Electronic Colloquium on Computational Complexity, Report No. 23 (2000)

ECCC

Pseudorandom Generators in Propositional Proof Complexity

Michael Alekhnovich*, Eli Ben-Sasson†
Alexander A. Razborov‡, Avi Wigderson§

May 11, 2000

Abstract

We call a pseudorandom generator $G_n : \{0,1\}^n \to \{0,1\}^m$ *hard* for a propositional proof system P if P can not efficiently prove the (properly encoded) statement $G_n(x_1, \ldots, x_n) \neq b$ for *any* string $b \in \{0,1\}^m$. We consider a variety of "combinatorial" pseudorandom generators inspired by the Nisan-Wigderson generator on the one hand, and by the construction of Tseitin tautologies on the other. We prove that under certain circumstances these generators are hard for such proof systems as Resolution, Polynomial Calculus and Polynomial Calculus with Resolution (PCR).

*Moscow State University, Moscow, Russia mike@mccme.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation

†Institute of Computer Science, Hebrew University, Jerusalem, Israel. elli@cs.huji.ac.il.

‡Steklov Mathematical Institute, Moscow, Russia razborov@genesis.mi.ras.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation; part of this work was done while visiting Princeton University and DIMACS

§Institute for Advanced Study, Princeton, and Institute of Computer Science, Hebrew University, Jerusalem, avi@math.ias.edu. This research was supported by grant number 69/96 of the Israel Science Foundation, founded by the Israel Academy for Sciences and Humanities. Support for this research has been provided by The Alfred P. Sloan Foundation

ISSN 1433-8092

1 Introduction

The notion of a pseudorandom generator originally introduced by Yao [Yao82] has become by now one of the most important concepts in theoretical computer science penetrating virtually all its subareas. In its simplest form it says the following: a mapping $G_n : \{0,1\}^n \to \{0,1\}^m$ is (computationally) secure w.r.t. some circuit class $\mathcal{C}$ if no "small" circuit $C(y_1, \ldots, y_m) \in \mathcal{C}$ can distinguish between the two probabilistic distributions $G_n(\boldsymbol{x})$ and $\boldsymbol{y}$ in the sense that $|\mathbf{P}[C(G_n(\boldsymbol{x})) = 1] - \mathbf{P}[C(\boldsymbol{y}) = 1]|$ is small ($\boldsymbol{x}$ is picked at random from $\{0,1\}^n$, and $\boldsymbol{y}$ is picked at random from $\{0,1\}^m$).

Propositional proof complexity is an area of study that has seen a rapid development over the last decade. It plays as important a role in the theory of feasible proofs as the role played by the complexity of Boolean circuits in the theory of efficient computations. Although the original motivations for this study were in many cases different (and originated from proof-theoretical questions about first-order theories), it turns out after all that the complexity of propositional proofs revolves around the following basic question. What can be *proved* (in the ordinary mathematical sense!) by a prover whose *computational* abilities are limited to small circuits from some circuit class $\mathcal{C}$ (see e.g. [BP98])? Thus, propositional proof complexity is in a sense complementary to the (non-uniform) computational complexity; moreover, there exist extremely rich and productive relations between the two areas ([Raz96, BP98]).

Given the importance of pseudorandom generators for computational complexity, it is natural to wonder which mappings $G_n : \{0,1\}^n \to \{0,1\}^m$ should be considered hard from the perspective of proof complexity? In this paper we propose the following paradigm: a generator $G_n : \{0,1\}^n \to \{0,1\}^m$ is hard for some propositional proof system P if and only if for *any* string $b \in \{0,1\}^m$ there is no efficient P-proof of the (properly encoded) statement $G(x_1, \ldots, x_n) \neq b$ ($x_1, \ldots, x_n$ are treated as propositional variables). A similar suggestion is independently made in the recent preprint of Kraijcek [Kra99].

This definition is very natural: it simply says (to the extent allowed by our framework) that P can not efficiently prove even the most basic thing about the behavior of G_n, namely that it is not an onto mapping. In fact, one a priori reasonable concern might be exactly if this exceedingly natural requirement is not at the same time too strong, and whether non-trivial

generators (say, with $m \geq n+1$) can exist at all: such a thing certainly can not exist in the computational framework. This concern is best addressed by exhibiting how several known lower bound results fit into our framework; these examples also explain some of our motivations for introducing this concept.

Example 1 (Tseitin tautologies) Let $G = (V, E)$ be a connected non-oriented graph. Consider the ($\mathbb{F}_2$-linear) mapping $T_G : \{0,1\}^E \to \{0,1\}^V$ given by $T_G(\vec{x})_v \stackrel{\text{def}}{=} \oplus_{e \ni v} x_e$, where $\vec{x} \in \{0,1\}^E$ is a $\{0,1\}$-valued function on edges. Then $b \in \{0,1\}^V$ is not in $\mathrm{im}(G)$ if and only if $\oplus_{v \in V} b_v = 1$, and if we properly encode this statement in propositional logic, we arrive exactly at the tautologies introduced by Tseitin in his seminal paper [Tse68]. These tautologies turned out to be extremely useful in propositional proof complexity, and the many strong lower bounds proved for them [Tse68, Urq87, BW99, Gri98, BGIP99, Gri99, ABSRW99] never depend on the particular choice of $b \in \{0,1\}^V$. This means that all of them can be viewed as showing that the generators T_G are hard for the corresponding proof system, as long as the graph G itself has good expansion properties.

Tseitin generators $T_G : \{0,1\}^E \to \{0,1\}^V$ make little sense from the computational point of view since the size of the seed $|E|$ is larger than the size of the output $|V|$. Our next two examples are more satisfactory in this respect.

Example 2 (Natural Proofs) Let $G_n : \{0,1\}^{n^k} \to \{0,1\}^{2^n}$ be any pseudorandom *function generator* that stretches n^k random bits to a Boolean function in n variables viewed as a string of length 2^n in its truth-table representation. Assume that G_n is hard w.r.t. $2^{O(n)}$-sized circuits. Then Razborov and Rudich [RR97] proved that for *any* function f_n there is no "natural" (in the strict sense also defined in that paper) proof of the fact $f_n \notin \mathrm{im}(G_n)$. Although in this result we are primarily interested in the case when f_n is the restriction of SAT (or any other **NP**-complete predicate) onto strings of length n, the argument, like in Example 1 absolutely does not depend on the particular choice of f_n.

One might argue that Natural Proofs is not a propositional proof system at all, and that their definition rather explicitly includes the transition "the proof works for a single $f_n \Rightarrow$ it works for many f_n", which provides the link

to the ordinary (randomized) definition of a pseudorandom generator. Our last example illustrates that this drawback sometimes can be circumvented.

Example 3 (Hardness in presence of Feasible Interpolation) Let $G_n : \{0,1\}^n \to \{0,1\}^m$ be an arbitrary pseudorandom generator that is hard w.r.t. poly-size (in $m+n$) circuits, and let $n < m/2$. Following Razborov [Raz95b], let us take bitwise XOR of two independent copies of this generator $G'_n : \{0,1\}^{2n} \to \{0,1\}^m$; $G'_n(x_1,\ldots,x_n,x'_1,\ldots,x'_n) \stackrel{\text{def}}{=} G_n(x_1,\ldots,x_n) \oplus G_n(x'_1,\ldots,x'_n)$. Then G'_n is hard for any propositional proof system P which has the property of feasible interpolation (for a definition see e.g. [BP98]).

The study of such a keystone concept in computational complexity as pseudorandom generators, but in the new framework of proof complexity, should be interesting in its own right. As suggested by the examples above, we also keep one quite pragmatic goal in mind: we believe that pseudorandom generators is methodologically the right way to think of lower bounds in the proof-theoretic setting for really strong proof systems. Whenever we have a generator $G_n : \{0,1\}^n \to \{0,1\}^{n+1}$ which is hard for a propositional proof system P, we have lower bounds for P. If we manage to increase significantly the number of output bits and construct a poly-time computable function generator $G_n : \{0,1\}^{n^k} \to \{0,1\}^{2^n}$ that is hard for P, we, similarly to [RR97, Raz95b], can conclude that in the framework proposed in [Raz95a] there are no efficient P-proofs of $\mathbf{NP} \not\subseteq \mathbf{P}/poly$.

In this paper we begin looking at a class of generators inspired by Nisan-Wigderson generator [NW94] on the one hand, and by Example 1 on the other. Let A be an $(m \times n)$ 0-1 matrix, $g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)$ be Boolean functions such that g_i essentially depends only on the variables $X_i(A) \stackrel{\text{def}}{=} \{x_j \mid a_{ij} = 1\}$, and $G_n : \{0,1\}^n \to \{0,1\}^m$ be given by $G_n(x_1,\ldots,x_n) \stackrel{\text{def}}{=} (g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n))$. Nisan and Wigderson [NW94] proved that if A satisfies certain combinatorial conditions (namely, if it is a (k,s)-design for suitable choice of parameters), and the functions g_i are computationally hard, then G_n is a good pseudorandom generator in the computational sense. In this paper we study which combinatorial properties of the matrix A and which hardness assumptions imposed on g_i guarantee that the resulting generator G_n is hard for such proof systems as Resolution or Polynomial Calculus.

The framework of proof complexity, however, adds also the third specific dimension that determines hardness properties of G_n. Namely, in our examples the base functions g_i are at least supposed to be hard for the circuit class underlying the propositional proof system P. Thus, P can not even express the base functions, and we should encode them using certain extension variables. Using these extension variables, our tautologies can be written as 3-CNFs, and thus can be expressed in any proof system. The choice of encoding makes an important part of the framework. We propose three different encodings - functional, circuit, and linear encodings, all natural from both computational and proof complexity viewpoints.

Our results are strong lower bounds for each of these encodings (and appropriate choices of base functions and combinatorial properties of the matrix A) in such standard proof systems like Resolution, Polynomial Calculus, and PCR (which combines the power of both). Naturally, the results get weaker as the encoding strength increases.

