Functional Lower Bounds in Algebraic Proofs: Symmetry, Lifting, and Barriers*

Tuomas Hakoniemi[†]
University of Helsinki

Nutan Limaye[‡]
IT University of Copenhagen

Iddo Tzameret[¶]
Imperial College London

March 2024

Abstract

Strong algebraic proof systems such as IPS (Ideal Proof System; Grochow-Pitassi [GP18]) offer a general model for deriving polynomials in an ideal and refuting unsatisfiable propositional formulas, subsuming most standard propositional proof systems. A major approach for lower bounding the size of IPS refutations is the Functional Lower Bound Method (Forbes, Shpilka, Tzameret and Wigderson [FSTW21]), which reduces the hardness of refuting a polynomial equation $f(\overline{x}) = 0$ with no Boolean solutions to the hardness of computing the function $1/f(\overline{x})$ over the Boolean cube with an algebraic circuit. Using symmetry we provide a general way to obtain many new hard instances against fragments of IPS via the functional lower bound method. This includes hardness over finite fields and hard instances different from Subset Sum variants both of which were unknown before, and stronger constant-depth lower bounds. Conversely, we expose the limitation of this method by showing it cannot lead to proof complexity lower bounds for any hard *Boolean* instance (e.g., CNFs) for any sufficiently strong proof systems. Specifically, we show the following:

Nullstellensatz degree lower bounds using symmetry: Extending [FSTW21] we show that every unsatisfiable symmetric polynomial with n variables requires degree $> n$ refutations (over sufficiently large characteristic). Using symmetry again, by characterising the $n/2$-homogeneous slice appearing in refutations, we show that unsatisfiable *invariant* polynomials of degree $n/2$ require degree $\geq n$ refutations.

Lifting to size lower bounds: Lifting our Nullstellensatz degree bounds to IPS-size lower bounds, we obtain exponential lower bounds for any poly-logarithmic degree symmetric instance against IPS refutations written as oblivious read-once algebraic programs (roABP-IPS). For invariant polynomials, we show lower bounds against roABP-IPS and refutations written as multilinear formulas in the *placeholder* IPS regime (studied by Andrews-Forbes [AF22]), where the hard instances do not necessarily have small roABPs themselves, including over *positive characteristic* fields. This provides the first IPS-fragment lower bounds over finite fields.

By an adaptation of the work of Amireddy, Garg, Kayal, Saha and Thankey [AGK+23], we extend and strengthen the constant-depth IPS lower bounds obtained recently in Govindasamy, Hakoniemi and Tzameret [GHT22] which held only for multilinear proofs, to $\mathsf{poly}(\log \log n)$ *individual degree* proofs. This is a natural and stronger constant depth proof system than in [GHT22], which admits small refutations for standard hard instances like the pigeonhole principle and Tseitin formulas.

Barriers for Boolean instances: While lower bounds against strong propositional proof systems were the original motivation for studying algebraic proof systems in the 1990s [BIK+96a, BIK+96b], we show that the functional lower bound method alone cannot establish any size lower bound for *Boolean* instances for any sufficiently strong proof systems, and in particular, cannot lead to lower bounds against $\mathrm{AC}^0[p]$-Frege and TC^0-Frege.

Contents

*A preliminary abbreviated version of this work appears in STOC 2024. The preliminary version included a quantitative strengthening of the lower bound against multilinear constant-depth IPS refutations from [GHT22]. The current version extends and strengthens the lower bound in [GHT22] to work against $O(\log\log n)$ individual degree constant-depth IPS refutations.

†Part of this work was done at Simons Institute for the Theory of Computing. This work was partly funded by Helsinki Institute of Information Technology (HIIT) and by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 101002742).

‡Part of this work was done at Simons Institute for the Theory of Computing, UC Berkeley. Part of this project has received funding from the Independent Research Fund Denmark (grant agreement No. 10.46540/3103-00116B).

¶Department of Computing. Part of this work was done at Simons Institute for the Theory of Computing, UC Berkeley. Part of this project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 101002742). Email: iddo.tzameret@gmail.com

1 Introduction

This work studies lower bounds against strong propositional proof systems. We focus on strong algebraic proof systems that extend the Nullstellensatz system, and explore the capabilities and limitations of the *functional lower bound method* which is arguably the most successful technique to date for achieving such lower bounds. Our goal is to expand the range of applications of this technique to yield new hard instances, as well as to provide new variants of this technique showing how to get lower bounds in new settings like finite fields, hard instances qualitatively different from previously known ones, and improved constant depth lower bounds. Finally, we ask whether this technique alone can lead to the solution of long-standing open problems in proof complexity, showing essentially it cannot reach this goal.

1.1 Proof Complexity and Strong Algebraic Proof Systems

Algebraic proof systems model efficient derivation within polynomial ideals. Starting from a set of polynomials over a field (the set of "axioms"), one uses addition and multiplication to form new polynomials in the ideal generated by the axioms. When the axioms are unsatisfiable, namely do not have a common root over the field, by Hilbert's Nullstellensatz one can derive the polynomial 1. This way, one has in fact *refuted* the set of axioms, since a common root of the axioms must nullify every polynomial in their ideal.

Due to its natural setup, algebraic proof systems attracted a lot of attention in complexity and specifically propositional proof complexity, in which one studies the efficiency with which different proof systems prove propositional tautologies or refute unsatisfiable propositional formulas. For that purpose, one can consider algebraic proof systems as propositional proof systems by adding as a default to the set of axioms *Boolean axioms* like $x_i^2 - x_i$ for all variables x_i. These Boolean axioms force any common root of the set of axioms to be Boolean in itself.

The starting point of algebraic proof systems is the work of Beame, Impagliazzo, Krajíček, Pitassi and Pudlák [BIK+96a] (cf. Buss, Impagliazzo, Krajíček, Pudlák and Razborov [BIK+96b]), which was motivated by the long-standing open problem of $\mathrm{AC}^0[p]$-Frege lower bounds. The $\mathrm{AC}^0[p]$-Frege proof system operates with constant-depth propositional formulas together with counting modulo p gates, for p a prime. Initial results on algebraic proof systems established connections between these proof systems and algebraic proof systems.

The algebraic proof system introduced by [BIK+96a] is the *Nullstellensatz* system. In Nullstellensatz a refutation witnessing the unsatisfiability of a set of axioms given as polynomial equations $\{f_i(\overline{x}) = 0\}_i$ over a field, is a polynomial combination of the axioms that equals 1 as a formal polynomial, namely:

$$\sum_i g_i(\overline{x}) \cdot f_i(\overline{x}) = 1\,, \tag{0.1}$$

for some polynomials $\{g_i(\overline{x})\}_i$. The degree of this Nullstellensatz refutation is the maximal degree of $g_i(\overline{x}) \cdot f_i(\overline{x})$. The size of this refutation is the sparsity, that is the total number of monomials in all the polynomials $g_i(\overline{x}) \cdot f_i(\overline{x})$. The sparsity measure is what makes these proof systems weak (e.g., even a simple polynomial like $(x_1 - 1) \cdots (x_n - 1) = 0$ accounts for an exponential size because the number of monomials in it is 2^n).

Although the initial motivation behind the introduction of the Nullstellensatz system was to achieve progress on $\mathrm{AC}^0[p]$-Frege lower bounds, it seems that Nullstellensatz lower bounds techniques that focus on the number of monomials or degree are not enough to reach lower bounds for relatively strong proof systems (including $\mathrm{AC}^0[p]$-Frege). For that purpose, one can consider stronger algebraic proof systems for which size is measured by *algebraic complexity*, namely by

the minimal size of an *algebraic circuit* computing the polynomials $g_i(\overline{x})$ in Equation (0.1). That way, one can hope to employ ideas from algebraic circuit complexity, in a similar way that proof techniques from Boolean circuit complexity like random restrictions and switching lemmas serve to study AC^0-Frege lower bounds [Ajt88, PBI93, KPW95].

The idea of considering algebraic proof systems operating with algebraic circuits was investigated initially by Pitassi [Pit97, Pit98]. And subsequently was studied in Grigoriev and Hirsch [GH03], Raz and Tzameret [RT08b, RT08a, Tza11], and finally in the introduction of the Ideal Proof System (IPS) by Grochow and Pitassi [GP18] which loosely speaking is the *Nullstellensatz proof system where the polynomials $g_i(\overline{x})$ are written as algebraic circuits*; indeed, Forbes, Shpilka, Tzameret and Wigderson [FSTW21] showed that IPS is equivalent to Nullstellensatz in which the polynomials g_i in Equation (0.1) are written as algebraic circuits. In other words, an IPS refutation of the set of axioms $\{f_i(\overline{x}) = 0\}_i$ can be defined similarly to Equation (0.1) (here we display explicitly the Boolean axioms):

$$\sum_i g_i(\overline{x}) \cdot f_i(\overline{x}) + \sum_j h_j(\overline{x}) \cdot (x_j^2 - x_j) = 1\,, \tag{0.2}$$

for some polynomials $\{g_i(\overline{x})\}_i$, where we think of the polynomials g_i, h_j written as algebraic circuits (instead of e.g., counting the number of monomials they have towards the size of the refutation). Thus, the size of the IPS refutation in Equation (0.2) is $\sum_i \mathsf{size}(g_i(\overline{x})) + \sum_j \mathsf{size}(h_j(\overline{x}))$, where $\mathsf{size}(g)$ stands for the (minimal) size of an algebraic circuit computing the polynomial g.

It turns out that IPS is very strong, and simulates most known concrete propositional proof systems (such as Frege, Extended Frege, and more); see [GP18, PT16]. It is thus natural to consider proof systems that sit between the weak Nullstellensatz on the one end and the strong IPS on the other end. This is done roughly by writing the polynomials g_i, h_j in Equation (0.2) as restricted kinds of algebraic circuits, such as constant-depth circuits [GP18, AF22, GHT22], noncommutative formulas [LTW18], algebraic branching programs [FSTW21, Kno17] and multilinear formulas [FSTW21], to give some examples.

When considering algebraic circuit classes weaker than general algebraic circuits, one has to be a bit careful with the definition of IPS. For technical reasons the formalization in Equation (0.2) does not capture the precise definition of IPS restricted to the relevant circuit class, rather the fragment which is denoted by $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ ("LIN" here stands for the linearity of the axioms f_i and the Boolean axioms; that is, they appear with power 1). In this work, we focus on $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ and a similar stronger variant denoted $\mathcal{C}\text{-IPS}_{\mathrm{LIN}'}$. *Henceforth, throughout the introduction, refutations in the system $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ are defined as in Equation (0.2) where the polynomials g_i, h_j are written as circuits in the circuit class $\mathcal{C}$.*

Technical comment: All our lower bounds are proved by lower bounding the algebraic circuit size of the g_i's in Equation (0.2), namely the products of the axioms f_i, and *not* the products of the Boolean axioms (that is, we ignore the circuit size of the h_i's). For this reason, our lower bounds are slightly stronger than lower bounds on $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$, rather they are lower bounds on the system denoted $\mathcal{C}\text{-IPS}_{\mathrm{LIN}'}$ (see Definition 8 for a precise formulation).

When considering the $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ refutation in Equation (0.2), we can see that its size as defined above does *not* depend on the size of the axioms f_i and $\overline{x}^2 - \overline{x}$. Therefore, it is possible to think of lower bounds on $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ refutations for axioms f_i that are large (e.g., super-polynomial in the number of variables) or outside the circuit class $\mathcal{C}$: although the axioms do not have small representation (or are even non-explicit) their $\mathcal{C}\text{-IPS}_{\mathrm{LIN}}$ refutations may be small, and we want to rule out this possibility. We call this regime of lower bounds a *placeholder IPS lower bound*. Here, "placeholder" stands for the fact that in the refutation Equation (0.2) we can replace the axioms

f_i and $\overline{x}^2 - \overline{x}$ by variables (which take the role of axiom placeholders), measure the size of the resulting refutation, and then replace the axioms in their place again to get Equation (0.2). Forbes *et al.* [FSTW21] considered placeholder IPS lower bounds using the approach of hard multiples, and studied its relation to the randomness versus hardness paradigm.

While it is reasonable to assume that we can establish placeholder IPS lower bounds using some (possibly non-explicit) polynomial equations that require large circuit size, it is interesting to consider *explicit* such hard instances in the IPS placeholder regime. Such explicit hard instances in the form of determinant identities were recently established by by Andrews and Forbes [AF22] in the placeholder IPS regime.

Different IPS Lower Bound Methods. The first to obtain proof complexity lower bounds by reductions to algebraic circuit complexity lower bounds were [FSTW21]. They introduced two methods: the *functional lower bound* method and the *lower bounds for multiples* method.

Functional lower bounds: At the moment, the functional lower bound method yields stronger lower bounds than the latter one. It produced several concrete proof complexity lower bounds for variants of subset-sum instances against fragments of IPS. These fragments include IPS refutations written as read once (oblivious) algebraic branching programs (roABPs), depth-3 powering formulas (introduced as "diagonal depth-3 circuits" in Saxena [Sax08]), and multilinear formulas. Alekseev, Hirsch, Grigoriev, and Tzameret [AGHT20] used a method very similar to the functional lower bound method to establish a conditional lower bound on (general) IPS (leading to [Ale21]). And [GHT22] used this method together with Limaye, Srinivasan, and Tavenas constant-depth algebraic circuit lower bounds [LST21] to establish multilinear constant depth IPS lower bounds.

Lower bound for multiples: On the other hand, the lower bound for multiples method was used in [FSTW21, AF22] to establish lower bounds against the weaker model of *placeholder* $\mathcal{C}$-IPS proofs, in which the hard instances do not necessarily have small circuits themselves in $\mathcal{C}$.

It is worth mentioning three other (fairly strong, IPS-style) algebraic proof lower bounds approaches in the literature, as follows.

Meta-complexity: Another method for IPS lower bounds is the *meta-complexity* technique introduced by Santhanam and Tzameret [ST21] who proved an IPS size lower bound on a self-referential statement. However, this lower bound is currently only conditional.

Noncommutative approach: Li, Tzameret and Wang [LTW18] (following [Tza11]) considered IPS refutations over noncommutative formulas. Using this, they showed that size lower bounds against Frege proofs can be reduced to the task of proving that the rank of certain families of matrices is high. This however, does not yet yield any concrete lower bound since it is unclear at the moment how to characterise precisely families of matrices that correspond to noncommutative IPS proofs (namely, given an unsatisfiable CNF formula we would like to characterise and identify certain properties of matrices that correspond to noncommutative IPS refutations of the CNF formula; and using those properties establish rank lower bounds).

PC with extension variables: Finally, Impagliazzo, Mauli and Pitassi [IMP23] (following Sokolov [Sok20]; see improvements in [DMM23]) proved a polynomial calculus with extension variable lower bounds for a CNF formula, over a finite field. Although this is a lower bound against the number of monomials appearing in refutations, due to the (restricted amount of) extension variables, this can be considered as a proof system between depth-2 IPS (i.e., Nullstellensatz) to depth-3 IPS—denoted informally as "depth 2.5-IPS". This lower bound is over finite fields. Apparently this method cannot go beyond this "depth 2.5-IPS" lower bounds.

It is important to notice also that all unconditional IPS size lower bounds (apart from those that are lower bounds against number of monomials only, and hence stated in the setting of Null-

stellensatz or Polynomial Calculus, including the result of [IMP23]), are all for hard instances that are *non-Boolean* (e.g., not CNF formulas; namely, polynomials that do not take on 0-1 values over the Boolean cube). We discuss this matter in Section 1.3.3.

1.2 The Functional Lower Bound Method

We start by recalling the functional lower bound method which is a reduction from algebraic circuit lower bounds to proof complexity lower bounds introduced in [FSTW21], which holds some resemblance to the well-known feasible interpolation lower bound technique in proof complexity [BPR97, Kra97].

We denote by $\overline{x}^2 - \overline{x}$ the set of Boolean axioms $\{x_i^2 - x_i : i \in [|\overline{x}|]\}$.

Theorem 1 (Functional Lower Bound Method; Lemma 5.2 in [FSTW21])**.** *Let $\mathcal{C} \subseteq \mathbb{F}[\overline{x}]$ be a circuit class closed under (partial) field-element assignments (which stands for the class of "polynomials with small circuits"). Let $f(\overline{x}) \in \mathcal{C}$ be a polynomial, where the collection of polynomials $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ is unsatisfiable (i.e., does not have a common root). A **functional lower bound against** $\mathcal{C}$-IPS$_{\text{LIN}'}$ **for** $f(\overline{x})$ **and** $\overline{x}^2 - \overline{x}$ is a lower bound argument using the following circuit lower bound for $\frac{1}{f(\overline{x})}$: Suppose that $g \notin \mathcal{C}$ for all $g \in \mathbb{F}[\overline{x}]$ with*

$$g(\overline{x}) = \frac{1}{f(\overline{x})}, \quad \forall \overline{x} \in \{0,1\}^n . \tag{1.1}$$

Then, $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ do not have $\mathcal{C}$-IPS$_{\text{LIN}'}$ refutations. Moreover, if $\mathcal{C}$ is a set of multilinear polynomials, then, $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ do not have $\mathcal{C}$-IPS refutations.

The idea behind this theorem is simple. Let

$$g(\overline{x}) \cdot f(\overline{x}) + \sum_i h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1$$

be a $\mathcal{C}$-IPS$_{\text{LIN}'}$ refutation of $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$, for some g, h_i's. Then, since the Boolean axioms nullify over the Boolean cube, Equation (1.1) holds for g (note that $1/f$ is defined over the Boolean cube because f is unsatisfiable, meaning it does not have a 0-1 root). Hence, since $g \notin \mathcal{C}$ for all g for which Equation (1.1) holds, we get the $\mathcal{C}$-IPS$_{\text{LIN}'}$ lower bound.

The method is called "functional" lower bound, since the algebraic circuit lower bounds are functional, namely apply to the *family of all polynomials* that compute the function $1/f$ over the Boolean cube (in contrast with the usual "syntactic" view of algebraic lower bounds which hold for a specific single polynomial defined as a vector of monomials). We refer the reader to the work of Forbes, Kumar, and Saptharishi [FKS16] which investigated functional lower bounds in algebraic circuit complexity.

1.3 Our Results and Techniques

Summary and Organisation

- Past results on algebraic proofs established degree lower bounds for (fully) symmetric instances of *degree only one*, namely subset sum instances of the form $\sum_i x_i - \beta$ (cf. [IPS99, FSTW21]). By making the use of symmetry explicit in these lower bounds, in Section 3.1 we generalise these Nullstellensatz degree lower bounds to symmetric instances of any degree.

- We further show that full symmetry is not necessary to obtain degree lower bounds. In particular, in Section 3.2 we show degree lower bounds against Nullstellensatz refutations for ("partially symmetric") vector invariant polynomials. Since these instances are different from subset sum variants, they are unsatisfiable over both positive and zero characteristics (unlike subset sum, which is unsatisfiable only over large or zero characteristics); and moreover, since we analyse precisely the $n/2$-degree slice of Nullstellensatz refutations of these instances, we are able to demonstrate degree lower bounds for these instances over every field, including over finite fields.

- We show how to lift our new degree lower bounds to *size* lower bounds against different fragments of IPS in Section 4.1 and Section 5. We use a more involved lifting on subset sum degree bounds to establish new size lower bounds against $O(\log\log n)$ individual degree IPS refutations of constant-depth in Section 6

- Finally, in Section 7 we show that the Functional Lower Bound approach alone cannot lead to lower bounds against Frege proof systems such as $\mathrm{AC}^0[p]$-Frege and TC^0-Frege.

Notation. Let $\mathbb{N}' := \mathbb{N}\cup\{0\}$. Given n variables $\overline{x} := \{x_1,\ldots,x_n\}$ and a vector $\overline{\alpha}\in\mathbb{N}'^n$, we denote by $\overline{x}^{\overline{\alpha}}$ the monomial $\prod_{i=1}^n x_i^{\alpha_i}$. Using this notation we have $\deg(\overline{x}^{\overline{\alpha}}) = \sum_{i\in[n]}\alpha_i$, denoting the *total degree* of $\overline{x}^{\overline{\alpha}}$. Given a filed $\mathbb{F}$, a polynomial in $\mathbb{F}[\overline{x}]$ is a linear combination of monomials. The *degree* of a polynomial (also called *the total degree*) is the maximal total degree of its (nonzero) monomials. The *individual degree* of a variable in a polynomial is the maximal power of the variable across all monomials in the polynomial. The individual degree of a polynomial is the maximal individual degree of a variable across all variables in the polynomial.

Given a polynomial $f(\overline{x})\in\mathbb{F}[\overline{x}]$ we say that $f(\overline{x})$ **is symmetric** if $f(\overline{x})$ is invariant (i.e., stays the same) under permutation of all the variables:

$$f(\overline{x}) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)}),$$

for every $\sigma\in S_n$, where S_n is the group of permutations over n element. The **elementary symmetric polynomial of degree** $0\le d\le n$ over the n variables $\overline{x}$ is defined as $\mathbf{e}_{d,n}(\overline{x}) := \sum_{\overline{\alpha}\in\binom{n}{d}}\overline{x}^{\overline{\alpha}}$, where for the sake of convenience we set $\mathbf{e}_{0,n}(\overline{x}) := 1$.

1.3.1 Nullstellensatz Degree Lower Bounds

We show two new Nullstellensatz degree lower bounds, which are later lifted to IPS size lower bounds.

Symmetric Instances. First we establish hardness for any symmetric polynomial.

Corollary (see Cor. 27; Single unsatisfiable symmetric polynomials require high degree refutations)**.** *Assume that $n\ge 1$ and $1\le d\le n$, $\mathbb{F}$ is a field of characteristic strictly greater than $\max(2^n, n^d)$, and $f(\overline{x})$ is a symmetric polynomial of degree d such that $f(\overline{x})-\beta$ has no 0-1 solution, for $\beta\in\mathbb{F}$. Suppose that g is a multilinear polynomial such that*

$$g(\overline{x})\cdot(f(\overline{x})-\beta) = 1 \mod \overline{x}^2-\overline{x}.$$

Then, the degree of $g(\overline{x})$ is at least $n-d+1$. Accordingly, the degree of every Nullstellensatz refutation of $f(\overline{x})-\beta$ is at least $n+1$.

Note indeed that the statement of the corollary gives a Nullstellensatz degree lower bound because a Nullstellensatz refutation of $f(\overline{x})-\beta$ looks like $g(\overline{x})\cdot(f(\overline{x})-\beta)+\sum_i h_i\cdot(x_i^2-x_i)=1$. Recall also that taking a polynomial modulo the Boolean axioms $\overline{x}^2-\overline{x}$, is the same as multilinearizing the polynomial.

The following claim is the main technical observation behind the degree lower bound and is a generalisation of the [FSTW21] lower bounds for the case of linear symmetric polynomials, i.e., when $d=1$. Intuitively, the idea is that the multilinearization of the product $(\mathbf{e}_{d,n}(\overline{x})-\beta)\cdot\mathbf{e}_{k,n}(\overline{x})$ contains nonzero monomials of degree ≥ 1 given that $d+k\leq n$, hence it cannot equal the polynomial 1. (Note that when $d+k>n$ we cannot make sure that this product when we multiply out terms, does not yield cancellations of monomials resulting potentially in the 1 polynomial.)

Claim (see Claim 26; Multilinearizing the product of elementary symmetric polynomials yields high degree)**.** *Let $n\geq 1$ and $1\leq d\leq n$. If k is such that $k\leq n-d$, then*

$$\mathbf{e}_{d,n}(\overline{x})\cdot\mathbf{e}_{k,n}(\overline{x})=2^{d+k}\cdot\mathbf{e}_{d+k,n}(\overline{x})+[\textit{degree}\leq d+k-1\ \textit{terms}]\mod \overline{x}^2-\overline{x}\,.$$

Using this claim and the fact that every symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials, we conclude the Nullstellensatz lower bounds for symmetric polynomials.

Vector Invariant Polynomials. We provide degree lower bounds for instances that are different from subset sum variant (this means formally that they are not a substitution instance of $\sum_{i=1}^n x_i$, for $n=\omega(1)$). Later we show how to lift those to size lower bounds. These instances are interesting because they are different from previous IPS hard instances which were all based on the subset sum, and they hold over finite fields as well.

Our hard instances are inspired by ideas from *invariant theory* and specifically vector invariants. Roughly speaking, an invariant polynomial in the variables $\overline{x}$ is a polynomial that stays the same when each variable x_i is replaced by the ith element of the vector $A\overline{x}$, for A a matrix taken from a matrix group. We provide some general information from invariant theory in Section 3.2. We consider a class of invariant polynomials known as *vector invariants*, which is a well-studied class of invariant polynomials [Ric90, CH97, DK15]

Let $\overline{x}:=\{x_1,x_2,\ldots,x_{2n}\}$ and $\overline{y}:=\{y_1,y_2,\ldots,y_{2n}\}$ be commuting variables over a field $\mathbb{F}$ of characteristic greater than 3 (for size lower bounds we would need $\mathrm{char}(\mathbb{F})\geq 5$). Let

$$\widetilde{Q}(\overline{x},\overline{y}):=\left(\prod_{i\in[2n],\ i\text{: odd}}(x_iy_{i+1}-y_ix_{i+1})\right).$$

The hard instance is defined as

$$Q(\overline{x},\overline{y}):=\widetilde{Q}(\overline{x},\overline{y})-\beta \tag{1.2}$$

where $\beta\in\mathbb{F}$ and $\beta\notin\{-1,0,1\}$.

We use several interesting properties of this polynomial to prove the lower bound (see Fact 28). Specifically, the polynomial is invariant under the following action: for every odd $i\in[2n]$ (it is sufficient for the present work to think of actions, denoted $\hookrightarrow$, as substitutions of variables by polynomials)

$$x_i\hookrightarrow x_i\qquad x_{i+1}\hookrightarrow x_{i+1}\qquad y_i\hookrightarrow x_i+y_i\qquad y_{i+1}\hookrightarrow x_{i+1}+y_{i+1}\,. \tag{1.3}$$

For $i\in[2n]$ and i odd, let $a_i:=(x_iy_{i+1}-y_ix_{i+1})$. Then, a_i is the determinant of the matrix $M_i=\begin{pmatrix}x_i & x_{i+1}\\ y_i & y_{i+1}\end{pmatrix}$. Moreover, $a_i\in\{-1,0,1\}$ over the Boolean cube. Note that $\widetilde{Q}(\overline{x},\overline{y})-\beta=0$ is unsatisfiable when $\beta\notin\{-1,0,1\}$.

Theorem (see Thm. 32; Nullstellensatz degree lower bounds for invariant instances)**.** *Let* $\mathbb{F}$ *be any field of characteristic at least* 3 *and let* $\beta \notin \{-1, 0, 1\}$*. Then,* $Q(\overline{x}, \overline{y}) = 0$*,* $\{x_i^2 - x_i = 0\}_i$*, and* $\{y_i^2 - y_i = 0\}_i$ *are unsatisfiable and any polynomial* $f(\overline{x}, \overline{y})$ *such that* $f(\overline{x}, \overline{y}) = 1/Q(\overline{x}, \overline{y})$*, for* $\overline{x} \in \{0,1\}^{2n}$ *and* $\overline{y} \in \{0,1\}^{2n}$*, has degree at least* $2n$*.*

Note indeed that the statement of the theorem gives a Nullstellensatz degree lower bound because a Nullstellensatz refutation of $\widetilde{Q}(\overline{x}, \overline{y}) - \beta$ looks like $f(\overline{x}, \overline{z}) \cdot (\widetilde{Q}(\overline{x}, \overline{z}) - \beta) + \sum_i h_i \cdot (x_i^2 - x_i) + \sum_i h'_i \cdot (y_i^2 - y_i) = 1$, meaning that $f(\overline{x}, \overline{z}) = 1/Q(\overline{x}, \overline{z})$ over the Boolean cube.

We show in Section 5.1 and Section 5.2 that the invariant theoretic properties specified in Equation (1.3) facilitate a complete understanding of the coefficient space pertaining to the homogeneous degree $2n$-slice of any refutation of $Q(\overline{x}, \overline{y})$.

1.3.2 Lifting Degree to Size Lower Bounds

The idea of "lifting" usually refers to the notion of taking a hard instance against a specific computational (or proof) model and altering the instance to make it hard even for a *stronger* computational (or proof) model (see the recent survey by de Rezende, Göös and Robere [dRGR22] for a discussion on the use of lifting in proof complexity and references therein). Standard lifting usually proceeds by taking a substitution instance of the original hard instance. In this case the substitution is defined according to a "gadget", which is a specific function or polynomial, applied separately on each of the variables. For example, $f(z_1, \ldots, z_n) \mapsto f(x_1 y_1, \ldots, x_n y_n)$, in which the gadget is defined as $z_i \mapsto x_i y_i$, for all $i \in [n]$.

The idea to use lifting to turn a hard instance against Nullstellensatz *degree* to a hard instance against $\mathcal{C}$-IPS *size* was introduced in [FSTW21]. The gadgets used in [FSTW21] were quite simple. Here we show that our new hard instances against Nullstellensatz degree can be lifted with similar gadgets to our IPS fragments of interest. In [GHT22] the gadget is more involved, and we show how to carry it over to the new setting of Amireddy *et al.* [AGK+23] to gain lower bounds against a stronger fragment of constant depth IPS refutations.

Using Lifting against IPS. Let us consider how lifting is used to yield size lower bounds. Recall that in the functional lower bound method, we reduced the task of lower bounding the size of a $\mathcal{C}$-IPS refutation of $f(\overline{x}) = 0$ into the task of lower bounding the size of an algebraic circuit from the class $\mathcal{C}$ that computes the function $g(\overline{x}) = 1/f(\overline{x})$ over the Boolean cube. To establish an algebraic circuit lower bound we usually need to lower bound the rank of a certain matrix denoted $\mathbf{Coeff}_{\overline{u}|\overline{v}}(g)$ corresponding to the coefficient matrix of the polynomial g under a partition of the variables $\overline{x} = (\overline{u}, \overline{v})$. In such a coefficient matrix, the (M, N) entry is the coefficient in g of the monomial $M \cdot N$, with M a monomial in the $\overline{u}$-variables and N a monomial in the $\overline{v}$-variables.

Note however that in our case g is not a polynomial, rather a *family* of many polynomials all of which compute the *function* $1/f(\overline{x})$ over the Boolean cube. To prove such a lower bound on a family of polynomials, [FSTW21] used an alternative rank argument: the *evaluation dimension* (as suggested by Saptharishi [Sap12]; cf. [FKS16]), which for us will be defined as the dimension of the following space of polynomials under partial assignments $\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$. For the most part, we also use evaluation dimension (except for the vector invariant polynomials in which our analysis is tighter). It is not hard to show (Lemma 17) that evaluation dimension is a lower bound on the rank of $\mathbf{Coeff}_{\overline{u}|\overline{v}}(g)$. We are thus left with the task of lower bounding $\dim\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$. This is where we need lifting. Specifically, we need to maintain two main properties:

1. We need to *substitute* the original variables $\overline{x}$ of our polynomial g (and accordingly f) with gadgets, resulting in a new polynomial equipped with a natural partition of variables $\overline{u}, \overline{v}$ that would provide high dimension to $\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$.
2. $g(\overline{u}, \overline{\alpha})$, for $\overline{\alpha} \in \{0,1\}^{|\overline{v}|}$, reduces to our *original* instance $g(\overline{x})$ (possibly at a smaller input length).

