

Definition 3.6 *Let P simulates resolution. A circuit is s-iterable in proof system P iff it satisfies the condition of Definition 3.1(Part 1.) with the restriction that circuits $B_1, \ldots, B_k$ are just substitutions of variables and constants for variables.*

A $\mathcal{P}/poly$ function g is $s(n)$-iterable iff the circuits computing it on inputs from $\{0,1\}^n$ are.

Theorem 3.7 *Let P simulates resolution. Let $C(x_1, \ldots, x_n)$ be a circuit with $m > n$ outputs. Let $\Theta := (C(u^1) = v^1, C(u^2) = v^2, \ldots, C(u^t) = v^t)$ be an iteration protocol for C of size t. Let $D(u_1^1, \ldots, u_n^1)$ be the circuit $Iter(C/\Theta)$.*

Assume that C is s-iterable for P. Then D is $\Omega(s/t)$-iterable for P.

The properties of g we have introduced in this section are stronger than just assuming the hardness of the $\tau(g)$-formulas: If g is free, pseudo-surjective or iterable for P then, in particular, the corresponding τ-formulas are hard for P.

4 Provability of circuit lower bounds

A prominent example of dWPHP is its instance for the truth table function (considered first by Razborov [26] in this context). It says that there is a boolean function that requires large circuits. Recall that a circuit of size s can be encoded by $c_0 s \log(s)$ bits, some fixed $c_0 > 0$.

Definition 4.1 *Let $s \geq k \geq 1$. The truth table function $\mathbf{tt}_{s,k}$ takes as input $c_0 s \log(s)$ bits describing a size $\leq s$ circuit C with k inputs, and outputs 2^k bits: the truth table of the function computed by C.*

$\mathbf{tt}_{s,k}$ is, by definition, equal to zero at inputs that do not encode a size $\leq s$ circuit with k inputs.

We think of the truth table function as of a polynomial time function defined on the whole $\{0,1\}^*$, and the parameters s and k in the notation $\mathbf{tt}_{s,k}$ just determine how large circuits the function considers when computing truth tables of functions in k variables. Note that for $\delta < 1$, $s = 2^{\delta k}$, and $n = 2^k$, $\mathbf{tt}_{s,k}$ maps $\{0,1\}^{n^{(1-\Omega(1))}}$ into $\{0,1\}^n$, i.e. from a smaller set into a bigger one.

The following theorem can be seen as a propositional version of a theorem of Jeřábek [11] that the dWPHP for polynomial-time functions is axiomatized, over S^1_2, by the dWPHP for the function $\mathbf{tt}_{s,k}$, where $s = 2^{\delta k}$, any fixed $\delta > 0$. In fact, for $P \supseteq EF$ and pseudo-surjectivity it can be deduced from Jeřábek's theorem using Theorem 3.2. We give instead a proof-theoretic argument that applies to any P at least as strong as resolution and also to iterability (for which a model-theoretic characterization analogous to Theorem 3.2 is somewhat unnatural as it deals with substructures of models of S^1_2).

Theorem 4.2 *Assume that P simulates resolution. Then the following hold:*

1. *There exists a g (exponentially resp.) pseudo-surjective for P iff for any $0 < \delta < 1$, the truth table function $\mathbf{tt}_{s,k}$ with $s = 2^{\delta k}$ is (exponentially resp.) pseudo-surjective for P too.*

2. *There exists a g is exponentially pseudo-surjective for P iff there is $c \geq 1$ such that for $s = k^c$ the truth table function $\mathbf{tt}_{s,k}$ is exponentially pseudo-surjective for P.*

3. *Both statements 1. and 2. hold if pseudo-surjectivity is replaced by iterability.*

This theorem is the chief (but not only) reason for introducing the pseudo-surjectivity property. It is not known to be valid if the pseudo-surjectivity is replaced by weaker properties of hardness of $\tau(g)$-formulas or freeness.

Proof :

The if-parts are trivial in all three statements, so we need to prove only the only-if parts. We start with the first statement, and analyzing its proof we derive the other two statements at the end.

We want to amplify first g to get at least n^2 outputs. Assume $m(n) < n^2$, say $m(n) = n+1$ for the worst case. Compose C_n with itself n -times, always applying C_n to the first n bits of the intermediate results. This gives C'_n

with $2n$ output bits. Then compose C'_n with itself along the binary tree (as in the remark after Theorem 3.4) of depth $O(\log n)$ to get n^2 output bits. The resulting $C''_n : \{0,1\}^n \to \{0,1\}^{n^2}$ was obtained from C_n by an iteration protocol of size $O(n)$ and so C''_n is, by Theorem 3.4, also (exponentially) pseudo-surjective. So without a loss of generality we will assume in the next that already C_n outputs n^2 bits.

