Electronic Colloquium on Computational Complexity, Report No. 98 (2025)

IPS Lower Bounds for Formulas and Sum of ROABPs

Prerona Chatterjee* Utsab Ghosal† Partha Mukhopadhyay‡ Amit Sinhababu§

July 11, 2025

Abstract

We give new lower bounds for the fragments of the Ideal Proof System (IPS) introduced by Grochow and Pitassi [GP18]. The Ideal Proof System is a central topic in algebraic proof complexity developed in the context of Nullstellensatz refutation [BIK+94] and simulates Extended Frege efficiently. Our main results are as follows.

- mult-IPS$_{\mathsf{Lin}'}$: We prove nearly quadratic-size formula lower bound for multilinear refutation (over the Boolean hypercube) of a variant of the subset-sum axiom polynomial. Extending this, we obtain a nearly matching qualitative statement for a constant degree target polynomial.
- IPS$_{\mathsf{Lin}'}$: Over the fields of characteristic zero, we prove exponential-size sum-of-ROABPs lower bound for the refutation of a variant of the subset-sum axiom polynomial. The result also extends over the fields of positive characteristics when the target polynomial is suitably modified. The modification is inspired by the recent results [HLT24, BLRS25].

The mult-IPS$_{\mathsf{Lin}'}$ lower bound result is obtained by combining the quadratic-size formula lower bound technique of Kalorkoti [Kal85] with some additional ideas. The proof technique of IPS$_{\mathsf{Lin}'}$ lower bound result is inspired by the recent lower bound result of Chatterjee, Kush, Saraf and Shpilka [CKSS24].

*Department of Mathematics, IIT Madras, Chennai, India. Email: prerona.ch@gmail.com
†Chennai Mathematical Institute, Chennai, India. Partially supported by Infosys grant. Email : ghosal@cmi.ac.in.
‡Chennai Mathematical Institute, Chennai, India. Partially supported by Infosys grant. Email : partham@cmi.ac.in.
§Chennai Mathematical Institute, Chennai, India. Partially supported by Infosys grant. Email : amitks@cmi.ac.in.

ISSN 1433-8092

1 Introduction

The main goal in propositional proof complexity is to prove lower bounds for computational resources required to prove propositional tautologies. This task in its full generality is strongly related to the separation problem of NP and coNP as shown by Cook and Reckhow [CR79]. Among the propositional proof systems, the Frege proof system is very well studied since the early work by Reckhow [Rec76]. In Frege proofs, the propositions are computable by *formulas* and lower bounds for the Frege system remain notoriously open. In the restricted setting, strong lower bounds for AC^0-Frege proof systems are known [Ajt88, BPI92, KPW95]. In an attempt to address the Frege lower bounds via algebraic methods, Beame, Cook, and Hoover [BCH94], and Pitassi and Impagliazzo [PI94], introduced the Nullstellensatz proof system. The weak version of Hilbert's Nullstellensatz says that a set of polynomials (usually called *axioms*) $f_1(\bar{x}), \ldots, f_m(\bar{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ is unsatisfiable (over the algebraic closure of $\mathbb{F}$) if and only if there are polynomials $g_1(\bar{x}), \ldots, g_m(\bar{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\sum_{j=1}^{m} g_j(\bar{x}) f_j(\bar{x}) = 1$. The coefficients $g_1, \ldots, g_m$ are the Nullstellensatz refutations of the axioms. The *degree* and the *sparsity* are two important notions of the size measure for the refutations, and the lower bounds for them are known [BIK+94]. However, the hard examples used in all such lower bound results admit polynomial-size Frege proofs. To overcome this, stronger algebraic proof systems were introduced that measure the size by the minimal size of the circuits computing the refutation polynomials $g_i(\bar{x})$. More precisely, this led to the Ideal Proof System (IPS) formulated by Grochow and Pitassi [GP18], where the refutation of $f_1(\bar{x}), \ldots, f_m(\bar{x})$ over the Boolean hypercube satisfies the equation

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

and $g_i(\bar{x}), h_j(\bar{x})$ are represented by algebraic circuits. The size of an IPS refutation is the total size of the circuits computing the polynomials g_i and h_i. Further formal description is given in Definition 2.5. The work of Grochow and Pitassi [GP18, Pit96] shows that IPS is powerful enough to polynomially simulate the Frege and the Extended Frege systems, making IPS lower bounds an important avenue of further research. The work of Forbes, Sphilka, Tzameret, and Wigderson [FSTW21] addresses fragments of linear IPS in models like ROABPs, multilinear formulas (both unrestricted and constant depth), and for some class of constant depth formulas. In another interesting line of work, Lee, Tzameret, and Wang [LTW18] connect the Frege lower bounds with noncommutative IPS lower bounds. More recently, the breakthrough result for the constant-depth circuit lower bounds by Limaye, Srinivasan, and Tavenas [LST21] led to a flurry of activities in this area [AF22, GHT22, HLT24]. Even over the fields of positive characteristic, new IPS lower bounds are shown [BLRS25, EGLT25]. These results are inspired by the result of Forbes [For24] on constant-depth circuit lower bounds in positive characteristic.

In this paper, we address the IPS lower bound problem in the setting of general algebraic

formulas. Note that the current best-known (general) formula size lower bound for an explicit polynomial is given by techniques due to Kalorkoti [Kal85][1]. We lift this result to the IPS setting by giving nearly similar quality lower bounds for general formulas, and the axiom polynomial is a variant of the subset-sum polynomial. More precisely, we prove the lower bound for mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ as detailed in Section 1.1. In fact, we are able to show such a lower bound (slightly weaker) even for a subset-sum axiom polynomial of *constant degree*. In recent times, proving polynomial-quality lower bounds for constant-degree polynomials has received considerable attention since this is generally considered to be an avenue to improve the state-of-the-art polynomial-quality lower bounds for various algebraic models [HY09, CKV24].

Next, we consider the IPS lower bound question for the sum-of-ROABPs model. Besides being a natural extension to the works that study the same question for ROABPs [FSTW21, HLT24, BLRS25, EGLT25], this model has an additional motivation in the context of VBP vs VNP conjecture. In particular, inspired by the connection that Bhargav, Dwivedi, and Saxena observe in the context of Valiant's VBP vs VNP conjecture [BDS25], the work of Chatterjee, Kush, Saraf, and Shpilka [CKSS24] shows exponential-size lower bounds for sum-of-ROABPs model. Our result can be seen as a lift of those in [CKSS24] to the IPS setting.

