

Optimality of size-degree trade-offs for Polynomial Calculus

NICOLA GALESI and MASSIMO LAURIA

Dipartimento di Informatica, Sapienza - Università di Roma

There are methods to turn short refutations in *Polynomial Calculus* (PC) and *Polynomial Calculus with Resolution* (PCR) into refutations of low degree. Bonet and Galesi [1999; 2003] asked if such size-degree trade-offs for PC [Clegg et al. 1996; Impagliazzo et al. 1999] and PCR [Alekhovich et al. 2004] are optimal.

We answer this question by showing a polynomial encoding of *Graph Ordering Principle* on m variables which requires PC and PCR refutations of degree $\Omega(\sqrt{m})$. Trade-offs optimality follows from our result and from the short refutations of Graph Ordering Principle in [Bonet and Galesi 1999; 2001].

We then introduce the algebraic proof system PCR_k which combines together *Polynomial Calculus* (PC) and *k-DNF Resolution* (RES_k). We show a size hierarchy theorem for PCR_k : PCR_k is exponentially separated from PCR_{k+1} . This follows from the previous degree lower bound and from techniques developed for RES_k .

Finally we show that random formulas in conjunctive normal form (3-CNF) are hard to refute in PCR_k .

Categories and Subject Descriptors: F.2 [**Theory of Computation**]: Analysis of Algorithms and Problem Complexity

General Terms: Theory

Additional Key Words and Phrases: Algebraic Proofs, Computational Complexity, Polynomial Calculus, Proof complexity.

1. INTRODUCTION

One of the research directions to tackle fundamental complexity questions like $\text{NP} \neq \text{CO-NP}$ is the field of Propositional Proof Complexity. This area it is mainly concerned with showing non-trivial lower bounds for the length of proofs in sound and complete proof systems. Obtaining such results for all possible proof systems would separate NP from CO-NP. The approach one usually takes is that of proving non-trivial lower bounds for stronger specific proof systems until we have sufficient knowledge to infer a general result. Proof complexity has been an active area for almost 30 years, and thus many proof systems have been considered and many strong and important lower bounds (see [Beame and Pitassi

Nicola Galesi: Dipartimento di Informatica, Sapienza - Università di Roma.

Email: galesi@di.uniroma1.it

URL: <http://www.dsi.uniroma1.it/~galesi>

Massimo Lauria: Dipartimento di Informatica, Sapienza - Università di Roma.

Email: lauria@di.uniroma1.it

URL: <http://www.dsi.uniroma1.it/~lauria>

The research was partly supported by the project *Limiti di compressione in combinatoria e complessità computazionale* granted by Sapienza - Università di Roma.

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

© 20YY ACM 1529-3785/20YY/0700-0001 \$5.00

2001; Wigderson 2006; Segerlind 2006] for surveys on the topic) have been proved so far. Nevertheless we are still far from having lower bounds for text-book propositional proof systems, like Hilbert systems or Gentzen's PK calculus.

In this paper we deal with algebraic refutational proof systems. Algebraic systems based on Hilbert Nullstellensatz were introduced by Beame et al. [1996]. Later, Clegg et al. [1996] defined the Polynomial Calculus (PC), where the formula to refute is encoded as a set of unsatisfiable polynomial equations. Polynomial Calculus with Resolution (PCR) is a simple extension of PC defined in [Alekhovich et al. 2004]. Deductions are multilinear polynomials derived as elements of the ideal generated from the equations. Besides the length, a significant complexity measure considered for algebraic systems is the degree of polynomials used in a proof. Proving degree lower bounds in these systems is one of the main tasks in proof complexity. The work of Razborov [1998] proves the first linear degree lower bounds for the Pigeonhole principle in PC. It has been followed by several other degree lower bounds [Ben-Sasson and Impagliazzo 1999; Buss et al. 2001; Alekhovich and Razborov 2001; Razborov 2003], even for the class of random formulas which is one of the prominent hard classes for many proof systems.

The study of degree is not just a mathematical curiosity. It is connected with the complexity of proof search algorithms. In many applications we are faced with the problem of finding a proof of a given formula, if one exists.

A very important feature of PC is that there is a proof search algorithm based on the Gröbner Basis algorithm due to Clegg et al. in [1996]. The running time of the algorithm is a polynomial of degree equal to the minimal degree required to refute the principle. Thus the algorithm produces a polynomial size refutation in polynomial time for any formula with constant degree PC refutations. A degree lower bound also implies a lower bound on the running time of such algorithm.

This is similar to what happens for another well-known proof system related to PC, the system called Resolution. After the well known result “short proofs are narrow” of Ben-Sasson and Wigderson [1999], size lower bounds for the number of clauses in a proof can be discovered using the minimal width (i.e. number of literals in a clause). In studying the role of width in the complexity of proofs for Resolution, Ben-Sasson and Wigderson obtained a proof search algorithm for Resolution which strategy is to infer clauses of increasing width.

Both the works in [Ben-Sasson and Wigderson 1999] and in [Clegg et al. 1996] highlight a connection between size complexity and width/degree complexity, by the means of size-width (size-degree) trade-offs. They show that any formula with a short refutation in Resolution or PC has respectively a low width or low degree refutation, and this fact can be used to reduce the search space for a theorem prover.

Investigating the efficiency of the proof search algorithm proposed by Ben-Sasson and Wigderson, Bonet and Galesi [1999; 2001] proved that the class of formulas GT_n has polynomial size Resolution proofs but requires width equal to the square root of the number of variables in the formula. This implies the asymptotic optimality of the algorithm proposed in [Ben-Sasson and Wigderson 1999]. In [Bonet and Galesi 1999; 2003] they tried to extend the previous results to PC. Informally they asked the following questions: what is the efficiency of the Gröbner Basis Algorithm for PC when compared to Resolution? Can the Gröbner Basis algorithm for PC perform better than Resolution? They conjectured this is not the case, suggesting that some modifications of the GT_n principle would re-

quire square root degree refutations in PC. They gave some partial results in this direction, showing that a modification of the Pigeonhole Principle admits polynomial size Resolution refutations but requires $O(\log n)$ degree in Polynomial Calculus.

The main result in this paper is the proof of their conjectures using the Graph Ordering Principle $\text{GOP}(G)$. We show that when G has good vertex expansion, any PC refutation of $\text{GOP}(G)$ requires degree which is the square root of the number of propositional variables. On the other hand $\text{GOP}(G)$ admits polynomial size Resolution refutations. The existence of a formula with *high degree complexity* and a *short refutation* implies optimality of the size-degree trade-off for polynomial calculus. It also proves that for formulas with small Resolution refutations the degree of the PC simulation of Resolution shown in [Clegg et al. 1996] is optimal.

A form of optimality of the size-degree trade-off for PC was already established by Razborov's linear degree lower bound for pigeonhole principle in [Razborov 1998]. Nevertheless such principle requires exponential size to be proved. The optimality of proof search algorithms in this case is less interesting. Our results on $\text{GOP}(G)$ show that any strategy based on degree can be very inefficient on formulas with short refutations.

Our result follows from a new degree lower bound for the system of polynomials $\text{GOP}(G)$, which encodes the negation of a linear ordering principle over graphs. Our formula is a generalization to graphs of the linear ordering formula GT_n of [Bonet and Galesi 1999; 2001] and is a slight modification of a formula introduced in [Segerlind et al. 2004].

To prove the degree lower bound we use the approach devised by Razborov [1998] and refined in [Alekhovich and Razborov 2001]. We build a linear operator which sets to true all the consequences of $\text{GOP}(G)$ which can be deduced in PC using low degree. So far Razborov's technique has been applied to "matching-like" formulas such as the Pigeonhole formulas, random CNF's, etc... [Razborov 1998; 2003; Alekhovich et al. 2004; Alekhovich and Razborov 2001]. Our result extends this technique to other types of formula.