The gist behind the two properties is this: to lower bound $\dim\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$ we use Item 2. This allows us to use our original Nullstellensatz refutation degree lower bound on each element of the set $\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$. Using such a degree lower bound on $g(\overline{u}, \overline{\alpha})$ for distinct assignments $\overline{\alpha} \in \{0,1\}^{|\overline{v}|}$ we can "isolate" enough distinct leading monomials (per some global fixed monomial ordering). By a known result, the number of distinct leading monomials in a space of polynomials is a lower bound on its dimension. Hence, we conclude the evaluation dimension lower bound (and the circuit lower bound).

Symmetric Instances under Lifting. We show lower bounds against $\mathcal{C}$-IPS$_{\text{LIN}'}$ of any symmetric polynomial under lifting, where $\mathcal{C}$ is the class of read once (oblivious) algebraic branching programs (roABPs). Accordingly, we denote this system by roABP-IPS$_{\text{LIN}'}$ (see Definition 9 for the definition of roABP). The lifting is defined by replacing the elementary symmetric polynomials with elementary symmetric polynomials with a bigger number of variables and then applying the gadget to each variable.

More precisely, given a symmetric polynomial $f(\overline{q})$ with n variables $q_1, \ldots, q_n$, by the fundamental theorem of symmetric polynomials (Proposition 6), it can be written as a polynomial in the elementary symmetric polynomials: $f(\overline{q}) := h(y_1/\mathbf{e}_{1,n}(\overline{q}), \ldots, y_n/\mathbf{e}_{n,n}(\overline{q}))$ for some polynomial $h(\overline{y})$. Consider the polynomial $f'(\overline{w}) := h(y_1/\mathbf{e}_{1,m}(\overline{w}), \ldots, y_n/\mathbf{e}_{n,m}(\overline{w}))$ for $m = \binom{2n}{2}$ and $\overline{w} = \{w_{i,j}\}_{i<j\in[2n]}$. We now apply a similar gadget to [FSTW21], defined by the mapping

$$w_{i,j} \mapsto z_{i,j} x_i x_j \,,$$

which substitutes the m variable $w_{i,j}$ by $m + 2n$ variables $\{z_{i,j}\}_{i<j\in[2n]}$, $x_1, \ldots, x_{2n}$:

$$f^\star(\overline{z}, \overline{x}) := h(y_1/(\mathbf{e}_{1,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}, \ldots, y_n/(\mathbf{e}_{n,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}) \,, \tag{1.4}$$

where $(\mathbf{e}_{j,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}$ means that we apply the lifting $w_{i,j} \mapsto z_{i,j}x_ix_j$ to the $\overline{w}$ variables.

Note that when we use lifting to change the variables in an instance, we also *add the Boolean axioms for each of the new variables.*

Corollary (Symmetric instances are hard for roABP-IPS$_{\text{LIN}'}$; see Cor. 38)**.** *Let $n \geq 1$, $m = \binom{n}{2}$, and $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) > \max(2^{4n+2m}, n^d)$. Let $f \in \mathbb{F}[\overline{q}]$ be a symmetric polynomial with n variables of degree $d = O(\log n)$, and $f^\star(\overline{z}, \overline{x})$ be as in Equation (1.4). Let $\beta \in \mathbb{F}$ be such that $f^\star(\overline{z}, \overline{x}) - \beta = 0$ and $f(\overline{q}) - \beta = 0$ are each unsatisfiable over Boolean values. Then, any* roABP-IPS$_{\text{LIN}'}$ *refutation (in any variable order) of $f^\star(\overline{z}, \overline{x}) - \beta = 0$ (together with the Boolean axioms to the $\overline{x}$- and $\overline{z}$-variables) requires $2^{\Omega(n)}$-size.*

The new idea we employ in this result is showing how to maintain Item 2 of the lifting scheme above, even in the *absence of maximal degree lower bounds* for the original hard polynomial $g(\overline{x})$ in that scheme. While in [FSTW21, see remark after Proposition 5.8] a maximal n lower bound on $g(\overline{x})$ was thought to be necessary to the dimension lower bound, we show that we can lower bound $\dim\{g(\overline{u}, \overline{\alpha}) : \overline{\alpha} \in \{0,1\}^{|\overline{v}|}\}$ with only an $\Omega(n)$ Nullstellensatz degree lower bound for $g(\overline{x})$ (n is the number of variables in $\overline{x}$). Recall that general symmetric polynomials have only

$\Omega(n)$ Nullstellensatz degree lower bounds according to Corollary 27 (for low enough symmetric polynomials). (This, on the other hand, will mean that we do not get size lower bounds for formula multilinear IPS refutations (as in [FSTW21]), since the results of Raz-Yehudayoff (Theorem 20) require full rank 2^n lower bounds, while the dimension lower bound we get is only $2^{\Omega(n)}$).

Invariant Instances under Lifting. We show how to lift the vector invariant polynomials hard against Nullstellensatz degree $Q(\overline{x},\overline{y})$ from Section 1.3.1 (Equation (1.2)), to hard instances against IPS refutation-size, where refutations are written as roABPs and multilinear formulas, respectively.

Let $\overline{u}=\{u_1,u_2,\ldots,u_{4n}\}$, let $m=\binom{4n}{4}$, and $\overline{z}=\{z_1,z_2,\ldots,z_m\}$. The hard instance $P(\overline{u},\overline{z})\in\mathbb{F}[\overline{u},\overline{z}]$ is defined by:

$$P(\overline{u},\overline{z}):=\left(\prod_{i<j<k<\ell\in[4n]} 1-z_{i,j,k,\ell}+z_{i,j,k,\ell}(u_iu_\ell-u_ju_k)\right)-\beta\,.$$

We show the following roABP-IPS$_{\text{LIN}'}$ and multilinear-formula-IPS$_{\text{LIN}'}$ lower bounds. Here, multilinear-formula-IPS$_{\text{LIN}'}$ denotes $\mathcal{C}$-IPS where $\mathcal{C}$ is the class of multilinear formulas, and we note that multilinear-formula-IPS$_{\text{LIN}'}$ is equivalent to full multilinear-formulas-IPS ([FSTW21]).

Theorem (see Thm. 41)**.** *Let $\mathbb{F}$ be a field of characteristic ≥ 5 and let $P(\overline{u},\overline{z})$ be as defined above. Then $P(\overline{u},\overline{z}),\{u_i^2-u_i\}_i,\{z_i^2-z_i\}_i$ is unsatisfiable as long as $\beta\notin\{-1,0,1\}$. And any* roABP-IPS$_{\text{LIN}'}$ *refutation of $P(\overline{u},\overline{z}),\{u_i^2-u_i\}_i,\{z_i^2-z_i\}_i$ requires $\exp(\Omega(n))$ size. Moreover, any multilinear-formula-IPS refutation requires $n^{\Omega(\log n)}$ size and any product-depth-Δ multilinear-formula-IPS requires size $n^{\Omega((n/\log n)^{1/\Delta}/\Delta^2)}$.*

This is the first IPS fragment lower bound over finite fields, solving an open problem in [PT16, GHT22]. Previous IPS fragment lower bounds were all using variants of the subset sum $\sum_{i=1}^n x_i-\beta=0$ as hard instances. They crucially used the fact that the field has large characteristic so that the instance first is indeed unsatisfiable (note that over characteristic at most n it is satisfiable over Boolean values), and second the degree lower bound can be carried through (see the proof of Lemma 25, paragraph before Claim 26 for an explanation).

Note that these lower bounds are in the placeholder IPS regime because the hard instances themselves do not have small roABPs and multilinear formulas.

Proof Overview. The starting point for this lower bound proof is the Nullstellensatz degree lower bound for $Q(\overline{x},\overline{y})$. The degree lower bound establishes that $f(\overline{x},\overline{y})$, namely the polynomial that agrees with $1/Q(\overline{x},\overline{y})$ over the Boolean cube, has a degree at least $2n$ (as stated in Theorem 32; see Section 1.3.1). Here, we further refine this statement. We completely characterise the homogeneous degree-$2n$ slice of the polynomial $f(\overline{x},\overline{y})$. Specifically, we show that any monomial of degree $2n$ in $f(\overline{x},\overline{y})$ has coefficient either $\frac{1}{\beta(1-\beta)}$ or $\frac{1}{\beta(1+\beta)}$. This allows us to give a lower bound on the coefficient space of the polynomial $f(\overline{x},\overline{y})$ under any order in which $\overline{x}<\overline{y}$. Here, we use the invariant properties of the polynomial $Q(\overline{x},\overline{y})$ crucially. We observe that if $Q(\overline{x},\overline{y})$ is invariant under a certain action, then so is the refutation (i.e., the polynomial $f(\overline{x},\overline{y})$).

To obtain a lower bound in any order (not just when $\overline{x}<\overline{y}$), we build further on the above. For this, we use a lifted version of $Q(\overline{x},\overline{y})$ (this is a different lifting than for the symmetric instances size lower bounds), namely the polynomial $P(\overline{u},\overline{z})$ mentioned above. Let $g(\overline{u},\overline{z})$ be the polynomial that agrees with $1/P(\overline{u},\overline{z})$ over the Boolean cube. We interpret $g(\overline{u},\overline{z})$ over $\mathbb{F}[\overline{z}][\overline{u}]$. And observe that for every partition of the variables $\overline{u}$ into equal parts, say $\overline{v},\overline{w}$, there exists a 0-1 assignment to the $\overline{z}$ variables, such that it recovers an instance of $f(\overline{v},\overline{w})$. This corresponds to Item 2 in the

conditions used in the lifting scheme above. Accordingly, using this condition allows us to prove lower bounds on the coefficient dimensions for any partition of variables.

Interestingly, the fact that our lower bound works for *all orders* of $\overline{u}$ variables, allows us to prove a functional lower bound for multilinear *formulas*. Formally, we get the following corollary as a byproduct of the above theorem.

Corollary 2 (New functional *formula* lower bound)**.** *Let $P(\overline{u},\overline{z})$ be as defined above. Let $g(\overline{u},\overline{z})$ be a polynomial that agrees with $1/P(\overline{u},\overline{z})$ over the Boolean cube. Then, any multilinear formula that agrees with $g(\overline{u},\overline{z})$ over the Boolean cube must have size* $\exp(\Omega(n))$.

Previously, functional lower bounds were known for the roABP model due to [FKS16]. In their case, the hard polynomial was in VNP. Above, our hard polynomial is $g(\overline{u},\overline{z})$. We suspect that the same functional lower bound as stated in Corollary 2 can also be proved for $P(\overline{u},\overline{z})$. If this is true, then we get a polynomial computable by a product-depth-2 circuits for which we have an exponential functional lower bound. This is likely to be of independent interest.

Extended Constant-Depth Lower Bounds. Using Limaye, Srinivasan, and Tavenas [LST21] constant-depth circuit lower bounds, Govindasamy, Hakoniemi, and Tzameret [GHT22] established constant-depth IPS lower bounds against a lifted subset sum. The lifting in [GHT22] was rather involved to fit the "lopsided" rank measure introduced by [LST21]. In [GHT22], the lower bound was not tight and it applied only to IPS refutations computable by *multilinear* polynomials.

We show how to use recent progress on constant-depth lower bounds by Amireddy, Garg, Kayal, Saha, and Thankey [AGK+23] to achieve tighter lower bounds for constant-depth IPS refutations, while also extending [GHT22] lower bounds to constant-depth IPS refutations computing polynomials of $O(\log\log n)$-individual degrees.

Theorem (Constant-depth IPS lower bounds; See Thm. 44)**.** *Let n,Δ and δ be positive integers, and assume that $\mathbb{F}$ is a field with* $\mathrm{char}(\mathbb{F})=0$*, and $\beta\in\mathbb{F}$.*[1] *Let g be a polynomial of individual degree at most δ such that it agrees with*

$$\frac{1}{\sum_{i,j,k,\ell\in[n]} z_{ijk\ell}x_ix_jx_kx_\ell-\beta} \quad \textit{over Boolean values.}$$

Then, any circuit of product-depth at most Δ computing g has size at least

$$\Omega\left(n^{\frac{(\log n)^{2^{1-2\Delta}}}{\delta^{2\cdot\Delta}}}\right).$$

Note that by the functional lower bound scheme above, this result gives immediately a constant-depth individual degree-δ IPS size lower bounds for $\sum_{i,j,k,\ell\in[n]} z_{ijk\ell}x_ix_jx_kx_\ell-\beta$ (whenever $\beta\in\mathbb{F}$ makes this polynomial unsatisfiable, namely, nonzero, over the Boolean cube).

Note that while [GHT22] established a similar size lower bound for the *unique multilinear* polynomial computing $1/\sum_{i,j,k,\ell\in[n]} z_{ijk\ell}x_ix_jx_kx_\ell-\beta$ over the Boolean cube, Theorem 44 establish this lower bound for the *family* of polynomials whose individual degree is δ, computing this polynomial over the Boolean cube.

This solves the question raised in [AGK+23] about the ability to use their framework to obtain functional lower bounds for low-depth algebraic formulas in a direct manner without hardness-escalation via set-multilinear formulas.[2] Specifically, in [LST21], the constant-depth circuit lower

[1] The lower bound also holds for fields of large enough characteristic that depends on the number of variables.

[2] [AGK+23] reads: "*Furthermore, it is conceivable that a direct argument can also be used to obtain functional lower bounds for low-depth formulas which might be useful in proof complexity.*"

bound is first proved for a restricted setting of *set-multilinear* constant-depth circuits. This is then *escalated* to first obtain homogeneous constant-depth circuit lower bounds and in turn this is escalated further to obtain general constant-depth circuit lower bounds. On the other hand, [AGK+23] show a lower bound for the homogeneous constant-depth circuits directly, thereby bypassing the need for proving set-multilinear lower bounds. A natural question arose from this development: can the techniques used in [GHT22] be extended using the ideas in [AGK+23] to get stronger proof complexity lower bounds for constant-depth IPS proofs? We answer this question affirmatively.

We briefly discuss the proof of this lower bound and what is new in it. [AGK+23] showed how to circumvent the use of set-multilinear polynomials in [LST21]. In doing so it also puts leaner requirements for the hard-instances, when the work of [LST21] required their hard instances to be set-multilinear. For [GHT22], this meant that in order to use constant-depth algebraic circuit lower bounds they needed to show that any constant-depth IPS proof embeds in some sense a hard set-multilinear polynomial. To embed set-multilinear polynomials in any proof, [GHT22] needed to stick to IPS refutations that compute multilinear polynomials only. Otherwise, if the IPS proofs themselves are not multilinear their set-multilinear projection (namely, the set-multilinear polynomials they "embed") could be zero, regardless of their functional behaviour over the Boolean cube (one can use multilinearization on the proofs, but there is no guarantee that this operation increases the evaluation dimension, meaning that a lower bound on multilinear proofs is achieved that may not hold for non-multilinear proofs).

In the circuit lower bound, [AGK+23] use a measure, introduced in [GKS20], called *Affine Projections of Partials* (APP). They analyse this measure and prove that lower bounds for this measure are enough to prove a superpolynomial lower bound for constant-depth homogeneous circuits. We benefit from their analysis to be able to extend the lower bounds from [GHT22]. Specifically, we are able to lower bound the APP measure for arbitrary IPS refutations (perhaps even highly non-multilinear) of our hard instance. From these lower bounds on the measure we are able to infer constant-depth lower bounds for refutations of bounded individual degree.

At the technical level, this gives two kinds of improvements. First, we are able to analyse more general class of proofs and prove lower bounds for them. And second, we are able to modify the framework of [AGK+23] in order to use it for functional lower bounds.

1.3.3 Barriers for Boolean Instances Lower bounds

Lower bounds against $\mathrm{AC}^0[p]$-Frege proofs stand as one of the most elusive lower bound questions in proof complexity, open for more than three decades, while still considered within reach using current techniques (especially, due to the known $\mathrm{AC}^0[p]$ circuit lower bounds). In light of the simulation of $\mathrm{AC}^0[p]$-Frege by constant-depth IPS refutations over $\mathbb{F}_p$ shown in [GP18], it is promising to think of using algebraic circuit lower bounds in the framework of IPS to solve this open problem. We show that at least when it comes to the functional lower bound method (as defined precisely in general in Definition 62), this goal is impossible to achieve.

When we attempt to prove a lower bound against a propositional proof system operating with Boolean formulas (such as $\mathrm{AC}^0[p]$-Frege) by way of algebraic proofs lower bounds, we need to focus on hard instances against the algebraic proof systems that are nevertheless Boolean. We say that an instance consisting of a set of polynomials $\{f_i(\overline{x}) = 0\}_i$, for $f_i(\overline{x}) \in \mathbb{F}[\overline{x}]$, is *Boolean* whenever $f_i(\overline{x}) \in \{0,1\}$ for $\overline{x} \in \{0,1\}^{|\overline{x}|}$. For example, a CNF written as a set of (polynomials representing) clauses is a Boolean instance. Similarly, the standard arithmetization of propositional formulas is Boolean instances. Note that up to this point, we discussed only *non*-Boolean hard instances. For example, the subset sum $\sum_i x_i - \beta$ is highly non-Boolean due to its image under $\{0,1\}$-assignments being $\{-\beta, 1-\beta, \ldots, n-\beta\}$. The vector invariant polynomial instances are also non-Boolean

because their image under Boolean assignments is $\{-1, 0, 1\}$. Similarly, previous hard instances against fragments of IPS are all non-Boolean.

Theorem (Main barrier; see Thm. 64)**.** *The functional lower bound method cannot establish lower bounds for any* Boolean *instance against sufficiently strong proof systems. In particular, it cannot establish any lower bounds against* $\mathrm{AC}^0[p]$*-Frege,* TC^0*-Frege (and constant-depth* $\mathrm{IPS}_{\mathrm{LIN}'}$ *when the hard instances are Boolean).*

Here, a *sufficiently strong proof system* (see Definition 63 for the precise definition) means a proof system that basically has the AND introduction rule, in the sense that from $\phi_1, \ldots, \phi_n$ one can efficiently derive $\bigwedge_i \phi_i$. Most reasonably strong proof systems such as $\mathrm{AC}^0[p]$-Frege and TC^0-Frege clearly have this property.

To understand this result, first, we need to understand how to potentially use the functional lower bound method for Boolean instances. For the sake of simplicity, let us discuss the case where the proof system we try to prove lower bounds against is $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$ for some algebraic circuit class $\mathcal{C}$ (in Section 7 we discuss the general case of any proof system including strictly propositional ones like $\mathrm{AC}^0[p]$-Frege).

Let $\mathcal{F} := \{f_i(\overline{x}) = 0\}_i$ be a collection of *Boolean* polynomial equations in $\mathcal{C}$, in the above sense, and suppose we wish to establish a lower bound for $\mathcal{F}$ against $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$ using the functional lower bound method. For this purpose, we prove a lower bound for $f(\overline{x}) = 0$ against $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$, using the functional lower bound method. We then need to show that there is a short $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$-proof of $\mathcal{F}$ from $f(\overline{x}) = 0$ (and $\overline{x}^2 - \overline{x}$) (it is possible that $\mathcal{F}$ is equal to $\{f(\overline{x}) = 0\}$). Then, we can conclude there is no $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$-refutations of $\mathcal{F}$ (otherwise, starting from $f(\overline{x}) = 0$, we can efficiently derive $\mathcal{F}$ and refute $f(\overline{x}) = 0$ in contradiction to the assumption that $f(\overline{x}) = 0$ is hard for $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$).

The idea behind the barrier is as follows: if $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$ is sufficiently strong we can efficiently derive the arithmetization of $\bigwedge_i f_i(\overline{x})$ in $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$ (for example, it can be written as $1 - \prod_i (1 - f_i(\overline{x}))$). The negation $\prod_i (1 - f_i(\overline{x}))$ of this single polynomial is a tautology, namely it is always zero over the Boolean cube, and hence is in the ideal generated by the Boolean axioms $\{x_j^2 - x_j\}_j$. Thus, $\mathcal{F}$ can be refuted using only the Boolean axioms (though not necessarily efficiently). From this, it is not hard to show that there is no functional lower bound against the function $g(\overline{x}) = \frac{1}{f(\overline{x})}, \quad \forall \overline{x} \in \{0,1\}^n$ (as in Equation (1.1) in the Functional Lower Bound Method Theorem 1).

It is interesting to note that recently Grochow [Gro23] showed that even a low-depth IPS fragment constitutes a sufficiently strong proof system in our sense.

We also note that the barrier is not sensitive to a specific arithmetization scheme, as long as it translates Boolean formulas to a polynomial that computes the same Boolean function over the Boolean cube (where possibly 1 is flipped with 0; see Section 7).

2 Preliminaries

2.1 Notation

For a natural number $n \in \mathbb{N}$, $[n] := \{1, \ldots, n\}$. We assume that $0 \in \mathbb{N}$. We call $\{0,1\}^n$ the *Boolean cube*.

Let $\mathbb{G}$ be a ring (we usually work with sufficiently large fields denoted $\mathbb{F}$ or fields of zero characteristic, and this is specified when important). Denote by $\mathbb{G}[\overline{x}]$ the ring of (commutative) polynomials with coefficients from $\mathbb{G}$ and variables $\overline{x} := \{x_1, x_2, \ldots\}$. A *polynomial* is a formal linear combination of monomials, whereas a *monomial* is a product of variables. Two polynomials are *identical* if all their monomials have the same coefficients. The (total) degree of a monomial is the sum of all the powers of variables in it. The (total) *degree* of a polynomial is the maximal total

degree of a monomial in it. The degree of an *individual* variable in a monomial is its power. The *individual degree* of a monomial is the maximal individual degree of its variables. The individual degree of a polynomial f, denoted $\operatorname{ideg} f$, is the maximal individual degree of its monomials. For a polynomial f in $\mathbb{G}[\overline{x}, \overline{y}]$ with $\overline{x}, \overline{y}$ being pairwise disjoint sets of variables, the *individual $\overline{y}$-degree* of f is the maximal individual degree of a $\overline{y}$-variable only in f.

Given n variables $\overline{x}$ and a vector $\overline{\alpha} \in \mathbb{N}^n$ we denote by $\overline{x}^{\overline{\alpha}}$ the monomial $\prod_{i=1}^{n} x_i^{\alpha_i}$. Using this notation we have $\deg(\overline{x}^{\overline{\alpha}}) = \sum_{i \in [n]} \alpha_i$, denoting the *total degree* of $\overline{x}^{\overline{\alpha}}$. Denote by $\operatorname{Coeff}_{\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}}(f)$ the coefficient of $\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}$ in f.

We say that a polynomial is *homogeneous* whenever every monomial in it has the same (total) degree. For a polynomial $f(\overline{x})$, the *degree-d homogeneous slice of $f(\overline{x})$* (degree-d slice, for short) is a polynomial defined by the degree d monomials of $f(\overline{x})$. We say that a polynomial is *multilinear* whenever the individual degrees of each of its variables are at most 1.

For two polynomials $g(\overline{y}), h(\overline{x})$ We denote by $g(y_i/h(\overline{x}))$ the *substitution* in $g(\overline{y})$ of the variable $y_i \in \overline{y}$ by the polynomial $h(\overline{x})$.

2.2 Algebraic Circuits

Algebraic circuits and formulas over the ring $\mathbb{G}$ compute polynomials in $\mathbb{G}[\overline{x}]$ via addition and multiplication gates, starting from the input variables and constants from the ring. More precisely, an *algebraic circuit* C is a finite directed acyclic graph (DAG) with *input nodes* (i.e., nodes of in-degree zero) and a single *output node* (i.e., a node of out-degree zero). Edges are labelled by ring $\mathbb{G}$ elements. Input nodes are labelled with variables or scalars from the underlying ring. In this work (since we work with constant-depth circuits) all other nodes have unbounded *fan-in* (that is, unbounded in-degree) and are labelled by either an addition gate $+$ or a product gate $\times$. Every node in an algebraic circuit C *computes* a polynomial in $\mathbb{G}[\overline{x}]$ as follows: an input node computes the variable or scalar that labels it. A $+$ gate computes the linear combination of all the polynomials computed by its incoming nodes, where the coefficients of the linear combination are determined by the corresponding incoming edge labels. A $\times$ gate computes the product of all the polynomials computed by its incoming nodes (so edge labels in this case are not needed). The polynomial computed by a node u in an algebraic circuit C is denoted $\widehat{u}$. Given a circuit C, we denote by $\widehat{C}$ the polynomial computed by C, that is, the polynomial computed by the output node of C. The ***size*** of a circuit C is the number of nodes in it, denoted $|C|$, and the ***depth*** of a circuit is the length of the longest directed path in it (from an input node to the output node). The ***product-depth*** of the circuit is the maximal number of product gates in a directed path from an input node to the output node. For excellent treatises on algebraic circuits and their complexity see Shpilka and Yehudayoff [SY10] as well as Saptharishi [Sap22].

Let $\overline{X} = \langle X_1, \ldots, X_d \rangle$ be a sequence of pairwise disjoint sets of variables, called *a variable-partition*. We call a monomial m in the variables $\bigcup_{i \in [d]} X_i$ *set-multilinear* over the variable-partition $\overline{X}$ if it contains exactly one variable from each of the sets X_i, i.e. if there are $x_i \in X_i$ for all $i \in [d]$ such that $m = \prod_{i \in [d]} x_i$. A polynomial f is set-multilinear over $\overline{X}$ if it is a linear combination of set-multilinear monomials over $\overline{X}$. For a sequence $\overline{X}$ of sets of variables, we denote by $\mathbb{F}_{\text{sml}}[\overline{X}]$ the space of all polynomials that are set-multilinear over $\overline{X}$.

We say that an algebraic circuit C is set-multilinear over $\overline{X}$ if C computes a polynomial that is set-multilinear over $\overline{X}$, and each internal node of C computes a polynomial that is set-multilinear over some sub-sequence of $\overline{X}$.

2.3 Symmetric Polynomials

We denote by S_n the *permutation group* over n elements. Concretely, an element $\sigma \in S_n$ can be identified with a (permutation) function $\sigma : [n] \to [n]$. Given n variables $\overline{x}$ we denote by $\sigma\overline{x}$ the application of $\sigma \in S_n$ to the variables; namely, their renaming according to σ. In this way, $f(\sigma\overline{x}) \in \mathbb{F}[\overline{x}]$ is the result of renaming in $f \in \mathbb{F}[\overline{x}]$ all the variables $\overline{x}$ according to σ.

Definition 3 (Symmetric polynomial)**.** *Given a polynomial $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ we say that $f(\overline{x})$ **is symmetric** if $f(\overline{x})$ is invariant (i.e., stays the same) under permutation of all the variables:*

$$f(\overline{x}) = f(\sigma\overline{x}), \tag{3.1}$$

for every $\sigma \in S_n$.

We will also consider polynomials that are not fully symmetric, in the sense that they stay the same, i.e. are invariant, under a specific subgroup G, which is not necessarily S_n. In this case we call this polynomial **invariant under** G.

Definition 4 (Elementary symmetric polynomial $\mathbf{e}_{d,n}(\overline{x})$)**.** *The **elementary symmetric polynomial of degree** $0 \leq d \leq n$ over the n variables $\overline{x}$ is defined as follows:*

$$\mathbf{e}_{d,n}(\overline{x}) := \sum_{\overline{\alpha} \in \binom{n}{d}} \overline{x}^{\overline{\alpha}} \,,$$

where for the sake of convenience we set $\mathbf{e}_{0,n}(\overline{x}) := 1$.

Note that $\mathbf{e}_{d,n}(\overline{x})$ is multilinear, and that there is only a *single* homogeneous multilinear symmetric polynomial over n variables $\overline{x}$, up to scalar multiplication:

Fact 5. *If $f \in \mathbb{F}[\overline{x}]$ is a symmetric multilinear and homogeneous polynomial of degree d, then $f(\overline{x}) = \lambda \cdot \mathbf{e}_{d,n}(\overline{x})$, for some $\lambda \in \mathbb{F}$.*

Fact 5 is immediate, because otherwise there was a pair of distinct multilinear monomials of total-degree d, $\overline{x}^{\alpha} \neq \overline{x}^{\alpha'}$, with $\overline{\alpha} \neq \overline{\alpha}' \in \{0, \ldots, n\}^d$ and with different respective coefficients $\lambda \neq \lambda' \in \mathbb{F}$. Then, there is a permutation $\sigma \in S_n$ of the n variables $\overline{x}$ such that $f(\sigma\overline{x})$ contains $\lambda\overline{x}^{\overline{\alpha}'}$ instead of $\lambda'\overline{x}^{\overline{\alpha}'}$, in contradiction to the symmetry of f.

Recall that for two polynomials $g(\overline{y}), h(\overline{x})$ We denote by $g(y_i/h(\overline{x}))$ the **substitution** in $g(\overline{y})$ of the variable $y_i \in \overline{y}$ by the polynomial $h(\overline{x})$.

Proposition 6 (The fundamental theorem of symmetric polynomials)**.** *Every symmetric polynomial $f \in \mathbb{F}[\overline{x}]$ with n variables can be written as a* polynomial *in the elementary symmetric polynomials. That is, there is a $g(\overline{y}) \in \mathbb{F}[\overline{y}]$ such that*

$$f(\overline{x}) = g(y_1/\mathbf{e}_{1,n}(\overline{x}), \ldots, y_n/\mathbf{e}_{n,n}(\overline{x})). \tag{6.1}$$

Moreover, if $f(\overline{x})$ is multilinear then $g(\overline{y})$ is linear, that is, $f(\overline{x})$ can be written as a linear *combination of elementary symmetric polynomials:*

$$f(\overline{x}) = \sum_{i=0}^{n} \lambda_i \mathbf{e}_{i,n}(\overline{x}), \qquad \text{with } \lambda_i \in \mathbb{F}. \tag{6.2}$$

Proof: For a proof of the first part of Proposition 6 see [CLO15, Chap. 7, Theorem 3]. For a proof of the second part, proceed by induction on the degree d of f as follows: write $f(\overline{x}) = A + B$ where B is the sum of all monomials of total degree $< d$ in f. Then, A is the (homogeneous polynomial) which consists of the sum of all (multilinear) monomials of degree precisely d in f. Note that A must be symmetric, since under any permutation of variables σ, monomials in $A(\sigma\overline{x})$ remain of degree d and monomials in $B(\sigma\overline{x})$ remain of degree at most $d-1$. Thus, A is a symmetric, homogeneous and multilinear polynomial of degree d, which by Fact 5 means that $A = \lambda_d \cdot \mathbf{e}_{d,n}(\overline{x})$ for some $\lambda_d \in \mathbb{F}$ (and where $n = |\overline{x}|$). □

2.4 Algebraic Proof Systems

For a survey about algebraic proof systems and their relations to algebraic complexity see the survey [PT16]. Grochow and Pitassi [GP18] suggested the following algebraic proof system which is essentially a Nullstellensatz proof system [BIK+96a] written as an algebraic circuit.

