Electronic Colloquium on Computational Complexity, Report No. 12 (2020)

(Semi)Algebraic Proofs over $\{\pm 1\}$ Variables

Dmitry Sokolov*

St. Petersburg State University
St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences

February 14, 2020

Abstract

One of the major open problems in proof complexity is to prove lower bounds on $\mathbf{AC}_0[p]$-Frege proof systems. As a step toward this goal Impagliazzo, Mouli and Pitassi in a recent paper suggested to prove lower bounds on the size for Polynomial Calculus over the $\{\pm 1\}$ basis. In this paper we show a technique for proving such lower bounds and moreover we also give lower bounds on the size for Sum-of-Squares over the $\{\pm 1\}$ basis.

We show lower bounds on random Δ-CNF formulas and formulas composed with a gadget. As a byproduct, we establish a separation between Polynomial Calculus and Sum-of-Squares over the $\{\pm 1\}$ basis by proving a lower bound on the Pigeonhole Principle.

1 Introduction

The main task of proof complexity is to quantify the size of the smallest proof required to prove that some given formula is unsatisfiable. Establishing superpolynomial lower bounds on the sizes in all proof systems will imply that $\mathbf{NP} \neq \mathbf{coNP}$.

In some situations if we can prove lower bound on some model of computations we can translate it into a lower bound for a proof system based on this model. The major success in such lower bounds was done by Ajtai for $\mathbf{AC}_0$-Frege proof system [Ajt94]. For a stronger proof system $\mathbf{AC}_0[p]$-Frege we also can try to translate lower bounds from $\mathbf{AC}_0[p]$ circuits, that were proved by Razborov and Smolensky [Raz87; Smo87]. But despite on well-developed techniques for $\mathbf{AC}_0[p]$ circuits we still do not know how to apply algebraic reasoning used by Razborov and Smolensky for proof systems. To deal with this approach it seems natural to study algebraic and semialgebraic proof systems: Nullstellensatz [Bea+94], Polynomial Calculus (PCR) [CEI96] and Sum-of-Squares (SOS) [Gri01].

Mod_p gates and limitations of current techniques. Despite the success in proving lower bounds on Polynomial Calculus and Sum-of-Squares the lower bounds we still do not know how to transfer lower bounds from these systems to $\mathbf{AC}_0[p]$-Frege. If we consider standard $\{0, 1\}$ basis then in these systems there is no efficient way to simulate Mod_p gates. In case of Sum-of-Squares there is a canonical hard example: Tseitin formulas (that are particular case of linear systems modulo 2) [Gri01]. In Polynomial Calculus over a proper field we can simulate limited number of Mod_p gates (one per line), that is enough solve Tseitin formulas but not enough to

*This work was done while at Lund University and the University of Copenhagen supported by the Knut and Alice Wallenberg grant KAW 2016.0433. sokolov.dmt@gmail.com

ISSN 1433-8092

say that we *can simulate* Mod_p gates in this proof system. This statement can be illustrated by current technique for proving lower bounds: we deal with monomials independently.

If we consider proof systems that are restriction of $\mathbf{AC}_0[p]$-Frege that can simulate nontrivial number of Mod_p gates per line [Bus+97; Kra97; GK18; RT08] then current techniques do not give us lower bounds on the size of proofs. Even for Resolution with parity [IS19] any non-trivial lower bound (without restrictions on the structure of proofs) on CNF formulas remains open.

The most popular approach for proving lower bounds is a "restriction technique". The main idea is the following: we hit a proof by some restriction in order to obtain a "well-structured" proof. In particular, for algebraic proof systems by using this approach we can reduce a question about the size of proof to a question about a degree of the proof:

- size-degree tradeoff [CEI96; IPS99; AH19];
- pure random restriction, for example [Ale+04].

For algebraic proof systems it is the only approach at current moment for size lower bounds, but Mod_p gates are "immune" to the restrictions. This approach will most likely not work for proof systems that can simulate Mod_p gates.

$\{\pm 1\}$ basis. One important benefit of the $\{\pm 1\}$ basis is that we can represent parity as a monomial: $\mathsf{Parity}(x_1, \dots, x_n) \coloneqq \prod_{i=1}^{n} x_i$ hence we can encode multiple parity gates in a single line in the proof. In this representation Grigoriev [Gri98] shows Nullstellansatz proof of polynomial size on Tseitin formulas as well as degree lower bound. Lower bound strategy was generalized by Grigoriev [Gri01] to the Positivestellensatz and by Buss, Grigoriev, Impagliazzo and Pitassi [Bus+01] to the Polynomial Calculus. These lower and upper bounds explain the power of the $\{\pm 1\}$ basis as well as weak points of current techniques for proving lower bounds.

The question about size lower bound in the $\{\pm 1\}$ basis was explicitly stated by Impagliazzo, Mouli and Pitassi [IMP19] as a step to lower bounds for $\mathbf{AC}_0[p]$-Frege.

1.1 Our results

In this work we give an answer to the question raised in [IMP19] by presenting a technique for proving size lower bounds on Sum-of-Squares and Polynomial Calculus over the $\{\pm 1\}$ basis. Denote these systems by $\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}_{\{\pm 1\}}$ (we omit index if we can use any basis). We also use notation $\mathrm{PCR}^{\mathbb{F}}$ to specify a field.

The first result is a lower bound on the size of $\mathrm{SOS}_{\{\pm 1\}}$-proofs.

Theorem 1.1 (Informal)**.** Let $\mathcal{F}$ be a polynomial system of degree d_0 on n variables. There is a function g on a constant number of variables such that if d is the minimal degree of an SOS-proof of $\mathcal{F}$ then any $\mathrm{SOS}_{\{\pm 1\}}$-proof of $\mathcal{F} \circ g$ has size $\exp\left[\Omega\left(\frac{(d-d_0)^2}{n}\right)\right]$.

We show by analogy with [Ber18] that a small $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proof can be transformed into a small $\mathrm{SOS}_{\{\pm 1\}}$-proof. Hence Theorem 1.1 also gives us a lower bound for $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proofs. This result shows the difference between the considered proof systems ($\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$) and $\mathbf{AC}_0[p]$-Frege since in the last system the size of the proofs should not depend on the small gadgets substitution.

The second lower bound works for $\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ over any field $\mathbb{F}$. And it is the canonical example of hard formulas.

Theorem 1.2 (Informal)**.** If $\Delta > 11$ is a constant and φ is a random Δ-CNF formula on m clauses where $m = O(n)$ then whp any $\mathrm{SOS}_{\{\pm 1\}}$ of $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of φ has size $\exp(\Omega(n))$.

In the last part we show a lower bound on $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proofs over any field $\mathbb{F}$ on formulas that encode the Pigeonhole Principle. Together with the upper bound on SOS-proofs (independent of basis) from [GHP02] we show an exponential separation between $\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ proof systems. Moreover our proof works for a strengthening of the Pigeonhole Principle, so called Graph Pigeonhole Principle.

Theorem 1.3 (Informal)**.** Let G be an $(r, \Delta, 4)$-boundary expander. Then any $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathsf{G\text{-}PHP}^{n+1}_n$ has size $\exp(\Omega(n))$.

1.2 Related Work

Various restrictions on $\mathbf{AC}_0$-Frege were studied by Krajíček [Kra97]. In this paper Krajíček showed exponential lower bounds on tree-like versions of proof system that can use one Mod_p gate. Generalizations of these systems were considered by Garlík and Kołodziejczyk [GK18].

Raz and Tzameret [RT08] introduced Resolution with linear functions over reals. Itsykson and Sokolov [IS19] considered similar proof system over $\mathbb{F}_2$. On both proof systems lower bounds on CNF formulas are still open. Partial progress in this direction was achieved by Part and Tzameret [PT18].

Pitassi [Pit96; Pit98] introduced strong generalization of Polynomial Calculus that operates directly with formulas. Groshow and Pitassi [GP18] consider even more powerful version, so called Ideal Proof System. On the one hand these proof systems are so strong that lower bounds on it will imply separation between **VP** and **VNP**, but on the other hand we do not have efficient deterministic verification algorithms for proofs hence these structures are not proof systems in terms of Cook–Reckhow [CR79] definition.

Grigoriev and Hirsch [GH03] considered extensions of algebraic systems that are still satisfy Cook–Reckhow definition. In this paper it was showed that even with small extensions these systems may be powerful enough to solve various formulas that are hard for $\mathbf{AC}_0$-Frege. "Constant depth" extensions was considered by Impagliazzo, Mouli and Pitassi [IMP19]. This systems are powerful enough to quasi-polynomially simulate $\mathbf{TC}_0$-Frege. It is still an open problem to prove any lower bound for these systems.

1.3 Technique

Let start with the $\{0, 1\}$ basis. We describe the basic idea of an algorithm that transforms proofs of small size into proofs of small degree. Together with a degree lower bound this algorithm gives a proof of size lower bound.

1. If we have a small proof of a polynomial system $\mathcal{F}$ then there are not so many terms of big degree.

2. Pick a literal x that appears in a significant fraction of terms of big degree.

3. Since 0 is a feasible assignment, we can assign x to 0 in the whole proof and thus banish all terms that contain x.

4. After this assignment, the resulting proof is still a proof of $\mathcal{F} \restriction (x = 0)$.

5. After some number of steps we banished all terms of big degree and it remains to show that after these partial assignments the system is still hard in terms of degree.

We will try to implement similar strategy for the $\{\pm 1\}$ basis. As mentioned above in some cases we have small proofs of big degree, which means that degree is not enough to prove lower bounds on size. This phenomena is not the only difference, in particular, in Polynomial Calculus, using the axiom $x^2 - 1$, which is the analogue of the "boolean" axiom for the $\{0, 1\}$ variables, we can invert multiplication by the x variable.

$$\cfrac{\cfrac{xp}{x^2p} \qquad \cfrac{x^2 - 1}{x^2p - p}}{p}$$

This derivation says that if a variable x is contained in all terms of a proof line, then we can erase it. This shows that degree is not really a representative measure. The crucial idea is that instead of the usual degree we consider the **quadratic representation** of the proof. In case of Polynomial Calculus we deal with the squares of the lines in the proof. The intuition behind it is that we want to measure the symmetric difference between monomials that appear in a single proof line.

The next problem that arises in the case of $\{\pm 1\}$ variables is that we do not have any assignment that removes terms from the proof. To solve this problem, we "force" an assignment that banishes a significant part of terms in the quadratic representation. The "forcing" operation uses different properties of formulas for different lower bounds.

1. **Symmetry.** For formulas with a gadget (Theorem 1.1), we consider two copies of the original proof with permuted variables. The symmetry of the formula then helps us to combine these copies into a new proof.

2. **Locality.** For random formulas and the Pigeonhole Principle (Theorems 1.2 and 1.3), we define a Split_x operation that depends on the considered proof system, but we can think of it as a linear combination of the original proof, hit by different partial assignment. We use locality to show that the result of the Split_x operation is a proof of a "locally damaged" version of $\mathcal{F}$.

In order to implement the last part of our strategy we have to show that the degree of the quadratic representation is related to the degree of the proof and keep the system $\mathcal{F}$ hard in terms of degree during the whole process.

1. For formulas with gadgets we use a result from [AH19] that states that we can carefully choose a partial assignment that does not decrease the degree of the proof.

2. For random formulas and the Pigeonhole Principle we use the iterative analogue of the **closure** operation on graphs, which seems to have originated in [AR03; Ale+04]. By using ideas of this operation we show that these formulas are "self-reducible": after some applications of the Split_x operation we have a proof of smaller instance of original formula.

1.4 Outline

The paper is organized as follows. In section 3 we give the definitions of the used proof systems and introduce the key notion of quadratic representation for Sum-of-Squares and Polynomial Calculus. In section 4 we prove lower bounds on polynomial systems composed with a gadget. In section 5 we show the lower bound on random Δ-CNF formulas, and in section 6 we prove lower bounds on the Pigeonhole Principle that give us a separation between $\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$.

2 Preliminaries

For the rest of the paper we fix some notation: $\mathcal{F} \coloneqq \{f_1 = 0, \dots, f_m = 0\}$ is a system of polynomial equations and $\mathcal{H} = \{h_1 \geq 0, \dots, h_s \geq 0\}$ is a system of polynomial inequalities over the set of variables $X \coloneqq \{x_1, \dots, x_n\}$.

Let $\mathbb{F}$ be a field. A **restriction** is a partial assignment to the variables that is a function $\rho : X \to X \cup \mathbb{F}$ such that the value of $\rho(x)$ is either x or a constant from $\mathbb{F}$. For a polynomial p, we denote by $p \restriction \rho$ the polynomial p in which any variable x is replaced by $\rho(x)$.