In the paper we also introduce a generalization of PCR. We define the system PCR_k which combines PC with RES_k . RES_k is a generalization of Resolution introduced by Krajíček in [2001], where k -DNFs (i.e. disjunctions of k -conjunctions) are used instead of clauses. Exactly as in PCR where monomials succinctly represent clauses, in PCR_k we generalize monomials to k -monomials to succinctly represent k -DNFs: monomials are then 1-monomials.

We show that the degree of a refutation in PCR_k is the same for PC and PCR. So we investigate the relative power of PCR_k with respect to PC and PCR in terms of the length of refutations, i.e. the number of k -monomials.

Using random restriction techniques and our PC/PCR degree lower bound for $\text{GOP}(G)$ we obtain lower bounds for the length of proofs in PCR_k (see Section 5). First we prove that PCR_k is a natural generalization of RES_k showing that any RES_k refutation can be simulated efficiently by PCR_k . Then using the switching lemma and the approach of Segerlind et al. in [2004] for RES_k and using our degree lower bound for $\text{GOP}(G)$ we prove an exponential separation between PCR_k and PCR_{k+1} . Finally using the results of Alekhovich in [Alekhovich 2005] together with PCR degree lower bounds for a certain encoding of linear equations developed in [Alekhovich et al. 2004], we prove that with high probability (as long as $k = o(\sqrt{\log n / \log \log n})$), any PCR_k refutation (over a field with characteristic

different from 2) of random 3-CNF with a linear number of clauses requires exponential size. We omit the details of this result, as it is very similar to the one in [Alekhovich 2005]. Details appeared in a preliminary version of this work at [Galesi and Lauria 2007].

The paper is organized as follows. In Section 2 we give all the preliminary definitions. In Section 3 we introduce our graph ordering principle, we prove the degree lower bounds for $\text{GOP}(G)$ and we discuss its consequences for the size-degree trade-off. In Section 4 we define PCR_k and discuss its relations with other proof systems. Finally in Section 5 we prove the exponential separation between PCR_k and PCR_{k+1} and we discuss the lower bounds for random 3-CNF.

2. PRELIMINARIES

Let V be a set of boolean variables. A literal l is either a variable x or its 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; a k -DNF is the disjunction of k -terms. The *width* of a clause is the number of literals in the clause. A partial assignment is a mapping $\rho : \{x_1, \dots, x_n\} \rightarrow \{0, 1, *\}$; we let $\text{Dom}(\rho)$ to be $\rho^{-1}(\{0, 1\})$. Given a restriction ρ and a boolean formula F by $F \upharpoonright_\rho$ we denote the formula obtained from F after setting all the variables in $\text{Dom}(\rho)$ according to ρ , simplifying F in the natural way and leaving all the other variables unassigned.

2.1 Notions from commutative algebra

Given a field \mathbb{F} , we consider polynomials in the ring $\mathbb{F}[x_1, \dots, x_n]$. Given a set $E = \{f_1, \dots, f_n\}$ of polynomials, by $\text{Span}(E)$ we denote the ideal generated by E , that is the set

$$\left\{ \sum_i (f_i \cdot h_i) \mid h_i \in \mathbb{F}[x_1, \dots, x_n] \right\}$$

. We say that a set of polynomials f_1, \dots, f_n *semantically implies* a polynomial g if any assignment that satisfies $f_i = 0$ for all $i \in [n]$, also satisfies $g = 0$. We write $f_1, \dots, f_n \models g$ or $E \models g$.

We define a notion of residue of polynomials with respect to an ideal. We consider the standard *graded lexicographic (grlex)* monomial order (denoted as $<_{\mathbb{P}}$) as given in [Cox et al. 2007]. In particular *grlex* is defined as follows: $1 <_{\mathbb{P}} x_1 <_{\mathbb{P}} x_2 <_{\mathbb{P}} \dots <_{\mathbb{P}} x_n$. For any two products of variables m, m' and a variable x the following two properties hold: (a) if $m <_{\mathbb{P}} m'$ then $xm <_{\mathbb{P}} xm'$; (b) $m <_{\mathbb{P}} xm$. This order is lexicographically extended to polynomials, and 0 is the smallest of them.

Notice that *grlex* is not a total order, thus there could be incomparable $q, q' \in \text{Span}(E)$. This can happen if and only if the underlying sets of monomials are equal but have different coefficients. In that case there exists a linear combination of q and q' which is strictly smaller than both, and which is in $\text{Span}(E)$. Thus a minimum element in $\text{Span}(E)$ always exists.

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

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

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

We shall consider polynomials on the field \mathbb{F} defined on the domain $\{0, 1\}^n$. More explicitly we consider elements of the ring $\mathbb{F}[x_1, \dots, x_n] / \{x_i^2 - x_i\}_{i \in [n]}$. Such polynomials are the base for all algebraic proof systems we will consider.

2.2 Proof systems

Polynomial Calculus (PC) is a refutational system defined in [Clegg et al. 1996], and based on the ring $\mathbb{F}[x_1, \dots, x_n]$ of polynomials. We always consider equations of the form $p = 0$, and we simply denote them as p . The equations are intended to hold on $\{0, 1\}^n$ thus 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 :

$$\frac{p \quad q}{\alpha p + \beta q} \quad \text{Sum Rule} \qquad \frac{p}{xp} \quad \text{Product Rule}$$

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

PC is a complete proof system, in the sense that a polynomial g has a PC proof from a set of polynomials E iff $g(\vec{x}) = 0$ for every $\vec{x} \in \{0, 1\}^n$ which is a common root of E . Moreover E has no common $\{0, 1\}$ solutions (we call E contradictory) iff $1 \in \text{Span}(E \cup \{x_i^2 - x_i\}_{i \in [n]})$. Completeness of PC comes as a corollary of Hilbert's Nullstellensatz (see [Cox et al. 2007]) and from complete algorithms based on Gröebner bases [Clegg et al. 1996].

Given a PC proof Π , the *degree* of Π , $\text{deg}(\Pi)$, 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.

We remark here that when we work in Polynomial Calculus, we implicitly assume that the polynomials $\{x_i^2 - x_i\}_{i \in [n]}$ are always included in the set of initial polynomials. With this assumption in mind we always have that $E \vdash p - R_E(p)$ for any polynomial p .

Polynomial Calculus with Resolution (PCR) [Alekhovich et al. 2004] is a refutational system which extends PC to polynomials in the ring $\mathbb{F}[x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n]$, where $\bar{x}_1, \dots, \bar{x}_n$ 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 cause an exponential increase in size. Moreover any Resolution refutation can be easily transformed in a PCR refutation of degree equal to the width of the original one.

Resolution on k -DNF (RES_k) [Krajíček 2001] is a sound and complete refutational system which extends *Resolution* (RES) with k -DNFs. The rules are the following ones:

$$\begin{array}{c} \frac{A}{A \vee l} \quad \text{Weakening} \qquad \frac{A \vee l_1 \quad \dots \quad A \vee l_j}{A \vee \bigwedge_{i=1}^j l_i} \quad \wedge\text{-intro}, 1 < j \leq k \\ \\ \frac{A \vee \bigwedge_{i=1}^j l_i}{A \vee l_i} \quad \wedge\text{-elim}, 1 < j \leq k \qquad \frac{A \vee \bigwedge_{i=1}^j l_i \quad B \vee \bigvee_{i=1}^j \neg l_i}{A \vee B} \quad \text{Cut}, 1 < j \leq k \end{array} \quad (1)$$

A *proof* in RES_k 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 the result of a rule application on 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 , denoted as $S(\Pi)$, is the total number of symbols appearing in Π . The *length* of Π , $|\Pi|$, is the number of lines in the sequence defining Π .