Definition 7 (Nullstellensatz refutations)**.** *Let $f_1(\overline{x}), \ldots, f_m(\overline{x}), p(\overline{x})$ be a collection of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ over the field $\mathbb{F}$. A **Nullstellensatz refutation of the axioms** $\{f_j(\overline{x}) = 0\}_{j\in[m]}$, showing that the set of axioms do not have a solution from the Boolean cube is a sequence of polynomials $\{g_i(\overline{x})\}_{j\in[m]}$, such that (the equality in what follows stands for a formal polynomial identity):*

$$\sum_{i\in[m]} g_i(\overline{x}) \cdot f(\overline{x}) + \sum_{i\in[n]} h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1\,.$$

*The **degree** of the refutation is* $\max\{\deg(g_i(\overline{x}) \cdot f_i(\overline{x})) : \ i \in [m]\}$.[3]

Notice that the definition above adds the equations $\{x_i^2 - x_i = 0\}_{i=1}^n$, called the **Boolean axioms** denoted $\overline{x}^2 - \overline{x}$, to the system $\{f_j(\overline{x}) = 0\}_{j=1}^m$. This allows to refute systems of equations that have no solution over $\{0,1\}^n$ (though they may be solvable over $\mathbb{F}$ in general).

A proof in the Ideal Proof System is given as a *single* polynomial. We provide below the *Boolean* version of IPS (which includes the Boolean axioms), namely the version that establishes the unsatisfiability over 0-1 of a set of polynomial equations. In what follows we follow the notation in [FSTW21]:

Definition 8 (Ideal Proof System (IPS), Grochow-Pitassi [GP18])**.** *Let $f_1(\overline{x}), \ldots, f_m(\overline{x}), p(\overline{x})$ be a collection of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ over the field $\mathbb{F}$. An **IPS proof of** $p(\overline{x}) = 0$ **from axioms** $\{f_j(\overline{x}) = 0\}_{j\in[m]}$, showing that $p(\overline{x}) = 0$ is semantically implied from the assumptions $\{f_j(\overline{x}) = 0\}_{j\in[m]}$ over 0-1 assignments, is an algebraic circuit $C(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{F}[\overline{x}, y_1, \ldots, y_m, z_1, \ldots, z_n]$ such that (the equalities in what follows stand for formal polynomial identities[4]; recall the notation $\widehat{C}$ for the* polynomial *computed by circuit C):*

1. $\widehat{C}(\overline{x}, \overline{0}, \overline{0}) = 0$;
2. $\widehat{C}(\overline{x}, f_1(\overline{x}), \ldots, f_m(\overline{x}), x_1^2 - x_1, \ldots, x_n^2 - x_n) = p(\overline{x})$.

*The **size of the IPS proof** is the size of the circuit C. An* IPS *proof $C(\overline{x}, \overline{y}, \overline{z})$ of $1 = 0$ from $\{f_j(\overline{x}) = 0\}_{j\in[m]}$ is called an **IPS refutation** of $\{f_j(\overline{x}) = 0\}_{j\in[m]}$ (note that in this case it must hold that $\{f_j(\overline{x}) = 0\}_{j\in[m]}$ have no common solutions in $\{0,1\}^n$). If $\widehat{C}$ is of individual degree ≤ 1 in*

[3] It can be shown that $\max\{\deg(g_i(\overline{x}) \cdot f_i(\overline{x})) : \ i \in [m]\} \geq \max\{\deg(h_i(\overline{x})) + 2 : \ i \in [n]\}$, hence there is no need to count the degrees of the h_i's in the size.

[4] That is, $C(\overline{x}, \overline{0}, \overline{0})$ computes the zero polynomial and $C(\overline{x}, f_1(\overline{x}), \ldots, f_m(\overline{x}), x_1^2 - x_1, \ldots, x_n^2 - x_n)$ computes the polynomial $p(\overline{x})$.

each y_j and z_i, then this is a ***linear*** *IPS refutation (called* Hilbert *IPS by Grochow-Pitassi [GP18]), which we will abbreviate as* $\mathrm{IPS}_{\mathrm{LIN}}$*. If $\widehat{C}$ is of individual degree ≤ 1 only in the y_j's then we say this is an* $\mathrm{IPS}_{\mathrm{LIN}'}$ *refutation (following [FSTW21]). If $\widehat{C}(\overline{x},\overline{y},\overline{0})$ is of individual degree $\leq k$ in each x_j and y_i variables, while $\widehat{C}(\overline{x},\overline{0},\overline{z})$ is not necessarily bounded in its individual degree, then this is called an* ***individual degree-k*** $\mathrm{IPS}_{\mathrm{LIN}'}$ ***refutation****.*

If C is of depth at most d, then this is called a depth-d IPS refutation*, and further called a* depth-d $\mathrm{IPS}_{\mathrm{LIN}}$ refutation *if $\widehat{C}$ is linear in $\overline{y},\overline{z}$, and a depth-$d$* $\mathrm{IPS}_{\mathrm{LIN}'}$ *refutation if $\widehat{C}$ is linear in $\overline{y}$, and* depth-d multilinear $\mathrm{IPS}_{\mathrm{LIN}'}$ *refutation if $\widehat{C}(\overline{x},\overline{y},\overline{0})$ is linear in $\overline{x},\overline{y}$.*

The variables $\overline{y},\overline{z}$ are called the *placeholder variables* since they are used as placeholders for the axioms. Also, note that the first equality in the definition of IPS means that the polynomial computed by C is in the ideal generated by $\overline{y},\overline{z}$, which in turn, following the second equality, means that C witnesses the fact that 1 is in the ideal generated by $f_1(\overline{x}),\ldots,f_m(\overline{x}),x_1^2-x_1,\ldots,x_n^2-x_n$ (the existence of this witness, for unsatisfiable set of polynomials, stems from the Nullstellensatz [BIK+96a]).

2.4.1 Oblivious Algebraic Branching Programs

Algebraic branching programs (ABPs) is a model whose strength lies between that of algebraic circuits and algebraic formulas. (We use notation from [FSTW21].)

Definition 9 (Nisan [Nis91]; ABP)**.** *An* algebraic branching program (ABP) with unrestricted weights *of* depth D *and* width $\leq r$*, on the variables $x_1,\ldots,x_n$, is a directed acyclic graph such that:*

- *The vertices are partitioned into $D+1$ layers $V_0,\ldots,V_D$, so that $V_0=\{s\}$ (s is the source node), and $V_D=\{t\}$ (t is the sink node). Further, each edge goes from V_{i-1} to V_i for some $0<i\leq D$.*
- $\max|V_i|\leq r$*.*
- *Each edge e is weighted with a polynomial $f_e\in\mathbb{F}[\overline{x}]$.*

The ***(individual) degree*** *d of the ABP is the maximum (individual) degree of the edge polynomials f_e. The* ***size*** *of the ABP is the product $n\cdot r\cdot d\cdot D$. Each s-t path is said to compute the polynomial which is the product of the labels of its edges, and the algebraic branching program itself computes the sum over all s-t paths of such polynomials.*

The following are restricted ABP variants:

- *An algebraic branching program is said to be* ***oblivious*** *if for every layer ℓ, all the edge labels in that layer are* univariate *polynomials in a* single *variable x_{i_ℓ}.*
- *An oblivious branching program is said to be a* ***read-once*** *oblivious ABP (***roABP***) if each x_i appears in the edge label of exactly one layer, so that $D=n$. That is, each x_i appears in the edge labels in exactly one layer. The layers thus define a* ***variable order****, which will be assumed to be $x_1<\cdots<x_n$ unless otherwise specified.*

The class of roABPs is essentially equivalent to non-commutative ABPs ([FS13]), a model at least as strong as non-commutative formulas. The study of non-commutative ABPs was initiated by Nisan [Nis91], who proved lower bounds for non-commutative ABPs (and thus also for roABPs, in any order). In terms of proof complexity, Tzameret [Tza11] studied a proof system with lines given

by roABPs, and Li, Tzameret and Wang [LTW18] showed that IPS over non-commutative formulas is quasipolynomially equivalent in power to the Frege proof system. Since non-commutative ABPs and roABPs are essentially equivalent, this last result motivates proving lower bounds for roABP-IPS as a way of attacking lower bounds for the Frege proof system.

2.5 Coefficient Dimension and roABPs

In this section, we define the *coefficient dimension* measure and recall basic properties. Full proofs of these claims can be found for example in the thesis of Forbes [For14]. Again, we use notation from [FSTW21].

We first define the *coefficient matrix* of a polynomial. This matrix is formed from a polynomial $f \in \mathbb{F}[\overline{x}, \overline{y}]$ by arranging its coefficients into a matrix. That is, the coefficient matrix has rows indexed by monomials $\overline{x}^{\overline{a}}$ in $\overline{x}$, columns indexed by monomials $\overline{y}^{\overline{b}}$ in $\overline{y}$, and the $(\overline{x}^{\overline{a}}, \overline{y}^{\overline{b}})$-entry is the coefficient of $\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}$ in the polynomial f. We now define this matrix, recalling that $\mathrm{Coeff}_{\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}}(f)$ is the coefficient of $\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}$ in f (see Section 2.1).

Definition 10 (Coefficient matrix)**.** *Consider $f \in \mathbb{F}[\overline{x}, \overline{y}]$. Define the **coefficient matrix of** f as the scalar matrix*

$$(C_f)_{\overline{a},\overline{b}} := \mathrm{Coeff}_{\overline{x}^{\overline{a}}\overline{y}^{\overline{b}}}(f) \ ,$$

where coefficients are taken in $\mathbb{F}[\overline{x}, \overline{y}]$, for $\sum_{j=1}^{|\overline{a}|} |a_j|, \sum_{j=1}^{|\overline{b}|} |b_j| \leq \deg f$.

We now give the related definition of *coefficient dimension*, which looks at the dimension of the row- and column-spaces of the coefficient matrix. Recall that $\mathrm{Coeff}_{\overline{x}|\overline{y}^{\overline{b}}}(f)$ extracts the coefficient of $\overline{y}^{\overline{b}}$ in f, where f is treated as a polynomial in $\mathbb{F}[\overline{x}][\overline{y}]$.

Definition 11 (Coefficient space)**.** *Let $\mathbf{Coeff}_{\overline{x}|\overline{y}} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{x}]}$ be the **space of** $\mathbb{F}[\overline{x}][\overline{y}]$ **coefficients**, defined by*

$$\mathbf{Coeff}_{\overline{x}|\overline{y}}(f) := \left\{ \mathrm{Coeff}_{\overline{x}|\overline{y}^{\overline{b}}}(f) \right\}_{\overline{b} \in \mathbb{N}^n} \ ,$$

where coefficients of f are taken in $\mathbb{F}[\overline{x}][\overline{y}]$. Similarly, define $\mathbf{Coeff}_{\overline{y}|\overline{x}} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{y}]}$ by taking coefficients in $\mathbb{F}[\overline{y}][\overline{x}]$.

The following basic lemma shows that the rank of the coefficient matrix equals the coefficient dimension, which follows from simple linear algebra.

Lemma 12 (Coefficient matrix rank equals dimension of polynomial space; Nisan [Nis91])**.** *Consider $f \in \mathbb{F}[\overline{x}, \overline{y}]$. Then, the rank of the coefficient matrix C_f (Definition 10) obeys*

$$\mathrm{rank}\, C_f = \dim \mathbf{Coeff}_{\overline{x}|\overline{y}}(f) = \dim \mathbf{Coeff}_{\overline{y}|\overline{x}}(f) \ .$$

Therefore, the ordering of the partition ($(\overline{x}, \overline{y})$ versus $(\overline{y}, \overline{x})$) does not influence the resulting dimension.

We now state a convenient normal form for roABPs (see for example Forbes [For14, Corollary 4.4.2]).

Lemma 13 (Characterising roABP as a matrix product)**.** *A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is computed by width-r roABP iff there exist n matrices $A_i(x_i) \in \mathbb{F}[x_i]^{r \times r}$, for $i \in [n]$, each of (individual) degree $\leq \deg f$ such that $f = (\prod_{i=1}^{n} A_i(x_i))_{1,1}$.*

Using this normal form we can characterise roABP-width as follows.

Lemma 14 (roABP-width equals dimension of coefficient space)**.** *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial. If f is computed by a width-r roABP then $r \geq \max_i \dim \mathbf{Coeff}_{\overline{x}_{\leq i}|\overline{x}_{>i}}(f)$. Conversely, f is computable by a width-$\left(\max_i \dim \mathbf{Coeff}_{\overline{x}_{\leq i}|\overline{x}_{>i}}(f)\right)$ roABP.*

We use the following closure properties of roABPs, taken from [FSTW21].

Fact 15. *If $f, g \in \mathbb{F}[\overline{x}]$ are computable by width-r and width-s* roABPs *respectively, then*

- *$f + g$ is computable by a width-$(r + s)$ roABP.*
- *$f \cdot g$ is computable by a width-(rs) roABP.*

Further, roABPs are also closed under the following operations.

- *If $f(\overline{x}, \overline{y}) \in \mathbb{F}[\overline{x}, \overline{y}]$ is computable by a width-r roABP in some variable order then the partial substitution $f(\overline{x}, \overline{\alpha})$, for $\overline{\alpha} \in \mathbb{F}^{|\overline{y}|}$, is computable by a width-r roABP in the induced order on $\overline{x}$, where the degree of this roABP is bounded by the degree of the roABP for f.*
- *If $f(z_1, \ldots, z_n)$ is computable by a width-r roABP in variable order $z_1 < \cdots < z_n$, then $f(x_1 y_1, \ldots, x_n y_n)$ is computable by a $\mathsf{poly}(r, \operatorname{ideg} f)$-width roABP in variable order $x_1 < y_1 < \cdots < x_n < y_n$.*

2.6 Evaluation Dimension

While coefficient dimension measures the size of a polynomial $f(\overline{x}, \overline{y})$ by taking all coefficients in $\overline{y}$, *evaluation dimension* is a somewhat relaxed complexity measure due to Saptharishi [Sap12] that measures the size by taking all possible evaluations in $\overline{y}$ over the field. This measure will be important for our applications as one can restrict such evaluations to the Boolean cube and obtain circuit lower bounds against a *family* of polynomials that compute $f(\overline{x}, \overline{y})$ as a *function* on the Boolean cube.

Definition 16 (Evaluation dimension; Saptharishi [Sap12])**.** *Let $S \subseteq \mathbb{F}$. Let $\mathbf{Eval}_{\overline{x}|\overline{y},S} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{x}]}$ be the **space of** $\mathbb{F}[\overline{x}][\overline{y}]$ **evaluations over** S, defined by*

$$\mathbf{Eval}_{\overline{x}|\overline{y},S}(f(\overline{x}, \overline{y})) := \left\{ f(\overline{x}, \overline{\beta}) \right\}_{\overline{\beta} \in S^{|\overline{y}|}} .$$

Define $\mathbf{Eval}_{\overline{x}|\overline{y}} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{x}]}$ to be $\mathbf{Eval}_{\overline{x}|\overline{y},S}$ when $S = \mathbb{F}$. Similarly, define $\mathbf{Eval}_{\overline{y}|\overline{x},S} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{y}]}$ by replacing $\overline{x}$ with all possible evaluations $\overline{\alpha} \in S^{|\overline{x}|}$, and likewise define $\mathbf{Eval}_{\overline{y}|\overline{x}} : \mathbb{F}[\overline{x}, \overline{y}] \to 2^{\mathbb{F}[\overline{y}]}$.

The equivalence between evaluation dimension and coefficient dimension was shown by Forbes-Shpilka [FS13] by appealing to interpolation.

Lemma 17 (Evaluation dimension lower bounds dimension of coefficient space; Forbes-Shpilka [FS13])**.** *Let $f \in \mathbb{F}[\overline{x}, \overline{y}]$. For any $S \subseteq \mathbb{F}$ we have that $\mathbf{Eval}_{\overline{x}|\overline{y},S}(f) \subseteq \operatorname{span} \mathbf{Coeff}_{\overline{x}|\overline{y}}(f)$ so that $\dim \mathbf{Eval}_{\overline{x}|\overline{y},S}(f) \leq \dim \mathbf{Coeff}_{\overline{x}|\overline{y}}(f)$. In particular, if $|S| > \operatorname{ideg} f$ then $\dim \mathbf{Eval}_{\overline{x}|\overline{y},S}(f) = \dim \mathbf{Coeff}_{\overline{x}|\overline{y}}(f)$.*

Note that evaluation dimension and coefficient dimension are equivalent when the field is large enough (and $|S|$ is bigger than the individual degree of the polynomial). However, when restricting our attention to inputs from the Boolean cube this equivalence no longer holds, but evaluation dimension will be still useful as it *lower bounds* coefficient dimension.

2.7 Multilinear Polynomials and Multilinear Formulas

We now turn to multilinear polynomials and classes that respect multilinearity such as multilinear formulas. We first state some well-known facts about multilinear polynomials (taken from [FSTW21]).

Fact 18. *For any two multilinear polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n]$, $f = g$ as polynomials iff they agree on the Boolean cube $\{0,1\}^n$. That is, $f = g$ iff $f|_{\{0,1\}^n} = g|_{\{0,1\}^n}$.*

*Further, there is a **multilinearization** map $\mathrm{ml} : \mathbb{F}[\overline{x}] \to \mathbb{F}[\overline{x}]$ such that for any $f, g \in \mathbb{F}[\overline{x}]$,*

1. *$\mathrm{ml}(f)$ is multilinear.*
2. *f and $\mathrm{ml}(f)$ agree on the Boolean cube, that is, $f|_{\{0,1\}^n} = \mathrm{ml}(f)|_{\{0,1\}^n}$.*
3. *$\deg \mathrm{ml}(f) \leq \deg f$.*
4. *$\mathrm{ml}(fg) = \mathrm{ml}(\mathrm{ml}(f)\mathrm{ml}(g))$, and if f and g are defined on disjoint sets of variables then $\mathrm{ml}(fg) = \mathrm{ml}(f)\mathrm{ml}(g)$.*
5. *ml is linear, so that for any $\alpha, \beta \in \mathbb{F}$, $\mathrm{ml}(\alpha f + \beta g) = \alpha \mathrm{ml}(f) + \beta \mathrm{ml}(g)$.*
6. *$\mathrm{ml}(x_1^{a_1} \cdots x_n^{a_n}) = \prod_i x_i^{\min\{a_i, 1\}}$.*
7. *If f is the sum of at most s monomials (s-sparse) then so is $\mathrm{ml}(f)$.*

Also, if $\hat{f}$ is a function $\{0,1\}^n \to \mathbb{F}$ that only depends on the coordinates in $S \subseteq [n]$, then the unique multilinear polynomial f agreeing with $\hat{f}$ on $\{0,1\}^n$ is a polynomial only in $\{x_i\}_{i \in S}$.

Multilinear Formulas. We shall consider the model of multilinear formulas.

Definition 19 (Multilinear formula)**.** *An algebraic formula is a **multilinear formula** if the polynomial computed by* each *gate of the formula is multilinear (as a formal polynomial, that is, as an element of $\mathbb{F}[x_1, \ldots, x_n]$). The **product depth** is the maximum number of multiplication gates on any input-to-output path in the formula.*

Raz [Raz09, Raz06] gave lower bounds for multilinear formulas using the above notion of coefficient dimension, and Raz-Yehudayoff [RY08, RY09] gave simplifications and extensions to constant-depth multilinear formulas.

Theorem 20 (Raz-Yehudayoff [Raz09, RY08, RY09])**.** *Let $f \in \mathbb{F}[x_1, \ldots, x_{2n}, \overline{z}]$ be a multilinear polynomial in the set of variables $\overline{x}$ and auxiliary variables $\overline{z}$. Let $f_{\overline{z}}$ denote the polynomial f in the ring $\mathbb{F}[\overline{z}][\overline{x}]$. Suppose that for any partition $\overline{x} = (\overline{u}, \overline{v})$ with $|\overline{u}| = |\overline{v}| = n$ that*

$$\dim_{\mathbb{F}(\overline{z})} \mathbf{Coeff}_{\overline{u}|\overline{v}} f_{\overline{z}} \geq 2^n \ .$$

Then f requires $\geq n^{\Omega(\log n)}$-size to be computed as a multilinear formula, and for $d = o(\log n / \log\log n)$, f requires $n^{\Omega((n/\log n)^{1/d}/d^2)}$-size to be computed as a multilinear formula of product-depth-d.

2.8 Monomial Orders

We recall here the definition and properties of a *monomial order*, following Cox, Little and O'Shea [CLO15]. We abuse notation and associate a monomial $\overline{x}^{\overline{a}}$ with its exponent vector $\overline{a}$, so that we can extend this order to the exponent vectors. Note that in this definition "1" is a monomial, and that scalar multiples of monomials such as $2x$ are not considered monomials. We now define a monomial order, which will be total order on monomials with certain natural properties.

Definition 21. *A **monomial ordering** is a total order $\prec$ on the monomials in $\mathbb{F}[\overline{x}]$ such that*

- *For all $\overline{a} \in \mathbb{N}^n \setminus \{\overline{0}\}$, $1 \prec \overline{x}^{\overline{a}}$.*
- *For all $\overline{a}, \overline{b}, \overline{c} \in \mathbb{N}^n$, $\overline{x}^{\overline{a}} \prec \overline{x}^{\overline{b}}$ implies $\overline{x}^{\overline{a}+\overline{c}} \prec \overline{x}^{\overline{b}+\overline{c}}$.*

*For nonzero $f \in \mathbb{F}[\overline{x}]$, the **leading monomial of f (with respect to a monomial order $\prec$)**, denoted $\mathrm{LM}(f)$, is the largest monomial in $\mathrm{Supp}(f) := \{\overline{x}^{\overline{a}} : \mathrm{Coeff}_{\overline{x}^{\overline{a}}}(f) \neq 0\}$ with respect to the monomial order $\prec$. The **trailing monomial of** f, denoted $\mathrm{TM}(f)$, is defined analogously to be the smallest monomial in $\mathrm{Supp}(f)$. The zero polynomial has neither leading nor trailing monomial.*

*For nonzero $f \in \mathbb{F}[\overline{x}]$, the **leading (resp. trailing) coefficient of** f, denoted $\mathrm{LC}(f)$ (resp. $\mathrm{TC}(f)$), is $\mathrm{Coeff}_{\overline{x}^{\overline{a}}}(f)$ where $\overline{x}^{\overline{a}} = \mathrm{LM}(f)$ (resp. $\overline{x}^{\overline{a}} = \mathrm{TM}(f)$).*

In contrast to [FSTW21], we will also use the existence of monomial orderings that *respect degree* in the sense that if $\deg(M) > \deg(N)$ for two monomials M, N, then $M \succ N$.

The following is a simple lemma about leading or trailing monomials (or coefficients) being homomorphic with respect to multiplication.

Lemma 22 ([FSTW21])**.** *Let $f, g \in \mathbb{F}[\overline{x}]$ be nonzero polynomials. Then the leading monomial and trailing monomials and coefficients are homomorphic with respect to multiplication, that is, $\mathrm{LM}(fg) = \mathrm{LM}(f)\,\mathrm{LM}(g)$ and $\mathrm{TM}(fg) = \mathrm{TM}(f)\,\mathrm{TM}(g)$, as well as $\mathrm{LC}(fg) = \mathrm{LC}(f)\,\mathrm{LC}(g)$ and $\mathrm{TC}(fg) = \mathrm{TC}(f)\,\mathrm{TC}(g)$.*

We shall use the well-known fact that for any set of polynomials the dimension of their span in $\mathbb{F}[\overline{x}]$ is equal to the number of *distinct* leading or trailing monomials in their span.

Lemma 23. *Let $S \subseteq \mathbb{F}[\overline{x}]$ be a set of polynomials. Then $\dim \mathrm{span}\, S = |\mathrm{LM}(\mathrm{span}\, S)| = |\mathrm{TM}(\mathrm{span}\, S)|$. In particular, $\dim \mathrm{span}\, S \geq |\mathrm{LM}(S)|, |\mathrm{TM}(S)|$.*

3 Degree Lower Bounds

3.1 Symmetric Instances

In this section we show that all symmetric unsatisfiable instances are hard for Nullstellensatz degree, as well as some vector invariant polynomial instances.

Let $\overline{x}$ denote the set $\{x_1, \ldots, x_n\}$.

Fact 24. *Let $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ be symmetric and unsatisfiable over 0-1 assignments (i.e., $f(\overline{x}) = 0$ has no 0-1 solutions). Then $f(\overline{x})$ is of the form $t(\overline{x}) - \beta$ with $0 \neq \beta \in \mathbb{F}$ and $t(\overline{x})$ a symmetric polynomial.*

Proof: If $f(\overline{x})$ is symmetric and does not contain a constant term, i.e., $f(\overline{0}) = 0$, then $f(\overline{x}) = 0$ is satisfiable. Thus, $f(\overline{x}) = t(\overline{x}) - \beta$, where $\beta = f(\overline{0})$. The polynomial $t(\overline{x})$ is symmetric because $f(\overline{x})$ is (since permuting the variables of $f(\overline{x})$ per Definition 3 of symmetric polynomials does not change the constant term $f(\overline{0})$). □

Lemma 25. *Let $n \geq 1$ and $1 \leq d \leq n$, and let $\mathbb{F}$ be a field of characteristic strictly greater than* $\max(2^n, n^d)$. *Let $\beta \in \mathbb{F} \setminus \{0, 1, \ldots, n^d\}$ and f be a* multilinear *polynomial such that*

$$f(\overline{x}) \cdot (\mathbf{e}_{d,n}(\overline{x}) - \beta) = 1 \mod \overline{x}^2 - \overline{x}. \tag{25.1}$$

Then, $n - d < \deg(f) \leq n$.

Proof: Note that $\mathbf{e}_{d,n}(\overline{x}) - \beta = 0$ is unsatisfiable whenever $\beta \in \mathbb{F} \setminus \{0, 1, \ldots, n^d\}$ and the characteristic of $\mathbb{F}$ is greater than n^d. This is because $\mathbf{e}_{d,n}(\overline{x})$ contains n^d distinct monomials with the coefficient 1, which evaluates to either 0 or 1 under Boolean assignments. Moreover, the characteristic of $\mathbb{F}$ needs to be greater than 2^n so that for any nonzero $\gamma_\ell \in \mathbb{F}$ we have $\gamma_\ell \cdot 2^n \neq 0$ in $\mathbb{F}$ (which is needed in Equation (26.3); see the ensuing explanation there).

$\underline{\leq n}$: This is clear as f is multilinear.

$\underline{> n - d}$: Begin by observing that $\beta \in \mathbb{F} \setminus \{0, 1, \ldots, n^d\}$ implies that $\mathbf{e}_{d,n}(\overline{x}) - \beta$ is never zero on the Boolean cube $\{0,1\}^n$, so that the by Equation (25.1) for $\overline{x} \in \{0,1\}^n$ the expression

$$f(\overline{x}) = \frac{1}{\mathbf{e}_{d,n}(\overline{x}) - \beta},$$

is well defined. Now observe that this implies that f *is a symmetric polynomial.* To see this, let us define $g(\overline{x})$ to be the symmetrizing polynomial for $f(\overline{x})$, i.e.,

$$g(x_1, x_2, \ldots, x_n) = \frac{1}{n!} \cdot \sum_{\sigma \in S_n} f(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)).$$

Then, we see $\frac{1}{n!} \cdot \sum_{\sigma \in S_n} f(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)) = \frac{1}{n!} \cdot \sum_{\sigma \in S_n} \frac{1}{\mathbf{e}_{d,n}(\sigma(\overline{x})) - \beta}$. As $\mathbf{e}_{d,n}(\overline{x})$ is symmetric, we see that $g(\overline{x}) = f(\overline{x})$, which means $f(\overline{x})$ is symmetric.[5]

The following claim is the main technical observation of the lower bound and is a generalisation of the [FSTW21] lower bounds for the case of linear symmetric polynomials, i.e., when $d = 1$. The idea is that the multilinearization of the product $(\mathbf{e}_{d,n}(\overline{x}) - \beta) \cdot \mathbf{e}_{k,n}(\overline{x})$ contains nonzero monomials of degree ≥ 1, given that $d + k \leq n$, hence it cannot equal the polynomial 1. On the other hand, note that when $d + k > n$ we cannot make sure that this product, when we multiply out terms, does not yield cancellations of monomials potentially resulting in the 1 polynomials.