In the rest of the paper we assume that $\mathbb{F}$ is an arbitrary field. Wlog the characteristic of $\mathbb{F}$ is different from 2, as otherwise $1 = -1$ and the $\{\pm 1\}$ basis does not make any sense.

2.1 Composition with Gadgets

Suppose we have a multilinear system $(\mathcal{F}, \mathcal{H})$ and we want to compose it with a gadget. We only consider gadgets that satisfy some properties.

Definition 2.1. Let Z be either $\{\pm 1\}$ or $\{0, 1\}$. A symmetric function $g : Z^k \to Z$ is **compliant** iff:

1. g is not parity i.e. not $\prod_i x_i$ in the case of the $\{\pm 1\}$ basis;
2. for any $b \in Z$ there is an assignment $\beta \coloneqq (\beta_1 \beta_2 \dots \beta_k) \in Z^k$ such that $\beta_1 \neq \beta_2$ and $g(\beta) = b$.

Note that the second property holds for any pair of indices since g is symmetric. $\mathsf{MAJ}(z_1, z_2, z_3)$ is an example of a compliant function.

Remark 2.2. For our purposes (Theorem 1.1) we cannot use parity as a gadget. For Tseitin formulas we have degree lower bound [Bus+01; GV01]. But composition of Tseitin formula with parity is still a Tseitin formula and we have a short proof of it in all considered proof systems [Gri98].

We say that the system $(\mathcal{F}, \mathcal{H}) \circ g$ is the **composed version** of the system $(\mathcal{F}, \mathcal{H})$ with a gadget g, if it is the result of the following process: for each variable x_i introduce new variables $z_{i,1}, \dots, z_{i,k}$ and replace each occurrence of x_i in $(\mathcal{F}, \mathcal{H})$ by a multilinear polynomial encoding of the function g.

Proposition 2.3.

1. $(\mathcal{F}, \mathcal{H}) \circ g$ is a multilinear system.
2. If $p \in (\mathcal{F}, \mathcal{H}) \circ g$ and g is symmetric then for any i polynomial p is stable under any permutation of the $z_{i,\cdot}$ variables.

Proof. The first claim follows by multilinearity of $(\mathcal{F}, \mathcal{H})$ and multilinearity of the encoding of g.

For the second claim note that $p \coloneqq r \circ g$ for some $r \in (\mathcal{F}, \mathcal{H})$. Since g is the symmetric gadget, then it is unaffected by permutations of $z_{i,\cdot}$ variables. Hence $r \circ g$ is also unaffected by permutation of $z_{i,\cdot}$ variables. Due to uniqueness of multilinear representation of the functions polynomial p remains the same after such permutations. $\square$

Remark 2.4. Suppose that each polynomial in $(\mathcal{F}, \mathcal{H})$ depends only on a constant number of variables and the gadget g has constant size. Let $(\mathcal{F}', \mathcal{H}')$ and $(\mathcal{F}'', \mathcal{H}'')$ be two encodings of the system $(\mathcal{F}, \mathcal{H}) \circ g$, that means for each constraint $p \in (\mathcal{F}, \mathcal{H}) \circ g$ there are constraints $p' \in (\mathcal{F}', \mathcal{H}')$ and $p'' \in (\mathcal{F}'', \mathcal{H}'')$ with the same set of satisfing assignment, but maybe not the

the same type (equality or inequality). Then each polynomial $f'' \in \mathcal{F}''$ (or $h'' \in \mathcal{H}$) can be derived in SOS and $\mathrm{PCR}^{\mathbb{F}}$ (independent of basis) from $(\mathcal{F}', \mathcal{H}')$ in constant size.

Hence if start with a proper polynomial system $(\mathcal{F}, \mathcal{H})$ for which we have linear degree lower bound (for example polynomial encoding of Tseitin formula) the results from section 4 can be used for any encoding of $(\mathcal{F}, \mathcal{H}) \circ g$.

2.2 Encodings of CNF formulas

We consider semialgebraic proof systems and thus we need to encode formulas as polynomials. There are two popular encodings: the CNF (aka multiplicative) and the Cutting Planes (CP, aka additive) encodings. In both encodings we encode clauses separately.

CNF $\bigvee_i x_i^{a_i} \Leftrightarrow \prod_i x_i^{a_i} = 0$ over $\{0,1\}$ or $\prod_i \frac{(1+(-1)^{1-a_i} x_i)}{2} = 0$ over $\{\pm 1\}$.

CP $\bigvee_i x_i^{a_i} \Leftrightarrow \sum_i x_i^{a_i} - 1 \geq 0$ over $\{0,1\}$ or $-\sum_i((-1)^{1-a_i} x_i - 1) - 1 \geq 0$ over $\{\pm 1\}$.

In this paper we deal with the CNF encoding. A very useful property of this encoding is that for any variable there is an assignment that sets the whole polynomial to zero.

Remark 2.5. As in the previous case if we deal with formulas of constant width then for each clause we can derive one encoding from the other in constant degree (and constant size). Hence results from sections 5 and 6 hold for both encodings.

3 Proof Systems

Let x be a variable and $\bar{x}$ its negation.

1. The **range axiom** for a variable x is one of the following polynomials:
   - $x^2 - x$ for the $\{0,1\}$ basis;
   - $x^2 - 1$ for the $\{\pm 1\}$ basis.
2. The **complementary axiom** for a variable x is a polynomial:
   - $x + \bar{x} - 1$ for the $\{0,1\}$ basis;
   - $x + \bar{x}$ for the $\{\pm 1\}$ basis.

We will use proof systems with an index that represents the basis if it is important to specify it, for example: $\mathrm{SOS}_{\{\pm 1\}}, \mathrm{PCR}^{\mathbb{F}}_{\{0,1\}}$. We omit the index to stress the fact that the current statement is independent of the basis. In particular we can switch from the $\{0,1\}$ basis to the $\{\pm 1\}$ basis via affine shift. Hence if we talk about the degree of a proof, we typically do not care about basis (see Lemma 3.7).

3.1 The Sum-of-Squares Proof System

Sum-of-Squares (SOS) is a semi-algebraic proof system. Formally, a Sum-of-Squares proof of $f > 0$ from $(\mathcal{F}, \mathcal{H})$ is a sequence of polynomials $(p_1, \ldots, p_a; r_1, \ldots, r_n; q_1, \ldots, q_b)$ such that:

$$\sum_{u=1}^{a} p_u f_u + \sum_{j=1}^{m} r_j R_j + \sum_{v=1}^{b} q_v^2 h_v = f$$

- R_j is a range axiom or a complementary axiom;
- $f_u \in \mathcal{F}$ and
- $h_v \in \mathcal{H} \cup \{1\}$.

Note that some polynomials $h \in \mathcal{H}$ may appear more than once in this sum. We do not want to charge for range axioms, so we assume that all operations are in $\mathbb{R}[X]\big/_I$, where I is the ideal that is generated by all range axioms. Since we care about the size in the $\{\pm 1\}$ basis, we assume that there are no negated variables (we can replace the variable $\bar{x}$ by $-x$ without increasing the size of the proof). Hence we can simplify the proof to:

$$\sum_{u=1}^{a} p_u f_u + \sum_{v=1}^{b} q_v^2 h_v = f,$$

where all polynomials assumed to be multilinear.

The **degree** of a proof is the maximum of the following two numbers: $\mathsf{deg}(p_u) + \mathsf{deg}(f_u), 2\mathsf{deg}(q_v) + \mathsf{deg}(h_v)$.

We need to be precise about the size and the degree measures. The **monomial size** of a polynomial p is $\mathsf{MSize}(p) :=$ number of monomials in p.

The **size** of a proof is:

$$\sum_{u=1}^{a} (\mathsf{MSize}(p_u) + \mathsf{MSize}(f_u)) + \sum_{v=1}^{b} \mathsf{MSize}(q_v) + \sum_{h \in \mathcal{H}} \mathsf{MSize}(h).$$

Here we count polynomials in H at most once.

To formulate the next property we need to consider another degree measure. The **reduced degree** of a proof is the maximum of the following numbers: $\mathsf{deg}(p_u), 2\mathsf{deg}(q_v)$.

The next lemma is a simplified version of Lemma 5 from [AH19] ($w := 1$, $c(u) := \mathsf{deg}(p_u)$, $c(v) := \mathsf{deg}(q_v)$).

Lemma 3.1 ([AH19])**.** For any variable $x \in X$. If the $\mathrm{SOS}_{\{0,1\}}$-reduced degrees of $(\mathcal{F}, \mathcal{H}) \restriction (x = 0)$ and $(\mathcal{F}, \mathcal{H}) \restriction (x = 1)$ are at most $2d$ then there is an $\mathrm{SOS}_{\{0,1\}}$-proof of $(\mathcal{F}, \mathcal{H})$ of reduced degree at most $2d + 2$.

Since the degree of any polynomial does not depends on basis the following corollary holds for any basis.

Corollary 3.2. If SOS-reduced degree of $(\mathcal{F}, \mathcal{H})$ is d then for any variable x there is an assignment α such that the SOS-reduced degree of $(\mathcal{F}, \mathcal{H}) \restriction (x = \alpha)$ is at least $d - 3$.

Proof. For contradiction we assume that for any assignment α there is an SOS-proof of $(\mathcal{F}, \mathcal{H}) \restriction (x = \alpha)$ with reduced degree $(d-4)$. By Lemma 3.1 there is a proof of $(\mathcal{F}, \mathcal{H})$ of reduced degree $(d - 1)$, which contradicts with the statement. $\square$

Quadratic representation. Let $\pi := (p_1, \ldots, p_a; q_1, \ldots, q_b)$ be a $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof. The **quadratic representation** of π is the sequence $(p_1, p_2, \ldots, p_a; q_1^2, \ldots, q_v^2)$ where squares are expanded without cancellations. For example, if $q_v := (xy - x - y)$ then $q_v^2 := (1 - y - x) - (y - 1 - xy) - (x - xy - 1)$ and we assume that it contains nine terms.

The **q-size** (quadratic size) of the proof is:

$$\sum_{u=1}^{a} \mathsf{MSize}(p_u) + \sum_{v=1}^{b} \mathsf{MSize}(q_v)^2$$

This definition of q-size is not usual.

1. We do not charge for the original polynomials. In terms of the Cook–Reckhow definition of proof system [CR79], this is not the right way to define size, since it is not clear whether proofs are checkable in polynomial time. But it will help us to simplify the computations in our proofs and makes our results only stronger.
2. Q-size is the monomial size of quadratic representation and quadratic representation is the crucial object for our proofs. Hence it is more useful to deal with the size of quadratic representation. Q-size is polynomially related to the usual size, the results hold for both measures up to a constant in the exponent.

See also the discussion about size measures in [AH19].

The following Lemma gives a transformation of $\mathrm{SOS}_{\{\pm 1\}}$-proof with low-degree quadratic representation into a proof of low degree, that is not straightforward since we deal with factor field and one can find a polynomial p such that $\mathsf{deg}(p^2) < \mathsf{deg}(p)$.

Lemma 3.3. Let π be an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H})$. If quadratic representation of π does not contain any term of degree greater than d then there is an SOS-proof π' of $(\mathcal{F}, \mathcal{H})$ of reduced degree $2d$.

Proof. Let $\pi := (p_1, \ldots, p_a; q_1, \ldots, q_b)$. Note that degree of all p_u is at most d.

Let $q_v := \sum\limits_i t_i$ and $q'_v := \sum\limits_i t_1 t_i$, where t_i are terms. Note that $(q'_v)^2 = (q_v)^2$ and moreover all terms $t_1 t_i$ are presented in the quadratic representation of q_v hence q'_v has degree at most d.

To conclude the proof note that $\pi' := (p_1, \ldots, p_a; q'_1, \ldots, q'_b)$ is a proof of $(\mathcal{F}, \mathcal{H})$. $\square$

3.2 Polynomial Calculus

The $\mathrm{PCR}^{\mathbb{F}}$ proof system is equipped with range and complementary axioms and has the following derivation rules:

- **linear combination:** $\frac{p \quad q}{\alpha p + \beta q}$ for any $\alpha, \beta \in \mathbb{F}, p, q \in \mathbb{F}[X]$;
- **multiplication:** $\frac{p}{xp}$ for any $p \in \mathbb{F}[X]$.

A polynomial f is **derivable** from a set of polynomials $f_1, \ldots, f_m$ (written $f_1, \ldots, f_k \vdash f$) if there is a sequence of polynomials such that each polynomial is either an axiom (an f_i, a range or a complementarity), or the conclusion of a derivation rule obtained from previously derived polynomials.

Definition 3.4. A **PCR proof** of a set of polynomials $f_1, \ldots, f_m$ is a derivation Π of the polynomial 1 from the polynomials $f_1, \ldots, f_m$.