We could continue now by an iteration along the binary tree. However, to get better estimate on the complexity of the resulting circuit (useful in Theorem 4.3) we shall proceed differently. Compose C_n along the n-ary tree. That is, define $C_n^{(1)}(x) := C_n(x)$ and $C_n^{(i+1)}(x)$ as $(C_n^{(i)}(y^1), \dots, C_n^{(i)}(y^{n^i}))$, where $C_n^{(i)}(x) = (y^1, \dots, y^{n^i})$ and all y's are from $\{0,1\}^n$. So $C_n^{(i)} : \{0,1\}^n \to \{0,1\}^{n^{i+1}}$. Note that $C_n^{(i)}$ is defined by an iteration protocol of size $O(n^i)$ and so is, for any fixed $i \geq 1$, also (exponentially) pseudo-surjective by Theorem 3.4.

Denote $t := |C_n|$. Assume $n^{i_0+1} = 2^k$ (disregarding some of the bits if n^{i_0+1} is not a power of 2) and let $w < 2^k$ be arbitrary. Hence we may think of w as a member of $\{0,1\}^k$. Let $a \in \{0,1\}^n$ and $b \in \{0,1\}^{2^k}$ be $b = C_n^{(i_0)}(a)$. Think of b as the truth table of a function, denoted also b, from $\{0,1\}^k$ to $\{0,1\}$. The w-th bit of b is simply the value of the function b on w. It is easy to see that there is a circuit E that computes $b(w)$ given a and w, and whose circuit size is $O(i_0 t)$: it computes as $C_n^{(i_0)}$ (hence the factor $O(t)$) but only along the branch of depth i_0 (hence the factor i_0) in the n-ary tree leading to the part of b containing the w-th bit.

Given $\delta < 1$ we fix $i_0 \geq 1$ such that $O(t i_0) \leq n^{\delta(i_0+1)}$. As $t = n^{O(1)}$, such a constant i_0 (depending on δ and the $O(1)$-exponent in $t = n^{O(1)}$ but not on n) exists.

It remains to turn this informal argument into a proof of the (exponential) pseudo-surjectivity of $\mathbf{tt}_{s,k}$. We have not been specific about a circuit that computes $\mathbf{tt}_{s,k}$. An inductive property we shall need is that if a circuit F is $F_1 \wedge F_2$ then there is a polynomial size resolution proof of the fact that $\mathbf{tt}_{s,k}(F)$ is obtained from $\mathbf{tt}_{s,k}(F_1)$ and $\mathbf{tt}_{s,k}(F_2)$ by a coordinate-wise conjunction (and similarly for other connectives).

We also need to fix an encoding of circuits with a particular property. We think of the usual encoding, that describes circuit as a straight line program with consecutively numbered nodes, and each node labelled by a connective, variable, or a constant, and by indices of its input nodes. Some constants in circuits we shall consider will have special role and we shall denote this by semicolon $F(p; x)$. We assume that the code $\lceil F(p; x) \rceil$ of this circuit is a string of 0, 1 and atoms from p. In this way for any particular substitution $p := a \in \{0,1\}^n$, the code $\lceil F(a;x) \rceil$ of $F(a;x)$ is obtained by the same substitution from $\lceil F(p;x) \rceil$. This can be achieved simply by encoding when at position of a node with in-degree 0 corresponding to some atom p_i the code expects 0 or 1 and not the index of a variable. This is only a technical requirement about the encodings of circuits, not about the truth table function. It will be need only in the proof of Part 3. of the theorem.

Let us now continue with the proof of Part 1..

Claim 1: *There is a P-proof of size $2^{O(k)}$ of $\bigwedge_{w \in \{0,1\}^k} E(p;w) = b_w$ from the hypothesis $D(p) = b$. Here $D = Iter(C_n/\Theta)$, where Θ is the protocol used above for iterating C_n.*

This is because for any fixed w, $E(p;w)$ with p interpreted as input computes exactly as C_n along the branch of the tree leading to b_w, and the computation of C_n along all branches is a part of the definition of D.

Claim 2: *There is a P-proof of size $2^{O(k)}$ of $\mathbf{tt}_{s,k}(\lceil E(p;w) \rceil) = b$ from the hypothesis $\bigwedge_{w \in \{0,1\}^k} E(p;w) = b_w$.*

This amounts to proving that the truth table function indeed computes the truth tables, and it is proved by induction on the size of E using the inductive properties of $\mathbf{tt}_{s,k}$ we described before Claim 1. As $|E| = O(i_0|C_n|) = n^{O(1)}$ this can be done in size $n^{O(1)}2^{O(k)} = 2^{O(k)}$.

Now we are ready to conclude the proof of Part 1. Assume that there is a P-refutation of some set of equations

$$\mathbf{tt}_{s,k}(x^1) = B^1, \mathbf{tt}_{s,k}(x^2) = B^2(x^1), \ldots, \mathbf{tt}_{s,k}(x^u) = B^u(x^1, \ldots, x^{u-1})$$

Substitute $x^1 := \lceil E(p^1;w) \rceil$ (p^1 an n-tuple of new atoms) and derive the substitution instance of the first equation $\mathbf{tt}_{s,k}(\lceil E(p^1;w) \rceil) = B^1$ from $D(p^1) = B^1$ by a P-proof of size $2^{O(k)}$, using Claims 1 and 2. Then substitute $x^2 := \lceil E(p^2;w) \rceil$ and derive the substitution instance of the second equation $\mathbf{tt}_{s,k}(\lceil E(p^2;w) \rceil) = B^2(\lceil E(p^1;w) \rceil)$ by a size $2^{O(k)}$ P-proof from the hypothesis $D(p^2) = B^2(\lceil E(p^1;w) \rceil)$.

