Lower Bounds for Polynomial Calculus: Non-Binomial Case

Michael Alekhnovich*, Alexander A. Razborov†

September 27, 2000

Abstract

We generalize recent linear lower bounds for Polynomial Calculus based on binomial ideals. We produce a general hardness criterion (that we call *immunity*) which is satisfied by a random function and prove linear lower bounds on the size of PC refutations for a wide class of tautologies based on immune functions. As some applications of our techniques, we introduce mod_p Tseitin tautologies in the Boolean case (e.g. in the presence of axioms $x_i^2 = x_i$), prove that they are hard for PC over fields with characteristic different from p, and generalize them to Flow tautologies which are based on the MAJORITY function and are proved to be hard over any field. We also show the $\Omega(n)$ lower bound for random k-CNF's over fields of characteristic 2.

1 Introduction

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

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

†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

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]).

The propositional proof systems which recently received much attention are so-called algebraic proof systems simulating the most basic algebraic facts and constructions. The idea to use algebraic machinery in the proof complexity originally appeared in [BIKPP94] who defined the Nullstellensatz refutation system motivated by Hilbert's Nullstellensatz. [CEI96] introduced an even more natural algebraic proof system that directly simulates the process of generating an ideal from a finite set of generators, called Polynomial Calculus (PC for short). This system is a potential candidate for automatic theorem provers [CEI96]; thus it seems interesting and important to prove lower bounds for Polynomial Calculus.

Known approaches to the lower bounds on the degree of Polynomial Calculus use the idea of locality (discussed in Section 2.3), with one notable exception [K97]. First papers [Raz98, IPS99] devoted to Pigeon-Hole Principle involved also rather technical and specific calculations (pigeon dance).

Recently [G98] came up with a simple idea how to avoid completely such calculations and prove $\Omega(n)$ degree lower bounds by using Tseitin tautologies. The original proof in [G98] embraced only Nullstellensatz proof system, then it was generalized to PC in [BGIP99] and further developed in [BI99, Gri99, ABRW00]. One drawback of this idea is that it essentially uses the representation with binomial ideals and can be applied only to binomial functions as the base functions. But there are very few binomials; if we insist on Boolean relations $x^2 - x = 0$, we have only PARITY functions, and in characteristic 2 there are no binomials at all (this restriction can be sometimes circumvented by using low degree reductions [BGIP99] but not always, see for example the case of random k-CNF in characteristic 2 in Section 4.3 below).

This situation was in a sharp contrast with the situation for Resolution where [ABRW00] gave a hardness criterion (robustness) satisfied by a random function and showed that the induced tautologies are hard provided the underlying structure has sufficient expansion. The ideology there is similar to that of Natural Proofs in [RR97]: every lower bound proof which works for a single function must also work for a large class of functions specified by a constructive combinatorial property.

In this paper we fill this gap by giving a hardness criterion (immunity) and proving linear lower bounds for PC refutations of wide class of tautologies based on immune functions.

As some applications of our results, we consider mod_p Tseitin tautologies from [BGIP99] in the Boolean framework (i.e., when our ideal contains the axioms $x_i^2 = x_i$) and prove their hardness over fields of characteristic different from p. Next we introduce the analog of Tseitin tautologies in characteristic 0 (called Flow tautologies) and show that they are hard over any field. The most important impact of our approach, however, is that we can work directly with the field $\mathbb{F}_2$ which is the most interesting case. In particular, we can do random k-CNF over this field, thus we prove the conjecture from [BI99]. At the end we show a weak relation between robust functions from [ABRW00] and immune polynomials in characteristic zero which allows us to get some lower bounds for the *polynomial calculus* (also in characteristic 0) based on the *robustness* of underlying functions.

The paper is organized as follows. Section 2 contains the necessary definitions and the intuition of the lower bound technic based on locality. We prove our main hardness results in Section 3 and show the implied lower bounds in Section 4. Finally we present some open questions in Section 5.

2 Preliminaries

Fix an arbitrary field $\mathbb{F}$. We will be working in the $\mathbb{F}$-algebra $S_n(\mathbb{F})$ which results from factoring the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ by the ideal generated by the relations $x_i^2 - x_i$ $(1 \leq i \leq n)$. Every element $f \in S_n(\mathbb{F})$ has a unique representation as a multilinear polynomial (which determines its *degree* $\deg(f)$), and a unique representation as a $\mathbb{F}$-valued function on $\{0,1\}^n$. We will be alternately exploiting both representations. All polynomials considered in this paper (unless the opposite is stated explicitly) will be multilinear so we sometimes omit this word.

For a polynomial f, $Vars(f)$ will denote the set of its essential variables.

An *assignment to* f is a mapping $\alpha : Vars(f) \to \{0,1\}$.

For historical reasons, when studying a system of algebraic equations one is interested in the set of its *roots*. Thus an assignment α *satisfies* a polynomial f iff α is the root of f. Accordingly, every Boolean function g generates the multilinear polynomial f which is equal to 0 on the assignment α if $g(\alpha) = 1$ and to 1 if $g(\alpha) = 0$.

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 polynomial 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.

If $\bar{v} = \{v_1, \ldots, v_k\}$ is a tuple of variables, and $\bar{\epsilon} \in \{0,1\}^k$ then by $\chi_{\bar{\epsilon}}(\bar{v})$ we denote the multilinear polynomial which is equal to 1 if $\bar{v} = \bar{\epsilon}$ and to 0 otherwise (formally, $\chi_{\bar{\epsilon}}(\bar{v}) \stackrel{\text{def}}{=} \prod_{i \in [k]}(1 - v_i - \epsilon_i + 2v_i\epsilon_i))$. The following identity is obvious but extremely useful:

$$f = \sum_{\bar{\epsilon} \in \{0,1\}^k} \chi_{\bar{\epsilon}}(\bar{v}) \cdot (f|_{\bar{v}=\bar{\epsilon}}) \tag{1}$$

($\bar{v} = \bar{\epsilon}$ is the restriction which assigns all v_i to ϵ_i and leaves all other variables unassigned).

Let $Span(f_1, \ldots, f_k)$ be the ideal generated by $f_1, \ldots, f_k$. We say that $f_1, \ldots, f_k$ *semantically imply* g (denoted $f_1, \ldots, f_k \models g$), if g equals zero on the set of roots of ideal $Span(f_1, ..., f_k)$ (i.e. $\forall \alpha \in \{0,1\}^V (f_1(\alpha) = \cdots = f_k(\alpha) = 0 \Rightarrow g(\alpha) = 0)$, where $V = Vars(f_1) \cup \ldots \cup Vars(f_k) \cup Vars(g))$.

Denote by T_n the set of all *multilinear terms*, i.e., products of the form $x_{i_1}x_{i_2}\ldots x_{i_d}$ with $1 \le i_1 < i_2 < \ldots < i_d \le n$. The *degree* $\deg(t)$ *of a term* t is the number of variables occurring in it. Let $T_{n,d} \stackrel{\text{def}}{=} \{t \in T_n \mid \deg(t) \le d\}$, and $S_{n,d}(\mathbb{F}) \stackrel{\text{def}}{=} \mathbb{F}T_{n,d}$ be the linear space of all multilinear polynomials of degree at most d. We write $t \in f$ if a term t is contained in polynomial f with non-zero coefficient.

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

2.1 Polynomial Calculus

Definition 2.1 ([CEI96]) Every line in a *polynomial calculus proof* is an element of $S_n(\mathbb{F})$, and it has two inference rules (called *addition* and *multi-*

plication, respectively):

$$\frac{f \qquad g}{\alpha f + \beta g} \tag{2}$$

and

$$\frac{f}{f \cdot x}, \tag{3}$$

where $f, g \in S_n(\mathbb{F})$; $\alpha, \beta \in \mathbb{F}$, and x is a variable. For $f_1, \ldots, f_m, g \in S_n(\mathbb{F})$, a *polynomial calculus proof of g from $f_1, \ldots, f_m$* is a proof in which initial polynomials are among $f_1, \ldots, f_m$, and the final polynomial is g. A *polynomial calculus refutation of $f_1, \ldots, f_m$* is a polynomial calculus proof of 1 from $f_1, \ldots, f_m$.