We strongly believe that this set of tautologies can serve as hard examples for much stronger systems, and specifically that the hardness of the base functions in the generators should be a key ingredient in the proof. This factor is evident in our modest results above, and if extended to stronger systems, it may be viewed as a generalization of the feasible interpolation results, reducing proof complexity to computational complexity.

The paper is organized as follows. In Section 2 we give necessary definitions and describe precisely combinatorial properties of the matrix A, hardness conditions imposed on the base functions g_i and types of their encodings needed for our purposes.

The next section 3 contains our hardness results for resolution width and polynomial calculus degree that hold for the most general functional encoding similar in spirit to the Functional Calculus from [ABSRW99]. These can be considered as far-reaching generalizations of lower bounds for Tseitin tautologies from [BW99, BGIP99]. We also state here size lower bounds directly implied by our results via the known width/size and degree/size relations.

Section 4 contains a stronger lower bound for the weaker linear encoding. In Section 5 we consider the question of maximizing the number of output bits $m = m(n)$ in the generators constructed in the previous sections. For that purpose we show that with high probability a random matrix A has very good expansion properties. The paper is concluded in Section 6 with

several open questions.

2 Preliminaries

Let x be a Boolean variable, i.e. a variable that ranges over the set $\{0,1\}$. A *literal* of x is either x (denoted sometimes as x^1) or $\bar{x}$ (denoted sometimes as x^0). A *clause* is a disjunction of literals.

For any Boolean function $f : \{0,1\}^n \to \{0,1\}$, $Vars(f)$ will denote the set of its essential variables. An *assignment to* f is a mapping $\alpha : Vars(f) \to \{0,1\}$. A *restriction of* f is a mapping $\rho : Vars(f) \to \{0,1,\star\}$. We denote by $|\rho|$ the number of assigned variables, $|\rho| \stackrel{\text{def}}{=} |\rho^{-1}(\{0,1\})|$.

The *restriction of* f *by* ρ, denoted $f|_\rho$, is the Boolean function obtained from f by setting the value of each $x \in \rho^{-1}(\{0,1\})$ to $\rho(x)$, and leaving each $x \in \rho^{-1}(\star)$ as a variable.

We say that an assignment α *satisfies* f if $f(\alpha) = 1$. For Boolean functions $f_1, \ldots, f_k, g$ we say that $f_1, \ldots, f_k$ *semantically imply* g, (denoted $f_1, \ldots, f_k \models g$), if every assignment to $V \stackrel{\text{def}}{=} Vars(f_1) \cup \ldots \cup Vars(f_k) \cup Vars(g)$ satisfying $f_1, \ldots, f_k$, satisfies g as well (i.e. $\forall \alpha \in \{0,1\}^V (f_1(\alpha) = \cdots = f_k(\alpha) = 1 \Rightarrow g(\alpha) = 1)$).

For n, a non-negative integer let $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$.

Let A be an $(m \times n)$ 0-1 matrix,

$$J_i(A) \stackrel{\text{def}}{=} \{\, j \in [n] \mid a_{ij} = 1 \,\}, \tag{1}$$

$X_i(A) \stackrel{\text{def}}{=} \{\, x_j \mid j \in J_i(A) \,\}$ and $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)$ be Boolean functions such that $Vars(g_i) \subseteq X_i(A)$. We will be interested in systems of Boolean equations

$$\begin{cases} g_1(x_1, \ldots, x_n) = 1 \\ \cdots \\ g_m(x_1, \ldots, x_n) = 1. \end{cases} \tag{2}$$

We want to state combinatorial properties of the matrix A and hardness conditions of the base functions g_i such that if we properly encode the system (2) as a CNF $\tau(A, \vec{g})$, then every refutation of this CNF in a propositional proof system P must be complex. This sentence has four ingredients, and the necessary definitions for each of them are provided fairly independently.

2.1 Combinatorial properties of the matrix A

All hardness results proved in this paper will be based on the following combinatorial property generalizing the "edge-expansion" property for ordinary graphs. It is similar to the expansion defined in [BW99].

Definition 2.1 For a set of rows $I \subseteq [m]$ in the matrix A, we define its *boundary* $\partial_A(I)$ as the set of all $j \in [n]$ (called *boundary elements*) such that $\{a_{ij} \mid i \in I\}$ contains exactly one 1. We say that A is an (r, s, c)-*expander* if $|J_i(A)| \leq s$ for all $i \in [m]$ and $\forall I \subseteq [m](|I| \leq r \Rightarrow |\partial_A(I)| \geq c \cdot |I|)$.

Let us relate (r, s, c)-expanders to several other combinatorial properties already known from the literature.

Example 4 For an ordinary graph $G = (V, E)$, its *edge-expansion coefficient* $c_E(G)$ is defined by

$$c_E(G) \stackrel{\text{def}}{=} \min_{|U| \leq |V|/2} \frac{e(U, V-U)}{|U|},$$

where $e(U, W)$ is the number of edges between U and W (see e.g., [Alo98] and the literature cited therein). Let A_G be the incidence matrix of a graph G with m vertices and n edges (i.e., $a_{ve} \stackrel{\text{def}}{=} 1$ if and only if $v \in e$), and let d be the maximal degree of a vertex in G. Then A_G is an $(m/2, d, c)$-expander if and only if $c_E(G) \geq c$.

Example 5 Let us turn to the combinatorially property originally used in [N91, NW94]. A matrix A is called (k, s)-*design* if $|J_i(A)| = s$ for all $i \in [m]$ and

$$|J_{i_1} \cap J_{i_2}| \leq k \tag{3}$$

for all $1 \leq i_1 < i_2 \leq m$. We have the following:

Fact 1 *Every (k, s)-design is also an $(r, s, s-kr)$-expander for any parameter r.*

Proof. Let $I \subseteq [m]$ and $|I| \leq r$. Then, due to the property (3), every $J_i(A)$ with $i \in I$ has at most $k \cdot (r-1)$ elements which are *not* in $\partial_A(I)$. Hence it contains at least $s - k \cdot (r-1)$ elements which *are* in $\partial_A(I)$.■

2.2 Hardness conditions on the base functions

As explained in the Introduction, we are interested in the methods which, given a mapping $G_n : \{0,1\}^n \to \{0,1\}^m$, allow us to show that the fact $b \notin \mathrm{im}(G_n)$ is hard to prove *for any* $b \in \{0,1\}^m$. This means that we want our lower bounds on the refutation complexity to work uniformly not only for the system (2) but also for *all* 2^m shifted systems

$$\begin{cases} g_1(x_1,\ldots,x_n) = b_1 \\ \cdots \\ g_m(x_1,\ldots,x_n) = b_m, \end{cases}$$

$b \in \{0,1\}^m$. We will enforce this simply by requiring that the conditions placed on the base functions $g_1,\ldots,g_m$ are symmetric, i.e., they are satisfied by some f if and only if they are satisfied by $(\neg f)$.

Definition 2.2 A Boolean function f is *ℓ-robust* if every restriction ρ such that $f|_\rho = const$, satisfies $|\rho| \geq \ell$.

Clearly, this property is symmetric. The most important example of robust functions are the PARITY functions $x_1 \oplus \cdots \oplus x_n \oplus b$, $b \in \{0,1\}$, which are n-robust. Our strongest hardness results for the polynomial calculus work only for this specific function.

In fact, ℓ-robust functions are already well familiar from the computational complexity literature. [FSS84, Ajt83, Yao85, Hås86] proved *computational* lower bounds for ℓ-robust functions (when ℓ is close to $n = |Vars(f)|$) w.r.t. bounded-depth circuits. $(1-\theta)n$-robust functions (where θ is meant to be a small positive constant) were recently used in [BST98] for obtaining strong lower bounds for branching programs (property "$\mathcal{P}(\theta)$"). In this paper we will use ℓ-robust functions for constructing generators that are hard for propositional *proof* systems. It is easy to see that most functions on n-bits are (say) $0.9n$-robust.

2.3 Encodings

Having constructed the system (2), we still should decide how to represent it in propositional logic. This step is non-trivial since we are deliberately interested in the case when the propositional system P can not directly speak of the functions $g_1,\ldots,g_m$. We consider three major possibilities: *functional*, *circuit* and *linear* encodings: all of them lead to CNFs that in fact w.l.o.g. can be further restricted to 3-CNFs (see the proof of Corollary 3.5 below).

2.3.1 Functional encoding

This is the strongest possible encoding which is also universal in the sense that it obviously simulates any other conceivable encoding (in fact, it is a "localized" variant of the Functional Calculus system considered in [ABSRW99]).

Definition 2.3 Let A be an $(m \times n)$ 0-1 matrix. For every Boolean function f with the property $\exists i \in [m](Vars(f) \subseteq X_i(A))$ we introduce a new *extension variable* y_f. Let $Vars(A)$ be the set of all these variables.

Given Boolean functions $\vec{g} = (g_1, \ldots, g_m)$ such that $Vars(g_i) \subseteq X_i(A)$, we denote by $\tau(A, \vec{g})$ the CNF in the variables $Vars(A)$ that consists of those clauses $y_{f_1}^{\epsilon_1} \vee \ldots \vee y_{f_w}^{\epsilon_w}$ for which there exists $i \in [m]$ such that

$$Vars(f_1) \cup \ldots \cup Vars(f_w) \subseteq X_i(A) \tag{4}$$

and

$$g_i \models f_1^{\epsilon_1} \vee \ldots \vee f_w^{\epsilon_w}. \tag{5}$$

Fact 2 *$\tau(A, \vec{g})$ is satisfiable if and only if the system (2) is consistent.*

Proof. If $(a_1, \ldots, a_n)$ is a solution to (2), then the assignment which assigns every y_f to $f(a_1, \ldots, a_n)$ is satisfying for $\tau(A, \vec{g})$. In another direction, let $\vec{b} = (b_f | y_f \in Vars(A))$ be a satisfying assignment for $\tau(A, \vec{g})$. Let $a_j \stackrel{\text{def}}{=} b_{x_j}$; then, using those axioms $y_{f_1}^{\epsilon_1} \vee \ldots \vee y_{f_w}^{\epsilon_w}$ from $\tau(A, \vec{g})$ for which $f_1^{\epsilon_1} \vee \ldots \vee f_w^{\epsilon_w} \equiv 1$, we can show by induction on the circuit size of f that $b_f = f(a_1, \ldots, a_n)$ for every $y_f \in Vars(A)$. In particular, $g_i(a_1, \ldots, a_n) = b_{g_i} = 1$ (since $\tau(A, \vec{G})$ contains the axiom y_{g_i}). Thus, the vector $(a_1, \ldots, a_n)$ is a solution to the system (2).■

2.3.2 Circuit encoding

This encoding is much more economical in terms of the number of variables than the functional encoding. Also, it looks more natural and better conforming to the underlying idea of the Extended Frege proof system. The tautologies under this encoding will be polynomial-size as long as all g_i's have poly-size circuits, and thus are potentially hard for Frege (assuming $\mathbf{P}/poly$ contains functions computationally hard for $\mathbf{NC^1}/poly$).