Claim 26 (Multilinearizing the product of elementary symmetric polynomials yields high degree)**.** *Let $n \geq 1$ and $1 \leq d \leq n$. If k is such that $k \leq n - d$, then*

$$\mathbf{e}_{d,n}(\overline{x}) \cdot \mathbf{e}_{k,n}(\overline{x}) = 2^{d+k} \cdot \mathbf{e}_{d+k,n}(\overline{x}) + [\textit{degree} \leq d + k - 1 \textit{ terms}] \mod \overline{x}^2 - \overline{x}\,.$$

Proof of claim:

$$\begin{aligned}
\mathbf{e}_{d,n}(\overline{x}) \cdot \mathbf{e}_{k,n}(\overline{x}) &= \sum_{\overline{a} \in \binom{n}{d}} \overline{x}^{\overline{a}} \cdot \sum_{\overline{b} \in \binom{n}{k}} \overline{x}^{\overline{b}} = \sum_{\overline{a} \in \binom{n}{d},\ \overline{b} \in \binom{n}{k}} \overline{x}^{\overline{a}} \cdot \overline{x}^{\overline{b}} \\
&= \sum_{\substack{\overline{a} \in \binom{n}{d},\ \overline{b} \in \binom{n}{k} \\ \overline{a} \cap \overline{b} = \emptyset}} \overline{x}^{\overline{a}} \cdot \overline{x}^{\overline{b}} + \sum_{\substack{\overline{a} \in \binom{n}{d},\ \overline{b} \in \binom{n}{k} \\ \overline{a} \cap \overline{b} \neq \emptyset}} \overline{x}^{\overline{a}} \cdot \overline{x}^{\overline{b}} \\
&= 2^{d+k} \cdot \sum_{\overline{c} \in \binom{n}{d+k}} \overline{x}^{\overline{c}} + \sum_{j=1}^{\min(d,k)} \sum_{\substack{\overline{a} \in \binom{n}{d},\ \overline{b} \in \binom{n}{k} \\ |\overline{a} \cap \overline{b}| = j}} \overline{x}^{\overline{a}} \cdot \overline{x}^{\overline{b}},
\end{aligned} \tag{26.1}$$

[5] Another way to show that $f(\overline{x})$ is symmetric is this: a multilinear polynomial is uniquely determined by the values it gets over the Boolean cube. And here we know that the function over the Boolean cube is symmetric (as a function; namely, stays the same under permutation of variables). This means that the polynomial itself is symmetric (because it is multilinear).

where 2^{d+k} in the last line follows by considering all possible partitions of each $(d+k)$-subset $\overline{c} \in \binom{n}{d+k}$ into two disjoint subsets $\overline{a} \in \binom{n}{d}$, $\overline{b} \in \binom{n}{k}$. Now, consider the second summand in Equation (26.1). If we multilinearize this polynomial we get a multilinear polynomial of degree at most $d+k-1$, concluding the claim. To be more precise, we have

$$\sum_{j=1}^{\min(d,k)} \sum_{\substack{\overline{a}\in\binom{n}{d},\ \overline{b}\in\binom{n}{k} \\ |\overline{a}\cap\overline{b}|=j}} \overline{x}^{\overline{a}} \cdot \overline{x}^{\overline{b}} = \binom{d+k-1}{1} \cdot 2^{d+k-2} \cdot \sum_{\overline{c}\in\binom{n}{d+k-1}} \overline{x}^{\overline{c}} + \binom{d+k-2}{2} \cdot 2^{d+k-3} \cdot \sum_{\overline{c}\in\binom{n}{d+k-2}} \overline{x}^{\overline{c}} + \binom{\max(d,k)}{\min(d,k)} \cdot \sum_{\overline{c}\in\binom{n}{\max(d,k)}} \overline{x}^{\overline{c}} \mod \overline{x}^2 - \overline{x}\,, \quad (26.2)$$

where $\binom{d+k-1}{1} \cdot 2^{d+k-2}$ in the first summand in the right-hand side of the equation means that for each choice of the single element in $\overline{c} = \overline{a} \cup \overline{b}$ that is common to both $\overline{a} \in \binom{n}{d}$ and $\overline{b} \in \binom{n}{k}$ (there are $\binom{d+k-1}{1}$ such choices) we can attribute the rest of the elements in $\overline{c}$ to $\overline{a}$ or $\overline{b}$ in 2^{d+k-2} different ways. Similar considerations apply to the rest of the summands in Equation (26.2). ■Claim

Suppose for contradiction that $\ell = \deg(f) \leq n-d$. Then, using the fact that modulo $\overline{x}^2 - \overline{x}$ the symmetric polynomial $f(\overline{x})$ must be symmetric and multilinear and hence a linear combination of elementary symmetric polynomials (Proposition 6), we have

$$\begin{aligned}
1 &= f(\overline{x}) \cdot (\mathbf{e}_{d,n}(\overline{x}) - \beta) \mod \overline{x}^2 - \overline{x} \\
&= \left(\sum_{k=0}^{\ell} \gamma_k \mathbf{e}_{k,n}(\overline{x})\right) \cdot (\mathbf{e}_{d,n}(\overline{x}) - \beta) \mod \overline{x}^2 - \overline{x} \\
&= \left(\sum_{k=0}^{\ell} \gamma_k \mathbf{e}_{k,n}(\overline{x}) \cdot \mathbf{e}_{d,n}(\overline{x})\right) - \left(\sum_{k=0}^{\ell} \beta\gamma_k \mathbf{e}_{k,n}(\overline{x})\right) \mod \overline{x}^2 - \overline{x} \\
&= \left(\sum_{k=0}^{\ell} \gamma_k 2^{d+k} \cdot \mathbf{e}_{d+k,n}(\overline{x}) + [\text{degree} \leq d+k-1 \text{ terms}]\right) - \left(\sum_{k=0}^{\ell} \beta\gamma_k \mathbf{e}_{k,n}(\overline{x})\right) \mod \overline{x}^2 - \overline{x} \\
&= \gamma_\ell 2^n \cdot \mathbf{e}_{d+\ell,n}(\overline{x}) + [\text{degree} \leq d+\ell-1 \text{ terms}] \mod \overline{x}^2 - \overline{x}\,. \quad (26.3)
\end{aligned}$$

Where the penultimate equation is by invoking Claim 26, which we can since $\ell \leq n-d$. By assumption that $\deg(f) = \ell$, we know that $\gamma_\ell \neq 0$. By assumption $\ell \leq n-d$, we have that $\mathbf{e}_{d+\ell,n}(\overline{x})$ is of degree at most n (if $\ell = n-d$ it is $\mathbf{e}_{n,n}(\overline{x})$) and at least d (in case $\ell = 0$), where $d \geq 1$ by assumption. Since the characteristic of the field is greater than 2^n we know that $\gamma_\ell 2^n \neq 0$. This shows that 1 (a multilinear degree 0 polynomial) equals because Equation (26.3) (a multilinear degree $d+\ell$ polynomial) modulo $\overline{x}^2 - \overline{x}$, which is a contradiction to the uniqueness of representation of multilinear polynomials modulo $\overline{x}^2 - \overline{x}$. Thus, we must have $\deg(f) > n-d$. □

We now generalise Lemma 25 from a lower bound for an *elementary* symmetric polynomial to a lower bound for all symmetric polynomials.

Corollary 27 (Single unsatisfiable symmetric polynomials require high degree refutations)**.** *Assume that $n \geq 1$ and $1 \leq d \leq n$, $\mathbb{F}$ is a field of characteristic greater than $\max(2^n, n^d)$, and $f(\overline{x})$ is a symmetric polynomial of degree d such that $f(\overline{x}) - \beta$ has no 0-1 solution, for $\beta \in \mathbb{F}$. Suppose that g is a multilinear polynomial such that*

$$g(\overline{x}) \cdot (f(\overline{x}) - \beta) = 1 \mod \overline{x}^2 - \overline{x}.$$

Then, the degree of $g(\overline{x})$ is at least $n-d+1$. Accordingly, the degree of every Nullstellensatz refutation of $f(\overline{x})-\beta$ is at least $n+1$.

Proof: By Proposition 6 we can write the symmetric polynomial $f(\overline{x})$ as $\sum_{i=0}^{d}\lambda_i e_d(\overline{x})$, with $\lambda_i \in \mathbb{F}$. Thus,

$$\begin{aligned}
1 &= g(\overline{x})\cdot(f(\overline{x})-\beta) \mod \overline{x}^2-\overline{x}\\
&= g(\overline{x})\cdot\left(\sum_{i=0}^{d}\lambda_i e_i(\overline{x})-\beta\right) \mod \overline{x}^2-\overline{x}\\
&= g(\overline{x})\cdot\left(\lambda_d e_d(\overline{x})+\sum_{i=0}^{d-1}\lambda_i e_i(\overline{x})-\beta\right) \mod \overline{x}^2-\overline{x}\\
&= g(\overline{x})\cdot\lambda_d e_d(\overline{x})+g(\overline{x})\cdot\left(\sum_{i=0}^{d-1}\lambda_i e_i(\overline{x})-\beta\right) \mod \overline{x}^2-\overline{x}. \qquad (27.1)
\end{aligned}$$

Assume for contradiction that $\deg(g)\leq n-d$. By Claim 26 $\deg\left(\mathrm{ml}\left(g(\overline{x})\cdot\lambda_d e_d(\overline{x})\right)\right) = \deg(g)+d$ (using also that $\lambda_d \neq 0$, by assumption on degree of f), while $\deg\left(\mathrm{ml}\left(g(\overline{x})\cdot(\sum_{i=0}^{d-1}\lambda_i e_i(\overline{x})-\beta)\right)\right)\leq \deg(g)+d+1$. Therefore, Equation (27.1) is a (multilinear) polynomial of degree at most $\deg(g)+d$. We assumed that $\deg(g)\leq n-d$, meaning that Equation (27.1) is a (multilinear) polynomial of degree at most n (and at least 1 since $d\geq 1$). But as before, this is a contradiction to the uniqueness of the multilinear polynomial 1. □

Comment. Some of the symmetric lower bounds in this section section can possibly be obtained by using the subset sum lower bounds in [FSTW21]. One way to do that would be to *lift* the hardness of subset sum to derive the hardness for $\mathbf{e}_{d,n}(\overline{x})-\beta$ (for $d\geq 2$). We believe that [FKS16] present preliminary ideas which should allow for such an approach to lower bounds. Specifically, they note that any $\mathbf{e}_{d,n}(\overline{x})$ is equal to a product of d affine forms over the Boolean cube. While this is a useful direction, this approach apparently can work to derive lower bounds only for some specific β's. Whereas, in Corollary 27 we can obtain such lower bounds for all β's that makes the instance unsatisfiable over Boolean assignments. On the other hand, assuming this approach could be made to work, a possible benefit is this: consider the case of two-axioms $\{f_1=\mathbf{e}_{d,n}-\beta_1, f_2=\sum_{i=1}^{n}x_i-\beta_2\}$. If we can show that $\mathbf{e}_{d,n}-\beta_1$ is in the ideal generated by f_2 above, then we will be able to obtain lower bounds for the interesting case of two axioms $\{f_1,f_2\}$.

3.2 Vector Invariant Polynomials

Here we show hardness for an instance that is not a subset sum variant (formally, it is not a substitution instance of $\sum_{i=1}^{n}x_i$, for $n=\omega(1)$). Our hard instance is inspired by ideas from *invariant theory*.

Polynomial Invariants. We start with a gentle introduction to polynomial invariants. For a detailed introduction please refer to [CLO15]. Let $\mathrm{GL}(n,\mathbb{F})$ denote the set of all $n\times n$ matrices over the field $\mathbb{F}$. Let $A\in\mathrm{GL}(n,\mathbb{F})$, then we can think of A acting on the polynomials in the polynomial ring $\mathbb{F}[x_1,\ldots,x_n]$ as follows. Let $A=(a_{i,j})\in\mathrm{GL}(n,\mathbb{F})$ and $f(x_1,\ldots,x_n)\in\mathbb{F}[x_1,\ldots,x_n]$, then

$$g(x_1,\ldots,x_n)=f(a_{1,1}x_1+\ldots+a_{1,n}x_n,\ldots,a_{n,1}x_1+\ldots+a_{n,n}x_n).$$

More compactly, let $\overline{x}=(x_1\ x_2\ldots\ x_n)^{\mathrm{T}}$, then $g(\overline{x})=f(A\cdot\overline{x})$.

We say that a polynomial $f(\overline{x})$ is *invariant* under the action of a finite matrix group $G \subset \mathrm{GL}(n, \mathbb{F})$, if $f(\overline{x}) = f(A \cdot \overline{x})$ for every $A \in G$. A set of all polynomials that are invariant under G is denoted by $\mathbb{F}[\overline{x}]^G$.

As an example, consider $\mathcal{S}_n$, the set of all $n \times n$ permutation matrices. Then, $\mathbb{F}[\overline{x}]^{\mathcal{S}_n}$ is the set of all symmetric polynomials. This is arguably the most well-studied class of invariant polynomials. In the previous section, we studied exactly this class of polynomials.

Here, we will consider a different class of invariant polynomials known as *vector invariants*, which is a well-studied class of invariant polynomials. Intuitively, vector invariants are a class of polynomials that are invariant under the action of *a decomposable* group, that is, a group that can be written down as a direct sum (taken say n times) of a smaller group. The action on the bigger group is then defined by *diagonally extending* the action on the smaller group. See [Ric90, CH97, DK15] for formal definitions of vector invariants and many interesting results about them.

Here, we will define the specific vector invariants relevant for our hard instances.

Vector Invariant Polynomials and the Hard Instance. Let $\overline{u} = (u_1\ u_2)^T$ and $\overline{v} = (v_1\ v_2)^T$. Let R be a linear transformation that maps u_1 to u_1, u_2 to u_2, v_1 to $u_1 + v_1$ and v_2 to $u_2 + v_2$. That is,

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

which has the property that

$$(u_1, u_2, u_1 + v_1, u_2 + v_2)^T = R \times (u_1, u_2, v_1, v_2)^T.$$

This specific action is based on the vector invariants of $U_2(\mathbb{F})$ studied in an influential paper of [Ric90]. (The definition of $U_2(\mathbb{F})$ is very similar to R above and can be found in [Ric90, CH97] or in [DK15].)

Let $p(\overline{u}, \overline{v}) \in \mathbb{F}[\overline{u}, \overline{v}]$ be equal to $u_1v_2 - v_1u_2$, that is, it is the determinant of the following matrix.

$$\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix}$$

Then, it is easy to see that $p(\overline{u}, \overline{v}) = p(R \cdot \overline{u}, \overline{v})$. That is, if we apply the linear transformation given by R to the variables of $p(\overline{u}, \overline{v})$, then the polynomial stays invariant. This polynomial on 4 variables is our main ingredient in the hard instance. We now describe our hard instance.

Let $\mathbb{F}$ be a field of characteristic greater than or equal to 5 for the rest of this section[6]. Let $\overline{x} := \{x_1, x_2, \ldots, x_{2n}\}$ and $\overline{y} := \{y_1, y_2, \ldots, y_{2n}\}$ be commuting variables over $\mathbb{F}$. Let

$$\widetilde{Q}(\overline{x}, \overline{y}) := \left(\prod_{i \in [2n],\ i\text{: odd}} (x_i y_{i+1} - y_i x_{i+1}) \right).$$

Informally, $\widetilde{Q}(\overline{x}, \overline{y})$ is obtained by taking n copies of the polynomial $p(\overline{u}, \overline{v})$ (with variable renaming) and extending the action of R on the polynomial thus obtained.

Finally, the hard instance is defined as follows.

[6]The degree lower bound in this section will work for characteristics 3 or more, but for size lower bounds, we will need characteristics 5 or more. For the sake of uniformity, we assume that the characteristic is 5 or more throughout.

$$Q(\overline{x},\overline{y}) := \widetilde{Q}(\overline{x},\overline{y}) - \beta, \tag{27.2}$$

where $\beta \in \mathbb{F}$. This polynomial has several interesting properties, summarized as follows:

Fact 28. *The polynomial $Q(\overline{x},\overline{y})$ defined above has the following properties.*

1. *$Q(\overline{x},\overline{y})$ is a multilinear polynomial of degree $2n$.*
2. *The polynomial is invariant under the following action: for every odd $i \in [2n]$ (it is sufficient for the present work to think of actions, denoted $\hookrightarrow$, as substitutions of variables by polynomials)*

$$x_i \hookrightarrow x_i \qquad x_{i+1} \hookrightarrow x_{i+1} \qquad y_i \hookrightarrow x_i + y_i \qquad y_i \hookrightarrow x_{i+1} + y_{i+1}\,.$$

3. *For $i \in [2n]$ and i odd, let $a_i := (x_i y_{i+1} - y_i x_{i+1})$. Then, a_i is the determinant of the matrix $M_i = \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix}$. Moreover, $a_i \in \{-1, 0, 1\}$ over the Boolean cube.*
4. *$Q(\overline{x},\overline{y})$ is not satisfiable as long as β is greater than or equal to 2.*

3.2.1 Degree lower bound for $Q(\overline{x},\overline{y})$

Notation. For any set $A \subseteq [2n]$, let $\overline{x}_A$ denote the monomial $\prod_{i\in A} x_i$. Let $\widetilde{\overline{x}_A}$ denote the product $\prod_{i\in A}(1-x_i)$. Similarly, let $\overline{y}_A = \prod_{i\in A} y_i$ and $\widetilde{\overline{y}_A}$ denote the product $\prod_{i\in A}(1-y_i)$. Let $\mathbb{1}_A$ denote a $2n$-length vector in which the ith bit is 1 if and only if $i \in A$. For a monomial m and a polynomial $f(\overline{x},\overline{y})$, let $\mathrm{Coeff}_m(f(\overline{x},\overline{y}))$ denote the coefficient of the monomial m in $f(\overline{x},\overline{y})$.

The degree lower bound. We define $f(\overline{x},\overline{y})$ to be the unique multilinear polynomial that it is equal to $1/Q(\overline{x},\overline{y})$ over $\{0,1\}^{2n}$, i.e., over the Boolean cube of dimension $2n$. We will show that it contains a degree-$2n$ monomial with a non-zero coefficient. This will show that the degree of $f(\overline{x},\overline{y})$ is at least $2n$.

Let $S = \{i \in [2n] \mid i \text{ is odd}\}$ and $T = \{i \in [2n] \mid i \text{ is even}\}$.

Lemma 29. *There exists a $\beta > 2$ such that the coefficient of the monomial $\overline{x}_S \cdot \overline{y}_T$ in $f(\overline{x},\overline{y})$ is non-zero.*

Proof: From the uniqueness of the evaluations of multilinear polynomials over the Boolean cube, we know that

$$f(\overline{x},\overline{y}) = \sum_{A\subseteq[2n], B\subseteq[2n]} f(\mathbb{1}_A,\mathbb{1}_B)\overline{x}_A \cdot \widetilde{\overline{x}_A} \cdot \overline{y}_B \cdot \widetilde{\overline{y}_B},$$

where $\mathbb{1}_A$ is the indicator vector of the set A.

First, note that to analyse the coefficient of $\overline{x}_S \cdot \overline{y}_T$ in $f(\overline{x},\overline{y})$, we can set $x_i = 0$ for $i \notin S$ and similarly, $y_i = 0$ for $i \notin T$. This is because, setting variables outside the set S, T to zero does not change the coefficient of $\overline{x}_S \cdot \overline{y}_T$ in $f(\overline{x},\overline{y})$. Now, notice that if $A \not\subseteq S$, then $\overline{x}_A$ will become zero under the above assignment. Similarly, if $B \not\subseteq T$ then $\overline{y}_B$ will be set to zero. Thus, it suffices to sum over $A \subseteq S$ and $B \subseteq T$, if we want to understand the coefficient of $\overline{x}_S \cdot \overline{y}_T$. Overall, we get

$$\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(f(\overline{x},\overline{y})\right) = \mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subseteq S,\ B\subseteq T} f(\mathbb{1}_A,\mathbb{1}_B)\overline{x}_A \cdot \widetilde{\overline{x}_{S\setminus A}} \cdot \overline{y}_B \cdot \widetilde{\overline{y}_{T\setminus B}}\right).$$

Observe that, $f(\mathbb{1}_S, \mathbb{1}_T) = \frac{1}{1-\beta}$, because $Q(\mathbb{1}_S, \mathbb{1}_T) = 1 - \beta$, and for any $A \subsetneq S$ or $B \subsetneq T$, $f(\mathbb{1}_A, \mathbb{1}_B) = -\frac{1}{\beta}$, because $Q(\mathbb{1}_A, \mathbb{1}_B) = -\beta$ (since at least one of the u_is is zeroed out by the assignment; see Item 3 above).

Hence, we can now simplify the above summation as follows.

$$\begin{aligned}\text{Coeff}_{\overline{x}_S \cdot \overline{y}_T}\left(f(\overline{x}, \overline{y})\right) &= \text{Coeff}_{\overline{x}_S \cdot \overline{y}_T}\left(\sum_{A \subseteq S, B \subseteq T} f(\mathbb{1}_A, \mathbb{1}_B)\overline{x}_A \cdot \widetilde{\overline{x}_{S \setminus A}} \cdot \overline{y}_B \cdot \widetilde{\overline{y}_{T \setminus B}}\right) \\ &= -\frac{1}{\beta} \cdot C + \frac{1}{1-\beta},\end{aligned}$$

where $C \in \mathbb{Z}$. Note that for as long as $\frac{\beta}{1-\beta}$ is not integral, the above number is non-zero for any integral value of C. We can ensure this by appropriately picking a value for β. For example, $\beta = 3$ will work here. This finishes the proof of the lemma. □

In fact, we can compute the coefficient of $\overline{x}_X \cdot \overline{y}_T$ exactly. This understanding about the exact value of the coefficient will crucial for lifting the degree lower bounds to obtain size lower bounds in subsequent sections.

Computing the exact coefficient of $\overline{x}_S \cdot \overline{y}_T$ Recall, here $S = \{i \in [2n] \mid i \text{ is odd}\}$ and $T = [2n] \setminus S$. In the following claim, we obtain the exact coefficient of $\overline{x}_S \cdot \overline{y}_T$. We will use this calculation again for Item 2 in Lemma 40.

Lemma 30. *The coefficient of $\overline{x}_S \cdot \overline{y}_T$ in $f(\overline{x}, \overline{y})$ is equal to $\frac{1}{\beta} + \frac{1}{1-\beta}$. That is, the constant C in the above computation is -1.*

Proof: In order to understand C, let us simplify the term we want to analyse. We will use the following simple fact about binomial coefficients in the proof.

Fact 31.

$$\sum_{0 \le j \le n-1} \binom{n}{j} (-1)^{n-j} = -1\,.$$

We have the following

$$\begin{aligned}
&\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subseteq S,B\subseteq T} f(\mathbb{1}_A,\mathbb{1}_B)\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)\\
=\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subsetneq S,B\subsetneq T} f(\mathbb{1}_A,\mathbb{1}_B)\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_B\cdot\widetilde{Y_{T\setminus B}}\right)+\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\frac{1}{1-\beta}\cdot\overline{x}_S\cdot\overline{y}_T\right)\\
+\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{B\subsetneq T} f(\mathbb{1}_S,\mathbb{1}_B)\overline{x}_S\cdot\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)+\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subsetneq S} f(\mathbb{1}_A,\mathbb{1}_T)\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_T\right)
\end{aligned}\tag{31.1}$$

$$\begin{aligned}
=\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subsetneq S,B\subsetneq T}\frac{-1}{\beta}\cdot\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)+\left(\frac{1}{1-\beta}\right)\\
+\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{0\le|B|\le n-1,B\subsetneq T}-\frac{1}{\beta}\cdot\overline{x}_S\cdot\overline{y}_B\cdot\widetilde{\overline{x}_{T\setminus B}}\right)+\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{0\le|A|\le n-1,A\subsetneq S}-\frac{1}{\beta}\cdot\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_T\right).
\end{aligned}\tag{31.2}$$

Observe that Equation (31.1) has 4 terms in it. The second term arises from taking $A=S$ and $B=T$. Due to our choice of S,T, the coefficient of this term is simply $1/(1-\beta)$.

Let us now analyse Terms 1, 3, and 4 from Equation (31.2).

$$\begin{aligned}
\text{Term 1} =\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{A\subsetneq S,B\subsetneq T}\frac{-1}{\beta}\cdot\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)\\
=\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{0\le|A|\le n-1,\ 0\le|B|\le n-1,\ A\subsetneq S,\ B\subsetneq T}\frac{-1}{\beta}\cdot\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\cdot\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)\\
=\ &\mathrm{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\frac{-1}{\beta}\cdot\left(\sum_{0\le|A|\le n-1,\ A\subsetneq S}\overline{x}_A\cdot\widetilde{\overline{x}_{S\setminus A}}\right)\cdot\left(\sum_{0\le|B|\le n-1,B\subsetneq T}\overline{y}_B\cdot\widetilde{\overline{y}_{T\setminus B}}\right)\right)\\
=\ &\left(\frac{-1}{\beta}\cdot\left(\sum_{0\le j\le n-1}\binom{n}{j}(-1)^{n-j}\right)\cdot\left(\sum_{0\le j\le n-1}\binom{n}{j}(-1)^{n-j}\right)\right)\\
=\ &\left(\frac{-1}{\beta}\cdot\left(\sum_{0\le j\le n-1}\binom{n}{j}(-1)^{n-j}\right)^2\right)\\
=\ &-\frac{1}{\beta}\qquad\qquad\text{(using Fact 31).}
\end{aligned}$$

Similarly,

$$\begin{aligned}\text{Term } 2 = \ & \text{Coeff}_{\overline{x}_S \cdot \overline{y}_T}\left(\sum_{0\le|B|\le n-1, B\subsetneq T} -\frac{1}{\beta}\cdot \overline{x}_S \cdot \overline{y}_B \cdot \widetilde{\overline{y}_{T\setminus B}}\right) \\ = \ & \text{Coeff}_{\overline{y}_T}\left(\sum_{0\le|B|\le n-1, B\subsetneq T} -\frac{1}{\beta}\cdot \overline{y}_B \cdot \widetilde{\overline{y}_{T\setminus B}}\right) \\ = \ & -\frac{1}{\beta}\cdot\left(\sum_{0\le j\le n-1}\binom{n}{j}(-1)^{n-j}\right) = \frac{1}{\beta} \qquad \text{(using Fact 31).}\end{aligned}$$

And by symmetry, we also get that

$$\text{Term } 3 = \text{Coeff}_{\overline{x}_S\cdot\overline{y}_T}\left(\sum_{0\le|A|\le n-1, A\subsetneq S} -\frac{1}{\beta}\cdot \overline{x}_A \cdot \widetilde{\overline{x}_{S\setminus A}} \cdot \overline{y}_T\right) = \frac{1}{\beta}\,.$$

And now, using all the above values in the computation, we get that

$$\text{Coeff}_{\overline{x}_S\overline{y}_T}\left(f(\overline{x},\overline{y})\right) = \frac{1}{\beta} + \frac{1}{1-\beta} = \frac{1}{\beta(1-\beta)}\,.$$

□

As a corollary of this lemma, we get that the refutation of $Q(\overline{x},\overline{y})$ ought to have degree at least $2n$. Specifically, we get the following statement.

Theorem 32. *Let $\mathbb{F}$ be any field of characteristic 5 or more and let $\beta \notin \{-1,0,1\}$. Then, $Q(\overline{x},\overline{y})$, $\{x_i^2 - x_i\}_i$, and $\{y_i^2 - y_i\}_i$ are unsatisfiable and any polynomial $f(\overline{x},\overline{y})$ with $f(\overline{x},\overline{y}) = 1/Q(\overline{x},\overline{y})$ for $\overline{x} \in \{0,1\}^{2n}$ and $\overline{y} \in \{0,1\}^{2n}$, satisfies that degree of $f(\overline{x},\overline{y})$ is at least $2n$.*

4 Lifting Degree-to-Size 𝕀: Symmetric Instances

In this section we show how to use Nullstellensatz degree lower bounds to obtain size lower bounds on a stronger proof system. In this sense, we "lift" a weak lower bound to a lower bound against a stronger model. This is done using a *gadget* g, or a *lift*, which is simply a substitution in the original hard instance. Namely, given a polynomial $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ we define a new polynomial $f'(\overline{y}) := f(g(x_1),\ldots,g(x_n))$, with $g(x_i) \in \mathbb{F}[\overline{y}]$, for all $i \in [n]$.

Recall the functional lower bound method which is a reduction from algebraic circuit lower bounds to proof complexity lower bounds developed in [FSTW21] shown above in Theorem 1.

4.1 Size Lower Bounds for Symmetric Instances via Lifting

Here we show how to lift the Nullstellensatz degree lower bound in Corollary 27 to size lower bounds. In particular, we show that the lifting used in [FSTW21] on the subset sum $\sum_i x_i - \beta$, applies to *every* unsatisfiable symmetric polynomial.

Henceforth, in this section we will assume $\mathbb{F}[\overline{x}]$ is equipped with some monomial order $\prec$. Unlike [FSTW21] wherein the IPS proof size lower bound argument holds for *any* chosen monomial order, our argument uses monomial orders that respect degree, i.e., $\deg(M) > \deg(N) \Rightarrow M \succ N$. For concreteness, one can consider the graded lexicographic ordering on monomials **grlex** (see Cox, Little and O'Shea [CLO15, Definition 5, page 58]).

4.1.1 roABP-IPS Lower Bounds in Fixed Order

Here we show an exponential lower bound against roABP-IPS$_{\text{LIN}'}$ for any sufficiently low degree symmetric polynomial, where the roABPs are in a *fixed* order of variables. In the next section we extend this to a lower bound for *every* order of variables.

For $\overline{x}, \overline{y}$ variables, with $|\overline{x}| = |\overline{y}| = n$, we use $\overline{x} \circ \overline{y}$ to denote the entry-wise product $(x_1y_1, \ldots, x_ny_n)$. In other words, the *gadget* we use is the mapping

$$x_i \mapsto x_i y_i \,,$$

which substitutes the variable x_i by x_iy_i, for every i. We use $\mathbb{1}_S \in \{0,1\}^n$ to denote the indicator vector for a set S.

We will need the following lemma that bounds from below the number of distinct leading monomials of the set of substitutions in a symmetric polynomial of high enough degree. We need this bound because, unlike [FSTW21], for symmetric polynomials of degree bigger than 1 we do not have a tight degree lower bound of n. We do not attempt to optimise this lower bound, rather show an $2^{\Omega(n)}$ lower bound, whenever $d = \log^{O(1)}(n)$.

Lemma 33. *Let $f(\overline{x})$ be a symmetric polynomial with n variables of degree $d = \log^k(n)$, for some constant k, that has no Boolean roots. Let $g(\overline{x}, \overline{y}) \cdot f(\overline{x} \circ \overline{y}) = 1 \mod \overline{x}^2 - \overline{x}$. Then,*

$$\left|\text{LM}\left(\{\text{ml}(g(\overline{x}, \mathbb{1}_S)) : S \subseteq [n]\}\right)\right| \geq 2^{\Omega(n)} \,. \tag{33.1}$$

Proof: Assume for simplicity that n is even and let

$$\mathcal{D} := \{S \ : \ S \subseteq [n] \text{ and } |S| = n/2\}.$$

We are going to show that $\left|\text{LM}\left(\{\text{ml}(g(\overline{x}, \mathbb{1}_S)) : S \in \mathcal{D}\}\right)\right| \geq 2^{\Omega(n)}$, which is enough to conclude Equation (33.1).

Claim 34. *There are $2^{\Omega(n)}$ many pairwise disjoint sets $S_1, \ldots, S_\ell \subseteq \mathcal{D}$ (with $\ell = 2^{\Omega(n)}$) that induce distinct leading monomials in $\text{ml}(g(\overline{x}, \mathbb{1}_{S_i}))$, in the sense that: $\forall i \neq j \in [\ell], \text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_{S_i}))\right) \neq \text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_{S_j}))\right)$.*

Proof of claim: The idea is to show that most pairs of sets in $\mathcal{D}$ induce distinct leading monomials. More precisely, for any given $S \in \mathcal{D}$ there are only $n^{\log^{O(1)} n}$ many sets $S' \in \mathcal{D}$ that induce the same leading monomial, namely $\text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_S))\right) = \text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_{S'}))\right)$. Since the number of subsets in $\mathcal{D}$ is $2^{\Omega(n)}$ we get that there exists at least $2^{\Omega(n)}/n^{\log^{O(1)} n} = 2^{\Omega(n)}$ sets $S_1, \ldots, S_\ell$ (with $\ell = 2^{\Omega(n)}$) that induce distinct leading monomials $\text{ml}(g(\overline{x}, \mathbb{1}_{S_i}))$. For that purpose, it is sufficient to show that for every set $S \in \mathcal{D}$ there exists a set $\mathcal{L}_S \subseteq \mathcal{D}$, such that

1. $S \in \mathcal{L}_S$; and
2. $|\mathcal{L}_S| = n^{\log^{O(1)} n}$; and
3. if $T \in \mathcal{D} \setminus \mathcal{L}_S$ and $T' \in \mathcal{L}_S$, then $\text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_T))\right) \neq \text{LM}\left(\text{ml}(g(\overline{x}, \mathbb{1}_{T'}))\right)$.

(This is sufficient to conclude the claim because starting from an arbitrary $S \in \mathcal{D}$, we can pick an $S' \in \mathcal{D} \setminus \mathcal{L}_S$ such that S, S' induce distinct leading monomials. After which we pick $S'' \in \mathcal{D} \setminus (\mathcal{L}_S \cup \mathcal{L}_{S'})$ which induces yet another distinct leading monomial. Since the size of each $|\mathcal{L}_S|, |\mathcal{L}_{S'}|, \ldots$ is $n^{\log^{O(1)} n}$ we can continue this process at least $2^{\Omega(n)}/n^{\log^{O(1)} n}$ many times.)