Both the results use the functional lower bound technique from [FSTW21, Lemma 5.1]. In particular, it shows that proving any refutation of the unsatisfiable system $\{f = 0,\ \bar{x}^2 - \bar{x} = 0\}$ is not in a circuit class $\mathcal{C}$ is equivalent to proving that each $g(\bar{x})$ which agrees with $\frac{1}{f(\bar{x})}$ over the Boolean hypercube, is not in $\mathcal{C}$.

For our first result, to show that any multilinear-$\mathsf{IPS}_{\mathsf{Lin}'}$ refutation of the system $\{f = 0, \bar{x}^2 - \bar{x} = 0\}$ requires a quadratic-size formula lower bound, note that it suffices to show that the unique multilinear polynomial $g(\bar{x})$ which agrees with $\frac{1}{f(\bar{x})}$ over the Boolean hypercube also requires a quadratic-size formula lower bound. This follows from the properties of the multilinear-$\mathsf{IPS}_{\mathsf{Lin}'}$ model as explained in Definition 2.5, Definition 2.6. This was first formulated in the work of Govindasamy, Hakoniemi and Tzameret [GHT22].

For our second result, observe that the sum of ROABPs can be multilinearized, just like ROABPs (Proposition 4.4). Hence, to show $\mathsf{IPS}_{\mathsf{Lin}'}$ lower bound in the sum of ROABPs model for any refutation of the unsatisfiable system $\{f = 0,\ \bar{x}^2 - \bar{x} = 0\}$, it is sufficient to a lower bound on the size of any sum of ROABPs computing the unique multilinear polynomial $g(\bar{x})$ which agrees with $\frac{1}{f(\bar{x})}$ over the Boolean hypercube.

1.1 Our Results

We now state our main results.

[1] Also see [CKSV22], [SY10, Section 3.2].

Formula Lower Bounds

We first define the target polynomial f for the unsatisfiable system.

Let $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_0, \ldots, y_{n-1}\}$ be two sets of variables. We partition X into $N = \frac{n}{\log n}$ parts $\{X_1, \ldots, X_N\}$ where $X_i = \{x_{(i-1)\log n+1}, \ldots, x_{i \log n}\}$ for each $i \in N$. Clearly, the size of each X_i is $\log n$.

Fix any $i \in [N]$. For each subset $S \subseteq X_i$, let $\Pi_S \in \{0,1\}^{\log n}$ be its characteristic vector, and define $t(S) = \sum_{j=1}^{\log n} \Pi_S[j] \cdot 2^{j-1}$. Clearly, for any $s \in [0, \ldots, n-1]$ there is a unique S such that $s = t(S)$. We define the polynomials,

Equation 1.1.

$$f'(\bar{x}, \bar{y}) = \sum_{i=1}^{N} \sum_{S \subseteq X_i} \left(\prod_{j \in S} x_j \cdot y_{t(S)} \right). \tag{1.1}$$

Equation 1.2.

$$f(\bar{x}, \bar{y}) = \begin{cases} f' + 1 & \text{if the characteristic of } \mathbb{F} = 0 \\ f' + \beta & \text{if the characteristic of } \mathbb{F} = p > 0,\ k > 0 \in \mathbb{Z}, \\ & \beta \in \mathbb{F}_{p^{k+1}} \setminus \mathbb{F}_{p^k} \text{ and } f' \in \mathbb{F}_{p^k}[X, Y] \end{cases} \tag{1.2}$$

Clearly, f is unsatisfiable over the Boolean hypercube.

Using this unsatisfiable system $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$, we show our first lower bound result. Note that the degree of f is $\log n + 1$ and sparsity is $O\left(\frac{n^2}{\log n}\right)$.

Theorem 1.3. *Consider the polynomial f is defined in Equation 1.2. Then the following statements are true :*

- *Over the fields of characteristic 0, any formula computing a* mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega\left(\frac{n^2}{\log n}\right)$.*
- *Over the fields of characteristic p, any formula computing the* mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system of equations $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega\left(\frac{n^2}{\log n}\right)$.*

Next, we describe a constant degree set-multilinear polynomial which is unsatisfiable over the Boolean hypercube such that any multilinear proof of unsatisfiability requires near quadratic formula size. We first state a fact about the set-multilinear polynomials.

Fact 1.4. *Let $X = \bigsqcup_{i=1}^{n} X_i$ be a set of variables such that $|X_i| = \ell$ and $X_i = \{x_{i,j} : j \in [\ell]\}$. Then the number of set-multilinear monomials respecting the partition $X_1, \ldots, X_n$ is ℓ^n. Another way to see it is that any set-multilinear monomial $m = \prod_{i=1}^{n} x_{i,j_i}$ defines uniquely a map $\tau_m : [n] \to [\ell]$, with $\tau_m(i) = j_i$. The number of such possible distinct maps is ℓ^n.*

We now define the constant-degree polynomial.

Let $c > 3$. Further, let $X = \{x_{i,j} : i \in [c], j \in [n^2/c]\}$ and $Y = \{y_{i,j} : i, j \in [n]\}$ be sets of variables. The polynomial we will be defining, say $f \in \mathbb{F}[X, Y]$, is set-multilinear with respect to the partition $\{X_1, \ldots, X_c, Y\}$ where $X_i = \{x_{i,j} : j \in [n^2/c]\}$.

We further partition X_i into $n^{2(1-1/c)}/c$ parts, each of size $n^{2/c}$, and denote it by $X_{i,k}$ for $k \in [n^{2(1-1/c)}/c]$. So now, for any $i \in [c]$ and $k \in [n^{2(1-1/c)}/c]$,

$$X_{i,k} = \left\{x_{i,j} : j \in \left\{(k-1)(n^{2/c}) + 1, \ldots, k(n^{2/c})\right\}\right\}$$

By Fact 1.4, it is easy to see that the number of set-multilinear monomials over the variable set $X^{(k)} = X_{1,k} \sqcup \cdots \sqcup X_{c,k}$ is $(n^{2/c})^c = n^2$.

Note that $|Y| = n^2$. Thus, for any $k \in [n^{2(1-1/c)}/c]$, we can define a bijection, say $\pi_k : \mathcal{M}_{\text{sm}}[X^{(k)}] \to Y$, which maps each set-multilinear monomial to a unique variable in Y. For any such k, we define the set-multilinear polynomial h_k of degree $c+1$, over the variable set $X_{1,k} \sqcup \cdots \sqcup X_{c,k} \sqcup Y$, as $h_k = \sum_{m \in \mathcal{M}_{\text{sm}}[X^{(k)} \sqcup Y]} m \cdot \pi_i(m)$. We then define the polynomial,

Equation 1.3.

$$h'(X, Y) = \sum_{k=1}^{n^{2(1-1/c)}/c} h_k. \tag{1.5}$$

Equation 1.4.

$$h(X, Y) = \begin{cases} h' + 1 & \text{if the characteristic of } \mathbb{F} = 0 \\ h' + \beta & \text{if the characteristic is } p > 0,\ k > 0 \in \mathbb{Z}, \\ & \beta \in \mathbb{F}_{p^{k+1}} \setminus \mathbb{F}_{p^k} \text{ and } h' \in \mathbb{F}_{p^k}[X, Y] \end{cases} \tag{1.6}$$

Note that the system of equations $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$ is clearly unsatisfiable. Further h is a polynomial over n^2 variables of sparsity $n^{4-2/c}/c$ and degree $c+1$. Using this system, we show our second lower bound result.