Polynomial Calculus on k -DNF (PCR_k) We discuss an extension of Polynomial Calculus which includes RES_k in the same way PCR includes Resolution. Any line in a proof is a sum of algebraic formulas called k -monomials, each of them is a succinct representation of a k -DNF in the same way PCR monomials succinctly represent boolean clauses. Such sum is called a k -polynomial. The following translation relates k -DNFs and k -monomials.

$$\prod_j \left(1 - \prod_{i=1}^{k_j} \bar{l}_i \right) \longleftrightarrow \bigvee_j \left(\bigwedge_{i=1}^{k_j} l_i \right) \quad \text{where } k_j \leq k$$

Such translation is consistent with the usual convention of algebraic proof systems in which 0 represents *true* and 1 represents *false*.

Notice that proof lines in PCR_k are algebraic formulas and can be written as polynomials. The issue here is that some functions have short k -polynomial representations, but require large size to be represented as polynomials. This is similar to what happens in RES_k , where a short k -DNF could require a very large number of clauses to be represented in RES.

The axioms of PCR_k include those of PCR plus axioms

$$1 - y_1 y_2 \dots y_j - (1 - y_1 y_2 \dots y_j) \text{ for } j \leq k$$

for any set $\{y_1, y_2, \dots, y_j\}$ of variables (even negated ones) of size less than or equal to k . These axioms introduce syntactical parentheses and allow expansion of k -polynomials. Analogously, the rules of PCR_k are those of PCR with one more weakening rule

$$\frac{p}{(1 - y_1 \dots y_j)p} \text{ for } j \leq k$$

Size $S(\Pi)$ of a proof Π is measured in term of number of k -monomials appearing in the proof. The length $|\Pi|$ is the number of lines in the proof.

A PCR_k proof of a k -polynomial g from k -polynomials f_1, \dots, f_n (denoted by $f_1, \dots, f_n \vdash g$) is a sequence of k -polynomials ending with g , each one obtained either from an axiom or by applying a rule to previously derived k -polynomials. In particular a PCR_k refutation is a proof of 1.

2.3 Expander Graphs of constant degree

DEFINITION 1. Let a graph $G = (V, E)$ be given, for any $U \subseteq V$, the neighborhood of U , $\Gamma(U)$, is the set of vertices in $V \setminus U$ which have an adjacent vertex in U . The graph G is said to be an (r, c) -vertex expander if for any set $U \subseteq V$ with $|U| \leq r$, $|\Gamma(U)| \geq c|U|$. We call c the vertex expansion of G .

Let $E(U, U')$ be the set of edges between U and U' for disjoint sets $U, U' \subseteq V$. The graph G is said to be an (r, c) -edge expander if for any set $U \subseteq V$ with $|U| \leq r$, $|E(U, V \setminus U)| \geq c|U|$. We call c the edge expansion of G .

For our result we need a family of $O(1)$ -regular graphs which are $(\Theta(n), \Theta(1))$ -vertex expanders of n vertices. Such families exist and there are several constructions in the literature. An efficient construction is given in [Hoory et al. 2006] using a graph composition devised in [Reingold et al. 2002] and called *zig-zag product*. Such construction provides a d regular $(\Theta(n), \Theta(1))$ -edge expander, and any d regular (r, c) -edge expander is also an $(r, c/d)$ -vertex expander.

PROPOSITION 1. (Proposition 9.2 [Hoory et al. 2006], d fixed to 3) For any t an undirected graph G can be constructed, such that G has d^{4t} vertices, it is 9 regular and is a $(\frac{V(G)}{2}, \frac{1}{2})$ -edge expander. Thus it is also a $(\frac{V(G)}{2}, \frac{1}{18})$ -vertex expander.

Notice that such graphs have multiple edges. This is not an issue because removing repeated edges only reduces the degree and does not modify vertex expansion. Whenever we say in the following that G is an (r, c) -vertex expander, we assume it has constant degree.

3. LOWER BOUND FOR GRAPH ORDERING PRINCIPLE

In this section we prove that certain graph ordering tautologies have no low degree PC refutations. Ordering tautologies were introduced in [Krishnamurty 1985; Stalmark 1996], they have been used in [Bonet and Galesi 1999; 2001] to prove the optimality of the size-width trade-off for resolution [Ben-Sasson and Wigderson 1999] and used in [Segerlind et al. 2004] to obtain an exponential separation between RES_k and RES_{k+1} .

We present a (negated) Graph Ordering Principle and we show that such formula has a short refutation (Lemma 1). Under some assumptions on the graph we also show a degree lower bound for such formula (Theorem 1). The core of the theorem is Lemma 2. We immediately prove the main results then we devote the rest of the section to the proof of Lemma 2.

Graph Ordering Principle: if we give directions to the edges of a simple undirected graph according to a total order \prec on its vertices, then there is a vertex which is less than any of its neighbours.

Directions are encoded as variables $x_{a,b}$ for any $a, b \in [n]$ such that $a < b$, where $<$ is the standard order of 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 polynomial constraints. The

first one, that we call \mathcal{T} , expresses that the relation \prec is a total order on $[n]$:

$$\forall a < b < c \quad x_{a,b}x_{b,c}(1 - x_{a,c}) \quad (2)$$

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

Equations in (2) and (3) say that there are no cycles of three elements in $[n]$ according to \prec . This implies transitivity. Moreover notice that we do not need the usual antisymmetry 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 is no vertex in G which is less than all its neighbours (according to \prec). We denote $\Gamma(u)$ the set of vertices adjacent to u in G .

$$\forall u \in V \quad \prod_{a \in \Gamma(u): a < u} (1 - x_{a,u}) \cdot \prod_{a \in \Gamma(u): a > u} x_{u,a} \quad (4)$$

Each equation has degree at most equal to the degree of G . We denote as M_u the equation in (4) which corresponds to the vertex $u \in G$ and we extend this notation to sets of vertices: for $U \subseteq [n]$ we denote with M_U the corresponding set of constraints in (4). We call $\text{GOP}(G)$ the union of \mathcal{T} with the equations $M_1 \dots M_n$ induced by G . The CNF encoding of $\text{GOP}(G)$ has a well known short refutation in Resolution [Stalmark 1996; Bonet and Galesi 1999; 2001] which has an efficient simulation in PCR.

LEMMA 1. *There are PC and PCR refutations of $\text{GOP}(G)$ of degree $O(n)$. Moreover if G has constant degree then PCR refutations have size $O(n^{O(1)})$.*

PROOF. Consider the proof system PCR and a vertex $u \in V$. By using M_u and the axioms $1 - x_{a,b} - \bar{x}_{a,b} = 0$ it is easy to prove that

$$M_u \vdash \prod_{a \in \Gamma(u): a < u} \bar{x}_{a,u} \cdot \prod_{a \in \Gamma(u): a > u} x_{u,a} = 0$$

in size $2^{\deg(G)}$ and degree $\deg(G)$. By weakening we deduce $\prod_{a < u} \bar{x}_{a,u} \cdot \prod_{a > u} x_{u,a} = 0$ in degree $O(n)$. Call M'_u such equation. Notice that $\mathcal{T} \cup \{M'_1 \dots M'_n\}$ is essentially a polynomial encoding of the GT_n formula considered in [Stalmark 1996; Bonet and Galesi 1999; 2001]. In those papers there are several polynomial size Resolution refutations of width $O(n)$. We get the claim for PCR by simulating any of them. We can also transform them in PC refutations by mapping \bar{x} variables to $1 - x$. The size increases exponentially but the degree does not change. \square

To prove a degree lower bound for $\text{GOP}(G)$ we follow the approach devised in [Alekhovich and Razborov 2001]. We show a non trivial linear operator which sets to 0 all polynomials deducible in low degree from $\text{GOP}(G)$.

LEMMA 2. *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 any polynomial $p \in \text{GOP}(G)$
- (2) for each monomial t and for each variable x , if $\deg(t) < cr/4$, then $\mathcal{L}(x \cdot t) = \mathcal{L}(x) \cdot \mathcal{L}(t)$

(3) $\mathcal{L}(1) = 1$.

We postpone the proof of this lemma to the end of the section. Now we show that Lemma 2 implies the following statement.