In this way we transform the original refutation into a refutation of equations $D(p^1) = F^1, D(p^2) = F^2(p^1), \ldots$ where $F^1 = B^1$, $F^2(p^1) = B^2(\lceil E(p^1;w) \rceil)$, etc. The size of the new refutation is longer than the size of the original refutation by a factor $2^{O(k)}$. So if C_n is (exponentially) pseudo-surjective, so is D (by Theorem 3.4), and hence $\mathbf{tt}_{s,k}$ is too.

To prove Part 2. assume that 2^{n^ϵ} is a lower bound from the hypothesis of exponential pseudo-surjectivity of C_n. Pick $0 < \delta < \epsilon$. We iterate C_n as before along the n-ary tree but now creating 2^{n^δ} outputs. The size of the protocol is $O(2^{n^\delta})$ and so D constructed in this way is exponentially pseudo-surjective too (by Theorem 3.4).

The circuits E for functions in $k := n^\delta$ unknowns have size $O(|C_n|n^\delta) = n^{O(1)} = k^{O(1)}$. Hence for $s := k^c$, some suitably large $c > 0$, $\mathbf{tt}_{s,k}$ is exponentially pseudo-surjective. This proves Part 2.

Part 3. follows by inspection of the proof of the first two parts. Namely, we need only that the substitutions $x^1 := \lceil E(p^1; w) \rceil, \dots$ substitute atoms from $p^1, \dots$ and constants for variables. Hence the requirement from the definition of iterability that B^i's are just substitutions of variables and constants for variables is not altered by the substitutions $x^1 := \lceil E(p^1; w) \rceil, \dots$ used in the construction.

q.e.d.

Informally, if P proves circuit lower bounds for a class of circuits then, depending on the rate of the lower bounds and on the class, it rules out a class of circuits as pseudo-surjective/iterable for P. In particular, we do not expect that all proof systems will admit pseudo-surjective/iterable circuits. This is because we hope that a strong lower bound can be eventually proved for some explicit function (say in E). Then P associated to the theory in which the proof is carried out will have short proof of the $\tau(\mathbf{tt}_{s,k})$-formula for the truth table of the function (if it is in E then its truth table can be recognized in time polynomial in the size of the truth table). Hence such P cannot admit pseudo-surjective/iterable functions.

On the other hand, I know of no such conditional limitation for free functions: A model-theoretic characterization of freeness in [15] analogous to Theorem 3.2 uses models of theory PV and PV does not seem to allow a general iteration of functions needed in the proof of Theorem 4.2.

There is an a priori lower bound on the trade-off between the circuit complexity and the output/input ratio of functions, should they be pseudo-surjective or iterable for strong proof systems. Let us give an example.

Theorem 4.3 *No AC^0-map outputting at least $n^{1+\Omega(1)}$ bits is iterable or pseudo-surjective for a proof system that admits a polynomial size proof of an $2^{\Omega(n)}$ lower bound to AC^0-circuits..*

Proof :

By the proof of Theorem 4.2, the iteration of an AC^0-circuit C with $n^{1+\Omega(1)}$ outputs yields an AC^0-circuit D, say of depth d (depending on the depth of C and on the $\Omega(1)$ constant).

q.e.d.

No lower bound to AC^0-circuits of the rate $2^{\Omega(n)}$ is known at present. But note that EF proves an exponential lower bound for constant depth circuits computing the parity (unfortunately this lower bound is only of the form $2^{n^{\Omega(1)}}$). In [13, Sec.15.2] this is done in $PV_1 + WPHP(PV_1)$ but for the formalization in which the function is given by its polynomial-time definition and not by the truth table. In the latter case the WPHP is used only for logarithmically small parameters, and for such parameters the WPHP is provable in PV_1 (cf. [13]).

It is not the case that we can simply take theory T proving (or axiomatized by) dWPHP, and hence to show that no g is pseudo-surjective for the corresponding P. The reason is that T has to be universal in a language with polynomial-time function and predicates (perhaps augmented by $S^1_2(PV)$) and we do not have, a priori, any such T proving dWPHP for polynomial-time functions. Theorem 4.2 shows that the only way how such a T can prove dWPHP is to prove an explicit (in the sense of the disjunction from the definition of freeness or pseudo-surjectivity) circuit lower bound. No such theory is in sight, no matter how strong (e.g. the universal consequences of ZFC in the appropriate language). This yields some additional credit to the conjecture that even strong P may admit free or pseudo-surjective functions.