Clearly, g has a polynomial calculus proof from $f_1, \ldots, f_m$ if and only if $g \in Span(f_1, \ldots, f_m)$. In particular, $(f_1, \ldots, f_m)$ is refutable if and only if $1 \in Span(f_1, \ldots, f_m)$, and if and only if (see e.g. [BIKPRS96, Theorem 5.2]) the system $f_1 = f_2 = \ldots = f_m = 0$ has no 0–1 solutions.

The *degree of the addition inference* (2) is $\max\{\deg(f),\ \deg(g)\}$, and the *degree of the multiplication inference* (3) is $\deg(f) + 1$. The *degree of a proof* is the maximum of the degrees of all its inferences.

2.2 Tautologies induced by expanders

In this section we define the general structure of our tautologies. We use the notion of expander matrix introduced in [CS88, ABRW00].

Let A be an $(m \times n)$ 0-1 matrix, and $J_i(A) \stackrel{\text{def}}{=} \{ j \in [n] \mid a_{ij} = 1 \}$.

Definition 2.2 ([ABRW00]) 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 $\forall I \subseteq [m](|I| \leq r \Rightarrow |\partial_A(I)| \geq c \cdot |I|)$.

This notion generalizes the notion of expander hypergraphs from [CS88] (they considered expanders with $c = 1/2$). We discuss the construction of good expanders in Section 4.1.

Let $X_i(A) \stackrel{\text{def}}{=} \{ x_j \mid j \in J_i(A) \}$ and $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$ be polynomials such that $Vars(f_i) \subseteq X_i(A)$. We will be interested in the system of equations

$$\begin{cases} f_1(x_1,\ldots,x_n)=0 \\ \cdots \\ f_m(x_1,\ldots,x_n)=0. \end{cases} \tag{4}$$

[ABRW00] proved that if f_i's posses certain hardness property called robustness (and A is a sufficiently good expander) then the system (4) is hard for Resolution. Based upon the machinery developed in [G98, BGIP99], they also showed that the system (4) is hard for Polynomial Calculus when f_i's are the PARITY functions and char $\mathbb{F} \neq 2$. In this paper we introduce a *general* hardness condition on f_i which will imply that this system is hard for Polynomial Calculus.

Definition 2.3 A polynomial f is called *ℓ-immune* iff for any non-zero polynomial g $f \models g$ implies $\deg(g) \geq \ell$. A Boolean function is ℓ-immune over a field if its associated multi-linear polynomial over this field (described in Section 2) is ℓ-immune.

This definition says that a polynomial is hard iff it has no non-trivial semantic corollaries of small degree. Clearly a polynomial g which depends on s variables can have immunity at most s. In Section 4 we will show several examples of ℓ-immune polynomials for $\ell = \Omega(s)$. We will also discuss the relation between ℓ-robust functions from [ABRW00] and ℓ-immune polynomials.

The following simple lemma shows that the notion of immunity behaves well with respect to restrictions.

Lemma 2.4 *If f is ℓ-immune then, for any restriction ρ, $f|_\rho$ is $(\ell - |\rho|)$-immune.*

Proof. Suppose that ρ assigns $v_1,\ldots,v_k$ to $\epsilon_1,\ldots,\epsilon_k$, and assume the contrary, that is $f|_{\bar{v}=\bar{\epsilon}} \models g$, where $g \neq 0$ and $\deg(g) < \ell - k$. We can assume w.l.o.g. that $Vars(g) \cap \{v_1,\ldots,v_k\} = \emptyset$. Then, clearly, $f \models \chi_{\bar{\epsilon}}(\bar{v}) \cdot g$ and $\chi_{\bar{\epsilon}}(\bar{v}) \cdot g \neq 0$, a contradiction.$\blacksquare$

2.3 Local strategy for lower bounds for PC

Now we briefly describe how the idea of locality can help in proving lower bounds on the degree of PC refutation. First, let us recall some standard notions from commutative algebra (adapted to the special case of the ring $S_n(\mathbb{F})$).

Definition 2.5 An ordering $\preceq$ of T_n is *admissible* if:

1. $\forall t_1, t_2 \in T_n(\deg(t_1) < \deg(t_2) \Rightarrow t_1 \prec t_2)$.
2. If $t_1 \preceq t_2$ and $t \in T_n$ does not contain any variables from t_1, t_2, then $tt_1 \preceq tt_2$.

Fix an admissible ordering $\preceq$ on T_n. For $f \in S_n(\mathbb{F})$, $LT(f) \in T_n$ is the *leading term* of f w.r.t. $\preceq$. Part 1 of Definition 2.5 implies that $\deg(LT(f)) = \deg(f)$.

Definition 2.6 For an ideal V the term t is called *reducible* mod V (and with respect to some admissible ordering $\preceq$) if V contains some polynomial f such that $LT(f) = t$. The set of irreducible terms Δ is linearly independent modulo V and the algebra $S_n(\mathbb{F})$ can be represented as the direct sum

$$S_n(\mathbb{F}) = \mathbb{F}\Delta \oplus V.$$

The operator of projection onto the first coordinate, called *reduction operator* (and denoted R_V) maps each term t to the unique polynomial $R_V(t) \in \mathbb{F}\Delta$ such that $t - R_V(t) \in V$.

[CEI96] were the first to consider these classical notions in the case when V is a pseudo-ideal, i.e. not necessarily closed under the multiplication rule. This leads to the following chain of definitions.

For $f_1, \ldots, f_m \in S_{n,d}(\mathbb{F})$, denote by $V_{n,d}(f_1, \ldots, f_m)$ the set of all $g \in S_{n,d}(\mathbb{F})$ that are provable from $f_1, \ldots, f_m$ by a polynomial calculus proof of degree at most d. Due to the presence of the addition rule, $V_{n,d}(f_1, \ldots, f_m)$ is a linear subspace in $S_{n,d}(\mathbb{F})$. A term $t \in T_{n,d}$ is called *reducible* if $t = LT(f)$ for some $f \in V_{n,d}(f_1, \ldots, f_m)$, and *irreducible* otherwise. Denote by $\Delta_{n,d}(f_1, \ldots, f_m)$ the set of all irreducible terms in $T_{n,d}$. Terms from

$\Delta_{n,d}(f_1, \ldots, f_m)$ are linearly independent modulo $V_{n,d}(f_1, \ldots, f_m)$, and analogously with the classical case we have the representation

$$S_{n,d}(\mathbb{F}) = \mathbb{F}\Delta_{n,d}(f_1, \ldots, f_m) \oplus V_{n,d}(f_1, \ldots, f_m) \tag{5}$$

of $S_{n,d}(\mathbb{F})$ as the direct sum. Denote the projection onto the first coordinate (also called *reduction operator*) by $R_{n,d,f_1,\ldots,f_m}$.

In order to prove that $1 \notin V_{n,d}(f_1, ..., f_m)$ one has to show that

$$R_{n,d,f_1,\ldots,f_m}(1) \neq 0.$$

For doing that it suffices to produce a non-trivial linear operator R on $S_{n,d}(\mathbb{F})$ which is stronger than $R_{n,d,f_1,\ldots,f_m}$ in the sense that

$$\mathrm{Ker}(R_{n,d,f_1,\ldots,f_m}) \subseteq \mathrm{Ker}(R)$$

and show that $\mathrm{Ker}(R) \neq S_{n,d}(\mathbb{F})$. The following lemma states what need be checked for that.

Lemma 2.7 ([Raz98]) *Suppose that $f_1, ..., f_m$ are axioms, and $d < n$. If there exist a linear operator $R \not\equiv 0$ on $S_{n,d}(\mathbb{F})$ such that:*

1) $\forall i\ R(f_i) = 0$;

2) $\forall t, x_j\ (\deg(t) < d \to R(x_j \cdot t) = R(x_j \cdot R(t)))$

then there is no PC refutation of $\{f_1, ..., f_m\}$ with degree less or equal than d.

[Raz98] proposed to construct the operator R from the previous lemma locally:

$$R(t) \stackrel{\text{def}}{=} R_{V(t)}(t), \tag{6}$$

where $R_{V(t)}$ is the classical reduction operator of the ordinary ideal $V(t)$ generated by some "small" subset of axioms dependent on t. The advantage we gain in this way is that the structure of classical reduction operators is much better understood, and, unlike their counterparts for pseudo-ideals, they can be also studied by semantical means.

