

Another look at degree lower bounds for polynomial calculus

Yuval Filmus*

August 20, 2019

Abstract

Polynomial complexity is an algebraic proof system inspired by Gröbner bases which was introduced by Clegg, Edmonds and Impagliazzo. Alekhovich and Razborov devised a method for proving degree lower bounds for polynomial calculus. We present an alternative account of their method, which also encompasses a generalization due to Galesi and Lauria.

1 Introduction

Polynomial calculus [5, 1] is an algebraic proof system whose lines are polynomials over a field. Given a list of initial polynomials, the rules of polynomial calculus allow deriving polynomials which are in the ideal generated by the initial polynomials. When used as a refutation system, the goal is to derive 1, showing that the ideal generated by the initial polynomials is empty, and so the set of initial polynomials is inconsistent (has no common solution).

Given a list of initial polynomials, there are several ways of measuring how difficult it is to refute them in polynomial calculus. One obvious measure is proof size, and another one is space complexity [1]. In this article we will be interested in a third measure, *degree*, which is the analog of width in Resolution. Width lower bounds translate to size lower bounds in Resolution [4]. Similarly, degree lower bounds translate to size lower bounds in polynomial calculus [8]. Moreover, degree lower bounds for the related Nullstellensatz proof system can be used to prove lower bounds on constant-depth Frege [3].

The principal method for proving lower bounds on degree in polynomial calculus is due to Alekhovich and Razborov [2]. Galesi and Lauria used the method to prove non-automatizability results for polynomial calculus [6]. They also used a generalized version of the method to prove lower bounds on the graph ordering principle [7]. Mikša and Nordström [9] used the method to prove lower bounds on formulas based on combinatorial block designs, and in subsequent work [10] unified all existing bounds based on this method.

The goal of this article is twofold. First, we provide a new proof of the original lower bound of Alekhovich and Razborov. Second, we present it in an abstract framework which separates the algebraic and combinatorial parts of the argument.

Both our paper and the work of Mikša and Nordström [10] generalize the original framework of Alekhovich and Razborov. However, the focus of the two works is rather different. Whereas our paper focuses on reproving known results in a new and hopefully illuminating way, Mikša and Nordström focus on applying the original proof of Alekhovich and Razborov to new situations,

*Technion — Israel Institute of Technology, Haifa, Israel. Taub Fellow — supported by the Taub Foundations

obtaining novel lower bounds. We believe that our framework can be adapted to encompass the generalization of Mikša and Nordström, but leave it for further research.

Organization After a few preliminaries in Section 2, we describe our abstract our abstract framework and alternative proof in Section 3. We provide two instantiations of our abstract framework: one which follows the original work of Alekhovich and Razborov [2] (Section 4), and another which follows the work of Galesi and Lauria [7] (Section 5).

Acknowledgements This article is based on work done while the author was visiting Jakob Nordström’s group at KTH in December 2012. We thank Jakob and his group for their hospitality and for exposing me to the fascinating subject matter of this article.

2 Preliminaries

2.1 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 .

The system has three deduction rules. *Axiom download* allows deriving any axiom. *Linear combination* allows deriving any linear combination of two derived lines. *Multiplication by variable* allows multiplying any derived line by a variable; the line is then reduced to its squarefree form.

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 [5].

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.

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. Similarly, it can be used to refute systems of polynomial equations over 0/1-valued assignments, by converting an equation $P = Q$ to the polynomial $P - Q$.

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

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: $\deg m_1 < \deg m_2$; or $\deg m_1 = \deg m_2$ and $x_1 < x_2$; or $\deg m_1 = \deg m_2$, $x_1 = x_2$, and $m'_1 < m'_2$.

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

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 iff 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 a monomial m and a polynomial P , we say that 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 $\text{Mon}(S) = \prod_{x \in S} x$.

3 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 Alekhovich and Razborov, as well as their extension due to Galesi and Lauria [7].