Remark 3.5. Let say that an assignment is feasible if it satisfies all range axioms. Observe that by definition, $f_1, \ldots, f_m \vdash f$ is equivalent to saying that f is in the ideal generated by $f_1, \ldots, f_m$ along with all range and complementarity axioms. Intuitively, a $\mathrm{PCR}^{\mathbb{F}}$-proof is a certificate that the system $\mathcal{F}$ has no feasible solution. It turns out that the converse is also true: if a system of polynomial equations has no feasible solution, then 1 is in the ideal generated by the polynomials arising in the system together with the polynomials from the range and complementary axioms. In other words, the system is *sound* and *complete*.

As in case of SOS we do not want to charge for the usage of range axioms. So we assume that all operations are in ${}^{\mathbb{F}[X]}\!/_{I}$, where I is the ideal that is generated by all range axioms. Further, in case of the $\{\pm 1\}$ basis we assume that there is no negated variables since we can replace $\bar{x}$ by $-x$.

The **size** of a $\mathrm{PCR}^{\mathbb{F}}$-proof is the total number of non-zero monomials (counted with repetition) that appear in a derivation when all polynomials are expanded out as linear combinations of monomials. The **degree** of a $\mathrm{PCR}^{\mathbb{F}}$-proof is the maximum degree of a non-zero monomial that appears in the derivation.

Let $\pi \coloneqq (p_1, p_2, p_3, \dots, p_\ell)$ be a $\mathrm{PCR}^{\mathbb{F}}$-proof. Define a **lazy** representation $((\ell_\pi p)_i)$ of polynomials in π:

- $(\ell_\pi p)_i \coloneqq p_i$, if p_i is an axiom or p_i is obtained by multiplication rule.
- $(\ell_\pi p)_i \coloneqq \alpha p_j + \beta p_k$ without cancellations, if p_i is obtained by linear combination from p_j and p_k with coefficients α, β.

The **quadratic representation** of π is the sequence $((\ell_\pi p)_1^2, (\ell_\pi p)_2^2, (\ell_\pi p)_3^2, \dots, (\ell_\pi p)_\ell^2)$ where squares are expanded without cancellations. The **q-size** of π is the number of monomials in the quadratic representation of π. Note that q-size of a proof π is bounded by $O(\mathrm{size}(\pi)^2)$.

The notion of lazy representation is technical and we use only for the following Lemma. As in case of Sum-of-Squares the statement is not trivial since we deal with factor field.

Lemma 3.6. Let $\mathcal{F}$ be a system of degree d_0 and π be a $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$. If quadratic representation of π does not contain any term of degree greater than d then there is a $\mathrm{PCR}^{\mathbb{F}}$-proof π' of $\mathcal{F}$ of degree $\max(2d, d_0)$.

Proof. Let $\pi \coloneqq (p_1, \dots, p_\ell)$, $p_i \coloneqq \sum\limits_j t_{i,j}$ and $s_i \coloneqq \sum\limits_j t_{i,1} t_{i,j}$. Note that $p_i = t_{i,1} s_i$ and $s_i = t_{i,1} p_i$.

By definition all monomials that appear in p_i^2 also appear in $(\ell_\pi p)_i^2$, hence all terms of s_i appear in $(\ell_\pi p)_i^2$ this implies that the degree of s_i is at most d. Consider the sequence $(s_1, \dots, s_\ell)$. It is not a $\mathrm{PCR}^{\mathbb{F}}$-proof but we want to show that all s_i are derivable in degree $2d$ from previous polynomials and polynomials from $\mathcal{F}$. We prove it by induction on i. Consider three cases.

1. $p_i \in \mathcal{F}$. Then s_i is derivable from p_i in degree $\max(d, d_0)$.
2. $p_i \coloneqq x p_j$. Then $s_i = s_j$.
3. $p_i \coloneqq \alpha p_a + \beta p_b$. In this case consider $(\ell_\pi p)_i \coloneqq \alpha \sum\limits_j t_{a,j} + \beta \sum\limits_j t_{b,j}$ and denote $q \coloneqq \alpha \sum\limits_j t_{a,1} t_{a,j} + \beta \sum\limits_j t_{a,1} t_{b,j}$ without cancellations. All terms of q appear in $(\ell_\pi p)_i^2$ hence it has degree at most d, in particular term $t_{a,1} t_{b,1}$ has degree at most d.

   Note that $q = \alpha s_a + \beta \sum\limits_j t_{a,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} \sum\limits_j \beta t_{b,1} t_{b,j} = \alpha s_a + \beta t_{a,1} t_{b,1} s_b$. Hence it is derivable in degree $2d$ from s_a and s_b.

   $s_i = \sum\limits_j t_{i,1} t_{i,j}$ but all $t_{i,j}$ appear in the collection $\bigcup\limits_k \{t_{a,k}\} \cup \bigcup\limits_k \{t_{b,k}\}$. Wlog $t_{i,1} \coloneqq t_{a,k}$ hence $s_i = t_{a,k} t_{a,1} q$ and it is derivable from q in degree $2d$.

$\square$

3.3 Switching Between Bases

We can change the basis via affine shift. Let $x \in \{0, 1\}$ and $y \coloneqq (1 - 2x)$. This fact allows us to transform proofs from one basis to another.

Lemma 3.7. Let C be either SOS or $\mathrm{PCR}^{\mathbb{F}}$ proof system and $(\mathcal{F}, \mathcal{H})$ be a polynomial system on n variables. If there a $\mathrm{C}_{\{0,1\}}$-proof of size s and degree d of $(\mathcal{F}, \mathcal{H})$ then there is a $\mathrm{C}_{\{\pm 1\}}$-proof of size $2^d \mathsf{poly}(n) s$ and degree d of $(\mathcal{F}, \mathcal{H})$.

Proof. Let π be a $\mathrm{C}_{\{0,1\}}$ proof of size s and degree d of $(\mathcal{F}, \mathcal{H})$. If we apply substitution $x_i \leftarrow \frac{1-y_i}{2}$ to all variables x_i then the result will be a $\mathrm{C}_{\{\pm 1\}}$-proof in $y_i \in \{\pm 1\}$ variables. To conclude the proof note that range axiom for a x_i can be derived in constant number of steps from range axiom for the y_i variable. $\square$

Remark 3.8. The same statement holds if we switch from the $\{\pm 1\}$ basis to the $\{0, 1\}$ basis.

4 "Lifted" Systems

In this section, we prove lower bounds on the size of $\mathrm{SOS}_{\{\pm 1\}}$-proofs. At first, if we have a short proof of the "lifted" system then we can get low-degree proof for the original system under certain partial assignment. Then, we show that we regain enough control over the partial assignment so that the remaining system will still have large degree, contradicting the first step.

The following theorem illustrates the first step of our plan.

Theorem 4.1. Let $(\mathcal{F}, \mathcal{H})$ be a system over $X \coloneqq \{x_1, \ldots, x_n\}$, let g be a compliant gadget of size k and let $\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots$ be an arbitrary string consisting of ± 1.

If there is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ g$ of size s, then there is a sequence of variables $x_{i_1}, x_{i_2}, \ldots, x_{i_\ell}$, where $\ell \geq 4k^2 \frac{n \log s}{d}$ such that:

- the choice of x_{i_j} is independent of $(\alpha_j, \alpha_{j+1}, \ldots)$;
- there is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \restriction \{x_{i_j} = \alpha_j\}_{j=1}^{\ell}$ of reduced degree d.

We defer the proof of this Theorem to the next section. Assuming the above Theorem we give the desired lower bound on the size.

Theorem 4.2 (Formalization of Theorem 1.1)**.** Let $(\mathcal{F}, \mathcal{H})$ be a system on n variables of degree d_0 and g be an compliant gadget of constant size. If d_1 is the minimal degree of SOS-proof of this system then any $\mathrm{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ g$ has size $\exp\left[\Omega\left(\frac{(d_1 - d_0)^2}{n}\right)\right]$.

Proof. Fix parameters $d \coloneqq \frac{d_1 - d_0}{2}$ and $\varepsilon \coloneqq \frac{1}{50k^2}$, where k is the size of the gadget g. For contradiction, assume that we have an $\mathrm{SOS}_{\{\pm 1\}}$-proof π of size $s = \exp\left(\varepsilon \frac{(d_1 - d_0)^2}{n}\right)$.

We want to apply Theorem 4.1 for the parameter d and some carefully chosen sequence $\alpha_1, \ldots, \alpha_\ell$, where $\ell \coloneqq 4k^2 \frac{n \log s}{d} = 4k^2 \frac{2n\varepsilon(d_1 - d_0)^2}{n(d_1 - d_0)} = 8k^2 \varepsilon (d_1 - d_0) < \frac{d_1 - d_0}{6}$.

The reduced SOS-degree of $(\mathcal{F}, \mathcal{H})$ is at least $d_1 - d_0$. By Corollary 3.2 for any variable there is an assignment that decrease the reduced degree by at most 3. By Theorem 4.1 there is a choice of variable x_{i_1} does not depend on α_i for all $i \geq 1$. Hence we can choose x_{i_1} and choose α_1 to be the value such that any SOS-proof of $(\mathcal{F}, \mathcal{H}) \restriction (x_{i_1} = \alpha_1)$ has reduced degree at least $(d_1 - d_0) - 3$. We can repeat this process and choose x_{i_2} dependent on x_{i_1} and α_1. Hence after the second step we have the system $(\mathcal{F}, \mathcal{H}) \restriction \{(x_{i_1} = \alpha_1), (x_{i_2} = \alpha_2)\}$ such that any SOS-proof of it has reduced degree at least $(d_1 - d_0) - 6$.

After ℓ repetitions we have a partial assignment $\rho \coloneqq \{(x_{i_1} = \alpha_1), \ldots, (x_{i_\ell} = \alpha_\ell)\}$ such that:

- the reduced SOS-degree of $(\mathcal{F}, \mathcal{H}) \restriction \rho$ is at least $(d_1 - d_0) - 3\ell$ (by the choice of α_i) and
- there is an SOS-proof of $(\mathcal{F}, \mathcal{H}) \restriction \rho$ with reduced degree d (by Theorem 4.1).

This implies that $d \geq (d_1 - d_0) - 3\ell > (d_1 - d_0) - \frac{d_1 - d_0}{2} = d$, which is a contradiction. Hence there is no proof of $(\mathcal{F}, \mathcal{H}) \circ g$ of size $\exp\left(\frac{1}{50k^2}\frac{(d_1-d_0)^2}{n}\right)$. $\square$

Corollary 4.3. Let $\mathcal{F}$ be a system on n variables of degree d_0 and g be a compliant gadget of constant size. If d_1 is the minimal degree of SOS-proofs of $\mathcal{F}$ then any $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proof of $\mathcal{F} \circ g$ has size at least $\exp\left[\Omega\left(\frac{(d_1-d_0)^2}{n}\right)\right]$.

The proof of this corollary follows from the next statement which is an analogue of the statement from [Ber18] for the $\{\pm 1\}$ basis.

Theorem 4.4. [Analogue of [Ber18]] Let $\mathcal{F}$ be a system of polynomial equations. If there is a $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ of size S and degree d then there is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of size $\mathsf{poly}(S)$ and degree $2d$.

The proof of this corollary is analogous to the proof for the $\{0, 1\}$ basis [Ber18]. For the sake of completeness, we state the proof in appendix A.2.

4.1 Proof of Theorem 4.1

Let $f'_i := f_i \circ g$ and $h'_i := h_i \circ g$. Denote by $Z := \{z_{i,j} \mid i \in [n], j \in [k]\}$ the set of variables of $(\mathcal{F}, \mathcal{H}) \circ g$. Let $\pi := (p_1, \ldots, p_a; q_1, \ldots, q_b)$ be an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $(\mathcal{F}, \mathcal{H}) \circ g$ of q-size $s_q \leq s^2$.

We say that monomial t on Z variables **touches** a variable $x_i \in X$ iff there is an unordered pair $j', j'' \in [k]$ such that $z_{i,j'} \in t$ and $z_{i,j''} \notin t$. We also say that term t is **fat** if it touches at least $\frac{d}{2}$ variables from the set X.

Let H be a multiset of fat terms in the quadratic representation of π, i.e. in the collection of polynomials $(p_1, \ldots, p_a; q_1^2, \ldots, q_b^2)$, where polynomials q_v^2 are represented without cancellations.

We would like to find a partial assignment that helps us to erase significant fraction of fat terms, but since $z_{i,j} \in \{\pm 1\}$ it is not so clear if such an assignment exists. Instead of it we modify the proof by using symmetry of the gadget and "force" such an assignment to a new proof.