So, let $S \in \mathcal{D}$. By assumption that $g(\overline{x},\overline{y}) \cdot f(\overline{x} \circ \overline{y}) = 1 \mod \overline{x}^2 - \overline{x}$, we have

$$\mathrm{ml}(g(\overline{x},\mathbb{1}_S)) \cdot f(\overline{x} \circ \mathbb{1}_S) = 1 \mod \overline{x}^2 - \overline{x}\,, \tag{34.1}$$

(note that multilinearizing $g(\overline{x},\mathbb{1}_S)$ does not affect the equality, since we work modulo $\overline{x}^2 - \overline{x}$).

Because our lifting turns every variable x_i into $x_i y_i$ we have that $\mathrm{ml}(g(\overline{x},\mathbb{1}_S))$ is a (multilinear symmetric) polynomial that *depends on the variables x_i, for $i \in S$* (that is, each nonzero monomial in this polynomial has only variables x_i, for $i \in S$ [though not necessarily all of such x_i's]). Similarly, $f(\overline{x} \circ \mathbb{1}_S)$ is a (symmetric) polynomial that *depends on the variables x_i, for $i \in S$*. Since $f(\overline{x})$ has no Boolean roots, $f(\overline{x} \circ \overline{y})$ also does not have Boolean roots (if there was a Boolean root for the latter, there was also a Boolean root for the former; note that $x_i y_i \in \{0,1\}$ whenever $x_i, y_i \in \{0,1\}$). This, together with Equation (34.1), mean that the conditions of Corollary 27 are met, so we have

$$|S| - d + 1 \leq \deg(\mathrm{ml}(g(\overline{x},\mathbb{1}_S))) \leq |S|.$$

Since we assumed that our monomial ordering respects degree,

$$|S| - d + 1 \leq \deg(\mathrm{LM}(\mathrm{ml}(g(\overline{x},\mathbb{1}_S)))) \leq |S|. \tag{34.2}$$

Given a set $S' \subseteq [n]$, denote by $\widehat{x}_{S'}$ the *corresponding multilinear monomial* $\prod_{i \in S'} x_i$. And conversely, given a monomial M, denote by S_M its "support", namely, the *corresponding subset of* $[n]$ such that $\widehat{x}_{S_M} = M$.

Denote by M_0 the monomial $\mathrm{LM}(\mathrm{ml}(g(\overline{x},\mathbb{1}_S))$ (for the $S \in \mathcal{D}$ we fixed above). Note that M_0 does not necessarily equal $\widehat{x}_S$, because our degree lower bound in Equation (34.2) is not tight. In other words, S_{M_0} does not necessarily equal S, but rather we only know that M_0 consists of at least $|S| - d + 1$ variables x_i, for $i \in S$ (and no other variables):

$$S_{M_0} \in \left\{ S' \subseteq S \;:\; |S| - d + 1 \leq |S'| \leq |S| \right\}.$$

Note that by construction of the lifting, if $S' \in \mathcal{D}$ (i.e., $|S'| = n/2$) and $\mathrm{LM}(\mathrm{ml}(g(\overline{x},\mathbb{1}_{S'})) = M_0$, then $S' \supseteq S_{M_0}$ (because the only variables in $\mathrm{ml}(g(\overline{x},\mathbb{1}_{S'}))$ are x_i, for $i \in S$). Thus, by Equation (34.2)

$$\left|\left\{ S' \in \mathcal{D} \;:\; S' \supseteq S_{M_0} \right\}\right| \leq \binom{n/2 + d - 1}{d-1} \approx \left(\frac{n/2 + d - 1}{e}\right)^{d-1} \leq n^{\log^c n}$$

for some constant c and sufficiently big n (since $d = \log^k n$, for a constant k).

Note that putting $\mathcal{L}_S := \{S' \in \mathcal{D} \;:\; S' \supseteq S_{M_0}\}$ we obtain an $\mathcal{L}_S$ that meets all three conditions Item 1 to Item 3 above. ■Claim

This concludes the proof of Lemma 33. □

Theorem 35. *Let $f(\overline{x})$ be an unsatisfiable symmetric polynomial with n variables of degree $d = \log^{O(1)} n$. Then, any* roABP-IPS$_{\mathrm{LIN}'}$ *refutation of $f(\overline{x} \circ \overline{y}) = 0$ is of size $2^{\Omega(n)}$, when the variables are ordered such that $\overline{x} < \overline{y}$ (i.e., $\overline{x}$-variables come before $\overline{y}$-variables).*

Proof: This is similar to similar to [FSTW21, Proposition 5.8], that we repeat for convenience.

Let $g(\overline{x},\overline{y})$ be a polynomial such that $g(\overline{x},\overline{y}) \cdot f(\overline{x} \circ \overline{y}) = 1$ over $\overline{x},\overline{y} \in \{0,1\}^n$. Hence,

$$g(\overline{x},\overline{y}) = \frac{1}{f(\overline{x} \circ \overline{y})} \quad \text{over} \quad \overline{x},\overline{y} \in \{0,1\}^n. \tag{35.1}$$

We show that $\dim \mathbf{Coeff}_{\overline{x}|\overline{y}} g \geq 2^{\Omega(n)}$. This will conclude the proof by Lemma 14 which will give the roABP size (width) lower bound and by the functional lower bound reduction in Theorem 1.

First, observe that $f(\overline{x} \circ \overline{y}) = 0$ is unsatisfiable over $\overline{x}, \overline{y} \in \{0,1\}^n$, since $f(\overline{x}) = 0$ is. Thus, the right hand side of Equation (35.1) is defined.

By lower bounding coefficient dimension by the evaluation dimension over the Boolean cube (Theorem 17),

$$\begin{aligned}\dim \mathbf{Coeff}_{\overline{x}|\overline{y}} g &\geq \dim \mathbf{Eval}_{\overline{x}|\overline{y},\{0,1\}} g \\ &= \dim\{g(\overline{x}, \mathbb{1}_S) : S \subseteq [n]\} \\ &\geq \dim\{\mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) : S \subseteq [n]\} \,.\end{aligned}$$

Here we used that dimension is non-increasing under linear maps. For $S \subseteq [n]$, denote by $\overline{x}_S := \{x_i \ : \ i \in S\}$ and note that for $\overline{x} \in \{0,1\}^n$,

$$g(\overline{x}, \mathbb{1}_S) = \frac{1}{f(\overline{x}_S)} \,.$$

It follows that $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))$ is a multilinear polynomial only depending on $\overline{x}|_S$ (Theorem 18), and by its functional behavior it follows from Lemma 25 that $\deg \mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) \in [|S| - d + 1, |S|]$.

Since $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))$ is multilinear we can use Lemma 33 to lower bound the number of distinct leading monomial of $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))$, when S ranges over subsets of $[n]$:

$$\left|\mathrm{LM}\left(\{\mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) : S \subseteq [n]\}\right)\right| \geq 2^{\Omega(n)} \,.$$

Therefore, we can lower bound the dimension of the above space by the number of leading monomials (Theorem 23),

$$\begin{aligned}\dim \mathbf{Coeff}_{\overline{x}|\overline{y}} g &\geq \dim\{\mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) : S \subseteq [n]\} \\ &\geq \left|\mathrm{LM}\left(\{\mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) : S \subseteq [n]\}\right)\right| \\ &\geq 2^{\Omega(n)} \,.\end{aligned}$$

□

4.1.2 roABP-IPS in Any Order Lower Bounds

Here we extend the results of the previous section to any variable order, which will imply lower bounds against roABP-IPS$_{\mathrm{LIN}'}$ of any variable order as well as multilinear formulas IPS. This extends the corresponding results in [FSTW21] to lifting of the subset sum to lifting of every symmetric instance.

Given a symmetric polynomial $f(\overline{q})$ with n variables $q_1, \ldots, q_n$, by Proposition 6 we have

$$f(\overline{q}) := g(y_1/\mathbf{e}_{1,n}(\overline{q}), \ldots, y_n/\mathbf{e}_{n,n}(\overline{q}))$$

for some polynomial $g(\overline{y})$. We now define a polynomial that will embed in itself the lifting from Section 4.1.1 of the symmetric polynomial $f(\overline{q})$ under suitable partial Boolean substitutions. In other words, we define a polynomial over the new variables $\overline{z}, \overline{x}$ such that under suitable Boolean assignments to the $\overline{z}$ variables we obtain the hard polynomial from Theorem 35. For each different such suitable Boolean assignment to $\overline{z}$ we will get an instance that is hard for a different variable ordering, concluding that our instance is hard for any variable ordering.

Consider the polynomial

$$f'(\overline{w}) := g(y_1/\mathbf{e}_{1,m}(\overline{w}), \ldots, y_n/\mathbf{e}_{n,m}(\overline{w})) \tag{35.2}$$

for $m = \binom{2n}{2}$ and $\overline{w} = \{w_{i,j}\}_{i<j\in[2n]}$. We now apply a similar gadget to [FSTW21], defined by the mapping

$$w_{i,j} \mapsto z_{i,j} x_i x_j \,,$$

which substitutes the m variable $w_{i,j}$ by $m + 2n$ variables $\{z_{i,j}\}_{i<j\in[2n]}$, $x_1, \ldots, x_{2n}$:

$$f^\star(\overline{z}, \overline{x}) := g(y_1/(\mathbf{e}_{1,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}, \ldots, y_n/(\mathbf{e}_{n,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}) \,, \tag{35.3}$$

where $(\mathbf{e}_{j,m}(\overline{w}))_{w_{i,j}\mapsto z_{i,j}x_ix_j}$ means that we apply the lifting $w_{i,j} \mapsto z_{i,j}x_ix_j$ to the $\overline{w}$ variables.

Let $f \in \mathbb{F}[\overline{x}, \overline{y}, \overline{z}]$. We denote by $f_{\overline{z}}$ the polynomial f considered as a polynomial in $\mathbb{F}[\overline{z}][\overline{x}, \overline{y}]$, namely as a polynomial whose indeterminates are $\overline{x}$, $\overline{y}$ and whose scalars are from the ring $\mathbb{F}[\overline{z}]$. We will consider the dimension of a (coefficient) matrix when the entries are taken from the ring $\mathbb{F}[\overline{z}]$, and where the dimension is considered over the field of rational functions $\mathbb{F}(\overline{z})$. Note that for any $\overline{\alpha} \in \mathbb{F}^{|\overline{z}|}$ we have that $f_{\overline{\alpha}}(\overline{x}, \overline{y}) = f(\overline{x}, \overline{y}, \overline{\alpha}) \in \mathbb{F}[\overline{x}, \overline{y}]$. We use the following simple lemma:

Lemma 36 ([FSTW21])**.** *Let $f \in \mathbb{F}[\overline{x}, \overline{y}, \overline{z}]$. Then for any $\overline{\alpha} \in \mathbb{F}^{|\overline{z}|}$*

$$\dim_{\mathbb{F}(\overline{z})} \mathbf{Coeff}_{\overline{x}|\overline{y}} f_{\overline{z}}(\overline{x}, \overline{y}) \geq \dim_{\mathbb{F}} \mathbf{Coeff}_{\overline{x}|\overline{y}} f_{\overline{\alpha}}(\overline{x}, \overline{y}) \,.$$

Proposition 37. *Let $n \geq 1$, $m = \binom{n}{2}$, and $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) > \max(2^{4n+2m}, n^d)$. Let $f \in \mathbb{F}[\overline{q}]$ be a symmetric polynomial with n variables of degree $d = O(\log n)$, and $f^\star(\overline{z}, \overline{x})$ be as in Equation (35.3). Suppose that $g \in \mathbb{F}[z_1, \ldots, z_m, x_1, \ldots, x_{2n}]$ be a polynomial such that*

$$g(\overline{z}, \overline{x}) = \frac{1}{f^\star(\overline{z}, \overline{x}) - \beta} \,,$$

for $\overline{z} \in \{0,1\}^{\binom{2n}{2}}$ and $\overline{x} \in \{0,1\}^{2n}$, and $\beta \in \mathbb{F}$ that makes $f^\star(\overline{z}, \overline{x}) - \beta = 0$ as well as $f(\overline{q}) - \beta = 0$ each unsatisfiable over Boolean values.[7] Let $g_{\overline{z}}$ denote f as a polynomial in $\mathbb{F}[\overline{z}][\overline{x}]$. Then, for any partition $\overline{x} = (\overline{u}, \overline{v})$ with $|\overline{u}| = |\overline{v}| = n$,

$$\dim_{\mathbb{F}(\overline{z})} \mathbf{Coeff}_{\overline{u}|\overline{v}} g_{\overline{z}} \geq 2^{\Omega(n)} \,.$$

Proof: We proceed as in [FSTW21] to embed $\frac{1}{f(\overline{u}\circ\overline{v})-\beta}$ in this instance via a restriction of $\overline{z}$. Define the $\overline{z}$-evaluation $\overline{\alpha} \in \{0,1\}^{\binom{2n}{2}}$ to restrict g to sum over those x_ix_j in the natural matching between $\overline{u}$ an $\overline{v}$, so that

$$\alpha_{ij} = \begin{cases} 1 & x_i = u_k, x_j = v_k \\ 0 & \text{else} \end{cases} \,.$$

It follows that $g(\overline{u}, \overline{v}, \overline{\alpha}) = \frac{1}{f(\overline{u}\circ\overline{v})-\beta}$ for $\overline{u}, \overline{v} \in \{0,1\}^n$. Thus, by using the our lower bound for a fixed partition (Theorem 35) and the relation between the coefficient dimension in $f_{\overline{z}}$ versus $f_{\overline{\alpha}}$ (Lemma 36),

$$\begin{aligned} \dim_{\mathbb{F}(\overline{z})} \mathbf{Coeff}_{\overline{u}|\overline{v}} g_{\overline{z}}(\overline{u}, \overline{v}) &\geq \dim_{\mathbb{F}} \mathbf{Coeff}_{\overline{u}|\overline{v}} g_{\overline{\alpha}}(\overline{u}, \overline{v}) \\ &\geq 2^{\Omega(n)} \,. \end{aligned}$$

□

[7] Observe that when the characteristic is sufficiently large there always exists a β that makes both $f^\star(\overline{z}, \overline{x}) - \beta = 0$ and $f(\overline{q}) - \beta = 0$ unsatisfiable over Boolean values for the variables $\overline{z}, \overline{x}, \overline{q}$.

Corollary 38. *Let $n \geq 1$, $m = \binom{n}{2}$, and $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) > \max(2^{4n+2m}, n^d)$. Let $f \in \mathbb{F}[\overline{q}]$ be a symmetric polynomial with n variables of degree $d = O(\log n)$, and $f^\star(\overline{z}, \overline{x})$ be as in Equation (35.3). Let $\beta \in \mathbb{F}$ be such that $f^\star(\overline{z}, \overline{x}) - \beta = 0$ and $f(\overline{q}) - \beta = 0$ are each unsatisfiable over Boolean values. Then, any* roABP-IPS$_{\mathrm{LIN}'}$ *refutation (in any variable order) of $f^\star(\overline{z}, \overline{x}) - \beta = 0$ requires $2^{\Omega(n)}$-size.*

Proof: Consider the polynomial $g \in \mathbb{F}[x_1, \ldots, x_{2n}, z_1, \ldots, z_{\binom{2n}{2}}]$ such that

$$g(\overline{z}, \overline{x}) = \frac{1}{f^\star(\overline{z}, \overline{x}) - \beta} ,$$

for $\overline{x} \in \{0,1\}^{2n}$, $\overline{z} \in \{0,1\}^{\binom{2n}{2}}$.

We continue similar to the proof of [FSTW21, Corollary 5.14, part 1]. Suppose that $f(\overline{x}, \overline{z})$ is computable by a width-r roABP in *some* variable order. By pushing the $\overline{z}$ variables into the fraction field, it follows that $f_{\overline{z}}$ (f as a polynomial in $\mathbb{F}(\overline{z})[\overline{x}]$) is also computable by a width-r roABP over $\mathbb{F}(\overline{z})$ in the induced variable order on $\overline{x}$ (Fact 15). By combining the coefficient dimension lower bound of Proposition 37 with its relation to roABPs (Lemma 14), and by splitting $\overline{x}$ in half along its variable order we obtain that any roABP computing g requires width $\geq 2^n$ in any variable order. The roABP-IPS$_{\mathrm{LIN}'}$ lower bound follows immediately from this functional lower bound for g along with our reduction (Theorem 1). □

5 Lifting Degree-to-Size II: Vector Invariant Polynomials

In this section, we will prove an roABP-IPS$_{\mathrm{LIN}}$ size lower bound for the vector-invariant-inspired hard instance.

In [FSTW21], roABP-IPS$_{\mathrm{LIN}}$ size lower bound was proved for a *lifted version* of the subset sum instance. In a similar spirit, one may try to lift the polynomial $Q(\overline{x}, \overline{y})$ from Equation (27.2). This does not seem very straightforward, because unlike the subset sum instance, which is linear, here we have a large degree instance. Fortunately, to obtain an roABP-IPS$_{\mathrm{LIN}}$ size lower bound in the order $\overline{x} < \overline{y}$ we do not need any lift (in Section 5.2 we do need to use a lift to get our result to work for any order). We can prove a lower bound for $Q(\overline{x}, \overline{y})$ directly. Moreover, we obtain a lower bound that holds over all fields of characteristic greater than or equal to 5. No such roABP-IPS$_{\mathrm{LIN}}$ size lower bound was known over small characteristic.

On the other hand, the polynomial $Q(\overline{x}, \overline{y})$ is not computable by an roABP in this order. In fact, provably an roABP in the order $\overline{x} < \overline{y}$ requires size $\exp(\Omega(n))$ to compute $Q(\overline{x}, \overline{y})$.

5.1 roABP-IPS$_{\mathrm{LIN}}$ Size Lower Bound for $Q(\overline{x}, \overline{y})$

We will now state our main theorem in this section.

Theorem 39. *Let $\mathbb{F}$ be a field of characteristic ≥ 5 and let $\beta \notin \{-1, 0, 1\}$. Then, $Q(\overline{x}, \overline{y})$, $\{x_i^2 - x_i\}_i$, and $\{y_i^2 - y_i\}_i$ is unsatisfiable and any roABP-IPS$_{LIN}$ refutation in order of the variables where $\overline{x}$ precedes $\overline{y}$ requires size* $\exp(\Omega(n))$.

Characterising the monomials of degree $2n$ in $f(\overline{x}, \overline{y})$. In Section 3.2 we computed the coefficient of one of the degree $2n$ monomials of $f(\overline{x}, \overline{y})$, namely the coefficient of $\overline{x}_S \cdot \overline{y}_T$, where $S = \{i \in [2n] \mid i \text{ odd}\}$ and $T = [2n] \setminus S$. Next, we will use the calculations from Lemma 30 to obtain the coefficients of the monomials of degree $2n$ in $f(\overline{x}, \overline{y})$. We first start with some notation.

For $\sigma \in \{0,1\}^n$, let $s_{\sigma,i} = 2i - 1$ if $\sigma_i = 0$ and $s_{\sigma,i} = 2i$ if $\sigma_i = 1$, for $i \in [n]$. And let $S_\sigma = \cup_{i\in[n]}\{s_{\sigma,i}\} \subset [2n]$ (and accordingly, $\overline{S_\sigma} := [2n] \setminus S_\sigma$). For example, if $\sigma = 0^n$, then $S_\sigma = S$ and $\overline{S_\sigma} = T$.

The monomial $\overline{x}_{S_\sigma}\overline{y}_{\overline{S_\sigma}}$ is defined by picking the x-variable from the first column of M_i if $\sigma_i = 0$ and from the second column of M_i if $\sigma_i = 1$, where M_i is an defined in Item 3, and then picking the y-variables from the *other* columns of each matrix. For example: if $\sigma = (0,1,0)$, then $\overline{x}_{S_\sigma}\overline{y}_{\overline{S_\sigma}} = x_1y_2x_4y_3x_5y_6$.

We now prove some additional properties of $f(\overline{x},\overline{y})$, which will help us with the roABP-IPS$_{\text{LIN}}$ size lower bound.

Lemma 40. *The polynomial $f(\overline{x},\overline{y})$ has the following properties over the Boolean cube.*

1. *For any odd $j \in [2n]$, let ϕ_j be the mapping $x_j \hookrightarrow x_j, x_{j+1} \hookrightarrow x_{j+1}, y_j \hookrightarrow x_j + y_j$, and $y_j \hookrightarrow x_{j+1} + y_{j+1}$. It leaves all the other variables unchanged. Then, $\phi_j(f(\overline{x},\overline{y})) = f(\overline{x},\overline{y})$ over the Boolean cube for any odd $j \in [2n]$.*
2. *$f(\overline{x},\overline{y})$ has 2^n monomials of degree $2n$ with non-zero coefficients. Moreover, for every $\sigma \in \{0,1\}^n$, the coefficient of $\overline{x}_{S_\sigma}\overline{y}_{\overline{S_\sigma}}$ in $f(\overline{x},\overline{y})$ is either $\frac{1}{\beta(1-\beta)}$ or $\frac{1}{\beta(1+\beta)}$.*
3. *If $S \subseteq [2n]$ and $0 < |S| < n$, then for any $T \subseteq [2n]$, the coefficient of $\overline{x}_S\overline{y}_T$ is equal to 0 and the coefficient of $\overline{x}_T\overline{y}_S$ is equal to 0 in $f(\overline{x},\overline{y})$.*
4. *There are no other monomials of degree $2n$ that have non-zero coefficients in $f(\overline{x},\overline{y})$.*

Let us first prove Theorem 39 assuming this lemma.

Proof of Theorem 39. It is easy to see that $Q(\overline{x},\overline{y})$, $\{x_i^2 - x_i\}_i$, and $\{y_i^2 - y_i\}_i$ are unsatisfiable, as long as $\beta > 2$. Now let $[f(\overline{x},\overline{y})]_{2n}$ denote the degree $2n$ slice of the polynomial $f(\overline{x},\overline{y})$. We now get the following inequalities.

$$\begin{aligned}\dim \text{Coeff}_{\overline{x}|\overline{y}}(f(\overline{x},\overline{y})) &\geq \dim \text{Coeff}_{\overline{x}|\overline{y}}([f(\overline{x},\overline{y})]_{2n}) \\ &\geq \left|\left\{\overline{x}_{S_\sigma} \cdot \overline{y}_{\overline{S_\sigma}} \mid \sigma \in \{0,1\}^n\right\}\right| \\ &= 2^n \end{aligned} \tag{40.1}$$

Here, the first inequality comes from the fact that the overall coefficient dimension is at least as much as that of the degree $2n$ slice. The second inequality follows from Parts 2, 3, and 4 of Lemma 40.

The final equality follows from Part 2 in Lemma 40. The main observation is that as long as $\mathbb{F}$ has characteristic greater than or equal to 5, all the coefficients of the monomials in the set $\left\{\overline{x}_{S_\sigma} \cdot \overline{y}_{\overline{S_\sigma}} \mid \sigma \in \{0,1\}^n\right\}$ are non-zero.

To conclude, note that the lower bound of 2^n on the coefficient dimension of $f(\overline{x},\overline{y})$ implies that $f(\overline{x},\overline{y})$ requires width 2^n to be computed as an roABP in the order $\overline{x} < \overline{y}$ (Lemma 14). □

Now, we prove Lemma 40.

Proof of Lemma 40.
Part 1: Over the Boolean hypercube, $f(\overline{x},\overline{y}) = 1/Q(\overline{x},\overline{y})$. Hence, we get the following over the Boolean hypercube.

$$\phi_j(f(\overline{x},\overline{y})) = \phi_j\left(\frac{1}{\left(\prod_{i\in[2n],i:\text{ odd}} x_iy_{i+1} - y_ix_{i+1}\right) - \beta}\right) = \frac{1}{\left(\phi_j\left(\prod_{i\in[2n],i:\text{ odd}} x_iy_{i+1} - y_ix_{i+1}\right)\right) - \beta}$$

As $\phi_j(x_jy_{j+1} - y_jx_{j+1}) = x_jy_{j+1} - y_jx_{j+1}$ and as ϕ_j keeps all other terms unchanged, we get that

$$\frac{1}{\left(\phi_j\left(\prod_{i\in[2n],i:\text{ odd}} x_iy_{i+1} - y_ix_{i+1}\right)\right) - \beta} = \frac{1}{\prod_{i\in[2n],i:\text{ odd}}(x_iy_{i+1} - y_ix_{i+1}) - \beta} = \frac{1}{Q(\overline{x},\overline{y})} = f(\overline{x},\overline{y})$$

Part 2: This is similar to the proof of Lemma 30. In fact, the computations for Terms 1, 3, and 4 remain exactly the same as before. The only thing that is different is the computation for Term 2.

We will say that $\sigma \in \{0,1\}^n$ is odd if it has odd number of 1s and even otherwise. For example, in Lemma 30, $\sigma = 0^n$ and hence it was even. Note that, when σ is even, then Term 2 gives a coefficient of $\frac{1}{1-\beta}$. Hence, in this case, the coefficient of $\overline{x}_{S_\sigma} \cdot \overline{y}_{\overline{S_\sigma}}$ is the same as the coefficient of $\overline{x}_S \cdot \overline{y}_T$. That is, it is $\frac{1}{\beta(1-\beta)}$. On the other hand, if σ is odd, then Term 2 becomes $\frac{1}{-1-\beta}$. So, in this case, the coefficient of $\overline{x}_{S_\sigma} \cdot \overline{y}_{\overline{S_\sigma}}$ is $\frac{1}{\beta} + \frac{1}{-1-\beta}$. This is equal to $\frac{1}{\beta(1+\beta)}$.

Part 3: Let us rewrite $f(\overline{x},\overline{y})$ as follows.

$$f(\overline{x},\overline{y}) = \sum_{m:\text{ monomial in } x \text{ variables}} f_m(\overline{y}) \cdot m = \sum_{U\subseteq[2n]} f_U(\overline{y})\overline{x}_U\,.$$

Here, we use the Boolean axioms for simplification to get the second equality. First, observe that for $U = \emptyset$, $f_\emptyset(\overline{y}) = \frac{1}{-\beta}$ by using the fact that $f(\overline{x},\overline{y}) = 1/Q(\overline{x},\overline{y})$.

Now, we will prove the statement by induction on the size of U. For $|U| = 1$,

$$\begin{aligned}
\text{Coeff}_{x_i}(f(\overline{x},\overline{y}) &= \text{Coeff}_{x_i}\left(\frac{1}{Q(\overline{x},\overline{y})}\right)\\
\text{Coeff}_{x_i}\left(f(\overline{x},\overline{y})\mid_{x_j=0\forall j\neq i}\right) &= \text{Coeff}_{x_i}\left(\frac{1}{Q(\overline{x},\overline{y})}\mid_{x_j=0\forall j\neq i}\right)\\
f_{x_i}(\overline{y})x_1 + f_\emptyset(\overline{y}) &= \frac{1}{-\beta}\,.
\end{aligned}$$

But we saw that $f_\emptyset(\overline{y}) = \frac{1}{-\beta}$, hence $f_{x_i}(\overline{y}) = 0$.

For the inductive case, we have a very similar argument. Let $|U| < n$.

$$\begin{aligned}
\text{Coeff}_{\overline{x}_U}(f(\overline{x},\overline{y})) &= \text{Coeff}_{x_U}\left(\frac{1}{Q(\overline{x},\overline{y})}\right)\\
\text{Coeff}_{X_U}\left(f(\overline{x},\overline{y})\mid_{x_j=0\forall j\notin U}\right) &= \text{Coeff}_{\overline{x}_U}\left(\frac{1}{Q(\overline{x},\overline{y})}\mid_{x_j=0\forall j\notin U}\right)\\
\sum_{V\subseteq U} f_V(\overline{y})\overline{x}_V &= \frac{1}{-\beta}\,.
\end{aligned}$$

By induction hypothesis, and by using the fact that $f_\emptyset(\overline{y}) = \frac{1}{-\beta}$, we get that $f_U(\overline{y}) = 0$. By a similar argument, we can also prove that the coefficient of $\overline{x}_T\overline{y}_S$ is equal to 0. This finishes the proof of Part 3.

Part 4: Assume for the sake of contradiction there is a monomial of degree $2n$ in $f(\overline{x},\overline{y})$ that does not have the structure as described in Part 2. Then it must contain an index $i \in [2n]$ such that the monomial contains x_i as well as y_i in it, that is, the monomial looks like this $x_iy_i\overline{x}_S\overline{y}_T$, where $|S| + |T| + 2 = 2n$.

If either $|S \cup \{i\}| < n$ or $|T \cup \{i\}| < n$, then by Part 3 above, we know that the coefficient of the monomial will be zero.

Now suppose that $|S \cup \{i\}| = n$ and $|T \cup \{i\}| = n$. By Part 1 above, we know that the set of invariants of $Q(\overline{x}, \overline{y})$ and that of $f(\overline{x}, \overline{y})$ are the same. Let us apply the map ϕ_i, that is $x_i \hookrightarrow x_i, y_i \hookrightarrow x_i + y_i, x_{i+1} \hookrightarrow x_{i+1}, y_{i+1} \hookrightarrow x_{i+1} + y_{i+1}$. This gives us $x_i(x_i + y_i)\phi_i(\overline{x}_S\overline{y}_T)$.

Consider the case when $i + 1 \notin T$. Then, we get $x_i(x_i + y_i)\phi_i(\overline{x}_S\overline{y}_T) = x_i^2\overline{x}_S\overline{y}_T + x_iy_i\overline{x}_S\overline{y}_T$. So, if the coefficient of $x_iy_i\overline{x}_S\overline{y}_T$ is non-zero, then after applying the map, the coefficients of the resulting monomials are also non-zero. Notice that, we are working modulo the Boolean axioms, which means, the expression above will simplify to $x_i\overline{x}_S\overline{y}_T + x_iy_i\overline{x}_S\overline{y}_T$. Now notice that by Part 3 above, the coefficient of the monomial $x_i\overline{x}_S\overline{y}_T$ must be zero, as $|T| < n$, which is a contradiction.

On the other hand, if $i + 1 \in T$, then $x_i(x_i + y_i)\phi_i(\overline{x}_S\overline{y}_T) = x_i(x_i + y_i)\overline{x}_S\overline{y}_{T\setminus\{i+1\}}(x_{i+1} + y_{i+1})$. After expanding, we see that one of the resulting monomials is again $x_i\overline{x}_S\overline{y}_T$. So, if $x_iy_i\overline{x}_S\overline{y}_T$ has a non-zero coefficient, then so should this monomial. But by Part 3 above, we know that this monomial must have coefficient 0, which gives a contraction. □

5.2 Coefficient Dimension in any Variable Order

In the previous section we proved a lower bound on the coefficient dimension in the $\overline{x}|\overline{y}$ variable partition. In this section we extend that result to give bounds on the coefficient dimension in any order.