If R is any operator satisfying assumptions of Lemma 2.7, then every polynomial $f = \sum_i a_i t_i$ derivable from $\{f_1, \ldots, f_m\}$ in degree $\leq d$ can be alternatively represented as the sum

$$f = \sum_i a_i (t_i - R(t_i)).$$

If, moreover, $R(t)$ is given by (6), then t_i's are leading terms in $(t_i - R(t_i))$, there is no cancellation between them, and each polynomial $t_i - R(t_i)$ is a corollary of a "small" number of axioms. Thus the idea of locality says that any polynomial in $V_{n,d}(f_1, ..., f_m)$ can be represented by the sum of corollaries of small number of axioms without leading terms cancellation or, informally, *everything we can infer in small degree we can also infer locally.*

3 Main results

In this section we prove that for any (r, s, c)-expander A and ℓ-immune f_i's any PC refutation of the system (4) has degree greater than $r(\ell/4 - (s - c))$ (Theorem 3.8). This bound presumes that $\ell > 4(s - c)$ and thus it is not applicable to expanders with small constant s and c. We managed to strengthen the degree lower bound to $rc/2$ in the case when f_i's have maximal immunity s (Theorem 3.13). This bound will allow us to estimate the hardness of refutation of the random k-CNF for small k in the fields of characteristic 2 (Section 4.3).

The heart of our proof is the following theorem.

Theorem 3.1 *Suppose that Y, V, Z is a partition of $\{x_1, ..., x_n\}$; $\bar{P} = \bar{P}(\bar{y}, \bar{v})$, $Q = Q(\bar{v}, \bar{z})$ are polynomials over $Y \cup V$, $V \cup Z$ respectively, where Q is $(2|V| + 1)$-immune. Suppose that a term $t(\bar{y}, \bar{v})$ free of Z-variables is reducible mod $Span(\bar{P}, Q)$ w.r.t some fixed admissible ordering. Then t is reducible mod $Span(\bar{P})$ w.r.t. the same ordering.*

Proof. The naive idea would be to apply an arbitrary homomorphism of the form $\rho : \bar{z} \to \bar{f}(\bar{v})$ which kills Q to 0 and therefore has the property $t = \rho(R_{Span(\bar{P},Q)}(t))$ mod $Span(\bar{P})$ (such a homomorphism always exists since Q is $(|V| + 1)$-immune and hence none of $\chi_{\bar{\epsilon}}(\bar{v})$ in $\sum \chi_{\bar{\epsilon}}(\bar{v}) Q|_{\bar{v}=\bar{\epsilon}} = Q$ is its corollary). This does not work in general because the degree of some terms in $R_{Span(\bar{P},Q)}(t)$ may increase under ρ and become more than $\deg(t)$.

Still as we show below this idea suffices in the partial case when Q has the maximal immunity (Lemma 3.14). But in the general case we have to use more complicated methods.

In Definition 3.2 and the following chain of lemmas we assume that $X, V, Z, \bar{P}, Q$ satisfy assumptions of Theorem 3.1, and all reduction operators are taken w.r.t. some fixed admissible ordering $\preceq$. Let $k \stackrel{\text{def}}{=} |V|$.

Definition 3.2 (Operator R^Q) The linear operator R^Q is defined on T_n in the following way:

$$R^Q(t) \stackrel{\text{def}}{=} \sum_{\bar{\epsilon} \in \{0,1\}^k} \chi_{\bar{\epsilon}}(\bar{v}) \cdot R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(t|_{\bar{v}=\bar{\epsilon}}),$$

and extended to $S_n(\mathbb{F})$ by linearity.

The intuitive meaning of the operator R^Q is that it tries to reduce Z-degree of the term t locally and independently within the subcubes specified by all possible assignments to V. It ignores Y-variables (since they do not appear in Q), but it can in general increase the number of V-variables.

Lemma 3.3 *For any polynomial f, $f = R^Q(f)$ mod $Span(Q)$.*

Proof. Due to linearity, we only need to prove that $Q \models t - R^Q(t)$ for every term t. This semantic inference holds if and only if for any tuple $\bar{\epsilon}$ the polynomial $Q|_{\bar{v}=\bar{\epsilon}}$ implies

$$(t - R^Q(t))|_{\bar{v}=\bar{\epsilon}} = (t|_{\bar{v}=\bar{\epsilon}} - R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(t|_{\bar{v}=\bar{\epsilon}})),$$

and the latter clearly takes place.∎

Lemma 3.4 *If $|Vars(t) \cap Z| \leq k$ then $R^Q(t) = t$.*

Proof.

We need to check that two polynomials t and $R^Q(t)$ are equal. For this it is sufficient to check the equality of $t|_{\bar{v}=\bar{\epsilon}}$ and $R^Q(t)|_{\bar{v}=\bar{\epsilon}} = R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(t|_{\bar{v}=\bar{\epsilon}})$ for each tuple $\bar{\epsilon} \in \{0,1\}^k$. But since Q is $(2k+1)$-immune, $Q|_{\bar{v}=\bar{\epsilon}}$ is $(k+1)$-immune by Lemma 2.4; therefore the term $t|_{\bar{v}=\bar{\epsilon}}$ of degree $\leq k$ is irreducible mod $Span(Q|_{\bar{v}=\bar{\epsilon}})$.∎

The following lemma is the heart of the whole argument.

Lemma 3.5 *Suppose that f is a polynomial and $\bar{P}, Q \models f$. Then $\bar{P} \models R^Q(f)$.*

Proof. As usual, we only have to prove that for any tuple $\bar{\epsilon}$, $\bar{P}|_{\bar{v}=\bar{\epsilon}} \models R^Q(f)|_{\bar{v}=\bar{\epsilon}}$. Since $\bar{P}, Q \models f$, by Lemma 3.3 we have $\bar{P}, Q \models R^Q(f)$, hence $\bar{P}|_{\bar{v}=\bar{\epsilon}}, Q|_{\bar{v}=\bar{\epsilon}} \models R^Q(f)|_{\bar{v}=\bar{\epsilon}}$.

Fix an arbitrary tuple $\bar{\delta}$ for $\bar{y}$ such that $\bar{P}|_{\bar{v}=\bar{\epsilon}}(\bar{\delta}) = 0$. We have

$$Q|_{\bar{v}=\bar{\epsilon}} \models R^Q(f)|_{\bar{v}=\bar{\epsilon},\bar{y}=\bar{\delta}}, \tag{7}$$

and we have to show that

$$R^Q(f)|_{\bar{v}=\bar{\epsilon},\bar{y}=\bar{\delta}}$$

is actually equal to 0. But $R^Q(f)|_{\bar{v}=\bar{\epsilon},\bar{y}=\bar{\delta}} = R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(f|_{\bar{v}=\bar{\epsilon}})|_{\bar{y}=\bar{\delta}}$. Since all terms in $R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(f|_{\bar{v}=\bar{\epsilon}})$ are irreducible mod $Span(Q|_{\bar{v}=\bar{\epsilon}})$, and the set of irreducible terms is closed downward, the same is true for

$$R_{Span(Q|_{\bar{v}=\bar{\epsilon}})}(f|_{\bar{v}=\bar{\epsilon}})|_{\bar{y}=\bar{\delta}}.$$

Along with (7) this implies $R^Q(f)|_{\bar{v}=\bar{\epsilon},\bar{y}=\bar{\delta}} = 0$ and completes the proof of Lemma 3.5.■

Lemma 3.6 *Suppose that $\bar{P} \models f_0 + \sum_{z_i \in Z} z_i f_i$, where f_0 is free of Z-variables. Then $\bar{P} \models f_0$.*

Proof. Apply the restriction which maps all z_i to 0.■

Let us now finish the proof of Theorem 3.1. Let $f \stackrel{\text{def}}{=} R_{Span(\bar{P},Q)}(t)$ and $f' \stackrel{\text{def}}{=} R^Q(f)$.

By Lemma 3.5, $\bar{P} \models R^Q(t-f)$, and by Lemma 3.4, $R^Q(t) = t$. Thus, $\bar{P} \models (t - f')$. Our goal is to show that all terms in f' are either less than t or contain some Z-variables, after that we can apply Lemma 3.6 and show that t can be reduced mod $Span(\bar{P})$.