Pick the most frequent variable $x_i \in X$ among variables that are touched by fat terms (it is the first variable x_{i_1} in the sequence). By an averaging argument x_i is touched by at least $\frac{d|H|}{2n}$ fat terms. For each of these terms there is an unordered pair $z_{i,j'}, z_{i,j''}$ such that $z_{i,j'} \in t$ and $z_{i,j''} \notin t$ or vise versa. Since there are at most $\frac{k^2}{2}$ different pairs we can fix j' and j'' such that there is at least $\frac{d|H|}{k^2 n}$ terms that contains exactly one of the variables $z_{i,j'}$ and $z_{i,j''}$. We say that these terms are **active**.

Consider the permutation σ that swaps $z_{i,j'}$ and $z_{i,j''}$ and leaves everything else in its place. Denote by p^σ the result of an application of the permutation σ to the polynomial p. Note that the sequence $\pi' := (\frac{1}{2}(p_1 + p_1^\sigma), \ldots, \frac{1}{2}(p_a + p_a^\sigma); \frac{1}{\sqrt{2}}q_1, \frac{1}{\sqrt{2}}q_1^\sigma, \ldots, \frac{1}{\sqrt{2}}q_b, \frac{1}{\sqrt{2}}q_b^\sigma)$ is a proof of $(\mathcal{F}, \mathcal{H}) \circ g$. Indeed

$$-1 = \sum_{u=1}^{a} (p_u f'_u)^\sigma + \sum_{v=1}^{b} (q_v^2 h'_v)^\sigma \qquad = \sum_{u=1}^{a} p_u^\sigma f'^\sigma_u + \sum_{v=1}^{b} (q_v^\sigma)^2 h'^\sigma_v = \sum_{u=1}^{a} p_u^\sigma f'_u + \sum_{v=1}^{b} (q_v^\sigma)^2 h'_v,$$

where the last equality holds by symmetry of g and the symmetric encoding of it. Hence

$$-1 = \sum_{u=1}^{a} \frac{p_u + p_u^\sigma}{2} f'_u + \sum_{v=1}^{b} ((\frac{1}{\sqrt{2}} q_v)^2 + (\frac{1}{\sqrt{2}} q_v^\sigma)^2) h'_v.$$

Since g is compliant we have that by property 2 and symmetry of g we can find for any $\alpha_1 \in \{\pm 1\}$ an assignment $\beta \in \{\pm 1\}^k$ to the $z_{i,\cdot}$ variables such that $g(\beta) = \alpha_1$ and $\beta_{j'} \neq \beta_{j''}$. Let ρ be a restriction that maps the $z_{i,\cdot}$ variable to β. Note that if term t

- is active, then $t := z_{i,j'}r$ and $t^\sigma := z_{i,j''}r$ (or vice versa), hence $(t+t^\sigma) \restriction \rho = (z_{i,j'}+z_{i,j''})r \restriction \rho = 0$;
- is not active then $t = t^\sigma$, hence $(t+t^\sigma) \restriction \rho = 2t \restriction \rho$.

Thus for any $u \in [a]$ the polynomial $\frac{1}{2}(p_u + p_u^\sigma) \restriction \rho$ only contains inactive terms t restricted by ρ.

Now consider a polynomial q_v for $v \in [b]$. Let us rewrite $q_v = r_{v,1} + z_{i,j'}r_{v,2} + z_{i,j''}r_{v,3}$ and denote $r_{v,4} := z_{i,j'}r_{v,2} + z_{i,j''}r_{v,3}$. We see that

$$(q_v)^2 = r_{v,1}^2 + z_{i,j'}r_{v,1}r_{v,2} + z_{i,j''}r_{v,1}r_{v,3} + z_{i,j'}r_{v,2}r_{v,1} + z_{i,j''}r_{v,3}r_{v,1} + r_{v,4}^2$$
$$(q_v^\sigma)^2 = r_{v,1}^2 + z_{i,j''}r_{v,1}r_{v,2} + z_{i,j'}r_{v,1}r_{v,3} + z_{i,j''}r_{v,2}r_{v,1} + z_{i,j'}r_{v,3}r_{v,1} + r_{v,4}^2$$

and hence

$$\frac{1}{2}\left((q_v)^2 + (q_v^\sigma)^2\right) \restriction \rho = r_{v,1}^2 + r_{v,4}^2$$

Not that only the following terms were active before the restriction: $z_{i,j'}r_{v,1}r_{v,2}$, $z_{i,j''}r_{v,1}r_{v,3}$, $z_{i,j'}r_{v,2}r_{v,1}$, $z_{i,j''}r_{v,3}r_{v,1}$. In the representation $r_{v,1}^2 + r_{v,4}^2$, all of these terms are erased. Here it is important that we do not allow any cancellation while representing squared polynomials, as otherwise the size of the new representation may be bigger than the size of the original polynomial q_v^2.

We conclude that the proof $\pi'' :=$

$$-1 = \sum_{u=1}^{a} \frac{1}{2}(p_u + p_u^\sigma) f'_u \restriction \rho + \sum_{v=1}^{b} r_{v,1}^2 h'_v \restriction \rho + \sum_{v=1}^{b} r_{v,4}^2 h'_v \restriction \rho$$

is a proof of $(\mathcal{F}, \mathcal{H}) \circ g \restriction \rho$ (and hence of $((\mathcal{F}, \mathcal{H}) \restriction (x_i = \alpha_1)) \circ g$) such that its quadratic representation contains at most $(1 - \frac{d}{k^2 n})|H|$ fat terms.

By repeating this process ℓ times we get a partial assignment $x_{i_1} = \alpha_1, x_{i_2} = \alpha_2, \dots, x_{i_\ell} = \alpha_\ell$ such that the choice of x_{i_j} only depends on the original proof π and $\alpha_{j'}$ for $j' < j$. We end up with a proof π_0 of $\left((\mathcal{F}, \mathcal{H}) \restriction \{x_{i_j} = \alpha_j\}_{j=1}^{\ell}\right) \circ g$ such that its quadratic representation contains at most $(1 - \frac{d}{k^2 n})^\ell s_q$ fat terms. But $(1 - \frac{d}{k^2 n})^\ell s_q \le (1 - \frac{d}{k^2 n})^{4k^2 n \log s/d} s^2 \le \exp(-4 \log s) s^2 < 1$, we see that in this setting, quadratic representation of π_0 does not contain any fat term.

To conclude the proof we want to transform π_0 into a proof of $(\mathcal{F}, \mathcal{H}) \restriction \{x_{i_j} = \alpha_j\}_{j=1}^{\ell}$ of small degree. And here we use the fact that g is not parity: there are two points $\beta, \gamma \in \{\pm 1\}^k$ such that:

- $\prod_{j=1}^{k} \beta_j = \prod_{j=1}^{k} \gamma_j$;
- $g(\beta) = 1$;
- $g(\gamma) = -1$.

For all $i \in [n], j \in [k]$ we make the following substitution in the proof π_0:

- if $\beta_j = \gamma_j$, we replace $z_{i,j}$ by β_i;
- if $\beta_j = 1$ and $\gamma_j = -1$, we replace $z_{i,j}$ by x_i;
- if $\beta_j = -1$ and $\gamma_j = 1$, we replace $z_{i,j}$ by $-x_i$.

Denote the result of this replacement applied to a term t by t^x. Note that after this replacement $g(z_{i,1}, z_{i,2}, \dots, z_{i,k})$ will return the value of x_i

Suppose term t over Z variables does not touch x_i, that means t does not contain any variable $z_{i,\cdot}$ or it contains $z_{i,j}$ for all $j \in [k]$. In the first case x_i will not appear in t^x. In the second case we observe that β and γ are different in even number of positions hence x_i will appear in t^x in even degree and we just erase it since we deal all operations in factor ring over range axioms. This fact implies that degree of the quadratic representation of $(\pi_0)^x$ is bounded by maximum over all terms t that appear in the quadratic representation of π_0 of number of variables $x_i \in X$ that are touched by t. But the quadratic representation of π_0 does not contain any fat term hence this replacement produces terms of degree at most $\frac{d}{2}$.

Also note that $(f'_u)^x$ pointwise equal to f_u. We consider only multilinear polynomials for that means for any function there is a unique representation hence $(f'_u)^x$ is the same polynomial as f_u. By analogy the same holds for h_v and by analogy the same holds after a partial assignment. Hence π_0^x is a proof of $(\mathcal{F}, \mathcal{H}) \restriction \{x_{i_j} = \alpha_j\}_{j=1}^{\ell}$ such that quadratic representation of it does not contain any term of degree greater than $\frac{d}{2}$. By Lemma 3.3 there is a proof of $(\mathcal{F}, \mathcal{H}) \restriction \{x_{i_j} = \alpha_j\}_{j=1}^{\ell}$ of degree at most $d + d_0$.

5 Random Δ-CNF

In this section we prove a lower bound on the size of $\mathrm{SOS}_{\{\pm 1\}}$ and $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proofs of random Δ-CNF formulas. The general idea is the same as in the case of "lifted" systems: we want to consider a linear combination of two proofs of the formula and hit it by a restriction in order to kill all terms of high degree. Unfortunately, instances of random Δ-CNF do not have symmetry that was crucially used in previous case, instead of it we will use "self-reducibility" of Δ-CNF instances. We describe the "self-reducibility" in terms of the dependency graph of the formula, hence lets start with some definitions and useful properties of graphs.

5.1 Expanders and Closure

We use the following notation: $N_G(S)$ is the set of neighbours of the set of vertices S in the graph G, $\partial_G(S)$ is the set of unique neighbours of the set of vertices S in the graph G. We omit the index G if the graph is evident from the context.

A bipartite graph $G \coloneqq (L, R, E)$ is an (r, Δ, c)-**expander** if all vertices $u \in L$ have degree at most Δ and for all sets $S \subseteq L$, $|S| \le r$, it holds that $|N(S)| \ge c \cdot |S|$. Similarly, $G \coloneqq (L, R, E)$ is an (r, Δ, c)-**boundary expander** if all vertices $u \in L$ have degree at most Δ and for all sets $S \subseteq L$, $|S| \le r$, it holds that $|\partial S| \ge c \cdot |S|$. In this context, a simple but useful observation is that

$$|N(S)| \le |\partial S| + \frac{\Delta|S| - |\partial S|}{2} = \frac{\Delta|S| + |\partial S|}{2}, \tag{1}$$

since all non-unique neighbours have at least two incident edges. This implies that if a graph G is an $(r, \Delta, (1-\varepsilon)\Delta)$-expander then it is also an $(r, \Delta, (1-2\varepsilon)\Delta)$-boundary expander.

The next proposition is well known in the literature. In this form it was used in [GMT09].

Proposition 5.1. If $G \coloneqq (L, R, E)$ is an (r, Δ, c)-boundary expander then for any set $S = \{v_1, \dots, v_k\} \subseteq L$ of size at most r there is a partition $\bigsqcup_i R_i = N(S)$ such that $R_i \subseteq N(v_i)$ and $|R_i| \ge c$. In particular, there is a matching on the set S.

Proof. Since $|S| \le r$ it holds that $|\partial S| \ge c|S|$ and there is a vertex $v_i \in S$ such that $|\partial v_i| \ge c$. Let $R_i \coloneqq \partial v_i$, and repeat the process on $S \setminus \{v_i\}$. $\square$

Let $G \coloneqq (L, R, E)$ denote a bipartite graph. Consider a *closure* operation that seems to have originated in [AR03; Ale+04].

Definition 5.2. For vertex sets $S \subseteq L, U \subseteq R$ we say that the set S is (U, r, ν)-**contained** if $|S| \leq r$ and $|\partial S \setminus U| < \nu|S|$. For any set $J \subseteq R$ let $S \coloneqq \mathrm{Cl}^{r,\nu}(J)$ denote an arbitrary but fixed set of maximal size such that S is (J, r, ν)-contained.

Lemma 5.3. Suppose that G is an (r, Δ, c)-boundary expander and that $J \subseteq R$ has size $|J| \leq \Delta r$. Then $|\mathrm{Cl}^{r,\nu}(J)| < \frac{|J|}{c-\nu}$.

Proof. By definition we have that $|\partial \mathrm{Cl}^{r,\nu}(J) \setminus J| < \nu|\mathrm{Cl}^{r,\nu}(J)|$. Since $|\mathrm{Cl}^{r,\nu}(J)| \leq r$ by definition, the expansion property of the graph guarantees that $c|\mathrm{Cl}^{r,\nu}(J)| - |J| \leq |\partial \mathrm{Cl}^{r,\nu}(J) \setminus J|$. The conclusion follows. □

Suppose $J \subseteq R$ is not too large. Then Lemma 5.3 shows that the closure of J is not much larger. Thus, after removing the closure and its neighbourhood from the graph, we are still left with a decent expander. The following lemma makes this intuition precise.