To achieve this, we use a similar lifting as before. Namely, we lift the instance to a new polynomial, $P(\overline{u}, \overline{z})$, using the new auxiliary variables $\overline{z}$. The polynomial $P(\overline{u}, \overline{z})$ has the property that given a partition of $\overline{u}$ variables into two equal parts, there exists a 0/1 assignment to the auxiliary variables that reveals a hard *planted* instance of Q (from our previous section) inside P. Below, we will start with the description of the hard instance.

Hard instance. Let $\overline{u} = \{u_1, u_2, \ldots, u_{4n}\}$, let $m = \binom{4n}{4}$, and $\overline{z} = \{z_1, z_2, \ldots, z_m\}$. Let $P(\overline{u}, \overline{z}) \in \mathbb{F}[\overline{u}, \overline{z}]$ be defined as follows.

$$P(\overline{u}, \overline{z}) = \left(\prod_{i<j<k<\ell \in [4n]} 1 - z_{i,j,k,\ell} + z_{i,j,k,\ell}(u_iu_\ell - u_ju_k) \right) - \beta$$

We will prove the following theorem about this polynomial.

Theorem 41. *Let $\mathbb{F}$ be a field of characteristic ≥ 5 and let $P(\overline{u}, \overline{z})$ be as defined above. Then $P(\overline{u}, \overline{z}), \{u_i^2 - u_i\}_i, \{z_i^2 - z_i\}_i$ is unsatisfiable as long as $\beta \notin \{-1, 0, 1\}$. And any roABP-IPS$_{LIN}$ refutation of this instance requires $\exp(\Omega(n))$ size. Any multilinear-formula-IPS requires $n^{\Omega(\log n)}$ size and any product-depth-Δ multilinear-formula-IPS requires size $n^{\Omega((n/\log n)^{1/\Delta}/\Delta^2)}$.*

Remark 42. *We note the following salient points regarding the result.*

- *Let N be the total number of variables in $P(\overline{u}, \overline{z})$. Then, $N = O(m) = O(\binom{4n}{4}) = O(n^4)$. Hence, in terms of N, the roABP size lower bound is $2^{\Omega(N^{1/4})}$.*
- *The polynomial $P(\overline{u}, \overline{z})$ is not multilinear. It is however a relatively easy-to-compute polynomial. Namely, it has a product-depth 2 formula of polynomial size.*
- *The lower bound holds over all characteristics (as long as it is ≥ 5). No IPS lower bounds over finite fields were known before.*

The following technical lemma is used to prove the above theorem.

Lemma 43. *Let $\mathbb{F}$ be a field with characteristic ≥ 5, let $\beta \notin \{-1, 0, 1\}$, and let $g(\overline{u}, \overline{z}) \in \mathbb{F}[\overline{u}, \overline{z}]$ be a polynomial such that*

$$g(\overline{u}, \overline{z}) = \frac{1}{P(\overline{u}, \overline{z})},$$

for $\overline{u} \in \{0,1\}^{4n}$ and $\overline{z} \in \{0,1\}^m$. Let $g_{\overline{z}}$ denote the polynomial in $\mathbb{F}[\overline{z}][\overline{u}]$. Then for any partition $\overline{u} = (\overline{v}, \overline{w})$ such that $|\overline{v}| = |\overline{w}| = 2n$

$$\dim_{\mathbb{F}[\overline{z}]} \mathrm{Coeff}_{\overline{v}|\overline{w}}(g_{\overline{z}}) \geq 2^n$$

We will first prove Theorem 41 using Lemma 43.

Proof of Theorem 41. *roABP* lower bound: Assume that $g(\overline{u}, \overline{z})$ is computable by width-r roABP in some order of variables. By *pushing* the $\overline{z}$ variables into the fraction field, $g_{\overline{z}} \in \mathbb{F}[\overline{z}][\overline{u}]$ is also computable by width-r roABP over $\mathbb{F}[\overline{z}]$ in the induced order of the variables in $\overline{u}$. (This follows from Fact 15), which states that roABPs are closed under variable substitutions.)

Now, by splitting the variables $\overline{u}$ in two halves in this order, say into $\overline{v}, \overline{w}$, we obtain a lower bound on the coefficient dimension of the roABP with partition $\overline{v}|\overline{w}$ using Lemma 43. To conclude, note that the lower bound of 2^n on the coefficient dimension implies a width 2^n lower bound for the roABP (Lemma 14).

The lower bounds stated in Theorem 41 for multilinear formulas and constant-depth multilinear formulas follow from our lower bound on the coefficient dimension and the results of Raz [Raz09] and Raz-Yehudayoff [RY09]. □

We now conclude this section with the proof of Lemma 43.

Proof of Lemma 43. Given a partition of $\overline{u}$ into two equal parts $(\overline{v}, \overline{w})$, consider the polynomial $g(\overline{v}, \overline{w}, \overline{z})$. We would like to bound the coefficient dimension of $g(\overline{v}, \overline{w}, \overline{z})$ for partition $\overline{v}|\overline{w}$. For this, we will first view $g \in \mathbb{F}[\overline{z}][\overline{v}, \overline{w}]$ and try to bound the coefficient dimension in the field of rational functions $\mathbb{F}[\overline{z}]$. Following the notation from [FSTW21] (Lemma 5.12), we will denote this quantity by $\dim_{\mathbb{F}[\overline{z}]} \mathrm{Coeff}_{\overline{v}|\overline{w}}\ g_{\overline{z}}(\overline{v}, \overline{w})$.

Another way to bound the coefficient dimension is to consider $\overline{\alpha} \in \{0,1\}^m$ and evaluate $\overline{z} \leftarrow \overline{\alpha}$ such that $g(\overline{v}, \overline{w}, \overline{\alpha}) \in \mathbb{F}[\overline{v}, \overline{w}]$. Thus, study the coefficient dimension over $\mathbb{F}$. We will denote this quantity by $\dim_{\mathbb{F}} \mathrm{Coeff}_{\overline{v}|\overline{w}}\ g_{\overline{\alpha}}(\overline{v}, \overline{w})$.

It is known that $\dim_{\mathbb{F}[\overline{z}]} \mathrm{Coeff}_{\overline{v}|\overline{w}}\ g_{\overline{z}}(\overline{v}, \overline{w}) \geq \dim_{\mathbb{F}} \mathrm{Coeff}_{\overline{v}|\overline{w}}\ g_{\overline{\alpha}}(\overline{v}, \overline{w})$. Therefore, it will suffice to lower bound the latter for an appropriate evaluation $\overline{\alpha}$ of the $\overline{z}$ variables.

Specifically, we will design $\overline{z}$-evaluation, that is, $\overline{\alpha}$ as follows.

$$\alpha_{i,j,k,\ell} = \begin{cases} 1 & \text{if } i \in [2n], i \text{ odd }, \\ & u_i = v_i, u_j = v_{i+1}, \\ & u_k = w_i, u_\ell = w_{i+1} \\ 0 & \text{otherwise} \end{cases}$$

For this evaluation, notice that when $z_{i,j,k,\ell} = 1$, we have that $i \in [2n]$ and is odd. Moreover, we get that the corresponding term in $P(\overline{v}, \overline{w}, \overline{\alpha})$ becomes $(1 - 1 + 1 \cdot (v_i w_{i+1} - w_i v_{i+1})) = (v_i w_{i+1} - w_i v_{i+1})$. On the other hand, when $z_{i,j,k,\ell} = 0$, the corresponding term just becomes $(1 - 0 + 0) = 1$. Therefore, we get that

$$g(\overline{v}, \overline{w}, \overline{\alpha}) = \frac{1}{\left(\prod_{i \in [2n], i \text{ odd}} (v_i w_{i+1} - w_i v_{i+1})\right) - \beta} = \frac{1}{Q(\overline{v}, \overline{w})} = f(\overline{v}, \overline{w})$$

for $\overline{v}, \overline{w} \in \{0,1\}^{2n}$. Now, using Equation (40.1), we get the lower bound of 2^n on the $\dim_{\mathbb{F}} \mathrm{Coeff}_{\overline{v}|\overline{w}}\ g_{\overline{\alpha}}(\overline{v}, \overline{w})$, which concludes this proof. □

6 Lifting Degree-to-Size III: Lower Bounds against Constant-Depth Refutations

In this section we prove lower bounds for constant-depth IPS, that is, IPS refutations that are computable by constant-depth algebraic circuits. The main theorem of this section is the following.

Theorem 44. *Let n, Δ and δ be positive integers, and assume that* $\mathrm{char}(\mathbb{F}) = 0$. *Let g be a polynomial of individual degree at most δ so that it agrees with*

$$\frac{1}{\sum_{i,j,k,\ell \in [n]} z_{ijk\ell} x_i x_j x_k x_\ell - \beta} \quad \text{over Boolean values.}$$

Then any circuit of product-depth at most Δ computing g has size at least

$$n^{\Omega\left(\frac{(\log n)^{2^{1-2\Delta}}}{\delta^{2\cdot\Delta}}\right)}.$$

Using the Theorem 1 this gives a constant-depth IPS refutation lower bound (with the same parameters and field) for the instance $\sum_{i,j,k,\ell \in [n]} z_{ijk\ell} x_i x_j x_k x_\ell - \beta$.

Previously, [GHT22] proved lower bounds for the same instance for multilinear refutations, i.e., in the case where $\delta = 1$. Our result improves on that work in two ways. Firstly, when $\delta = 1$, the result improves slightly the exponent in the expression (from $1/(2^{2\Delta} - 1)$ to $1/2^{2\Delta - 1}$). Secondly, and more importantly, the result gives lower bounds for larger individual degrees.

The lower bound shows a natural *trade-off* between the depth and individual degree of refutations. It gives superpolynomial lower bounds for refutations of individual degree $\mathsf{poly}(\log \log n)$ for any constant depth refutations, and for any fixed depth we get lower bounds up to individual degree $\log^\epsilon n$ for some small ϵ depending on the depth.

Our hard instance does have a small constant-depth refutation, but of high individual degree. This is obtained by substituting the gadget $z_{ijk\ell} x_i x_j x_k x_\ell$ to the small depth-3 refutations of the standard instance of knapsack $(\sum_i x_i - \beta)$ given in [FSTW21]. The obtained refutation is a polynomial of individual degree $O(n^3)$.

To prove our lower bound for the bounded individual degree refutations, we employ the framework put forward by Amireddy *et al.* in [AGK+23] to prove constant-depth algebraic circuit lower bounds. They show that the lower bounds for constant-depth algebraic circuits originally proved in [LST21] can also be obtained more directly via homogeneous constant-depth circuit lower bounds without going through the final hardness escalation step through set-multilinear circuits that was used in [LST21].

Amireddy *et al.* [AGK+23] suggest that their approach could also be used to prove functional lower bounds for constant-depth algebraic circuits. This seems viable since their framework puts leaner requirements for the polynomials than that of [LST21]. Our work achieves this goal, showing how to modify their framework to obtain Theorem 44.

The rest of this section is organized as follows. First, we recall the framework of [AGK+23], and discuss some modifications needed to prove our functional lower bounds. Then we recall an intermediate hard instance used in [GHT22] and prove lower bounds for that instance for the affine projections of partial APP complexity measure used in [AGK+23] (while in [GHT22] a different measure was used). After this, we are ready to prove our main lower bound for this section.

6.1 Lower Bounds via Affine Projections of Partials

We introduce some notation that matches and extends that of [AGK+23]. For any non-negative integers n and k we denote by $M(n, k)$ the number of distinct monomials of degree exactly k in n

variables, and by $M_{\leq}(n,k)$ the number of distinct monomials of degree at most k in n variables. The following lemma gives useful approximations for these quantities and is shown in [AGK+23, Lemma 2.2] (the only new information is that in the first item, the upper bound also applies to $M_{\leq}(n,k)$).

Lemma 45. *Let $n \geq k \geq \ell$ and m be positive integers. Then,*

(i) $(n/k)^k \leq M(n,k) \leq M_{\leq}(n,k) \leq (6n/k)^k$;

(ii) $(n/2k)^\ell \leq \frac{M(n,k+\ell)}{M(n,k)} \leq (2n/k)^\ell$;

(iii) $\frac{M(\ell,m)}{M(k,m)} \geq (\ell/k)^m$.

The following quantity is crucial for the analysis of [AGK+23]. Let $d_1, \ldots, d_t$ be non-negative integers such that $d := \sum_{i\in[t]} d_i \geq 1$, and let $k < d$. Then define

$$\mathrm{residue}_k(d_1,\ldots,d_t) := \frac{1}{2} \min_{k_1,\ldots,k_t \in \mathbb{Z}} \sum_{j\in[t]} \left| k_j - \frac{k}{d}\cdot d_j \right|$$

For constants a, b we write $a \approx_c b$ if $a \in [b/c, b]$ and $a \approx b$ if $a \approx_c b$ for some unspecified constant c.

6.1.1 The APP Measure

Let us now recall the *Affine Projections of Partials* (APP) measure that [AGK+23] used to prove their lower bounds. They actually considered in addition another measure, the *Shifted Partials* measure, but APP seems to be much more amenable to proving functional lower bounds than the Shifted Partials measure, and thus we consider here exclusively the APP measure.

To define the measure, let k and n_0 be non-negative integers, let P be a polynomial in $\mathbb{F}[x_1,\ldots,x_n]$, and let $L = \langle \ell_1, \ldots, \ell_n \rangle$ be a tuple of affine forms over the variables $z_1, \ldots, z_{n_0}$ (an affine form is a linear form $\sum_i \alpha_i x_i + a$, for some scalars α_i and a). We denote π_L the affine projection that maps each x_i to ℓ_i. Now define

$$\mathsf{APP}_{k,n_0}(P) := \max_L \dim \left\langle \pi_L \left(\partial^k P \right) \right\rangle .$$

The first key lemma in [AGK+23] is the following structural lemma about the space of partial derivatives. It shows that the space can be realized as suitable shifts of partial derivatives of smaller arities.

Lemma 46 ([AGK+23])**.** *Let n and t be positive integers and $Q_1, \ldots, Q_t$ be non-constant, homogeneous polynomials in $\mathbb{F}[x_1,\ldots,x_n]$ with degrees $d_1,\ldots,d_t$, respectively. Let $d := \deg(Q_1 \cdots Q_t) = \sum_{i=1}^t d_i$ and $k < d$ be a non-negative integer. Then*

$$\left\langle \partial^k (Q_1 \cdots Q_t) \right\rangle \subseteq \sum_{\substack{S\subseteq[t], k_0, \ell_0 \\ k_0 + \frac{k}{d-k}\cdot\ell_0 \leq k - \mathrm{residue}_k(d_1,\ldots,d_t)}} \left\langle \overline{x}^{\ell_0} \cdot \partial^{k_0} \left(\prod_{i\in S} Q_i \right) \right\rangle .$$

The lemma above is then used to prove the following upper bound for the APP measure.

Lemma 47 ([AGK+23]). *Let $Q = Q_1 \cdots Q_t$ be a homogeneous polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ of degree $d = d_1 + \ldots d_t \geq 1$, where Q_i is homogeneous and $d_i := \deg(Q_i)$ for all $i \in [t]$. Then for any non-negative integers $k < d$ and $n_0 \leq n$,*

$$\mathsf{APP}_{k,n_0}(Q) \leq 2^t \cdot d^2 \cdot \max_{\substack{k_0,\ell_0 \geq 0 \\ k_0 + \frac{k}{d-k}\cdot\ell_0 \leq k - \mathrm{residue}_k(d_1,\ldots,d_t)}} M(n,k_0) \cdot M_{\leq}(n_0,\ell_0).$$

There is a minor difference in the lemma as stated above and as stated in [AGK+23], and this is the term $M_{\leq}(n_0, \ell_0)$. In [AGK+23], the authors consider only sequences $L = \langle \ell_1, \ldots, \ell_n \rangle$ of linear polynomials in the projections rather than affine ones, and thus they can replace $M_{\leq}(n_0, \ell_0)$ by $M(n_0, \ell_0)$. However with affine polynomials their proof gives the bound above.

As we are interested in functional lower bounds for low-individual degree polynomials, we need the following modification of Lemma 46. A very important ingredient in the lemma is the fact that the individual-degree bound δ only appears in the term $\mathrm{residue}_k(d'_1, \ldots, d'_t)/\delta$, and thus it only decreases the influence of the residue-term.

Lemma 48. *Let n, t, d and δ be positive integers and let $Q_1, \ldots, Q_t$ be non-constant, homogeneous polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ with degrees $d'_1, \ldots, d'_t$, respectively, so that $d' := \deg(Q_1, \ldots, Q_t) = \sum_{i=1}^t d'_i$ is between d and $\delta \cdot d$, and let $k < d$ be a non-negative integer. Then*

$$\left\langle \partial^k (Q_1 \cdots Q_t) \right\rangle \subseteq \sum_{\substack{S \subseteq [t], k_0, \ell_0 \\ k_0 + \frac{k}{d-k}\cdot\ell_0 \leq k - \mathrm{residue}_k(d'_1,\ldots,d'_t)/\delta}} \left\langle \overline{x}^{\ell_0} \cdot \partial^{k_0} \left(\prod_{i \in S} Q_i \right) \right\rangle.$$

Proof sketch. Our proof is in essence the same as that of Lemma 46 in [AGK+23]. We sketch the argument for completeness.

As in the proof of Lemma 46, denote by $\mathcal{V}$ the set

$$\sum_{\substack{S \subseteq [t], k_0, \ell_0 \\ k_0 + \frac{k}{d-k}\cdot\ell_0 \leq k - \mathrm{residue}_k(d'_1,\ldots,d'_t)/\delta}} \left\langle \overline{x}^{\ell_0} \cdot \partial^{k_0} \left(\prod_{i \in S} Q_i \right) \right\rangle.$$

Let $\mu \colon [k] \to x$ be an arbitrary total function. We want to show that $\partial_{\mu([k])} \in \mathcal{V}$. Let $S \subseteq [t]$ and denote by $\bar{S}$ the complement of S relative to $[t]$, i.e. the set $[t] \setminus S$. Let $\tilde{\kappa} \colon \bar{S} \to 2^{[k]}$ be such that $|\tilde{\kappa}_i| > \frac{k}{d'} \cdot d'_i$ for all $i \in \bar{S}$. With this bound we have that

$$|\tilde{\kappa}_i| - \frac{k}{\delta \cdot d} \cdot d'_i \geq \frac{1}{\delta^2} \cdot \left(|\tilde{\kappa}_i| - \frac{k}{d'} \cdot d'_i \right)$$

for any $i \in \bar{S}$. The usefulness of this inequality will be apparent later in the proof. Define a polynomial $R_{S,\tilde{\kappa}}$ as

$$R_{S,\tilde{\kappa}} := \sum_{\substack{\kappa \colon [t] \to 2^{[k]} \\ \kappa \text{ extends } \tilde{\kappa} \\ \bigsqcup_{i \in [t]} \kappa_i = [k] \\ \forall i \in S, |\kappa_i| \leq \frac{k}{d'} \cdot d'_i}} \prod_{i \in [t]} \partial_{\mu(\kappa_i)} Q_i.$$

Now as in the proof of Lemma 46, one can show that

$$\partial_{\mu([k])} \left(\prod_{i \in [t]} Q_i \right) = \sum_{S \subseteq [t]} \sum_{\substack{\tilde{\kappa} \colon \bar{S} \to 2^{[k]} \\ \forall i \in \bar{S}, |\kappa_i| > \frac{k}{d'} \cdot d'_i}} R_{S,\tilde{\kappa}},$$

and thus to prove the claim it suffices to show that $R_{S,\tilde{\kappa}} \in \mathcal{V}$ for all S and $\tilde{\kappa}$. To prove this, one argues by induction on the size of S. If $|S| = 0$, then $R_{S,\tilde{\kappa}} = 0$ and thus $R_{S,\tilde{\kappa}} \in \mathcal{V}$.

Suppose then that $S \subseteq [t]$ is non-empty and let $\tilde{\kappa}\colon \bar{S} \to 2^{[k]}$ be a function so that $|\tilde{\kappa}_i| > \frac{k}{d'} \cdot d'_i$ for any $i \in \bar{S}$. Let $\kappa\colon [t] \to 2^{[k]}$ be a function extending $\tilde{\kappa}$ so that $\bigsqcup_{i\in[t]} \kappa_i = [k]$ and $|\kappa_i| \leq \frac{k}{d'} \cdot d'_i$ for any $i \in S$. Denote by P_S the set $\bigsqcup_{i\in S} \kappa_i$, and define the polynomial

$$\mathcal{U}_{S,\kappa} := \left(\partial_{\mu(P_S)} \prod_{i\in S} Q_i\right) \cdot \prod_{i\in\bar{S}} \partial_{\kappa_i} Q_i.$$

Again, as in the proof of Lemma 46, one shows that

$$R_{S,\tilde{\kappa}} = \mathcal{U}_{S,\kappa} - \sum_{\substack{T\subsetneq S \text{ and } \kappa'\colon S\setminus T\to 2^{[k]} \\ \forall i\in S\setminus T, |\kappa'_i| > \frac{k}{d'}\cdot d'_i}} R_{T,\tilde{\kappa}\sqcup\kappa'}.$$

By the induction hypothesis, we know that $R_{T,\tilde{\kappa}\sqcup\kappa'} \in \mathcal{V}$ for any $T \subsetneq S$ and κ'. Hence it suffices to show that $\mathcal{U}_{S,\kappa} \in \mathcal{V}$. By its definition, we have that

$$\mathcal{U}_{S,\kappa} \in \left\langle x^{\ell_0} \cdot \partial^{k_0} \left(\prod_{i\in S} Q_i\right)\right\rangle,$$

where $k_0 := |\mu(P_S)| = |P_S| = \sum_{i\in S} |\kappa_i|$ and $\ell_0 := \sum_{i\in\bar{S}} \deg\left(\partial_{\mu(\kappa_i)} Q_i\right) = \sum_{i\in\bar{S}} \left(d'_i - |\kappa_i|\right)$. Moreover

$$\begin{aligned}
k - k_0 - \frac{k}{d-k}\cdot\ell_0 &= k - \sum_{i\in S}|\kappa_i| - \frac{k}{d-k}\cdot\sum_{i\in\bar{S}}\left(d'_i - |\kappa_i|\right) \\
&= \sum_{i\in\bar{S}}|\kappa_i| - \frac{k}{d-k}\cdot\sum_{i\in\bar{S}}\left(d'_i - |\kappa_i|\right) \\
&= \sum_{i\in\bar{S}}\left(|\kappa_i| - \frac{k}{d-k}\cdot\left(d'_i - |\kappa_i|\right)\right) \\
&= \sum_{i\in\bar{S}}\frac{\delta\cdot d}{d-k}\cdot\left(|\kappa_i| - \frac{k}{\delta\cdot d}\cdot d'_i\right) \\
&\geq \sum_{i\in\bar{S}}\frac{\delta\cdot d}{d-k}\cdot\frac{1}{\delta^2}\cdot\left(|\tilde{\kappa}_i| - \frac{k}{d'}\cdot d'_i\right) \\
&\geq \sum_{i\in\bar{S}}\frac{1}{\delta}\cdot\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right) \\
&= \frac{1}{\delta}\cdot\sum_{i\in\bar{S}}\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right) \\
&= \frac{1}{2\delta}\cdot\sum_{i\in\bar{S}}\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right) + \frac{1}{2\delta}\cdot\sum_{i\in S}\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right) \\
&\quad + \frac{1}{2\delta}\cdot\sum_{i\in\bar{S}}\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right) - \frac{1}{2\delta}\cdot\sum_{i\in S}\left(|\kappa_i| - \frac{k}{d'}\cdot d'_i\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2\delta} \cdot \sum_{i\in[t]} \left(|\kappa_i| - \frac{k}{d'} \cdot d'_i \right) + \frac{1}{2\delta} \cdot \sum_{i\in\bar{S}} \left(|\kappa_i| - \frac{k}{d'} \cdot d'_i \right) - \frac{1}{2\delta} \cdot \sum_{i\in S} \left(|\kappa_i| - \frac{k}{d'} \cdot d'_i \right) \\
&= \frac{1}{2\delta} \cdot \left(k - \frac{k}{d'} \cdot d' \right) + \frac{1}{2\delta} \cdot \sum_{i\in\bar{S}} \left(|\kappa_i| - \frac{k}{d'} \cdot d'_i \right) - \frac{1}{2\delta} \cdot \sum_{i\in S} \left(|\kappa_i| - \frac{k}{d'} \cdot d'_i \right) \\
&= \frac{1}{2\delta} \cdot \sum_{i\in[t]} \left| |\kappa_i| - \frac{k}{d'} \cdot d'_i \right| \\
&\geq \frac{1}{\delta} \cdot \mathrm{residue}_k(d'_1, \ldots, d'_t).
\end{aligned}
$$

Hence we have that $\mathcal{U}_{S,\kappa} \in \mathcal{V}$ as $k_0 + \frac{k}{d-k} \cdot \ell_0 \leq k - \frac{1}{\delta} \cdot \mathrm{residue}_k(d'_1, \ldots, d'_t)$. □

As a consequence we have the following variant of Lemma 47, which gives an upper bound for the APP measure that we can use to prove the functional lower bounds.

Corollary 49. *Let d and δ be non-negative integers, and let $Q = Q_1 \cdots Q_t$ be a homogeneous polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ of degree $d' = d'_1 + \ldots d'_t \geq 1$, where Q_i is homogeneous; $d'_i := \deg(Q_i)$ for all $i \in [t]$ and $d \leq d' \leq \delta \cdot d$. Then for any non-negative integers $k < d$ and $n_0 \leq n$,*

$$
\mathsf{APP}_{k,n_0}(Q) \leq 2^t \cdot \delta^2 \cdot d^2 \cdot \max_{\substack{k_0,\ell_0\geq 0 \\ k_0 + \frac{k}{d-k}\cdot\ell_0 \leq k - \mathrm{residue}_k(d_1,\ldots,d_t)/\delta}} M(n,k_0) \cdot M_{\leq}(n_0,\ell_0).
$$

6.1.2 Low-Depth Homogeneous Formulas Have High Residue

Secondly [AGK+23] showed that any small low-depth homogeneous formula has a representation as a small sum of products of homogeneous polynomials, and moreover the residue of the degrees of the polynomials in the products is relatively large for suitably chosen parameters.

Lemma 50 ([AGK+23])**.** *Suppose C is a homogeneous formula of product-depth $\Delta \geq 1$ computing a homogeneous polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ of degree d, where $d^{2^{1-\Delta}} = \omega(1)$. Then there exist homogeneous polynomials $\{Q_{i,j}\}_{i,j}$ in $\mathbb{F}[x_1, \ldots, x_n]$ such that $C = \sum_{i=1}^{s} Q_{i,1} \cdots Q_{i,t_i}$ for some $s \leq \mathrm{size}(C)$. Fixing an arbitrary $i \in [s]$, let $t := t_i$ and let $d_j := \deg(Q_{i,j})$ for $j \in [t]$. Then*

$$
\mathrm{residue}_k(d_1, \ldots, d_t) \geq \Omega\left(d^{2^{1-\Delta}} \right),
$$

where $k := \left\lfloor \frac{\alpha \cdot d}{1+\alpha} \right\rfloor$, $\alpha := \sum_{\nu=0}^{\Delta-1} \frac{(-1)^\nu}{\tau^{2^\nu - 1}}$ and $\tau := \left\lfloor d^{2^{1-\Delta}} \right\rfloor$.

For us the following variant of the previous lemma will be important.

Lemma 51. *Let $\delta \geq 1$ be a positive integer, and suppose C is a homogeneous formula of product-depth $\Delta \geq 1$ computing a homogeneous polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ of degree $d' \in [d, \delta \cdot d]$, where $d^{2^{1-\Delta}} = \omega(1)$. Then there exist homogeneous polynomials $\{Q_{i,j}\}_{i,j}$ in $\mathbb{F}[x_1, \ldots, x_n]$ such that $C = \sum_{i=1}^{s} Q_{i,1} \cdots Q_{i,t_i}$ for some $s \leq \mathrm{size}(C)$. Fixing an arbitrary $i \in [s]$, let $t := t_i$ and let $d'_j := \deg(Q_{i,j})$ for $j \in [t]$. Then*

$$
\mathrm{residue}_k(d'_1, \ldots, d'_t) \geq \Omega\left(\frac{d^{2^{1-\Delta}}}{\delta} \right),
$$

where $k := \left\lfloor \frac{\alpha \cdot d}{1+\alpha} \right\rfloor$, $\alpha := \sum_{\nu=0}^{\Delta-1} \frac{(-1)^{nu}}{\tau^{2^\nu - 1}}$ and $\tau := \left\lfloor d^{2^{1-\Delta}} \right\rfloor$.

Proof sketch: First we note that by an argument identical to the proof of Lemma 50 in [AGK+23] one can find an appropriate decomposition of C as a sum of products of homogeneous polynomials, and show that

$$\frac{1}{2}\min_{k_1,\ldots,k_t\in\mathbb{Z}}\sum_{j\in[t]}\left|k_j-\frac{k}{d}\cdot d'_j\right|\geq\Omega\left(d^{2^{1-\Delta}}\right).$$

As $d\leq d'\leq\delta\cdot d$ we further have that

$$\begin{aligned}
\text{residue}_k(d'_1,\ldots,d'_t)&=\frac{1}{2}\min_{k_1,\ldots,k_t\in\mathbb{Z}}\sum_{j\in[t]}\left|k_j-\frac{k}{d'}\cdot d'_j\right|\\
&=\frac{1}{2}\sum_{j\in[t]}\min\left\{\left\{\frac{k}{d'}d'_j\right\},1-\left\{\frac{k}{d'}d'_j\right\}\right\}\\
&=\frac{1}{2}\sum_{j\in[t]}\min\left\{\left\{\frac{d}{d'}\cdot\frac{k}{d}\cdot d'_j\right\},1-\left\{\frac{d}{d'}\cdot\frac{k}{d}\cdot d'_j\right\}\right\}\\
&=\frac{1}{2}\cdot\frac{d}{d'}\sum_{j\in[t]}\min\left\{\left\{\frac{k}{d}\cdot d'_j\right\},\frac{d'}{d}-\left\{\frac{k}{d}\cdot d'_j\right\}\right\}\\
&\geq\frac{1}{2}\cdot\frac{d}{d'}\sum_{j\in[t]}\min\left\{\left\{\frac{k}{d}\cdot d'_j\right\},1-\left\{\frac{k}{d}\cdot d'_j\right\}\right\}\\
&=\frac{1}{2}\cdot\frac{d}{d'}\min_{k_1,\ldots,k_t\in\mathbb{Z}}\sum_{j\in[t]}\left|k_j-\frac{k}{d}\cdot d'_j\right|\geq\Omega\left(\frac{d^{2^{1-\Delta}}}{\delta}\right).
\end{aligned}$$

□

6.1.3 High Residue Implies Lower Bounds

Finally, [AGK+23] show that high residue together with APP lower bounds imply lower bounds for homogeneous formulas.

