On the Alekhnovich–Razborov degree lower bound

Yuval Filmus*

October 17, 2014

1 Introduction

Polynomial calculus is a Hilbert-style proof system in which lines are polynomials modulo $x^2 = x$ (for each variable x) and the rules allow deriving $c_1P_1 + c_2P_2$ from P_1, P_2 and xP from P for a variable x. A polynomial calculus refutation of a set of axioms is a derivation of 1 from these axioms.

Research in proof complexity tends to concentrate on the length of proofs. We will rather be interested in the degree of a refutation, which is the largest degree of a polynomial in the refutation. The degree of a polynomial calculus refutation is analogous to the width of a resolution proof, a quantity which has proved useful in obtaining length lower bounds [BSW01]. Although no such connection is known for polynomial calculus, it is still interesting to prove lower bounds on the degree required to refute certain sets of axioms.

One of the few general techniques for proving degree lower bounds is due to Alekhnovich and Razborov [AR03]. The purpose of this note is to present an alternative proof of their lower bound. We illustrate the technique with two applications, refutations of random CNFs and refutations of the graph ordering principle over a random graph. The former appears already in [AR03], and the latter is due to Galesi and Lauria [GL10].

Section 3 provides background from commutative algebra. We formally introduce polynomial calculus in Section 2. We prove the main lower bound in an abstract framework in Section 4. In Section 5, we instantiate the framework for CNFs whose defining graph is a unique expander, following Alekhnovich and Razborov [AR03]. In Section 6, we instantiate the framework for the graph ordering principle over a unique expander, following Galesi and Lauria [GL10].

2 Polynomial calculus

Polynomial calculus is a Hilbert-style refutation system for polynomials over an arbitrary field $\mathbb{F}$. The goal of the system is to show that a given set of squarefree polynomials $\mathcal{A}$ doesn't have a common 0/1 solution. Each line in the system is a squarefree polynomial. The intended meaning of a line P is that every 0/1 assignment to the variables of P zeroes P. For a polynomial P, let $\mathrm{SF}(P)$ be the squarefree polynomial obtained by reducing all powers of variables to 1 (for example, $\mathrm{SF}(x^2+x) = 2x$). The system has the following deduction rules:

- Axiom download: For any $C \in \mathcal{A}$, deduce C.
- Linear combination: Given P_1, P_2, deduce $\mathrm{SF}(c_1P_1 + c_2P_2)$ for any $c_1, c_2 \in \mathbb{F}$.
- Multiplication by variable: Given P, deduce $\mathrm{SF}(xP)$ for any variable x.

A *polynomial calculus refutation* is a sequence of lines, each line following from previous lines via a deduction rule, which culminates at the line 1. It is not hard to check that the system is sound: if there is a refutation for $\mathcal{A}$ then no 0/1 assignment zeroes all polynomials in $\mathcal{A}$. It is also complete.

The *degree* of a polynomial calculus refutation is the maximal degree of a line in the refutation. We say that $\mathcal{A}$ cannot be refuted in degree $\mathbf{D}$ if $\mathcal{A}$ has no refutation of degree $\mathbf{D}$ or less.

*Work done while the author was visiting Jakob Nordström's group at KTH during the month of December, 2012.

Polynomial calculus can be used to refute unsatisfiable CNFs. A clause of width w is replaced by a monomial of degree w using the substitutions $x \mapsto x$ and $\bar{x} \mapsto 1-x$, and $\mathcal{A}$ is the set of monomials corresponding to the various clauses. For example, the CNF $(x \vee y) \wedge (\neg x) \wedge (\neg y)$ corresponds to the set of polynomials $\{xy, 1-x, 1-y\}$. A corresponding polynomial calculus refutation is:

$1-x$	axiom download
$y-xy$	multiplication of $1-x$ by y
xy	axiom download
y	linear combination of $y-xy$ and xy
$1-y$	axiom download
1	linear combination of y and $1-y$

This refutation has degree 2.

Polynomial calculus can also be used to refute systems of polynomial equations over 0/1-valued assignments, by converting each polynomial equation $P = Q$ to the polynomial $P - Q$. For example, the system of equations $\{x = y, x = 1-y\}$ corresponds to the set of polynomials $\{x-y, x+y-1\}$.

3 Background from commutative algebra

Let $\mathcal{V}$ be an ordered set of variables, and let $S = \{S_i\}$ be a set of polynomials over $\mathcal{V}$ with coefficients in the field $\mathbb{F}$. The *ideal* generated by S is

$$I(S) = \left\{ \sum_i P_i S_i : P_i \in \mathbb{F}[\mathcal{V}] \right\}.$$

The *degree* of a monomial $\prod_i x_i^{p_i}$ is $\sum_i p_i$. We define a total ordering of monomials as follows. Let $m_1 = x_1 m_1'$, $m_2 = x_2 m_2'$, where x_1, x_2 are the minimal variables in m_1, m_2 (respectively) according to the order of $\mathcal{V}$. Then $m_1 < m_2$ if either of the following is true:

- $\deg m_1 < \deg m_2$.
- $\deg m_1 = \deg m_2$ and $x_1 < x_2$.
- $\deg m_1 = \deg m_2$, $x_1 = x_2$ and $m_1' < m_2'$.

For example, if $\mathcal{V} = \{x, y, z\}$ (in that order) then

$$1 < x < y < z < x^2 < xy < xz < y^2 < yz < z^2 < x^3 < \cdots.$$

For a non-zero polynomial P, the leading monomial (the largest in the monomial ordering) is denoted $\mathrm{LM}(P)$. The entire leading term is $\mathrm{LT}(P)$. For example, $\mathrm{LT}(3x^2 + y) = 3x^2$ while $\mathrm{LM}(3x^2 + y) = x^2$.

A monomial m is *reducible* modulo an ideal I if it is the leading term of some polynomial in I. Otherwise, we say that it is irreducible modulo I. For example, if $I_{\mathcal{V}} = \{x^2 - x : x \in \mathcal{V}\}$ then m is irreducible if m is squarefree. In the sequel, we will always work modulo $I_{\mathcal{V}}$, and so we will assume that all monomials are squarefree. For example, $x \cdot xy = xy$.

