Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 41 (2007)

Extending Polynomial Calculus with k-DNF Resolution

Nicola Galesi galesi@di.uniroma1.it
Massimo Lauria lauria@di.uniroma1.it

Dipartimento di Informatica
Sapienza - Universitá di Roma

Abstract

We consider two well-known algebraic proof systems: *Polynomial Calculus* (PC) and *Polynomial Calculus with Resolution* (PCR), a system introduced in [2] which combines together PC and Resolution.

Moreover we introduce an algebraic proof system PCR_k, which combines together *Polynomial Calculus* (PC) and *k-DNF Resolution* (RES_k). This is a natural generalization to RES_k of PCR.

In the paper we study the complexity of proofs in such systems.

First we prove that a set of polynomials encoding a *Graph Ordering Principle* ($\text{GOP}(G)$) requires PCR refutations of degree $\Omega(n)$. This is the first linear degree lower bound for PCR refutations for ordering principles. This result immediately implies that the size-degree tradeoff for PCR Refutations of Alekhnovich *et al.* [3] is optimal, since there are polynomial size PCR refutations for $\text{GOP}(G)$.

We then study the complexity of proofs in PCR_k, extending to these systems the lower bounds known for RES_k:

- we prove that random 3-CNF formulas with a linear number of clauses are hard to prove in PCR_k (over a field with characteristic different from 2) as long as k is in $o(\sqrt{\log n/\log\log n})$. This is the strongest daglike system where 3-CNF formulas are hard to prove.
- Moreover we prove a strict hierarchy result showing that PCR_{k+1} is exponentially stronger than PCR_k.

1 Introduction

Algebraic proof systems were studied for the first time in the context of Proof Complexity by Beame et al. in [7], where they introduce a refutational system based on the Hilbert Nullstellensatz. Later, Clegg et al. in [15] defined a more natural algebraic proof system, called Polynomial Calculus (PC) and based on deriving elements of the ideal generated from a set of given polynomials.

These systems have great importance for two reasons. First they generalize the well-studied, used and known boolean system of Resolution. Second because of the applications in the field of automatic generation of proofs that well-known algorithms, like the Gröbner Basis Algorithm, can have. One of the main problem arising in proof complexity is that of proving degree lower bounds for these systems. The work of Razborov [21] proving linear degree lower bounds for the Pigeonhole principle in PC was followed by several other important results [9, 12, 5, 20] proving degree lower bounds also for random formulas, which is one of the prominent class of formulas proved to be hard in many systems.

The PC system was extended in [2, 3] to a system combining together the strength of Resolution and PC called Polynomial Calculus with Resolution, PCR. Since in this system clauses can be translated directly to monomials, then the *width* of a clause (i.e. the number of literals) in Resolution has its counterpart in the degree in PCR. This system has been also well studied. Several degree lower bounds have been proved for random formulas and for a more general class of contradictions arising from pseudorandom generators [3, 20]. It is important to notice that the well known tradeoff between number

ISSN 1433-8092

of clauses and width, found for Resolution by Ben-Sasson and Wigderson in [10], has its counterpart in the tradeoff between number of monomials and degree in PCR found by Alekhnovich, Ben-Sasson, Razborov and Wigderson in [3].

The Resolution system was extended by Krajíček in [19] to a system, called k-DNF Resolution (RES$_k$), where instead of clauses we have the power of deriving k-DNFs, i.e. disjunctions of k-conjunctions. Although a subsystem of bounded depth Frege, where we already know lower bounds for the Pigeon Hole principle [8], RES$_k$ has a lot of importance. It is a natural extension of resolution and moreover is a powerful system to experiment new techniques to prove lower bounds for random formulas, whose complexity in bounded depth Frege is still unknown. Indeed lower bounds for random 3-CNF formulas had been firstly proved for RES$_2$ in [6]. Then a lower bound for random $O(k^2) - CNF$ in RES$_k$ was proved in [23]. Finally a random 3-CNF lower bound in RES$_k$ was proved for $k = o(\sqrt{\log n / \log\log n})$ in [1]. Moreover Segerlind et al. in [23] proved a strict hierarchy result, finding family of contradictions requiring exponential size in RES$_k$ but provable in polynomial size in RES$_{k+1}$.

In this paper we generalize the PCR system, defining the system PCR$_k$ which combines the strength of PC and that of RES$_k$. Exactly as in PCR monomials succinctly represent clauses, in PCR$_k$ we generalize monomials to k-monomials in such a way to succinctly represent k-DNFs. Then we define k-polynomials as linear combinations of k-monomials. As the role of the degree is the same for PC and PCR refutations, we have that in PCR$_k$ the degree of a refutation is essentially the same as in PC or PCR. In this paper we investigate if k-monomials allow to refute more efficiently than PC and PCR.

First we prove that PCR$_k$ is a natural generalization of RES$_k$ showing that any RES$_k$ refutation can be simulated efficiently in number of k-monomials in PCR$_k$.

To study the complexity of proofs in PCR$_k$ we follow the approach used by Segerlind et al. in [23] to prove RES$_k$ lower bounds. We can easily adapt their Switching Lemma to transform k-DNFs into low height decision trees, into an analogous Switching Lemma to transform k-monomials into multilinear polynomials of low degree. So exactly as Segerlind et al. in [23] can reduce lower bounds for RES$_k$ to width lower bounds in Resolution, we can reduce lower bounds on the number of k-monomials in PCR$_k$ to degree lower bounds in PC or PCR.

Using Segerlind's et al. Switching Lemma [23], Alekhnovich [1] was able to get exponential lower bounds for RES$_k$ refutations of random 3-CNF. We apply the technique used by Alekhnovich to PCR$_k$. Using a PCR degree lower bound for certain encodings of systems of linear equations developed in [3], we get that with high probability (as long as $k = o(\sqrt{\log n / \log\log n})$), any PCR$_k$ (over a field with characteristic different from 2) refutation of random 3-CNF over a linear number of clauses requires an exponential number of k-monomials. Lower bounds for PCR$_k$ can be also obtained (but only for certain counting principles) by a result of Krajíček in [18] proving lower bounds for a stronger system. Nevertheless our result give the strongest daglike system for which we can prove hardness of refuting random 3-CNF's.

In analogy with RES$_k$, we then approach the question of proving a strict hierarchy result for PCR$_k$ too. Together with the switching lemma, the main part of the RES$_k$ hierarchy separation in [23] was proving that a family of contradictions arising from a graph ordering principle is refutable in polynomial size but always demands high width in Resolution. This example is a generalization of the GT contradiction of [11] proving that the size-width tradeoff for Resolution is optimal. While for Resolution this optimality is known, that is not the case for the analogous tradeoff between size and degree for PCR found in [3].

Our first step towards the PCR$_k$ hierarchy separation is then that of proving the optimality of the size-degree tradeoff for PCR, i.e. finding a family of contradictions admitting PCR refutations with a polynomial number of monomials, but always requiring high degree. We use a slight modification of the graph ordering principle GOP(G) of [23], and we get the expected result when G has good vertex expansion properties. To prove the lower bound we follow the method, invented by Razborov in [21]

and refined in [5], of finding a linear operator which sets to true all the consequence of a given set of polynomials derivable in low degree. It should be noticed that the Razborov's technique so far was applied and worked for "matching-like" examples of formulas as the Pigeonhole formulas, random CNF's, etc. [21, 20, 3, 5]. We extend the use of this technique also to other examples of formulas, giving a stronger evidence that whenever we have width lower bounds in Resolution, we also have degree lower bounds in PCR (at least for certain polynomial encodings of formulae).

With this result in hand we then can use our version of the switching lemma and follow the approach of Segerlind et al in [23] to prove the desired PCR_k hierarchy exponential separation.

The paper is organized as follows. In Section2 we give the preliminary definitions and define all the known proof system we cite and use in the paper. In section 3 we introduce the PCR_k proof system, we show its relation with other systems and we prove the switching lemma we use in the paper. In Section 4 we prove the lower bounds for random 3-CNFs. In Section 5 we introduce our graph ordering principle and prove a degree lower bounds in PCR. Finally in Section 6 we prove the exponential separation between PCR_k and PCR_{k+1}.

Notice that Section 4 is added for completeness: although differently organized, a big part of it is already contained in the paper of Alekhnovich [1]. We added some parts not contained there or that we found should have been slightly modified. Section 5 can be read independently from the rest after the Preliminaries section.

2 Preliminaries

Let V be a set of boolean variables. A literal l is either a variable x or is negation $\bar{x}$. A *k-clause* is a disjunction of at most k literals; a *k-term* is a conjunction of at most k-literals. A boolean formula F is a k-CNF if it is a conjunction of k-clauses; it is a k-DNF if it is the disjunction of k-terms. If we omit k we have no bounds on the number of literals in clauses or terms. The *width* of a clause is the number of literals in the clause. $Vars(F)$ denotes the set of variables occurring in F. An assignment to a formula F is a mapping $\rho : Vars(F) \to \{0, 1\}$. A partial assignment to F is a mapping $\rho : Vars(F) \to \{0, 1, *\}$; we let $Dom(\rho)$ to be $\rho^{-1}(\{0, 1\})$. Given a restriction ρ for F by $F \restriction_\rho$ we denote the formula obtained from F after setting all the variables in $Dom(\rho)$ according to ρ, simplifying F in the standard way and leaving all the other variables unassigned.

Given a field $\mathbb{F}$, we consider polynomials over $\mathbb{F}[x_1, \ldots, x_n]$. Given a set $E = \{f_1, \ldots, f_n\}$ of polynomials, by $Span(E)$ we denote the ideal generated by E, that is the set $\{ \sum_i (f_i \cdot h_i) \mid h_i \in \mathbb{F}[x_1, \ldots, x_n]\}$. Polynomials will be always evaluated on $\{0, 1\}$ assignments. We extend the notions of assignment, restriction and domain from boolean formulas to polynomials. We say that a set of polynomials $f_1, \ldots, f_n$ *semantically implies* a polynomial g if any $\{0, 1\}$ assignment that satisfies $f_i = 0$ for all $i \in [n]$, also satisfies $g = 0$. We write $f_1, \ldots, f_n \models g$. Notice that if $g \in Span(E \cup \{x_i^2 - x_i\}_{i\in[n]})$, then $E \models g$.