Lemma 52 ([AGK+23])**.** *Let $P=\sum_{i=1}^{s}Q_{i,1}\cdots Q_{i,t_i}$ be a homogeneous polynomial in $\mathbb{F}[x_1,\ldots,x_n]$ of degree d, where $Q_{i,j}$ are homogeneous and*

$$\mathsf{APP}_{k,n_0}(P)\geq 2^{-O(d)}\cdot M(n,k)$$

for some $1<k<d/2$ and $n_0\leq n$ such that $n_0\approx 2(d-k)\cdot\left(\frac{n}{k}\right)^{\frac{k}{d-k}}$. If there is some $\gamma>0$ so that for all $i\in[s]$,

$$\text{residue}_k(\deg(Q_{i,1}),\ldots,\deg(Q_{i,t_i}))\geq\gamma,$$

then $s\geq 2^{-O(d)}\cdot\left(\frac{n}{d}\right)^{\gamma}$.

Again, for our purposes we need a small modification of this result.

Lemma 53. *Let d,δ be positive integers. Let $P=\sum_{i=1}^{s}Q_{i,1}\cdots Q_{i,t_i}$ be a homogeneous polynomial in $\mathbb{F}[x_1,\ldots,x_n]$ of degree d', where $Q_{i,j}$ are homogeneous, $d\leq d'\leq\delta\cdot d$ and*

$$\mathsf{APP}_{k,n_0}(P)\geq 2^{-O(d)}\cdot M(n,k)$$

for some $1 < k < d/2$ *and* $n_0 \leq n$ *such that* $n_0 \approx 2(d-k) \cdot \left(\frac{n}{k}\right)^{\frac{k}{d-k}}$. *If there is some* $\gamma > 0$ *so that for all* $i \in [s]$,

$$\mathrm{residue}_k(\deg(Q_{i,1}), \ldots, \deg(Q_{i,t_i})) \geq \gamma,$$

then $s \geq 2^{-O(d)} \cdot \delta^{-2} \cdot \left(\frac{n}{d}\right)^{\gamma/\delta}$.

Proof sketch. The proof is again like the proof of Lemma 52, and we sketch the argument for completeness.

By Corollary 49 and the sub-additivity of APP we have that

$$\mathsf{APP}_{k,n_0}(P) \leq \sum_{i=1}^{s} \mathsf{APP}_{k,n_0}(Q_{i,1} \cdots Q_{i,t_i}) \leq s \cdot 2^t \cdot \delta^2 \cdot d^2 \cdot \max_{\substack{k_0,\ell_0 \geq 0 \\ k_0 + \frac{k}{d-k}\cdot \ell_0 \leq k - \gamma/\delta}} M(n,k_0) \cdot M_{\leq}(n_0,\ell_0).$$

On the other hand, by assumption, $\mathsf{APP}_{k,n_0}(P) \geq 2^{-O(d)} \cdot M(n,k)$. These together yield two integers $k_0, \ell_0 \geq 0$ satisfying

$$k_0 + \frac{k}{d-k} \cdot \ell_0 \leq k - \gamma/\delta \tag{53.1}$$

and

$$s \geq 2^{-O(d)} \cdot 2^{-t} \cdot \delta^{-2} \cdot d^{-2} \cdot \frac{M(n,k)}{M(n,k_0) \cdot M_{\leq}(n_0,\ell_0)}.$$

As in the proof of Lemma 52 one shows using Lemma 45 that this yields

$$s \geq 2^{-O(d)} \cdot \delta^{-2} \cdot \frac{(n/d)^{k-k_0-\frac{k}{d-k}\cdot\ell_0}}{(d/k_0)^{k_0} \cdot (d/\ell_0)^{\ell_0}}.$$

With 53.1 and the fact that $x^x \geq e^{-1/e}$ for all $x > 0$ we arrive at

$$s \geq 2^{-O(d)} \cdot \delta^{-2} \cdot \left(\frac{n}{d}\right)^{\gamma/\delta}.$$

□

6.2 Knapsack over a Word w

Now we turn to the lower bound proof itself. We first recall from [GHT22] the intermediate hard instance used there to prove the lower bound for multilinear refutations, which is called *knapsack over a word* w. We will also use the same intermediate instance to prove our lower bound.

Let $w \in \mathbb{Z}^d$ be a word, and associate with each entry w_i a set of fresh variables $X(w_i)$ of size $2^{|w_i|}$. Denote by P_w the set of indices $i \in [d]$ so that $w_i \geq 0$, and by N_w the set of indices so that $w_i < 0$. For some subset $S \subseteq [d]$ we denote by w_S the sum $\sum_{i \in S} w_i$ and by $w|_S$ the subword of w indexed by the set S. We say that a monomial m is set-multilinear on some $w|_S$ if it contains exactly one variable from each of the sets $X(w_i)$ for $i \in S$.

In the following we fix a useful representation of the variables $X(w_i)$ for all $i \in [d]$. For any $i \in P_w$, we write the variables of $X(w_i)$ in the form $x_\sigma^{(i)}$, where σ is a binary string indexed by the integer interval

$$A_w^{(i)} := \left[\sum_{\substack{i' \in P_w \\ i' < i}} w_{i'} + 1, \sum_{\substack{i' \in P_w \\ i' \leq i}} w_{i'} \right]$$

Similarly for any $j \in N_w$, we write the variables of $X(w_j)$ in the form $y_\sigma^{(j)}$, where σ is a binary string indexed by the set

$$B_w^{(j)} := \left[\sum_{\substack{j' \in N_w \\ j' < j}} |w_{j'}| + 1, \sum_{\substack{j' \in N_w \\ j' \leq j}} |w_{j'}| \right].$$

We call the variables of the form $x_\sigma^{(i)}$ the positive variables, or simply $\overline{x}$ variables, and the variables of the form $y_\sigma^{(j)}$ the negative variables, or simply $\overline{y}$ variables. For any $S \subseteq P_w$, write A_w^S for the set $\bigcup_{i \in S} A_w^{(i)}$, and define the set B_w^T similarly for any $T \subseteq N_w$.

Each monomial that is set-multilinear on $w|_S$ for some $S \subseteq P_w$ is in one-to-one correspondence with a binary string indexed by the set A_w^S. For a set-multilinear monomial $\overline{x}^\alpha$ on some $w|_S$ we denote by $\sigma(\overline{x}^\alpha)$ the associated binary string indexed by A_w^S associated with $\overline{x}^\alpha$. Similarly any monomial that is set-multilinear on $w|_T$ for some $T \subseteq N_w$ corresponds to a binary string indexed by the set B_w^T, and for any $\overline{y}^\gamma$ that is set-multilinear on some $w|_T$ for $T \subseteq N_w$ we denote by $\sigma(\overline{y}^\gamma)$ the associated binary string indexed by B_w^T.

We say that the word w is N-heavy in the case that $|w_{N_w}| \geq |w_{P_w}|$ and P-heavy in the case that $|w_{P_w}| \geq |w_{N_w}|$. We call the word balanced if for any $i \in P_w$ there is some $j \in N_w$ so that $A_w^{(i)} \cap B_w^{(j)} \neq \emptyset$ and vice versa.

We define the polynomial ks_w as follows. For this definition we assume that w is N-heavy. Otherwise we switch the roles of the positive and negative variables in the definition. For binary strings σ and σ' indexed by some sets A and B respectively we write $\sigma \sim \sigma'$ if $\sigma(i) = \sigma'(i)$ for any $i \in A \cap B$.

For $i \in P_w$ and $\sigma \in A_w^{(i)}$ define the polynomial $f_\sigma^{(i)}$ with

$$f_\sigma^{(i)} := \prod_{\substack{j \in N_w: \\ A_w^{(i)} \cap B_w^{(j)} \neq \emptyset}} \sum_{\substack{\sigma_j \colon B_w^{(j)} \to \{0,1\}: \\ \sigma_j \sim \sigma}} y_{\sigma_j}^{(j)}$$

and define the polynomial ks_w as

$$\mathrm{ks}_w := \sum_{i \in P_w} \sum_{\sigma \colon A_w^{(i)} \to \{0,1\}} x_\sigma^{(i)} f_\sigma^{(i)} - \beta$$

for any β so that ks_w is unsatisfiable over Boolean values.

6.3 Lower Bounds for the APP Measures

This section is devoted to proving a APP lower bounds for refutations of ks_w. We will first prove a lower bound that does not take into account any bounds on the individual degree. The first proof however highlights some key ideas in the proof in a clean manner. After this we discuss how to obtain APP lower bounds for suitable homogeneous slices of bounded individual degree refutations of ks_w.

Unlike usually in algebraic circuit complexity we are given the refutations of ks_w only implicitly; we only know something about their functional behaviour. However we still want to prove suitable lower bounds for the dimension of the space spanned by the affine projections of the partial derivatives. The key idea in the proof below is to represent the affine projections of partial derivatives as an alternating sum of suitable partial assignments. This allows us to infer useful information about the structure of the given refutation, and prove the wanted lower bound.

Lemma 54. *Let h, d be positive integers so that $h > 100$, and let k be a parameter in the interval $[\frac{d}{4}, \frac{d}{2}]$. Then there are*

- *a balanced word $w \in [-h, \ldots, h]^d$;*
- *an integer $n_0 \leq n$ with $n_0 \approx 2(d-k)\left(\frac{n}{k}\right)^{\frac{k}{d-k}}$*

so that for any polynomial g such that

$$g = \frac{1}{\mathrm{ks}_w} \quad \text{over Boolean assignments}$$

the following bound holds:

$$\mathsf{APP}_{k,n_0}(g) \geq 2^{h \cdot k}.$$

Proof: To construct the word we follow [AGK+23]. Let $h' = \frac{h \cdot k}{d-k}$, and note that this lies in the interval $[h/3, h]$. The word consists of k many copies of the entry h, $k_1 := (d-k)\lceil h' \rceil - kh$ many copies of $-\lfloor h' \rfloor$ and $k_2 := d - k - k_1$ copies of $-\lceil h' \rceil$. The total sum of all the entries is 0, and thus the word (in any order) is balanced.

Consider the set of variables $\overline{x} \cup \overline{y}$, where $\overline{x}$ stands for the positive variables of ks_w and $\overline{y}$ stands for the negative variables of ks_w. Here ks_w is defined as if w is N-heavy; note that w is in fact both N- and P-heavy. Take now $n_0 := |\overline{y}|$. Then we have that $n_0 \approx 2(d-k) \cdot \left(\frac{n}{k}\right)^{\frac{k}{d-k}}$ [AGK+23].

Write g in two different ways as a polynomial in $\mathbb{F}[\overline{x}][\overline{y}]$ and as a polynomial in $\mathbb{F}[\overline{y}][\overline{x}]$. Write $g = \sum_\gamma g_\gamma(\overline{x})\overline{y}^\gamma$, where and g_γ are polynomials in the positive variables, and write $g = \sum_\alpha g_\alpha(\overline{y})\overline{x}^\alpha$, where $g_\alpha(\overline{y})$ are polynomials in the negative variables.

Define now a linear map L as follows:

$$L(z) := \begin{cases} z, & \text{if } z \in \overline{y}; \\ 1, & \text{if } z \in \overline{x}. \end{cases}$$

To lower bound the APP measure with L, we consider the set of partial derivatives of g with respect to the set-multilinear monomials over all the positive variables. Now it is easy to see that for a set-multilinear monomial $\overline{x}^\alpha$ in the positive variables,

$$L\left(\partial_\alpha g\right) = \sum_{\substack{\alpha': \\ \alpha \subseteq \alpha'}} g_{\alpha'}(\overline{y}).$$

Hence we need to lower bound the dimension of the space spanned by such sums. First note that in order to lower bound this dimension, it suffices to lower bound the dimension of the multilinearizations of such sums, as multilinearization of the spanning set can only decrease the dimension. Thus we are interested in the following polynomials

$$h_\alpha := \sum_{\substack{\alpha': \\ \alpha \subseteq \alpha'}} \mathrm{ml}\left(g_{\alpha'}(\overline{y})\right)$$

for set-multilinear monomials $\overline{x}^\alpha$ on the positive variables.

We will prove a lower bound on the dimension by showing that the polynomials h_α are linearly independent for all distinct set-multilinear monomials $\overline{x}^\alpha$. This immediately gives the claimed lower bound as there are $2^{h \cdot k}$ many distinct set-multilinear monomials in the positive variables.

We prove the linear independence in a series of claims. First we give a useful representation for the polynomials h_α as sums of reciprocals of knapsack instances. For a monomial $\overline{x}^\alpha$ we denote by τ_α the Boolean assignment that maps all the variables appearing in $\overline{x}^\alpha$ to 0 and all the other $\overline{x}$-variables to 1, and leaves $\overline{y}$ variables untouched.

Claim 55. *Let $\overline{x}^\alpha$ be a set-multilinear monomial in the positive variables. Then*

$$h_\alpha = \sum_{\mu \subseteq \alpha} (-1)^{|\mu|} \tau_\mu \left(\frac{1}{\mathrm{ks}_w} \right) \quad \text{over Boolean values.}$$

Proof of Claim 55: First note that

$$h_\alpha = \sum_{\mu \subseteq \alpha} (-1)^{|\mu|} \tau_\mu(\mathrm{ml}(g)).$$

This follows from a straightforward argument using the inclusion-exclusion principle. Indeed, note that for any $\mu \subseteq \alpha$ we have that

$$\tau_\mu(\mathrm{ml}(g)) = \sum_{\substack{\nu: \\ \mu \wedge \nu = \emptyset}} \mathrm{ml}(g_\nu(\overline{y})).$$

Now if $\alpha' \supseteq \alpha$, then the only $\mu \subseteq \alpha$ so that $\alpha' \wedge \mu = \emptyset$ is $\mu = \emptyset$. Hence the terms $\mathrm{ml}(g_{\alpha'}(\overline{y}))$ for all the supersets α' of α survive in the expression above. If on the other hand $\alpha' \not\supseteq \alpha$, then there is some i so that $\alpha(i) = 1$, but $\alpha'(i) = 0$. The set of all $\mu \subseteq \alpha$ satisfying $\mu \wedge \alpha' = \emptyset$ forms a non-trivial finite Boolean lattice. It follows by inclusion-exclusion principle that no term of the form $\mathrm{ml}(g_{\alpha'}(\overline{y}))$ for $\alpha' \not\supseteq \alpha$ survives in the final expression.

On the other hand by definition

$$\mathrm{ml}(g) = \frac{1}{\mathrm{ks}_w} \quad \text{over Boolean values,}$$

and hence for any $\mu \subseteq \alpha$

$$\tau_\mu(\mathrm{ml}(g)) = \tau_\mu \left(\frac{1}{\mathrm{ks}_w} \right) \quad \text{over Boolean values.}$$

This concludes the proof of Claim 55. □

For a monomial $\overline{y}^\alpha$ we denote by π_α the partial Boolean mapping that send each variable in $\overline{y}^\alpha$ to 1 and any other $\overline{y}$ variable to 0, and leaves $\overline{x}$ variables untouched.

Claim 56. *Let $\overline{x}^\alpha$ be a set-multilinear monomial in the positive variables and let $\overline{y}^\gamma$ be a set-multilinear monomial in the negative variables. Then*

$$\pi_\gamma(h_\alpha) \neq 0 \quad \textit{if and only if} \quad \sigma(\overline{y}^\gamma) = \sigma(\overline{x}^\alpha).$$

Proof of Claim 56: From Claim 55 we know that

$$h_\alpha = \sum_{\mu \subseteq \alpha} (-1)^{|\mu|} \tau_\mu \left(\frac{1}{\mathrm{ks}_w} \right) \quad \text{over Boolean values.}$$

Hence we have the following chain of equalities.

$$\begin{aligned}\pi_\gamma(h_\alpha) &= \sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\pi_\gamma\left(\tau_\mu\left(\frac{1}{\mathrm{ks}_w}\right)\right)\\ &= \sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\tau_\mu\left(\frac{1}{\pi_\gamma(\mathrm{ks}_w)}\right)\\ &= \sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\tau_\mu\left(\frac{1}{\sum x_\sigma^{(i)}-\beta}\right),\end{aligned}$$

where in the last row the sum in the denominator ranges over those i and σ so that σ agrees with $\sigma(\overline{y}^\gamma)$ on the interval $A_w^{(i)}$.

Let now f_γ be the multilinear polynomial so that

$$f_\gamma = \frac{1}{\sum x_\sigma^{(i)}-\beta} \quad \text{over Boolean values.}$$

From [FSTW21] we know that the leading monomial of f_γ is the product of all the variables appearing in the sum. Other monomials in f_γ are naturally submonomials of the full-degree monomial.

Thus we want to analyze the value of

$$\sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\tau_\mu(f_\gamma)$$

for different set-multilinear monomials $\overline{x}^\alpha$.

Suppose first that $\sigma(\overline{x}^\alpha)=\sigma(\overline{y}^\gamma)$, i.e. $\overline{x}^\alpha$ is the leading monomial of the polynomial f_γ. Now $\tau_\emptyset(\overline{x}^\alpha)=1$, but for any $\mu\neq\emptyset$ we have that $\tau_\mu(\overline{x}^\alpha)=0$. For any proper submonomial $\overline{x}^\mu$ of $\overline{x}^\alpha$ we have for all $\mu'\subseteq\alpha$ that $\tau_{\mu'}(\overline{x}^\mu)\neq 0$ if and only if $\mu\wedge\mu'=\emptyset$. The set of such μ''s forms a non-trivial Boolean lattice and thus by the inclusion-exclusion principle

$$\sum_{\substack{\mu'\subseteq\alpha\\ \mu\wedge\mu'=\emptyset}}(-1)^{|\mu'|}\tau_{\mu'}\left(\overline{x}^\mu\right)=0.$$

We have shown that when $\sigma(\overline{x}^\alpha)=\sigma(\overline{y}^\gamma)$,

$$\sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\tau_\mu(f_\gamma)=a_\alpha,$$

where a_α is the coefficient of $\overline{x}^\alpha$ in f_γ.

Suppose then that $\sigma(\overline{x}^\alpha)\neq\sigma(\overline{y}^\gamma)$, and let $\overline{x}^{\hat{\alpha}}$ be so that $\sigma(\overline{x}^{\hat{\alpha}})=\sigma(\overline{y}^\gamma)$. Now for any $\mu\subseteq\alpha$ and any $\hat{\mu}\subseteq\hat{\alpha}$ we have that $\tau_\mu(\overline{x}^{\hat{\mu}})\neq 0$ if and only if $\mu\wedge\hat{\mu}=\emptyset$. For any fixed $\hat{\mu}\subseteq\hat{\alpha}$ the set of all those $\mu\subseteq\alpha$ that satisfy the latter condition forms again a non-trivial Boolean lattice, and thus by inclusion-exclusion principle we have that

$$\sum_{\substack{\mu\subseteq\alpha\\ \mu\wedge\hat{\mu}=\emptyset}}(-1)^{|\mu|}\tau_\mu\left(\overline{x}^{\hat{\mu}}\right)=0.$$

Above $\hat{\mu}$ was an arbitrary substring of $\hat{\alpha}$ and thus we have that

$$\sum_{\mu\subseteq\alpha}(-1)^{|\mu|}\tau_\mu(f_\gamma)=0.$$

This concludes the proof of Claim 56. □

To finish the proof of Lemma 54, suppose that for some set-multilinear $\overline{x}^{\alpha}$ there are $a_{\alpha'} \in \mathbb{F}$ for each $\alpha' \neq \alpha$ so that

$$h_\alpha = \sum_{\alpha' \neq \alpha} a_{\alpha'} h_{\alpha'}.$$

Consider then the mapping π_γ, where γ is so that $\sigma(\overline{x}^{\alpha}) = \sigma(\overline{y}^{\gamma})$. Then by Claim 56 we have that

$$1 = \pi_\gamma(h_\alpha) = \sum_{\alpha' \neq \alpha} a_{\alpha'} \pi_\gamma(h_{\alpha'}) = 0.$$

Hence the polynomials h_α are linearly independent for all distinct set-multilinear $\overline{x}^{\alpha}$. □

Lemma 54 demonstrates an APP lower bound on any refutation of ks_w. In order to derive meaningful circuit lower bounds from these bounds however we need bounds for some low-degree homogeneous polynomial, while no refutation of ks_w is homogeneous and low-degree. In the following lemma we show however that assuming a bound on the individual degree of the given refutation, we can infer useful APP lower bounds for some homogeneous low-degree slice of the refutation.

Lemma 57. *Let h, d, δ be positive integers so that $h > 100$, and let k be a parameter in $[\frac{d}{4}, \frac{d}{2}]$. Then there are*

- *a balanced word $w \in [-h, \ldots, h]^d$;*
- *an integer $n_0 \leq n$ so that $n_0 \approx 2(d-k)\left(\frac{n}{k}\right)^{\frac{k}{d-k}}$;*
- *an integer d' between d and $\delta \cdot d$*

so that for any polynomial g of individual degree at most δ such that

$$g = \frac{1}{\mathrm{ks}_w} \quad \text{over Boolean assignments}$$

the following bound holds

$$\mathsf{APP}_{k,n_0}(g_{d'}) \geq \frac{2^{hk}}{(\delta-1)\cdot d + 1},$$

where $g_{d'}$ denotes the homogeneous d'-slice of g.

Proof: We will comment on what needs to be changed in the proof of the previous lemma in order to take into account the bounds on the degrees.

Consider the slice $\bar{g}$ of g of monomials of degrees between d and $\delta \cdot d$, and write this fragment as $\bar{g} = \sum_\alpha g_\alpha(\overline{y})\overline{x}^{\alpha}$, where now $d \leq |\alpha| \leq \delta \cdot d$.

For the same choice of partial derivatives and linear function L we again obtain that

$$L(\partial_\alpha \bar{g}) = \sum_{\substack{\alpha': \\ \alpha \subseteq \alpha'}} g_{\alpha'},$$

where again the sum runs over those α' satisfying $d \leq |\alpha'| \leq \delta \cdot d$.

Now define again for any set-multilinear $\overline{x}^{\alpha}$ the polynomial

$$\bar{h}_\alpha := \sum_{\substack{\alpha': \\ \alpha \subseteq \alpha'}} \mathrm{ml}(g_{\alpha'})$$

and note as in Claim 55 that

$$\bar{h}_\alpha = \sum_{\mu \subseteq \alpha} (-1)^{|\mu|} \tau_\mu(\mathrm{ml}(\bar{g})).$$

Then we have that

$$\pi_\gamma\left(\bar{h}_\alpha\right) = \sum_{\mu \subseteq \alpha} (-1)^{|\mu|} \tau_\mu\left(\pi_\gamma(\mathrm{ml}(\bar{g}))\right).$$

Now one can show that the leading monomial of the multilinear polynomial f_γ is present in $\pi_\gamma(\mathrm{ml}(\bar{g}))$. This follows from the following claim whose proof can be found in [GHT22].

Claim 58. *For a set-multilinear $\overline{y}^\gamma$ the leading monomial of the polynomial*

$$\sum_{\substack{\gamma' \\ \mathrm{Supp}(\gamma')=\gamma}} \mathrm{ml}(g_{\gamma'})$$

is the set-multilinear $\overline{x}^\alpha$ so that $\sigma(\overline{x}^\alpha) = \sigma(\overline{y}^\gamma)$.

Now, again by a similar argument one can show that for any set-multilinear $\overline{x}^\alpha$ and $\overline{y}^\gamma$

$$\pi_\gamma(\bar{h}_\alpha) \neq 0 \quad \text{if and only if} \quad \sigma(\overline{x}^\alpha) = \sigma(\overline{y}^\gamma),$$

and hence the polynomials $\bar{h}_\alpha$ are also linearly independent.

Now, by subadditivity of the APP measure, we have that

$$2^{hk} \leq \mathsf{APP}_{k,n_0}(\bar{g}) \leq \sum_{d'=d}^{\delta \cdot d} \mathsf{APP}_{k,n_0}\left(g_{d'}\right).$$

Hence there is some d' between d and $\delta \cdot d$ so that

$$\mathsf{APP}_{k,n_0}\left(g_{d'}\right) \geq \frac{2^{h \cdot k}}{(\delta - 1) \cdot d + 1}.$$

□

6.4 Constant-Depth Lower Bounds for the Lifted Knapsack

Lemma 59. *Let h, d and δ be positive integers so that $h > 100$. There is a balanced word $w \in [-h, h]^d$ and an integer d' between d and $\delta \cdot d$ so that for any polynomial g of individual degree at most δ satisfying*

$$g = \frac{1}{\mathrm{ks}_w} \qquad \textit{over Boolean values}$$

any homogeneous formula of product-depth Δ computing the d'-slice of g has size at least

$$2^{-O(d)} \cdot \left(\frac{n}{d}\right)^{\Omega\left(\frac{d 2^{1-\Delta}}{\delta^2}\right)}.$$

Proof: Let k be defined as in Lemma 50. Then $k \in \left[\frac{d}{4}, \frac{d}{2}\right]$. Let w, n_0 and d' be as in Lemma 57, and let F be a homogeneous formula of product-depth Δ computing the d'-slice of g.

We can assume that $\delta < d$ as otherwise the claim is trivial. On the other hand

$$k \cdot 2^h \leq n \leq d \cdot 2^h, \text{ and so } 2^h \approx \left(\frac{n}{k}\right),$$

and hence, by Lemma 45,

$$\frac{2^{h\cdot k}}{(\delta-1)\cdot d+1} \geq 2^{-O(d)} \cdot \left(\frac{n}{k}\right)^k \geq 2^{-O(d)} \cdot M(n,k).$$

By Lemma 51 there exists homogeneous polynomials $\{Q_{i,j}\}_{i,j}$ so that

$$F = \sum_{i\in[s]} Q_{i,1} \cdots Q_{i,t_i}$$

for some $s \leq \text{size}(F)$ and

$$\text{residue}_k\left(\deg\left(Q_{i,1}\right), \ldots, \deg\left(Q_{i,t_i}\right)\right) \geq \Omega\left(\frac{d^{2^{1-\Delta}}}{\delta}\right)$$

for all $i \in [s]$. Now by Lemma 53 and Lemma 57 we have that

$$s \geq 2^{-O(d)} \cdot \left(\frac{n}{d}\right)^{\Omega\left(\frac{d^{2^{1-\Delta}}}{\delta^2}\right)}.$$

□

Finally, we are ready to prove our main result of this section

Proof of Theorem 44: Let C be a circuit of size s and product-depth Δ computing g. Let $h := \lfloor \log n/2 \rfloor$, let $d := \lfloor \log n \rfloor$, and note that $d \cdot 2^h < n$ for large enough n. We can again assume that $\delta < d$ as otherwise the claim is trivial.

Let $w \in [-h,h]^d$ be defined as in Lemma 54. The polynomial ks_w is of degree at most 4 as any $A_w^{(i)}$ overlaps with at most 3 distinct $B_w^{(j)}$. This is due to the fact that h' as defined in Lemma 54 lives in the interval $[h/3, h]$. Hence there is some partial assignment to the variables $z_{ijk\ell}$ and x_i that maps $\sum_{i,j,k,\ell} z_{ijk\ell}x_ix_jx_kx_\ell - \beta$ to ks_w up to renaming of variables. By applying this partial assignment to C we obtain a circuit C' of size at most s and product-depth Δ computing a polynomial g' of individual degree at most δ that equals $1/\text{ks}_w$ over Boolean values. We can expand this circuit to a formula F of the same product-depth and size $s^{O(\Delta)}$.

Using the homogenization transformation of [LST21] we can compute the d'-slice of F with a homogeneous formula of product depth 2Δ and size $s^{O(\Delta)} \cdot 2^{O(\sqrt{d'})} = s^{O(\Delta)} \cdot 2^{O(d)}$. By Lemma 59 we have that

$$s^{O(\Delta)} \cdot 2^{O(d)} \geq 2^{-O(d)} \cdot \left(\frac{n}{d}\right)^{\Omega\left(\frac{d^{2^{1-2\Delta}}}{\delta^2}\right)}.$$

With the chosen value of d this proves our lower bound. □

6.5 Relative Strength of Low Individual Degree and Low Depth Refutations

To finish this section we discuss the strength of the proofs we have just considered, i.e., low depth and low individual degree IPS refutations. We demonstrate the strength by giving upper bounds for few standard benchmark formulas in proof complexity, Tseitin formulas and two variants of the pigeonhole principle. Afterwards we discuss some weaknesses caused by the individual degree restriction.

It was already observed in [GHT22] that Tseitin formulas have small multilinear constant-depth IPS refutations. This simple observation is due to the fact that Tseitin formulas have refutations

with small number of monomials in the weaker Nullstellensatz proof system when the Boolean values are represented in the *Fourier* basis with -1 representing true and 1 representing false [Gri98]. Constant depth multilinear IPS can easily simulate this small Nullstellensatz refutation in the usual $\{0,1\}$ basis by small formulas computing the appropriate change of basis.

We turn now to two variants of the pigeonhole principle: the functional pigeonhole principle PHP_n^{n+1}, and the graph pigeonhole principle over bipartite graphs on $n+1$ pigeons and n holes with bounded left-degree, where each pigeon has only a limited number of holes available to fly to. We prove the upper bounds for the CNF encodings of these principles, but both proofs rely on a reduction to the polynomial representation of the functional pigeonhole principle used by Razborov in [Raz98], where the pigeon axioms are represented by the polynomial constraints $x_{i1}+\cdots+x_{in}=1$, for all $i \in [n+1]$.

We prove first the upper bound for this polynomial encoding. This proof borrows from the proof given by Grigoriev and Hirsch in [GH03] and Raz and Tzameret [RT08b] with small modifications. Recall that along with the pigeon axioms we have the hole axioms $x_{ik}x_{jk}=0$ for any $i,j \in [n+1]$ and $k \in [n]$. Define auxiliary terms y_k by $y_k := \sum_{i\in[n+1]} x_{ik}$ for every $k \in [n]$. Now y_k are Boolean as one can easily derive $y_k^2 - y_k$ from the hole axioms and the Boolean axioms $x_{ik}^2 - x_{ik}$. On the other hand by adding up all the pigeon axioms we arrive at the expression

$$y_1 + \cdots + y_n = n+1.$$

This is an unsatisfiable instance of the standard knapsack formula. The unique multilinear p so that

$$p \cdot (y_1 + \cdots + y_n - (n+1)) \equiv 1 \mod \overline{y}^2 - \overline{y}$$

is symmetric, and thus can be written as weighted sum of elementary symmetric polynomials. Since these have small multilinear constant depth formulas by the standard Ben-Or result (see Shpilka and Wigderson [SW01, Theorem 5.1]), the polynomial p has also a small multilinear constant depth representation. Forbes *et al.* gave an explicit representation of the polynomial p in [FSTW21]. Moreover it is easy to verify that the certificate for the equivalence modulo the Boolean axioms above is also computable by small multilinear constant depth formula. That is, there are small multilinear constant depth formulas $p, p_1, \ldots, p_n$ so that

$$1 = p \cdot (y_1 + \cdots + y_n - (n+1)) + \sum_{k\in[n]} p_k \cdot (y_k^2 - y_k).$$

Substituting $\sum_{i\in[n+1]} x_{ik}$ for y_k in the expression above and using the small derivations of $y_k^2 - y_k$ from the hole axioms and the Boolean axioms, we obtain a small multilinear constant depth refutation of the polynomial encoding of the functional pigeonhole principle.