Theorem 1.7. *Consider the polynomial h in Equation 1.6. Then the following statements are true.*

- *Over the fields of characteristic 0, any formula computing a* mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega(n^{4-2/c})$.*
- *Over the fields of characteristic p, any formula computing a* mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at-least $\Omega\left(n^{4-2/c}\right)$.*

Remark 1.8. *Since f and h are sparse polynomials, they can be obtained by substitutions of monomials in the usual subset-sum axiom polynomial of the form $\sum_i z_i - \gamma$. See Appendix A for further details.* ◊

Remark 1.9. *We also note that the unsatisfiable systems given by f and h have* non-multilinear *refutations of polynomial size constant depth formulas. This follows easily from the known results [FSTW21, BLRS25]. A proof sketch is given in Appendix A for completeness.* ◊

Sum of ROABPs Lower Bounds

Over the fields of characteristic 0, we use a variant of the subset-sum polynomial to show exponential-size lower bound for the $\mathsf{IPS}_{\mathsf{Lin}'}$ refutations in the sum of ROABPs model. The same polynomial has been used earlier to prove exponential-size lower bound for $\mathsf{IPS}_{\mathsf{Lin}'}$ refutations in (any order) ROABPs model [FSTW21]. More precisely, we prove the following.

Theorem 1.10. *For $X = \{x_0, \ldots, x_{2n-1}\}$, $T = \{t_{i,j} : i, j \in [0, \ldots, 2n-1] \text{ with } i < j\}$ and $\beta = 2^{\binom{2n}{2}}$, let $f \in \mathbb{F}[X, T]$ be the polynomial defined as*

$$f = \left(\sum_{0 \le i < j \le 2n-1} t_{i,j} x_i x_j \right) - \beta$$

which is unsatisfiable over the Boolean hypercube. Then there exists $\gamma > 0$ such that the total width of any sum of ROABP *computing the linear proof of unsatisfiability ($\mathsf{IPS}_{\mathsf{Lin}'}$), for the system $\{f = 0, X^2 - X = 0, T^2 - T = 0\}$, is at-least* $\exp(n^\gamma)$.

Similar lower bounds can be achieved over the fields of positive characteristic as well. We refer the readers to Section 4.3 for further details.

Remark 1.11. *Further, we note that there is a* non-multilinear *refutation of the unsatisfiable system given by f which is computable by* $\mathrm{poly}(n)$ *size ABP. More details can be found in Appendix A.* ◊

1.2 Proof Sketches

Formula lower bounds The main ideas behind the mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ lower bounds in the formula model (Theorem 1.3, and Theorem 1.7) are based on the techniques from [Kal85] and the functional lower bound method of [FSTW21]. The functional method shows that, the proof of a $\mathcal{C}$-$\mathsf{IPS}_{\mathsf{Lin}'}$ lower bound for the unsatisfiable system $\{f = 0, x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0\}$, is equivalent to the fact that every polynomial $g(\bar{x})$ that agrees with $\frac{1}{f(\bar{x})}$ over the Boolean hypercube satisfies that $g \notin \mathcal{C}$. Since our goal is to show a formula lower bound in the mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ model, it suffices to show that the unique multilinear polynomial g that agrees with $\frac{1}{f}$ over the Boolean hypercube requires nearly quadratic size formulas.

Let $X = \{x_1, \ldots, x_n\}$ and $f \in \mathbb{F}[X]$. For a subset $S \subseteq X$, one can express the polynomial $f = \sum_{m \in \mathcal{M}[S]} m \cdot f_m$, where $\mathcal{M}[S]$ is the set of monomials defined on S and $f_m \in \mathbb{F}[X \setminus S]$. Let

$\mathsf{coeff}_S(f) := \{f_m : m \in \mathcal{M}[S], f_m \neq 0\}$ and $\mathsf{alg\text{-}rank}_S(f)$ be the algebraic rank of $\mathsf{coeff}_S(f)$. The main result of [Kal85] states that, if f is computable by a formula of size s, then for any partition $X_1 \sqcup X_2 \sqcup \ldots \sqcup X_t$, we have that $s \geq \Omega\left(\sum_{i=1}^{t} \mathsf{alg\text{-}rank}_{X_i}(f)\right)$.

It is a well-known fact that for any set of polynomials, the algebraic rank is lower bounded by the algebraic rank of their leading or trailing monomials. We would like to apply Kalorkoti's method on the unique multilinear polynomial g that agrees with $\frac{1}{f}$ over the Boolean hypercube. To do that, we need to study the relationship between the support structure of f and g.

Note that our polynomials have the property that for any two monomials, the support of one is not contained in the other. We show that for any polynomial f that satisfies this property, $\mathsf{supp}(f) \subseteq \mathsf{supp}(g)$ (Proposition 3.1). Furthermore, if a monomial m cannot be written as a multilinearized product of monomials from $\mathsf{supp}(f)$, then its coefficient in g is 0 (Lemma 3.3). Using these, it can be observed that for any $S \subseteq X$, the trailing monomials (under graded-lex ordering) of $\mathsf{coeff}_S(g)$ are equal to the trailing monomials of $\mathsf{coeff}_S(f)$.

Under the partition $X_1 \sqcup \cdots \sqcup X_N$ considered in the definition of Equation 1.2, since $\mathsf{coeff}_{X_i}(f)$ is a set of algebraically independent monomials, the trailing monomials in $\mathsf{coeff}_{X_i}(g)$ are also algebraically independent. The result now follows from [Kal85].

Sum of ROABPs Lower Bounds The $\mathsf{IPS}_{\mathsf{Lin}'}$ lower bound for the sum of ROABPs model combines techniques from the works of Forbes, Shpilka, Tzameret and Wigderson [FSTW21] and Chatterjee, Kush, Saraf, and Shpilka [CKSS24]. Similar to the formula setting, it is enough to show a lower bound against all polynomials g that agree with $1/f$ over the Boolean hypercube. Additionally, since sum of ROABPs can be efficiently multilinearized (Proposition 4.4), it is enough to show a lower bound against the unique multilinear polynomial satisfying the above property.