2.1 Proof systems

The *Polynomial Calculus* (PC) is a refutational system, defined in [15], and based on the ring $\mathbb{F}[x_1, \ldots, x_n]$ of polynomials. We always assume equations of the form $p = 0$ so we refers only to p. To restrict the polynomials to be evaluated only on $\{0, 1\}$, the system contains the following axioms:

$$x_i^2 - x_i, \quad i \in [n]$$

Moreover it has two rules. For any $\alpha, \beta \in \mathbb{F}$, p, q polynomials and variable x:

$$\frac{p \qquad q}{\alpha p + \beta q} \quad \textit{Scalar Addition} \qquad \frac{p}{xp} \quad \textit{Multiplication}$$

A PC proof of a polynomial g from a set of initial polynomials $f_1, \ldots, f_m$ (denoted by $f_1, \ldots, f_m \vdash g$) is a sequence of polynomials where each one is either an initial one, or a an axiom, or is obtained applying one of the rules to previously derived polynomials. A PC refutation is a proof of the polynomial 1.

Observe that a polynomial g has a PC proof from a set E of polynomials iff $g \in Span(E \cup \{x_i^2 - x_i\}_{i\in[n]})$. Moreover E has no common $\{0,1\}$ solutions (we call E contradictory) iff $1 \in Span(E \cup \{x_i^2 - x_i\}_{i\in[n]})$ and in particular if $E \models g$, then $E \vdash g$ (see Theorem 5.2 in [13]).

Given a PC proof Π, the *degree* of Π, $deg(\Pi)$, is the maximal degree of a polynomial in the proof; the *size* of Π, $S(\Pi)$, is the number of monomials in the proof, the *length* of Π, $|\Pi|$, is the number of lines in the proof.

Polynomial Calculus with Resolution (PCR) [3] is a refutational system which extends PC to polynomials in the ring $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, where $\bar{x}_1, \ldots, \bar{x}_n$ are new formal variables. PCR includes the axioms and rules of PC plus a new set of axioms defined by

$$1 - x_i - \bar{x}_i \quad i \in [n]$$

to force $\bar{x}$ variables to have the opposite values of x variables.

We extend to PCR the definitions of proof, refutation, degree, size and length given for PC. Observe that using the linear transformation $\bar{x} \mapsto 1 - x$, any PCR refutation can be converted into a PC refutation without increasing the degree. Notice that such transformation could increase the size exponentially. Moreover PCR efficiently simulates RES with refutations of degree equals to the width of the original RES proof.

Resolution on k-DNF (RES_k) [19] is a sound and complete refutational system which extends *Resolution* (RES) to k-DNFs. The rules are the following ones:

$$\frac{A}{A \vee l} \quad \textit{Weakening} \qquad \frac{A \vee l_1 \quad \cdots \quad A \vee l_j}{A \vee \bigwedge_{i=1}^{j} l_i} \quad \wedge\textit{-intro}, 1 < j \leq k$$

$$\frac{A \vee \bigwedge_{i=1}^{j} l_i}{A \vee l_i} \quad \wedge\textit{-elim}, 1 < j \leq k \qquad \frac{A \vee \bigwedge_{i=1}^{j} l_i \quad B \vee \bigvee_{i=1}^{j} \neg l_i}{A \vee B} \quad \textit{Cut}, 1 < j \leq k \tag{1}$$

A *proof* of a k-DNF G from a set of clauses F, is a sequence of k-DNFs where each one is either an axiom of RES_k, or a clause in F, or is derived by one of the rule from two previously derived k-DNFs. A *refutation* of F is proof of the empty disjunction. Let Π be a RES_k proof. Then the *size* of Π, $S(\Pi)$, is the total number of symbols appearing in Π. The *length* of Π, $|\Pi|$, is the number of lines in the sequence defining Π.

2.2 Notions from commutative algebra

We are going to define a notion of reminder on polynomials with respect to an ideal. We consider the *grlex* order $<_{\mathbb{P}}$ on monomials as given in [16]. In particular *grlex* is monotone with respect to the product and satisfies the property that if $deg(t_1) < deg(t_2)$, then $t_1 <_{\mathbb{P}} t_2$. $<_{\mathbb{P}}$ can be extended easily to polynomials (see [16]).

Given a polynomial q, we define $R_E(q)$ as the minimal, with resepct to $<_{\mathbb{P}}$, polynomial p such that $q - p \in Span(E)$.

$$R_E(q) = \min\{p \in \mathbb{F}[x_1, \ldots, x_n] \ : \ q - p \in Span(E)\}$$

In the following sections we use some properties of the operator R_E which can be easily derived from the definition:

Property 1. *Let E be a set of polynomials and let p and q be two polynomials. Then:*

- $R_E(p) \leq_{\mathbb{P}} p$;
- *if* $p - q \in Span(E)$, *then* $R_E(p) = R_E(q)$;
- R_E *is a linear operator;*
- $R_E(pq) = R_E(p \cdot R_E(q))$.

Notice that when the polynomials $\{x_i^2 - x_i\}_{i\in[n]} \subseteq E$, then, by minimality, $R_E(q)$ is multilinear. We remark here that when we work in Polynomial Calculus, we implicitly assume to have such polynomials always included in the set E. When p is multilinear and $\{x_i^2 - x_i\}_{i\in[n]} \subseteq E$, $R_E(p)$ is the same polynomial given by the operator R_E of Alekhnovich and Razborov in [5].

3 PCR$_k$, degree complexity and switching lemma

PCR combines Resolution with PC. The strength of PCR with respect to PC is the ability of representing a clause with only one monomial. We want PCR$_k$ to be a system that combines RES$_k$ with PC and manages succint representations of k-DNF.

We introduce the notion of k-*monomials*, which are algebraic representations of k-DNFs obtained as products of variables in $V = \{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ and expressions of the form $(1 - \prod_{i=1}^{j} y_i)$ with $0 \leq j \leq k$ and $y_i \in V$, where the product of 0 variables is intended to be 1. An example of a 3-monomial is: $x_3\bar{x}_2(1-\bar{x}_5x_2)x_4(1-x_1\bar{x}_2x_3)$. *k-polynomials* are linear combinations of k-monomials.

k-monomials algebraically represent k-DNFs by the following sintactical transformation

$$\prod_i l_i \cdot \prod_j \left(1 - \prod_{i=1}^{k_j} l_i\right) \longleftrightarrow \bigvee_i \bar{l}_i \vee \bigvee_j \left(\bigwedge_{i=0}^{k_j} l_i\right)$$

Notice that this transformation is a essentially a bijection modulo the fact that a one variable term x in a k-DNF can be equivalently mapped either to $\bar{x}$ or $(1 - x)$.

The axioms of PCR$_k$ includes those of PCR plus axioms

$$1 - y_1y_2 \cdots y_j - (1 - y_1y_2 \cdots y_j) \text{ for } j \leq k, y_i \in V$$

which introduce syntactical parentheses and allow to work with k-polynomials.

Analogously, the rules of PCR$_k$ are those of PCR with one more rule to deduce k-polynomials

$$\frac{p}{(1 - y_1 \cdots y_j)p} \text{ for } j \leq k, y_i \in V$$

A PCR$_k$ proof of a k-polynomial g from k-polynomials $f_1, \ldots, f_n$ (denoted by $f_1, \ldots, f_n \vdash_k g$) is a sequence of k-polynomials ended by g, each one obtained from either an axiom or by applying a rule to previously derived k-polynomials. In particular a PCR$_k$ *refutation* is a proof of 1.

Given a k-polynomial p, let p^* be the polynomial obtained expanding the parenthesis in p. The degree of a k-polynomial $deg(p)$ is defined as $deg(p^*)$. Let Π be a refutation in PCR$_k$. The *degree* $deg(\Pi)$ af Π is the maximal degree of a k-polynomial used in Π. The *size* $S(\Pi)$ is the total number of k-monomials used in the proof Π. The *length* $|\Pi|$ is the number of lines.

Given a k-polynomial p, it is possible to derive its equivalence with p^* in PCR$_k$.

Fact 1. *For any k-polynomial p we have $\vdash_k p - p^*$.*

As an immediate corollary and by the completeness of PCR, we get the completeness of PCR_k. Indeed $f_1, \ldots, f_n \models g$ imply $f_1^*, \ldots, f_n^* \models g^*$, and, by PCR completeness $f_1^*, \ldots, f_n^* \vdash g^*$ and finally, using previous lemma, $f_1, \ldots, f_n \vdash_k g$.

Applying the transformation $(1 - x) \mapsto \bar{x}$, we can define an homomorphism from 1-polynomials into polynomials, which moreover maps PCR_1 proofs into PCR proofs without increasing degree, size and length.

From the previous observation PCR_k efficiently simulates RES, PC, PCR and by the next lemma also RES_k.

Lemma 1. *Let Π be a RES_k refutation of a CNF F. Let p_F be the set of polynomials arising from the polynomial translation of F. Then there is a PCR_k refutation Γ of p_F such that $S(\Gamma) = O(2^k S(\Pi)^{O(1)})$*

Proof. We refer to names and notation of RES_k rules given in preliminaries (see (1)). Weakening rule is simulated by multiplication rule. For the other three rules consider the case in which A and B are empty DNFs. By completeness these rules can be easily simulated in size $O(2^k)$ because they involve at most k original variables. Consider now non-empty k-DNFs A, B and the corresponding k-monomials m_A, m_B. Observe that if $p_1, \cdots p_l \vdash_k q$ then $m_A p_1, \cdots m_A p_l \vdash_k m_A q$ in the same size. Also if $p_1, p_2 \vdash_k q$ then $m_A p_1, m_B p_2 \vdash_k m_A m_B p_1, m_A m_B p_2 \vdash_k m_A m_B q$ in size equal to the original plus to the number of factors of m_A and m_B. □

3.1 Degree complexity for k-polynomials

Given a boolean function f on $x_1, \ldots, x_n$, with values in a field $\mathbb{F}$, we denote as $\tilde{f}$ the multilinear polynomial on $x_1, \ldots, x_n$ which evaluates as f on all boolean assignments. This polynomial exists and is unique (see [24, 13]).