THEOREM 1. *If G is an (r, c) -vertex expander then there is no PC refutation of $\text{GOP}(G)$ of degree less than or equal to $cr/4$.*

PROOF. Assume for the sake of contradiction that such refutation exists. Apply \mathcal{L} on all its lines. Any polynomial in $\text{GOP}(G)$ is set to 0 because of property 1 of \mathcal{L} stated by Lemma 2; any inference using sum rule is set to 0 because of linearity of \mathcal{L} ; any inference using the product rule of PC keeps all terms below degree $cr/4$ by assumption, so property 2 of \mathcal{L} implies that the result of such inference is set to 0. By induction on the lines of the proof the last line is mapped to 0. This is a contradiction because the last line (i.e the polynomial 1) is not mapped to 0 according to property 3 of \mathcal{L} . \square

Before proving Lemma 2 we give an overview of the argument. We want to estimate the amount of information required to deduce an equation. In particular we are interested in the set of premises of the form (4) used for any deduction. It is natural to identify such set as a set of vertices. The intuition is that any equation deduced from a small set of vertices is “locally deducible”. More concretely for any monomial t we are interested in deductions like $t - R_{\mathcal{T}, M_I}(t) = 0$, which is a locally deducible if I is a small set. The lower bound comes from the following considerations:

- $1 = 0$ is not locally deducible.
- When G is an expander, any non-local deduction requires high degree (i.e. low degree deductions are local).

We capture local reasoning with the operator \mathcal{L} : its kernel will contain all linear combinations of local deducible equations. In the following we assume G to be given and to be a constant degree (r, c) -vertex expander. All the definitions are given with respect to such graph.

Our candidate for the set of relevant vertices of a monomial t is called *Support* of t . In Lemma 4, 5, 6 we prove that this choice is correct.

DEFINITION 2. *Given a set of vertices U we define the inference relation \rightsquigarrow_U in this way: For $A, B \subseteq [n]$,*

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

Consider a **maximal** sequence of sets B_1, B_2, \dots, B_k such that for all $1 \leq i \leq k$:

$$\left(\bigcup_{j < i} B_j \right) \rightsquigarrow_U B_i \tag{5}$$

$$B_i \not\subseteq \left(\bigcup_{j < i} B_j \right) \tag{6}$$

We define the support of U as

$$\text{Sup}(U) := \bigcup_{i=1}^k B_i$$

We call $\text{Vertex}(p)$ the set of vertices mentioned in the variables occurring in a polynomial p . We denote the set $\text{Sup}(\text{Vertex}(p))$ as $\text{Sup}(p)$.

FACT 1. *The value of $\text{Sup}(U)$ is uniquely determined by U .*

PROOF. Any new set in the sequence must contain a new vertex because of (6), thus any sequence is finite. Consider two sequences B_1, \dots, B_k and C_1, \dots, C_l obtained from U as in the previous definition. Fix $S := C_1 \cup \dots \cup C_l$: we will show that $B_i \subseteq S$ for all i . This implies that the union of the first sequence is included in the union of the second. By swapping sequences we also have the reverse inclusion. Thus any two different sequences give rise to the same support.

We proceed by induction on i . Notice the fact (immediate from the definition) that if $X \rightsquigarrow_U Y$ then $Z \cup X \rightsquigarrow_U Y$ for any Z . Thus $\emptyset \rightsquigarrow_U B_1$ implies $S \rightsquigarrow_U B_1$. This means $B_1 \subseteq S$ otherwise the second sequence would not be maximal. For $i > 0$ we know $(\bigcup_{j < i} B_j) \rightsquigarrow_U B_i$. By inductive hypothesis $(\bigcup_{j < i} B_j) \subseteq S$ thus $S \rightsquigarrow_U B_i$ which again implies $B_i \subseteq S$ because of the maximality of S . \square

FACT 2. *If $\text{Sup}(U) := B_1 \cup \dots \cup B_k$ then for any $1 \leq i \leq k$, $\Gamma(B_1 \cup \dots \cup B_i) \subseteq U$.*

PROOF. By induction on i . If $i = 1$ then $\Gamma(B_1) \subseteq U$ by definition. For $i > 1$ any $v \in \Gamma(B_1 \cup \dots \cup B_i)$ is either in $\Gamma(B_1 \cup \dots \cup B_{i-1})$ or in $\Gamma(B_i) \setminus (B_1 \cup \dots \cup B_{i-1})$. In the former case $v \in U$ by inductive hypothesis. In the latter case $v \in U$ because of equation (5). \square

Let us discuss briefly the intuition behind the definition of support. To infer equations from $\text{GOP}(G)$ we use the hypothesis that some vertices are not local minimums. To deduce a useful equation about a monomial t a proof uses either knowledge about vertices in t , or knowledge about vertices appearing in previous steps in order to take advantage of monomial cancellation. Each set in the sequence should capture a local deduction (i.e. based on small sets of vertices), and the support roughly estimates the knowledge required for the whole sequence. The following lemma says that if the underlying graph is an expander then all low degree monomials have small supports.

LEMMA 3. *If a set U has size less than or equal to $cr/2$ then $\text{Sup}(U)$ has size less than or equal to $r/2$. If a monomial t has degree less than or equal to $cr/4$ then $\text{Sup}(t)$ has size less than or equal to $r/2$.*

PROOF. Let $\text{Sup}(U) = I_1 \cup I_2 \cup I_3 \cup \dots \cup I_l$ where each I_i is the set added in the i -th step of the inference. If the size of $\text{Sup}(U)$ is bigger than $r/2$, then there is a step j where $r/2$ is overcome. Let us denote $A = I_1 \cup \dots \cup I_{j-1}$ 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 $|\Gamma(A \cup I)| > cr/2$ because of the vertex expansion of the graph. This proves the first part of the claim since $\Gamma(A \cup I) \subseteq U$ as shown in Fact 2.

The second part follows since the number of vertices appearing in term t is at most twice the degree of t . \square

So far we have shown that a low degree monomial has small support, but this is not sufficient. We need to show that the support captures the reasoning power of local deductions. Consider a fixed monomial t and a locally deducible equation $t - p = 0$ with $p <_{\mathbb{P}} t$. For any vertex v which is not in the support of t , we show that equation M_v is not needed to

deduce $t - p = 0$. To do this we observe that v has a neighbour u which is completely irrelevant for the local deduction. By assigning u to be a global minimum, we restrict M_v to 0 without changing the deduction. In Lemma 4, 5, 6 we show that we can remove superfluous premises one by one. This implies that local deductions are actually captured by the support. By the expansion of the graph we know that support in a low degree proof is small, and in particular it is insufficient for a refutation.

A partial assignment ρ to the variables of $\text{GOP}(G)$ is a u -cta (critical truth assignment) when it sets u as a global minimum and leaves unassigned all other variables.

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

LEMMA 4. *Let t be a monomial. For any set of vertices A of size less than or equal to $r/2$ and such that $A \not\subseteq \text{Sup}(t)$, there exists an edge $\{u, v\}$ in G such that $v \in A \setminus \text{Sup}(t)$, $u \notin \text{Sup}(t) \cup A \cup \text{Vertex}(t)$.*

PROOF. By definition of $\text{Sup}(t)$ and the hypothesis, it follows that $\text{Sup}(t) \not\rightsquigarrow_{\text{Vertex}(t)} A$. Then $\Gamma(A) \not\subseteq \text{Sup}(t) \cup \text{Vertex}(t)$, therefore there is a vertex u in $\Gamma(A) \setminus (\text{Sup}(t) \cup \text{Vertex}(t))$. Let v be a neighbour of u in A , then $v \notin \text{Sup}(t)$ because of Fact 2. \square