Let us divide the terms in f into two groups:

$$\begin{aligned} G_1 &= \{t_1 \mid |Vars(t) \cap Z| \le k\} \\ G_2 &= \{t_1 \mid |Vars(t) \cap Z| > k\}. \end{aligned}$$

Consider some monomial $t_1' \in f'$ such that $|Vars(t_1') \cap Z| = \emptyset$. Clearly, $t_1' \in R^Q(t_1)$ for some term $t_1 \in f$. If $t_1 \in G_1$ then, since G_1 is invariant under R^Q by Lemma 3.4, $t'_1 = t_1 \prec t$. Assume that $t_1 \in G_2$. Then $\deg(t'_1) = |Vars(t'_1) \cap V| + |Vars(t'_1) \cap Y| \leq k + |Vars(t'_1) \cap Y| = k + |Vars(t_1) \cap Y| < |Vars(t_1) \cap Y| + |Vars(t_1) \cap Z| \leq \deg(t_1) \leq \deg(t)$.

Thus all monomials in f' which are free of Z-variables either are contained in f or have degree less than $\deg(t)$. Hence Lemma 3.6 implies that t is reducible by $\bar{P}$. Theorem 3.1 is proved.■

Corollary 3.7 *Under the assumptions of Theorem 3.1,*

$$R_{Span(\bar{P},Q)}(t) = R_{Span(\bar{P})}(t).$$

Proof. Obviously, all terms in $R_{Span(\bar{P})}(t)$ are free of Z-variables. Therefore, by Theorem 3.1 all of them are irreducible also mod $Span(\bar{P}, Q)$.■

Theorem 3.8 *Assume that A is an (r, s, c)-expander, ℓ is an integer such that $s \leq r(\ell/4 - (s - c))$ and $f_1, \ldots, f_m$ are ℓ-immune polynomials over an arbitrary field such that $Vars(f_i) \subseteq X_i(A)$. Then any PC refutation of the system $f_1 = \ldots = f_m = 0$ has degree greater than $r(\ell/4 - (s - c))$.*

Proof. The idea of the proof is to construct a linear operator R which behaves locally like the reduction operator modulo the corresponding ideal, and use Lemma 2.7 after that. To describe R it is sufficient to define it on the set of terms t with $\deg(t) \leq r(\ell/4 - (s - c))$. First we need to give some more notation.

Definition 3.9 Assume that A is an $(m \times n)$-matrix and $f_1, ..., f_m$ are polynomials with $Vars(f_i) \subseteq X_i(A)$. For a term t denote by $J(t)$ the index set $\{j | t \text{ contains } x_j\}$. For a set of rows $I \subseteq [m]$ let $Span(I) \stackrel{\text{def}}{=} Span(\{f_i | i \in I\})$.

Now we are ready to define our linear operator R. Fix $A, f_1, \ldots, f_m, r, s, c, \ell$ satisfying assumptions of Theorem 3.8. For a term t we define a set of axioms $Sup(t) \subseteq [m]$ and then reduce t mod $Span(Sup(t))$:

Definition 3.10 For a term t define the following inference relation $\vdash_t$ on the set $[m]$ of rows of A:

$$I \vdash_t i \equiv \left| J_i(A) \cap \left[\bigcup_{i' \in I} J_{i'}(A) \cup J(t) \right] \right| > \frac{\ell}{4}. \tag{8}$$

Let the *support* $Sup(t)$ of t be the set of all rows which can be inferred via $\vdash_t$ from the empty set. Define $R(t) \stackrel{\text{def}}{=} R_{Span(Sup(t))}(t)$.

The rest of the proof is devoted to checking that R satisfies conditions 1) and 2) of Lemma 2.7. First we need to estimate the cardinality of $Sup(t)$.

Lemma 3.11 *For a term t with $\deg(t) \leq r(\ell/4 - (s-c))$, $|Sup(t)| < r$.*

Proof. Assume the contrary. Then there exists a set $I = \{i_1, \ldots, i_r\}$ of distinct rows such that $\{i_1, \ldots, i_{\nu-1}\} \vdash_t i_\nu$ $(1 \leq \nu \leq r)$. By Definition 2.2 it has at least cr boundary elements. By (8), each row $i \in I$ has strictly less than $s - \ell/4$ boundary elements not contained in $J(t)$. Thus, $J(t)$ has more than $cr - r(s - \ell/4) = r(\ell/4 - (s-c))$ elements. We got contradiction, which proves Lemma 3.11.$\blacksquare$

Lemma 3.12 *Assume that $s - c < \ell/4$, t is a term and I is a set of rows such that $I \supseteq Sup(t)$ and $|I| \leq r$. Then*

$$R_{Span(I)}(t) = R_{Span(Sup(t))}(t).$$

Proof. Let us apply the expansion property to the set $I \setminus Sup(t)$. It will yield a row $i \in I \setminus Sup(t)$ with at least c boundary elements. In other words,

$$J_i(A) \cap [\cup_{i' \in I \setminus (Sup(t) \cup \{i\})} J_{i'}(A)] \leq s - c.$$

Also, since $Sup(t)$ is closed under $\vdash_t$, we have

$$J_i(A) \cap [\cup_{i' \in Sup(t)} J_{i'}(A) \cup J(t)] \leq \ell/4.$$

Altogether it implies that

$$J_i(A) \cap [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \leq (s-c) + \ell/4 < \ell/2.$$

Let us now set in Theorem 3.1

$$\begin{array}{rcl} Y & := & \{x_1, \ldots, x_n\} \setminus J_i(A),\ V := J_i(A) \cap [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \\ Z & := & J_i(A) \setminus [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \\ \bar{P} & := & \{\, f_{i'} \mid i' \in I \setminus \{i\} \,\} \\ Q & := & f_i, \end{array}$$

and apply in this situation its Corollary 3.7. We conclude that $R_{Span(I)}(t) = R_{Span(I \setminus \{i\})}(t)$. We continue this elimination process until we descend to $R_{Sup(t)}(t)$.$\blacksquare$

Now we finish the proof of Theorem 3.8. We have produced an operator R on T_n, and we consider its restriction on $T_{n,r(\ell/4-(s-c))}$. Let us check that it indeed satisfies the conditions of Lemma 2.7.

To see that $R(f_i) = 0$ for each axiom f_i, let $t_i \stackrel{\text{def}}{=} \prod X_i(A)$. Recall that $\deg(t_i) \le s \le r(\ell/4 - (s-c))$. Thus $|Sup(t_i)| < r$ (by Lemma 3.11) and for any term t in f_i clearly $Sup(t) \subseteq Sup(t_i)$. Next, $i \in Sup(t_i)$. By Lemma 3.12, $R(f_i) = R_{Sup(t)}(f_i) = 0$. Thus 1) is satisfied.

To check the second condition, consider a term t with $\deg(t) \le r(\ell/4 - (s-c)-1$ and a variable x_j. By Lemma 3.11, $|Sup(x_jt)| < r$. By Lemma 3.12, $R_{Sup(t)}(t) = R_{Sup(x_jt)}(t)$. For any term $t' \in R_{Sup(t)}(t)$, $Sup(x_jt') \subseteq Sup(x_jt)$. To see this, it is sufficient to notice that $J(t') \subseteq \bigcup_{i' \in Sup(t)} J_{i'}(A) \cup J(t)$. Thus $R_{Sup(x_jt')}(x_jt') = R_{Sup(x_jt)}(x_jt')$ and

$$R(x_jR(t)) = R_{Sup(x_jt)}(x_jR_{Sup(x_jt)}(t)) = R_{Sup(x_jt)}(x_jt),$$

where the last equality follows from the fact that $x_jR_{Sup(x_jt)}(t)$ and x_jt are equal modulo the ideal $Span(Sup(x_jt))$.

Finally, $|J_i(A)| \ge \ell$ for every $i \in [m]$ (since f_i is ℓ-immune), hence $Sup(1) = \emptyset$ and $R(1) = 1$.

Theorem 3.8 is proved.■

The bound proved in Theorem 3.8 is not applicable in the case when c is small (say, $c < 1$). We will see in Section 4.1 that for sufficiently large constant s "good expanders" (that is, with c close to s) do exist but for small s the question about the hardness of the system (4) remains open even for random matrices. When c is small, we succeeded in proving lower bounds only in the partial case, when all f_i have the maximal immunity $\ell = s$. It is easy to see that the class of polynomials with maximal immunity consists exactly of polynomials having the form $\alpha \cdot \chi_{\bar{\epsilon}}(\bar{v}),\ \alpha \in \mathbb{F}^*$.