The proof broadly consists of two parts. The first part is to establish a structural weakness of the sum of ROABPs. Roughly speaking, under a random partition of the variables, the rank of the partial derivative matrix of a polynomial computed efficiently by a sum of ROABPs is low with high probability (Lemma 4.7). The proof is developed using the ideas implicit in [CKSS24]. On the other hand, for any balanced partition, the derivative matrix corresponding to the unique multilinear polynomial g that agrees with $1/f$ (where f is defined in Theorem 1.10) has high rank ([FSTW21]). The lower bound follows by combining these two statements.

Organization

In Section 2, we present the necessary definitions and preliminary concepts. Section 3 details the proofs of our results on formula lower bounds. The results on the sums of ROABPs is presented in Section 4. The conclusion raises a few questions for further study and the appendix provides some additional observations.

2 Preliminaries

We begin by stating the Chernoff Bound.

Theorem 2.1 (Chernoff Bound). *Let $X_1, \ldots, X_n$ be a set of* 0-1 *independent random variables. Let $X = \sum_{i=1}^{n} X_i$ and $\mu = \mathbb{E}[X]$ is the expected value of X. Then for any $\delta \in (0,1)$,*

$$\Pr[X \leq (1-\delta)\mu] \leq \exp\left(-\frac{\delta^2 \mu}{2}\right).$$

2.1 Notations

For a set X, a partition is written as $X = X_1 \sqcup \cdots \sqcup X_k$. The set of natural numbers is $\mathbb{N}$. For $n \in \mathbb{N}$, the set $\{1, \ldots, n\}$ is denoted by $[n]$. The symmetric group over $\{1, 2, \ldots, n\}$ is S_n. For notational clarity, sometime $\bar{x}$ or X is used for the set of variables $\{x_1, \ldots, x_n\}$. The set of all possible monomials over X is denoted by $\mathcal{M}(X)$. The set of equations $\{x_i^2 - x_i = 0 \,:\, i \in [n]\}$ is sometime shorten as $X^2 - X$. For $\{a_1, \ldots, a_n\} \subseteq \mathbb{N}$, we denote by $\bar{x}^{\bar{a}}$, the monomial $\prod_{i \in [n]} x_i^{a_i}$. Given a monomial $\bar{x}^{\bar{a}}$, define $\mathsf{supp}(\bar{x}^{\bar{a}})$ to be the set $\{x_i \,:\, a_i \geq 1\}$. Given a monomial $\bar{x}^{\bar{a}}$, we define $\mathsf{mult}(\bar{x}^{\bar{a}})$ to be the multilinear version of the monomial. That is, $\mathsf{mult}(\bar{x}^{\bar{a}}) = \prod_{i=1}^{n} x_i^{\min\{a_i, 1\}}$. By linearity, we extend this to define $\mathsf{mult}(f)$ for any polynomial $f \in \mathbb{F}[X]$.

For a subset $S \subseteq [n]$, we denote by $\mathbb{1}_S : [n] \to \{0,1\}$ the characteristic function for S. That is, for any $i \in [n]$, $\mathbb{1}_S(i) = 1 \iff i \in S$.

2.2 Definitions

Models of Computation

Definition 2.2 (Algebraic Formulas). *An algebraic formula C is a directed tree with a unique output gate (root) of out-degree* 0*, and input gates of in-degree* 0 *(leaves) labeled by variables $x_1, \ldots, x_n$ or constants from $\mathbb{F}$. The internal gates are labeled by $+$ or $\times$. Each gate v computes a polynomial f_v defined recursively: if v is an input, then $f_v = \mathsf{label}(v) \in \{x_1, \ldots, x_n\} \cup \mathbb{F}$; if $v = u \ \mathsf{op}\ w$ for $\mathsf{op} \in \{+, \times\}$, then $f_v = f_u \ \mathsf{op}\ f_w$. The polynomial computed at the output gate is the polynomial computed by the formula.* $\lozenge$

Definition 2.3 (ROABPs). *A Read-once Oblivious ABP* (ROABP) *is a directed acyclic graph where the vertex set is partitioned into layers $0, 1, \ldots, n$ with directed edges only between adjacent layers (i to $i+1$). Layers* 0 *and n have a single vertex each (called the source s and terminal t respectively), whereas the other layers can have any number of vertices.*

The labels on the edges satisfy the property that for every $i \in [n]$, there is a unique $j \in [n]$ such that every edge in between layer $j-1$ and j is labelled by a univariate polynomial in x_i. The polynomial computed by any s-to-t path is the product of the edge labels on it and the polynomial computed by the ROABP *is the sum of all polynomials computed by such paths.*

An ROABP *is said to have order $\sigma \in S_n$ if for every $j \in [n]$, the edges in between layers $j-1$ and j are labelled by univariates in $x_{\sigma(j)}$. An* ROABP *is said to be multilinear if each of the edge labels are linear polynomials.*

The size of an ROABP *is the total number of vertices in it; the width of any layer in the* ROABP *is the number of vertices in it and the width of an* ROABP *is the width of its widest layer. A sum of* ROABP*s is defined as the sum of individual* ROABP*s, with total width equal to the sum of their widths.* ◊

Definition 2.4 (Set-Multilinear Polynomial)**.** *Let $(X_1, \ldots, X_d)$ be a partition of the variable set X, with $X_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,n}\}$. A polynomial $f \in \mathbb{F}[X]$ is said to be set-multilinear with respect to the given partition if each monomial in f is of the form $(x_{1,j_1} x_{2,j_2} \cdots x_{d,j_d})$.* ◊

It is sometimes useful to think of the variables as coming from a matrix $M_{d \times n}$ where the i^{th} row is $\{x_{i,1}, x_{i,2}, \ldots, x_{i,n}\}$ and a set-multilinear polynomial is one in which each monomial is constructed by picking exactly one variable from each row.

Ideal Proof System

We begin with the definition of the Ideal Proof System (IPS) and some of its restrictions.