LEMMA 5. *Let t be a monomial. Let I be a set of vertices such that $|I| \leq r/2$ and $I \supset \text{Sup}(t)$. Then there exists a $v \in I \setminus \text{Sup}(t)$ such that:*

$$R_{\mathcal{T}, M_I}(t) = R_{\mathcal{T}, M_{I-\{v\}}}(t)$$

PROOF. Applying Lemma 4 to t and I we get an edge $\{u, v\}$ such that $v \in I \setminus \text{Sup}(t)$ and $u \notin I \cup \text{Vertex}(t)$. 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 $\mathcal{T} \upharpoonright_{\rho} \subseteq \mathcal{T}$. Moreover since $u \notin \text{Vertex}(t)$, $t \upharpoonright_{\rho} = t$. Finally note that $M_I \upharpoonright_{\rho} \subseteq M_{I-\{v\}}$ since ρ is setting to 0 at least M_v . Recall that if $A \vdash p$ and $B \supseteq A$ then $B \vdash p$. Thus we have the following derivations:

$$\mathcal{T}, M_I \quad \vdash \quad t - R_{\mathcal{T}, M_I}(t) \quad \text{By definition of } R_E \quad (7)$$

$$\mathcal{T} \upharpoonright_{\rho}, M_I \upharpoonright_{\rho} \quad \vdash \quad t \upharpoonright_{\rho} - R_{\mathcal{T}, M_I}(t) \upharpoonright_{\rho} \quad \text{By restriction from (7)} \quad (8)$$

$$\mathcal{T}, M_{I-\{v\}} \quad \vdash \quad t - R_{\mathcal{T}, M_I}(t) \upharpoonright_{\rho} \quad \text{By previous observations on (8)} \quad (9)$$

From (9) and minimality of the residue we then have that $R_{\mathcal{T}, M_{I-\{v\}}}(t) \leq_{\mathbb{P}} R_{\mathcal{T}, M_I}(t) \upharpoonright_{\rho}$. Moreover, since $\mathcal{T}, M_I \vdash t - R_{\mathcal{T}, M_{I-\{v\}}}(t)$, we have that $R_{\mathcal{T}, M_I}(t) \leq_{\mathbb{P}} R_{\mathcal{T}, M_{I-\{v\}}}(t)$, also by minimality. Finally $R_{\mathcal{T}, M_I}(t) \upharpoonright_{\rho} \leq_{\mathbb{P}} R_{\mathcal{T}, M_I}(t)$ holds since a restriction can only decrease the order of a polynomial. Hence it must be $R_{\mathcal{T}, M_{I-\{v\}}}(t) = R_{\mathcal{T}, M_I}(t)$. \square

We have shown that from any local deduction we can remove at least one of the superfluous assumptions. As an immediate corollary we get that any vertex out of the support is superfluous (at least when we limit ourselves to local deductions!).

LEMMA 6. *Let t be a monomial. For any set of vertices I of size less than or equal to $r/2$ and such that $I \supseteq \text{Sup}(t)$, the following holds:*

$$R_{\mathcal{T}, M_I}(t) = R_{\mathcal{T}, M_{\text{Sup}(t)}}(t)$$

PROOF. If $I = \text{Sup}(t)$ then $R_{\mathcal{T}, M_I}(t) = R_{\mathcal{T}, M_{\text{Sup}(t)}}(t)$. If I is strictly bigger than S , then by Lemma 5 there is a vertex $v \in I \setminus \text{Sup}(t)$ such that $R_{\mathcal{T}, M_I}(t) = R_{\mathcal{T}, M_{I-\{v\}}}(t)$. The lemma follows by induction on the size of $I \setminus \text{Sup}(t)$. \square

Next lemma is only a technical detail: it says the obvious fact that deductions do not need to introduce any vertex which is not in the support and in the original monomial.

LEMMA 7. For any term t , $Vertex(R_{\mathcal{T}, M_{Sup(t)}}(t)) \subseteq Sup(t) \cup Vertex(t)$.

PROOF. Assume for the sake of contradiction that there is a vertex $u \in Vertex(R_{\mathcal{T}, M_{Sup(t)}}(t))$ not in $Vertex(t) \cup Sup(t)$. Consider a u -cta ρ . By an argument analogous to that of Lemma 5 we have $R_{\mathcal{T}, M_{Sup(t)}}(t) \leq_{\mathbb{P}} R_{\mathcal{T}, M_{Sup(t)}}(t) \upharpoonright_{\rho} <_{\mathbb{P}} R_{\mathcal{T}, M_{Sup(t)}}(t)$. \square

We are ready to give the proof of Lemma 2.

PROOF. **Lemma 2**

For any monomial t , the linear operator $\mathcal{L}(t)$ is defined by

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

and is extended by linearity to any polynomial. We prove that this operator satisfies the three claimed requirements.

Requirement 1. For any polynomial $p \in \text{GOP}(G)$, $\mathcal{L}(p) = 0$.

Let $p = \sum \beta_i t_i$ in \mathcal{T} . By definition $\mathcal{L}(p) = \sum \beta_i \mathcal{L}(t_i) \leq_{\mathbb{P}} \sum \beta_i R_{\mathcal{T}}(t_i) = R_{\mathcal{T}}(p) = 0$. For any equation M_v let $M_v = t+w$, where t is the leading term. Since $\Gamma(v) \subseteq Vertex(t)$, then $v \in Sup(t)$. Hence $\mathcal{L}(v) = \mathcal{L}(t) + \mathcal{L}(w) \leq_{\mathbb{P}} R_{M_v}(t) + \mathcal{L}(w) = -w + \mathcal{L}(w) \leq_{\mathbb{P}} -w + w = 0$.

Requirement 2. For any term t of degree strictly less than $\frac{cr}{4}$ and any variable x , it is true that $\mathcal{L}(xt) = \mathcal{L}(x\mathcal{L}(t))$.

Notice that by monotonicity of Sup function, $Sup(xt) \supseteq Sup(t)$. Moreover since $deg(xt) \leq \frac{cr}{4}$, then by Lemma 3 we get $|Sup(xt)| \leq r/2$. Therefore we have the following chain of equalities:

$$\mathcal{L}(xt) = R_{\mathcal{T}, M_{Sup(xt)}}(xt) \quad \text{by definition} \quad (10)$$

$$= R_{\mathcal{T}, M_{Sup(xt)}}(xR_{\mathcal{T}, M_{Sup(xt)}}(t)) \quad \text{by Property 1 of residue} \quad (11)$$

$$= R_{\mathcal{T}, M_{Sup(xt)}}(xR_{\mathcal{T}, M_{Sup(t)}}(t)) \quad \text{by monotonicity of } Sup \text{ and Lemma 6} \quad (12)$$

$$= R_{\mathcal{T}, M_{Sup(xt)}}(x\mathcal{L}(t)) \quad \text{by definition} \quad (13)$$

Let us write $x\mathcal{L}(t)$ as a polynomial $\sum \alpha_i r_i$. The following inclusions hold respectively: in (14) because r_i is a monomial in the polynomial expansion of $x\mathcal{L}(t)$; in (15) by Lemma 7; in (16) by monotonicity of Sup .

$$Vertex(r_i) \subseteq Vertex(x) \cup Vertex(\mathcal{L}(t)) \quad (14)$$

$$\subseteq Vertex(x) \cup Vertex(t) \cup Sup(t) \quad (15)$$

$$\subseteq Vertex(xt) \cup Sup(xt) \quad (16)$$

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

Finally the second requirement follows from the following chain of equalities.

$$\mathcal{L}(x\mathcal{L}(t)) = \sum \alpha_i R_{\mathcal{T}, M_{Sup(r_i)}}(r_i) \quad \text{by definition} \quad (17)$$

$$= \sum \alpha_i R_{\mathcal{T}, M_{Sup(xt)}}(r_i) \quad \text{by Lemma 6 applied to } Sup(r_i) \text{ and } Sup(xt) \quad (18)$$

$$= R_{\mathcal{T}, M_{Sup(xt)}}\left(\sum \alpha_i r_i\right) \quad \text{by linearity} \quad (19)$$

$$= R_{\mathcal{T}, M_{Sup(xt)}}(x\mathcal{L}(t)) \quad \text{by rewriting } x\mathcal{L}(t) \quad (20)$$

$$= \mathcal{L}(xt) \quad \text{by equalities (10)-(13)} \quad (21)$$

Requirement 3. Observe that the support of a constant polynomial is the empty set, so $\mathcal{L}(1) = R_{\mathcal{T}}(1) = 1$ since \mathcal{T} is satisfiable. \square

We conclude the section by claiming that there are indeed infinite families of graphs with the desired properties. This implies that there are actual formulas for which both upper and lower bounds applies.