A connection between various forms of WPHP and circuit lower bounds has been noted originally by Razborov [26]. However, his construction is different. Namely, assume that we can consistently think in P (i.e. we have strong lower bounds) that a map F is, say, a bijection between 2^k and $t << 2^k$. Then all truth assignments to k variables can be enumerated using F by numbers $< t$. Consequently, we cannot disprove that every boolean function has a DNF with $\leq t$ clauses and, in particular, we cannot prove $>> O(tk)$ circuit lower bounds. By proving lower bounds for (various forms of) WPHP(F) in P one thus proves also the independence of circuit lower bounds in P, i.e. lower bounds for the size of P-proofs of the τ-formulas for suitable $\mathbf{tt}_{s,k}$; see e.g. [27] for the strongest result of this form.

The construction has less to do with circuits; one simply enumerates a large set by a smaller set of indices. Also, it cannot work even for systems a bit stronger that resolution (like $R(\log)$), as these systems do admit short proofs of WPHP(F). The remark on p.4 of [2] is meant to suggest a way how to overcome this limit: Construct g of the form $NW_{A,f}$ yielding P-hard τ-formulas with $m \geq 2^{n^{\Omega(1)}}$. Then interpreting $b \in \{0,1\}^m$ as the truth table of a boolean function b^* in $k \geq n^{\Omega(1)}$ variables allows to compute b^* by a size $O(n + C(f))$ circuit. If $C(f) = n^{O(1)}$ this yields $C(b^*) = k^{O(1)}$, i.e. P cannot prove superpolynomial circuit lower bounds. The price to be paid for this construction is that now ℓ (the number of ones in a row) cannot be small (must be at least $n^{\Omega(1)}$) and one cannot take a random function on ℓ variables but some suitable polynomial size computable one (or, at least, in $\mathcal{NP} \cap co\mathcal{NP}$), and encode the circuit computing it into the τ-formula.

The notions of pseudo-surjective and iterable circuits offer an alternative approach towards lower bounds for the $\tau(\mathbf{tt}_{s,k})$-formulas.

Let me conclude the section with a general comment. We are not interested in an interpretation of the hardness of the $\tau(\mathbf{tt}_{s,k})$-formulas as saying that $\mathcal{NP} \not\subseteq \mathcal{P}/poly$ (or its variants depending on the actual s) are unprovable in some weak formal systems. If one is interested in such unprovability of complexity conjectures then I think still the strongest such statement is that a theory corresponding to a proof system (containing EF) does not prove super-polynomial lower bounds for the system, cf.[18].

We are interested in $\tau(\mathbf{tt}_{s,k})$ as they are, in the sense of pseudo-surjectivity, the canonical hard τ-formulas. But we may note in this context that it is well-know (see [17, 13]) that *any* super-polynomial lower bound for P implies that P does not disprove the conjecture $\mathcal{NP} \not\subseteq \mathcal{P}/poly$ (this seems to me be the most interesting of the possible independence/consistency results about complexity, cf. the last page in [13]). Formally, in propositional logic, this means that if $Sat_n(\overline{x}, \overline{y})$ is a canonical circuit expressing that $\overline{x} = (x_1, \ldots, x_n)$ is a truth assignment satisfying the formula (encoded by) $\overline{y} = (y_1, \ldots, y_n)$ and $D(\overline{y})$ is any size $n^{O(1)}$ circuit with n outputs then no implication of the form $Sat_n(\overline{x}, \overline{y}) \to Sat_n(D(\overline{y}), \overline{y})$ has a polynomial size P-proof.

5 Pseudo-surjective functions and WF

Jeřábek [11] has found an elegant extension of EF corresponding to the theory BT (mentioned in the introduction). Let CF (Circuit Frege) be a formulation of EF as a Frege system working directly with circuits, cf. [11] for a formulation.

Definition 5.1 ([11]) *Associate with all circuits $C(x_1, \ldots, x_n)$ with m outputs, $m > n$, an m-tuple of different variables $y_1^C, \ldots, y_m^C$. Different circuits are assigned disjoint tuples of variables.*

WF is CF together with new axioms of the form:

$$C(D_1, \ldots, D_n) \not\equiv (y_1^C, \ldots, y_m^C)$$

where $D_1, \ldots, D_n$ are arbitrary circuits (that may contain y_i^C's as well as y_j^E's for other circuits E).[10]

It is not known if EF simulates WF but WF itself p-simulates (by [11]) the Unrestricted Extended Nullstellensatz proof system $UENS$ of [5]. $UENS$ p-simulates EF and is not known to be simulated by it.

Theorem 5.2 *Let $P \supseteq CF$ be a proof system that does not admit any pseudo-surjective circuit. Then $P \geq WF$.*

Proof :

Let M_n be a canonical structure. Let $\pi \in M_n$ be a WF-proof of formula α. It is enough to prove that in any cofinal extension N of M_n, that is a model of S_2^1 and in which P is sound, the formula α is a tautology.

Let $C^i(D_1^{i,j}, \ldots, D_{n_i}^{i,j}) \not\equiv (y_1^{C^i}, \ldots, y_{m_i}^{C^i})$, $m_i > n_i$, and $1 \leq i \leq t$, $1 \leq j \leq s_i$ be all special axioms of WF used in π.