Definition 2.5 (Ideal Proof System [FSTW21, GP18])**.** *Let $f_1, \ldots, f_m \in \mathbb{F}[X]$ be a set of polynomials such that $\{f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\}$ has no common solution over the Boolean hypercube*[2]*.*

A proof *of the unsatisfiability of this set of polynomial equations, in the* Ideal Proof System (IPS)*, is a polynomial $P(X, y_1, \ldots, y_m, z_1, \ldots, z_n) \in \mathbb{F}[X, Y, Z]$ such that the following holds:*

- $P(X, \bar{0}, \bar{0}) = 0$;
- $P(X, f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n) = 1$. ◊

Definition 2.6 (Restrictions of IPS [GHT22, HLT24])**.** *Some restrictions of the Ideal Proof System that we will be considering are as follows.*

- $\mathsf{IPS}_{\mathsf{Lin}}$*: A proof, P, in the Ideal Proof System is said to be in* $\mathsf{IPS}_{\mathsf{Lin}}$ *if it additionally satisfies the conditions $\forall i \in [n], \deg_{y_i}(P), \deg_{z_i}(P) \leq 1$.*
- $\mathsf{IPS}_{\mathsf{Lin}'}$*: A proof, P, in the Ideal Proof System is said to be in* $\mathsf{IPS}_{\mathsf{Lin}'}$ *if it only satisfies the conditions $\forall i \in [n], \deg_{y_i}(P) \leq 1$.*
- mult-$\mathsf{IPS}_{\mathsf{Lin}'}$*: A proof, P, in* $\mathsf{IPS}_{\mathsf{Lin}'}$ *is said to be in* mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *if it additionally satisfies the condition that $P(X, Y, \bar{0})$ is multilinear polynomial. Note that $P(X, \bar{0}, Z)$ is not necessarily multilinear.*
- $\mathcal{C}$-$\mathsf{IPS}_{\mathsf{Lin}'}$ *and* $\mathcal{C}$-mult-$\mathsf{IPS}_{\mathsf{Lin}'}$*: For any polynomial class $\mathcal{C}$, a proof in* $\mathsf{IPS}_{\mathsf{Lin}'}$ *is said to be in* $\mathcal{C}$-$\mathsf{IPS}_{\mathsf{Lin}'}$ *if it is additionally contained in $\mathcal{C}$.* $\mathcal{C}$-mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ *is defined analogously.* ◊

[2]That is, there does not exist $\bar{x} \in \{0,1\}^n$ such that for every $i \in [n]$, $f_i(\bar{x}) = 0$.

Monomial Ordering

Definition 2.7 (Monomial Ordering)**.** *Given a set of variables $X = \{x_1, \ldots, x_n\}$, let $(x_{i_1}, \ldots, x_{i_n})$ be a total ordering on it. We extend it to a total ordering $\succ$ on $\mathcal{M}(X)$ as follows.*

For any two distinct monomials $\bar{x}^{\bar{a}}, \bar{x}^{\bar{b}}$,

- *if $\deg(\bar{x}^{\bar{a}}) > \deg(\bar{x}^{\bar{b}})$ then $\bar{x}^{\bar{a}} \succ \bar{x}^{\bar{b}}$;*
- *if $\deg(\bar{x}^{\bar{a}}) = \deg(\bar{x}^{\bar{b}})$, $a_{i_j} = b_{i_j}$ for every $j < j_0$ and $a_{i_{j_0}} > b_{i_{j_0}}$, then $\bar{x}^{\bar{a}} \succ \bar{x}^{\bar{b}}$.*

For a polynomial $f \in \mathbb{F}[X]$ and a total order $\succ$ on $\mathcal{M}[X]$, we denote the leading monomial *of f (largest monomial under $\succ$ that present in f) and* trailing monomial *of f (smallest monomial under $\succ$ that is present in f) by $\mathrm{LM}(f)$ and $\mathrm{TM}(f)$ respectively.*

For a subset $S \subseteq \mathbb{F}[X]$, we define $\mathrm{LM}(S) := \{\mathrm{LM}(f) \ : \ f \in S\}$. $\mathrm{TM}(S)$ is defined similarly. ◊

Algebraic Independence and Algebraic Rank

Definition 2.8. *A set of polynomials $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[X]$ is said to be algebraically dependent over $\mathbb{F}$ if there exists a non-zero polynomial $A(y_1, \ldots, y_m) \in \mathbb{F}[Y]$ such that $A(f_1, \ldots, f_m) = 0$. If no such A exists, then $f_1, \ldots, f_m$ are said to be algebraically independent.*

Given any set of polynomials $S \subseteq \mathbb{F}[X]$, the algebraic rank of S is the size of largest algebraic independent subset of S. ◊

Definition 2.9. *Given a polynomial $f \in \mathbb{F}[X]$ and $S \subseteq X$, let $\mathcal{M}[S]$ be the set of all monomials that can be defined over the variables in S. Furthermore, for each $m \in \mathcal{M}[S]$, let $f_m \in \mathbb{F}[X \setminus S]$ be the unique polynomial such that $f = \sum_{m \in \mathcal{M}[S]} m \cdot f_m$. We define $\mathsf{alg\text{-}rank}_S(f)$ as the algebraic rank of the set $\mathsf{coeff}_S(f) := \{f_m \ : \ m \in \mathcal{M}[S], \ f_m \neq 0\}$.* ◊

Here is a standard theorem on algebraic independence, that we need.

Theorem 2.10 ([KR05])**.** *Let $f_1, \ldots, f_k \in \mathbb{F}[X]$ and $\succ$ be a total ordering over the monomials. If $f_1, \ldots, f_k$ are algebraically dependent then both sets $\{\mathrm{LM}(f_i) \mid i \in [1, 2, \ldots, k]\}$ and $\{\mathrm{TM}(f_i) \mid i \in [1, 2, \ldots, k]\}$ are algebraically dependent.*

Partial Derivative Matrix

Definition 2.11 (Partial Derivative Matrix [SY10, Sap21])**.** *Let $f \in \mathbb{F}[X]$ be a polynomial and (Y, Z) be a partition of X (that is, $X = Y \sqcup Z$). The partial derivative matrix of f with respect to (Y, Z), say $M_{Y,Z}(f)$, is defined as follows.*

- *The rows of $M_{Y,Z}(f)$ are indexed by monomials in the variables Y and the columns are indexed by monomials in the variables Z.*

- *Given monomials $m_Y = \bar{y}^{\bar{a}}$ and $m_Z = \bar{z}^{\bar{b}}$, the entry of $M_{Y,Z}(f)$ in the row labelled m_Y and column labelled m_z is the coefficient of $m_Y \cdot m_Z$ in f (denoted by $\mathsf{coeff}_{m_Y \cdot m_Z}(f)$).* $\Diamond$

Given a partition (Y, Z) of X and $f \in \mathbb{F}[X]$, note that we can also consider f to be a polynomial over the variables Z with coefficients being polynomials over in the variables Y variables. We define $\mathsf{coeff}_{Y,Z}(f) = \left\{ \sum_{m_Y \in \mathcal{M}(Y)} m_Y \cdot \mathsf{coeff}_{m_Y \cdot \bar{z}^{\bar{b}}}(f) \ : \ \bar{z}^{\bar{b}} \in \mathcal{M}(Z) \right\}$.