Lemma 5.4. Let $J \subseteq R$ be such that $|J| \leq \Delta r$ and $|\mathrm{Cl}^{r,\nu}(J)| \leq \frac{r}{2}$ and let $G' \coloneqq G \setminus (\mathrm{Cl}^{r,\nu}(J) \cup J \cup N(\mathrm{Cl}^{r,\nu}(J)))$. Then any set S of vertices from the left side of G', with size $|S| \leq \frac{r}{2}$, satisfies that $|\partial_{G'} S| \geq \nu|S|$.

Proof. Suppose the set $S \subseteq L(G')$ violates the boundary expansion guarantee. Observe that $\mathrm{Cl}^{r,\nu}(J)$ and S are both sets of size at most $\frac{r}{2}$. Furthermore, the set $(\mathrm{Cl}^{r,\nu}(J) \cup S)$ is (J, r, ν)-contained in the graph G. As $\mathrm{Cl}^{r,\nu}(J)$ is a (J, r, ν)-contained set of maximal cardinality, this leads to a contradiction. □

5.2 Random Formulas

Let φ be a formula on X variables. We denote a restriction of dependency graph of φ to a subset of variables $X_0 \subseteq X$ by $G_\varphi^{X_0} \coloneqq (L_\varphi, X_0, E_\varphi^{X_0})$. To be precise L_φ corresponds to the set of clauses of φ (and we identify these two sets) and $(u, x) \in E_\varphi^{X_0}$ iff clause u contains a variable x_v or its negation. We omit superscript X_0 if we assume the full set of variables. We will also deal with the formulas after application of some partial assignment, in this case we erase all vertices from the left part of dependency graph that correspond to satisfied constrains.

Definition 5.5. Let $\varphi(m, n, \Delta)$ denote the distribution of random Δ-CNF on n variables obtained by sampling m clauses (out of the $\binom{n}{\Delta}2^\Delta$ possible clauses) uniformly at random with replacement.

Lemma 5.6 ([CS88])**.** For any $\Delta \geq 3$ whp $\varphi \sim \varphi(m, n, \Delta)$ is unsatisfiable if $m \geq \ln 2 \cdot 2^\Delta n$.

The next Lemma is a modification of well-known result for random graphs (see [Vad12]).

Lemma 5.7. If $m = O(n)$, $\Delta > 11$ and $\varphi \sim \varphi(m, n, \Delta)$ then whp G_φ is an $(r, \Delta, 5)$-boundary expander where $r = \Omega(\frac{n}{\Delta})$.

Proof. For proof see appendix A. □

A next Lemma is a straightforward corollary from the main result of [Gri01] (see also [GV01]).

Lemma 5.8 ([Gri01])**.** If φ is an unsatisfiable Δ-CNF formula and G_φ is an $(r, \Delta, 2)$-expander then SOS-degree of φ is $\Omega(r)$.

5.3 Lower Bound on Random Formulas

Before we formulate the main theorem we want to reduce the degrees of all vertices in the dependency of the instances of random formulas.

Lemma 5.9. Let φ be a Δ-CNF formula on n variables and m clauses. If G_φ is an (r, Δ, c)-boundary expander then there is a constant ℓ and partial assignment ρ of size at most $(\Delta+1)\frac{r}{2}$ such that $G_{\varphi\restriction\rho}$ is an $(\frac{r}{2}, \Delta, \nu)$-boundary expander and the degree of all vertices of $G_{\varphi\restriction\rho}$ is bounded by $2\Delta\frac{m}{r}$, where $\nu \leq c-1$.

Proof. Pick a set $J \subseteq R$ of vertices of degree greater than $2\Delta\frac{m}{r}$. There are at most Δm edges in the graph G hence $|J| \leq \frac{r}{2}$. By Lemma 5.3 there is a set $S \coloneqq \mathrm{Cl}^{r,\nu}(J)$ such that $|S| \leq |J|$. By a straightforward corollary of Proposition 5.1 there is a matching M on the set S. Define a partial assignment ρ in the following way:

- for all $(s, x_s) \in M$ assign x_s by the value that satisfy clause s;
- assign variables from $N(S) \cup J$ in an arbitrary way.

We assign all variables from J hence the degree of all vertices in $G_{\varphi\restriction\rho}$ is bounded by $2\Delta\frac{m}{r}$. Note that $R_{\varphi\restriction\rho} = R_\varphi \setminus (J \cup N(S))$ and $L_{\varphi\restriction\rho} \subseteq L_\varphi \setminus S$ since ρ satisfy all clauses from S. By Lemma 5.4 $G_{\varphi\restriction\rho}$ is an $(\frac{r}{2}, \Delta, \nu)$-boundary expander. $|\mathrm{Vars}(\rho)| \leq |N_{G_\varphi}(S)| + |J| \leq (\Delta+1)\frac{r}{2}$. $\square$

Now can formulate the main statement of this section.

Theorem 5.10. Let $\Delta > 0$ be an integer and φ be an unsatisfiable Δ-CNF formula on n variables and m clauses.

If G_φ is an $(r, \Delta, 4)$-boundary expander such that degree of all vertices are bounded by η then any $\mathrm{SOS}_{\{\pm1\}}$-proof of φ has size $\exp(\Omega(\frac{r^2}{\eta^2 n}))$.

We defer the proof of this Theorem to the section 5.5.

Corollary 5.11 (Formalization of Theorem 1.2)**.** If $\Delta > 11$ is a constant, $\varphi \sim \varphi(m, n, \Delta)$ where $m = O(n)$ then whp any $\mathrm{SOS}_{\{\pm1\}}$-proof of φ has monomial size $\exp(\Omega(n))$.

Proof. Wlog $\frac{m}{n} > 1$ (otherwise φ is satisfiable with high probability). Let $\eta \coloneqq 2\Delta\frac{m}{n}$. Fix a formula φ. By Lemma 5.7 there is some $\delta > 0$ such that whp G_φ is an $(\delta\frac{n}{\Delta}, \Delta, 5)$-boundary expander. Wlog assume that $\delta < \frac{1}{20}$. By Lemma 5.9 there is assignment ρ of size at most $\frac{n}{5}$ such that $G_{\varphi\restriction\rho}$ is an $(\frac{\delta}{2\Delta}n, \Delta, 4)$-boundary expander with degrees bounded by η. By Theorem 5.10 any $\mathrm{SOS}_{\{\pm1\}}$-proof of $\varphi \restriction \rho$ has size $\exp(\Omega(n))$ hence the same holds also for φ. $\square$

5.4 Split **Operation**

The heart of proof of Theorem 5.10 is a Split_x operation. The idea of this operation is the following:

- we want to banish all terms in the proof that contain a variable x;
- after application of this operation to an $\mathrm{SOS}_{\{\pm1\}}$ or $\mathrm{PCR}^{\mathbb{F}}_{\{\pm1\}}$ proof the result still be a proof, but maybe of a "damaged" formula.

Unfortunately it is not clear how to define this operation for both considered proof systems in the same way, so we will do it separately. Let φ be a boolean formula and $\mathcal{F}$ is a CNF encoding of φ as a polynomial system.

Sum-of-Squares. Let $\pi := (p_1, \ldots, p_a; q_1, \ldots, q_b)$ be an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $\mathcal{F}$. Recall that we consider CNF encodings of boolean formulas, hence there is no inequalities.

Pick a variable x and consider a linear combination of proof with different assignments to x. Lets do it more formally and consider the following operation $\frac{1}{2}\left(p \restriction (x = -1) + p \restriction (x = 1)\right)$. Note that the result of this operation contains only terms of p and only those terms that do not touch x.

1. If $f_u \in \mathcal{F}$ is a constraint that does not depend on x then $p_u f_u \restriction (x = -1) + p_u f_u \restriction (x = 1) = (p_u \restriction (x = -1) + p_u \restriction (x = 1)) f_u$ and we banish all terms that contain x variable.
2. If $f_u \in \mathcal{F}$ is a constraint that depends on x then we cannot simplify the expression $p_u f_u \restriction (x = -1) + p_u f_u \restriction (x = 1)$ and we say that constraint f_u (that correspond to some clause in φ) is **damaged**.
3. Let $q_v := (r_v + x e_v)$ where r_v, e_v are polynomials that do not contain x then:

$$\begin{aligned} q_v^2 &= r_v^2 + 2x r_v e_v + e_v^2 \\ q_v^2 \restriction (x = -1) + q_v^2 \restriction (x = 1) &= 2(r_v^2 + e_v^2) \end{aligned}$$

   And r_v and e_v be a new representation of q_v after restriction. Note that we banish all terms that touch x. And as in case of lifted formulas this is a place there we use the fact that we do not allow cancellations while computing squares.

The result of $\mathrm{Split}_x(\pi)$ is a proof:

$$-1 = \sum_{u \in D} \left(\frac{1}{2} p_u f_u \restriction (x = -1) \right) + \sum_{u \in D} \left(\frac{1}{2} p_u f_u \restriction (x = 1) \right) + \sum_{u \notin D} p'_u f_u + \sum r_v^2 + \sum e_v^2,$$

where p'_u is a polynomial that contain only those terms of p_u that do not touch x, D is a set of damaged constraints.

Observe important property that damages constrains are original constraints with some partial assignment and if we assign any variable except x in order to satisfy clause $u \in D$ of φ we will set to 0 all damaged constraints that correspond to u.

The result of $\mathrm{Split}_x(\pi)$ is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of damaged system, but the size of it maybe bigger than the size of π because of damaged part. In our applications we will care about and:

- exclude monomials that corresponds to damaged part from counting (see. Remark 5.13)
- satisfy all damaged damaged constraints.

Polynomial Calculus. Let $\pi := (p_1, \ldots, p_a)$ be a $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of $\mathcal{F}$. A naive idea is to do the same operation as in case of $\mathrm{SOS}_{\{\pm 1\}}$, but lets consider the following example:

$$\frac{\dfrac{p}{xp}}{p}$$

where p does not contain x. If we apply operation $\frac{1}{2}\left(q \restriction (x = -1) + q \restriction (x = 1)\right)$ to all polynomials in this proof then first and third line will not be affected but the middle line will be set to 0 and it will not be a valid $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of anything.

For each line of the proof p_i consider a decomposition $p_i := r_i + x q_i$ where r_i and q_i do not contain x. We use this decomposition to define Split operation. More formally, the result of $\mathrm{Split}_x(\pi)$ is a proof: $(r_1, q_1, r_2, q_2, \ldots, r_a, q_a)$ where we omit trivially zero polynomials.

We want to show that $\mathrm{Split}_x(\pi)$ gives a $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof.

1. If p_i is an axiom that does not depend on x then $r_i \coloneqq p_i$ and $q_i \coloneqq 0$ hence we do not change this line.

2. If p_i is a CNF encoding of an axiom that depends on x and it corresponds to clause $(C \vee x)$ of φ (with $\bar{x}$ situation is similar) then:

   - $r_i \coloneqq \frac{1}{2}p_c$ and $q_i \coloneqq \frac{1}{2}p_c$, or equivalently
   - $r_i \coloneqq \frac{1}{2}p_i \restriction (x = 1)$ and $q_i \coloneqq \frac{1}{2}p_i \restriction (x = 1)$,

   where p_c is a CNF encoding of the clause C. We say that this constraint is **damaged**.

3. Let $p_i = \alpha p_j + \beta p_k$ where $j, k < i$ then $r_i = \alpha r_j + \beta r_k$ and $q_i = \alpha q_j + \beta q_k$.

4. Let $p_i = x p_j$ where $j < i$ then $r_i = q_j$ and $q_i = r_j$.

5. Let $p_i = x' p_j$ where $j < i$ and x' is different from x then $r_i = x' r_j$ and $q_i = x' q_j$.

As in previous case observe important property that damages constrains are correspond to clauses of φ without x and if we assign any variable except x in order to satisfy clause $u \in D$ of φ we will set to 0 all damaged constraints that correspond to u. We deal with the result of $\mathrm{Split}_x(\pi)$ as with usual proof of damaged system, in particular quadratic representation of it is well-defined (this situation is a bit easier than in Sum-of-Squares where we need to pay some attention to the damaged part of the proof).

The only problem with this transformation that it does not kill any term. But lets consider some polynomial p_i^2 in the quadratic representation of π. $p_i^2 = r_i^2 + x r_i q_i + q_i^2$ the only parts of this polynomial that touch x is $x r_i q_i$ and in the quadratic representation of $\mathrm{Split}_x(\pi)$ we have only polynomials r_i^2 and q_i^2. By analogy the same holds for lazy representations hence this operation banish all terms that contain x in the quadratic representation.

Remark 5.12. In some sense Split_x corresponds to "double false" assignment since we erase all occurrences of x from clauses of our formula independently of the signs.

5.5 Proof of Theorem 5.10

By Lemma 5.8 there is a constant ε_0 such that there is no SOS and $\mathrm{PCR}^{\mathbb{F}}$ proof of degree $\varepsilon_0 r$ of any formula based on $(\frac{r}{2}, \Delta, 2)$-boundary expander. Fix $\varepsilon \coloneqq \frac{\varepsilon_0}{100}$.