By the hypothesis of the theorem no C^i is pseudo-surjective for P. So no C^i is pseudo-surjective for P in N either. The P-provable disjunctions witnessing these facts are, by the soundness of P, tautologically valid in N.

Claim: *No C^i is onto in N. In N, there is a t-tuple $b = (b^1, \ldots, b^t)$, $b^i \in \{0,1\}^{m_i}$, such that $b^i \notin Rng(C^i)$, for all $i \leq t$.*

Fix one $i \leq t$, and let

$$\tau(C^i)_{B^1} \vee \ldots \vee \tau(C^i)_{B^k}$$

be a tautological disjunction in N witnessing the non-pseudo-surjectivity of C^i. By S_2^1 find maximal $r \leq k$ such that there is an r-tuple $a^1, \ldots, a^r \in \{0,1\}^{n_i}$ for which it holds

$$C^i(a^1) = B^1 \wedge \ldots \wedge C^i(a^r) = B^r(a^1, \ldots, a^{r-1})$$

As the above disjunction is a tautology in N, $r < k$, and $B^{r+1}(a^1, \ldots, a^r)$ is outside the range of C^i. Doing this simultaneously for all $i \leq t$ gives us the wanted t-tuple b.

Substituting (in N) for $y_j^{C^i} := b_j^i$ makes all special axioms in π tautologically valid. Hence π becomes an CF derivation of α from tautologically valid formulas. As CF is sound, α is a tautology in N too.

q.e.d.

[10] Jeřábek [11] defines WF in an equivalent but slightly different way in order to simplify the proof of its soundness in BT.

6 Iterability of the NW-generator in resolution

The notion of iterability (pseudo-surjectivity) and theorems in Sections 3 and 4 (with the exception of Theorem 3.2) hold for all proof systems containing at least resolution. While our primary goal are strong systems, we will prove here a particular form of iterability for resolution. In particular, we shall consider $NW_{B,\oplus}$ based on a sparse $n^{2-\Omega(1)} \times n$-matrix and the parity function, and we shall prove that it is exponentially iterable in resolution by a protocol that is a particular depth 1 tree. This will yield an output/input ratio $n^{3-\epsilon}$, any $\epsilon > 0$, which is somewhat better that $o(n^2)$ obtained by a direct construction in [2] (although Razborov [28] has announced recently an improvement to $n^{o(\log n)}$ and even for systems $R(k)$ with small k).

Let us clarify the output/input ratio of what we want to maximize. As shown in Section 4, a way to get lower bounds for the τ-formulas from $\mathbf{tt}_{s,k}$ (and for as small s as possible) is to show lower bounds for iterability along protocols with as much outputs as possible. Hence we aim at proving exponential lower bounds for iterability of $NW_{B,\oplus}$ along a particular iteration protocol with many outputs.

The corresponding thing in the direct approach of [2] is to prove lower bounds for τ-formulas from g with as many outputs $m(n)$ as possible (see the remark after Theorem 4.3). This enforces large ℓ (say, at least $n^{\Omega(1)}$) and a need for encodings of computations of g. Specifically, they need lower bounds for τ-formulas from g with as many outputs as possible and under the functional encoding (cf.[2, 2.3]).

These two approaches are analogous to two ways how to get a pseudo-random function generator: either by iteration of a pseudo-random number generator or by a direct construction.

Thus, for the consequences about $\tau(\mathbf{tt}_{s,k})$, one is not particularly interested in lower bounds for τ-formulas based on a sparse $m \times n$ matrix with large m. In fact, exponential lower bounds for such formulas for any $m = n^k$ follow quite easily by the same proof as we shall give for Theorem 6.6, or from [2, Thm.3.1] if one disregards the terms coming in from the encoding.

Definition 6.1 ([2, Def.2.1]) *Let A be an $m \times n$ matrix. A boundary of a set of rows $I \subseteq [m]$, denoted $\partial_A(I)$, is the set of $j \in [n]$ such that exactly one entry A_{ij} equals 1 for $i \in I$.*

Let $1 \leq r \leq m$, $\ell \leq n$ and $c > 0$ be any parameters. An $m \times n$ matrix is an (r, ℓ, c)-expander iff A is ℓ-sparse and for all $I \subseteq [m]$, $|I| \leq r$, $|\partial_A(I)| \geq c|I|$.

Recall from Section 2 the random process for getting an ℓ-sparse $m \times n$

matrices. The following theorem is proved by estimating the expected size of $|\bigcup_{i\in I} S_i|$ for $I \subseteq [m]$ of size $|I| \leq r$.

Theorem 6.2 ([2, Thm.5.1]) *There is $\alpha > 0$ such that for any parameters $1 \leq \ell \leq n$ the random ℓ-sparse $n^2 \times n$-matrix is an $(\frac{\alpha n}{\ell} n^{-(1/\alpha\ell)}, \ell, \frac{3}{4}\ell)$-expander with probability at least $1/2$.*

In particular, for any $\delta > 0$ there is $\ell > 1$ such that for all n large enough the random ℓ-sparse $n^2 \times n$-matrix is an $(n^{1-\delta}, \ell, \frac{3}{4}\ell)$-expander with probability at least $1/2$.