Theorem 3.13 *Assume that A is an (r,s,c)-expander, $|J_i(A)| = s$ for all rows $i \in [m]$ and $\epsilon^{(i)} \in \{0,1\}^{X_i(A)}$. Then any PC refutation of the system $\{\chi_{\epsilon^{(i)}}(X_i(A)) \mid i \in [m]\}$ has degree greater than $(rc/2)$.*

Proof. Analogous to the proof of Theorem 3.8, but in this partial case the statement of Theorem 3.1 can be strengthened while the proof becomes trivial:

Lemma 3.14 *Suppose that Y, V, Z is a partition of $\{x_1, ..., x_n\}$; $\bar{P} = \bar{P}(\bar{y}, \bar{v})$, $Q = Q(\bar{v}, \bar{z})$ are polynomials over $Y \cup V$, $V \cup Z$ respectively, where Q is divisible by $(z - \epsilon)$ for some $z \in Z$, $\epsilon \in \{0, 1\}$. Suppose that a term $t(\bar{y}, \bar{v})$ free of Z-variables is reducible mod Span$(\bar{P}, Q)$ w.r.t some fixed admissible ordering. Then t is reducible mod Span$(\bar{P})$.*

Proof. Consider any polynomial f s.t. $\bar{P}, Q \models f$ and $t = LT(f)$. Applying the restriction $z = \epsilon$, we obtain $\bar{P}|_{z=\epsilon}, Q|_{z=\epsilon} \models f|_{z=\epsilon}$. Since $\bar{P}$ does not depend on z and $Q|_{z=\epsilon} = 0$, $\bar{P} \models f|_{z=\epsilon}$, and clearly $t = LT(f|_{z=\epsilon})$.■

Now we build our operator R in the same way as in Definition 3.10, but this time we use another inference relation (notice that this relation infers a *set* of rows at a time rather than a single row):

Definition 3.15 For a term t define the following inference relation $\vdash_t$ on the set $[m]$ of rows of A:

$$I \vdash_t I_1 \equiv \; |I_1| \leq r/2 \; \wedge \; \partial_A(I_1) \subseteq \left[\bigcup_{i \in I} J_i(A) \cup J(t) \right]. \tag{9}$$

Let the *support* $Sup(t)$ of t be the set of all rows which can be inferred via $\vdash_t$ from the empty set, and $R(t) \stackrel{\text{def}}{=} R_{Span(Sup(t))}(t)$.

Lemma 3.16 *For a term t with* $\deg(t) \leq (cr/2)$, $|Sup(t)| \leq r/2$.

Proof. Assume the contrary, and choose a chain of subsets $I_1, \ldots, I_2, \ldots$ such that $I_1 \cup \ldots \cup I_{\nu-1} \vdash_t I_\nu$ and $|\cup_\nu I_\nu| > r/2$. Let k be the *smallest* index for which $\left|\bigcup_{\nu=1}^k I_\nu\right| > r/2$. Then, clearly, $\left|\bigcup_{\nu=1}^k I_\nu\right| \leq r$ (since $|I_\nu| \leq r/2$). Therefore, $\left|\partial_A\left(\bigcup_{\nu=1}^k I_\nu\right)\right| > (rc/2)$. On the other hand, (9) implies that every new boundary element that results from appending via $\vdash_t$ some set of rows must belong to $J(t)$, therefore $\partial_A\left(\bigcup_{\nu=1}^k I_\nu\right) \subseteq J(t)$. This contradiction with the assumption $\deg(t) \leq (cr/2)$ proves Lemma 3.16.■

The following is analogous to Lemma 3.12.

Lemma 3.17 *Assume that t is a term, and I is a subset of rows such that $I \supseteq Sup(t)$ and $|I| \leq r/2$. Then*

$$R_{Span(I)}(t) = R_{Span(Sup(t))}(t).$$

Proof. Since $Sup(t) \not\vdash_t I \setminus Sup(t)$, by (9) some row $i \in I \setminus Sup(t)$ contains an element from $\partial_A(I) \setminus J(t)$. Thus we can remove i by Lemma 3.14. In such a way we consequently get rid of all the axioms in $I \setminus Sup(t)$.■

The rest of the proof is quite analogous to that of Theorem 3.8.■

4 Applications

In this section we describe some concrete lower bounds that can be proved using the results of Section 3.

4.1 Constructions of expanders

[CS88] in their work introduced the notion of a sparse hypergraph which in our language (rows correspond to edges, columns correspond to vertices) looks as follows: an $(m \times n)$ 0-1 matrix A is (x, y)-*sparse* if for every $J \subseteq [n]$ with $|J| \leq xn$ we have $|\{i \in [m] \mid J_i(A) \subseteq J\}| \leq y \cdot |J|$. They also established (implicitly and for the case $c = 1/2$) the following connection between sparsity and expansion (*union bound*) which was later utilized in [BP96, BKPS98, ABRW00]: any $(m \times n)$ $\left(\frac{r(k+c)}{2n}, \frac{2}{k+c}\right)$-sparse matrix in which every row contains exactly k ones is an (r, k, c)-expander, for arbitrary parameters r, k, c.

[CS88, Lemma 1] gave a sufficient condition for a random $(\Delta n \times n)$ matrix (in which every row has exactly k ones) to be (x, y)-sparse. They considered only the case when the parameters k, y, Δ (the latter is denoted in [CS88] by c) are constants. We need the following simple generalization of their lemma.

Let k be an integer constant, $y = y(n)$ be any real parameter such that $(k-1)y > 1$ and $\Delta = \Delta(n)$ be an arbitrary integer parameter satisfying

$$\Delta = o\left(n^{(k-1-y^{-1})}\right). \tag{10}$$

Then a random $(\Delta n \times n)$ matrix in which every row has exactly k ones is $\left(\Omega\left(\Delta^{-y/((k-1)y-1)}\right), y\right)$-sparse with probability $1 - o(1)$.

The proof literally follows the proof of [CS88, Lemma 1]; we only need to change the values of their bounds $f(n), g(n)$ to

$$f(n) \stackrel{\text{def}}{=} e\left(\frac{e}{y}\right)^y \cdot n^{-((k-1)y-1)/2} \cdot \Delta^{y/2},$$

$$g(n) \stackrel{\text{def}}{=} \left(n \cdot \Delta^{-1/(k-1-y^{-1})}\right)^{1/2}.$$

The necessary asymptotics $f(n) \to 0,\ g(n) \to \infty$ then follow from (10).

Putting things together by setting $y \stackrel{\text{def}}{=} \frac{2}{k+c}$, we have:

Lemma 4.1 *Assume that $k \geq 3$ is a fixed integer constant, $0 < c = c(n) < k-2$ is an arbitrary real parameter, and $\Delta = \Delta(n)$ is an arbitrary integer parameter satisfying $\Delta = o\left(n^{(k-c-2)/2}\right)$. Then a random $(\Delta n \times n)$ matrix A in which each line $J_i(A)$ is chosen from all $\binom{n}{k}$ k-subsets of $[n]$ independently and at random is $\left(\Omega\left(\frac{n}{\Delta^{2/(k-c-2)}}\right), k, c\right)$-expander with probability $1 - o(1)$.*

Now let us turn to another source of good expanders. For an ordinary graph $G = (V, E)$ and $r \geq 1$ let

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

where $e(U, W)$ is the number of edges between U and W. This is a minor generalization of the edge-expansion coefficient $c_E(G) = c_E(|V|/2, G)$ previously studied in graph theory (see e.g. [Alo98] and the literature cited therein). Clearly, the incidence matrix A_G of a graph G is an $(r, d(G), c_E(r, G))$-expander for an arbitrary r (cf. [ABRW00, Example 4]), where $d(G)$ is the maximal degree of a vertex.