Alekhovich and Razborov proved a lower bound for CNFs in which the vertex-clause incidence graph is an expander. Galesi and Lauria proved a lower bound for the graph ordering principle. We describe these applications in more detail in the following sections, and use them as running examples to illustrate some of our definitions.

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 2^S denote the power set of S , and let $S_{\leq z} = \{T \subseteq S : |T| \leq z\}$.

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”.

In the work of Alekhovich and Razborov, the objects are the same as the variables: $\mathcal{O} = \mathcal{V}$. Galesi and Lauria consider the graph ordering principle on a graph $G = (V, E)$. In their case, $\mathcal{V} = \{x_{ij} : \{i, j\} \in E\}$ corresponds to the edges, and $\mathcal{O} = V$ is the set of vertices.

Let $\text{Objs} : \mathcal{V} \rightarrow 2^{\mathcal{O}}$ and $\text{Objs}_{\mathcal{A}} : \mathcal{A} \rightarrow 2^{\mathcal{O}}$ be functions satisfying the following axiom:

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

In the case of Alekhovich and Razborov, $\text{Objs}(x) = \{x\}$ and $\text{Objs}_{\mathcal{A}}(C)$ is the set of variables appearing in C . In this case (VO) is trivial: σ_x can be any assignment to x . For the graph ordering principle considered by Galesi and Lauria, $\text{Objs}(x_{ij}) = \{i, j\}$. The axioms come in two flavors: axioms stating that the x_{ij} encode a linear order on the vertices, and axioms M_i stating that vertex i is not a local minimum. Then $\text{Objs}_{\mathcal{A}}(M_i) = \{i\}$, and $\text{Objs}_{\mathcal{A}}(C) = \emptyset$ for all other axioms C .

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

Let the *support* be a function $\text{Sup} : \text{Objs}(\mathcal{V}_{\leq \mathbf{D}}) \rightarrow 2^{\mathcal{A}}$ whose input is a set of the form $\text{Objs}(S)$ for some $S \in \mathcal{V}_{\leq \mathbf{D}}$. For a monomial or set of variables m , define $\text{Sup}(m) = \text{Sup}(\text{Objs}(m))$. For a non-zero polynomial P , define $\text{Sup}(P) = \text{Sup}(\text{LM}(P))$. We say that a subset $A \subseteq \mathcal{A}$ is *legal* if $A = \text{Sup}(S)$ for some $S \in \mathcal{V}_{\leq \mathbf{D}}$. For a polynomial P , define the *total support* $\text{TSup}(P)$ of P to be the union of $\text{Sup}(m)$ for all monomials $m \in P$.

We assume that the support satisfies the following axioms:

- (S1) Non-triviality: $1 \notin I(\text{Sup}(1))$.
- (S2) For $C \in \mathcal{A}$, $C \in \text{Sup}(C)$ and $\text{Objs}(C) \subseteq \text{Objs}(\text{LM}(C)) \cup \text{Objs}_{\mathcal{A}}(\text{Sup}(C))$.
- (S3) Let $S_1, S_2 \in \mathcal{V}_{\leq \mathbf{D}}$. If $\text{Objs}(S_1) \subseteq \text{Objs}(S_2) \cup \text{Objs}_{\mathcal{A}}(\text{Sup}(S_2))$ then $\text{Sup}(S_1) \subseteq \text{Sup}(S_2)$.
- (S4) Let $S \in \mathcal{V}_{\leq \mathbf{D}}$ and let $A \subseteq \mathcal{A}$ be legal. If $\text{Sup}(S) \subseteq A$ and $\text{Mon}(S)$ is reducible modulo $I(A)$ then it is reducible modulo the smaller ideal $I(\text{Sup}(S))$.

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

The support of a monomial is intended to be the set of “relevant” axioms. The definition of support in particular applications is rather subtle. When instantiating our framework in Section 4 and Section 5, we use the exact same definition of the support used by Alekhovich and Razborov [2] and by Galesi and Lauria [7], in a slightly simplified form.