Definition 1. *Given a boolean partial assignment ρ over $\{x_1, \ldots, x_n\}$, we define its* extension *ρ^e over $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ as follows: for each $x \in \rho^{-1}(\{0,1\}) : \rho^e(\bar{x}) = 1 - \rho(x)$, and for each $x \in \rho^{-1}(\{*\}) : \rho^e(\bar{x}) = *$.*

A k-polynomial p over $\{x_1, \ldots, x_n, \bar{x_1}, \ldots, \bar{x}_n\}$, computes a boolean function f_p over $\{x_1, \ldots, x_n\}$ defined in such a way that for all total assignment ρ over $\{x_1, \ldots, x_n\}$, $f \restriction_\rho = p \restriction_{\rho^e}$. $\tilde{f_p}$ is the *multilinear representation over* $\{x_1, \ldots, x_n\}$ of the k-polynomial p. We will write $\tilde{p}$ instead of $\tilde{f_p}$. Notice that over $\{x_1, \ldots, x_n\}$ the multilinear representaion of a k-polynomial p is unique.

Definition 2. *The* degree complexity *$DC(p)$ of a k-polynomial p is the degree of $\tilde{p}$.*

A boolean *decision tree* over $\{x_1, \ldots, x_n\}$ as a binary tree structure where each internal node is labelled by a variable, the leaves are labelled with values from a field $\mathbb{F}$, the outgoing edges of a node are labelled respectively with 0 and 1, and in each path from the root to a node each variable appears at most once. The height $ht(T)$ of a tree T is the length of the longest path in T. Each path from the root to a node defines a partial boolean assignment on $\{x_1, \ldots, x_n\}$ in the usual way. So a decision tree computes a boolean function f with values in $\mathbb{F}$ if for each path ρ from the root to a leaf, in all assignments completing ρ, f is equal to the value labelling the leaf.

We say that a boolean decision tree *represents* a k-polynomial p if it computes f_p. Given a k-polynomial p, by $ht(p)$ we indicate the height of the tree represeting p. Notice that in this tree only variables from $\{x_1, \ldots, x_n\}$ appear.

Lemma 2. *For any k-polynomial p, $DC(p) \leq ht(p)$.*

Proof. Let ρ be a partial assignment induced by a path in the tree T representing p. Let $I = \rho^{-1}(1)$, $J = \rho^{-1}(0)$ and χ_ρ the polynomial $\prod_{i \in I} x_i \cdot \prod_{j \in J}(1 - x_j)$. Then the polynomial $q = \sum_\rho (f_p \restriction_\rho \cdot \chi_\rho)$, where ρ ranges over all paths in T, is multilinear (by definition of T) and clearly computes the same boolean function computed by p. □

The following lemma shows that PCR_k refutations of low degree complexity can be transformed into PC refutations of low degree.

Lemma 3. *Let Π be a PCR_k refutation over $\mathbb{F}[x_1, \ldots, x_n, \bar{x_1}, \ldots, \bar{x}_n]$ of a set of k-polynomials $Q = \{q_1, \ldots, q_n\}$. There exists a PC refutation Γ over $\mathbb{F}[x_1, \ldots, x_n]$ for $\tilde{Q} = \{\tilde{q}_1, \ldots, \tilde{q}_n\}$ such that $deg(\Gamma) \leq \max_{p \in \Pi} DC(p) + k$.*

Proof. Let $\Pi = p_1 \cdots p_l$ be a PCR_k refutation of Q. We build a PC refutation $\tilde{p}_1 \cdots \tilde{p}_l$ of $\tilde{Q}$ such that $deg(\tilde{p}_i) \leq DC(p_i)$. We will show how to deduce each $\tilde{p}_i$ from $\tilde{Q}$ and $\tilde{p}_1 \cdots \tilde{p}_{i-1}$. If p_i is an axiom, then there is nothing to prove. If p_i is obtained from scalar addtion by p and q, then p_i is $\alpha p + \beta q$ and we can use the fact that $\widetilde{\alpha p + \beta q} \equiv \alpha \tilde{p} + \beta \tilde{q}$ because of uniqueness of multilinear representation. We show the case of the rule $\frac{p}{p(1-\bar{x}_1 \cdots \bar{x}_k)}$. The others are obtained similarly. Assume p_i is obtained from p using the above rule. Then from $\tilde{p}$ we can build a PC proof of $\tilde{p}(1 - \widetilde{\bar{x}_1 \cdots \bar{x}_k})$, of degree at most $DC(p) + k$. Then we use boolean axioms to remove squares to finally obtain a proof of $\widetilde{p(1 - \bar{x}_1 \cdots \bar{x}_k)}$ which is $\tilde{p}_i$. Notice that for all polynomials p_i, $deg(\tilde{p}_i) \leq DC(p_i)$, while intermediate lines have degree at most $DC(p_i) + k$. □

Notice that in the previous simulation the number of monomials could increase exponentially, but we are interested only in the degree of such simulation.

3.2 Switching lemma for k-monomials

Recall Corollary 3.4 in [23].

Corollary 1. *([23]) Let k, s, d be positve integers, let γ and δ be real numbers from the range $(0, 1]$, and let $\mathcal{D}$ be a distribution on partial assignments so that for every k-DNF G, $\Pr_{\rho \in \mathcal{D}}[G \restriction_\rho \neq 1] \leq d2^{-\delta(c(G))^\gamma}$. For every k-DNF F,*

$$\Pr_{\rho \in \mathcal{D}}[ht(F \restriction_\rho) > 2s] \leq dk2^{-\delta' s^{\gamma'}}$$

where $\delta' = 2(\delta/4)^k$ and $\gamma' = \gamma^k$.

Let F be a k-DNF F and m_F the corresponding k-monomial, then $F \restriction_\rho = 1$ iff $m_F \restriction_{\rho^e} = 0$. On the other hand any $\{0, 1\}$ partial assignment for a k-monomial m which consistently assigns variables x and $\bar{x}$, can be viewed as the extension ρ^e of a boolean assignment ρ for the corresponding k-DNF F_m, such that $m \restriction_{\rho^e} = 0$ iff $F_m \restriction_\rho = 1$.

Since any k-monomial evaluates to 0 iff the corresponding k-DNF evaluates to 1, swapping 0 and 1 in the leaves of a decision tree T representing a k-monomial we obtain a decision tree that *strongly represent* (in the sense of Definition 3.1 in [23]) the corresponding k-DNF. Notice that the height is not changing.

The mapping between k-monomials and k-DNFs and lemma 2 allow us to restate for k-monomials and degree complexity, the switching lemma given for k-DNF in [23].

Definition 3. *Let τ be a k-DNF on $\{x_1, \ldots, x_n\}$ we call $c(\tau)$ the size of the smallest set of variables containing at least one variable from every term in τ. Let m be a k-monomial we define $c(m)$ as $c(\tau_m)$, where τ_m is the k-DNF corresponding to m. We call c the* covering number.

Lemma 4. *Let k, h be positive integers, and let $\mathcal{D}$ be a distribution over partial assignments on $\{x_1, \ldots, x_n\}$ such that for every k-monomial m, $\Pr_{\rho \in \mathcal{D}}[m \restriction_{\rho^e} \not\equiv 0] \leq 2^{-\delta c(m)}$, for some $\delta > 0$. Then for every k-monomial τ:*

$$\Pr_{\rho \in \mathcal{D}}[DC(\tau \restriction_{\rho^e}) > h] \leq k2^{-(\delta/4)^k h}$$

Proof. Let m be a k-monomial, and F_m the corresponding k-DNF. By Lemma 2 and we have:

$$\Pr_{\rho\in\mathcal{D}}[DC(m\restriction_{\rho^e})>h]\leq\Pr_{\rho\in\mathcal{D}}[ht(m\restriction_{\rho^e})>h]$$

Moreover

$$\Pr_{\rho\in\mathcal{D}}[ht(m\restriction_{\rho^e})>h]=\Pr_{\rho\in\mathcal{D}}[ht(F_m\restriction_{\rho})>h]$$

by previous considerations.

Since for any k-DNF F, $c(F)=c(m_F)$ and $F\restriction_\rho=1$ iff $m_F\restriction_{\rho^e}=0$, then by the hypothesis of the lemma, we have that for any k-DNF F, $\Pr_{\rho\in\mathcal{D}}[F\restriction_\rho\not\equiv 1]\leq 2^{-\delta c(F)}$. Then we can apply the switching lemma of [23]. Setting $\gamma=1$, $d=1$ and $s=h/2$ in Corollary 1, we get

$$\Pr_{\rho\in\mathcal{D}}[ht(F_m\restriction_\rho)>h]\leq k2^{-(\delta/4)^k h}$$

□

3.3 An equivalent formulation of PCR_k

We give an equivalent and more compact formulation of PCR_k as follows: to the axioms of PCR we add the axioms $1-x-(1-x)$ for any variables (positive or negative) and the axioms $(0), 1-(1), (1-1)$. To the rule of PCR we add the new rule:

$$\frac{a(1-s)+p\qquad b(1-t)+q}{ab(1-st)+asq+btp-pq}\tag{2}$$

where a,b are k-monomials, s,t are products of variables such that st contains at most k variables and p,q are k-polynomials.

It is not difficult to see that the two formulations are equivalent, in the sense that from the axioms and the rules of one we can derive axioms and the rules of the other. Applying the rule (2) to the k-polynomials $1-s-(1-s)$ and $1-t-(1-t)$ we get $1-st-(1-st)$, so we can build the axioms of PCR_k. Moreover applying the rule (2) to $p+(1-1)$ and $1-s-(1-s)$ we immediately derive $p(1-s)$ and hence simulate the rule of PCR_k. On the other hand using axioms and rules of PCR_k it is easy to simulate the rule (2).