Suppose now that the graph G is d-regular. Then, clearly, $c_E(r, G) = d - \max_{|U| \leq r} ad(G|_U)$, where $G|_U$ is the subgraph induced on U, and ad is the average degree. [BCS78] proved the following bound on this quantity in terms of the second eigenvalue $\lambda_2(G)$ of the graph G:

$$ad(G|_U) \leq \frac{|U|(d - \lambda_2(G))}{|V|} + \lambda_2(G).$$

This implies

$$c_E(r, G) \geq d\left(1 - \frac{r}{|V|}\right) - \lambda_2(G).$$

Recall that a *Ramanujan graph* is a d-regular graph G with $\lambda_2(G) \leq 2\sqrt{d-1}$; explicit constructions of such graphs were given in [LPS88, Mar88]. Summing up the above, we have:

Lemma 4.2 *The incidence matrix of any d-regular Ramanujan graph G on n vertices is an $(r, d, d(1-r/n)-2\sqrt{d-1})$-expander for any parameter $r > 0$.*

4.2 Tseitin tautologies: Boolean version

A Tseitin tautology is an unsatisfiable CNF capturing the basic combinatorial principle that for every graph, the sum of degrees of all vertices is even. These tautologies were originally used by Tseitin [T68] to present the first superpolynomial lower bounds on refutation size for a certain restricted form of Resolution (regular resolution).

In the sequence of works [G98, BGIP99, BI99] their authors studied the hardness of Tseitin tautologies for Polynomial Calculus. This research was essentially dependent on the fact that the tautologies can be written in the form of binomial ideals. Then the arguments proposed in [BGIP99] (and simplified in [BI99]) show that any PC-refutation of Tseitin tautologies has degree $\Omega(n)$.

[BGIP99] generalized Tseitin tautologies to the case when each vertex in the graph contains MOD_p function and used them to lower bound the refutation degree of the counting principle $Count_p$. Their definition, stated informally in terms of a flow on a graph, says the following: each directed edge e has the corresponding variable x_e which ranges over $\{0, ..., p-1\}$; the intuitive meaning of x_e is the value that flows along the edge e. The mod_p Tseitin principle says that the sum of flows in all vertices is equal to 0 mod p.

This definition is a natural generalization of the usual mod_2 Tseitin tautologies. [BGIP99] proved an $\Omega(n)$ lower bound on the refutation degree of these tautologies in the version of Polynomial Calculus in which the relations $x_i^2 - x_i$ (hardwired in our definition of $S_n(\mathbb{F})$) are weakened to $x_i^p - x_i$. They also observed that a Boolean version can be obtained by repeating every edge of the underlying graph p times. We would like to propose another Boolean version which is more straightforward and does not involve any encodings.

In our variant the variable x_e written on the directed edge e can have only Boolean values 0 and 1. There are two different constants F_0 and F_1 from $\{0, \ldots, p-1\}$ which define the amount of flow along e when x_e is equal to 0 and 1 respectively. One can easily see (by applying an affine transformation) that the exact choice of constants is not essential; for definiteness we set $F_0 := 0,\ F_1 := 1$.

Definition 4.3 (mod_p **Tseitin Formulas)** Let G be a finite oriented graph and $\sigma : V(G) \to \{0, ..., p-1\}$ be an arbitrary function. Assign a distinct Boolean variable x_e to each directed edge $e \in E(G)$. For $v \in V(G)$ denote by $MOD_p(G, \sigma, v)$ the following Boolean predicate:

$$\sum_{\{w \mid <w,v> \in E\}} x_{<w,v>} - \sum_{\{w \mid <v,w> \in E\}} x_{<v,w>} = \sigma(v) \bmod p.$$

The mod_p *Tseitin formula* of G and σ is defined as

$$T_p(G, \sigma) \stackrel{\text{def}}{=} \bigwedge_{v \in V(G)} \{MOD_p(G, \sigma, v)\}.$$

It is easy to see that $T_2(G, \sigma)$ coincides with ordinary Tseitin tautologies. We prove that for graphs G with sufficiently large edge-expansion $T_p(G, \sigma)$ requires large refutation degree in fields $\mathbb{F}$ with char $\mathbb{F} \neq p$.

Theorem 4.4 *The Boolean function in d variables which outputs 1 on $\alpha_1, \ldots, \alpha_d$ if and only if $\sum_{j=1}^d \epsilon_j \alpha_j \equiv \sigma \bmod p$, where $\epsilon_j \in \{\pm 1\}$ and $\sigma \in \{0, \ldots, p-1\}$ are arbitrary, is $\lfloor \frac{d}{4(p-1)^2} \rfloor$-immune over any field $\mathbb{F}$ with* char $\mathbb{F} \neq p$.

Proof. We can assume w.l.o.g. $\epsilon_1 = \epsilon_2 = \ldots = \epsilon_{d_1} = 1$, $\epsilon_{d_1+1} = \ldots = \epsilon_d = -1$ and $d_1 \geq d/2$. Let $\ell \stackrel{\text{def}}{=} \lfloor \frac{d_1}{(p-1)} \rfloor \geq \lfloor \frac{d}{2(p-1)} \rfloor$, and let $MOD_p^k(x_1, ..., x_{\ell(p-1)})$ be the Boolean function

$$\sum_{j=1}^{l(p-1)} x_j = k \bmod p.$$

Assume that a polynomial f is a non-trivial corollary of the Boolean function $\sum_{j=1}^d \epsilon_j x_j \equiv \sigma \bmod p$ (i.e., for any $\alpha \in \{0,1\}^d$, $\sum_{j=1}^d \epsilon_j \alpha_j \equiv \sigma \bmod p \Rightarrow f(\alpha) = 0$) with $\deg(f) < \lfloor \frac{d}{4(p-1)^2} \rfloor$. Then we can restrict the variables $x_{\ell(p-1)+1}, \ldots, x_d$ so that f remains non-trivial under this restriction and gets transformed into a corollary g of $MOD_p^k(x_1, \ldots, x_{\ell(p-1)})$ for some k.

Choose any Boolean vector $\bar{\alpha}$ such that $g(\bar{\alpha}) \neq 0$. W.l.o.g. assume that $\bar{\alpha}$ is monotonely decreasing on each cluster $x_{j(p-1)+1}, x_{j(p-1)+2}, ..., x_{j(p-1)+(p-1)}$ (i.e., ones are followed by zeros). We describe another algebra in which MOD_p^k becomes binomial (cf. [BGIP99]). Let us extend our field $\mathbb{F}$ to $\mathbb{F}'$ so that it contains a primitive p-th root of unity ξ. Consider the algebra $A_\ell(\mathbb{F}') = \mathbb{F}'[z_1, \ldots, z_\ell]/Span(z_1^p - 1, \ldots, z_\ell^p - 1)$. The elements f of $A_\ell(\mathbb{F}')$ naturally correspond to $\mathbb{F}'$-valued functions $\hat{f}$ on $\mathbb{F}_p^\ell$:

$$\hat{f}(i_1, ..., i_\ell) \stackrel{\text{def}}{=} f(\xi^{i_1}, ..., \xi^{i_\ell}).$$

Let us introduce the homomorphism ρ from $S_{\ell(p-1)}(\mathbb{F})$ to $A_\ell(\mathbb{F}')$ given by $x_{(j-1)(p-1)+i} \mapsto \phi_i(z_j)$, where $i \in [1, \dots, p-1]$ and $\phi_i(z)$ is the unique polynomial of degree $\leq p-1$ such that

$$\phi_i(\xi^t) = \begin{cases} 0 \text{ if } 0 \leq t \leq i-1 \\ 1 \text{ if } i \leq t \leq p-1. \end{cases} \tag{11}$$

The definition of ρ is fair since $\phi_i(z)^2 = \phi_i(z)$ in $A_\ell(\mathbb{F}')$.

Let us now look more closely at the function which corresponds to $\rho(MOD_p^k)$. Notice that the set $\{\phi_1(\xi^t), \dots, \phi_{p-1}(\xi^t)\}$ contains exactly t ones, therefore $\rho(MOD_p^k)(\xi^{t_1}, ..., \xi^{t_\ell}) = 0$ iff $t_1 + t_2 + ... + t_\ell = k \bmod p$. Hence, the binomial $\prod_{i=1}^{\ell} z_i - \xi^k$ has the same set of roots as $\rho(MOD_p^k)$.