Let $\mathcal{F}$ be a CNF encoding of the formula φ as a polynomial system. For the sake of contradiction assume that we have an $\mathrm{SOS}_{\{\pm 1\}}$ or $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ proof π of q-size $\exp(\frac{\varepsilon}{\eta^2} \cdot \frac{r^2}{n})$ (here we can choose size measure).

Fix the parameter $d \coloneqq \frac{\varepsilon_0}{10} r$. We say that a term t is **fat** if $\mathsf{deg}(t) \geq d$ and H is a multiset of all fat term in the quadratic representation of the proof π.

The idea of the proof is the following.

1. In order to erase all fat terms we iteratively apply Split operation (instead of ordinary restrictions). On each iteration we choose a variable x and replace a proof π by $\mathrm{Split}_x(\pi)$ to banish all fat terms in the quadratic representation that contain x.

2. During this process our formula may become "easy" for SOS or $\mathrm{PCR}^{\mathbb{F}}$. To avoid this situation we hit the formula after each iteration by a partial assignment. This allows us to restore the expansion property on the remainder of the formula.

Now we can describe the general algorithm. It takes a proof π and transforms it into a proof of small degree of a "damaged" formula. On each iteration

Algorithm 1 Degree reduction

$A_1 \coloneqq X$ ▷ Set of **alive** variables
$J_1 \coloneqq \emptyset$ ▷ Set of **active** variables
$D_1 \coloneqq \emptyset$ ▷ Set of **damaged** constraints
$\ell \coloneqq 1$
$\pi_1 \coloneqq \pi$
$\rho_1 \coloneqq \emptyset$
while $H \neq \emptyset$ **do**
  Pick the most frequent variable x in H
  $J_{\ell+1} \coloneqq J_\ell \cup \{x\}$
  $\pi' \coloneqq \mathrm{Split}_x(\pi)$
  $G_{\ell+1} \coloneqq G^{A_\ell\setminus\{x\}}_{\varphi\restriction\rho_\ell}$
  $B_\ell \coloneqq \max\{B \subseteq L_{\ell+1} \mid |B| \leq r, |\partial_{G_{\ell+1}}(B)| \leq 3|B|\}$
  $D_{\ell+1} \coloneqq \Big(D_\ell \cup N_{G_{\varphi\restriction\rho_\ell}}(x)\Big) \setminus B_\ell$
  Find a matching M on B_ℓ in $G_{\ell+1}$ ▷ Proposition 5.1
  $\rho_{\ell+1} \coloneqq \rho_\ell$
  for $(u, x_u) \in M$ **do**
    $\rho_{\ell+1} \coloneqq \rho_{\ell+1} \cup \{x_u = \text{value that satisfies } u\}$ ▷ -1 is True, 1 is False
  $\pi_{\ell+1} \coloneqq \pi' \restriction \rho_{\ell+1}$
  $A_{\ell+1} \coloneqq A_\ell \setminus (\{x\} \cup \mathrm{Vars}(\rho_{\ell+1}))$
  $H \coloneqq$ set of fat terms of the quadratic representation of $\pi_{\ell+1}$ ▷ See remark 5.13
  $\ell \coloneqq \ell + 1$
return π_ℓ

Remark 5.13. In case of $\mathrm{SOS}_{\{\pm 1\}}$ we do not add fat terms to H that correspond to the damaged part of the formula.

We start with the system $\mathcal{F}$ and assume that all constraints are not damaged.

In each iteration we pick a variable x that appears in at least $\frac{d}{n}|H|$ fat terms and consider $\mathrm{Split}_x(\pi)$. The fact that $\mathrm{Split}_x(\pi)$ banish all terms that contain x allows us to estimate the number of iterations. In case of $\mathrm{SOS}_{\{\pm 1\}}$ the $\mathrm{Split}_x(\pi)$ may not kill terms in the damaged part of the proof but we do not count these terms (see Remark 5.13) since we will set the damaged constraints to 0 later.

Proposition 5.14. $\ell \leq \frac{r}{5\eta^2}$.

Proof. We kill at least fat $\frac{d}{n}|H|$ terms. Hence the process will terminate when $(1 - \frac{d}{n})^\ell |H| < 1$. $|H|$ is at most the q-size of the proof π and $(1 - \frac{d}{n})^\ell |H| \leq (1 - \frac{d}{n})^\ell \exp(\frac{\varepsilon}{\eta^2}\frac{r^2}{n}) \leq \exp(-\frac{\ell d}{n} + \frac{\varepsilon}{\eta^2}\frac{r^2}{n})$ is less than 1 if $\ell d > \frac{\varepsilon}{\eta^2} r^2$. This implies that $\ell \frac{\varepsilon_0}{10} > \frac{\varepsilon}{\eta^2} r$ and hence $\ell > \frac{10\varepsilon}{\varepsilon_0 \eta^2} r$. By the choice of ε we obtain desired result. $\square$

Damaged axioms are axioms from $\mathcal{F}$ that are hit by partial assignments to active variables. If we assign to any alive variable x the value that satisfies clause u in our formula, then all damaged axioms that correspond to u will be set to 0. Note that this assignment is independent of ρ_i and the assignments to the active variables. In order to find such an assignment and keep the formula hard for SOS (and $\mathrm{PCR}^{\mathbb{F}}$), we polish it after each iteration by a partial assignment that satisfy the set B_i.

First we want to show that all sets B_j are not too big and we can always find a matching on B_j. Let $C_i \coloneqq \bigcup_{j=1}^{i} B_j$. The following Lemma formalizes this statement. The proof is similar to the proof of Lemmas 5.3 and 5.4, but, unfortunately, we need to care about parameters during all iterations simultaneously.

Proposition 5.15. 1. $|C_\ell| \le \ell$.

2. $\forall i \in [\ell], G^{A_i}_{\varphi\restriction\rho_i}$ is an $(r, \Delta, 3)$-boundary expander.

Proof. See appendix A.1. □

Since $G^{A_i}_{\varphi\restriction\rho_i}$ is an $(r, \Delta, 3)$-boundary expander, G_{i+1} is an $(r, \Delta, 2)$-boundary expander (as we just remove one vertex on the right side). By Proposition 5.1 there is a matching on B_i.

To conclude the proof we note that the number of damaged constraints in the end is at most $\eta|J'| \le \frac{r}{5\eta}$ and by Proposition 5.15 we have an $(r, \Delta, 3)$-boundary expander on alive variables. Denote it by G and consider $S \coloneqq \mathrm{Cl}^{r,2}_G(N_G(D_\ell))$. By Lemma 5.3 $|S| \le |N_G(D_\ell)| \le \frac{r}{5}$. By Proposition 5.1 there is a matching on $S \cup D_\ell$ and hence there is a partial assignment γ on $N_G(S \cup D_\ell)$ that satisfies all clauses in $S \cup D_\ell$. But by Lemma 5.4 the graph of the remaining formula will be an $(\frac{r}{2}, \Delta, 2)$-boundary expander and $\pi_\ell \restriction \gamma$ is a proof of this formula. Moreover the quadratic representation of $\pi_\ell \restriction \gamma$ does not contain any fat terms and hence by Lemmas 3.6 and 3.3 the proof $\pi_\ell \restriction \gamma$ can be transformed into a proof of degree at most $2d$. This is a contradiction with the choice of d.

6 Separation Between $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ and $\mathrm{SOS}_{\{\pm 1\}}$

In this section we show a separation between $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ and $\mathrm{SOS}_{\{\pm 1\}}$.

6.1 Pigeonhole Principle

We consider a graph version of the Pigeonhole Principle for two reasons:

- our lower bounds depends on the number of variables and we want to reduce it;
- in case of constant width formulas we can choose the encoding that suit us best.

It is convenient to think of the Pigeonhole Principle in terms of a bipartite graph $G \coloneqq (L, R, E)$ with pigeons $L \coloneqq [m]$ and holes $R \coloneqq [n]$ for $m \ge n + 1$. Every pigeon i can fly to its neighbouring holes $N(i)$ as specified by the graph G.

We encode the claim that there does in fact exist an injective mapping of pigeons to holes as a CNF formula consisting of **pigeon axioms**

$$f^i = \bigvee_{j \in N_G(i)} x_{i,j} \qquad \text{for } i \in [m]$$

and **hole axioms**

$$f^{i,i'}_j = (\bar{x}_{i,j} \vee \bar{x}_{i',j}) \qquad \text{for } i \ne i' \in [m], j \in N_G(i) \cap N_G(i')$$

that require that every hole contains get at most one pigeon (where the intended meaning of the variables is that $x_{i,j}$ is true if pigeon i flies to hole j).

We consider a CNF encoding of the Pigeonhole Principle $\mathsf{G\text{-}PHP}^m_n$.

Theorem 6.1 ([AR03; MN15])**.** Let G be an $(r, \Delta, 2)$-boundary expander. Then any $\mathrm{PCR}^{\mathbb{F}}_{\{0,1\}}$-proof of the $\mathsf{G\text{-}PHP}^m_n$ has degree $\Omega(r)$ and size $\exp\left[\Omega\left(\frac{r^2}{\Delta m}\right)\right]$.

The next claim is an interpretation of the result from [GHP02].

Theorem 6.2 ([GHP02])**.** Let G be a constant degree graph. Then there is an $\mathrm{SOS}_{\{0,1\}}$-proof of the $\mathsf{G\text{-}PHP}^m_n$ in CNF encoding of constant degree and size $\mathsf{poly}(n)$.

Theorem 6.3. Let G be an $(r, \Delta, 4)$-boundary expander then any $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$-proof of the $\mathsf{G\text{-}PHP}^m_n$ has size $\exp\left[\Omega\left(\frac{r^2}{\Delta m}\right)\right]$.

6.2 Proof of Theorem 6.3

The proof is similar to the lower bound proof of random formulas, but we need to take care of hole axioms.

We choose a constant ε_0 such that there is no $\mathrm{PCR}^{\mathbb{F}}$ proof of degree $\varepsilon_0 r$ of Pigeonhole Principle based on $(\frac{r}{2}, \Delta, 2)$-boundary expander. By Theorem 6.1 such constant exists. Fix $\varepsilon := \frac{\varepsilon_0}{100}$.

Let $\mathcal{F}$ be a CNF encoding of $\mathsf{G\text{-}PHP}^m_n$ as a polynomial system. For the sake of contradiction assume that we have a $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ proof π of size $\exp(\frac{\varepsilon}{2} \cdot \frac{r^2}{\Delta m})$ and hence of q-size $\exp(\varepsilon \frac{r^2}{\Delta m})$.

Fix the parameter $d := \frac{\varepsilon_0}{10} r$. We say that a term t is **fat** if $\mathsf{deg}(t) \geq d$ and let H be the multiset of all fat term in the quadratic representation of the proof π.

The idea of the proof is similar to the proof of Theorem 5.10.

The following algorithm takes a proof π and transforms it into a proof of small degree of a Pigeonhole Principle over a smaller graph. This case is a bit simpler than in section 5.5 since we do not need to take care about $\mathrm{SOS}_{\{\pm 1\}}$.

Algorithm 2 Degree reduction. PHP

1: $R_1 \coloneqq R$ ▷ Set of **alive** holes
2: $L_1 \coloneqq L$ ▷ Set of pigeons that are not yet satisfied
3: $J_1 \coloneqq \emptyset$ ▷ Set of **active** variables
4: $\ell \coloneqq 1$
5: $\pi_1 \coloneqq \pi$
6: $\rho_1 \coloneqq \emptyset$
7: **while** $H \neq \emptyset$ **do**
8:     Pick the most frequent variable $x_{i,j}$ in H.
9:     $J_{\ell+1} \coloneqq J_\ell \cup \{x_{i,j}\}$
10:     $\pi' \coloneqq \mathrm{Split}_{x_{i,j}}(\pi)$
11:     $\rho_{\ell+1} \coloneqq \rho_\ell$
12:     **for** $k \in (N(j) \setminus \{i\})$ **do**
13:         $\rho_{\ell+1} \coloneqq \rho_{\ell+1} \cup (x_{k,j} = \mathrm{False})$
14:     $L_{\ell+1} \coloneqq L_\ell$
15:     $R_{\ell+1} \coloneqq R_\ell \setminus \{j\}$
16:     $B_\ell \coloneqq \max\{B \subseteq L_{\ell+1} \mid |B| \leq r, |\partial_{R_{\ell+1}}(B)| \leq 3|B|\}$
17:     Find a matching M on B_ℓ in $(L_{\ell+1}, R_{\ell+1}, E)$ ▷ Proposition 5.1
18:     **for** $(i', j') \in M$ **do**
19:         $L_{\ell+1} \coloneqq L_{\ell+1} \setminus \{i'\}$
20:         $R_{\ell+1} \coloneqq R_{\ell+1} \setminus \{j'\}$
21:         $\rho_{\ell+1} \coloneqq \rho_{\ell+1} \cup \{x_{i',j'} = \mathrm{True}\}$
22:         **for** $k \in N_{L_{\ell+1}}(j')$ **do**
23:             $\rho_{\ell+1} \coloneqq \rho_{\ell+1} \cup (x_{k,j'} = \mathrm{False})$
24:     $\pi_{\ell+1} \coloneqq \pi' \restriction \rho_{\ell+1}$
25:     $H \coloneqq$ set of fat terms of the quadratic representation of $\pi_{\ell+1}$
26:     $\ell \coloneqq \ell + 1$
return π_ℓ

Note that $\mathrm{Split}_{x_{i,j}}(\pi)$:

- transforms polynomial representation of pigeon axiom for the pigeon i into the polynomial representation of the same axiom without hole j;
- damages hole axioms for hole j;
- does not affect all other axioms.