Definition 2.12 (Evaluation Dimension[FSTW21])**.** *Let $f(X, Y) \in \mathbb{F}[X, Y]$ be a polynomial and $S \subseteq \mathbb{F}$. We define evaluation dimension of f on partition (X, Y) in the following way,*

$$\text{Eval-dim}_{X,Y,S}[f(\bar{x}, \bar{y})] = \dim_{\mathbb{F}} \left\{ f(\bar{x}, \bar{\beta}) : \bar{\beta} \in S^{|Y|} \right\}$$ $\Diamond$

Lemma 2.13 ([FS15])**.** *Let $f \in \mathbb{F}[X, Y]$ and S be any subset of $\mathbb{F}$. Then*

$$\dim_{\mathbb{F}} \left(\mathsf{coeff}_{X,Y}(f) \right) \geq \text{Eval-dim}_{X,Y,S}(f).$$

2.3 Functional Lower Bound Method for proving lower bounds for IPS proofs

We will be crucially using the following technique described in [FSTW21] for proving lower bounds against $\mathsf{IPS}_{\mathsf{Lin}}$ and $\mathsf{IPS}_{\mathsf{Lin}'}$.

Theorem 2.14. ([FSTW21, Lemma 5.1]) *Let $f \in \mathbb{F}[X]$ be a polynomial such that for some $\beta > 0$ the system $\{f - \beta, X^2 - X\}$ has no common solutions over the Boolean hypercube. Further, let $\mathcal{C} \subseteq \mathbb{F}[X]$ be a class of polynomials that is closed under partial $\mathbb{F}$-assignments*[3]*.*

If there does not exist any $g \in \mathcal{C}$ that satisfies $g(\bar{x}) = \frac{1}{f(\bar{x}) - \beta}$ for every $\bar{x} \in \{0,1\}^n$, then there is no proof of unsatisfiability for the system $\{f - \beta, X^2 - X\}$ that is contained in $\mathcal{C}$-$\mathsf{IPS}_{\mathsf{Lin}}$, $\mathcal{C}$-$\mathsf{IPS}_{\mathsf{Lin}'}$.

This is called the functional lower bound method, since one needs to prove a lower bound against all polynomials which evaluate to the same value as $\frac{1}{f-\beta}$ over the entire Boolean hypercube.

Proposition 2.15. *Let $f \in \mathbb{F}[X]$ and $\{f = 0, X^2 - X = 0\}$ be a unsatisfiable system against which we want to show $\mathcal{C}$-mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ lower bound. Let $g(X)$ be the unique multilinear polynomial that agrees with $\frac{1}{f(X)}$ over the Boolean hypercube. If $g \notin \mathcal{C}$ then the system does not have $\mathcal{C}$-mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ refutation.*

Proof. Let $C(X, y, Z)$ be a $\mathcal{C}$-mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ refutation for the unsatisfiable system. Assume $g(X)$ be the unique multilinear polynomial such that $g(X) = \frac{1}{f(X)} \pmod{X^2 - X}$. Since, f is the only non-Boolean axiom and C is linear in y, by Definition 2.6, $C(X, y, Z) = g(X) \cdot y + C'(X, Z, y)$ and $C(X, f, X^2 - X) = g(X) \cdot f(X) + \sum_{i=1}^{n} C'_i(X)(x_i^2 - x_i) = 1$. So, $C(X, y, 0) = y \cdot g(X) \implies C(X, 1, 0) = g(X)$. This implies $g(X) \in \mathcal{C}$, but this contradicts the assumption : $g \notin \mathcal{C}$. $\square$

[3] If $f \in \mathbb{F}[X]$ with $f \in \mathcal{C}$ and $Y \subseteq X$, then $f|_{Y=\bar{a}}(X \setminus Y) \in \mathcal{C}$ for any $\bar{a} \in \mathbb{F}^{|Y|}$.

3 Lower Bound Against Formulas for mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ Proofs

In this section, we prove Theorem 1.3 and Theorem 1.7.

Given an unsatisfiable system $\{f = 0, X^2 - X = 0\}$, to prove the formula complexity lower bound of the mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ refutation for f, it suffices to consider the unique multilinear polynomial $g(X)$ such that,

$$g(X) = \frac{1}{f(X)} \pmod{X^2 - X}.$$

Towards that we first note a few structural properties of the polynomial $g(X)$.

3.1 Some Structural Results

Proposition 3.1. *Let $\mathbb{F}$ be any field and $f \in \mathbb{F}[X]$ be a multilinear polynomial such that the system of equations $\{f = 0, X^2 - X = 0\}$ is unsatisfiable over $\{0,1\}^n$. Additionally, suppose f has the property that for any two monomials $m_i, m_j \in f$, $\mathsf{supp}(m_i) \nsubseteq \mathsf{supp}(m_j)$ and $\mathsf{supp}(m_j) \nsubseteq \mathsf{supp}(m_i)$. Let $g \in \mathbb{F}[X]$ be the unique multilinear polynomial such that $g(X) = \frac{1}{f(X)} \pmod{X^2 - X}$.*

Then, for any monomial m whose coefficient in f is non-zero, its coefficient in g is also non-zero[4].

Proof. Let $f(X) = f'(X) - \beta$ where $f(0) = -\beta$. Note that since f is unsatisfiable, $\beta \neq 0$. The unique multilinear polynomial $g(X) = \frac{1}{f(X)} \pmod{X^2 - X}$ is given by the following.

$$g(\bar{x}) = \sum_{T \subseteq [n]} g(\mathbb{1}_T) \prod_{i \in T} x_i \prod_{i \notin T} (1 - x_i).$$

Let m be a monomial with non-zero coefficient α in f and $S = \mathsf{supp}(m)$. Setting the variables $x_i \notin S$ to 0, it is easy to see that the coefficient of m in g (denoted by c_m), is given by the expression $c_m = \sum_{A \subseteq S} g(\mathbb{1}_A)(-1)^{|S \setminus A|}$. Notice that, $g(\mathbb{1}_S) = \frac{1}{f(\mathbb{1}_S)} = \frac{1}{\alpha - \beta}$ and $g(\mathbb{1}_\emptyset) = \frac{(-1)^{|S|}}{-\beta}$. Moreover, from the monomial support property, for any $S' \subset S$, $g(\mathbb{1}_{S'}) = -\frac{1}{\beta}$. Thus,

$$\begin{aligned} c_m &= \sum_{A \subseteq S} g(\mathbb{1}_A)(-1)^{|S \setminus A|} = \frac{1}{\alpha - \beta} - \frac{1}{\beta} \sum_{A \subset S} (-1)^{|S \setminus A|} \\ &= \frac{1}{\alpha - \beta} - \frac{1}{\beta} \left(\sum_{A \subseteq S} (-1)^{|S \setminus A|} - 1 \right) = \frac{1}{\alpha - \beta} + \frac{1}{\beta}. \end{aligned} \tag{3.2}$$

In the above Equation 3.2, we use the standard fact that

$$\sum_{A \subseteq S} (-1)^{|S \setminus A|} = \sum_{i=0}^{|S|} \binom{|S|}{i} (-1)^{|S|-i} = 0. \qquad \square$$

[4] If f is not multilinear, then for any non-multilinear monomial m with non-zero coefficient in f, the coefficient of $\mathsf{mult}(m)$ in g is non-zero.