Recall that we are given a non-trivial corollary g of MOD_p^k with $\deg(g) < \lfloor \frac{d}{4(p-1)^2} \rfloor$. Clearly, $\rho(g)$ is a corollary of $\rho(MOD_p^k)$ and $\deg(\rho(g)) \leq (p-1)\deg(g) < \lfloor \frac{d}{4(p-1)} \rfloor \leq \ell/2$. Also, it is easy to see that since $g(\alpha) \neq 0$ and α is monotone on each cluster $[x_{j(p-1)+1}, \dots, x_{j(p-1)+(p-1)}]$, $\rho(g)$ is non-zero in $A_l(\mathbb{F}')$.

Thus $\rho(g)$ is a non-trivial corollary of $\prod_{i=1}^{\ell} z_i - \xi^k$ and we have reduced our problem to the binomial case. The following lemma can be easily proved by the binomial technics of [BGIP99]:

Lemma 4.5 ([BGIP99]) *The polynomial $\prod_{i=1}^{\ell} z_i - \xi^k$ has no semantic corollaries in $A_\ell(\mathbb{F}')$ of degree less than $\ell/2$.*

Theorem 4.4 is proved.■

If we now apply Theorem 3.8 and Lemma 4.2 we get

Corollary 4.6 *For any fixed prime p there exists a constant $d_0 = d_0(p)$ such that the following holds. If $d \geq d_0$, G is a d-regular Ramanujan graph on n vertices (augmented with an arbitrary orientation of its edges), and* char $\mathbb{F} \neq p$, *then for every function σ every PC refutation of $T_p(G, \sigma)$ over $\mathbb{F}$ has degree $\Omega(dn)$.*

4.3 Random k-CNF in characteristic 2

An interesting test for a propositional proof system is how effective it behaves on the random input.

Definition 4.7 (Random k-CNF's) Let $\mathcal{F} \sim \mathcal{F}_k^{n,\Delta}$ denote that $\mathcal{F}$ is a random k-CNF formula on n variables and $\Delta \cdot n$ clauses, chosen by picking $\Delta \cdot n$ clauses independently and at random from the set of all $\binom{n}{k} \cdot 2^k$ clauses, with repetitions. Δ is called the *clause density.*

[CS88] showed that the random 3-CNF with n variables and $\Delta \cdot n$ clauses requires exponential refutation in Resolution, for an arbitrary constant Δ. [BI99] proved that the random 3-CNF requires Polynomial Calculus refutation of degree $\Omega(n)$ over any field $\mathbb{F}$ with char $\mathbb{F} \neq 2$, provided $\Delta = \Delta(n)$ is small enough. They used binomial technics proposed in [BGIP99] and the fact that the random CNF has good expansion properties proved in [CS88]. [BI99] conjectured that the same lower bound on the degree holds for 3-CNF's over the fields $\mathbb{F}$ with char $\mathbb{F} = 2$ as well. We give a positive answer to their conjecture.

Using Theorem 3.13 and Lemma 4.1 with $c = 1/\ln(\Delta+2)$ we immediately get the following

Corollary 4.8 *Let $\mathcal{F} \sim \mathcal{F}_k^{n,\Delta}$, where $k \geq 3$ is a fixed integer and $\Delta = \Delta(n)$ is an arbitrary parameter satisfying $\Delta \leq o\left(n^{(k-2)/2}\right)$. Then every Polynomial Calculus refutation of $\mathcal{F}$ over an arbitrary field $\mathbb{F}$ has degree $\Omega\left(\frac{n}{\Delta^{2/(k-2)} \cdot \log \Delta}\right)$ with probability $1 - o(1)$.*

4.4 Collapsable functions and flow tautologies

In this section we define a wide class of *collapsable* functions and prove that they have strong immunity. Then we introduce the analog of Tseitin tautologies in characteristic zero, in which each vertex contains a linear inequality over $\mathbb{R}$. The principle says that the flow can not be positive in all vertices of the graph. We call this family *flow tautologies.*

Definition 4.9 A Boolean function f is *ℓ-collapsable* iff for any subset of variables $S \subseteq \{x_1, ..., x_n\}$ with $|S| < \ell$ there exists a restriction ρ which leaves variables from S unassigned and such that $f|_\rho = 1$. A polynomial is *ℓ-collapsable* iff the characteristic function of the set of its roots in $\{0,1\}^n$ is ℓ-collapsable.

In other words, a polynomial $f \in S_n(\mathbb{F})$ is ℓ-collapsable iff for any choice of $n - \ell + 1$ variables we can satisfy it (make equal to 0) by some restriction of these variables to 0 and 1. It turns out that collapsable polynomials have strong immunity.

Theorem 4.10 *Every ℓ-collapsable polynomial f is ℓ-immune.*

Proof. Assume that $f \models g$ and $\deg(g) < \ell$. Let us choose any term t in g of maximal possible degree. Let $S \stackrel{\text{def}}{=} Vars(t)$. By the definition of ℓ-collapsable polynomial, there exists a restriction ρ which sends f (and hence g) to 0 and does not touch t. But $g|_\rho$ still contains t and hence is non-zero. This contradiction proves Theorem 4.10.$\blacksquare$

One good example of collapsable functions is made by threshold functions $\sum_{i=1}^n x_i > k$. In particular, the majority function MAJ_n defined by the predicate $\sum_{i=1}^n x_i > n/2$ is $n/2$-collapsable. To see that, assume that a subset of variables S with $|S| < n/2$ is given. Assign the rest of variables to 1, it will satisfy the function.

Now we are ready to define the analog of Tseitin principle in the characteristics 0. Recall that in the case of mod_p Tseitin tautologies we have an oriented graph G with Boolean variables corresponding to its edges, and the axioms in each vertex v saying that its flow is equal to $\sigma(v) \bmod p$. If instead of fixing the flow mod p we demand that it is positive in each vertex, we get *flow tautologies*.

Definition 4.11 (Flow tautologies) Let G be a finite oriented graph. Assign a distinct Boolean variable x_e to each directed edge $e \in E(G)$. For $v \in V(G)$ denote by $PosFlow(G, v)$ the following Boolean predicate:

$$\sum_{\{w \mid <w,v> \in E\}} (1 - 2x_{<w,v>}) > \sum_{\{w \mid <v,w> \in E\}} (1 - 2x_{<v,w>}).$$

The *Flow tautology* of G is defined as (the negation of)

$$Fl(G) \stackrel{\text{def}}{=} \bigwedge_{v \in V(G)} PosFlow(G, v).$$

It is easy to see that, up to negating some variables, $PosFlow(G, v)$ coincides with the majority function in $d(v)$ variables and hence is $d(v)/2$-collapsable. Thus by Theorem 4.10 and Lemma 4.2 we have

Corollary 4.12 *If G is a d-regular Ramanujan graph on n vertices with $d \geq 255$ (augmented with an arbitrary orientation of its edges) then every PC refutation of $Fl(G)$ over an arbitrary field has degree $\Omega(dn)$.*

4.5 Relation between robustness and immunity

In this section we discuss the relation between the hardness condition considered in [ABRW00] and that of our paper. We show that every $(s-k)$-robust function (see the definition below) is also $\omega(1)$-immune in the fields of characteristic 0 ($k = const,\ s \to \infty$). This estimate is extremely week but still even sufficiently large constant immunity gives non-trivial lower bounds on the degree of PC refutations.

Definition 4.13 ([ABRW00]) *A Boolean function f is ℓ-*robust *if every restriction ρ such that $f|_\rho = const$, satisfies $|\rho| \geq \ell$.*

This notion is clearly invariant under negations. In order to compare it with non-invariant immunity let us call the function f *ℓ-semi-robust* if $f|_\rho \not\equiv 0$ implies $|\rho| \geq \ell$. Thus, a Boolean function is ℓ-robust iff it is ℓ-semi-robust and so is its negation.

According to the convention made in Section 2 (cf. Definition 2.3), we say that a polynomial f is *ℓ-semi-robust* if for any restriction ρ with $|\rho| < \ell$, $f|_\rho$ has at least one $(0-1)$ root. Every ℓ-immune polynomial is ℓ-semi-robust by Lemma 2.4, thus the notion of immunity is stronger. As the example of the MOD_p function shows, over finite fields immunity can be a much stronger requirement than (semi-)robustness.