Definition 2.4 Let A be an $(m \times n)$ 0-1 matrix, and $C_1, \ldots, C_m$ be single-output Boolean circuits over an arbitrary fixed finite basis, C_i being a circuit in the variables $X_i(A)$. For every $i \in [m]$ and every gate v of the circuit C_i we introduce a special *extension variable* y_v, and we identify extension variables corresponding to input gates labeled by the same variable x_j. Let $Vars_{\vec{C}}(A)$ be the set of all these extension variables.

By $\tau(A, \vec{C})$ we denote the CNF that consists of the following clauses:

1. $y_{v_1}^{\bar{\epsilon}_1} \vee \ldots \vee y_{v_d}^{\bar{\epsilon}_d} \vee y_v^{\pi(\epsilon_1,\ldots,\epsilon_d)}$, whenever $v := \pi(v_1, \ldots, v_d)$ is an instruction of one of the circuits $C_1, \ldots, C_m$ and $\epsilon \in \{0,1\}^d$ is an arbitrary vector;

2. y_{v_i} when v_i is the output gate of C_i, for all $i \in [m]$.

For a circuit C, let $||C||$ be the Boolean function it computes.

Fact 3 *$\tau(A, \vec{C})$ is satisfiable if and only if the system $||C_1|| = \ldots = ||C_m|| = 1$ is consistent.*

Proof. Similarly to the proof of Fact 2.■

Fact 4 *There exists a substitution σ of variables from $Vars_{\vec{C}}(A)$ by variables from $Vars(A)$ such that $\sigma(\tau(A, \vec{C}))$ is a subset of the set of clauses $\tau(A, ||\vec{C}||)$. In particular, every refutation of $\tau(A, \vec{C})$ in every "reasonable" propositional proof system can be transformed (by applying σ) into a refutation of $\tau(A, ||\vec{C}||)$ in the same system which is simpler w.r.t. any "reasonable" complexity measure.*

Proof. Let $\sigma(y_v) \stackrel{\text{def}}{=} y_{||v||}$, where $||v||$ is the function computed by the gate v.■

2.3.3 Linear encoding

This encoding makes sense only when g_is are $\mathbb{F}_2$-linear forms. It is only somewhat more economical than the functional encoding in terms of the number of variables. However, it is much better structured, and we will take advantage of this in Section 4.

Definition 2.5 Let A be an $(m \times n)$ 0-1 matrix. For every $J \subseteq [n]$ such that $\exists i \in [m](J \subseteq J_i(A))$ we introduce a new *extension variable* y_J (with the intended meaning $y_J \sim \oplus_{j \in J} x_j$). Let $Vars_{\oplus}(A)$ be the set of all these variables.

Given a Boolean vector $b \in \{0,1\}^m$, we denote by $\tau_{\oplus}(A,b)$ the CNF in the variables $Vars_{\oplus}(A)$ that consists of the following clauses:

1. $y_{J_1}^{\epsilon_1} \vee \ldots \vee y_{J_d}^{\epsilon_d}$, whenever there exists $i \in [m]$ such that $J_1 \cup \ldots \cup J_d \subseteq J_i(A)$, the symmetric difference $J_1 \triangle \ldots \triangle J_d$ is empty and $\bar{\epsilon}_1 \oplus \ldots \oplus \bar{\epsilon}_d = 1$;

2. $y_{J_i(A)}^{b_i}$, for all $i \in [m]$.

Let us denote by $\Sigma_i(A,b_i)$ the Boolean function $\bigoplus_{j \in J_i(A)} x_j \oplus \bar{b}_i$.

Fact 5 *$\tau_{\oplus}(A,b)$ is satisfiable if and only if the system $\Sigma_1(A,b_1) = \Sigma_2(A,b_2) = \ldots = \Sigma_m(A,b_m) = 1$ of linear equations over $\mathbb{F}_2$ is consistent.*

Fact 6 *There exists a substitution σ of variables from $Vars_{\oplus}(A)$ by variables from $Vars(A)$ such that $\sigma(\tau_{\oplus}(A,b))$ is a subset of the set of clauses $\tau(A,\vec{\Sigma}(A,b)) \stackrel{\text{def}}{=} \tau(A,\Sigma_1(A,b_1),\Sigma_2(A,b_2),\ldots,\Sigma_m(A,b_m))$.*

Proof. $\sigma(y_J) \stackrel{\text{def}}{=} y_{\bigoplus_{j \in J} x_j}$.■

It might be instructive to look at the place occupied in our framework by original Tseitin tautologies (cf. Examples 1,4). Let A_G be the incidence matrix of an undirected graph G. Then our framework provides three different ways[1] to talk of Tseitin tautologies for graphs G of *arbitrary* degree. All these possibilities are *reasonable* in the sense that although the resulting CNF τ may have a huge size, it always possesses a sub-CNF of *polynomial* size that is still unsatisfiable. The fourth (unreasonable!) encoding is *primitive*: we allow no extension variables at all and simply represent the functions $\Sigma_i(A,b_i)$ themselves as CNFs of exponential size. For graphs of bounded degree (which is the only case researchers were interested in prior to this paper), the subtle differences between the four encodings disappear, and the whole rich spectrum of various possibilities collapses to ordinary Tseitin tautologies.

[1]For the circuit encoding we additionally have to fix some natural circuits computing the functions $\Sigma_i(A,b_i)$.

In fact, the unreasonable primitive encoding can in principle be considered in the framework of our paper as well. Namely, as we will see in Section 5, good (r, s, c)-expanders exist even for large constants s (say, $s = 10$). And for constant values of s results proved in any of our reasonable encodings can be translated to the primitive encoding with only constant time increase in the size of the tautology. The primitive encoding, however, is very counterintuitive to the main idea that the base functions g_i's should be hard for the circuit class underlying our propositional theory, and to the hope of using these tautologies for stronger proof systems. For this reason we do not discuss in this paper neither the primitive encoding itself, nor the trade-off between the tautology size and the bounds appearing in this encoding when $s \to \infty$.

2.4 Propositional proof systems

2.4.1 Resolution

Resolution is the simplest and probably the most widely studied model. It operates with clauses and has one rule of inference called *resolution rule*:

$$\frac{A \vee x \qquad B \vee \bar{x}}{A \vee B}.$$

A *resolution refutation* of a CNF formula τ is a resolution proof of the empty clause from the clauses appearing in τ.

The *size* of a resolution proof is the number of different clauses in it. The *width* $w(C)$ *of a clause* C is the number of literals in C. The *width* $w(\tau)$ *of a set of clauses* τ (in particular, the width of a resolution proof) is the maximal width of a clause appearing in this set.

The story of propositional proof complexity began over 30 years ago when in the seminal paper [Tse68] Tseitin proved super-polynomial lower bounds on the size of any resolution refutation of (what was afterwards called) Tseitin tautologies under one extra regularity assumption on the structure of refutation. Haken [Hak85] was the first to remove this restriction and prove exponential lower bounds for general resolution (for the pigeonhole principle). Urquhart [Urq87] proved exponential lower bounds on the size of general resolution refutations for Tseitin tautologies.

Ben-Sasson and Wigderson [BW99], strengthening a result from [CEI96] (cf. Section 2.4.2 below) proved the following width-size relation:

Proposition 2.6 *Let τ be an unsatisfiable CNF in n variables that has a resolution refutation of size S. Then τ has a resolution refutation of width at most $w(\tau) + O(\sqrt{n \log S})$.*

[BW99] also established a linear lower bound on the width of resolution refutation for Tseitin tautologies. In combination with Proposition 2.6 this gave an alternate (and much simpler) proof of the size lower bound from [Urq87].

2.4.2 Polynomial Calculus and Polynomial Calculus with Resolution

Polynomial Calculus, introduced by Clegg, Edmonds and Impagliazzo in [CEI96] is a proof system that models common algebraic reasoning. Despite its algebraic nature, Polynomial Calculus (PC) turned out extremely useful for studying "pure" propositional proof systems.

PC operates with polynomials $P \in F[x_1, \ldots, x_n]$ for some fixed field F; a polynomial P is interpreted as, and often identified with, the polynomial equation $P = 0$. Polynomial Calculus has polynomials $x_i^2 - x_i$ ($i \in [n]$) as *default axioms* and has two inference rules:

$$\frac{P_1 \qquad P_2}{\alpha P_1 + \beta P_2};\ \alpha, \beta \in F \quad \text{(Scalar Addition)}$$

and

$$\frac{P}{x \cdot P} \quad \text{(Variable Multiplication)}.$$

A *polynomial calculus refutation* of a set of polynomials Γ is a polynomial calculus proof of 1 from Γ. The *degree of a PC proof* is the maximal degree of a polynomial appearing in it. The *size of a PC proof* is the total number of monomials in the proof.

First non-trivial lower bounds on the degree of PC refutations were proved by Razborov [Raz98] (for the pigeonhole principle). Grigoriev [Gri98] proved linear lower bounds on the degree of Nullstellensatz refutations (which is a subsystem of Polynomial Calculus) for Tseitin tautologies. Finally, Buss, Grigoriev, Impagliazzo and Pitassi [BGIP99] extended the latter bound to arbitrary polynomial calculus proofs. Following [BGIP99] and the research whose outcome is presented in this paper, Ben-Sasson and Impagliazzo [BI99]

further simplified this argument, and derived linear degree lower bounds for random CNFs.