We prove our degree lower bound by showing that each line appearing in the proof can be reduced to zero using the following algorithm: repeatedly reduce the line P modulo $\text{Sup}(P)$, each time working only over the variables appearing in $\text{LM}(P)$ and $\text{Sup}(P)$. 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*; (S2) implies that this is the case for axioms. 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.

Here are the formal definition of the two concepts just mentioned:

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

The definition of semisimple polynomials immediately implies the following lemma.

Lemma 3.1. *Suppose P is a semisimple polynomial with semisimple decomposition $\sum_i P_i$. Then for some i , $\text{LT}(P_i) = \text{LT}(P)$, and for $j \neq i$, $\text{LM}(P_j) < \text{LM}(P)$.*

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

We have defined simple polynomials so that the following property holds.

Lemma 3.2. *If P is simple then $\text{TSup}(P) = \text{Sup}(P)$.*

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

Our plan is to show that everything derivable from \mathcal{A} in degree \mathbf{D} is semisimple, while 1 is not semisimple. This will require a criterion for semisimplicity, Lemma 3.4 below. In order to prove our criterion, we need a way of coming up with simple polynomials. This is the contribution of the following lemma.

Lemma 3.3. *If m is a monomial of degree at most \mathbf{D} reducible modulo $I(\text{Sup}(m))$ then there is a simple polynomial P whose leading term is m .*

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

The following lemma, which contains the only application of (S4), is our crucial criterion for semisimplicity.

Lemma 3.4. *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 $\text{TSup}(P)$ then P is semisimple.*

Proof. The proof is by induction on $\text{LM}(P)$. The base case is $P = 0$. If $P \neq 0$ then $\text{LM}(P)$ is reducible modulo $I(A)$, and so modulo $I(\text{Sup}(\text{LM}(P)))$, by (S4). Lemma 3.3 shows that there exists a simple polynomial Q with $\text{LT}(Q) = \text{LT}(P)$. Since $\text{Sup}(Q) = \text{Sup}(P) \subseteq \text{TSup}(P)$ and Q is simple, $Q \in I(A)$ and so $P - Q \in I(A)$. Since Q is simple, Lemma 3.2 shows that $\text{TSup}(Q) = \text{Sup}(Q) \subseteq \text{TSup}(P) \subseteq A$. Since $\text{LM}(P - Q) < \text{LM}(P)$, we can apply the induction hypothesis to $P - Q$, deducing that it is semisimple. Lemma 3.1 shows that all polynomials in a semisimple decomposition $\sum_i R_i$ of $P - Q$ satisfy $\text{LM}(R_i) \leq \text{LM}(P - Q) < \text{LM}(P) = \text{LM}(Q)$, and so $Q + \sum_i R_i$ is a semisimple decomposition of P . \square

We can now follow up on our plan to show that everything derivable from \mathcal{A} in degree \mathbf{D} is semisimple, starting with the base case, axiom download; this is the only place we use (S2).

Lemma 3.5. *Every $C \in \mathcal{A}$ is simple, and so semisimple.*

Proof. This is an immediate consequence of (S2). \square

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

Lemma 3.6. *Suppose P_1, P_2 are simple polynomials with $\text{LT}(P_1) = \text{LT}(P_2)$. Then $P_1 - P_2$ is semisimple.*

Proof. Since P_1 and P_2 are simple and $\text{Sup}(P_1) = \text{Sup}(P_2)$, Lemma 3.2 shows that $\text{TSup}(P_1 - P_2) \subseteq \text{Sup}(P_1)$. Since $P_1 - P_2 \in I(\text{Sup}(P_1)) = I(\text{Sup}(P_2))$, Lemma 3.4 shows that $P_1 - P_2$ is semisimple. \square