4 A lower bound for refuting random 3-CNF in PCR_k

We will prove a lower bound on the number of k-monomials needed to refute a random 3-CNF in PCR_k. We closely follow the proof method in Alekhnovich[1] to get size lower bounds for random formulas in RES_k. In the whole section we will always consider the systems PC, PCR and PCR_k defined over a field of characteristic different from 2.

4.1 Expanders, random 3-CNF, encodings and PC lower bounds

We start with the definition of boundary expander.

Definition 4. *([3, 5, 1]) Let A be a $m\times n$ boolean matrix. For a set of rows I we define the* boundary of I *(denoted as ∂I) as the set of all $j\in[n]$ (the boundary elements) such that there exists exactly one row $i\in I$ that contains j. Then, A is a (r,c)-expander if the following condition holds: for all $I\subseteq[m]$, if $|I|\leq r$, then $|\partial I|\geq c\cdot|I|$.*

Let $\phi_{n,\Delta}$ be the random 3-CNF obtained selecting Δn clauses uniformly from the set of all possible 3-clauses over n variables. Following [1], instead of proving a lower bound for $\phi_{n,\Delta}$ refutations, we will prove it for a polynomial encoding of a set of linear $\mod 2$ equations, which semantically implies $\phi_{n,\Delta}$. We will always consider linear systems modulo 2.

For each possible formula $\phi_{n,\Delta}$ consider the matrix $A_{\phi_{n,\Delta}}$ defined by $A_{\phi_{n,\Delta}}[i,j] = 1$ iff the i-th clause of $\phi_{n,\Delta}$ contains the variable x_j. Let $b_{\phi_{n,\Delta}}$ be the boolean m vector defined by $b_{\phi_{n,\Delta}}[i] =$ (# of positive variables in the i-the clauses) mod 2. The random system of linear equations we consider is the system defined by $A_{\phi_{n,\Delta}}x = b_{\phi_{n,\Delta}}$.

Given a sistem of linear equations $Ax = b$, we define its *polynomial encoding* $Poly(A,b)$ as follows: for each equation $\ell \in Ax = b$, let f_ℓ is the characteristic function of ℓ that is 0 if and only if the equation is satisfied. Let $\tilde{\ell}$ be the unique multilinear polynomial representing the function f_ℓ. Then $Poly(A,b) = \bigcup_{\ell \in Ax=b} \tilde{\ell}$. Notice that $deg(\tilde{\ell}) = 3$.

Lemma 5. *Each* PCR_k *refutation of* $\phi_{n,\Delta}$ *can be transformed into a* PCR_k *refutation of* $Poly(A_{\phi_{n,\Delta}}, b_{\phi_{n,\Delta}})$ *with a polynomial increase in the size.*

Proof. Any equation ℓ in $A_{\phi_{n,\Delta}}x = b_{\phi_{n,\Delta}}$ semantically implies the clause C in $\phi_{n,\Delta}$, from which ℓ arose. Then by completeness we have a PCR_k proof of the polynomial encoding of C from $\tilde{\ell}$. □

The following observation is crucial to find 3-CNF which are hard for PC, PCR, PCR_k refutation systems. Such result is rephrased and used many times (see [10, 12, 9, 5, 1, 3]).

Fact 2. *([14],[5]) For all constant* $\Delta > 0$ *and for all* $c < 1$*, let* $\phi_{n,\Delta}$ *be a random* $3 - CNF$ *of* n *variables and* Δn *clauses. Then with probability* $1 - o(1)$ $\phi_{n,\Delta}$ *is unsatisfiable and* $A_{\phi_{n,\Delta}}$ *is a* $(\frac{n}{\Delta^{2/(1-c)}}, c)$*-expander.*

The reason we consider the expansion of a random 3-CNF (of the corresponding linear system) is the following theorem, stating expanders need high degree to be refuted by PC and PCR.

Theorem 1. *(Theorem 3.10 in [3]) Given an unsatisfiable linear system* $Ax = b$ *where* A *is an* (r,c)*-boundary expander, any* PCR *refutation of* $Poly(A,b)$ *in a field* $\mathbb{F}$ *with characteristic* $\neq 2$ *require degree* $\geq \frac{rc}{4}$.

Definitions and results in the next three subsections are essentially taken from [1], sometimes applied to k-monomials instead of k-DNFs.

4.2 How to restrict $Ax = b$ preserving expansion

In the following subsections we will apply restrictions to linear systems $Ax = b$ where A is an expander. In some cases such restrictions could destroy the expansion property of the system. Following [1] in this subsection we develop a tool which extracts a good expander from the restricted system.

Definition 5. *Let* A *be an* $m \times n$ *matrix and let* $r, c > 0$*. For a set* $J \subseteq [n]$*, the relation* $\vdash^e_{J,r,c}$ *on the set* $[m]$ *is defined as follows:*

$$I \vdash^e_{J,r,c} I_1 \text{ iff } |I_1| \leq r/2 \wedge |\partial I_1 - (\bigcup_{i \in I} \{j \ : \ A[i,j] = 1\} \cup J)| < (c/2)|I_1|$$

Since r, c will be always clear from the context, from now on we will omit them. Let I and J be subsets of the rows and the columns of a matrix A. Consider the following algorithm $Cl^e(A, I, J)$:

$R := [m]$
while (there exists $I_1 \subseteq R$ s.t $I \vdash^e_J I_1$)
    $I := I \cup I_1$
    $R := R - I_1$
end
output I;

Define $Cl^e(J) := Cl^e(A, \emptyset, J)$. Two lemmata are immediate from the definition and proved in [1].

Lemma 6. *(Lemma 2.4 in [1]) Let A be any boolean $m \times n$ matrix and let $J \subseteq [n]$. Let $I' = Cl^e(J)$ and let $J' = \bigcup_{i \in I'} A_i$. Let $\hat{A}$ be the matrix obtained from A removing the rows in I' and the columns in $J' \cup J$. Either $\hat{A}$ is empty or it is a $(r/2, c/2)$-boundary expander.*

Proof. For any set of row $I \in \hat{A}$, we will denote $\partial_A I$ and $\partial_{\hat{A}} I$ the boundary computer w.r.t. A and $\hat{A}$ respectively. Assume $|I| \leq r/2$. By construction $\partial_A I \subseteq \partial_{\hat{A}} I \cup J \cup J'$. I has no element in common with $Cl^e(J)$, then $|\partial_A I - (J' \cup J)| \geq (c/2)|I|$. It follows $|\partial_{\hat{A}} I| \geq (c/2)|I|$. □

It is important to remark that Cl^e does not increase too much the number of columns to remove from A.

Lemma 7. *([1, 4]) If A is an (r, c)-boundary expander, $|J| \leq cr/4$, then $|Cl^e(J)| < 2c^{-1}|J|$.*

Proof. Assume $|Cl^e(J)| \geq 2c^{-1}|J|$ and consider $I_1 \cdots I_i \cdots I_l$, the inference of $Cl^e(J)$. Wlog we can assume I_i to be pairwise dijoint. Consider the first step t such that $C = \cup_{i=1}^{t} I_i$ and $|C| \geq 2c^{-1}|J|$. Since $|C - I_t| < 2c^{-1}|J| \leq r/2$ and $|I_t| \leq r/2$, then $|C| \leq r$. Thus $|\partial C| \geq c|C|$ by expansion of A. Then $|\partial C - J| \geq c|C| - |J| \geq \frac{c}{2}|C|$. But at any step each I_i add strictly less than $c/2$ elements to $|\partial C - J|$. We have the contraddiction. □

We combine previous lemmata in a useful tool for restricting linear systems while keeping both unsatisfiability and expansion.

Lemma 8. *Consider $Ax = b$ be an m equations, n variables unsatisfiable linear system where A is an (r, c)-boundary expander. Let J be a set of columns (i.e. variables of the system) with $|J| \leq \frac{cr}{4}$. Define:*

- *$I' = Cl^e(J)$ and $J' = \bigcup_{i \in I'} \{j : A[i, j] = 1\}$;*
- *$A_{I'}x = b_{I'}$ as the linear system containing rows I' from $Ax = b$;*
- *$\hat{A}$ is the matrix A with rows I' and columns $J \cup J'$ removed.*

Then: (1) $A_{I'}x = b_{I'}$ is a satisfiable system on the variables corresponding to columns $J \cup J'$. For any assignment ρ on such variables which satisfies $A_{I'}x = b_{I'}$, we have that: (2) $(Ax = b) \restriction_\rho$ is $\hat{A}x = \hat{b}$ for some $\hat{b}$, (3) $\hat{A}x = \hat{b}$ is unsatisfiable and $\hat{A}$ is and an $(r/2, c/2)$-boundary expander.

Proof. If $A_{I'}x = b_{I'}$ was unsatisfiable, then by gaussian elimination we could obtain a non empty linear combination of rows resulting in $0 = 1$, (in the field $\mathbb{F}_2$) such linear combination is a subset H of rows. No variables in ∂H can be eliminated, so ∂H is empty. Since $|J| \leq \frac{cr}{4}$, then by Lemma 7 $|I'| \leq r/2$. Thus $|H| \leq r/2$. But then, by the expansion of A, ∂H can't be empty. Contradiction.

$(Ax = b) \restriction_\rho$ is $\hat{A}x = \hat{b}$ because assigned columns become constants and satisfied conditions are set to $0 = 0$.

The expansion of $\hat{A}$ is guaranteed by Lemma 6. □

4.3 Normal forms

Let us start by recalling that when speaking of k-monomials, a *term* is a either a variable or an expression of the form $(1 - \prod x_i)$. For a term t, $V(t) := \{i : x_i \text{ appears in } t\}$.

Let us consider another relation on the set of rows of the matrix A.