[CEI96] proved that small size resolution proofs can be simulated by low degree PC proofs (Proposition 2.6 is a later improvement of this result). [IPS99] observed that the same simulation works also for small size *polynomial calculus* proofs.

Motivated in part by this similarity, [ABSRW99] proposed to consider the following natural system PCR extending both Polynomial Calculus and Resolution. PCR operates with polynomials $P \in F[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, where $\bar{x}_1, \ldots, \bar{x}_n$ are treated as new formal variables. PCR has all default axioms and inference rules of PC (including, of course, those that involve new variables $\bar{x}_i$), plus additional default axioms $x_i + \bar{x}_i = 1$ ($i \in [n]$). The *size* and *degree of a PCR proof* are defined in the same way as for Polynomial Calculus. It should be noted that there is not much sense in giving a separate definition for the degree of PCR proofs since the linear transformation $\bar{x}_i \mapsto 1 - x_i$ takes a PCR-proof to (essentially) PC-proof while preserving degree. This system, however, becomes extremely convenient when it is the number of clauses which matters (see [ABSRW99]).

PCR is an extension of PC by definition. Also, PCR extends Resolution via the following translation. For a clause C, let C_+ [(C_-)] be the set of positive [respectively, negative] literals appearing in it. Then a CNF formula τ gets translated into the set of polynomials Γ_τ defined by $\Gamma_\tau \stackrel{\text{def}}{=} \left\{ \left(\prod_{\bar{x} \in C_-} x \cdot \prod_{x \in C_+} \bar{x} \right) \middle| \; C \in \tau \right\}$. Clearly, τ is satisfiable if and only if Γ_τ has a common root in F satisfying all default axioms

$$x_i^2 = x_i; \;\; \bar{x}_i^2 = \bar{x}_i; \;\; x_i + \bar{x}_i = 1. \tag{6}$$

Moreover, it is easy to see that every width w size S resolution refutation of τ can be transformed into a degree $(w+1)$ size $O(nS)$ PCR refutations of the associated set of polynomials Γ_τ. For ease of notation, we will omit the translation and define a *PCR refutation of a CNF* τ as PCR refutation of Γ_τ. A *PC refutation* of τ is a PC refutation of the set of polynomials

$$\Gamma'_\tau \stackrel{\text{def}}{=} \left\{ \left(\prod_{\bar{x} \in C_-} x \cdot \prod_{x \in C_+} (1 - x) \right) \middle| \; C \in \tau \right\} \tag{7}$$

obtained from Γ_τ by the linear transformation $\bar{x}_i \mapsto 1 - x_i$.

In fact all our lower bounds for PC hold also for PCR so we will usually use the translation to PCR and prove PCR lower bounds which imply the hardness for PC.

[ABSRW99] observed that the two simulations from [CEI96, IPS99] can be merged into one as follows:

Proposition 2.7 *Let Γ be a system of polynomials in the variables $x_1, \ldots, x_n$, $\bar{x}_1, \ldots, \bar{x}_n$ that have no common roots in F satisfying all default axioms* (6)*, and let $d(\Gamma) \stackrel{\text{def}}{=} \max\{\deg(P) \mid P \in \Gamma\}$. Then every size S PCR refutation of Γ can be transformed into another PCR refutation of Γ that has degree at most $d(\Gamma) + O(\sqrt{n \log S})$.*

3 Lower bounds on width and degree in the functional encoding

In this section we establish strong lower bounds on the resolution width and PC degree in the most general functional encoding, and derive from them some size lower bounds. Our results in this section can be viewed as a far-reaching generalization of the corresponding lower bounds for Tseitin tautologies from [BW99, BGIP99].

But first a word about important and less important parameters. The parameters s, c, l of the defining tautologies will feature in most of the calculations (recall that s is the number of 1's in each row of the matrix A, which is also the number of arguments to each function g_i, c is the expansion factor of the matrix A, and ℓ will lower bound the robustness of the g_i's). We will show in Section 5 that almost all matrices satisfy $c > 0.9s$. Similarly, most functions satisfy $\ell > 0.9s$. Assuming this, Theorem 3.1 and Theorem 3.7 provide $\Omega(r)$ lower bounds on the width of Resolution and degree of Polynomial Calculus, respectively (recall that r is the key parameter defining what size sets expand, and can be taken to be essentially n/s; see Section 5 for details). Our corollaries for the size lower bounds implied by the width and degree lower bounds will be stated (for simplicity) only for this situation.

Theorem 3.1 *Let A be an (r, s, c)-expander of size $(m \times n)$, and $g_1, \ldots, g_m$ be ℓ-robust functions with $Vars(g_i) \subseteq X_i(A)$, where $c + \ell \geq s + 1$. Then every resolution refutation of $\tau(A, \vec{g})$ must have width $> \frac{r(c+\ell-s)}{2\ell}$.*

Proof. The proof follows the ideology developed in [BW99]. We define a measure μ with sub-additive growth on the clauses, we show that the measure of the empty clause is large ($\mu(0) > r$), hence there must be a clause with medium size measure ($r/2 < \mu(C) \leq r$). We show that such a clause must have large width.

Fix an (r, s, c)-expander A of size $(m \times n)$ and ℓ-robust functions $g_1, \ldots, g_m$ with $Vars(g_i) \subseteq X_i(A)$, where $c + \ell \geq s + 1$.

Definition 3.2 *For C a clause in the variables $Vars(A)$, define $\mu(C)$ to be the size of a minimal $I \subseteq [m]$ such that the following pair of conditions hold:*

$$\forall y_f^\epsilon \in C \ \exists i \in I \ (Vars(f) \subseteq X_i(A)); \tag{8}$$

$$\{ g_i \mid i \in I \} \models ||C||. \tag{9}$$

Claim 3.3 *1. For a clause C with $r/2 < \mu(C) \leq r$, $w(C) \geq \frac{r(c+\ell-s)}{2\ell}$.*

2. $\mu(0) > r$.

Proof. **Part 1)** Let I be a set of minimal size satisfying Definition 3.2. Since $|I| \leq r$, we get $|\partial_A(I)| \geq c \cdot |I|$. Let us partition I into I_0, any minimal subset satisfying (8), and $I_1 = I \setminus I_0$. Notice that by the minimality of I, removing any row from I_1 will ruin property (9).

We claim that for any $i_1 \in I_1$, $J_{i_1}(A)$ has small intersection with $\partial_A(I)$. Namely,

$$|J_{i_1}(A) \cap \partial_A(I)| \leq s - \ell. \tag{10}$$

Indeed, as we noticed above, $\{ g_i \mid i \in I \setminus \{i_1\} \} \not\models ||C||$. Let α be any assignment such that $g_i(\alpha) = 1$ ($i \in I \setminus \{i_1\}$) but $||C||(\alpha) = 0$. Let ρ be the restriction given by

$$\rho(x_j) \stackrel{\text{def}}{=} \begin{cases} \alpha(x_j) \text{ if } j \notin \partial_A(I) \cap J_{i_1}(A) \\ \star \text{ if } j \in \partial_A(I) \cap J_{i_1}(A). \end{cases}$$

Then, since ρ is totally defined on $Vars(g_i)$ for $i \neq i_1$, and also on $Vars(||C||)$ (by (8) and $i_1 \notin I_0$) we have $g_i|_\rho \equiv 1$ ($i \neq i_1$) and $C|_\rho \equiv 0$. Hence, using (9), we conclude that $g_{i_1}|_\rho \equiv 0$. Since g_{i_1} is ℓ-robust and $|J_{i_1}(A)| \leq s$, this implies the desired inequality (10).

Now we may sum up:

$$\left.\begin{array}{rcl} c\cdot|I| & \leq & |\partial_A(I)| \\ & \leq & s\cdot|I_0|+(s-\ell)|I_1| \\ & = & (s-\ell)|I|+\ell\cdot|I_0| \\ & \leq & (s-\ell)|I|+\ell\cdot w(C). \end{array}\right\} \quad (11)$$

Recalling that $|I| > r/2$, we get our bound. Part 1) is proven.

Part 2) Suppose the contrary, that is $\mu(0) \leq r$. Then we can repeat the first part of the above argument (since that part did not use the condition $|I| > r/2$) and still get (11). But now $I_0 = \emptyset$, hence (11) alone implies a contradiction with the expansion property. This proves part 2).■

Claim 3.4 *Any refutation of $\tau(A,\vec{g})$ must include a clause C with $r/2 < \mu(C) \leq r$.*

Proof. μ is sub-additive, i.e. if C was derived from C_0, C_1 by a single resolution step, then $\mu(C) \leq \mu(C_0)+\mu(C_1)$. Additionally, for any axiom C, $\mu(C) = 1$. The statement now follows from Claim 3.3(2).■

Theorem 3.1 is immediately implied by Claims 3.4, 3.3(1).■

In order to see which *size* lower bounds are implied by Theorem 3.1 via Proposition 2.6, we consider only the typical (and most important) case $c+\ell-s = \Omega(s)$, for which our width lower bound is $\Omega(r)$.

Corollary 3.5 *Let $\epsilon > 0$ be an arbitrary fixed constant, A be an $(r,s,\epsilon s)$-expander of size $(m\times n)$, and $g_1,\ldots,g_m$ be $(1-\epsilon/2)s$-robust functions. Then every resolution refutation of $\tau(A,\vec{g})$ must have size* $\exp\left(\Omega\left(\frac{r^2}{m\cdot 2^{2s}}\right)\right)/2^s$.