4 Main argument

In this section we describe a method for proving that a set $\mathcal{A}$ of axioms cannot be refuted in degree $\mathbf{D}$ in polynomial calculus. This method abstracts the arguments of Alekhnovich and Razborov appearing in [AR03] ("the basic version"), as well as their extension due to Galesi and Lauria [GL10]. The inputs to the method, beside $\mathcal{A}$ and $\mathbf{D}$, are three functions $\mathrm{Objs}, \mathrm{Objs}_{\mathcal{A}}, \mathrm{Sup}$ satisfying several axioms described below.

Notation We denote the image of a set S under a function f by $f(S)$. For a set S and a number z, let $\mathbb{P}(S)$ denote the power set of S, and let $S_{\leq z} = \{T \subseteq S : |T| \leq z\}$. For a monomial m and a polynomial P, m *appears in* P, denoted $m \in P$, if the coefficient of m in P is non-zero. For a set S of variables, let $\mathrm{Mon}(S) = \prod_{x \in S} x$.

Setup For the rest of this section, let $\mathbf{D} \in \mathbb{N}$ be a parameter, let $\mathcal{A}$ be a set of polynomials of degree at most $\mathbf{D}$ over the set of variables $\mathcal{V}$, and let $\mathcal{O}$ be an auxiliary set of abstract "objects". The basic version has $\mathcal{O} = \mathcal{V}$.

Let $\mathrm{Objs}\colon \mathcal{V} \to \mathbb{P}(\mathcal{O})$ and $\mathrm{Objs}_{\mathcal{A}}\colon \mathcal{A} \to \mathbb{P}(\mathcal{O})$ be functions satisfying the following axiom:

(V) For each $o \in \mathcal{O}$ there exists an assignment σ_o to all variables $x \in \mathcal{V}$ satisfying $o \in \mathrm{Objs}(x)$, such that for all $C \in \mathcal{A}$ for which $o \notin \mathrm{Objs}_{\mathcal{A}}(C)$, either $\sigma_o(C) = 0$ or $\sigma_o(C) = C$.

The basic version defines $\mathrm{Objs}(x) = \{x\}$ and $\mathrm{Objs}_{\mathcal{A}}(C)$ to be the set of variables appearing in C, in which case (V) is trivial: σ_x can be any assignment to x.

For a monomial m, define $\mathrm{Objs}(m)$ to be the union of $\mathrm{Objs}(x)$ for all variables x appearing in m. For a polynomial P, define $\mathrm{Objs}(P)$ to be the union of $\mathrm{Objs}(m)$ for all monomials $m \in P$. For a subset $A \subseteq \mathcal{A}$, define $\mathrm{Objs}_{\mathcal{A}}(A)$ to be the union of $\mathrm{Objs}_{\mathcal{A}}(C)$ for all $C \in A$.

Let $\mathrm{Sup}\colon \mathrm{Objs}(\mathcal{V}_{\leq \mathbf{D}}) \to \mathbb{P}(\mathcal{A})$ be a function satisfying the following axioms:

(S1) Non-triviality: $1 \notin I(\mathrm{Sup}(\emptyset))$.

(S2) For all $C \in \mathcal{A}$ with $O = \mathrm{Objs}(\mathrm{LM}(C))$, $C \in \mathrm{Sup}(O)$ and $\mathrm{Objs}(C) \subseteq O \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(O))$.

(S3) Let $S_1, S_2 \in \mathcal{V}_{\leq \mathbf{D}}$. If $\mathrm{Objs}(S_1) \subseteq \mathrm{Objs}(S_2) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(\mathrm{Objs}(S_2)))$ then $\mathrm{Sup}(\mathrm{Objs}(S_1)) \subseteq \mathrm{Sup}(\mathrm{Objs}(S_2))$.

(S4) Let $S \in \mathcal{V}_{\leq \mathbf{D}}$ and $A \in \mathrm{Sup}(\mathrm{Objs}(\mathcal{V}_{\leq \mathbf{D}}))$. If $\mathrm{Sup}(\mathrm{Objs}(S)) \subseteq A$ and $\mathrm{Mon}(S)$ is reducible modulo $I(A)$ then it is reducible modulo the smaller ideal $I(\mathrm{Sup}(\mathrm{Objs}(S)))$.

For a monomial m, define $\mathrm{Sup}(m) = \mathrm{Sup}(\mathrm{Objs}(m))$. For a non-zero polynomial P, define $\mathrm{Sup}(P) = \mathrm{Sup}(\mathrm{LM}(P))$. For a polynomial P, define the *total support* $\mathrm{TSup}(P)$ of P to be the union of $\mathrm{Sup}(m)$ for all monomials $m \in P$. If $A \in \mathrm{Sup}(\mathrm{Objs}(\mathcal{V}_{\leq \mathbf{D}}))$ then we say that A is *legal*.

When all axioms in $\mathcal{A}$ are monomials, (S2) reduces to $C \in \mathrm{Sup}(C)$.

Proof idea Consider the basic version, in which Sup is a mapping from low-degree monomials to small sets of axioms (even though no axiom requires the image of Sup to consist of small sets, this is going to be the case in both applications we consider). For a low-degree monomial m, $\mathrm{Sup}(m)$ is the set of axioms in $\mathcal{A}$ which are "relevant" for m. We will show that each line appearing in the proof can be reduced to zero using the following algorithm: repeatedly reduce the line P modulo $\mathrm{Sup}(P)$, each time working only over the variables appearing in $\mathrm{LM}(P)$ and $\mathrm{Sup}(P)$. We call a polynomial which can be reduced to zero in this way *semisimple*. If one step already reduces the polynomial to zero, we call it *simple*. Every semisimple polynomial is a sum of simple polynomials with decreasing leading monomials, and it turns out that the converse holds as well; we use this property to *define* semisimple polynomials. Since the algorithm doesn't reduce 1 to zero (due to (S1)), this shows that no refutation is possible.