Definition 6. *([5]) Let A be an $m \times n$ matrix and let $r > 0$. For a set $J \subseteq [n]$ (a set of indices of variables) the relation $\vdash_{J,r}$ on the set $[m]$ is defined as follows:*

$$I \vdash_{J,r} I_1 \text{ iff } |I_1| \leq r/2 \wedge \partial I_1 \subseteq (\bigcup_{i \in I} \{j \ : \ A[i,j] = 1\} \cup J)$$

For $J \subseteq [n]$, $Cl(J)$ is the set of all rows that can be inferred from $\emptyset$ via the relation $\vdash^r_J$. For a term t, $Cl(t) := Cl(V(t))$.

The next lemma is proved in [5, 1] and we omit its proof.

Lemma 9. *([5, 1]) If $|J| \leq cr/2$, then $|Cl(J)| \leq c^{-1}|J|$.*

Let t be a term over variables $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$. We identify t with the linear system over $\{x_1, \ldots, x_n\}$ defined by $x = \epsilon_x$ for all variables appearing in t. $\epsilon_x = 1$ for positive variables and $\epsilon_x = 0$ for negative variables. Such system is satisfied iff $t = 0$.

Definition 7. *Let A a $m \times n$ matrix which is a (r, c)-boundary expander and let b be a boolean m vector. Let t be a term and let $I = Cl(t)$. t is* locally consistent with respect to $Ax = b$ *if the system $t \wedge A_I x = b_I$ is satisfiable.*

Lemma 10. *([1]) Let $Ax = b$ where A is an (r, c)-boundary expander, with $r > 3/c$. t is locally consistent with $Ax = b$ iff for any subset I of equations with $|I| < r/2$, the system $t \wedge A_I x = b_I$ is satisfiable.*

Proof. Assume that t is locally consistent with A and that there exists a I s.t $|I| < r/2$ and $t \wedge A_I x = b_I$ inconsistent. Then by linear algebra there exist $I' \subseteq I$ and a $V' \subseteq V(t)$, such that $\sum_{i \in I'}(A_i x - b_i) + \sum_{x \in V'}(x - \epsilon_x) \equiv 1$. Then it must be that $\partial I' \subseteq V(t)$. Thus $I \subseteq Cl(t)$ which is a contradiction with locally consistency of t. The other direction follows since by Lemma 9 $Cl(t) < r/2$. □

Corollary 2. *Let $Ax = b$ where A is a $m \times n$ boolean matrix which is an (r, c)-boundary expander, with $r > 3/c$. Then for any set $I \subseteq [m]$ such that $|I| < r/2$ the system $A_I x = b_I$ is satisfiable.*

Proof. The statement follows immediately by proving that the constant 0 is locally consistent with respect to $Ax = b$. This in turn follows since otherwise there was a set I whose boundary is empty. But this is in contradiction with expansion of A. □

Definition 8. *Let A be a boolean $m \times n$ matrix and let b be a boolean m vector. A k-monomial m is in* normal form *with respect to $Ax = b$ if each of its term is locally consistent wrt $Ax = b$.*

Definition 9. *Let $Ax = b$ be an unsatisfiable system where A is boolean $m \times n$ matrix and b be a boolean m vector. A PCR_k refutation Π of $Poly(A, b)$ is in* normal form *with respect to $Ax = b$ if all the locally inconsistent terms wrt to $Ax = b$ appearing in Π are only in monomials of degree $O(k)$.*

We end by showing that, as long as $k = O(\log n)$, every PCR_k refutation of $Poly(A, b)$ can be transformed into a PCR_k refutation in normal form with only a polynomial increase in the number of k-monomials.

Lemma 11. *Let be a linear system $Ax = b$ where A is an $m \times n$ matrix which is an (r, c)-boundary expander. Let $k = O(\log n)$ and Γ be a PCR_k refutation of $Poly(A, b)$. Then there is refutation Π of $Poly(A, b)$ in normal form and such that $S(\Pi) = S(\Gamma)^{O(1)}$.*

Proof. We first get rid from Γ of the locally inconsistent terms of the form $t = (1 - \prod_{1 \leq i \leq k} x_i)$. We want to replace this term by the constant 1 along the proof. By defitinion there exists some set $I = Cl(t)$ of rows, with $|I| \leq k/c$, such that t is inconsistent with the system $A_I x = b_I$. By completeness of PCR there must be a PCR proof Γ_t of $\prod_i x_i$ from $Poly(A_I, b_I)$. Such proof involves at most $O(k)$ variables so $S(\Gamma_t) = 2^{O(k)}$ and $deg(\Gamma_t) = O(k)$.

Let Π' be the proof where all occurrence of t will be deleted as follows. t could have been introduced in some k-monomial either by the multiplication rule, in which case in the Π' we simply skip this rule, or it was introduced by some axiom of the form $1 - \prod_i x_i - (1 - \prod_i x_i)$. In this case in the new proof we replace this axiom with the PCR proof Γ_t of $\prod_i x_i$. Notice that the PCR proofs Γ_t could introduce in Π' locally inconsistent terms but only occurring in monomials of degree $O(k)$.

Now we obtain Π getting rid from Π' of the locally inconsistent terms $t = x$ with only one variable. Using the PCR proofs Γ_t of $\bar{x}$, we can delete x in the axioms of $Poly(A, b)$, in the axioms $1 + x + \bar{x}$ and $x^2 - x$. The PCR_k axioms containing x can be just replaced by the same axiom without x. So x disappears from Π'. As above the Γ_t PCR proofs are of size $S(\Gamma_t) = 2^{O(k)}$ and degree $deg(\Gamma_t) = O(k)$ and can introduce locally inconsistent terms in Π, but only occurring in monomials of degree $O(k)$. So Π is in normal form and, since $k = O(\log n)$, $S(\Pi)$ is polynomial in $S(\Gamma)$. □

4.4 Random restriction lemma

In this section we define the distribution $\mathcal{D}$ over partial assignments over $\{x_1 \ldots, x_n\}$ that will guarantee the applicability of the switching lemma (Lemma 4). The distribution is that defined by Alekhnovich in [1].

Definition 10. *Let A be a $m \times n$ boolean matrix which is a (r, c)-boundary expander. Let $b \in \{0,1\}^m$. Let X be the set of variables $\{x_1, \ldots, x_n\}$. Let $\mathcal{D}_{A,b}$ be the distribution over partial assignments ρ over X obtained by the following experiment: choose a random subset X_1 of X of size $cr/4$. Let $\hat{I} = Cl^e(X_1)$. Let $\hat{X} = X_1 \cup Y_1$, where $Y_1 = \{j : \exists i \in \hat{X} : A[i,j] = 1\}$. ρ is obtained by selecting uniformly at random an assignment $\hat{x}$ for the set of variables whose indices are in $\hat{X}$ that satisfies the system $A_{\hat{I}}\hat{x} = b_{\hat{I}}$.*

The proof of the next main lemma is the same as that of the analogous Theorem 3.1 in [1] where instead of k-DNF we use k-monomials.

Lemma 12. *([1]) Let A be a $m \times n$ boolean matrix which is a (r, c)-boundary expander such that A has at most $\hat{\Delta}$ ones in each column. Let $b \in \{0,1\}^m$ and assume $r = \Omega(n/\hat{\Delta})$. For any k-monomial m in normal form,*

$$\Pr_{\rho \in \mathcal{D}_{A,b}}[m \restriction_{\rho^e} \neq 0] < (1 - 2^{-k})^{c(m)/\hat{\Delta}^{O(k)}}$$

Corollary 3. *There exists a constant D such that, under the assumptions of the previous lemma, for any k-monomial in normal form m we have:*

$$\Pr_{\rho \in \mathcal{D}_{A,b}}[m \restriction_{\rho^e} \neq 0] < 2^{-c(m)/\hat{\Delta}^{Dk}}$$

4.5 Main result

We are ready to give the main result of this section.

Theorem 2. *For any constant Δ let $\phi_{n,\Delta}$ be a random 3-CNF on n variables and Δn clauses. For $k = o(\sqrt{\log n / \log \log n})$ any refutation of $\phi_{n,\Delta}$ in PCR_k over a field with characteristic different from 2, has size $S > 2^{n^{1-o(1)}}$ with high probability.*

Proof. Assume that $\phi_{n,\Delta}$ is an unsatisfiable formula and $A_{\phi_{n,\Delta}}$ is an (r,c)-expander for some constant $c < 1$ and any $r = \Omega(n)$. Consider the system $A_{\phi_{n,\Delta}} x = b_{\phi_{n,\Delta}}$ as defined in Subsection 4.1. For easiness of notation let us omit the indices $\phi_{n,\Delta}$ from both A and b. Remember k is $O(\log n)$ and let Γ be a PCR$_k$ refutation of $\phi_{n,\Delta}$ of size S. Then by Lemma 5 there is a PCR$_k$ refutation Π of $Poly(A,b)$ of size $S^{O(1)}$.

To apply the switching Lemma 4, according to Corollary 3 we need to transform the proof Π of $Poly(A,b)$ in a proof of $Poly(\hat{A},\hat{b})$ where k-monomials are in normal form and $\hat{A}$ only contains a constant $\hat{\Delta}$ number of ones in each column.

Pick in A the set J of the $cr/4$ columns with the biggest number of ones, By Lemma 8 there is a restriction α that, applied to $Ax = b$, restricts this system to $\hat{A}x = \hat{b}$, where $\hat{A}$ is a submatrix of A with at least the columns J removed and is an $(r/2, c/2)$-expander. Notice moreover that in each column of $\hat{A}$ there are at most $\hat{\Delta} \leq 12\Delta n/cr$ ones, which is a constant since $r = \Omega(n)$. If we now apply Lemma 11 to $\Pi \restriction_\alpha$ we get a PCR$_k$ normal form refutation $\hat{\Pi}$ of $Poly(\hat{A},\hat{b})$ of size at most $S^{O(1)}$.