Proof. Fix a resolution refutation of $\tau(A,\vec{g})$ that has size S. It is easy to see that every axiom in $\tau(A,\vec{g})$ contains a sub-clause of width $\leq 2^s$ which is also an axiom of $\tau(A,\vec{g})$. Moreover, this latter clause can be easily inferred in $O(2^s)$ steps from those axioms in $\tau(A,\vec{g})$ that have width ≤ 3. This allows us to replace the original refutation by a refutation that may have a slightly bigger size $O(S\cdot 2^s)$ but uses only those axioms from $\tau(A,\vec{g})$ that have width $\leq$

3. Hence, by Proposition 2.6, $\tau(A, \vec{g})$ also has a resolution refutation of width $O\left(\sqrt{|Vars(A)| \cdot \log(S \cdot 2^s)}\right) \leq O\left(\sqrt{m \cdot 2^{2^s} \cdot \log(S \cdot 2^s)}\right)$. Comparing this with the lower bound of $\Omega(r)$ that comes from Theorem 3.1, we finish the proof of Corollary 3.5.■

We can obtain much better size lower bounds (i.e., get rid of the disappointing term 2^{2^s} in the denominator) for the circuit encoding. We further confine ourselves to the optimal case when the circuits $C_1, \ldots, C_m$ have size $O(s)$.

Corollary 3.6 *Let $\epsilon > 0$ be an arbitrary fixed constant, A be an $(r, s, \epsilon s)$-expander of size $(m \times n)$, and $C_1, \ldots, C_m$ be single-output Boolean circuits over arbitrary fixed finite basis such that C_i is a circuit of size $O(s)$ in the variables $X_i(A)$, and all functions $||C_i||$ are $(1 - \epsilon/2)s$-robust. Then every resolution refutation of $\tau(A, \vec{C})$ must have size* $\exp\left(\Omega\left(\frac{r^2}{ms}\right)\right)$.

Proof. By Fact 4 and Theorem 3.1, every resolution refutation of $\tau(A, \vec{C})$ must have width $\Omega(r)$. Since $|Vars_{\vec{C}}(A)| \leq O(ms)$, the required bound immediately follows from Proposition 2.6.■

Our second major result in this section generalizes the bound from [BGIP99]. Unfortunately, it also inherits all the limitations of their technique: essentially the only base functions $g_1, \ldots, g_m$ we can handle are $\mathbb{F}_2$-linear forms, and for $char(F) = 2$ our approach fails completely (cf. [Gri98]). On the positive side, note that although we do require the linearity of the base functions, the bound itself still holds for the most general *functional* framework.

Theorem 3.7 *Let A be an (r, s, c)-expander of size $(m \times n)$, and $b_1, \ldots, b_m \in \{0, 1\}$. Then every PCR refutation of $\tau(A, \vec{\Sigma}(A, b))$ over an arbitrary field F with $char(F) \neq 2$ must have degree $\geq \frac{rc}{4s}$.*

Proof. As the first step toward proving Theorem 3.7, we show one simple reduction to a lower bound problem about PC refutations in the *original* variables $x_1, \ldots, x_n$. This step is very general and does not depend on the linearity of the base functions g_i.

Definition 3.8 For a Boolean function $f(x_1,\ldots,x_n)$, $P_f(x_1,\ldots,x_n)$ is the (unique) multi-linear polynomial such that

$$P_f(\alpha) = \begin{cases} 0 \text{ if } f(\alpha)=1 \\ 1 \text{ if } f(\alpha)=0 \end{cases}$$

for all $\alpha \in \{0,1\}^n$.

Lemma 3.9 *For any $(m \times n)$ 0-1 matrix A and any functions $g_1,\ldots,g_m$ with $Vars(g_i) \subseteq X_i(A)$, every degree d PCR refutation of $\tau(A,\vec{g})$ can be transformed into a PC refutation of the system*

$$P_{g_1} = \ldots = P_{g_m} = 0 \tag{12}$$

(in the original *variables $x_1,\ldots,x_n$) that has degree $\leq s \cdot d$.*

Proof of Lemma 3.9. Let us consider some PCR refutation π of $\tau(A,\vec{g})$. Substitute in π the polynomial $P_{f^\epsilon}(x_1,\ldots,x_n)$ for every variable y_f^ϵ. Since $\deg(P_{f^\epsilon}) \leq s$ for any $f(x_1,\ldots,x_n)$ such that $Vars(f) \subseteq X_i(A)$ for some $i \in [m]$, the degrees of all lines resulting from this substitution are at most $s \cdot d$. Moreover, any axiom from $\tau(A,\vec{g})$, as well as default axioms, gets transformed into a polynomial P such that for some $i \in [m]$ P contains only variables from $X_i(A)$, and is a semantical corollary of P_{g_i} on $\{0,1\}^{X_i(A)}$. Hence, it can be inferred from P_{g_i} in degree $\leq s$, using only variables from $X_i(A)$. Appending these auxiliary inferences to the beginning of the transformed refutation π, we obtain the required PC refutation of the system (12). Lemma 3.9 is proved.■

Thus, in order to complete the proof of Theorem 3.7, we should establish the $\frac{rc}{4}$ lower bound on the degree of any PC refutation π of the system (12) for $g_i = \Sigma_i(A,b_i)$.

The original proof, found in September of 1998, directly adapted the argument from [BGIP99] to our setting. After that, [BI99] came up with an elegant connection between PC-degree and Gaussian width (another concept considered by us in August of 1998). With this connection in hand, we may quote here, word by word, Theorem 3.3 from [BI99], plugging in our current parameters.

Theorem 3.10 *For A an (r,s,c) expander, $\{g_i\}$ linear equations mod 2, and F a field of characteristic $\neq 2$, any PCR refutation of $P_{g_1} = \ldots = P_{g_m} = 0$ has degree $\geq \frac{rc}{4}$.*

Theorem 3.7 follows.■

Corollary 3.11 *Let $\epsilon > 0$ be an arbitrary fixed constant, A be an $(r, s, \epsilon s)$-expander of size $(m \times n)$ and $b_1, \ldots, b_m \in \{0,1\}$. Then every PCR refutation of $\tau(A, \vec{\Sigma}(A,b))$ over an arbitrary field F with $char(F) \neq 2$ must have size* $\exp\left(\Omega\left(\frac{r^2}{m \cdot 2^{2^s}}\right)\right)/2^s$.

Proof. Identical to the proof of Corollary 3.5, using Proposition 2.7.■

Corollary 3.12 *Let $\epsilon > 0$ be an arbitrary fixed constant, A be an $(r, s, \epsilon s)$-expander of size $(m \times n)$, $b_1, \ldots, b_m \in \{0,1\}$, and $C_1, \ldots, C_m$ be single-output Boolean circuits over arbitrary fixed finite basis such that C_i is a circuit of size $O(s)$ in the variables $X_i(A)$ that computes the function $\Sigma_i(A, b_i)$. Then every PCR refutation of $\tau(A, \vec{C})$ over an arbitrary field F with $char(F) \neq 2$ must have size* $\exp\left(\Omega\left(\frac{r^2}{ms}\right)\right)$.

Proof. Identical to the proof of Corollary 3.6, using Proposition 2.7.■

4 Size lower bounds for linear encoding

In this section we show better lower bounds (although our requirement on the expansion rate is somewhat stronger) on the size of PCR refutation for the more structured linear encoding than those provided by Corollaries 3.11, 3.12. We will apply the random restriction method for killing large clauses rather than directly refer to the general degree/size relation from Proposition 2.7. In this sense our approach is similar in spirit to that of [BP96].

Theorem 4.1 *Let A be an $(r, s, \frac{3}{4}s)$-expander of size $(m \times n)$, and let $b_1, \ldots, b_m \in \{0,1\}$. Then every PCR refutation of $\tau_{\oplus}(A, \vec{b})$ over an arbitrary field F with $char(F) \neq 2$ must have size* $\exp\left(\Omega\left(\frac{r^2}{m}\right)\right)$.

Proof. As the first step toward proving Theorem 4.1, we show how to get rid of the variables y_J for large (= of size $> s/2$) sets J. For technical reasons, we also switch during this step from the linear encoding to the functional one.

Definition 4.2 For an $(m \times n)$-matrix A, the set of variables $Vars_{\oplus}(A) \subseteq Vars(A)$ consists of those $y_f \in Vars(A)$ for which f has the form $\bigoplus_{j \in J} x_j$. Let also $\widetilde{Vars}_{\oplus}(A) \stackrel{\text{def}}{=} \left\{ y_{(\bigoplus_{j \in J} x_j)} \in Vars_{\oplus}(A) \mid |J| \leq s/2 \right\}$.

$\tau_{\oplus}(A,b)$ $[\tilde{\tau}_{\oplus}(A,b)]$ is the set of those axioms in $\tau(A, \vec{\Sigma}(A,b))$ that contain variables only from $Vars_{\oplus}(A)$ [from $\widetilde{Vars}_{\oplus}(A)$, respectively].

It is worth noting that $\tau_{\oplus}(A,b)$ possesses the following clean algebraic description: if $g_i = \Sigma_i(a, b_i)$, and $f_1, \ldots, f_w$ are $\mathbb{F}_2$-linear forms then (5) holds if *either* the system of linear equations $f_1 = \bar{\epsilon}_1, \ldots, f_w = \bar{\epsilon}_w$ is inconsistent *or* the vector space spanned by these equations contains $\bar{g}_i$.