Next we prove the upper bounds for the CNF encodings of the mentioned variants of pigeonhole principle. We consider the usual translation of CNFs to polynomial constraints, where, for example, the clause $x \vee \overline{y} \vee z$ is translated to the polynomial constraint $(1-x)y(1-z)=0$. Any Boolean assignment that satisfies the clause satisfies also the polynomial constraint and vice versa.

Lemma 60. *There is a constant-depth IPS refutation of* FPHP_n^{n+1} *of size polynomial in* n *and individual degree* 2.

Proof: Recall that FPHP_n^{n+1} consists of the following clauses

- $\bigvee_{k\in[n]} x_{ik}$ for any $i \in [n+1]$; (pigeon axioms)
- $\overline{x}_{ik} \vee \overline{x}_{jk}$ for any $i \neq j \in [n+1]$ and $k \in [n]$; (hole axioms)

- $\overline{x}_{ik} \vee \overline{x}_{i\ell}$ for any $i \in [n+1]$ and $k \neq \ell \in [n]$. (functionality axioms)

From the pigeon axioms and functionality axioms one derives easily the polynomials

$$x_{i1} + \cdots + x_{in} - 1 \text{ for all } i \in [n+1].$$

Combining these derivations with the multilinear refutations for the polynomial encoding discussed above yields refutations of individual degree 2. □

Lemma 61. *Let $G = ([n+1], [n], E)$ be a bipartite graph with left-degree at most δ. Then there is a constant depth IPS refutation of PHP_G of size polynomial in n and individual degree $O(\delta)$.*

Proof: For this result we need to use slightly modified reduction to a suitable polynomial encoding of the functional pigeonhole principle. Our argument however follows closely the one presented by Grigoriev and Hirsch in [GH03].

For $i \in [n+1]$ denote by $N(i)$ the set of neighbours of i. Recall that PHP_G consists of the following clauses

- $\bigvee_{k \in N(i)} x_{ik}$ for every $i \in [n+1]$; (pigeon axioms)
- $\overline{x}_{ik} \vee \overline{x}_{jk}$ for every $i \neq j \in [n+1]$ and $k \in N(i) \cap N(j)$. (hole axioms).

For any $i \in [n+1]$ and $k \in N(i)$ we consider an auxiliary polynomials q_{ik} defined as

$$q_{ik} := x_{ik} \cdot \prod_{\substack{\ell < k \\ \ell \in N(i)}} (1 - x_{i\ell}).$$

Note that q_{ik} is the polynomial translation of $\bigvee x_{i\ell} \vee \overline{x}_{ik}$ and hence satisfies $q_{ik}^2 = q_{ik}$ over Boolean values. Now the pigeon axioms translate into the form $1 - \sum_{k \in N(i)} q_{ik}$ and the products $q_{ik}q_{jk}$ for any $i \neq j \in [n+1]$ and $k \in N(i) \cap N(j)$ are easily derivable from the hole axioms.

Consider now the polynomials r_k defined as

$$r_k := \sum_{\substack{i \in [n+1] \\ i \in N(k)}} q_{ik}.$$

These polynomials are again Boolean valued as one can derive $r_k^2 - r_k$ easily from the pigeon axioms and the product $q_{ik}q_{jk}$. By adding up all the polynomial r_k we end up with an unsatisfiable instance of the basic knapsack formula

$$r_1 + \cdots + r_n - (n+1).$$

As observed before, this formula has small multilinear constant depth refutations. Now substituting back in this refutation the definitions of r_k and subsequently those of q_{ik} we obtain a small constant depth refutation of PHP_G of individual degree $O(\delta)$. □

The previous lemma demonstrate an unfortunate weakness of the restriction to bounded individual degree. The restriction has the effect that our proof system is not closed under substitutions — substituting multilinear formulas to a multilinear formula can yield a polynomial of very high individual degree. This makes it also hard to simulate rule-based propositional proof systems. The straightforward simulation quickly blows up the individual degree. Currently it is unclear which traditional propositional proof systems can be simulated by low depth and low individual degree IPS refutations, if any.

7 Barriers: Hardness for Boolean Instances

Recall that an instance consisting of a set of polynomials $\{f_i(\overline{x}) = 0\}_i$, for $f_i(\overline{x}) \in \mathbb{F}[\overline{x}]$, is said to be *Boolean* whenever $f_i(\overline{x}) \in \{0,1\}$ for $\overline{x} \in \{0,1\}^{|\overline{x}|}$. Here we show that for sufficiently strong proof systems the functional lower bound method cannot lead to lower bounds for Boolean instances (e.g., CNF formulas). And hence cannot settle major open problems in proof complexity about lower bounds against constant depth Frege proofs with counting modulo p gates ($\mathrm{AC}^0[p]$-Frege), as well as Threshold Logic system (TC^0-Frege).

Let $\mathbb{F}$ be field and $\mathcal{T} \in \mathbb{F}[\overline{x}]$ be a set of polynomials (that will stand for the set of polynomials we prove or derive, possibly encoded in different way; e.g., as Boolean formulas corresponding to their arithmetization). We say that a proof system P is a (sound and complete) *proof system for the set of polynomial equations from* $\mathcal{T}$ if given a set of polynomial equations $\{f_i(\overline{x}) = 0\}_i$ where $f_i \in \mathcal{T}$, there is a P-proof (equivalently, a P-derivation) of $g(\overline{x}) = 0$ with $g \in \mathcal{T}$, iff $g(\overline{x}) = 0$ is semantically implied by the equations, where semantic implication means:

$$\forall \overline{a} \in \mathbb{F}^n \left(\left(\bigwedge_i (f_i(\overline{a}) = 0) \right) \Rightarrow g(\overline{z}) = 0 \right).$$

The following is a more general setting for the functional lower bound method from the one in Theorem 1.

Definition 62 (General Functional Lower Bound Method)**.** *Let $\mathcal{C} \subseteq \mathbb{F}[\overline{x}]$ be a circuit class closed under (partial) field-element assignments (which stands as the class of "polynomials with small circuits"). Let $\mathcal{F} := \{f_i(\overline{x}) = 0\}_i$ be a collection of polynomial equations in $\mathcal{C}$, such that the system $\mathcal{F}$ and $\overline{x}^2 - \overline{x}$ is unsatisfiable (i.e., does not have a common root). A* ***functional lower bound against*** *$\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$* ***for*** *$\mathcal{F}$* ***and*** *$\overline{x}^2 - \overline{x}$ is a lower bound argument using the following three steps.*

1. *Circuit lower bound for $\frac{1}{f(\overline{x})}$: Let $f(\overline{x}) \in \mathcal{C}$ be a polynomial, where the system $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ is unsatisfiable. Suppose that $g \notin \mathcal{C}$ for all $g \in \mathbb{F}[\overline{x}]$ with*

$$g(\overline{x}) = \frac{1}{f(\overline{x})}, \quad \forall \overline{x} \in \{0,1\}^n.$$

   By Theorem 1 this means that $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ do not have $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$ refutations, and moreover, if $\mathcal{C}$ is a set of multilinear polynomials, then $f(\overline{x})$ and $\overline{x}^2 - \overline{x}$ do not have $\mathcal{C}$-IPS refutations.

2. *$\mathcal{F}$ is efficiently derivable from $f(\overline{x})$: Suppose that there is a $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$-proof of $\mathcal{F}$ from $f(\overline{x}) = 0$ (and $\overline{x}^2 - \overline{x}$) (it is possible that $\mathcal{F}$ is equal to $\{f(\overline{x})\}$).*

3. *Conclusion: Then, we can conclude by Item 1 that there is no $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$-refutations of $\mathcal{F}$ (otherwise, starting from $f(\overline{x}) = 0$, by Item 2 we can derive $\mathcal{F}$ and refute $f(\overline{x}) = 0$).*

Let P be a proof system for the language of polynomial equations in $\mathcal{C} \subseteq \mathbb{F}[\overline{x}]$, that is not necessarily equal to $\mathcal{C}$-$\mathrm{IPS}_{\mathrm{LIN}'}$. Let $\mathcal{F} := \{f_i(\overline{x}) = 0\}_i$ be polynomial equations in $\mathcal{C}$ and suppose we wish to establish a lower bound for $\mathcal{F}$ against P using the Functional Lower Bound Method. For this purpose, we take a proof system $\mathcal{C}'$-$\mathrm{IPS}_{\mathrm{LIN}'}$ that simulates P and such that $\mathcal{C}' \supseteq \mathcal{C}$, and prove a lower bound for $f(\overline{x}) = 0$ against $\mathcal{C}'$-$\mathrm{IPS}_{\mathrm{LIN}'}$, with $\mathcal{F}$ semantically implied by $f(\overline{x}) = 0$ and $\overline{x}^2 - \overline{x}$ (for $f(\overline{x}) \in \mathcal{C}'$).

We say that a circuit class $\mathcal{C}' \subseteq \mathbb{F}[\overline{x}]$ is *closed under polynomial many sum of products* if $h_i, g_i \in \mathcal{C}' \cap \mathbb{F}[x_1, \ldots, x_n]$, for $i \in I$ and $|I| = \mathsf{poly}(n)$, then $\sum_{i \in I} h_i \cdot g_i \in \mathcal{C}'$.

An *arithmetization scheme* denoted tr is any translation between Boolean formulas (or circuits) to polynomials, that maintains their functional behaviour over the Boolean cube. In other words, an arithmetization scheme is a mapping $\Gamma:$ Boolean formulas $\to \mathbb{F}[\overline{x}]$, such that for all $\overline{\alpha} \in \{0,1\}^n$, $\Gamma(\phi)(\overline{\alpha}) = 0$ iff $\phi(\overline{\alpha}) =$ TRUE (we can also flip "=0" to "=1" in $\Gamma(\phi)(\overline{\alpha}) = 0$ or use other pair of values in $\mathbb{F}$ to represent TRUE and FALSE). The standard one is the following: define tr inductively on the formula structure by $tr(x_i) := 1 - x_i$, $t(A \wedge B) = 1 - (1 - tr(A)) \cdot (1 - tr(B))$, and $tr(A \vee B) = tr(A) \cdot tr(B)$ and $tr(MOD_p(A_1, \ldots, A_r)) = (\sum_{i=1}^{r} tr(A_i))^{p-1})$.

Definition 63 (Sufficiently strong proof system)**.** *Let P be a proof system for a set of polynomial equations in $\mathcal{C}$, for some $\mathcal{C} \in \mathbb{F}[\overline{x}]$, that can be simulated by some $\mathcal{C}'$-IPS$_{\text{LIN}'}$ with $\mathcal{C}' \supseteq \mathcal{C}$ that is closed under partial assignments and sum of products. We say that P is a* ***sufficiently strong proof system*** *if there exists an arithmetization scheme $tr(\cdot)$ such that for every set of Boolean polynomial equations $\{f_i(\overline{x}) = 0\}_i$, there is a P-proof (equivalently, a P-derivation) of the arithmetization of $\bigwedge_i f_i$ of size $\mathsf{poly}(\sum_i |f_i|)$ (where $|f_i|$ denotes the size of the circuit computing f_i in $\mathcal{C}$).*

Examples of proof systems that are sufficiently strong (under the arithmetization tr shown above) are AC$^0[p]$-Frege, TC^0-Frege and constant-depth IPS. First note that AC$^0[p]$-Frege, for a prime p, can be viewed as a proof system for sets of polynomial equations in $\mathcal{T} \in \mathbb{F}[\overline{x}]$, where $\mathcal{T}$ consists of all standard arithmetizations of constant-depth Boolean formulas. And similarly, TC^0-Frege can be considered as operating with the set of constant depth polynomials over the integers. The fact that AC$^0[p]$-Frege, TC^0-Frege are sufficiently strong is immediate from the $\wedge$-introduction rules. The fact that constant-depth IPS$_{\text{LIN}}$ is sufficiently strong (under the arithmetization tr) stems from the fact that the $\wedge$-introduction rule can be easily simulated in constant-depth IPS$_{\text{LIN}}$ (cf. [GP18, PT16]) (using the arithmetization scheme tr).

Theorem 64 (Main barrier for Boolean instances)**.** *The functional lower bound method (Definition 62) cannot establish lower bounds for any* Boolean *instance against sufficiently strong proof systems (Definition 63).*[8] *In particular, it cannot establish any lower bounds against* AC$^0[p]$*-Frege,* TC^0*-Frege (and constant-depth* IPS$_{\text{LIN}'}$ *when the hard instances are Boolean).*

Proof: Let P be a sufficiently strong proof system for the set of polynomial equations $\mathcal{C} \in \mathbb{F}[\overline{x}]$, and suppose that $\mathcal{C}'$-IPS$_{\text{LIN}'}$ simulates P, for some $\mathcal{C} \subseteq \mathcal{C}' \subseteq \mathbb{F}[\overline{x}]$, that is closed under partial assignments and sum of products in the following sense: if $h_i, g_i \in \mathcal{C}' \cap \mathbb{F}[x_1, \ldots, x_n]$, for $i \in I$ and $|I| = \mathsf{poly}(n)$, then $\sum_{i \in I} h_i \cdot g_i \in \mathcal{C}'$. Let $\mathcal{F} := \{f_i(\overline{x}) = 0\}_i$ be a collection of polynomial equations in $\mathcal{C}$, where all $f_i(\overline{x})$ are Boolean.

We show that the following cannot all hold:

1. $g \notin \mathcal{C}'$ for all $g \in \mathbb{F}[\overline{x}]$ such that $g(\overline{x}) = \frac{1}{f(\overline{x})}$, $\forall \overline{x} \in \{0,1\}^n$.
2. There is a $\mathcal{C}'$-IPS$_{\text{LIN}'}$-proof of $\mathcal{F}$ from $f(\overline{x}) = 0$ and $\overline{x}^2 - \overline{x}$.
3. There is no $\mathcal{C}'$-IPS$_{\text{LIN}'}$-refutations of $\mathcal{F}$.

We show that if Item 2 and Item 3 above hold then Item 1 does not.

Inside $\mathcal{C}'$-IPS$_{\text{LIN}'}$, we start with $f(\overline{x})$ and derive $\mathcal{F}$ by assumption that Item 2 holds. Now, derive from $\mathcal{F}$ the polynomial $1 - \prod_i (1 - f_i(\overline{x}))$, by the assumption that P is sufficiently strong and that $\mathcal{C}'$-IPS$_{\text{LIN}'}$ simulates P. But this polynomial is always 1 over the Boolean cube, which implies

[8] Formally, we also require that the functional lower bound method is used on P, as in the proof, by lower bounding $\mathcal{C}$-IPS$_{\text{LIN}'}$, where $\mathcal{C} \in \mathbb{F}[\overline{x}]$ is closed under partial assignments and *polynomial many sum of products*.

that there is a polynomial-size circuit $g \in \mathcal{C}'$ such that $g(\overline{x}) = \frac{1}{f(\overline{x})}$, $\forall \overline{x} \in \{0,1\}^n$, contradicting Item 1 above. More formally, we have the following.

By Item 2,

$$\text{there exist } g_i \in \mathcal{C}' \text{ such that } g_i \cdot f(\overline{x}) = f_i(\overline{x}), \forall i. \tag{64.1}$$

By assumption that P is sufficiently strong and that $\mathcal{C}'$-IPS$_{\text{LIN}'}$ simulates P,

$$\text{there exist } h_i \in \mathcal{C}' \text{ such that } \sum_i h_i \cdot f_i(\overline{x}) = 1 - \prod_i (1 - f_i(\overline{x})). \tag{64.2}$$

Hence, since there is no Boolean assignment that satisfies all the Boolean axioms $f_i(\overline{x})$'s,

$$\left(\sum_i h_i \cdot g_i(\overline{x})\right) \cdot f(\overline{x}) = 1 - \prod_i (1 - f_i(\overline{x})) = 1 \mod \overline{x}^2 - \overline{x}. \tag{64.3}$$

By the assumption that $\mathcal{C}'$ is closed under polynomial many sum of products we know that $\sum_i h_i \cdot g_i(\overline{x}) \in \mathcal{C}'$, and so Equation (64.3) contradicts Item 1. □

7.1 Conclusion

This work wraps up to some extent research on IPS lower bounds via the functional lower bound method, showing how far it can be pushed, and where it cannot be applied. It generalises and improves previous work on IPS lower bounds obtained via the functional lower bound method in [FSTW21, GHT22]. We established size lower bounds for symmetric instances, and hard instances qualitatively different from previously known hard instances. This allows us also to show lower bounds over finite fields, which were open. We then showed how to incorporate recent developments on constant-depth algebraic circuit lower bounds [AGK+23] in the setting of proof complexity. This enables us to improve the constant-depth IPS lower bounds in [GHT22] to stronger fragments, namely IPS refutations of constant depth and $O(\log \log n)$-individual degrees. As a corollary, we show a new finite field functional lower bound for *multilinear formulas* which may be of independent interest.

As for the barrier we uncovered, it is now evident that the functional lower bound method *alone* cannot be used to settle the long-standing open problems about the proof complexity of constant-depth propositional proofs with counting gates. This does not rule out however the ability of IPS lower bounds, and the IPS "paradigm" in general, to progress on these open problems, since other relevant methods may be found helpful (the meta-complexity method established in [ST21], the lower bounds for multiples method [FSTW21, AF22], and the noncommutative reduction; see summary of methods at the end of Section 1.1). Moreover, our barrier only shows that we cannot hope to use a single non-Boolean unsatisfiable axiom $f(\overline{x}) = 0$ and consider the function $1/f(\overline{x})$ over the Boolean cube to obtain a CNF IPS lower bound (whenever the CNF is semantically implied from $f(\overline{x}) = 0$ over the Boolean cube). However, it does not rule out in general the use of a reduction to matrix rank, which is the backbone of many algebraic circuit lower bounds (as well as the functional lower bound method), and should potentially be helpful in proof complexity as well.

A very interesting problem that remains open is to prove CNF lower bounds using the functional method against fragments of IPS that sit below the reach of the barrier, namely fragments that cannot derive efficiently the conjunction of arbitrarily many polynomials (that is, systems that are not sufficiently strong in the above terminology).

References

[AF22] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: proving and using lower bounds for polynomial ideals. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, page 389402, New York, NY, USA, 2022. Association for Computing Machinery. Available from: https://doi.org/10.1145/3519935.3520025, doi:10.1145/3519935.3520025. (document), 1.1, 1.1, 7.1

[AGHT20] Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semi-algebraic proofs, ips lower bounds, and the τ-conjecture: can a natural number be negative? In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 5467, New York, NY, USA, 2020. Association for Computing Machinery. Available from: https://doi.org/10.1145/3357713.3384245, doi:10.1145/3357713.3384245. 1.1

[AGK+23] Prashanth Amireddy, Ankit Garg, Neeraj Kayal, Chandan Saha, and Bhargav Thankey. Low-Depth Arithmetic Circuit Lower Bounds: Bypassing Set-Multilinearization. In Kousha Etessami, Uriel Feige, and Gabriele Puppis, editors, *50th International Colloquium on Automata, Languages, and Programming (ICALP 2023)*, volume 261 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:20, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Available from: https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.ICALP.2023.12, doi:10.4230/LIPIcs.ICALP.2023.12. (document), 1.3.2, 1.3.2, 2, 6, 6.1, 6.1, 6.1.1, 46, 47, 6.1.1, 6.1.1, 6.1.2, 50, 6.1.2, 6.1.3, 52, 6.3, 7.1

[Ajt88] Miklós Ajtai. The complexity of the pigeonhole principle. In *Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science*, pages 346–355, 1988. 1.1

[Ale21] Yaroslav Alekseev. A Lower Bound for Polynomial Calculus with Extension Rule. In Valentine Kabanets, editor, *36th Computational Complexity Conference (CCC 2021)*, volume 200 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21:1–21:18, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Available from: https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2021.21, doi:10.4230/LIPIcs.CCC.2021.21. 1.1

[BIK+96a] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc. (3)*, 73(1):1–26, 1996. doi:10.1112/plms/s3-73.1.1. (document), 1.1, 2.4, 2.4

[BIK+96b] Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiří Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1996. doi:10.1007/BF01294258. (document), 1.1

[BPR97] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):708–728, 1997. Available from: https://doi.org/10.2307/2275569. 1.2

[CH97] H.E.A. Campbell and I.P. Hughes. Vector invariants ofu2(fp) : A proof of a conjecture of richman. *Advances in Mathematics*, 126(1):1–20, 1997. Available from: https://www.sciencedirect.com/science/article/pii/S000187089691590X, doi:https://doi.org/10.1006/aima.1996.1590. 1.3.1, 3.2, 3.2

[CLO15] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer Cham, fourth edition, 2015. doi:10.1007/978-3-319-16721-3. 2.3, 2.8, 3.2, 4.1

[DK15] Harm Derksen and Gregor Kemper. *Computational Invariant Theory*, volume 130 of *Encyclopaedia of Mathematical Sciences*. Springer, Berlin, Heidelberg, 2 edition, 2015. doi:10.1007/978-3-662-48422-7. 1.3.1, 3.2, 3.2

[DMM23] Yogesh Dahiya, Meena Mahajan, and Sasank Mouli. New lower bounds for polynomial calculus over non-boolean bases. *Electron. Colloquium Comput. Complex.*, TR23-132, 2023. Available from: https://eccc.weizmann.ac.il/report/2023/132, arXiv:TR23-132. 1.1

[dRGR22] Susanna F. de Rezende, Mika Göös, and Robert Robere. Guest column: Proofs, circuits, and communication. *SIGACT News*, 53(1):59–82, 2022. Available from: https://doi.org/10.1145/3532737.3532746, doi:10.1145/3532737.3532746. 1.3.2

[FKS16] Michael A. Forbes, Mrinal Kumar, and Ramprasad Saptharishi. Functional Lower Bounds for Arithmetic Circuits and Connections to Boolean Circuit Complexity. In Ran Raz, editor, *31st Conference on Computational Complexity (CCC 2016)*, volume 50 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 33:1–33:19, Dagstuhl, Germany, 2016. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Available from: https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2016.33, doi:10.4230/LIPIcs.CCC.2016.33. 1.2, 1.3.2, 1.3.2, 3.1

[For14] Michael A. Forbes. *Polynomial Identity Testing of Read-Once Oblivious Algebraic Branching Programs*. PhD thesis, Massachusetts Institute of Technology, June 2014. Available from: http://hdl.handle.net/1721.1/89843. 2.5, 2.5

[FS13] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 243–252. IEEE Computer Society, 2013. Available from: https://doi.org/10.1109/FOCS.2013.34, doi:10.1109/FOCS.2013.34. 2.4.1, 2.6, 17, 7.1

[FSTW21] Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. *Theory Comput.*, 17:1–88, 2021. Available from: https://theoryofcomputing.org/articles/v017a010/. (document), 1.1, 1.1, 1.1, 1.2, 1, 1.3, 1.3.1, 1.3.2, 1.3.2, 1.3.2, 1.3.2, 1.3.2, 2.4, 8, 2.4.1, 2.5, 2.5, 2.7, 2.8, 22, 3.1, 3.1, 4, 4.1, 4.1.1, 4.1.1, 4.1.2, 4.1.2, 36, 4.1.2, 4.1.2, 5, 5.2, 6, 6.3, 6.5, 7.1

[GH03] Dima Grigoriev and Edward A. Hirsch. Algebraic proof systems over formulas. *Theoretical Computer Science*, 303(1):83–102, 2003. Available from: https://www.sciencedirect.com/science/article/pii/S0304397502004462, doi:https://doi.org/10.1016/S0304-3975(02)00446-2. 1.1, 6.5, 6.5

[GHT22] Nashlen Govindasamy, Tuomas Hakoniemi, and Iddo Tzameret. Simple hard instances for low-depth algebraic proofs. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 188–199. IEEE, 2022. Available from: https://doi.org/10.1109/FOCS54457.2022.00025, doi:10.1109/FOCS54457.2022.00025. (document), ∗, ∗, 1.1, 1.1, 1.3.2, 1.3.2, 1.3.2, 6, 6.2, 6.3, 6.5, 7.1

[GKS20] Ankit Garg, Neeraj Kayal, and Chandan Saha. Learning sums of powers of low-degree polynomials in the non-degenerate case. In Sandy Irani, editor, *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 889–899. IEEE, 2020. doi:10.1109/FOCS46700.2020.00087. 1.3.2

[GP18] Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–37:59, 2018. Available from: https://doi.org/10.1145/3230742, doi:10.1145/3230742. (document), 1.1, 1.1, 1.3.3, 2.4, 8, 8, 7

[Gri98] Dima Grigoriev. Tseitin's tautologies and lower bounds for Nullstellensatz proofs. In *IEEE Symposium on Foundations of Computer Science*, pages 648–652, 1998. doi:10.1109/SFCS.1998.743515. 6.5

[Gro23] Joshua A. Grochow. Polynomial identity testing and the ideal proof system: PIT is in NP if and only if IPS can be p-simulated by a cook-reckhow proof system. *CoRR*, abs/2306.02184, 2023. Available from: https://doi.org/10.48550/arXiv.2306.02184, arXiv:2306.02184, doi:10.48550/ARXIV.2306.02184. 1.3.3

[IMP23] Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. Lower Bounds for Polynomial Calculus with Extension Variables over Finite Fields. In Amnon Ta-Shma, editor, *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 7:1–7:24, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Available from: https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2023.7, doi:10.4230/LIPIcs.CCC.2023.7. 1.1

[IPS99] 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. doi:10.1007/s000370050024. 1.3

[Kno17] Alexander Knop. IPS-like proof systems based on binary decision diagrams. *Electron. Colloquium Comput. Complex.*, TR17-179, 2017. Available from: https://eccc.weizmann.ac.il/report/2017/179, arXiv:TR17-179. 1.1

[KPW95] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995. Available from: https://doi.org/10.1002/rsa.3240070103. 1.1

[Kra97] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997. Available from: https://doi.org/10.2307/2275541. 1.2

[LST21] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 804–814. IEEE, 2021. Available from: https://doi.org/10.1109/FOCS52979.2021.00083, doi:10.1109/FOCS52979.2021.00083. 1.1, 1.3.2, 6, 6.4

[LTW18] Fu Li, Iddo Tzameret, and Zhengyu Wang. Characterizing propositional proofs as noncommutative formulas. *SIAM Journal on Computing*, 47(4):1424–1462, 2018. Available from: https://doi.org/10.1137/16M1107632, doi:10.1137/16M1107632. 1.1, 1.1, 2.4.1

[Nis91] Noam Nisan. Lower bounds for non-commutative computation. In *Proceedings of the Annual ACM Symposium on the Theory of Computing 1991*, pages 410–418, 1991. doi:10.1145/103418.103462. 9, 2.4.1, 12

[PBI93] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *computational complexity*, 3(2):97–140, 1993. Available from: https://doi.org/10.1007/BF01200117, doi:10.1007/BF01200117. 1.1

[Pit97] Toniann Pitassi. Algebraic propositional proof systems. In Neil Immerman and Phokion G. Kolaitis, editors, *Descriptive Complexity and Finite Models, Proceedings of a DIMACS Workshop 1996, Princeton, New Jersey, USA, January 14-17, 1996*, volume 31 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 215–244, Providence, RI, 1997. American Mathematical Society. Available from: https://doi.org/10.1090/dimacs/031/07, doi:10.1090/DIMACS/031/07. 1.1

[Pit98] Toniann Pitassi. Unsolvable systems of equations and proof complexity. In *Proceedings of the International Congress of Mathematicians, Berlin, 1998*, volume Extra Vol. ICM Berlin 1998, Vol. III, pages 451–460, 1998. doi:10.4171/DMS/1-3/44. 1.1

[PT16] Toniann Pitassi and Iddo Tzameret. Algebraic proof complexity: progress, frontiers and challenges. *ACM SIGLOG News*, 3(3):2143, aug 2016. Available from: https://doi.org/10.1145/2984450.2984455, doi:10.1145/2984450.2984455. 1.1, 1.3.2, 2.4, 7

[Raz98] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998. 6.5

[Raz06] Ran Raz. Separation of multilinear circuit and formula size. *Theory of Computing*, 2(6):121–135, 2006. Preliminary version appeared in IEEE Annual Symposium on Foundations of Computer Science 2004. doi:10.4086/toc.2006.v002a006. 2.7

[Raz09] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, 56(2), 2009. Preliminary version appeared in Proceedings of the Annual ACM Symposium on the Theory of Computing 2004. doi:10.1145/1502793.1502797. 2.7, 20, 5.2

[Ric90] David R Richman. On vector invariants over finite fields. *Advances in Mathematics*, 81(1):30–65, 1990. Available from: https://www.sciencedirect.com/science/article/pii/0001870890900036, doi:https://doi.org/10.1016/0001-8708(90)90003-6. 1.3.1, 3.2, 3.2

[RT08a] Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008. Available from: http://dx.doi.org/10.1016/j.apal.2008.04.001, doi:10.1016/j.apal.2008.04.001. 1.1

[RT08b] Ran Raz and Iddo Tzameret. The strength of multilinear proofs. *Computational Complexity*, 17(3):407–457, 2008. Available from: http://dx.doi.org/10.1007/s00037-008-0246-0, doi:10.1007/s00037-008-0246-0. 1.1, 6.5

[RY08] Ran Raz and Amir Yehudayoff. Balancing syntactically multilinear arithmetic circuits. *Computational Complexity*, 17(4):515–535, 2008. doi:10.1007/s00037-008-0254-0. 2.7, 20

[RY09] Ran Raz and Amir Yehudayoff. Lower bounds and separations for constant depth multilinear circuits. *Computational Complexity*, 18(2):171–207, 2009. Preliminary version appeared in IEEE Conference on Computational Complexity CCC 2008. doi:10.1007/s00037-009-0270-8. 2.7, 20, 5.2

[Sap12] Ramprasad Saptharishi, 2012. Personal communication to Forbes-Shpilka [FS13]. 1.3.2, 2.6, 16

[Sap22] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity, 2016-2022. Available from: https://github.com/dasarpmar/lowerbounds-survey/releases. 2.2

[Sax08] Nitin Saxena. Diagonal circuit identity testing and lower bounds. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Automata, Languages and Programming*, pages 60–71, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg. Available from: https://doi.org/10.1007/978-3-540-70575-8_6. 1.1

[Sok20] Dmitry Sokolov. (semi)algebraic proofs over ± 1 variables. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 78–90. ACM, 2020. Available from: https://doi.org/10.1145/3357713.3384288, doi:10.1145/3357713.3384288. 1.1

[ST21] Rahul Santhanam and Iddo Tzameret. Iterated lower bound formulas: a diagonalization-based approach to proof complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, page 234247, New York, NY, USA, 2021. Association for Computing Machinery. Available from: https://doi.org/10.1145/3406325.3451010, doi:10.1145/3406325.3451010. 1.1, 7.1

[SW01] Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complexity*, 10:1–27, 2001. 6.5

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. 2.2

[Tza11] Iddo Tzameret. Algebraic proofs over noncommutative formulas. *Inf. Comput.*, 209(10):1269–1292, 2011. Available from: http://dx.doi.org/10.1016/j.ic.2011.07.004, doi:10.1016/j.ic.2011.07.004. 1.1, 1.1, 2.4.1

— Page left blank for ECCC stamp —