Iterative application of (V) shows that if a monomial m is reducible modulo $I(\mathrm{Sup}(m))$ then some simple polynomial has m as its leading monomial. Iterative application of this result gives a crucial criterion for semisimplicity: a polynomial P is semisimple if $P \in I(A)$ for some legal superset A of $\mathrm{TSup}(P)$. The idea is to use (S4) to conclude that $\mathrm{LM}(P)$ is reducible modulo $I(\mathrm{Sup}(\mathrm{LM}(P))$, subtract from P a simple polynomial with the same leading term, and repeat if necessary. This criterion is useful since $\mathrm{TSup}(P) = \mathrm{Sup}(P)$ for simple polynomials P, a simple consequence of (S3).

The fact that axioms in $\mathcal{A}$ are simple follows directly from (S2). The next step is to show that the sum of two simple polynomials P_1, P_2 is semisimple ("the sum property"). If they don't have the same leading monomials, then $P_1 + P_2$ is semisimple by definition. If $\mathrm{LM}(P_1) = \mathrm{LM}(P_2)$ and the leading monomials do not cancel in $P_1 + P_2$, then $P_1 + P_2$ remains simple. If the leading monomials do cancel, since P_1, P_2 are simple and $\mathrm{Sup}(P_1) = \mathrm{Sup}(P_2)$ we have $\mathrm{TSup}(P_1 + P_2) \subseteq \mathrm{Sup}(P_1)$, and so the semisimplicity criterion implies that $P_1 + P_2$ is semisimple.

Having shows that the sum of two simple polynomials is semisimple, we can show that any linear combination of two semisimple polynomials is semisimple. Write the linear combination of the two semisimple polynomials as a sum of simple polynomials. If no two simple polynomials have the same leading monomial, we are done. Otherwise, the sum property allows us to choose two simple polynomials with the same leading monomial, and replace them with the simple components of their semisimple sum. This operation results in a new collection of simple polynomials with lower leading monomials (in a lexicographic sense), and so repeated applications of this procedure result eventually in a collection of simple polynomials with distinct leading monomials, showing that the linear combination is semisimple.

It remains to show that multiplying a semisimple polynomial P by a variable x results in a semisimple polynomial. In view of the preceding result, we can assume that P is simple. There are two cases. If x appears in $\mathrm{LM}(P)$ then (S3) implies that $\mathrm{TSup}(xP) = \mathrm{Sup}(P)$, and so xP is semisimple by the semisimplicity criterion. If x doesn't appear in $\mathrm{LM}(P)$ then $\mathrm{LM}(xP) = x\,\mathrm{LM}(P)$, and so (S3) implies that $\mathrm{Sup}(xP) \supseteq \mathrm{Sup}(P)$ and so xP is simple.

Argument We make two important definitions:

- A polynomial P is *simple* if
  - $\deg P \leq \mathbf{D}$,
  - $\mathrm{Objs}(P) \subseteq \mathrm{Objs}(\mathrm{LM}(P)) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(P))$,
  - $P \in I(\mathrm{Sup}(P))$.
- A polynomial P is *semisimple* if it can be written as $\sum_i P_i$ where each P_i is simple and $\mathrm{LM}(P_i) \neq \mathrm{LM}(P_j)$ for $i \neq j$. We call $\sum_i P_i$ a *semisimple decomposition* of P.

Simplicity in conjunction with (S3) implies the following property.

Lemma 4.1. *If P is simple then $\mathrm{TSup}(P) = \mathrm{Sup}(P)$.*

Proof. Since $\mathrm{TSup}(P) \supseteq \mathrm{Sup}(\mathrm{LM}(P)) = \mathrm{Sup}(P)$, it is enough to prove that $\mathrm{Sup}(m) \subseteq \mathrm{Sup}(P)$ for every $m \in P$. Indeed, since P is simple, $\mathrm{Objs}(m) \subseteq \mathrm{Objs}(\mathrm{LM}(P)) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(\mathrm{LM}(P))$, and so (S3) implies $\mathrm{Sup}(\mathrm{Objs}(m)) \subseteq \mathrm{Sup}(\mathrm{LM}(p))$. □

The following lemma is our main source for simple polynomials.

Lemma 4.2. *If m is a monomial of degree at most $\mathbf{D}$ reducible modulo $I(\mathrm{Sup}(m))$ then there is a simple polynomial P whose leading term is m.*

Proof. Let $Q \in I(\mathrm{Sup}(m))$ satisfy $\mathrm{LT}(Q) = m$, and define $S = \mathrm{Objs}(Q) \setminus (\mathrm{Objs}(m) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(m)))$. The proof is by induction on $|S|$. If $S = \emptyset$ then we are done. Otherwise, let $o \in S$. According to (V), there exists an assignment σ_o to all variables $x \in \mathcal{V}$ satisfying $o \in \mathrm{Objs}(x)$, such that for all $C \in \mathcal{A}$ for which $o \notin \mathrm{Objs}_{\mathcal{A}}(C)$, either $\sigma_o(C) = 0$ or $\sigma_o(C) = C$. Consider the polynomial $R = \sigma_o(Q)$. Since $o \notin \mathrm{Objs}(m)$, the assignment σ_o doesn't affect any variable in m, and so $\mathrm{LT}(R) = m$. Since $o \notin \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(m))$, the assignment σ_o either zeroes or leaves unchanged every $C \in \mathrm{Sup}(m)$, and so $R \in I(\mathrm{Sup}(m))$. Finally, since σ_o assigns a value to each variable $x \in \mathcal{V}$ satisfying $o \in \mathrm{Objs}(x)$, we have $\mathrm{Objs}(R) \setminus (\mathrm{Objs}(m) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(m))) \subseteq S \setminus \{o\}$, and so we can apply the induction hypothesis to complete the proof. □

Semisimple polynomials enjoy the following important property.