Let now ρ drawn from $D_{\hat{A},\hat{b}}$ according to Definition 10 and denote by $A'x = b'$ and Π' respectively the system and the refutation obtained restricting $\hat{A}x = \hat{b}$ and $\hat{\Pi}$ by ρ^e.

By Corollary 3 and by setting the parameter of Lemma 4 as follows: $\delta = (1/\hat{\Delta})^{Dk}$ and $h = (rc/64) - k - 1$, we have that for any k-monomial in normal form m in $\hat{\Pi}$

$$\Pr_{\rho}[DC(m \restriction_{\rho^e}) > (rc/64) - k - 1] \leq 2^{\frac{-rc}{2^{O(k^2)}}}$$

With probability greater than $1 - S^{O(1)} \cdot 2^{\frac{-rc}{2^{O(k^2)}}}$ we have that $\Pi' = \hat{\Pi} \restriction_{\rho^e}$ has degree complexity strictly less than $(rc/64) - k$ by union bound[1], and it is a refutation of $Poly(A',b')$.

Fix any $c < 1$ and $r = \frac{n}{\Delta^{2/(1-c)}}$. Notice that $\rho \in D_{\hat{A},\hat{b}}$ is defined in such a way that Lemma 8 applies. Thus A' is an $(r/4, c/4)$-boundary expander. If $S < 2^{\frac{rc}{2^{O(k^2)}}}$ then using Lemma 3 on Π' we get a PCR refutation of $Poly(A',b')$ of degree $< rc/64$. This is impossible because of Theorem 1, and then it follows $S \geq 2^{\frac{rc}{2^{O(k^2)}}}$.

Since by Fact 2 with high probability A is an (r,c)-boundary expander, then the theorem follows. □

5 A degree lower bound for Graph Ordering Principle in PC

In this section we prove that certain graph ordering tautologies have no low degree PC refutations. Ordering tautologies are considered in [11] to prove the optimality of the size-width relation found in [10] for resolution. In [23] they consider an ordering tautology on a graph to prove separation between RES$_k$ and RES$_{k+1}$ proof systems.

We want to encode into a formula the following *Graph Ordering Principle*: if we give directions to the edges of a simple undirected graph G according to a total order $\prec$ on its vertices, then there will be a source node in G.

We consider variables $x_{a,b}$ for any $a, b \in [n]$ such that $a < b$, where $<$ is the standard order on integers. The variables $x_{a,b}$ are intended to take the value 1 when $a \prec b$. The negation of the principle is made of two sets of constraints. The first one, that we call $\mathcal{T}$, expresses that the relation $\prec$ is a total order on $[n]$:

$$\forall a < b < c \qquad x_{a,b}x_{b,c}(1 - x_{a,c}) \tag{3}$$

$$\forall a < b < c \quad (1 - x_{a,b})(1 - x_{b,c})x_{a,c} \tag{4}$$

[1]Notice that locally inconsistent terms which were not eliminated from $\hat{\Pi}$ occur in monomial of degree at most $O(k)$ because of Lemma 11

Notice that equations in (3) and (4) also say there are no cycles of three elements in $[n]$ according to $\prec$. Moreover notice that we do not need the usual antisimmetry constraints because of the definition of our variables. Equations in $\mathcal{T}$ are satisfied if and only if the assignment defines a proper total order over $[n]$.

The second set of constraints depends on the underlying graph G and expresses that there will be no source node in G. We denote $\Gamma(u)$ the set of vertices adjacent to u in G.

$$\forall u \in V \qquad \prod_{a \in \Gamma(u): a<u} (1 - x_{a,u}) \cdot \prod_{a \in \Gamma(u): a>u} x_{u,a} \tag{5}$$

Each equation has degree at most equal to the degree of G. To simplify notations, we denote as u both a vertex of G and the corresponding equation in (5) and we extend this notation to sets of vertices: for $U \subseteq [n]$ we denote with U also the corresponding set of constraints in (5). We call GOP(G) the union of $\mathcal{T}$ and equations $[n]$ induced by G.

Let $GOP^*(G)$ the graph ordering principle used in [23]. From the resolution refutations of width $O(n)$ for this principle we immediately get PCR refutations of degree $O(n)$ for the same principle. In this proof we first apply the transformations $x_{i,j} \mapsto \bar{x}_{j,i}$ and $\bar{x}_{i,j} \mapsto x_{j,i}$ for $i > j$ to reduce to our set of variables (notice that this way the antisimmetry axioms simplify to 0); then we further apply the transformation $\bar{x} \mapsto (1 - x)$ to get a proper a PC refutation of GOP(G).

Lemma 13. *There are degree $O(n)$ PC and PCR refutations for GOP(G). Moreover PCR refutations can be done with $O(n^3)$ monomials.*

To prove a degree lower bound for GOP(G) we follow the approach of [5].

Definition 11. *Let a graph $G = (V, E)$ be given, for any $U \subseteq V$ we say $\Gamma(U)$ is the set of vertices in V/U which have an adjacent vertex in U. It is called the* vertex boundary *of U. The graph G is said to be an (r, c)-*vertex expander *if for any set U with less or equal than r vertices, its vertex boundary $\Gamma(U)$ is greater or equal than $c|U|$.*

The degree lower bound for GOP(G) is a corollary of the existence of a non trivial linear operator which sets to 0 all consequences of GOP(G) derived in low degree. This strategy follows that of [21, 5].

Lemma 14 ([5, 21])**.** *Let G be a (r, c)-vertex expander. There exists a linear operator $\mathcal{L}$ defined on polynomials such that: (1) $\mathcal{L}(p) = 0$, for all polynomial $p \in$ GOP(G); (2) $\mathcal{L}(x^2 - x) = 0$ for all variable x of GOP(G); (3) for each monomial t and for each variable x, if $deg(t) < cr/4$, then $\mathcal{L}(x \cdot t) = \mathcal{L}(x \cdot \mathcal{L}(t))$; (4) $\mathcal{L}(1) = 1$.*

We postpone the proof of this lemma to the end of the section.

Theorem 3. *If G is an (r, c)-vertex expander then there is no PC refutation of GOP(G) of degree less than or equal to $cr/4$.*

Proof. Assume for the sake of contradiction such refutation does exist. Then by lemma 14 all polynomials in this proof are mapped to 0 by $\mathcal{L}$. This is a contradiction with the fact that the last line (i.e the polynomial 1) is not mapped to 0 by $\mathcal{L}$. □

In the following we assume G to be given and to be an (r, c)-vertex expander. All the definitions are given w.r.t. such graph.

Definition 12. *We call $Vertex(p)$ the set of vertices which appears in the variables in p. Given a set of vertices U we define the inference relation $\rightsquigarrow_U$ in this way: For $A, B \subseteq [n]$,*

$$A \rightsquigarrow_U B \quad \textit{if} \quad |B| \leq \frac{r}{2} \quad \textit{and} \quad \Gamma(B) \subseteq A \cup U$$

$Sup(U)$, the support of U, is defined as the closure of $\emptyset$ with respect to $\rightsquigarrow_U$. We denote by $Sup(p)$ the set $Sup(Vertex(p))$ for any polynomial p.

The notion of support is closely related with the notion of vertex boundary in a graph: $Sup(U)$ is the maximal set of vertices for which the vertex-boundary is inside U and which is not big enough to break the expansion barrier r. The following lemma gives the link between the vertex expansion and degree of monomials: a small set of vertices (hence a low degree term) has small support.

Lemma 15. *If a set U has size less or equal than $cr/2$ then $Sup(U)$ has size less or equal than $r/2$. If a monomial t has degree less than $cr/4$ then $Sup(t)$ has size less or equal than $r/2$.*

Proof. Let $Sup(U) = I_1 \cup I_2 \cup I_3 \cup \cdots \cup I_l$ where each I_i is the set added in the i-th step of the inference. Assume it has size strictly greater than $r/2$, then there is a step j where such size is overcome. Let us denote $A = I_1 \cup \ldots \cup I_{j-1}$ and $I = I_j$. Then $|A| \leq r/2$ and $|A \cup I| > r/2$. Also $|I| \leq r/2$ because of the size constraint in the definition of $\rightsquigarrow_U$. Then $|A \cup I| \leq r$ and hence by the vertex-expansion condition $|\Gamma(A \cup I)| > cr/2$. This proves the first part since $\Gamma(A \cup I) \subseteq U$.

The second part follows since the vertices appearing in term t are at most twice the degree of t. □

Recall the definition of $R_E(p)$ from subsection 2.2 and that in the set of polynomials E we always implicitly include the polynomials $x^2 - x$, for all variables of GOP(G).