THEOREM 2. *There exists an infinite family \mathcal{G} of simple graphs of constant degree such that for any G in \mathcal{G} the principle $\text{GOP}(G)$ has polynomial size in $|V(G)|$ and any PC refutation of $\text{GOP}(G)$ requires degree at least $\frac{|V(G)|}{108}$.*

PROOF. Fix any integer t . By Proposition 1 we can construct a 9-regular graph G of $n := 81^t$ vertices, such that G is a $(\frac{n}{2}, \frac{1}{2})$ -edge expander. Since G is 9-regular, it is also a $(n/2, 1/18)$ -vertex expander. To obtain a simple graph without losing vertex expansion it is sufficient to collapse multi-edges in simple edges. By Theorem 1 the theorem follows. \square

3.1 Optimality of Size vs Degree Trade-offs

There exists a relation between the smallest size S and smallest degree D of a proof in Polynomial Calculus and Polynomial Calculus with Resolution. Let d be the degree of polynomials used to formulate the principle and m the number of its variables, then in [Clegg et al. 1996; Alekhovich et al. 2004] it is shown:

$$S \geq 2^{\Theta(\frac{D-d}{m})} \quad D \leq \Theta(\sqrt{m \log S})$$

thus $\text{GOP}(G)$ is tight in term of the exponent because it has $m = \Theta(n^2)$, $D = \Theta(\sqrt{m})$, $d = O(1)$ and $S = m^{O(1)}$.

We state the simulation Theorem of Clegg, Edmonds and Impagliazzo [1996]:

THEOREM 3. *([Clegg et al. 1996]) If a set of clauses F over n variables and of width at most k , has a dag-like resolution refutation of size S , then the set of polynomials encoding F has a PC refutation of degree at most $3\sqrt{n \log_e S} + k + 1$.*

The trade-off of the previous Theorem is optimal, since there is a trivial resolution proof of size $O(2^n)$ for the PHP_n^{n+1} , and Razborov [1998] shows that PHP_n^m requires $\Omega(n)$ degree PC refutations for any $m > n$. Notice that this optimality result uses formulas requiring exponential size in Resolution.

Bonet and Galesi [1999; 2003] asked to prove the optimality of the trade-off with formulas having polynomial size refutations. They show partial results in this direction proving that a modification of the pigeonhole principle has efficient refutations in Resolution but requires degree $\Omega(\log n)$.

Our result on $\text{GOP}(G)$ exponentially improves that result: it shows a square root degree lower bound for a formula with efficient refutations in Resolution and PCR. Notice that optimality of the trade-off is true for PC even if PC would require exponential size to simulate such efficient refutation of $\text{GOP}(G)$. This is not an issue because PCR proof system is nothing else than PC with more axioms and variables. Thus we can extend $\text{GOP}(G)$ with these missing bits. The resulting principle has obviously an efficient refutation and a square root degree lower bound.

4. EXTENDING POLYNOMIAL CALCULUS TO K -DNF'S: PCR_K

To study the complexity of proofs in PCR_k we follow the approach used by Segerlind et al. [2004] for RES_k . In [Segerlind et al. 2004] they prove a Switching Lemma: with high probability any k -DNF is restricted to a shallow decision tree by a random assignment. This easily translates to Lemma 8 where we deal with k -monomials restricted into low degree multilinear polynomials. So, as Segerlind et al. [2004] reduce size lower bounds for RES_k to width lower bounds for Resolution, we can reduce size lower bounds for PCR_k to degree lower bounds for PC.

4.1 Boolean functions, polynomials and Switching Lemma

We consider *boolean polynomials* on the field \mathbb{F} , i.e. polynomials defined on the domain $\{0, 1\}^n$, that is elements of the ring $\mathbb{F}[x_1, \dots, x_n]/\{x_i^2 - x_i\}_{i \in [n]}$. We say that a boolean polynomial p on a field $\mathbb{F}[x_1, \dots, x_n]$, *represents* a boolean function F over variables x_1, \dots, x_n and with values in \mathbb{F} , if p and F agree on all possible assignments to their variables. We state the following easy facts about boolean polynomials.

PROPOSITION 2. *The following hold:*

- Any function on $\{0, 1\}^n$ with values in \mathbb{F} has a unique representation in terms of boolean polynomials.
- If a boolean function F is computed by a decision tree of height h , then there is a boolean polynomial representing F with degree less than or equal to h .

PROOF. (1) For any $\alpha \in \{0, 1\}^n$ consider the boolean function χ_α which is 1 on α and 0 everywhere else, and the multilinear polynomial $p_\alpha := \prod_{\alpha_i=0} (1 - x_i) \prod_{\alpha_i=1} x_i$. A map from χ_α to p_α induces an injective homomorphism between vector spaces, because linear independent functions are mapped to linear independent polynomials. It is also a bijection because the spaces have the same dimension. (2) Consider a leaf l of the decision tree. Let v_l be the value of the function, and ϕ_l be the conjunction of width at most h which is true if and only if the decision tree evaluates to the leaf l : ϕ_l is computable by the boolean polynomial $p_l := \prod_{\bar{x}_i \in \phi_l} (1 - x_i) \prod_{x_i \in \phi_l} x_i$. Clearly F is computed by the polynomial $\sum_l v_l p_l$. \square

For a function F on boolean variables we define the concept of *semantic degree* $\text{sdeg}(F)$ as the degree of the boolean polynomial representing F . By the previous proposition the semantic degree of a boolean function is well-defined and is less than or equal to the minimal height of a decision tree representing F .

DEFINITION 3. Let τ be a k -monomial on $\{x_1, \dots, x_n\}$ we call $c(\tau)$ the size of the smallest set of variables containing at least one variable from every factor of τ . We call c the covering number of τ .

Recall Corollary 3.4 in [Segerlind et al. 2004]. It says that a random restriction chosen according to an appropriate distribution decreases the height of decision tree for a k -DNF with good probability. Here a k -DNF is equivalent to a k -monomial and the covering number is defined accordingly. We also know that its semantic degree is lower than the height of its decision tree. Thus we can correctly rephrase the corollary in our terminology.

LEMMA 8. (Corollary 3.4 [Segerlind et al. 2004]) Let k, s, d be positive 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 -monomial m , $\Pr_{\rho \in \mathcal{D}}[m \upharpoonright_{\rho} \neq 0] \leq d2^{-\delta(c(m))^\gamma}$. Then for every k -monomial M ,

$$\Pr_{\rho \in \mathcal{D}}[sdeg(M \upharpoonright_{\rho}) > 2s] \leq dk2^{-\delta' s^{\gamma'}}$$

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

4.2 Relations between PCR_k and PC, PCR, RES, RES_k

Our point of view to study the connection between PCR_k and PC is the degree measure. We say that the semantic degree of a PCR_k proof Π (denoted as $sdeg(\Pi)$) is the maximum among the semantic degree of all lines in the proof. We also denote as p^* the boolean polynomial representation of a k -polynomial p .

LEMMA 9. (1) For any k -polynomial p , $\vdash p - p^*$ in PCR_k .

(2) PCR_k is complete.

(3) Any CNF refutation Π in PCR_k can be simulated by a proof Γ in PC or PCR such that $\deg(\Gamma) \leq sdeg(\Pi) + k$.