Lemma 3.7. *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 $\text{LM}(P_1 + P_2) = m$ 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 $\text{LM}(P_1 + P_2) < m$ then Lemma 3.6 (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 3.1. 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 $\Phi(S) = \sum_{P \in S} \omega^{\iota(\text{LM}(P))}$, where ω is the ordinal of the natural numbers. 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_1P_1 and c_2P_2 . We deduce that $\sum S = c_1P_1 + c_2P_2$ is semisimple. \square

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

Lemma 3.8. *Suppose P is a semisimple polynomial and x is a variable. If $\deg(xP) \leq \mathbf{D}$ then xP is semisimple.*

Proof. In view of Lemma 3.7, we can assume that P is simple.

Suppose first that $\text{Obj}_s(x) \subseteq \text{Obj}_s(\text{LM}(P))$. Since P is simple, every monomial $xm \in xP$ satisfies $\text{Obj}_s(xm) \subseteq \text{Obj}_s(\text{LM}(P)) \cup \text{Obj}_s(\text{Sup}(P))$. Therefore $\text{Sup}(xm) \subseteq \text{Sup}(P)$ by (S3), and so $\text{TSup}(xP) \subseteq \text{Sup}(P)$. Since P is simple, $xP \in I(\text{Sup}(P))$, and so Lemma 3.4 shows that xP is semisimple.

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

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

Lemma 3.9. *The polynomial 1 is not semisimple.*

Proof. If 1 were semisimple, then Lemma 3.1 would show that there is some simple polynomial P with $\text{LT}(P) = 1$. This is impossible since $1 \notin I(\text{Sup}(1))$ by (S1). \square

We are now ready to prove the main theorem of this section.

Theorem 3.10. *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 $\text{Obj}_s: \mathcal{V} \rightarrow 2^{\mathcal{O}}$, $\text{Obj}_{s\mathcal{A}}: \mathcal{A} \rightarrow 2^{\mathcal{O}}$, and $\text{Sup}: \text{Obj}_s(\mathcal{V}_{\leq \mathbf{D}}) \rightarrow 2^{\mathcal{A}}$, satisfying axioms (V), (S1-4). Then the set \mathcal{A} cannot be refuted in degree \mathbf{D} .*

Proof. Lemma 3.5, Lemma 3.7 and Lemma 3.8 show that everything derivable in degree \mathbf{D} is semisimple. Conversely, Lemma 3.9 shows that 1 is not semisimple, and so cannot be derived in degree \mathbf{D} . \square

4 Expanding formulas in conjunctive normal form

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

Let Φ be a formula in conjunctive normal form. We 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 3 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 4.1. *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 $\partial(S_1 \cup S_2) \subseteq \partial(S_1) \cup \partial(S_2)$. \square

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 4.2. *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 $|S| \leq s/2$. \square

Lemma 4.3. *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 4.2 shows that $|S_1 \cup S_2| \leq s$. Lemma 4.1 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 . \square

We can now define the support.

Definition 4.4. Let V be a set of at most $se/2$ variables. We define $\text{Sup}(V)$ as the union of all sets $S \subseteq \Phi$ relevant for V .

Lemma 4.5. *Let V be a set of at most $se/2$ variables. Then $\text{Sup}(V)$ is relevant for V and $|\text{Sup}(V)| \leq s/2$.*

Proof. The first part follows from Lemma 4.3, the second part from Lemma 4.2. \square

We now show that the support satisfies the prerequisites of Theorem 3.10. Since $\mathcal{O} = \mathcal{V}$, (VO) trivially holds. We prove the rest of the prerequisites in order. The proof of (S4) uses the bound $|A| \leq s/2$ on all legal sets A given by Lemma 4.5.