Proof :

The first part is exactly [2, Thm.5.1], and it immediately implies the second part.

q.e.d.

Let us fix for the next few definitions and lemmas an $m \times n$ $(r, \ell, \frac{3}{4}\ell)$-expander A. For $I \subseteq [m]$ let $J(I) := \{j \in [n] \mid \exists i \in I, A_{ij} = 1\}$ and let A_I be the $(m - |I|) \times (n - |J(I)|)$ matrix obtained from A by deleting all rows in I and columns in $J(I)$. Note that $J(I) = \bigcup_{u\in I} S_u$.

In the next lemma we slightly append the original formulation, adding to it what is really proved.

Lemma 6.3 ([2, L.4.6]) *For any set of rows $I \subseteq [m]$ of size $|I| \leq r/2$ there is $\hat{I} \supseteq I$, $|\hat{I}| \leq 2|I|$, such that*

(*) For any $i \notin \hat{I}$, $|S_i \setminus J(\hat{I})| \geq \ell/2$.

Moreover, for any $\hat{I}$ of size $|\hat{I}| \leq r$ having this property $(*)$, $A_{\hat{I}}$ is an $(r, \ell, \frac{1}{4}\ell)$-expander. Furthermore, there exists the smallest (w.r.t inclusion) such an $\hat{I}$.

Definition 6.4

1. *Any I satisfying the condition $(*)$ from Lemma 6.3 is called a safe set of rows.*
2. *A partial assignment $\rho :\subseteq \{x_1, \ldots, x_n\} \to \{0, 1\}$ is called safe iff $dom(\rho) = \bigcup_{i\in I} S_i$, for some safe I.*

   We pick any such I and call it the support of ρ, denoted $supp(\rho)$.
3. *Let $b \in \{0, 1\}^m$. A safe partial assignment ρ with support I is a safe partial solution of $A \cdot x = b$ iff for all $S_i \subseteq J(I)$, $\bigoplus_{j\in S_i} \rho(x_j) = b_i$.*

4. *For ρ a safe partial solution with support I, b^ρ is an $(m - |I|)$-vector with the ith coordinate being $b_i \oplus \bigoplus_{j \in S_i \cap dom(\rho)} \rho(x_j)$, for i such that $S_i \not\subseteq dom(\rho)$.*

   Vector x_I consists of those variables not in $J(I)$.

Note that if ρ is a safe solution with support I, and ξ is a solution of $A_I \cdot x_I = b^\rho$, then $\rho \cup \xi$ is a solution of $A \cdot x = b$.

Lemma 6.5 *Let $I \subseteq I' \subseteq [m]$ be two safe systems, with $|I' \setminus I| \leq r$. Assume that ρ is a safe assignment with support I. Let $b_i \in \{0,1\}$, $i \in I' \setminus I$, be arbitrary.*

Then ρ can be extended to a safe assignment ρ' with support I' such that $\bigoplus_{j \in S_i} \rho'(x_j) = b_i$, for all $i \in I' \setminus I$.

Proof :

By Lemma 6.3, A_I is an $(r, \ell, \frac{1}{4}\ell)$-expander. By the expansion property, every nonempty subset of $I' \setminus I$ has a non-empty border in A_I and hence, in particular, cannot constitute a linearly dependent set of rows of A_I. Thus the linear system

$$\bigoplus_{j \in S_i \setminus dom(\rho)} x_j = b_i \oplus \bigoplus_{j \in S_i \cap dom(\rho)} \rho(x_j)$$

has a solution ξ. Put $\rho' := \rho \cup \xi$.

q.e.d.

For $\epsilon > 0$ let B_ϵ be the submatrix of A consisting of the first $n^{2-\epsilon}$ rows. We shall denote (the circuit computing) $NW_{B_\epsilon,\oplus}$ as $B_\epsilon \cdot x$. For the next theorem let Θ_ϵ be the iteration protocol consisting of the following formulas:

- $B_\epsilon \cdot x = (y^1_1, \ldots, y^1_n, \ldots, y^{n^{1-\epsilon}}_1, \ldots, y^{n^{1-\epsilon}}_n)$
- $B_\epsilon \cdot y^i = (z_{(i-1)n^{2-\epsilon}+1}, \ldots, z_{in^{2-\epsilon}})$

where $y^i = (y^i_1, \ldots, y^i_n)$ for $i \leq n^{1-\epsilon}$, and z is an $n^{3-2\epsilon}$-tuple of variables.

The following theorem will be proved by proving a lower bound on the width of the proof in a way analogous to the width lower bound for resolution proofs of Ramsey theorem in [14].