PROOF. (1) It is sufficient to prove the first statement holds for a k -monomials m . We proceed by induction on the number of factors. We denote here the generic factor as $(1 - \prod x)$. If m has one factor then the statement is an axiom of PCR_k . Consider now a k -monomial $(1 - \prod x)m$. By induction $m - m^*$ is deducible, thus we get $(1 - \prod x)m - (1 - \prod x)m^*$ by multiplication rule. From axiom $(1 - \prod x) - 1 + \prod x$ we get $(1 - \prod x)m^* - m^* + \prod x m^*$ by applying multiplications and sums. By another sum rule we obtain $(1 - \prod x)m - m^* + \prod x m^*$. We complete the derivation by applying PCR boolean axioms on the expanded part to eliminate from it negated variables and non-multilinear term. By soundness of PCR_k and uniqueness of the representation this is the boolean polynomial p^* .

(2) $f_1, \dots, f_n \models g$ implies $f_1^*, \dots, f_n^* \models g^*$. By completeness of PC we get $f_1^*, \dots, f_n^* \vdash g^*$. Finally by using (1) we can prove $f_1, \dots, f_n \vdash g$.

(3) The formulas encoding a CNF in PCR_k are also proper lines if a PC proof. Now consider a refutation $\Pi = \{p_i\}_i$ of the encoded CNF. We show how to derive p_i^* in PC. This is sufficient because $1^* = 1$. If p_i is a premise then $p_i^* = p_i$. If p_i is an axiom, then either it is an axiom in PCR or it is a parenthesis axiom. In both cases $p_i^* = 0$. If $p_i = p_a + p_b$ then $p_i^* = p_a^* + p_b^*$. If $p_i = xp_a$ ($p_i = \bar{x}p_a$) then p_i^* is the multilinearization of xp_a^* ($p_a^* - xp_a^*$). If $p_i = (1 - \prod x)p_a$ then the product of $(1 - \prod x)^*$ and p_a^* can be

obtained and multilinearized in PCR. In all such derivations the degree is always lower than $\deg(p_a^*) + k$ which is less or equal than $sdeg(p_a) + k$. Notice that any proof in PC is also a proof in PCR. \square

FACT 3. *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 are 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 (2.2)). 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 $O(2^k)$ and degree 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 $p_1, \dots, p_l \vdash q$ then $m_A p_1, \dots, m_A p_l \vdash m_A q$ in PCR_k in the same size. Also if $p_1, p_2 \vdash q$ then $m_A p_1, m_B p_2 \vdash m_A m_B p_1, m_A m_B p_2 \vdash m_A m_B q$ in size equal to the original plus the number of factors of m_A and m_B . Now if F is the empty k -DNF then p_F is 1. Thus the simulation is complete. \square

5. LOWER BOUNDS FOR PCR_K

We give size lower bounds for PCR_k refutations. Size vs Degree and Size vs Width trade-offs are powerful tools for proving size lower bounds in PC and Resolution respectively. Stronger proof systems like RES_k and Bounded Depth Frege (a sequent system in which formulas have constant depth) require different ideas. Consider two proof systems P_H and P_L , where P_H is stronger than P_L . The following pattern has been fruitful for proving size lower bounds for P_H :

- Show a formula F_L which requires high complexity in the proof system P_L .
- Consider a distribution of partial assignments that with good probability restricts any line of P_H to a low complexity line in P_L .
- Consider a formula F_H such that the distribution restricts F_H to a formula which is efficiently deducible from F_L .
- Notice that such a restriction turns a P_H refutation into a P_L refutation.
- A small P_H refutation of F_H is turned into a low complexity P_L refutation of F_L with positive probability. That is a contradiction.

In [Ben-Sasson and Wigderson 1999] there are several examples in which P_H and P_L are both Resolution, and the width is considered as measure of complexity in P_L . The case of P_L different from P_H is more interesting. The size lower bound for random CNF refutations in [Alekhovich 2005] is achieved with $P_H := \text{RES}_k$ and $P_L := \text{Resolution}$. In [Alekhovich 2005] a distribution of partial assignments is shown which restricts k -DNFs to CNF of small width with high probability. In this case F_H and F_L are random CNF with different density.

For this strategy to work we need the partial assignments to be weak enough to maintain hardness in F_L , and strong enough to reduce P_H lines to small complexity P_L lines. Of course such conflicting conditions cannot always be met. For example $\text{GOP}(G)$ is not hard after a restriction because the underlying graph would lose expansion. Thus a width/degree lower bound for $\text{GOP}(G)$ does not imply size lower bounds for Resolution

or PC (there aren't!). In [Segerlind et al. 2004] and in the following subsection this problem has been overcome by considering a more complex version of $\text{GOP}(G)$ in which any variable is substituted by a XOR of several new disjoint variables. A restriction fixes all variables but one for each XOR. The resulting formula is essentially $\text{GOP}(G)$, thus hardness against Resolution width is preserved. Furthermore (and this is the most important result of [Segerlind et al. 2004]) this restriction transforms a k -DNF in a CNF of small width with high probability.

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

In this section we will give a variant of $\text{GOP}(G)$, which is polynomially refutable by PCR_{k+1} but it is not polynomially refutable by PCR_k . We closely follow the ideas developed for RES_k in [Segerlind et al. 2004].

Let $\text{Even}(a_1, \dots, a_k)$ 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 $\text{GOP}(G)$ we introduce k new variables $x_{a,b}^1, \dots, x_{a,b}^k$. $\text{GOP}^{\oplus k}(G)$ is defined as a modification of $\text{GOP}(G)$: substitute any $x_{a,b}$ with $\text{Even}(x_{a,b}^1, \dots, x_{a,b}^k)$. 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 $\text{GOP}^{\oplus k}(G)$.

Since for any graph G , $\text{GOP}^{\oplus k}(G)$ has a polynomial size refutation in RES_k [Segerlind et al. 2004], then by Fact 3 it follows:

PROPOSITION 3. *For any graph G , $\text{GOP}^{\oplus k}(G)$ has a polynomial size refutation in PCR_k .*

We now prove the lower bound for PCR_k . Following [Segerlind et al. 2004], 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 $x_{a,b}^j$. The next lemma guarantees the applicability of the switching lemma and was proved in [Segerlind et al. 2004] for k -DNF. We rephrase it in terms of k -monomials, but its proof is exactly the same.

LEMMA 10. ([Segerlind et al. 2004]) *Let k be given and let m be a k -monomial on the variables of $\text{GOP}^{\oplus k+1}(G)$ with their negations. There exists a constant $\gamma > 0$ which dependent only on k , such that*

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

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

COROLLARY 1. *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 $\text{GOP}^{\oplus k+1}(G) \upharpoonright_{\rho}$ of degree less than or equal to $cr/4$.*

THEOREM 4. *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 10 applying the Switching Lemma setting $h = (rc/4 - k)$, we have that for any k -monomial m ,

$$\Pr_{\rho \in D_{k+1}(G)} [sdeg(m \upharpoonright_{\rho}) > (rc/4 - k)] \leq k2^{-(\frac{7}{4})(rc/4 - k)}$$

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

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

Assume that there is PCR_k refutation of $\text{GOP}^{\oplus k+1}(G)$ of size strictly less than $2^{-(\epsilon_{k,c}n)}$, then by the union bound there is a PCR_k refutation Π of $\text{GOP}^{\oplus k+1}(G)|_{\rho}$ with $sdeg(\Pi) \leq (rc/4 - k)$. Hence by Lemma 9 there is a PC refutation of $\text{GOP}^{\oplus k+1}(G)|_{\rho}$ of degree $\leq rc/4$. This is in contradiction with Corollary 1. \square

Using the family of vertex expanders defined at the end of Section 3, the previous theorem and Proposition 3 give the following exponential separation.