Lemma 4.6. *We have $\text{Sup}(\emptyset) = \emptyset$.*

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

Lemma 4.7. *For every clause $C \in \Phi$ we have $C \in \text{Sup}(C)$.*

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

Lemma 4.8. *Suppose V_1, V_2 are sets of at most $se/2$ variables. If $V_1 \subseteq V_2 \cup \text{Objs}_{\mathcal{A}}(\text{Sup}(V_2))$ then $\text{Sup}(V_1) \subseteq \text{Sup}(V_2)$.*

Proof. Lemma 4.5 shows that $\text{Sup}(V_1)$ is relevant for V_1 , and so $\partial \text{Sup}(V_1) \subseteq V_1 \subseteq V_2 \cup \text{Objs}_{\mathcal{A}}(\text{Sup}(V_2))$. The lemma also shows that $\text{Sup}(V_2)$ is relevant for V_2 , and so $\partial \text{Sup}(V_2) \subseteq V_2$. Moreover, the lemma shows that $|\text{Sup}(V_1) \cup \text{Sup}(V_2)| \leq s$.

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

Lemma 4.9. *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 $A \supseteq \text{Sup}(m)$ then m is reducible modulo $I(\text{Sup}(m))$.*

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

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

Having verified all the properties of the support, we conclude the following lower bound from Theorem 3.10.

Theorem 4.10 ([2]). *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 $se/2$.*

5 Graph ordering principle

In this section, we instantiate the lower bound framework for the graph ordering principle, following Galesi and Lauria [7]. 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* σ_{ij} : $x_{ij} + x_{ji} = 1$. For every triple $i, j, k \in V$ of different vertices, there is a *transitivity axiom* $\tau_{i,j,k}$: $x_{ij}x_{jk}x_{ki} = 0$. 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 : $\prod_{j \in N(i)} x_{ij} = 0$. 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 4. We will instantiate the framework of Section 3 with $\mathbf{D} = se/4$ and $\mathcal{O} = V$.

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

Lemma 5.1. *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. \square

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 $\text{VSup}(X) = \text{VSup}(\text{Objs}(X))$. Similarly, for a monomial m , we define $\text{VSup}(m) = \text{VSup}(\text{Objs}(m))$. Given VSup , we define $\text{Sup}(X) = \mathcal{T} \cup \{M_i : i \in \text{VSup}(X)\}$.

Our definition of VSup mimics the definition of the support in Section 4. Therefore we skip some of the identical proofs.

Lemma 5.2. *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 $\Gamma(S_1 \cup S_2) \subseteq \Gamma(S_1) \cup \Gamma(S_2)$. \square

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

Lemma 5.4. *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 .*

We can now define the vertex support.

Definition 5.5. Let T be a set of at most $se/2$ vertices. We define $\text{VSup}(T)$ as the union of all sets $S \subseteq V$ relevant for T .

Lemma 5.6. *Let T be a set of at most $se/2$ vertices. Then $\text{VSup}(T)$ is relevant for T and $|\text{VSup}(T)| \leq s/2$. Also, $N(\text{VSup}(T)) \subseteq T \cup \text{VSup}(T)$.*

Proof. The first part follows from Lemma 5.4. The second part follows from Lemma 5.3. The third part follows from $N(\text{VSup}(T)) \subseteq \Gamma(\text{VSup}(T)) \cup \text{VSup}(T)$ and the first part. \square

Recall that given the vertex support, we defined the support as $\text{Sup}(X) = \mathcal{T} \cup \{M_i : i \in \text{VSup}(X)\}$. We now show that the support satisfies the prerequisites of Theorem 3.10. When proving (S3), we use the simple identity $\text{Obj}_{\mathcal{A}}(\text{Sup}(X)) = \text{VSup}(X)$. When proving (S4), we use the property that every legal A contains at most $s/2$ minimality axioms, which follows from Lemma 5.6 and the definition of Sup .