Lemma 4.3. *Suppose P is a semisimple polynomial with semisimple decomposition $\sum_i P_i$. Then for some i, $\mathrm{LT}(P_i) = \mathrm{LT}(P)$, and for $j \neq i$, $\mathrm{LM}(P_j) < \mathrm{LM}(P)$.*

Proof. Let P_i be the polynomial maximizing $\mathrm{LM}(P_i)$. By definition, $\mathrm{LM}(P_j) < \mathrm{LM}(P_i)$ for all $j \neq i$. Therefore $\mathrm{LT}(P) = \mathrm{LT}(P_i)$. □

We will use (S4) only through the following lemma, which is our crucial criterion for semisimplicity.

Lemma 4.4. *If P is a polynomial of degree at most $\mathbf{D}$ and $P \in I(A)$ for some legal superset $A \subseteq \mathcal{A}$ of $\mathrm{TSup}(P)$ then P is semisimple.*

Proof. The proof is by induction on $\mathrm{LM}(P)$. The base case is $P = 0$. If $P \neq 0$ then $\mathrm{LM}(P)$ is reducible modulo $I(A)$, and so modulo $I(\mathrm{Sup}(\mathrm{LM}(P)))$, by (S4). Lemma 4.2 shows that there exists a simple polynomial Q with $\mathrm{LT}(Q) = \mathrm{LT}(P)$. Since $\mathrm{Sup}(Q) = \mathrm{Sup}(P) \subseteq \mathrm{TSup}(P)$ and Q is simple, $Q \in I(A)$ and so $P - Q \in I(A)$. Since Q is simple, Lemma 4.1 shows that $\mathrm{TSup}(Q) = \mathrm{Sup}(Q) \subseteq \mathrm{TSup}(P)$. Hence $P - Q$ satisfies the prerequisites of the lemma. Since $\mathrm{LM}(P - Q) < \mathrm{LM}(P)$, $P - Q$ is semisimple by the induction hypothesis. Lemma 4.3 shows that all polynomials in a semisimple decomposition $\sum_i R_i$ of $P - Q$ satisfy $\mathrm{LM}(R_i) \leq \mathrm{LM}(P - Q) < \mathrm{LM}(P) = \mathrm{LM}(Q)$, and so $Q + \sum_i R_i$ is a semisimple decomposition of P. □

Our plan is to show that everything derivable from $\mathcal{A}$ in degree $\mathbf{D}$ is semisimple, while 1 is not semisimple. We start with the base case, axiom download, which is the only place we use (S2).

Lemma 4.5. *Every $C \in \mathcal{A}$ is simple, and so semisimple.*

Proof. This is an immediate consequence of (S2). □

We proceed to prove that the sum of two semisimple polynomials is semisimple.

Lemma 4.6. *Suppose P_1, P_2 are simple polynomials with $\mathrm{LT}(P_1) = \mathrm{LT}(P_2)$. Then $P_1 - P_2$ is semisimple.*

Proof. Since P_1 and P_2 are simple and $\mathrm{Sup}(P_1) = \mathrm{Sup}(P_2)$, Lemma 4.1 shows that $\mathrm{TSup}(P_1 - P_2) \subseteq \mathrm{Sup}(P_1)$. Since $P_1 - P_2 \in I(\mathrm{Sup}(P_1)) = I(\mathrm{Sup}(P_2))$, Lemma 4.4 shows that $P_1 - P_2$ is semisimple. □

Lemma 4.7. *Suppose P_1, P_2 are semisimple and $c_1, c_2 \in \mathbb{F}$. Then $c_1 P_1 + c_2 P_2$ is semisimple.*

Proof. We first show that if S is any collection (multiset) of simple polynomials then $\sum S$ is semisimple. If there are no two polynomials with the same leading monomial in S, then $\sum S$ is clearly semisimple. Otherwise, take any two polynomials P_1, P_2 with the same leading monomial m. If $\mathrm{LM}(P_1 + P_2) = m$ then it is easy to check that $P_1 + P_2$ is simple, and we replace P_1, P_2 with $P_1 + P_2$. If $\mathrm{LM}(P_1 + P_2) < m$ then Lemma 4.6 (applied to $P_1, -P_2$) shows that $P_1 + P_2$ is semisimple, and we replace P_1, P_2 with the simple components of $P_1 + P_2$, all of which have smaller leading monomials than m due to Lemma 4.3. Continue this way until no two polynomials in S share a leading monomial.

To show that this process converges, we define a potential function which decreases after each step. For a monomial m, let $\iota(m)$ be its index in the increasing order of monomials. We use the potential function given by

$$\Phi(S) = \sum_{P \in S} \omega^{\iota(\mathrm{LM}(P))},$$

where ω is the ordinal of the natural numbers[1]. It is routine to check that Φ decreases after each step: in the first case we replace $2\omega^d$ with ω^d for some d, and in the second case we replace ω^d with $\sum_i \omega^{d_i}$ for some d, d_i, where $d_i < d$ for all i. Since the ordinal numbers are well-ordered, the process must terminate.

Finally, take S to be the collection of simple polynomials forming $c_1 P_1$ and $c_2 P_2$. We deduce that $\sum S = c_1 P_1 + c_2 P_2$ is semisimple. □

Next, we prove that multiplying a semisimple polynomial by a variable yields another semisimple polynomial.

Lemma 4.8. *Suppose P is a semisimple polynomial and x is a variable. If $\deg(xP) \le \mathbf{D}$ then xP is semisimple.*

Proof. In view of Lemma 4.7, we can assume that P is simple.

Suppose first that $\mathrm{Objs}(x) \subseteq \mathrm{Objs}(\mathrm{LM}(P))$. Since P is simple, every monomial $xm \in xP$ satisfies $\mathrm{Objs}(xm) \subseteq \mathrm{Objs}(\mathrm{LM}(P)) \cup \mathrm{Objs}(\mathrm{Sup}(P))$. Therefore $\mathrm{Sup}(xm) \subseteq \mathrm{Sup}(P)$ by (S3), and so $\mathrm{TSup}(xP) \subseteq \mathrm{Sup}(P)$. Since P is simple, $xP \in I(\mathrm{Sup}(P))$, and so Lemma 4.4 shows that xP is semisimple.