COROLLARY 2. *There is a family of contradictions \mathcal{F} over n variables which exponentially separates PCR_k from PCR_{k+1} : there are polynomial size refutations of \mathcal{F} in PCR_{k+1} and any refutation of \mathcal{F} in PCR_k requires exponential size.*

5.2 Lower bounds for random formulas 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 . Since to get lower bounds for random formulas we use the result in Alekhovich[2005] applied on k -monomials instead of k -DNFs, we are not giving any proof (the interested reader can find them in the ECCC version of the paper [Galesi and Lauria 2007]). We give the necessary definitions to describe our random formulas and then we state the main theorem. We assume here that the systems PC, PCR and PCR_k are defined over a field of characteristic different from 2.

DEFINITION 4. ([Alekhovich et al. 2004; Alekhovich and Razborov 2001; Alekhovich 2005]) *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 an (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 [Alekhovich 2005], 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 $\phi_{n,\Delta}$.

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 $b_{\phi_{n,\Delta}}[i] = (\# \text{ of positive variables in the } i\text{-th clauses}) \bmod 2$. The random system of linear equations we consider is the system defined by $A_{\phi_{n,\Delta}}x = b_{\phi_{n,\Delta}}$.

Given a system of linear equations $Ax = b$, we define its *polynomial encoding* $\text{Poly}(A, b)$ 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 $\text{Poly}(A, b) = \bigcup_{\ell \in Ax=b} \tilde{\ell}$. Notice that $\text{deg}(\tilde{\ell}) = 3$.

LEMMA 11. *Each PCR_k refutation of $\phi_{n,\Delta}$ can be transformed into a PCR_k refutation of the system of equations $\text{Poly}(A_{\phi_{n,\Delta}}, b_{\phi_{n,\Delta}})$ 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 $\tilde{\ell}$. \square

The following observation is crucial to find 3-CNF which are hard for PC, PCR, PCR_k refutation systems. Such result has been rephrased and used many times (see [Ben-Sasson and Wigderson 1999; Buss et al. 2001; Ben-Sasson and Impagliazzo 1999; Alekhovich and Razborov 2001; Alekhovich 2005; Alekhovich et al. 2004]).

THEOREM 5. ([Chvátal and Szemerédi 1988],[Alekhovich and Razborov 2001]) *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 $1 - o(1)$, $A_{\phi_{n,\Delta}}$ 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 that expanders need high degree to be refuted by PC and PCR. We will use this theorem in our main theorem, since, through the Switching Lemma, we can reduce size lower bounds for PCR_k to degree lower bounds for PCR.

THEOREM 6. (Theorem 3.10 in [Alekhovich et al. 2004]) *Given an unsatisfiable linear system $Ax = b$ where A is an (r, c) -boundary expander, any PCR refutation of $\text{Poly}(A, b)$ in a field \mathbb{F} with characteristic $\neq 2$ requires degree $\geq \frac{rc}{4}$.*

The following theorem follows from Lemma 8 and Theorem 6. The proof is essentially the same as the corresponding lower bound for RES_k in [Alekhovich 2005]. Since this proof has already appeared in [Alekhovich 2005] for RES_k and in Section 4 of [Galesi and Lauria 2007] for PCR_k , we only give a sketch here.

THEOREM 7. *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. (Sketch) Consider $\phi_{n,\Delta}$ and the relative system $A_{\phi_{n,\Delta}}x = b_{\phi_{n,\Delta}}$. By Theorem 5 the system is an (r, c) -expander with $r = O(n)$ and $c = O(1)$. In [Alekhovich 2005] it is defined a random partial assignment which satisfies the requirements of Lemma 8 and also maintains the restricted system to be an $(r/4, c/4)$ -expander. Assume there exists a small PCR_k refutation for $\phi_{n,\Delta}$ (and for $A_{\phi_{n,\Delta}}x = b_{\phi_{n,\Delta}}$ by Lemma 11) then with positive probability the restricted proof has small semantic degree. This and Lemma 9 would give a small degree PC refutation for the restricted system, which contradicts Theorem 6. \square

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for the careful work and the several suggestions. Some of them were substantial and really improved this article.

REFERENCES

- ALEKHOVICH, M. 2005. Lower bounds for k -dnf resolution on random 3-cnfs. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. 251–256.

- ALEKHNovich, M., BEN-SASSON, E., RAZBOROV, A. A., AND WIGDERSON, A. 2004. Pseudorandom generators in propositional proof complexity. *SIAM J. Comput.* 34, 1, 67–88.
- ALEKHNovich, M. AND RAZBOROV, A. A. 2001. Lower bounds for polynomial calculus: Non-binomial case. In *42nd Annual Symposium on Foundations of Computer Science*. 190–199.
- BEAME, P., IMPAGLIAZZO, R., KRAJÍČEK, J., PITASSI, T., AND PUDLÁK, P. 1996. Lower bounds on hilbert’s nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society* 73, 1–26.
- BEAME, P. AND PITASSI, T. 2001. Propositional proof complexity: Past, present and future. In *Current Trends in Theoretical Computer Science Entering the 21st Century*. 42–70.
- BEN-SASSON, E. AND IMPAGLIAZZO, R. 1999. Random cnf’s are hard for the polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*. 415–421.
- BEN-SASSON, E. AND WIGDERSON, A. 1999. Short proofs are narrow - resolution made simple. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*. 517–526.
- BONET, M. L. AND GALESI, N. 1999. A study of proof search algorithms for resolution and polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*. 422–432.
- BONET, M. L. AND GALESI, N. 2001. Optimality of size-width tradeoffs for resolution. *Computational Complexity* 10, 4, 261–276.
- BONET, M. L. AND GALESI, N. 2003. Degree complexity for a modified pigeonhole principle. *Archive for Mathematical Logic* 42, 5, 403–414.
- BUSS, S. R., GRIGORIEV, D., IMPAGLIAZZO, R., AND PITASSI, T. 2001. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.* 62, 2, 267–289.
- CHVÁTAL, V. AND SZEMERÉDI, E. 1988. Many hard examples for resolution. *J. ACM* 35, 4, 759–768.
- CLEGG, M., EDMONDS, J., AND IMPAGLIAZZO, R. 1996. Using the groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*. 174–183.
- COX, D., LITTLE, J., AND O’ SHEA, D. 2007. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd edition. Springer.
- GALESI, N. AND LAURIA, M. 2007. Extending polynomial calculus to k - dnf resolution. In *ECCC TR Series n. TR07-41*.
- HOORY, S., LINIAL, N., AND WIGDERSON, A. 2006. Expander graphs and their applications. *Bull. Amer. Math. Soc.* 43, 4, 439–561.
- IMPAGLIAZZO, R., PUDLÁK, P., AND SGALL, J. 1999. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity* 8, 2, 127–144.
- KRAJÍČEK, J. 2001. On the weak pigeonhole principle. *Fundamenta Mathematicae* 170, 1-3, 123–140.
- KRISHNAMURTY, B. 1985. Short proofs for tricky formulas. *Acta Informatica* 22, 253–257.
- RAZBOROV, A. 2003. Pseudorandom generators hard for k -dnf resolution and polynomial calculus resolution. Manuscript available at author’s webpage.
- RAZBOROV, A. A. 1998. Lower bounds for the polynomial calculus. *Computational Complexity* 7, 4, 291–324.
- REINGOLD, O., VADHAN, S., , AND WIGDERSON, A. 2002. Entropy waves, the zig-zag graph product, and new constant-degree. *Ann. of Math.* 155, 1, 157–187.
- SEGERLIND, N. 2006. The complexity of propositional proofs. *Bulletin of symbolic Logic* 13, 4, 482–537.
- SEGERLIND, N., BUSS, S. R., AND IMPAGLIAZZO, R. 2004. A switching lemma for small restrictions and lower bounds for k -dnf resolution. *SIAM J. Comput.* 33, 5, 1171–1200.
- STALMARK, G. 1996. Short resolution proofs for a sequence of tricky formulas. *Acta Informatica* 33, 277–280.
- WIGDERSON, A. 2006. P, NP and mathematics - a computational complexity perspective. In *Proceedings of the ICM 06 (Madrid), 1 volume*. 665–712.

Received July 2008; revised June 2009; accepted September 2009