We record some further structural properties in the following lemma. The lemma shows that any monomial m which is not expressible by the multilinearization of any product of monomials from $\mathsf{supp}(f)$, has coefficient 0 in g.

Lemma 3.3. *Let $\mathbb{F}$ be any field and $f \in \mathbb{F}[X]$ be a multilinear polynomial such that $\{f = 0, X^2 - X = 0\}$ is unsatisfiable. Let $g \in \mathbb{F}[X]$ be the unique multilinear polynomial such that $g(X) = \frac{1}{f(X)} \pmod{X^2 - X}$. Consider a monomial m such that $m \neq \mathsf{mult}(\prod_{m \in S} m)$ for any subset $S \subseteq \mathsf{supp}(f)$. Then the coefficient of m in g is 0.*

Proof. Consider a monomial m such that $m \neq \mathsf{mult}(\prod_{m \in S} m)$ for any subset $S \subseteq \mathsf{supp}(f)$. The idea is to decompose m as a product of monomials m_1 and m_2 with the following property : There is a set $S_1 \subseteq \mathsf{supp}(f)$, such that $m_1 = \mathsf{mult}(\prod_{m' \in S_1} m')$ and $S_2 = \mathsf{supp}(m_2) \notin \mathsf{supp}(f)$. Moreover for any subset $T_1 \subseteq S_1$ and a nonempty subset $T_2 \subseteq S_2$, $T_1 \cup T_2 \notin \mathsf{supp}(f)$. It is not hard to see that such a decomposition can be constructed in a greedy manner.

Next, we make a few simple observations. Clearly, $S_1 \cap S_2 = \emptyset$ due to multilinearity. Moreover, $g(\mathbb{1}_{S_2}) = 1/f(0)$. Furthermore, for any subset $T_1 \subseteq S_1$ and $T_2 \subseteq S_2$,

$$g(\mathbb{1}_{T_1 \cup T_2}) = \frac{1}{f(\mathbb{1}_{T_1 \cup T_2})} = \frac{1}{f(\mathbb{1}_{T_1})}.$$

Recall that,

$$g(\bar{x}) = \sum_{T \subseteq [n]} g(\mathbb{1}_T) \prod_{i \in T} x_i \prod_{i \notin T} (1 - x_i).$$

Hence,

$$\begin{aligned} c_m = \sum_{A \subseteq S_1 \cup S_2} g(\mathbb{1}_A)(-1)^{|S_1 \cup S_2 \setminus A|} &= \sum_{A_1 \subseteq S_1} (-1)^{|S_1 \setminus A_1|} \sum_{A_2 \subseteq S_2} g(\mathbb{1}_{A_1 \cup A_2})(-1)^{|S_2 \setminus A_2|} \\ &= \sum_{A_1 \subseteq S_1} (-1)^{|S_1 \setminus A_1|} \sum_{A_2 \subseteq S_2} g(\mathbb{1}_{A_1})(-1)^{|S_2 \setminus A_2|} \\ &= \sum_{A_1 \subseteq S_1} g(\mathbb{1}_{A_1})(-1)^{|S_1 \setminus A_1|} \sum_{A_2 \subseteq S_2} (-1)^{|S_2 \setminus A_2|} = 0. \end{aligned}$$

Here we have used the fact that $\sum_{A_2 \subseteq S_2} (-1)^{|S_2 \setminus A_2|} = 0$ and $g(\mathbb{1}_{A_1 \cup A_2}) = g(\mathbb{1}_{A_1})$. □

3.2 The Lower Bound

In this section, we prove a near-quadratic mult-$\mathsf{IPS}_{\mathsf{Lin}'}$ size lower bound in the formula setting. We use the structural results developed in Section 3.1 along with the lower bound technique of [Kal85].

Theorem 3.4 (Kalorkoti, [Kal85])**.** *Let $f \in \mathbb{F}[X]$ be a polynomial computed by a size s formula. Let $(X_1, X_2, \ldots, X_t)$ be any partition of the variables set X. Then s is at-least $\Omega\left(\sum_{i=1}^{t} \mathsf{alg\text{-}rank}_{X_i}(f)\right)$.*

Next, we recall the axiom polynomial from Section 1.1, for which we show the lower bound result for $\mathsf{IPS}'_{\mathsf{Lin}}$ refutations.

Let $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_0, \ldots, y_{n-1}\}$ be two sets of variables. We partition X into $N = \frac{n}{\log n}$ parts, $\{X_1, \ldots, X_N\}$ where $X_i = \{x_{(i-1)\log n+1}, \ldots, x_{i \log n}\}$. Clearly, the size of each X_i is $\log n$.

For a subset $S \subseteq X_i$, let $\Pi_S \in \{0,1\}^{\log n}$ be its characteristic vector, and define $t(S) = \sum_{j=1}^{\log n} \Pi_S[j] \cdot 2^{j-1}$. Now we define the polynomial,

Equation 1.1.

$$f'(\bar{x}, \bar{y}) = \sum_{i=1}^{N} \sum_{S \subseteq X_i} \left(\prod_{j \in S} x_j \cdot y_{t(S)} \right). \tag{1.1}$$

Equation 1.2.

$$f(\bar{x}, \bar{y}) = \begin{cases} f' + 1 & \text{if the characteristic of } \mathbb{F} = 0 \\ f' + \beta & \text{if the characteristic of } \mathbb{F} = p > 0,\ k > 0 \in \mathbb{Z}, \\ & \beta \in \mathbb{F}_{p^{k+1}} \setminus \mathbb{F}_{p^k} \text{ and } f' \in \mathbb{F}_{p^k}[X, Y] \end{cases} \tag{1.2}$$

We now prove the first lower bound of this section: a $\log n$-degree unsatisfiable system whose $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation by formulas requires near-quadratic size. We first recall the statement.