Lemma 16. *Let t be a term. For any not empty set of vertices A of size less or equal than $r/2$ and such that $A \cap Sup(t) = \emptyset$, there exists an edge (u, v) in G such that $v \in A$, $u \notin Sup(t) \cup A \cup Vertex(t)$.*

Proof. By definition of $Sup(t)$ and the hypothesis of the lemma, it follows that $Sup(t) \not\rightsquigarrow_{Vertex(t)} A$. Then $\Gamma(A) \not\subseteq Sup(t) \cup Vertex(t)$, therefore there is an edge between A and $\Gamma(A)/(Sup(t) \cup Vertex(t))$. □

A partial assignment ρ to the variables of GOP(G)is a u-cta (critical truth assignment) when it sets u as a global minimum.

$$\rho = \begin{cases} x_{a,u} = 1 & \forall a, a < u \\ x_{u,a} = 0 & \forall a, u < a \end{cases}$$

Lemma 17. *Let t be a term. Let I be a set of vertices such that $|I| \leq r/2$ and $I \supset Sup(t)$. Then there exists a $v \in I/Sup(t)$ such that:*

$$R_{\mathcal{T},I}(t) = R_{\mathcal{T},I/\{v\}}(t)$$

Proof. Applying lemma 16 to t and $I/Sup(t)$ we get an edge (u, v) such that $v \in I/Sup(t)$ and $u \notin I \cup Vertex(t)$. Let ρ be a u-cta. Note that any equation in $\mathcal{T}$ containing the vertex u is satisfied by ρ. Any other equation in $\mathcal{T}$ is not touched, so $\mathcal{T} \restriction_\rho \subseteq \mathcal{T}$. Moreover since $u \notin Vertex(t)$, $t \restriction_\rho = t$. Finally note that $I \restriction_\rho \subseteq I/\{v\}$ since ρ is setting to 0 at least v. Recall that if $A \vdash p$, then $B \vdash p$, for any p, A and $B \supseteq A$. Thus we have the following derivations:

$$\mathcal{T}, I \quad \vdash t - R_{T,I}(t) \quad \text{By definition of } R_E \tag{6}$$

$$\mathcal{T} \restriction_\rho, I \restriction_\rho \quad \vdash t \restriction_\rho - R_{\mathcal{T},I}(t) \restriction_\rho \quad \text{By restriction from (6)} \tag{7}$$

$$\mathcal{T}, I/\{v\} \quad \vdash t - R_{\mathcal{T},I}(t) \restriction_\rho \quad \text{By previous observations on (7)} \tag{8}$$

From (8) and minimality of the remainder we then have that $R_{T,I/\{v\}}(t) \leq_{\mathbb{P}} R_{\mathcal{T},I}(t) \restriction_\rho$. Moreover, since $\mathcal{T}, I \vdash t - R_{T,I/\{v\}}(t)$, we have that $R_{T,I}(t) \leq_{\mathbb{P}} R_{T,I/\{v\}}(t)$, also by the minimality. Finally $R_{\mathcal{T},I}(t) \restriction_\rho \leq_{\mathbb{P}} R_{T,I}(t)$ holds since a restriction can only decrease the order of a polynomial. Hence it must be $R_{T,I/\{v\}}(t) = R_{T,I}(t)$. □

Lemma 18. *Let t be a term. For any set of vertices I of size less than or equal to than $r/2$ and such that $I \supseteq Sup(t)$, the following holds:*

$$R_{\mathcal{T},I}(t) = R_{\mathcal{T},Sup(t)}(t)$$

.

Proof. If $I = Sup(t)$ then $R_{\mathcal{T},I}(t) = R_{\mathcal{T},Sup(t)}(t)$. If I is strictly bigger than S, then by lemma 17 there is a vertex $v \in I/Sup(t)$ such that $R_{\mathcal{T},I}(t) = R_{\mathcal{T},I/\{v\}}(t)$, from which the lemma follows by iterating the argument. □

Lemma 19. *For any term t, $Vertex(R_{\mathcal{T},Sup(t)}(t)) \subseteq Sup(t) \cup Vertex(t)$.*

Proof. Assume for the sake of contradiction that there is a node $u \in Vertex(R_{\mathcal{T},Sup(t)}(t))$ not in $Vertex(t) \cup Sup(t)$. Consider a u-cta ρ. By an argument analogous to that of lemma 17 we then have $R_{\mathcal{T},Sup(t)}(t) \leq_{\mathbb{P}} R_{\mathcal{T},Sup(t)}(t) \restriction_{\rho} <_{\mathbb{P}} R_{\mathcal{T},Sup(t)}(t)$. □

We are ready to give the proof of Lemma 14.

Proof. **Lemma 14**
For any monomial t, the linear operator $\mathcal{L}(t)$ is defined by

$$\mathcal{L}(t) := R_{\mathcal{T},Sup(t)}(t)$$

and is extended by linearity to any polynomial.

First we prove that for any polynomial $p \in \textsc{Gop}(G)$, $\mathcal{L}(p) = 0$. If p is in $\mathcal{T}$, then $R_{\mathcal{T}}(p) = 0$. Now, $\mathcal{L}(p) = \sum \beta_i \mathcal{L}(t_i) \leq_{\mathbb{P}} \sum \beta_i R_{\mathcal{T}}(t_i) = R_{\mathcal{T}}(p) = 0$. For any axiom $v \in [n]$ let $v = t + w$, where t is the leading term. Since $\Gamma(v) \subseteq Vertex(t)$, then $v \in Sup(t)$. Hence $\mathcal{L}(v) = \mathcal{L}(t) + \mathcal{L}(w) \leq_{\mathbb{P}} R_{\{v\}}(t) + \mathcal{L}(w) = -w + \mathcal{L}(w) \leq_{\mathbb{P}} -w + w = 0$.

For the second property, consider that $Sup(x^2) = Sup(x)$ and that we are reducing also against $x^2 - x$. Then:

$$\begin{aligned} \mathcal{L}(x^2 - x) &= \mathcal{L}(x^2) - \mathcal{L}(x) \\ &= R_{T,Sup(x)}(x^2) - R_{T,Sup(x)}(x) \\ &= R_{T,Sup(x)}(x^2 - x) = 0 \end{aligned}$$

Let us prove that $\mathcal{L}(xt) = \mathcal{L}(x\mathcal{L}(t))$ for any term t of degree strictly less than $\frac{rc}{4}$. Notice that by monotonicity of Sup function, $Sup(xt) \supseteq Sup(t)$. Moreover since $deg(xt) \leq \frac{cr}{4}$, then by lemma 15 we get $|Sup(xt)| \leq r/2$. Therefore we have the following chain of equalities by applying respectively: in (9) the definition; in (10) the Property 1; in (11) the monotonicity of Sup and lemma 18; in (12) again the definition.

$$\begin{aligned} \mathcal{L}(xt) &= R_{\mathcal{T},Sup(xt)}(xt) && (9) \\ &= R_{\mathcal{T},Sup(xt)}(xR_{\mathcal{T},Sup(xt)}(t)) && (10) \\ &= R_{\mathcal{T},Sup(xt)}(xR_{\mathcal{T},Sup(t)}(t)) && (11) \\ &= R_{\mathcal{T},Sup(xt)}(x\mathcal{L}(t)) && (12) \end{aligned}$$

Let us write $x\mathcal{L}(t)$ as a polynomial $\sum \alpha_i r_i$. The following inclusions hold respectively: in (13) because r_i is a monomial in the polynomial expansion of $x\mathcal{L}(t)$; in (14) by lemma 19; in (15) by monotonicity of Sup.

$$\begin{aligned} Vertex(r_i) &\subseteq Vertex(x) \cup Vertex(\mathcal{L}(t)) && (13) \\ &\subseteq Vertex(x) \cup Vertex(t) \cup Sup(t) && (14) \\ &\subseteq Vertex(xt) \cup Sup(xt) && (15) \end{aligned}$$

From the definition of Sup and the previous inclusions it follows that $Sup(r_i) \subseteq Sup(xt)$.

Finally the third property of the operator is obtained from the following chain of equalities given respectively: in (16) by definition; in (17) by lemma 18 applied to $Sup(r_i)$ and $Sup(xt)$; in (18) by linearity; in (19) by the form of $x\mathcal{L}(t)$; finally in (20) by equalities (9)-(12).

$$\begin{aligned}
\mathcal{L}(x\mathcal{L}(t)) &= \sum \alpha_i R_{\mathcal{T},Sup(r_i)}(r_i) && (16)\\
&= \sum \alpha_i R_{\mathcal{T},Sup(xt)}(r_i) && (17)\\
&= R_{\mathcal{T},Sup(xt)}(\sum \alpha_i r_i) && (18)\\
&= R_{\mathcal{T},Sup(xt)}(x\mathcal{L}(t)) && (19)\\
&= \mathcal{L}(xt) && (20)
\end{aligned}$$

Finally for the fourth property observe that the support of a constant is the empty set, so $\mathcal{L}(1) = R_{\mathcal{T}}(1) = 1$ since $\mathcal{T}$ is satisfiable. □

To complete the proof we need to show that a constant degree (r, c)-vertex expander exists. Consider a graph $G = (V, E)$ of degree d (i.e. all vertices have at most d edges). The adjacency matrix is a (r, c')-boundary expander if and only if for any set $S \subseteq V$ smaller than r, the edges going outside S are at least $c' \cdot |S|$. At most d edges can be connected to a single vertex. Thus such graph is an $(r, c'/d)$-vertex expander. This reduce the search of a vertex expander to the search of a constant degree boundary expander. An efficient construction is given in [17] using a graph composition devised in [22] and called *zig-zag product*.

Proposition 1. *(Proposition 9.2 [17]) For any t and d an undirected graph G can be constructed, such that G has d^{4t} vertices, it is d^2 regular and is a $(\frac{V(G)}{2}, 1/2)$-boundary expander.*

Theorem 4. *There exists an infinite family $\mathcal{G}$ of simple graphs of constant degree such that for any G in $\mathcal{G}$ the principle* GOP(G) *has polynomial size in $|V(G)|$ and any* PC *refutation of* GOP(G) *requires degree at least $\frac{|V(G)|}{108}$.*

Proof. Fix any integer t. By construction claimed in Proposition 1 we can construct a 9-regular graph G of $n := 81^t$ vertices, such that G is $(\frac{n}{2}, \frac{1}{2})$-boundary expander. Since G is 9-regular, it is a $(n/2, 1/18)$-vertex expander. To obtain a simple graph without losing vertex expansion it is sufficient to remove edges in excess between pair of nodes.

By Theorem 3 the theorem follows. □

6 A separation between PCR_k and PCR_{k+1}

In this section we will give a variant of GOP(G), which is polynomially refutable by PCR_{k+1} but it's not polynomially refutable by PCR_k. We closely follows the ideas developed for RES_k in [23].

Let $Even(a_1, \ldots, a_k)$ be the function from $\{0,1\}^k$ to $\{0,1\}$ which gives 0 if the number of input variables at 0 are even. Such function can be written as a 2^{k-1} size multilinear polynomial with degree k.

For each variable $x_{a,b}$ of GOP(G) we introduce k new variables $x^1_{a,b}, \ldots, x^k_{a,b}$. $\mathrm{GOP}^{\oplus k}(G)$ is defined as a modification of GOP(G): substitute any $x_{a,b}$ with $Even(x^1_{a,b}, \ldots, x^k_{a,b})$. Such principle is specified by kd degree polynomials with less than 2^{dk} monomials each, where d is the degree of G. We now give a polynomial refutation in PCR_k for $\mathrm{GOP}^{\oplus k}(G)$.