Suppose next that $\mathrm{Objs}(x) \not\subseteq \mathrm{Objs}(\mathrm{LM}(P))$, and in particular x doesn't appear in $\mathrm{LM}(P)$. The ordering of monomials satisfies the property that $m_1 \ge m_2$ implies $xm_1 \ge xm_2$ whenever x doesn't appear in m_1, and this shows that $\mathrm{LM}(xP) = x\,\mathrm{LM}(P)$. Therefore $\mathrm{Sup}(xP) \supseteq \mathrm{Sup}(P)$ by (S3), and so it is easy to verify that xP is simple. □

Finally, we prove that 1 is not semisimple, making our only use of (S1).

Lemma 4.9. *The polynomial 1 is not semisimple.*

Proof. If 1 were semisimple, then Lemma 4.3 would show that there is some simple polynomial P with $\mathrm{LT}(P) = 1$. This is impossible since $1 \notin I(\mathrm{Sup}(1))$ by (S1). □

We are now ready to prove the main theorem of this section. For convenience, we state the theorem with all the required prerequisites.

[1] The reader who is not fond of ordinal arithmetic can rephrase the argument in terms of lexicographic order.

Theorem 4.10. *Let $\mathbf{D} \in \mathbb{N}$ be a parameter, let $\mathcal{A}$ be a set of polynomials of degree at most $\mathbf{D}$ over the variables $\mathcal{V}$, and let $\mathcal{O}$ be an arbitrary set. Suppose that there exist functions $\mathrm{Objs}\colon \mathcal{V} \to \mathbb{P}(\mathcal{O})$, $\mathrm{Objs}_{\mathcal{A}}\colon \mathcal{A} \to \mathbb{P}(\mathcal{O})$, and $\mathrm{Sup}\colon \mathrm{Objs}(\mathcal{V}_{\leq \mathbf{D}}) \to \mathbb{P}(\mathcal{A})$, satisfying the following axioms:*

(V) For each $o \in \mathcal{O}$ there exists an assignment σ_o to all variables $x \in \mathcal{V}$ satisfying $o \in \mathrm{Objs}(x)$, such that for all $C \in \mathcal{A}$ for which $o \notin \mathrm{Objs}_{\mathcal{A}}(C)$, either $\sigma_o(C) = 0$ or $\sigma_o(C) = C$.

(S1) Non-triviality: $1 \notin I(\mathrm{Sup}(\emptyset))$.

(S2) For all $C \in \mathcal{A}$ with $O = \mathrm{Objs}(\mathrm{LM}(C))$, $C \in \mathrm{Sup}(O)$ and $\mathrm{Objs}(C) \subseteq O \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(O))$.

(S3) Let $S_1, S_2 \in \mathcal{V}_{\leq \mathbf{D}}$. If $\mathrm{Objs}(S_1) \subseteq \mathrm{Objs}(S_2) \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(\mathrm{Objs}(S_2)))$ then $\mathrm{Sup}(\mathrm{Objs}(S_1)) \subseteq \mathrm{Sup}(\mathrm{Objs}(S_2))$.

(S4) Let $S \in \mathcal{V}_{\leq \mathbf{D}}$ and $A \in \mathrm{Sup}(\mathrm{Objs}(\mathcal{V}_{\leq \mathbf{D}}))$. If $\mathrm{Sup}(\mathrm{Objs}(S)) \subseteq A$ and $\mathrm{Mon}(S)$ is reducible modulo $I(A)$ then it is reducible modulo the smaller ideal $I(\mathrm{Sup}(\mathrm{Objs}(S)))$.

Then the set $\mathcal{A}$ cannot be refuted in degree $\mathbf{D}$.

Proof. Lemma 4.5, Lemma 4.7 and Lemma 4.8 show that everything derivable in degree $\mathbf{D}$ is semisimple. Conversely, Lemma 4.9 shows that 1 is not semisimple, and so cannot be derived in degree $\mathbf{D}$. □

5 Expanding formulas in conjunctive normal form

In this section, we instantiate the basic version of the lower bound framework for the case of expanding formulas in conjunctive normal form.

Let Φ be a formula in conjunctive normal form. We can think of Φ as a set of monomials (clauses). For a subset $S \subseteq \Phi$, say that a variable x is a *unique neighbor* if x appears in exactly one clause in S. We denote the set of unique neighbors of S by ∂S, the *boundary* of S.

For the rest of this section, suppose that there are parameters $s, e > 0$ such that every subset $S \subseteq \Phi$ of size at most s satisfies $|\partial S| \geq e|S|$; this property is known as *unique expansion*. We will use the framework of Section 4 with $\mathbf{D} = se/2$. Without loss of generality, we can assume that each clause of Φ contains at most $se/2$ literals.

We start with a simple property satisfied by the boundary operator.

Lemma 5.1. *Let $S_1, S_2 \subseteq \Phi$. Then $\partial(S_1 \cup S_2) \subseteq \partial(S_1) \cup \partial(S_2)$.*

Proof. Let $x \in \partial(S_1 \cup S_2)$. Then x appears in a unique clause $C \in S_i$ for some $i \in \{1, 2\}$. This implies that $x \in \partial S_i$. We conclude that $\partial(S_1 \cup S_2) \subseteq \partial(S_1) \cup \partial(S_2)$. □

Let V be a set of at most $se/2$ variables. A set $S \subseteq \Phi$ is *relevant* for V if $|S| \leq s$ and $\partial S \subseteq V$.