Lemma 4.3 *Suppose that A is an $(2, s, \frac{3}{4}s)$-expander. Then every PCR refutation of $\tau_{\oplus}(A,b)$ can be transformed into a PCR refutation of $\tilde{\tau}_{\oplus}(A,b)$ that has the same size.*

Proof of Lemma 4.3. For every two distinct rows i_1 and i_2 we have $|\partial_A(\{i_1, i_2\})| \geq \frac{3}{2}s$ which implies $|J_{i_1}(A) \cap J_{i_2}(A)| \leq s/2$. Hence, for every $J \subseteq [n]$ with $|J| > s/2$ there can exist at most one row $i \in [m]$ such that $J \subseteq J_i(A)$. Therefore, the following mapping:

$$y_J \mapsto \begin{cases} y_{\bigoplus\{x_j \mid j \in J\}} \text{ if } |J| \leq s/2 \\ y^{\bar{b}_i}_{\bigoplus\{x_j \mid j \in J_i(A) \setminus J\}} \text{ if } |J| > s/2 \text{ and } J \subseteq J_i(A) \end{cases}$$

is well-defined. It is easy to see that it takes every axiom from $\tau_{\oplus}(A,b)$ to an axiom from $\tilde{\tau}_{\oplus}(A,b)$ which proves Lemma 4.3.■

Now, for a monomial $m = y_{f_1}^{\epsilon_1} \ldots y_{f_d}^{\epsilon_d}$ in the variables $\widetilde{Vars}_{\oplus}(A)$, we define its *$A$-degree* $\deg_A(m)$ as the minimal cardinality of a set of rows I with the property $Vars(f_1) \cup \ldots \cup Vars(f_d) \subseteq \bigcup_{i \in I} X_i(A)$. The *$A$-degree of a polynomial* is the maximal A-degree of a monomial in it, and similarly the *A-degree of a PCR* proof is the maximal A-degree of a polynomial in it. The following lemma rephrases Theorem 3.7 for $\deg_A$:

Lemma 4.4 *Let A be an (r, s, c)-expander of size $(m \times n)$, and $b_1, \ldots, b_m \in \{0,1\}$. Then every PCR refutation of $\tau(A, \vec{\Sigma}(A,b))$ over an arbitrary field F with $char(F) \neq 2$ must have A-degree $\geq \frac{rc}{4s}$.*

Proof of Lemma 4.4.
The only difference from Theorem 3.7 is that we consider here A-degree instead of ordinary one. It is easy to see by inspection that this change does not affect the reduction in Lemma 3.9, and the same proof applies here as well.■

Lemmas 4.3 and 4.4 determine the strategy of the rest of the proof (cf. [BP96]). We want to hit the prospective refutation of $\tilde{\tau}_{\oplus}(A,b)$ by a random restriction $\boldsymbol{\rho}$ in such a way that $\boldsymbol{\rho}$ preserves the structure of $\tau(A,\vec{\Sigma}(A,b))$, and, if the size of the original refutation is small, with a high probability also kills all monomials in the variables $\widetilde{Vars}_{\oplus}(A)$ that have high A-degree.

Definition 4.5 For a set of rows I, let us denote by M_I the set of all restrictions ρ such that $\rho^{-1}(\{0,1\}) = \bigcup_{i\in I} X_i(A)$ and ρ satisfies all equations $\Sigma_i(A,b_i) = 1$ for all $i \in I$.

Note that if $|I| \leq r$, then, since A is an $(r,s,\frac{3}{4}s)$-expander, the linear forms $\bigoplus\{x_j \mid x_j \in X_i(A)\} = \Sigma_i(A,b_i) \oplus \bar{b}_i$ are linearly independent and thus M_I is a non-empty linear subspace. Let $A|_I$ be the result of removing from the matrix A all rows $i \in I$ and all columns $j \in \bigcup_{i\in I} J_i(A)$. Any restriction $\rho \in M_I$ can be naturally extended to the variables from $Vars(A)$ by letting $\rho(y_f) \stackrel{\text{def}}{=} y_{f|_\rho}$. ρ takes variables from $Vars(A)$ to variables from $Vars(A|_I)$. Moreover, those y_f for which $\exists i \in I\ (Vars(f) \subseteq X_i(A))$ are set to a constant. Finally, ρ always takes axioms from $\tau(A,\vec{g})$ to axioms from $\tau(A|_I, \vec{g}|_\rho)$. The only remaining problem is that $A|_I$ may not inherit good expansion properties: as an easy example shows, it may even contain an empty row! We circumvent this difficulty by further removing all rows that have large intersection with $\bigcup_{i\in I} J_i(A)$, and show in the following lemma that this can always be done in an efficient manner.

Lemma 4.6 *Let A be an (r,s,c)-expander. Then every set of rows I with $|I| \leq r/2$ can be extended to a larger set of rows $\hat{I} \supseteq I$ such that $|\hat{I}| \leq 2\cdot|I|$ and $A|_{\hat{I}}$ is an $(r,s,3c-2s)$-expander.*

Proof of Lemma 4.6. Let us recursively add to I new rows (one row i_0 at a time) with the property $\left|J_{i_0(A)} \cap \left(\bigcup_{i\in I'} J_i(A)\right)\right| > 2(s-c)$, where I' is the current value of I. We claim that this process will terminate (i.e., no new row can be added) in less than $|I|$ steps.

Suppose the contrary, and let $\hat{I}$ be the set of cardinality $2\cdot|I|$ reached after $|I|$ steps. Then every row $i_0 \in \hat{I} \setminus I$ contains less than $|J_{i_0}(A) - 2(s-c)| \leq (2c-s)$ boundary elements from $\partial_A(\hat{I})$. Hence, $|\partial_A(\hat{I})| < s\cdot|I| + (2c-s)\cdot|I| = 2c\cdot|I|$, a contradiction.

We choose as our $\hat{I}$ the result of termination of this process. Let I_0 be a set of rows in $A|_{\hat{I}}$ (i.e., $I_0 \cap \hat{I} = \emptyset$) of cardinality at most r. Then $\partial_{A|_{\hat{I}}}(I_0) = \partial_A(I_0) \setminus \bigcup_{i\in\hat{I}} J_i(A)$. Since for every $i \in I_0$, $\left|J_{i_0}(A) \cap \left(\bigcup_{i\in\hat{I}} J_i(A)\right)\right| \leq 2(s-c)$, we have the bound $\left|\partial_{A|_{\hat{I}}}(I_0)\right| \geq |\partial_A(I_0)| - 2(s-c)\cdot|I_0| \geq c\cdot|I_0| - 2(s-c)|I_0| = (3c-2s)\cdot|I_0|$. Lemma 4.6 is proved.■

Now we are ready to finish the proof of Theorem 4.1. Fix a PCR refutation π of $\tilde{\tau}_{\oplus}(A,b)$. Assume w.l.o.g. that 18 divides r, and pick at random a set of rows $\boldsymbol{I}$ of cardinality $r/3$. Choose arbitrarily $\hat{\boldsymbol{I}} \supseteq \boldsymbol{I}$ according to Lemma 4.6, i.e., such that $|\hat{\boldsymbol{I}}| \leq \frac{2r}{3}$ and $A|_{\hat{\boldsymbol{I}}}$ is an $(r, s, s/4)$-expander. Pick $\boldsymbol{\rho} \in M_{\hat{\boldsymbol{I}}}$ at random, and apply this restriction to our PCR-refutation π. This will produce a PCR-refutation $\boldsymbol{\rho}(\pi)$ of $\tilde{\tau}_{\oplus}(A|_{\hat{\boldsymbol{I}}}, \boldsymbol{\rho}(\vec{\Sigma}(A,b)))$. By Lemma 4.4 (with $c = s/4$), $\boldsymbol{\rho}(\pi)$ must contain a non-zero monomial $\boldsymbol{\rho}(m)$ of $A|_{\hat{\boldsymbol{I}}}$-degree $> r/18$. Thus, π contains a monomial m that has A-degree $> r/18$ and *is not killed by* $\boldsymbol{\rho}$. In order to finish the proof, we only have to estimate from above the probability $\mathbf{P}[\boldsymbol{\rho}(m) \neq 0]$ for every individual monomial m with $\deg_A(m) > r/18$.

Fix any such $m = y_{f_1}^{\epsilon_1} \ldots y_{f_d}^{\epsilon_d}$, and recall that $f_1, \ldots, f_d$ are $\mathbb{F}_2$-linear forms of weight $\leq s/2$. W.l.o.g. assume that $f_1, \ldots, f_\ell$ form a linear basis of the space $Span(f_1, \ldots, f_d)$. Then $\bigcup_{\nu=1}^{\ell} Vars(f_\nu) = \bigcup_{\nu=1}^{d} Vars(f_\nu)$ and, therefore, $\deg_A(y_{f_1}^{\epsilon_1} \ldots y_{f_\ell}^{\epsilon_\ell}) = \deg_A(m) > r/18$. Hence, w.l.o.g. we can assume from the very beginning that $f_1, \ldots, f_d$ are linearly independent.

Let us now introduce one variation of the notion of A-degree. Namely, for $m = y_{f_1}^{\epsilon_1} \ldots y_{f_d}^{\epsilon_d}$, let $\deg'_A(m)$ be the minimal cardinality of a set of rows I such that these rows "cover" m in the stronger sense $\forall \nu \in [d] \exists i \in I (Vars(f_\nu) \subseteq X_i(A))$. Clearly, $\deg_A(m) \leq \deg'_A(m)$. Also, $\deg'_A$ is "continuous" in the sense that for every monomial m, and every variable y_f^{ϵ}, $\deg'_A(m) \leq \deg'_A(m \cdot y_f^{\epsilon}) \leq \deg'_A(m) + 1$. Therefore, we can gradually remove variables from the monomial m, one variable at a time, until we find in it a sub-monomial m' such that $\deg'_A(m')$ is *exactly* equal to $r/18$. For ease of notation, assume w.l.o.g. that $\deg'_A(m) = r/18$ for the original monomial m.

Fix now any set of rows I_0 with $|I_0| = r/18$ and such that

$$\forall \nu \in [d] \exists i \in I_0 (Vars(f_\nu) \subseteq X_i(A)). \tag{13}$$

We estimate the probability $\mathbf{P}[\boldsymbol{\rho}(m) \neq 0]$ as follows:

$$\mathbf{P}[\boldsymbol{\rho}(m) \neq 0] \leq \mathbf{P}\left[|I_0 \cap \boldsymbol{I}| < \frac{r^2}{100m}\right] + \max_{\substack{|I|=r/3 \\ |I_0 \cap I| \geq \frac{r^2}{100m}}} \mathbf{P}[\boldsymbol{\rho}(m) \neq 0 \,|\, |\boldsymbol{I} = I|]\,.$$

Since $|I_0| = r/18$ and $|\boldsymbol{I}| = r/3$, we can estimate the first term by Chernoff inequality as

$$\mathbf{P}\left[|I_0 \cap \boldsymbol{I}| < \frac{r^2}{100m}\right] \leq \exp\left(-\Omega\left(r^2/m\right)\right). \tag{14}$$

For estimating the second term, fix any individual I such that $|I| = r/3$ and $|I_0 \cap I| \geq \frac{r^2}{100m}$, and let $\hat{I} \supseteq I$ be a corresponding set of rows satisfying the conclusion of Lemma 4.6. We want to estimate $\mathbf{P}[\boldsymbol{\rho}|_{\hat{I}}(m) \neq 0]$, where $\boldsymbol{\rho}|_{\hat{I}}$ is picked at random from $M_{\hat{I}}$.