Theorem 6.6 *For any $\epsilon > 0$ there is $\delta > 0$ such that the following holds. Let B_ϵ and Θ_ϵ be as above. Let $b \in \{0,1\}^{n^{3-2\epsilon}}$ be arbitrary.*

Then any resolution refutation of $\Theta_\epsilon(z/b)$ must have the size at least $2^{n^{1-\delta}}$.

Proof :

Denote by b^i the $n^{2-\epsilon}$-tuple $(b_{(i-1)n^{2-\epsilon}+1}, \ldots, b_{in^{2-\epsilon}})$. We shall denote the coordinate in y corresponding to y^i_j simply also y^i_j rather than $(i-1)n+j$, and the set of ones in the corresponding row of B_ϵ by $S_{y^i_j}$.

Let π be a resolution refutation of $\Theta_\epsilon(z/b)$. Let w denote the width of π, i.e. the maximal cardinality of a clause in π. We shall construct a sequence of clauses $C_0, \ldots, C_e$ occurring in π and a sequence of partial safe assignments $\alpha_t :\subseteq \{x_1, \ldots, x_n\} \rightarrow \{0,1\}$ and $\beta^i_t :\subseteq \{y^i_1, \ldots, y^i_n\} \rightarrow \{0,1\}$, $i \leq n^{1-\epsilon}$, $t = 0, \ldots, e$ such that the following conditions are satisfied:

1. $C_0 := \emptyset$ is the end clause of π, i.e. the empty clause. Any C_{t+1} is a hypothesis of an inference in π yielding C_t, and C_e is an initial clause.

2. If x_j occurs in C_t then $x_j \in dom(\alpha_t)$, and if y^i_j occurs in C_t then $y^i_j \in dom(\beta^i_t)$.

3. y^i_j gets a value by α_t (i.e. if the row $S_{y^i_j} \subseteq dom(\alpha_t)$) then $y^i_j \in dom(\beta^i_t)$ and $\beta^i_t(y^i_j) = \bigoplus_{x \in S_{y^i_j}} \alpha_t(x)$.

4. β^i_t is a partial safe solution of $B_\epsilon \cdot y^i = b^i$.

5. C_t is false under the assignments α_t, β^i_t's.

6. Let $w_x(C)$ and $w_y(C)$ denote the number of occurrences of the x-literals and y-literals in C respectively. Then $|supp(\alpha_t)| \leq 2w_x(C_t)$ and $\sum_i |supp(\beta^i_t)| \leq 4w_x(C_t) + 2w_y(C_t)$.

Put all α_0 and β^i_0 equal to $\emptyset$. Assume we have C_t and α_t, β^i_t's, and that C_t has been inferred in π

(a) either from $D_1 \cup \{y^i_j\}$ and $D_2 \cup \{\neg y^i_j\}$,

(b) or from $D_1 \cup \{x_j\}$ and $D_2 \cup \{\neg x_j\}$.

In case (a) extend the support of β^i_t by some row containing j, and let I be the smallest safe set of rows containing this row and $supp(\beta^i_t)$. Such I

exists, by Lemma 6.3, provided $|supp(\beta^i_t)| + 1 \leq 4w_x(C_t) + 2w_y(C_t) + 1 \leq 4w + 1 \leq r/2$, i.e. if $w < r/8$. Extend β^i_t to γ, a partial safe solution to $B_\epsilon \cdot y^i = b^i$, with support I. This can be done by Lemma 6.5. If $\gamma(y^i_j) = 0$, put $C_{t+1} := D_1 \cup \{y^i_j\}$, else put $C_{t+1} := D_2 \cup \{\neg y^i_t\}$. Let $\beta^i_{t+1} \subseteq \gamma$ be minimal safe solution of $B_\epsilon \cdot y^i = b^i$ covering all y^i-variables occurring in C_{t+1} and satisfying the condition 3. w.r.t. α_t. Further put $\alpha_{t+1} \subseteq \alpha_t$ and $\beta^v_{t+1} \subseteq \beta^v_t$ for all $v \neq i$ to be the minimal assignments satisfying the conditions 2.-6..

In case (b) we proceed as follows. Let $I \supseteq supp(\alpha_t)$ be a minimal safe set with some row containing j. Let $I^i \supseteq supp(\beta^i_t)$ be minimal safe systems such that any j for which $S_{y^i_j} \subseteq J(I^i)$ (this is in order to extend β^i_t's to all y^i_j's that will get a value by α_{t+1}). Let ${\beta'}^i_{t+1}$ be a partial safe solution of $B_\epsilon \cdot y^i = b^i$ with support I^i (it exists by Lemma 6.5 as long as $|I^i| \leq r/2$). Let ${\alpha'}_{t+1}$ extend α_t to a safe solution of all equations $\bigoplus_{x \in S_{y^i_j}} {\alpha'}_{t+1}(x) = {\beta'}^i_{t+1}(y^i_j)$. Finally, let $\alpha_{t+1} \subseteq {\alpha'}_{t+1}$ and $\beta^i_{t+1} \subseteq {\beta'}^i_{t+1}$ be minimal assignments obeying conditions 2. and 3.