After $\mathrm{Split}_{x_{i,j}}(\pi)$ operation we assign all variables $x_{k,j}$ to False that sets all "damaged" hole axioms to zero and remove hole j from our graph. Hence at line 14 π' is a proof of G-PHP based on graph without hole j. In the last part we try to restore expansion property on the graph of Pigeonhole Principle after removing hole j. We put some pigeons into holes and remove these pigeons and holes from the graph. Hence in the end of iteration $\pi_{\ell+1}$ will be a proof of G-PHP on graph induced by $L_{\ell+1}$ and $R_{\ell+1}$.

We start with the system $\mathcal{F}$. In each iteration we pick a variable $x_{i,j}$ that appears in at least $\frac{d}{\Delta m}|H|$ fat terms and consider $\mathrm{Split}_{x_{i,j}}(\pi)$. The fact that $\mathrm{Split}_{x_{i,j}}(\pi)$ banishes all terms that contain x allows us to estimate the number of iterations.

Proposition 6.4. $\ell \leq \frac{r}{5}$.

Proof. We kill at least fat $\frac{d}{\Delta m}|H|$ terms. Hence the process will terminate if $(1-\frac{d}{\Delta m})^{\ell}|H| < 1$. $|H|$ is at most the q-size of the proof π and $(1-\frac{d}{\Delta m})^{\ell}|H| \le (1-\frac{d}{\Delta m})^{\ell}\exp(\varepsilon\frac{r^2}{\Delta m}) \le \exp(-\frac{\ell d}{\Delta m}+\varepsilon\frac{r^2}{\Delta m})$ is less than 1 if $\ell d > \varepsilon r^2$. The choice of ε implies the desired result. $\square$

We know that damaged axioms are pigeon axioms that are hit by a partial assignment. If we put all damaged pigeons into alive holes, this assignment will set all damaged axioms to zero. Again, as in case of random formulas, in order to be able to find such an assignment, and keep the formula hard for $\mathrm{PCR}^{\mathbb{F}}$ we polish it after each iteration by a partial assignment that satisfies the set B_i.

The next Proposition is an analogue of Proposition 5.15 in section 5.10 and the proof of this Proposition is the same.

Proposition 6.5. 1. $|C_\ell| \le \ell$.

2. $\forall i \in [\ell], (L_i, R_i, E)$ is an $(r, \Delta, 3)$-boundary expander.

Where $C_i \coloneqq \bigcup_{j=1}^{i} B_j$.

Since (L_i, R_i, E) is an $(r, \Delta, 3)$-boundary expander then $(L_i, R_i \setminus \{x\}, E)$ is an $(r, \Delta, 2)$-boundary expander (we just remove one vertex on the right side). By Proposition 5.1 there is a matching on B_i.

π_ℓ is a proof of the $\mathsf{G\text{-}PHP}$ on a graph that is $(r, \Delta, 3)$-boundary expander. Moreover the quadratic representation of π_ℓ does not contain any fat terms. Hence by Lemma 3.6 the proof π_ℓ can be transformed into a proof of degree at most $2d$ which is a contradiction to the choice of d.

6.3 Separation

Theorem 6.6 (Formalization of 1.3)**.** Let G be an $(r, \Delta, 4)$-boundary expander then:

- there is an $\mathrm{SOS}_{\{0,1\}}$ and $\mathrm{SOS}_{\{\pm 1\}}$-proof of the $\mathsf{G\text{-}PHP}_n^{n+1}$ of size $\mathsf{poly}(n)$;
- any $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ or $\mathrm{PCR}^{\mathbb{F}}_{\{0,1\}}$-proof of $\mathsf{G\text{-}PHP}_n^{n+1}$ has size $\exp(n)$.

Proof. The upper bounds follows from Theorem 6.2 and Lemma 3.7.

For the lower bounds we apply Theorems 6.1 and 6.3 to an $(\Omega(n), \Delta, 4)$-boundary expander. $\square$

7 Concluding Remarks

In this paper we present techniques for proving lower bounds on the algebraic proof systems on the $\{\pm 1\}$ basis. We demonstrate that gadget substitution helps us to transfer the lower bound from degree to size. But this bound was demonstrated only for real numbers (since we can prove it for Sum-of-Squares but can not prove it directly for Polynomial Calculus). It is interesting to do it directly for Polynomial Calculus.

Also we showed the lower bounds for the classical hard formula examples. The main idea of all the results based on the quadratic representation of the proofs. It is interesting to find other applications of this representation and also to study the power of the high-order representations.

Open problems. To develop new techniques it would be interesting to study the size of proofs for concrete formulas.

1. The proof of Theorem 6.3 works only for the basic version of the Pigeonhole Principle. Can we prove lower bounds for Functional or Onto Pigeonhole Principle?
2. Algebraic proof systems over $\{\pm 1\}$ basis are exponentially stronger than proof systems over $\{0, 1\}$ on Tseitin formulas. Can we find the opposite separation? Can we simulate Resolution in $\mathrm{PCR}^{\mathbb{F}}_{\{\pm 1\}}$ or $\mathrm{SOS}_{\{\pm 1\}}$?

Acknowledgements

I would like to thank Kilian Risse, Anastasia Safronova, Edward Hirsch for fruitful discussions and attempts to fix my writing; Jakob Nordström and Shuo Pang for fruitful discussions; Albert Atserias for references; Sasank Mouli, Russell Impagliazzo and anonymous reviewers for helpful comments and pointing out that Lemma 3.6 is not trivial; Igor Shenderovich for the technical assistance at the hospital.

References

[AH19] Albert Atserias and Tuomas Hakoniemi. "Size-Degree Trade-Offs for Sums-of-Squares and Positivstellensatz Proofs". In: *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*. 2019, 24:1–24:20. DOI: 10.4230/LIPIcs.CCC.2019.24. URL: https://doi.org/10.4230/LIPIcs.CCC.2019.24.

[Ajt94] Miklós Ajtai. "The Complexity of the Pigeonhole Principle". In: *Combinatorica* 14.4 (1994), pp. 417–433. DOI: 10.1007/BF01302964. URL: https://doi.org/10.1007/BF01302964.

[Ale+04] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. "Pseudorandom Generators in Propositional Proof Complexity". In: *SIAM J. Comput.* 34.1 (2004), pp. 67–88. DOI: 10.1137/S0097539701389944. URL: https://doi.org/10.1137/S0097539701389944.

[AR03] Michael Alekhnovich and Alexander A. Razborov. "Lower Bounds for Polynomial Calculus: Non-Binomial Case". In: *Proceedings of the Steklov Institute of Mathematics* 242 (2003). Available at http://people.cs.uchicago.edu/~razborov/files/misha.pdf. Preliminary version in *FOCS '01.*, pp. 18–35.

[Bea+94] Paul Beame, Russell Impagliazzo, Jan Krajícek, Toniann Pitassi, and Pavel Pudlák. "Lower Bound on Hilbert's Nullstellensatz and propositional proofs". In: *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. 1994, pp. 794–806. DOI: 10.1109/SFCS.1994.365714. URL: https://doi.org/10.1109/SFCS.1994.365714.

[Ber18] Christoph Berkholz. "The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs". In: *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France*. 2018, 11:1–11:14. DOI: 10.4230/LIPIcs.STACS.2018.11. URL: https://doi.org/10.4230/LIPIcs.STACS.2018.11.

[Bus+01] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. "Linear Gaps between Degrees for the Polynomial Calculus Modulo Distinct Primes". In: *J. Comput. Syst. Sci.* 62.2 (2001), pp. 267–289. DOI: 10.1006/jcss.2000.1726. URL: https://doi.org/10.1006/jcss.2000.1726.

[Bus+97] Samuel R. Buss, Russell Impagliazzo, Jan Krajícek, Pavel Pudlák, Alexander A. Razborov, and Jirí Sgall. "Proof Complexity in Algebraic Systems and Bounded Depth Frege Systems with Modular Counting". In: *Computational Complexity* 6.3 (1997), pp. 256–298. DOI: 10.1007/BF01294258. URL: https://doi.org/10.1007/BF01294258.

[CEI96] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. "Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. 1996, pp. 174–183. DOI: 10.1145/237814.237860. URL: https://doi.org/10.1145/237814.237860.

[CR79] Stephen Cook and Robert Reckhow. "The Relative Efficiency of Propositional Proof Systems". In: *Journal of Symbolic Logic* 44.1 (Mar. 1979), pp. 36–50. URL: https://projecteuclid.org:443/euclid.jsl/1183740343.

[CS88] Vašek Chvátal and Endre Szemerédi. "Many Hard Examples for Resolution". In: *J. ACM* 35.4 (Oct. 1988), pp. 759–768. ISSN: 0004-5411. DOI: 10.1145/48014.48016. URL: http://doi.acm.org/10.1145/48014.48016.

[GH03] Dima Grigoriev and Edward A. Hirsch. "Algebraic proof systems over formulas". In: *Theor. Comput. Sci.* 303.1 (2003), pp. 83–102. DOI: 10.1016/S0304-3975(02)00446-2. URL: https://doi.org/10.1016/S0304-3975(02)00446-2.

[GHP02] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. "Complexity of semi-algebraic proofs". In: *Mosc. Math. J.* 2.4 (2002), pp. 647–679, 805. ISSN: 1609-3321. DOI: 10.17323/1609-4514-2002-2-4-647-679. URL: https://doi.org/10.17323/1609-4514-2002-2-4-647-679.

[GK18] Michal Garlík and Leszek Aleksander Kołodziejczyk. "Some Subsystems of Constant-Depth Frege with Parity". In: *ACM Trans. Comput. Log.* 19.4 (2018), 29:1–29:34. DOI: 10.1145/3243126. URL: https://doi.org/10.1145/3243126.

[GMT09] Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. "Optimal Sherali-Adams Gaps from Pairwise Independence". In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Ed. by Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 125–139. ISBN: 978-3-642-03685-9.

[GP18] Joshua A. Grochow and Toniann Pitassi. "Circuit Complexity, Proof Complexity, and Polynomial Identity Testing: The Ideal Proof System". In: *J. ACM* 65.6 (2018), 37:1–37:59. DOI: 10.1145/3230742. URL: https://doi.org/10.1145/3230742.

[Gri01] Dima Grigoriev. "Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity". In: *Theoretical Computer Science* 259.1 (2001), pp. 613–622. ISSN: 0304-3975. DOI: https://doi.org/10.1016/S0304-3975(00)00157-2. URL: http://www.sciencedirect.com/science/article/pii/S0304397500001572.

[Gri98] Dima Grigoriev. "Tseitin's Tautologies and Lower Bounds for Nullstellensatz Proofs". In: *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*. 1998, pp. 648–652. DOI: 10.1109/SFCS.1998.743515. URL: https://doi.org/10.1109/SFCS.1998.743515.

[GV01] Dima Grigoriev and Nicolai Vorobjov. "Complexity of Null- and Positivstellensatz proofs". In: *Annals of Pure and Applied Logic* 113.1 (2001). First St. Petersburg Conference on Days of Logic and Computability, pp. 153–160. ISSN: 0168-0072. DOI: https://doi.org/10.1016/S0168-0072(01)00055-0. URL: http://www.sciencedirect.com/science/article/pii/S0168007201000550.

[IMP19] Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. "The Surprising Power of Constant Depth Algebraic Proofs". In: *Electronic Colloquium on Computational Complexity (ECCC)* 26 (2019), p. 24. URL: https://eccc.weizmann.ac.il/report/2019/024.

[IPS99] Russell Impagliazzo, Pavel Pudlák, and Jirí Sgall. "Lower Bounds for the Polynomial Calculus and the Gröbner Basis Algorithm". In: *Computational Complexity* 8.2 (1999), pp. 127–144. DOI: 10.1007/s000370050024. URL: https://doi.org/10.1007/s000370050024.