Lemma 5.7. *We have $1 \notin I(\text{Sup}(1))$.*

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

Lemma 5.8. *For every axiom C we have $C \in \text{Sup}(C)$ and $\text{Obj}(C) = \text{Obj}(\text{LM}(C))$.*

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

Lemma 5.9. *Suppose X_1, X_2 are sets of at most $se/4$ variables. If $\text{Obj}(X_1) \subseteq \text{Obj}(X_2) \cup \text{VSup}(X_2)$ then $\text{Sup}(X_1) \subseteq \text{Sup}(X_2)$.*

Proof. Let $S_1 = \text{Obj}(X_1)$ and $S_2 = \text{Obj}(X_2)$, so that $S_1 \subseteq S_2 \cup \text{VSup}(S_2)$. We will show that $\text{VSup}(S_1) \subseteq \text{VSup}(S_2)$ by showing that $\text{VSup}(S_1) \cup \text{VSup}(S_2)$ is relevant for S_2 . Indeed, Lemma 5.3 shows that $|\text{VSup}(S_1) \cup \text{VSup}(S_2)| \leq s$. Lemma 5.2 shows that $\Gamma(\text{VSup}(S_1) \cup \text{VSup}(S_2)) \subseteq \Gamma(\text{VSup}(S_1)) \cup \Gamma(\text{VSup}(S_2)) \subseteq S_2 \cup \text{VSup}(S_2)$. However, by definition $\Gamma(\text{VSup}(S_1) \cup \text{VSup}(S_2))$ is disjoint from $\text{VSup}(S_2)$, and so $\Gamma(\text{VSup}(S_1) \cup \text{VSup}(S_2)) \subseteq S_2$. We conclude that $\Gamma(\text{VSup}(S_1) \cup \text{VSup}(S_2))$ is relevant for S_2 . \square

Lemma 5.10. *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 $\mathcal{T} \cup M \supseteq \text{Sup}(m)$ then m is reducible modulo $I(\text{Sup}(m))$.*

Proof. Let $M = \{M_i : i \in S\}$, where $|S| \leq s/2$. The proof is by induction on $|S \setminus \text{VSup}(m)|$. If $S = \text{VSup}(m)$ then there is nothing to prove. Otherwise, by definition of VSup , $\Gamma(S) \not\subseteq \text{Obj}(m)$. Therefore there exists an $i \in S$ which has a neighbor $j \notin \text{Obj}(m) \cup S$. Let σ_j be the substitution given by Lemma 5.1.

Since m is reducible modulo $I(\mathcal{T} \cup M)$ there is a polynomial $P \in I(\mathcal{T} \cup M)$ such that $\text{LT}(P) = m$. The substitution σ_j satisfies some axioms including M_i , 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 $j \notin \text{Obj}(m)$, $\text{LT}(P|_{\sigma_j}) = m$. Therefore we can apply the induction hypothesis. \square

Having verified all the properties of the support, we conclude the following lower bound from Theorem 3.10.

Theorem 5.11 ([7]). *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

- [1] Michael Alekhovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002.
- [2] Misha Alekhovich and Alexander Razborov. Lower bounds for polynomial calculus: non-binomial case. *Proceedings of the Steklov Institute of Mathematics*, 242:18–35, 2003.
- [3] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert’s Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73(1):1–26, July 1996.
- [4] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.
- [5] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithms to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC ’96)*, pages 174–183, May 1996.
- [6] Nicola Galesi and Massimo Lauria. On the automatizability of polynomial calculus. *Theory of Computing Systems*, 47(2):491–506, 2010.
- [7] 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.
- [8] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999.
- [9] Mladen Mikša and Jakob Nordström. Long proofs of (seemingly) simple formulas. In *Proceedings of the 17th International Conference on Theory and Applications of Satisfiability Testing (SAT 14)*, volume 8561 of *Lecture Notes in Computer Science*, pages 121–137. Springer, July 2014.
- [10] Mladen Mikša and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. In *Proceedings of the 30th Annual Computational Complexity Conference (CCC ’15)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 467–487, June 2015.