Lemma 5.2. *Let V be a set of at most $se/2$ variables, and $S \subseteq \Phi$. If S is relevant for V then $|S| \leq s/2$.*

Proof. By the unique expansion property, $|\partial S| \geq e|S|$. Since S is relevant for V, $|\partial S| \leq |V| \leq se/2$. We deduce that $|S| \leq s/2$. □

Lemma 5.3. *Let V be a set of at most $se/2$ variables, and $S_1, S_2 \subseteq \Phi$. If S_1, S_2 are relevant for V then $S_1 \cup S_2$ is relevant for V.*

Proof. Lemma 5.2 shows that $|S_1 \cup S_2| \leq s$. Lemma 5.1 shows that $\partial(S_1 \cup S_2) \subseteq \partial(S_1) \cup \partial(S_2) \subseteq V$, and so $S_1 \cup S_2$ is relevant for V. □

We can now define the support.

Definition 5.4. Let V be a set of at most $se/2$ variables. We define $\mathrm{Sup}(V)$ as the union of all sets $S \subseteq \Phi$ relevant for V.

Lemma 5.5. *Let V be a set of at most $se/2$ variables. Then $\mathrm{Sup}(V)$ is relevant for V and $|\mathrm{Sup}(V)| \leq s/2$.*

Proof. The first part follows from Lemma 5.3, the second part from Lemma 5.2. □

We now show that the support satisfies the prerequisites of Theorem 4.10. Since we are using the basic version, there is no need to prove (V). We prove the rest of the prerequisites in order. The proof of (S4) uses the bound $|A| \leq s/2$ on all legals sets A given by Lemma 5.5.

Lemma 5.6. *We have* $\mathrm{Sup}(\emptyset) = \emptyset$.

Proof. Suppose that S is relevant for $\emptyset$. Then $\partial S = \emptyset$. Since $|\partial S| \geq e|S|$ and $e > 0$, we conclude that $S = \emptyset$. □

Lemma 5.7. *For every clause $C \in \Phi$ we have $C \in \mathrm{Sup}(\mathrm{Objs}(C))$.*

Proof. By assumption, $|\mathrm{Objs}(C)| \leq se/2$. Clearly $\partial C \subseteq \mathrm{Objs}(C)$, and so $\{C\}$ is relevant for $\mathrm{Objs}(C)$. Therefore $C \in \mathrm{Sup}(\mathrm{Objs}(C))$. □

Lemma 5.8. *Suppose V_1, V_2 are sets of at most $se/2$ variables. If $V_1 \subseteq V_2 \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(V_2))$ then $\mathrm{Sup}(V_1) \subseteq \mathrm{Sup}(V_2)$.*

Proof. Lemma 5.5 shows that $\mathrm{Sup}(V_1)$ is relevant for V_1, and so $\partial\,\mathrm{Sup}(V_1) \subseteq V_1 \subseteq V_2 \cup \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(V_2))$. The lemma also shows that $\mathrm{Sup}(V_2)$ is relevant for V_2, and so $\partial\,\mathrm{Sup}(V_2) \subseteq V_2$. Moreover, the lemma shows that $|\mathrm{Sup}(V_1) \cup \mathrm{Sup}(V_2)| \leq s$.

Let $x \in \partial(\mathrm{Sup}(V_1) \cup \mathrm{Sup}(V_2))$. If x is a unique neighbor of a clause from $\mathrm{Sup}(V_2)$, then $x \in V_2$. Otherwise, x is a unique neighbor of a clause from $\mathrm{Sup}(V_1)$, and so $x \notin \mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(V_2))$, and again $x \in V_2$. We conclude that $\mathrm{Sup}(V_1) \cup \mathrm{Sup}(V_2)$ is relevant for V_2, and so $\mathrm{Sup}(V_1) \cup \mathrm{Sup}(V_2) \subseteq \mathrm{Sup}(V_2)$, which implies $\mathrm{Sup}(V_1) \subseteq \mathrm{Sup}(V_2)$. □

Lemma 5.9. *Let m be a monomial of degree at most $se/2$ which is reducible modulo $I(A)$, for some $A \subseteq \Phi$ of size at most $s/2$. If $A \supseteq \mathrm{Sup}(m)$ then m is reducible modulo $I(\mathrm{Sup}(m))$.*

Proof. The proof is by induction on $|A \setminus \mathrm{Sup}(m)|$. If $A \subseteq \mathrm{Sup}(m)$ then we are done, so suppose $\mathrm{Sup}(m)$ doesn't contain A. By the definition of $\mathrm{Sup}(m)$, $\partial\,\mathrm{Sup}(m) \subseteq \mathrm{Objs}(m)$ while $\partial A \nsubseteq \mathrm{Objs}(m)$. Thus there is a clause $C \in A \setminus \mathrm{Sup}(m)$ and a variable $x \in \mathrm{Objs}(C) \setminus \mathrm{Objs}(m)$ which is a unique neighbor, that is $x \notin \mathrm{Objs}(A \setminus \{C\})$.

Suppose $x = b$ zeroes C. Take any polynomial $P \in I(A)$ with $\mathrm{LT}(P) = m$. Substituting $x = b$, we get a polynomial $Q \in I(A \setminus \{C\})$ with $\mathrm{LT}(P) = m$, and so m is reducible modulo $I(A \setminus \{C\})$. The induction hypothesis shows that m is reducible modulo $I(\mathrm{Sup}(m))$. □

Having verified all the properties of the support, we conclude the following lower bound from Theorem 4.10.

Theorem 5.10 ([AR03])**.** *Suppose φ is a CNF such that any set S of up to s clauses satisfies $|\partial S| \geq e|S|$, for some $s, e > 0$. Then φ cannot be refuted in degree $se/2$.*

6 Graph ordering principle

In this section, we instantiate the lower bound framekwork for the graph ordering principle, following Galesi and Lauria [GL10]. Let $G = (V, E)$ be an undirected graph. The *neighborhood* of a vertex i is $N(i) = \{j : \{i, j\} \in E\}$. The neighborhood of a set $S \subseteq V$ of vertices is $N(S) = \bigcup_{i \in S} N(i)$. The *boundary* of S is $\Gamma(S) = N(S) \setminus S$. In other words, the boundary of S is the set of vertices *outside* S which have a neighbor in S. While $N(S \cup T) = N(S) \cup N(T)$, it is *not* true in general that $\Gamma(S \cup T) = \Gamma(S) \cup \Gamma(T)$.