[IS19] Dmitry Itsykson and Dmitry Sokolov. "Resolution over linear equations modulo two". In: *Annals of Pure and Applied Logic* (2019), p. 102722. ISSN: 0168-0072. DOI: https://doi.org/10.1016/j.apal.2019.102722. URL: http://www.sciencedirect.com/science/article/pii/S0168007219300855.

[Kra97] Jan Krajícek. "Lower Bounds for a Proof System with an Expentential Speed-up over Constant-Depth Frege Systems and over Polynomial Calculus". In: *Mathematical Foundations of Computer Science 1997, 22nd International Symposium, MFCS'97, Bratislava, Slovakia, August 25-29, 1997, Proceedings*. 1997, pp. 85–90. DOI: 10.1007/BFb0029951. URL: https://doi.org/10.1007/BFb0029951.

[MN15] Mladen Miksa and Jakob Nordström. "A Generalized Method for Proving Polynomial Calculus Degree Lower Bounds". In: *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*. 2015, pp. 467–487. DOI: 10.4230/LIPIcs.CCC.2015.467. URL: https://doi.org/10.4230/LIPIcs.CCC.2015.467.

[Pit96] Toniann Pitassi. "Algebraic Propositional Proof Systems". In: *Descriptive Complexity and Finite Models, Proceedings of a DIMACS Workshop 1996, Princeton, New Jersey, USA, January 14-17, 1996*. 1996, pp. 215–244. DOI: 10.1090/dimacs/031/07. URL: https://doi.org/10.1090/dimacs/031/07.

[Pit98] Toniann Pitassi. "Unsolvable Systems of Equations and Proof Complexity". In: *Proceedings of the International Congress of Mathemeticians*. Vol. III. 1998, pp. 451–460.

[PT18] Fedor Part and Iddo Tzameret. "Resolution with Counting: Lower Bounds over Different Moduli". In: *CoRR* abs/1806.09383 (2018). arXiv: 1806.09383. URL: http://arxiv.org/abs/1806.09383.

[Raz87] Alexander Razborov. "Lower bounds on the size of bounded depth circuits over a complete basis with logical addition". In: *Mathematical Notes* (4 1987), pp. 333–338.

[RT08] Ran Raz and Iddo Tzameret. "Resolution over linear equations and multilinear proofs". In: *Ann. Pure Appl. Logic* 155.3 (2008), pp. 194–224. DOI: 10.1016/j.apal.2008.04.001. URL: https://doi.org/10.1016/j.apal.2008.04.001.

[Smo87] Roman Smolensky. "Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity". In: *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*. 1987, pp. 77–82. DOI: 10.1145/28395.28404. URL: https://doi.org/10.1145/28395.28404.

[Vad12] Salil P. Vadhan. *Pseudorandomness*. Hanover, MA, USA: Now Publishers Inc., 2012. ISBN: 1601985940, 9781601985941.

A Missed Proofs

A.1 Proposition 5.15

At first note a simple auxiliary statement.

Lemma A.1. Suppose that $G \coloneqq (L, R, E)$ is an (r, Δ, c)-boundary expander and that $J \subseteq R$ has size $|J| \leq \Delta r$. Then if $X \subseteq L$ has size $|X| \leq r$ and $|\partial X \setminus J| \leq \nu |X|$ then $X < \frac{|J|}{c-\nu}$.

Proof. The expansion property of the graph guarantees that $c|X| - |J| \leq |\partial X \setminus J|$. The conclusion follows. $\square$

Proposition 5.15. 1. $|C_\ell| \leq \ell$.

2. $\forall i \in [\ell], G^{A_i}_{\varphi\restriction\rho_i}$ is an $(r, \Delta, 3)$-boundary expander.

Proof. At first by induction on i we show that $|C_i| \leq \ell$. $C_0 = \emptyset$. Assume that $|C_{i-1}| \leq \ell$.

Note that ρ_{i-1} assign only variables from $N_{G_\varphi}(C_{i-1})$ that implies that right part of G_i is a superset of $X \setminus \big(N_{G_\varphi}(C_{i-1}) \cup J_\ell\big)$. Hence $|\partial_{G_\varphi} B_i \setminus N_{G_\varphi}(C_{i-1}) \cup J_\ell| \leq |\partial_{G_i} B_i| \leq 3|B_i|$. By definition $|B_i| \leq r$ hence by Lemma A.1 $|B_i| \leq |N_{G_\varphi}(C_{i-1}) \cup J_\ell| \leq 2\Delta |J_\ell| \frac{2}{5} r$ and $|C_i| \leq \frac{3}{5} r$.

By analogy with previous expression: $\partial_{G_\varphi} C_i \subseteq \bigcup\limits_i \partial_{G_i} B_i \cup J_\ell$, but:

$$\begin{aligned} 4|C_i| &\leq \\ |\partial_{G_\varphi} C_i| &\leq && \text{by expansion} \\ \sum_{j=1}^{i} |\partial_{G_j} B_j| + |J_\ell| &\leq \\ 3\sum_{j=1}^{i} |B_j| + |J_\ell| &\leq && \text{by the choice of } B_i \\ 3|C_i| + |J_\ell| & && \text{since all } B_j \text{ are disjoint} \end{aligned}$$

Thus $|C_i| \leq |J_\ell| = \ell$ as desired.

We prove the second item by contradiction. Pick the minimal i such that $G \coloneqq G^{A_i}_{\varphi\restriction\rho_i}$ is not an $(r, \Delta, 3)$-boundary expander and S be a subset of its left part of size $|S| \leq r$ such that $|\partial_G S| \leq 3|S|$. As in previous case $|\partial_{G_\varphi} S \setminus \big(N_{G_\varphi}(C_{i-1}) \cup J_\ell\big)| \leq |\partial_G S| \leq 3|S|$ hence by Lemma A.1 $|S| \leq \Delta \ell + 1 \leq \frac{2}{5} r$.

Consider a set $S \cup B_{i-1}$ and note that size of it at most r. $\partial_{G_{i-1}}(S \cup B_{i-1}) \subseteq \partial_{G_i} S \cup \partial_{G_{i-1}} B_{i-1}$ since $\mathrm{Vars}(\rho_i) \setminus \mathrm{Vars}(\rho_{i-1}) \subseteq \partial_{G_{i-1}} B_{i-1}$. This implies $|\partial_{G_{i-1}}(S \cup B_{i-1})| \leq 3|S_i| + 3|B_{i-1}| = 3|S_i \cup B_{i-1}|$. That contradicts with the choice of B_{i-1}. $\square$

A.2 Theorem 4.4

Theorem 4.4. [Analogue of [Ber18]] Let $\mathcal{F}$ be a system of polynomial equations. If there is a $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proof of $\mathcal{F}$ of size S and degree d then there is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of size $\mathsf{poly}(S)$ and degree $2d$.

Proof. Let $p_1, p_2, \ldots, p_a$ be a Polynomial Calculus proof of $\mathcal{F}$ of size S. We construct by induction on i an $\mathrm{SOS}_{\{\pm 1\}}$-derivation of $-p_i^2$ from $\mathcal{F}$. More formally, we represent each p_i in a following way:

$$\sum_{f \in \mathcal{F}} (-a_{i,f} f) f + \sum_{v=1}^{i} c_{i,v} q_v^2 = -p_i^2$$

where $a_{i,f}, c_{i,v} \in \mathbb{R}$ and $c_{i,v} \geq 0$.

If $p_i \in \mathcal{F}$ then $-p_i^2$ is already in this form. If $p_i \coloneqq x_\ell p_j$ for some $j < i$ then $p_i^2 = p_j^2$ hence we consider factor field over range axioms. Representation of p_j is a representation of p_i. The remaining case $p_i \coloneqq \alpha p_j + \beta p_k$ for some $j, k < i$. By induction we have:

$$\sum_{f \in \mathcal{F}} (-a_{j,f} f) f + \sum_{v=1}^{j} c_{v,j}^2 q_v^2 = -p_j^2$$

$$\sum_{f \in \mathcal{F}} (-a_{k,f} f) f + \sum_{v=1}^{k} c_{v,k}^2 q_v^2 = -p_k^2$$

Let $a'_f \coloneqq \alpha^2 a_{j,f} + \beta^2 a_{k,f}$ and $c'_v \coloneqq \alpha^2 c_{v,j} + \beta^2 c_{v,k}$, hence:

$$\sum_{f \in \mathcal{F}} (-a'_f f) f + \sum_{v=1}^{i-1} c'_v q_v^2 = -(\alpha p_j)^2 - (\beta p_k)^2$$

Note that $-p_i^2 = -(\alpha p)_j^2 - 2\alpha\beta p_j p_k - (\beta p_k)^2$. Let $q_i \coloneqq \alpha p_j - \beta p_k$ then:

$$-2(\alpha p_j)^2 - 2(\beta p_k)^2 + q_i^2 = -(\alpha p_j)^2 - 2\alpha\beta p_j p_k - (\beta p_k)^2 = -p_i^2$$

and hence

$$\sum_{f \in \mathcal{F}} (-2a'_f f) f + \sum_{v=1}^{i-1} 2c'_v q_v^2 + q_i^2 = -p_i^2$$

that is desired representation.

Since $p_a = 1$ this representation for $-p_a^2$ is an $\mathrm{SOS}_{\{\pm 1\}}$-proof of $\mathcal{F}$. To conclude the proof note that at each iteration we add at most one polynomial that is square of linear combination of two polynomials from $\mathrm{PCR}^{\mathbb{R}}_{\{\pm 1\}}$-proof. Hence the size of the $\mathrm{SOS}_{\{\pm 1\}}$-proof is at most $\mathsf{poly}(S)$. $\square$

A.3 Lemma 5.7

Lemma 5.7. If $m = O(n)$, $\Delta > 11$ and $\varphi \sim \varphi(m, n, \Delta)$ then whp G_φ is an $(r, \Delta, 5)$-boundary expander where $r = \Omega(\frac{n}{\Delta})$.

Proof. Let $m \coloneqq Kn$. Fix $r \coloneqq \frac{1}{10^4 K} \frac{n}{\Delta}$ and $c \coloneqq \frac{\Delta+5}{2} \leq \frac{3}{4}\Delta$. Let $G_\varphi \coloneqq (L, X, E)$. We first estimate the probability that a set $S \subseteq R$ of size at most r violates the boundary expansion. This probability can be bounded by:

$$\begin{aligned}
\Pr[|\partial S| < 5s] &\leq \Pr\left[|N(S)| < \left(\frac{\Delta - 5}{2} + 5\right) s\right] \\
&\leq \binom{n}{cs} \cdot \left(\frac{\binom{cs}{\Delta}}{\binom{n}{\Delta}}\right)^s \\
&\leq \binom{n}{cs} \cdot \left(\frac{cs}{n}\right)^{\Delta s} \\
&\leq \left(\frac{ne}{cs}\right)^{cs} \cdot \left(\frac{cs}{n}\right)^{\Delta s} \\
&\leq \left(\left(\frac{100cs}{n}\right)^{\Delta - c}\right)^s,
\end{aligned}$$

where $s := |S|$.

Hence the probability that G_φ is not a boundary expander can be bounded by:

$$\begin{aligned}
\Pr[G \text{ is not an expander}] &\leq \sum_{s=1}^{r} \binom{m}{s} \left(n^{c-\Delta}(cs)^{\Delta-c}e^{c}\right)^{s} \\
&\leq \sum_{s=1}^{r} \left(\frac{Kne}{s}\left(\frac{100cs}{n}\right)^{\Delta-c}\right)^{s} \\
&\leq \sum_{s=1}^{r} \left(cK\left(\frac{100cs}{n}\right)^{\Delta-c-1}\right)^{s} \\
&\leq \sum_{s=1}^{\sqrt{n}} \left(cK\left(\frac{100cs}{n}\right)^{\Delta-c-1}\right)^{s} + \sum_{s=\sqrt{n}+1}^{r} \left(cK\left(\frac{100cs}{n}\right)^{\Delta-c-1}\right)^{s} \\
&\leq \sum_{s=1}^{\sqrt{n}} \left(cK\left(\frac{100\Delta}{\sqrt{n}}\right)^{\Delta-c-1}\right)^{s} + \sum_{s=\sqrt{n}+1}^{r} \left(cK\left(\frac{100cs}{n}\right)^{\Delta-c-1}\right)^{s} \\
&\leq O\left(\frac{1}{\sqrt{n}}\right) + \sum_{s=\sqrt{n}+1}^{r} \left(cK\left(\frac{1}{10K}\right)^{\Delta-c-1}\right)^{s} \\
&\leq O\left(\frac{1}{\sqrt{n}}\right) + \exp(-\sqrt{n})
\end{aligned}$$

□

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il