Let $I_0' = I_0 \cap \hat{I}$, $I_0' = \{i_1, \ldots, i_\ell\}$; $\ell \geq r^2/100m$. Since I_0 is minimal with the property (13), for every $\nu \in [\ell]$ we can choose $f \in \{f_1, \ldots, f_d\}$ such that $Vars(f) \subseteq X_{i_\nu}(A)$ but $Vars(f) \not\subseteq X_i(A)$ for any other $i \in I_0$. Hence, we can assume w.l.o.g. that $Vars(f_\nu) \subseteq X_{i_\nu}(A)$ for $\nu = 1, \ldots, \ell$.

Now, let $V_0 \stackrel{\text{def}}{=} Span(f_1, \ldots, f_\ell)$ be the $\mathbb{F}_2$-linear space generated by the linear functions $f_1, \ldots, f_\ell$, and let $\hat{V} \stackrel{\text{def}}{=} Span\left(\left\{ \bigoplus_{j \in J_i(A)} x_j \,\middle|\, i \in \hat{I} \right\}\right)$. $\mathbf{P}[\boldsymbol{\rho}|_{\hat{I}}(m) \neq 0] \leq \mathbf{P}\left[\boldsymbol{\rho}|_{\hat{I}}(y_{f_1}^{\epsilon_1} \ldots y_{f_\ell}^{\epsilon_\ell}) \neq 0\right]$, and the latter probability is equal either to 0 or to $2^{-(V_0 : V_0 \cap \hat{V})} = 2^{\dim(V_0 \cap \hat{V}) - \ell}$. Hence, we only have to upper bound $\dim(V_0 \cap \hat{V})$.

Let us denote by $\hat{I}^+$ the set of all rows $i \in \hat{I}$ which appear with coefficient $\alpha_i = 1$ in *at least one* sum of the form

$$\bigoplus_{i \in \hat{I}} \alpha_i \cdot \bigoplus_{j \in J_i(A)} x_j \tag{15}$$

that happens to belong to V_0, and let $\hat{V}^+ \stackrel{\text{def}}{=} Span\left(\left\{ \bigoplus_{j \in J_i(A)} x_j \,\middle|\, i \in \hat{I}^+ \right\}\right)$. Then, clearly, $V_0 \cap \hat{V} = V_0 \cap \hat{V}^+$ and $\dim(V_0 \cap \hat{V}) \leq |\hat{I}^+|$.

In order to bound from above $|\hat{I}^+|$, we apply the expansion property to $I_0' \cup \hat{I}^+$ (its cardinality does not exceed $r/18 + 2r/3 < r$). We get $|\partial_A(I_0' \cup$

$\hat{I}^+)| \geq \frac{3}{4}s \cdot |I'_0 \cup \hat{I}^+|$. Note that rows from $\hat{I}^+ \setminus I'_0$ may not contain elements from $\partial_A(I'_0 \cup \hat{I}^+)$ at all; otherwise, the corresponding variable would have appeared in the left-hand side of (15), and this would prevent the latter from being in V_0.

The key observation is that every row i_ν from $\hat{I}^+ \cap I'_0$ may also contain only a relatively small number of boundary elements, namely, at most $(s/2)$. Indeed, $|Vars(f_\nu)| \leq s/2$ (see Definition 4.2). Therefore, if J_{i_ν} would have contained $> s/2$ border elements, then at least one of them would not belong to this J'_ν, and would once more prevent the sum (15) from lying in V_0.

Summing up the above remarks, we have the upper bound $|\partial_A(I'_0 \cup \hat{I}^+)| \leq s \cdot |I'_0 \setminus \hat{I}^+| + \frac{s}{2} \cdot |I'_0 \cap \hat{I}^+|$. Comparing the two bounds on $|\partial_A(I'_0 \cup \hat{I}^+)|$, we obtain via elementary calculations that $|\hat{I}^+| \leq \frac{2}{3}|I'_0| = \frac{2\ell}{3}$.

Therefore, $\dim(V_0 \cap \hat{V}) \leq \frac{2\ell}{3}$ and $\mathbf{P}[\boldsymbol{\rho}|_{\hat{I}}(m) \neq 0] \leq 2^{-\ell/3} \leq \exp(-\Omega(r^2/m))$. Together with (14) this implies $\mathbf{P}[\boldsymbol{\rho}(m) \neq 0] \leq \exp(-\Omega(r^2/m))$. Hence, π must contain at least $\exp(\Omega(r^2/m))$ monomials (of A-degree $\geq r/18$) since otherwise we could find a restriction ρ that kills all of them, contrary to Lemma 4.4. The proof of Theorem 4.1 is complete.■

5 Existence of strong expanders and hard generators

All our hardness results in the previous two sections are based upon the notion of an (r, s, c)-expander. As we noticed in Introduction, one of our eventual goals is to be able to stretch n seed bits to as many output bits m as possible so that the resulting generator is hard for as strong propositional proof systems P as possible. In this section we will see what I/O ratio can we achieve with the results from the two previous sections.

All explicit constructions of (r, s, c)-expanders we know of are based upon Examples 4, 5 from Section 2.1. Unfortunately, the resulting expanders turn out to be virtually useless for our purposes since they can not even break the barrier $m = n$. Let us turn instead to a simple probabilistic argument. We note that in the context of proof complexity, there is not that much advantage to having explicit constructions of hard tautologies over existence proofs.

Theorem 5.1 *For any parameters s, n there exists an $\left(\Omega(n/s)\cdot n^{-O(1/s)}, s, \frac{3}{4}s\right)$-expander of size $(n^2 \times n)$.*

Proof. Let us construct a random $(n^2 \times n)$ matrix $\boldsymbol{A}$ as follows. For every $i \in [n^2]$, let $J_i(\boldsymbol{A}) \stackrel{\text{def}}{=} \{\boldsymbol{j_{i1}}, \ldots, \boldsymbol{j_{is}}\}$, where all $\boldsymbol{j_{i\nu}}$ $(i \in [n^2], \nu \in [s])$ are picked from $[n]$ independently and at random (in fact, we would also obtain the same result by letting $J_i(\boldsymbol{A})$ be uniformly and independently distributed over all s-subsets of $[n]$, but with our choice of $J_i(\boldsymbol{A})$ calculations become simpler). We wish to show that

$$\mathbf{P}[\boldsymbol{A} \text{ is not an } (r, s, 3s/4)\text{-expander}] < 1,$$

for some $r \geq \Omega(n/s)\cdot n^{-0(1/s)}$. Let p_ℓ be the probability that any given ℓ rows of the matrix $\boldsymbol{A}$ violate the expansion property. Then, clearly,

$$\mathbf{P}[\boldsymbol{A} \text{ is not an } (r, s, 3s/4)\text{-expander}] \leq \sum_{\ell=1}^{r} n^{2\ell} p_\ell. \tag{16}$$

Fix an arbitrary I of cardinality $\ell \leq r$. Since every column $j \in \bigcup_{i\in I} J_i(\boldsymbol{A}) \setminus \partial_{\boldsymbol{A}}(I)$ belongs to at least two sets $J_i(\boldsymbol{A})$, we have the bound $\left|\bigcup_{i\in I} J_i(\boldsymbol{A})\right| \leq |\partial_{\boldsymbol{A}}(I)| + \frac{1}{2}\cdot\left(\sum_{i\in I}|J_i(\boldsymbol{A})| - |\partial_{\boldsymbol{A}}(I)|\right) \leq \frac{1}{2}(s\ell + |\partial_{\boldsymbol{A}}(I)|)$. Hence $\partial_{\boldsymbol{A}}(I) < \frac{3}{4}s\ell$ implies also $\left|\bigcup_{i\in I} J_i(\boldsymbol{A})\right| < \frac{7}{8}s\ell$, and we have $p_\ell \leq \mathbf{P}\left[\left|\bigcup_{i\in I} J_i(\boldsymbol{A})\right| \leq \frac{7}{8}s\ell\right]$.

$\bigcup_{i\in I} J_i(\boldsymbol{A})$, however, is equally distributed with $\{\boldsymbol{j_1}, \boldsymbol{j_2}, \ldots, \boldsymbol{j_{s\ell}}\}$, where all $\boldsymbol{j_\mu}$ are chosen from $[n]$ independently and at random, and we can replace $\bigcup_{i\in I} J_i(\boldsymbol{A})$ with this simpler distribution. The event $|\{\boldsymbol{j_1}, \boldsymbol{j_2}, \ldots, \boldsymbol{j_{s\ell}}\}| < \frac{7}{8}s\ell$ is equivalent to the existence of $\frac{1}{8}s\ell$ indices μ among $\{1, \ldots, s\ell\}$ such that $\mathrm{j}_\mu \in \{\boldsymbol{j_1}, \ldots, \boldsymbol{j_{\mu-1}}\}$. Therefore, we can further estimate

$$p_\ell \leq \binom{s\ell}{\frac{1}{8}s\ell} \cdot \max_{1\leq\mu_1<\mu_2<\ldots<\mu_{(s\ell/8)}\leq s\ell} \mathbf{P}\left[\forall\nu \in [s\ell/8](\boldsymbol{j}_{\mu_\nu} \in \{\boldsymbol{j_1}, \ldots, \boldsymbol{j_{\mu_\nu-1}}\})\right].$$

The events $\boldsymbol{j}_{\mu_\nu} \in \{\boldsymbol{j_1}, \ldots, \boldsymbol{j_{\mu_\nu-1}}\}$, however, form a Markov chain and $\mathbf{P}[\boldsymbol{j}_{\mu_\nu} \in \{\boldsymbol{j_1}, \ldots, \boldsymbol{j_{\mu_\nu-1}}\}] \leq (s\ell)/n$. Therefore, we finally have the bound $p_\ell \leq \binom{s\ell}{\frac{1}{8}s\ell}\cdot(s\ell/n)^{s\ell/8} \leq (O(s\ell/n))^{s\ell/8} \leq (O(sr/n))^{s\ell/8}$. Substituting this bound into (16), we obtain

$$\mathbf{P}[\boldsymbol{A} \text{ is not an } (r, s, 3s/4)\text{-expander}] \leq \sum_{\ell=1}^{r} n^{2\ell}\cdot\left(O\left(\frac{sr}{n}\right)\right)^{s\ell/8}. \tag{17}$$

The sum in the right-hand side is the geometric progression with the base $n^2 \cdot (O(sr/n))^{\Omega(s)}$. Hence, if $r = (\epsilon n/s) \cdot n^{-1/s\epsilon}$ for a sufficiently small $\epsilon > 0$, the right-hand side of (17) is less than (1/2) which completes the proof of Theorem 5.1.■

Corollary 5.2 *There exists a family of $(m \times n)$ matrices $A^{(m,n)}$ such that for every $b = (b_1, \ldots, b_m) \in \{0,1\}^m$, any PCR-refutation of $\tau(A^{(m,n)}, \vec{\Sigma}(A^{(m,n)}, b))$ over an arbitrary field with $char(F) \neq 2$ must have size* $\exp\left(\frac{n^{2-O(1/\log\log n)}}{m}\right)$.