Condition 6. remains valid throughout the construction as $supp(\alpha_t)$ is obtained by Lemma 6.3 from, at most, one row per x-variable in C_t (i.e. $|supp(\alpha_t)| \leq 2w_x(C_t)$) and $supp(\beta^i_t)$ from, at most, one row per y^i-variable in C_t ($\leq w_y(C_t)$) and one row per variable y^i_j getting a value by α_t (at most $2w_x(C_t)$ of them).

Now note that conditions on C_e and the assignments lead to a contradiction. C_e is an initial clause and so its asserts either the validity of an equation in $B_\epsilon \cdot x = y^i$ or of an equation in $B_\epsilon \cdot y^i = b^i$. But all those equations are indeed satisfied by conditions 3. and 4. This contradicts condition 5.

We have constructed the sequence under the assumption that $w < r/8$. Hence $w \geq r/8$. The width-size relation proved in [4] implies that the size of π is at least $\exp(\Omega(\frac{(w-\ell)^2}{n}))$, as ℓ bounds the width of the initial clauses. By Theorem 6.2 there is B_ϵ with $r \geq n^{1-\delta/2}$ and ℓ a constant. For such B_ϵ, the size of π is at least $\exp(\Omega(n^{1-\delta}))$.

q.e.d.

It would be interesting to modify this argument to get an exponential iterability of $B_\epsilon \cdot x$ in resolution, irrespective of an iteration protocol.[11]

[11] Razborov [28] pointed out subsequently that any proof of an exponential lower bound for τ_b that uses only an "expansion property" of matrix A automatically yields also exponential iterability. Hence the question has an affirmative answer, see [28].

Acknowledgements

I am indebted to O. Beyersdorff (Berlin), P. Pudlák (Prague), A. A. Razborov (Princeton) and A. Woods (W. Australia) for comments on the draft of the paper and for discussions about these topics.

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, *Electronic Colloquium on Computational Complexity*, Rep. No.**23**, (2000). Ext. abstract in: *Proc. of the 41st Annual Symp. on Foundation of Computer Science*, (2000), pp.43-53.

[3] A. Atserias and M. L. Bonet, On the Automatizability of Resolution and Related Propositional Proof Systems, in: *11th Annual Conference of the European Association for Computer Science Logic (CSL)*, Springer, Lecture Notes in Computer Science,**2471**, (2002), pp.569-583.

[4] E. Ben-Sasson and A. Wigderson, Short proofs are narrow - resolution made simple, in: *Proc. of the 31st ACM Symp. on Theory of Computation*, (1999), pp. 517-526.

[5] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall, Proof complexity in algebraic systems and bounded depth Frege systems with modular counting, *Computational Complexity*, **6(3)**, (1996/1997), pp.256-298.

[6] Cook, S A., Feasibly constructive proofs and the propositional calculus, in: *Proc. 7th 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] O. Goldreich, Candidate one-way functions based on expander graphs, *Electronic Colloquium on Computational Complexity*, Rep. No.**90**, (2000).

[9] O. Goldreich, S. Goldwasser, and S. Micali, How to construct random functions, *J. of the ACM*, **33(4)**, (1986), pp.792-807.

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

[11] E. Jeřábek, Dual weak pigeonhole principle, Boolean complexity, and derandomization, *Annals of Pure and Applied Logic*, to app.

[12] J. Krajíček, No counter-example interpretation and interactive computation, 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.287-293. Springer-Verlag.

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

[14] J. Krajíček, On the weak pigeonhole principle, *Fundamenta Mathematicae*, Vol.**170(1-3)**, (2001), pp.123-140.

[15] J. Krajíček, Tautologies from pseudo-random generators, *Bulletin of Symbolic Logic*, **7(2)**, (2001), pp.197-212.

[16] J. Krajíček, Hardness assumptions in the foundations of theoretical computer science, (preprint in ITI series: `http://iti.mff.cuni.cz/series/index.html`, Jan.'03).

[17] J. Krajíček, 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, 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.

[20] 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.

[21] N. Nisan, and A. Wigderson, Hardness versus randomness, *J. of Computer and System Sciences*, **49**, (1994), pp.149-167.

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

[23] 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.

[24] 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.

[25] P. Pudlák, The lengths of proofs, in: *Handbook of Proof Theory*, S.R. Buss ed., Elsevier, (1998), pp.547-637.

[26] 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.

[27] A. A. Razborov, Resolution lower bounds for perfect matching principles, in: *Proc. of the 17th IEEE Conf. on Computational Complexity*, (2002), pp.29-38.

[28] A. A. Razborov, Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution, preprint, (May'03).

[29] S. Rudich, Super-bits, demi-bits, and $\tilde{NP}/qpoly$-natural proofs, in: *Proc. of the 1st Int.Symp. on Randomization and Approximation Techniques in Computer Science*, LN in Comp.Sci., Springer-Verlag, Vol.**1269**, (1997), pp.85-93.

Mailing address:

Mathematical Institute
Academy of Sciences
Žitná 25, Prague 1, CZ - 115 67
The Czech Republic
krajicek@math.cas.cz