The graph ordering principle is defined as follows. For every pair $i, j \in V$ of different vertices we have a variable x_{ij}. The variables x_{ij} define an order relation $\prec$ on V, $x_{ij} = 0$ meaning $j \prec i$, and $x_{ij} = 1$ meaning $i \prec j$. We have three kinds of axioms.

For every pair i, j of different vertices, there is a *complementarity axiom*

$$\sigma_{ij} \colon x_{ij} + x_{ji} = 1.$$

For every triple $i, j, k \in V$ of different vertices, there is a *transitivity axiom*

$$\tau_{i,j,k} \colon x_{ij} x_{jk} x_{ki} = 0.$$

This axiom states that if $i \prec j \prec k$ then $i \prec k$. Let $\mathcal{T}$ denote the set of *trivial axioms*, which include all complementarity and transitivity axioms. Together the trivial axioms state that $\prec$ is a linear order.

For each $i \in V$, there is a *minimality axiom*

$$M_i\colon \prod_{j \in N(i)} x_{ij} = 0.$$

This axiom states that for some $j \in N(i)$, $j \prec i$. In other words, no vertex is a local minimum. All axioms taken together are contradictory since the global minimum is also a local minimum.

For the rest of the section, we assume that there are parameters $s, e > 0$ such that for every set $S \subseteq V$ of size at most s, $|\Gamma(S)| \geq e|S|$; we call this the *expansion property*. This property is similar to the property we used in Section 5. We will instantiate the framework of Section 4 with $\mathbf{D} = se/4$ and $\mathcal{O} = V$.

For a set X of variables, let $\mathrm{Objs}(X)$ be the set of vertices mentioned in X. For example, $\mathrm{Objs}(x_{ij}) = \{i, j\}$. Note that $|\mathbb{V}(X)| \leq 2|X|$, and so $|X| \leq \mathbf{D}$ implies $|\mathrm{Objs}(X)| \leq se/2$. Also, define $\mathrm{Objs}_{\mathcal{A}}(C) = \emptyset$ for all trivial axioms $C \in \mathcal{T}$, and $\mathrm{Objs}_{\mathcal{A}}(M_i) = \{i\}$. Our first order of business is to show that Objs and $\mathrm{Objs}_{\mathcal{A}}$ satisfy (V).

Lemma 6.1. *For each $i \in V$ there is a substitution σ_i to the variables $\{x_{ij}, x_{ji} : j \in N(i)\}$ that satisfies M_j for each $j \in N(i)$ (i.e., sets M_j to 0), falsifies M_i (i.e., sets it to 1), and doesn't affect the remaining minimality axioms. Furthermore, each trivial axiom is either satisfied or unaffected.*

Proof. The substitution σ_i is of the form $x_{ij} = 1$ and $x_{ji} = 0$ for every $j \in N(i)$. In other words, σ_i states that i is a local minimum. It is easy to verify that all the required properties hold. □

We will define an operator VSup (the *vertex support*) which takes a set of at most $se/2$ vertices and returns a set of at most $s/2$ relevant vertices. For a set X of variables, we define $\mathrm{VSup}(X) = \mathrm{VSup}(\mathrm{Objs}(X))$. Similarly, for a monomial m, we define $\mathrm{VSup}(m) = \mathrm{VSup}(\mathrm{Objs}(m))$. Given VSup, we define $\mathrm{Sup}(X) = \mathcal{T} \cup \{M_i : i \in \mathrm{VSup}(X)\}$.

Our definition of VSup mimics the definition of the support in Section 5, and satisfies similar properties.

Lemma 6.2. *Let $S_1, S_2 \subseteq V$. Then $\Gamma(S_1 \cup S_2) \subseteq \Gamma(S_1) \cup \Gamma(S_2)$.*

Proof. Let $x \in \Gamma(S_1 \cup S_2)$. Thus $x \in N(S_i)$ for some $i \in \{1, 2\}$, and furthermore $x \notin S_1 \cup S_2$ and so $x \notin S_i$. This implies that $x \in \Gamma(S_i)$. We conclude that $\Gamma(S_1 \cup S_2) \subseteq \Gamma(S_1) \cup \Gamma(S_2)$. □

Let T be a set of at most $se/2$ vertices. A set $S \subseteq V$ is *relevant* for T if $|S| \leq s$ and $\Gamma(S) \subseteq T$.

Lemma 6.3. *Let T be a set of at most $se/2$ vertices, and $S \subseteq V$. If S is relevant for T then $|S| \leq s/2$.*

Proof. By the expansion property, $|\Gamma(S)| \geq e|S|$. Since S is relevant for T, $|\Gamma(S)| \leq |T| \leq se/2$. We deduce that $|S| \leq s/2$. □

Lemma 6.4. *Let T be a set of at most $se/2$ vertices, and $S_1, S_2 \subseteq V$. If S_1, S_2 are relevant for T then $S_1 \cup S_2$ is relevant for T.*

Proof. Lemma 6.3 shows that $|S_1 \cup S_2| \leq s$. Lemma 6.2 shows that $\Gamma(S_1 \cup S_2) \subseteq \Gamma(S_1) \cup \Gamma(S_2) \subseteq T$, and so $S_1 \cup S_2$ is relevant for T. □

We can now define the vertex support.

Definition 6.5. Let T be a set of at most $se/2$ vertices. We define $\mathrm{VSup}(T)$ as the union of all sets $S \subseteq V$ relevant for T.