In the opposite direction the following estimate holds:

Theorem 4.14 *Assume that* $\mathrm{char}\,\mathbb{F} = 0$, *$k$ is a constant. Then every $(s-k)$-semi-robust polynomial f in s variables has immunity $\omega(1)$ when $s \to \infty$.*

Proof.

Replacing f by the multi-linear polynomial f' given by its values on $\{0,1\}^s$ as

$$f'(a) \stackrel{\mathrm{def}}{=} \begin{cases} 0 \text{ if } f(a) = 0 \\ 1 \text{ if } f(a) \neq 0 \end{cases}$$

(which does not affect either immunity or semi-robustness), we can assume w.l.o.g. that f has integer coefficients.

Next, we reduce our field $\mathbb{F}$ with $\mathrm{char}\,\mathbb{F} = 0$ to $\mathbb{Q}$ using the standard trick which says that if the linear system over integers has a solution, then it has a rational solution.

Lemma 4.15 *Assume that f is a polynomial with integer coefficients, $\mathbb{F}$ is a field with* char $\mathbb{F} = 0$ *and f has a semantic corollary of degree d. Then f has also a semantic corollary of degree d with rational coefficients.*

Proof. It is proved in [BIKPRS96] that g is a corollary of f iff there exists a polynomial $f' \in S_s(\mathbb{F})$ s.t. $g = f' \cdot f$.

Introduce $\mathbb{F}$-valued variables g_t and f'_t where $t \in T_s$ corresponding to the coefficients of g and f'. The condition $g = f' \cdot f$ is equivalent to a certain system of linear equations over g_t, f'_t with integer coefficients. Let us add the conditions $g_t = 0$ for all terms t with $\deg(t) > d$ and $g_t \neq 0$ for an arbitrary term t appearing in g.

We defined the system of linear equations and inequalities with integer coefficients which has a solution in $\mathbb{F}$. It follows from the basics of algebra that it also has a solution over rationals. Thus f has a non-trivial corollary of degree $\deg(g)$ with rational coefficients.∎

Now assume that $\mathbb{F} = \mathbb{Q}$. We will need the following classical definition of Ramsey numbers.

Definition 4.16 *The* Ramsey number *$R_k(l_1, \ldots, l_r)$ is the smallest n such that if all k-subsets of $[n]$ are coloured in r colours, then there exists a colour ν and an ℓ_ν-subset of $[n]$ all of whose k-subsets have colour ν.*

Let $N_k(d)$ be the smallest s such that for every non-zero polynomial $g \in \mathbb{Q}[x_1, \ldots, x_s]$ with $\deg(g) \leq d$ there is a restriction ρ such that $|\rho| \leq s - k - 1$ and $g|_\rho$ does not have $(0-1)$ roots. Thus, this is the inverse function to what we are studying: namely, if g is a semantic corollary of a $(s-k)$-semi-robust polynomial f then $N_k(\deg(g)) > s$. N_k is monotone and we need to prove that $\forall d\ N_k(d) < \infty$. Clearly, $N_k(0) = k + 1$. Our result follows from the following recursive bound:

$$N_k(d) \leq R_d(2^{k+1}d, 2^{k+1}d, N_k(d-1)).$$

In order to see this, let $s \geq R_d(2^{k+1}d, 2^{k+1}d, N_k(d-1))$ and suppose that $\deg(g) \leq d$. Colour all d-subsets of $[s]$ in three colours, $+, -, 0$, according to the sign of the coefficient in front of the corresponding monomial in g. Let us denote $m = 2^{k+1}d$. According to the definition of Ramsey numbers, we have two cases.

Case 1. *For some m variables, say, $x_1, \ldots, x_m$, g contains all monomials x_I with $I \in [m]^d$, and it contains them with the same sign.* Consider $k+1$ variables $x_{m+1}, x_{m+2}, ..., x_{m+k+1}$. If there exists a restriction ρ to all variables except $x_{m+1}, x_{m+2}, ..., x_{m+k+1}$ s.t. $g|_\rho$ does not have $(0-1)$ roots, then our recursive bound follows. Otherwise for any assignment of $Vars(g) \setminus \{x_{m+1}, x_{m+2}, ..., x_{m+k+1}\}$ there exist values for $x_{m+1}, x_{m+2}, ..., x_{m+k+1}$ which map g to 0. In other words, at least one of the functions

$$g|_{(x_{m+1}=\epsilon_1, \ldots, x_{m+k+1}=\epsilon_{k+1})}$$

is equal to 0 on the chosen assignment or, equivalently,

$$\prod_{\bar{\epsilon} \in \{0,1\}^{k+1}} g|_{(x_{m+1}=\epsilon_1, \ldots, x_{m+k+1}=\epsilon_{k+1})} = 0 \text{ in } S_s(\mathbb{Q}).$$

This, however, is impossible since all monomials x_I with $I \in [m]^d$ still appear in all $g|_{(x_{m+1}=\epsilon_1, \ldots, x_{m+k+1}=\epsilon_{k+1})}$ with the same sign, and therefore the monomial $\prod_{i=1}^m x_i$ has a non-zero coefficient in this product.

Case 2. *For some $N_k(d-1)$ varaiables, say, $x_1, \ldots, x_{N_k(d-1)}$, g contains no monomial x_I with $I \in [N_k(d-1)]^d$.* In this case we simply apply any restriction to the remaining variables that does not kill g completely (which reduces the degree), and then apply the inductive assumption.

Theorem 4.14 is proved.■

Theorem 4.17 *For any fixed integers k, α there exists an integer s_0 s.t. for any $s \geq s_0$, $(r, s, s-\alpha)$-expander A and $f_1, \ldots, f_m$ $(s-k)$-semi-robust polynomials over an arbitrary field of characteristics 0 with $Vars(f_i) \subseteq X_i(A)$, any PC refutation of the system $f_1 = \ldots = f_m = 0$ has degree $\Omega(r)$.*

This theorem follows from Theorems 3.8 and 4.14. Using the construction of random expanders from Lemma 4.1 we can build various families of hard tautologies based on $(s-k)$-semi-robust functions.

5 Open questions

The most interesting of remaining questions is what can be said about the system (4) in the case of small expansion factor $c > 0$? Can one show its hardness provided that f_i are sufficiently immune, otherwords is it possible to combine our Theorems 3.8, 3.13 into one general statement?

Does there exist a relation between robustness and immunity stronger than that of Theorem 4.14?

References

[ABRW00] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Pseudorandom generators in propositional complexity. Technical Report TR00-023, Electronic Colloquium on Computational Complexity, ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/2000/TR00-023/index.html, 2000. To appear in *Proceedings of the* 41*st IEEE FOCS*.

[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.

[BIKPP94] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings of the* 35*th IEEE FOCS*, 1994, 794–806. Journal version to appear in *Proc. of the London Math. Soc.*

[BKPS98] P. Beame, R. Karp, T. Pitassi, and M. Saks. On the complexity of unsatisfiability of random k-cnf formulas. In *Proceedings of the* 30*th ACM Symposium on Theory of Computing*, pages 561–571, 1998.

[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.

[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.

[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.

[BIKPRS96] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity* **6**(3) (1996/1997), 256–298.

[BCS78] F. C. Bussemaker, D. M. Cvetković, and J. J. Seidel. Graphs related to exceptional root systems. In A. Hajnal and V. T. Sós, editors, *Combinatorics, Coll. Math. Soc. J. Bolyai, Vol. 18*, pages 185–191. North-Holland, Amsterdam, 1978.

[CS88] V. Chvátal, E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35 (4):759-768, October 1988.

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

[G98] D. Grigoriev. Nullstellensatz lower bounds for Tseitin tautologies. In *Proceedings of the* 39*th IEEE FOCS*, 1998, 648–652.

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

[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.

[K97] J. Krajíček. On the degree of ideal membership proofs from uniform families of polynomials over a finite field. Manuscript, 1997.

[LPS88] A. Lubotsky, R. Philips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988.

[Mar88] G. A. Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators. *Problemy Peredachi Informatsii (in Russian)*, 24:51–60, 1988. English translation in *Problems of Information Transmission, Vol. 24, pages 39-46*.

[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.

[T68] G. Tseitin. On the Complexity of Derivation in Propositional Calculus. In *Studies in Constructive Mathematics and Mathematical Logic*, Part 2. Consultants Bureau, New-York-London, 1968, pp. 115-125.