Proof. Since for $m \geq n^2$ the bound becomes trivial, we can assume that $m \leq n^2$. Apply Theorem 5.1 with $s = \frac{1}{2}\log_2\log_2 n$, and cross out in the resulting matrix all rows but (arbitrarily chosen) m. This will result in an $(r, s, \frac{3}{4}s)$-expander $A^{(m,n)}$ of size $(m \times n)$, where $r \geq n^{1-O(1/\log\log n)}$. Now we only have to apply Corollary 3.11 and notice that $2^{2^s} = 2^{\sqrt{\log n}} \leq n^{1/\log\log n}$.■

Corollary 5.2 shows that in the functional encoding we can stretch n random bits to $n^{2-O(1/\log\log n)}$ bits so that this generator will be hard for (polynomial size) PCR-proofs over an arbitrary field F with $char(F) \neq 2$. In particular, it is hard for Resolution.

Corollary 5.3 *There exists a family of $(m \times n)$ matrices $A^{(m,n)}$ such that $\left|J_i\left(A^{(m,n)}\right)\right| \leq \log_2 n$ for all $i \in [m]$ and for every $b = (b_1, \ldots, b_m) \in \{0,1\}^m$ we have the following bounds.*

1. *Let $C_1, \ldots, C_m$ be single-output Boolean circuits over an arbitrary fixed finite basis, where C_i is a circuit of size $O(\log n)$ in the variables $X_i(A^{(m,n)})$ that computes the function $\Sigma_i(A^{(m,n)}, b_i)$. Then every PCR-refutation of $\tau(A^{(m,n)}, \vec{C})$ over an arbitrary field with $char(F) \neq 2$ must have size* $\exp\left(\Omega\left(\frac{n^2}{m(\log n)^3}\right)\right)$.

2. *Every PCR-refutation of $\tau_{\oplus}(A^{(m,n)}, b)$ over an arbitrary field with $char(F) \neq 2$ must have size* $\exp\left(\Omega\left(\frac{n^2}{m(\log n)^2}\right)\right)$.

Proof. Same as the proof of Corollary 5.2, only this time we let $s = \log_2 n$.■

Corollary 5.3 allows us to construct generators stretching n bits to $m = o(n^2/(\log n)^4)$ bits in the circuit encoding, and to $m = o(n^2/(\log n)^3)$ bits in the linear encoding which are hard for poly-size PCR-proofs in odd characteristic.

6 Open problems

The open problem which looks absolutely major to us is to break through the quadratic barrier in the I/O ratio. In other words, construct a generator[2] $G_n : \{0,1\}^n \to \{0,1\}^{n^2}$ that would be hard for poly-size resolution proofs. This seems to be essential with the techniques we use, and is reminiscent of the same bottleneck with the weak Pigeon-Hole Principle.

We were mostly concerned in this paper with proving absolute hardness results for pseudorandom generators. Can some structural theory of such generators be developed in the framework of proof complexity? To begin with, can we formulate and prove any reasonable statement that would say, possibly in a restricted way, that if $G_1 : \{0,1\}^n \to \{0,1\}^m$ and $G_2 : \{0,1\}^m \to \{0,1\}^k$ are hard (for a given propositional proof system), then their composition is also hard? That might provide an alternate approach to the quadratic barrier problem.

Our results for Polynomial Calculus and PCR are by far less satisfactory than our results for Resolution. In the latter case we employed quite a natural (and THE natural in the sense of [RR97]) notion of hardness for base functions ("ℓ-robustness"), enjoyed by a random function and used many times in circuit complexity. We simply put it to work in the new context of propositional proofs. On the contrary, for PC(R) we were able to show hardness for essentially one base function, and, in addition, only over fields F with $char(F) \neq 2$. Can we find a reasonably general hardness criterium for the base functions that would enforce the hardness of the resulting generators w.r.t. PCR? It is more or less equivalent to asking whether the machinery from [BGIP99, BI99] can in certain cases work with non-binomial ideals as well?

Can we find explicit constructions of (r, s, c)-expanders with parameters that would be sufficient for (at least, some of) our applications?

Can we git rid of the discouraging 2^{2^s} factor in our size lower bounds for the functional framework (Corollaries 3.5 and 3.11)? One way to think of this would be to look for generalizations of the basic Proposition 2.6 that would take into account the structure of the variables y_f (which can be originally divided into m large groups).

[2]For the reasons explained at the end of Section 2.3, we are interested only in non-primitive encodings. One possible way to formalize this requirement rigorously is to demand that G_n is encoded by 3-CNF's, as opposed to s-CNF's with $s > 3$.

References

[ABSRW99] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Space complexity in propositional calculus. Technical Report TR99-040, Electronic Colloquium on Computational Complexity, ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/1999/TR99-040/index.html, 1999. To appear in *Proceedings of the* 32*st ACM STOC*, 2000.

[Ajt83] M. Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, May 1983.

[Alo98] N. Alon. Spectral techniques in graph algorithms. In C. L. Lucchesi and A. V. Moura, editors, *Lecture Notes in Computer Science* 1380, pages 206–215, Berlin, 1998. Springer-Verlag.

[BGIP99] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi. Linear gaps between degrees for the Polynomial Calculus modulo distinct primes. In *Proceedings of the* 31*st ACM STOC*, pages 547–556, 1999.

[BP96] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *Proceedings of the* 37*th IEEE FOCS*, pages 274–282, 1996.

[BP98] P. Beame and T. Pitassi. Propositional proof complexity: Past, present and future. Technical Report TR98-067, Electronic Colloquium on Computational Complexity, 1998.

[BST98] P. Beame, M. Saks, and J. S. Thathachar. Time-space tradeoffs for branching programs. In *Proceedings of the* 39*th IEEE FOCS*, pages 254–263, 1998.

[BI99] E. Ben-Sasson and R. Impagliazzo. Random CNF"s are Hard for the Polynomial Calculus. In *Proceedings of the* 40*th IEEE FOCS*, pages 415–421, 1999.

[BW99] E. Ben-Sasson and A. Wigderson. Short proofs are narrow - resolution made simple. In *Proceedings of the* 31*st ACM STOC*, pages 517–526, 1999.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th ACM STOC*, pages 174–183, 1996.

[FSS84] M. Furst, J. B. Saxe, and M. Sipser. Parity, circuits and the polynomial time hierarchy. *Math. Syst. Theory*, 17:13–27, 1984.

[Gri98] D. Grigoriev. Tseitin's tautologies and lower bounds for nullstellensatz proofs. In *Proceedings of the 39th IEEE FOCS*, pages 648–652, 1998.

[Gri99] D. Grigoriev. Linear lower bounds on degrees of Postivestellensatz calculus proofs for the parity. Manuscript, 1999.

[Hak85] A. Haken. The intractability or resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Hås86] J. Håstad. *Computational limitations on Small Depth Circuits.* PhD thesis, Massachusetts Institute of Technology, 1986.

[IPS99] R. Impagliazzo, P. Pudlák, and J. Sgall. Lower bounds for the polynomial calculus and the Groebner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999.

[Kra99] J. Krajíček. On the weak pigeonhole principle. Manuscript, 1999.

[N91] N. Nisan. Pseudo-random bits for constant-depth circuits. *Combinatorica*, 11(1):63-70, 1991.

[NW94] N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49(2):149–167, October 1994.

[Raz95a] A. Razborov. Bounded Arithmetic and lower bounds in Boolean complexity. In P. Clote and J. Remmel, editors, *Feasible Mathematics II. Progress in Computer Science and Applied Logic, vol.* 13, pages 344–386. Birkhaüser, 1995.

[Raz95b] A. Razborov. Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic. *Izvestiya of the RAN*, 59(1):201–224, 1995.

[Raz96] A. Razborov. Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In F. Meyer auf der Heide and B. Monien, editors, *Proceedings of the* 23*rd ICALP, Lecture Notes in Computer Science,* 1099, pages 48–62, New York/Berlin, 1996. Springer-Verlag.

[Raz98] A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.

[RR97] A. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[Tse68] Г. С. Цейтин. О сложности вывода в исчислении высказываний. In А. О. Слисенко, editor, *Исследования по конструктивной математике и математической логике,* II*; Записки научных семинаров ЛОМИ, т. 8*, pages 234–259. Наука, Ленинград, 1968. Engl. translation: G. C. Tseitin, On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic, Part II*, ed. A. O. Slissenko, pp. 115-125.

[Urq87] A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.

[Yao82] A. Yao. Theory and applications of trapdoor functions. In *Proceedings of the* 23*rd IEEE FOCS*, pages 92–99, 1982.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the* 26*th IEEE FOCS*, pages 1–10, 1985.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'