Lemma 6.6. *Let T be a set of at most $se/2$ vertices. Then $\mathrm{VSup}(T)$ is relevant for T and $|\mathrm{VSup}(T)| \leq s/2$. Also, $N(\mathrm{VSup}(T)) \subseteq T \cup \mathrm{VSup}(T)$.*

Proof. The first part follows from Lemma 6.4. The second part follows from Lemma 6.3. The third part follows from $N(\mathrm{VSup}(T)) \subseteq \Gamma(\mathrm{VSup}(T)) \cup \mathrm{VSup}(T)$ and the first part. □

Recall that given the vertex support, we defined the support as $\mathrm{Sup}(X) = \mathcal{T} \cup \{M_i : i \in \mathrm{VSup}(X)\}$. We now show that the support satisfies the prerequisites of Theorem 4.10. When proving (S3), we use the simple identity $\mathrm{Objs}_{\mathcal{A}}(\mathrm{Sup}(X)) = \mathrm{VSup}(X)$. When proving (S4), we use the property that every legal A contains at most $s/2$ minimality axioms, which follows from Lemma 6.6 and the definition of Sup.

Lemma 6.7. *We have* $1 \notin I(\mathrm{Sup}(\emptyset))$.

Proof. First, we claim that $\mathrm{VSup}(\emptyset) = \emptyset$. Indeed, if S is relevant for $\emptyset$, then $\Gamma(S) = \emptyset$, contradicting the expansion property. Hence $\mathrm{Sup}(\emptyset) = \mathcal{T}$. Any linear order satisfies all trivial axioms, showing that $1 \notin I(\mathrm{Sup}(\emptyset))$. □

Lemma 6.8. *For every axiom C we have $C \in \mathrm{Sup}(C)$ and $\mathrm{Objs}(C) = \mathrm{Objs}(\mathrm{LM}(C))$.*

Proof. There are two cases. If C is a trivial axiom, then $C \in \mathrm{Sup}(C)$ by definition and $\mathrm{Objs}(C) = \mathrm{Objs}(\mathrm{LM}(C))$ by inspection. If $C = M_i$ is a minimality axiom, then $\mathrm{Sup}(C) = \mathrm{Sup}(\mathrm{Objs}(\mathrm{LM}(C)))$ and $\mathrm{Objs}(\mathrm{LM}(C)) = \{i\} \cup \Gamma(\{i\})$. Therefore $\{i\}$ is relevant for $\mathrm{Objs}(\mathrm{LM}(C))$, and we deduce that $i \in \mathrm{VSup}(\mathrm{Objs}(\mathrm{LM}(C)))$ and so $C \in \mathrm{Sup}(\mathrm{Objs}(C))$. Since C is a monomial, clearly $\mathrm{Objs}(C) = \mathrm{Objs}(\mathrm{LM}(C))$. □

Lemma 6.9. *Suppose X_1, X_2 are sets of at most $se/4$ variables. If $\mathrm{Objs}(X_1) \subseteq \mathrm{Objs}(X_2) \cup \mathrm{VSup}(X_2)$ then $\mathrm{Sup}(X_1) \subseteq \mathrm{Sup}(X_2)$.*

Proof. Let $S_1 = \mathrm{Objs}(X_1)$ and $S_2 = \mathrm{Objs}(X_2)$, so that $S_1 \subseteq S_2 \cup \mathrm{VSup}(S_2)$. We will show that $\mathrm{VSup}(S_1) \subseteq \mathrm{VSup}(S_2)$ by showing that $\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2)$ is relevant for S_2. Indeed, Lemma 6.3 shows that $|\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2)| \leq s$. Lemma 6.2 shows that $\Gamma(\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2)) \subseteq \Gamma(\mathrm{VSup}(S_1)) \cup \Gamma(\mathrm{VSup}(S_2)) \subseteq S_2 \cup \mathrm{VSup}(S_2)$. However, by definition $\Gamma(\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2))$ is disjoint from $\mathrm{VSup}(S_2)$, and so $\Gamma(\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2)) \subseteq S_2$. We conclude that $\Gamma(\mathrm{VSup}(S_1) \cup \mathrm{VSup}(S_2))$ is relevant for S_2. □

Lemma 6.10. *Let m be a monomial of degree at most $se/4$ which is reducible modulo $I(\mathcal{T} \cup M)$, where M is a collection of at most $s/2$ minimality axioms. If $\mathcal{T} \cup M \supseteq \mathrm{Sup}(m)$ then m is reducible modulo $I(\mathrm{Sup}(m))$.*

Proof. Let $M = \{M_i : i \in S\}$, where $|S| \leq s$. The proof is by induction on $|S \setminus \mathrm{VSup}(m)|$. If $S = \mathrm{VSup}(m)$ then there is nothing to prove. Otherwise, by definition of VSup, $\Gamma(S) \nsubseteq \mathrm{Objs}(m)$. Therefore there exists an $i \in S$ which has a neighbor $j \notin \mathrm{Objs}(m) \cup S$. Let σ_j be the substitution given by Lemma 6.1.

Since m is reducible modulo $I(\mathcal{T} \cup M)$ there is a polynomial $P \in I(\mathcal{T} \cup M)$ such that $\mathrm{LT}(P) = m$. The substitution σ_j satisfies some axioms, falsifies M_j, and leaves the rest unaffected. Since $j \notin S$, we deduce that $P|_{\sigma_j} \in I(\mathcal{T} \cup (M \setminus \{M_i\}))$. Since $j \notin \mathrm{Objs}(m)$, $\mathrm{LT}(P|_{\sigma_j}) = m$. Therefore we can apply the induction hypothesis. □

Having verified all the properties of the support, we conclude the following lower bound from Theorem 4.10.

Theorem 6.11 ([GL10])**.** *Suppose G is a graph in which any set S of up to s vertices satisfies $|\Gamma(S)| \geq e|S|$, for some $s, e > 0$. Then the graph ordering principle defined by G cannot be refuted in degree $se/4$.*

References

[AR03] Misha Alekhnovich and Alexander Razborov. Lower bounds for polynomial calculus: non-binomial case. *Proceedings of the Steklov Institute of Mathematics*, 242:18–35, 2003.

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

[GL10] Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Transactions on Computational Logic*, 12(1):4:1–4:22, 2010.