Proposition 2. *For any graph G, $\mathrm{GOP}^{\oplus k}(G)$ has a polynomial size refutation in PCR_k*

Proof. We consider an auxiliary principle called pseudo-$\text{GOP}^{\oplus k}(G)$, we give a polynomial PCR_k refutation for this and we polynomially reduce $\text{GOP}^{\oplus k}(G)$ to pseudo-$\text{GOP}^{\oplus k}(G)$.

First notice that $Even(x^1_{a,b}, \ldots, x^k_{a,b})$ (respectively $1 - Even(x^1_{a,b}, \ldots, x^k_{a,b})$) can be written as $\prod(1 - l_1 \cdots l_k)$ where $l_1 \cdots l_k$ range among all tuples of variables $x^1_{a,b}, \ldots, x^k_{a,b}$ with an even (respectively odd) number of negated variables. We denote such k-monomials as $Even_{a,b}$ and $Odd_{a,b}$.

pseudo-$\text{GOP}^{\oplus k}(G)$ is defined form $\text{GOP}(G)$ as follows: each $x_{a,b}$ is substituted with the k-monomial $Even_{a,b}$. pseudo-$\text{GOP}^{\oplus k}(G)$ has the property to translate any monomial in $\text{GOP}(G)$ with a single k-monomial in pseudo-$\text{GOP}^{\oplus k}(G)$. So a PCR refutation of $\text{GOP}(G)$ can be translated in a PCR_k refutation of pseudo-$\text{GOP}^{\oplus k}(G)$ by the mapping $\{x_{a,b} \mapsto Even_{a,b}, \bar{x}_{a,b} \mapsto Odd_{a,b}\}$ and the pseudo axioms: $Even_{a,b} \cdot Even_{a,b} - Even_{a,b}$, $Odd_{a,b} \cdot Odd_{a,b} - Odd_{a,b}$ and $1 - Odd_{a,b} - Even_{a,b}$. Each of these pseudo axioms is derivable in PCR_k with a size at most exponential in k.

Since $Even_{a,b}$ (respectively $Odd_{a,b}$) are semantically equivalent to $Even(x^1_{a,b}, \ldots, x^k_{a,b})$ (respectively $1 - Even(x^1_{a,b}, \ldots, x^k_{a,b})$) then, by completeness, in PCR_k we can derive the axioms of pseudo-$\text{GOP}^{\oplus k}(G)$ from those of $\text{GOP}^{\oplus k}(G)$ with a proof of size at most $O(2^k)$ each. □

We now prove the lower bound for PCR_k. Following [23], given a graph G, we consider the distribution $D_{k+1}(G)$ on partial assignments on variables of $\text{GOP}^{\oplus k+1}(G)$ defined as follows: for any variable $x_{a,b}$ of $\text{GOP}(G)$, select uniformly and independently $i \in [k+1]$ and then for all $j \in [k+1] - \{i\}$ uniformly and independently assign a $\{0,1\}$ value to $x^j_{a,b}$. The next lemma guarantees the applicability of the switching lemma and was proved in [23] for k-DNF. We rephrase it in terms of k-monomials, but its proof is exactly the same.

Lemma 20. *([23]) Let k be give and let m be a k-monomial formed by variables of $\text{GOP}^{\oplus k+1}(G)$ and their negations. There exists a constant $\gamma > 0$, dependent only on k, such that*

$$\Pr_{\rho \in D_{k+1}(G)}[m \restriction_{\rho^e} \neq 0] < 2^{-\gamma c(m)}$$

Proof. We say a collection of terms is independent when for any vertices a, b in G, at most one of its term contains a variable in $\{X^1_{a,b}, \ldots, X^{k+1}_{a,b}\}$ or in the corresponding negated set. The greatest independent collection of terms in m has at least $\frac{c(m)}{k(k+1)}$ members (otherwise we could build a cover smaller than $c(m)$). Notice that restrictions distributed according to $\mathcal{D}_{k+1}$ act independently on terms in such collection. A term contains at most k variables, each one assigned by the restriction with probability at least $1/2$: whatever happens to the variables corresponding to the same couple of vertices, only k of then are considered in an independent collection. Thus for each variable there is always at least $1/2$ probability that an alternative variable is left unassigned. Then with probability $(1/2)^k$ the term is fully assigned. With probability $(1/4)^k$ it is set to zero. Then the restriction fails to satisfy with probability

$$(1 - \frac{1}{4})^{\frac{c(m)}{k(k+1)}} < 2^{-\gamma c(m)}$$

for a γ which depends only from k. □

Notice that when we apply a restriction $\rho \in D_{k+1}(G)$ to $\text{GOP}^{\oplus k+1}(G)$ we not always reduce exactly to $\text{GOP}(G)$. It could happen that some variables have the opposite polarity. Anyway is clear that from a PCR refutation of $\text{GOP}^{\oplus k+1}(G)\restriction_\rho$ we can reconstruct a PCR proof of $\text{GOP}(G)$ of the same degree. Hence applying Theorem 3 we have the following Corollary.

Corollary 4. *Let G be an (r,c)-vertex expander. Then for all $k \geq 1$ and for all $\rho \in D_{k+1}(G)$, there are no* PC *refutations of $\text{GOP}^{\oplus k+1}(G)\restriction_\rho$ of degree less than or equal to $cr/4$.*

Theorem 5. *Let G be $(\delta n, c)$-vertex expander on n vertices, for some $\delta > 1$. Let $k \geq 1$, there exists a constant $\epsilon_{k,c}$, such that any PCR_k refutation of $\text{GOP}^{\oplus k+1}(G)$ contains at least $2^{\epsilon_{k,c} n}$ k-monomials.*

Proof. Let $r = \delta n$. By Lemma 20 applying the Switching Lemma setting $h = (rc/4 - k)$, we have that for any k-monomial m,

$$\Pr_{\rho \in D_{k+1}(G)}[DC(m\restriction_{\rho^e}) > (rc/4 - k)] \leq k2^{-(\frac{\gamma}{4})(rc/4-k)}$$

Hence there exists a constant $\epsilon_{k,\delta}$ such that

$$\Pr_{\rho \in D_{k+1}(G)}[DC(m\restriction_{\rho^e}) > (rc/4 - k)] \leq 2^{-(\epsilon_{k,c}n)}$$

Assume that there is PCR_k refutation of $\mathrm{GOP}^{\oplus k+1}(G)$ of size strictly less than $2^{-(\epsilon_{k,c}n)}$, then by the union bound there is a PCR_k refutation Π of $\mathrm{GOP}^{\oplus k+1}(G)\restriction_\rho$ with $DC(\Pi) \leq (rc/4 - k)$. Hence by Lemma 3 there is a PC refutation of $\mathrm{GOP}^{\oplus k+1}(G)\restriction_\rho$ of degree $\leq rc/4$. This is in contradiction with Corollary 4. □

Using the family of vertex expander used at the end of Section 5, previous Theorem and Proposition 2 we get the following exponential separation.

Corollary 5. *There is a family of contradictions $\mathcal{F}$ over n variables separating exponentially PCR_k from PCR_{k+1}, that is such that there are polynomial size refutations of $\mathcal{F}$ in PCR_{k+1} and any refutation of $\mathcal{F}$ in PCR_k requires exponential size.*

Acknowledgment We would like to thank Nathan Segerlind for interesting and helpful discussions about the paper of M. Alekhnovich [1] and to suggest a new strategy in a part of the proof of Lemma 2.4 in [1] that led us to the proof of Lemma 11.

References

[1] Michael Alekhnovich. Lower bounds for k-dnf resolution on random 3-cnfs. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 251–256, 2005.

[2] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM J. Comput.*, 31(4):1184–1211, 2002.

[3] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM J. Comput.*, 34(1):67–88, 2004.

[4] Michael Alekhnovich, Edward A. Hirsch, and Dmitry Itsykson. Exponential lower bounds for the running time of dpll algorithms on satisfiable formulas. In *31st International Colloquium on Automata, Languages and Programming*, pages 84–96, 2004.

[5] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *42nd Annual Symposium on Foundations of Computer Science*, pages 190–199, 2001.

[6] Albert Atserias, Maria Luisa Bonet, and Juan Luis Esteban. Lower bounds for the weak pigeonhole principle and random formulas beyond resolution. *Inf. Comput.*, 176(2):136–152, 2002.

[7] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on hilbert's nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.

[8] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, Pavel Pudlák, and Alan R. Woods. Exponential lower bounds for the pigeonhole principle. In *STOC*, pages 200–220, 1992.

[9] Eli Ben-Sasson and Russell Impagliazzo. Random cnf's are hard for the polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*, pages 415–421, 1999.

[10] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, pages 517–526, 1999.

[11] Maria Luisa Bonet and Nicola Galesi. A study of proof search algorithms for resolution and polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*, pages 422–432, 1999.

[12] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001.

[13] Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiri Sgall. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1997.

[14] Vasek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.

[15] 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*, pages 174–183, 1996.

[16] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3rd edition.* Springer, 2007.

[17] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43(4):439–561, 2006.

[18] J. Krajíček. Lower bounds for a proof system with an exponential speed-up over constant-depth frege systems and over polynomial calculus. In *Proceedings of the 22nd Inter. Symp. Mathematical Foundations of Computer Science*, pages 85–90, 1997.

[19] Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-3):123–140, 2001.

[20] Alexander Razborov. Pseudorandom generators hard for k-dnf resolution and polynomial calculus resolution. *Manuscript availbale at author's webpage*, 2003.

[21] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998.

[22] Omer Reingold, Salil Vadhan, , and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree. *Ann. of Math.*, 155(1):157–187, 2002.

[23] Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. A switching lemma for small restrictions and lower bounds for k-dnf resolution. *SIAM J. Comput.*, 33(5):1171–1200, 2004.

[24] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/