Theorem 1.3. *Consider the polynomial f is defined in Equation 1.2. Then the following statements are true :*

- *Over the fields of characteristic 0, any formula computing a $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation of the unsatisfiable system $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega\left(\frac{n^2}{\log n}\right)$.*
- *Over the fields of characteristic p, any formula computing the $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation of the unsatisfiable system of equations $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega\left(\frac{n^2}{\log n}\right)$.*

Proof. Let $g(X, Y)$ be the unique multilinear polynomial such that $g(X, Y) = \frac{1}{f(X,Y)} \pmod{X^2 - X, Y^2 - Y}$. For any two monomials $m_1, m_2 \in \mathsf{supp}(f)$, $\mathsf{supp}(m_1) \nsubseteq \mathsf{supp}(m_2)$ and $\mathsf{supp}(m_2) \nsubseteq \mathsf{supp}(m_1)$. Hence Proposition 3.1 implies that, all monomials of f appear in g with non-zero coefficients. Moreover, Lemma 3.3 implies every other monomial in g with non-zero coefficient can only be the multilinearized product of monomials from $\mathsf{supp}(f)$. Consider the variable partition $X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_N$ as defined above, and fix any X_i. Order monomials with $X \succ Y$, then extend as in Definition 2.7, using any order within X and Y. Under this ordering, $\mathrm{TM}(\mathsf{coeff}_{X_i}(g)) = \{y_0, \ldots, y_{n-1}\}$, which is algebraically independent. So using Theorem 2.10, the set $\mathsf{coeff}_{X_i}(g)$ is also algebraically independent. Let g has a formula of size s. Then using Theorem 3.4, we conclude

$$s \geq \Omega\left(\sum_{i=1}^{N} \mathsf{alg\text{-}rank}_{X_i}(g) + \mathsf{alg\text{-}rank}_{Y}(g) \right) = \Omega\left(\frac{n^2}{\log n} \right)$$

Here we have used $N = \frac{n}{\log n}$. Using Proposition 2.15, any mult-IPS$_{\mathsf{Lin}'}$ refutation of the unsatisfiable system $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ computed by a formula needs size at-least $\Omega\left(\frac{n^2}{\log n}\right)$. Note that both Lemma 3.3 and Proposition 3.1 are characteristic independent statement. So, under the given partition $X_1 \sqcup X_2 \sqcup \cdots \sqcup X_N$, the set $\mathsf{TM}(\mathsf{coeff}_{X_i}(g)) = \{y_0, \ldots, y_{n-1}\}$ remains unchanged for any X_i. The algebraic independence of this set is independent of the characteristic of the field. So, the lower bound works over characteristic p as well. □

Next we show an example of a constant degree unsatisfiable system of equations such that any refutation in mult-IPS$_{\mathsf{Lin}'}$ computed by formula needs near quadratic size. For that, first we recall polynomial h' from Equation 1.5. Let $c > 3$. Further, let $X = \{x_{i,j} : i \in [c], j \in [n^2/c]\}$ and $Y = \{y_{i,j} : i, j \in [n]\}$ be sets of variables. The polynomial h is set multilinear with respect to the partition $\bigsqcup_{i=1}^{c}\left(\bigcup_{k=1}^{n^{2(1-1/c)}/c} X_{i,k}\right) \bigsqcup Y$ where for any $i \in [c]$ and $k \in [n^{2(1-1/c)}/c]$,

$$X_{i,k} = \left\{x_{i,j} : j \in \left\{(k-1)(n^{2/c}) + 1, \ldots, k(n^{2/c})\right\}\right\}$$

Equation 1.3.

$$h'(X, Y) = \sum_{k=1}^{n^{2(1-1/c)}/c} h_k. \tag{1.5}$$

Where each h_k is set-multilinear over $\bigsqcup_{i=1}^{c} X_{i,k} \bigsqcup Y$ described in Equation 1.5. Let $\bigsqcup_{i=1}^{c} X_{i,k} = X^{(k)}$ and $\left(\sqcup_{k=1}^{n^{2(1-1/c)}/c} X^{(k)}\right) \sqcup Y$ be a partition of variables. We use this partition to prove the mult-IPS$_{\mathsf{Lin}'}$-lower bound against constant degree unsatisfiable systems. We first recall the polynomial.

Equation 1.4.

$$h(X, Y) = \begin{cases} h' + 1 & \text{if the characteristic of } \mathbb{F} = 0 \\ h' + \beta & \text{if the characteristic is } p > 0,\ k > 0 \in \mathbb{Z}, \\ & \beta \in \mathbb{F}_{p^{k+1}} \setminus \mathbb{F}_{p^k} \text{ and } h' \in \mathbb{F}_{p^k}[X, Y] \end{cases} \tag{1.6}$$

Next, we recall the theorem statement.

Theorem 1.7. *Consider the polynomial h in Equation 1.6. Then the following statements are true.*

- *Over the fields of characteristic 0, any formula computing a* mult-IPS$_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at least $\Omega(n^{4-2/c})$.*
- *Over the fields of characteristic p, any formula computing a* mult-IPS$_{\mathsf{Lin}'}$ *refutation of the unsatisfiable system $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$ must have size at-least $\Omega\left(n^{4-2/c}\right)$.*

Proof. Let $g(X,Y)$ be the multilinear polynomial such that $g(X,Y) = \frac{1}{h(X,Y)} \pmod{X^2 - X, Y^2 - Y}$. For any two monomials $m_1, m_2 \in \mathsf{supp}(h)$, $\mathsf{supp}(m_1) \not\subseteq \mathsf{supp}(m_2)$ and $\mathsf{supp}(m_2) \not\subseteq \mathsf{supp}(m_1)$. Hence Proposition 3.1 implies all monomials of h appear in g with a non-zero coefficient. Moreover, Lemma 3.3 implies every other monomial in g with non-zero coefficient can only be the multilinearized product of monomials from $\mathsf{supp}(h)$.

Consider the partition of variables $\left(\bigsqcup_{k=1}^{n^{2(1-1/c)}/c} X^{(k)}\right) \bigsqcup Y$. Consider the following monomial ordering: Over the variables, $X \succ Y$ and extend it to monomials naturally (Definition 2.7). Within variable set X (and similarly Y), choose any order. Under this ordering, $\mathsf{TM}(\mathsf{coeff}_{X^{(k)}}(g)) = \left\{Y_{i,j} : i,j \in [n]\right\}$ for every $X^{(k)}$ where $k \in [n^{2(1-1/c)}/c]$. All these variables are algebraically independent. So, using Theorem 2.10, $\mathsf{alg\text{-}rank}_{X^{(k)}}(g) \geq n^2$. If g has a formula of size s, then using Theorem 3.4,

$$s \geq \Omega\left(\sum_{i=1}^{n^{2(1-1/c)}/c} \mathsf{alg\text{-}rank}_{X^i}(g) + \mathsf{alg\text{-}rank}_Y(g)\right) \geq \Omega\left(n^2 \cdot n^{2(1-1/c)}/c + 1\right) \geq \Omega\left(n^{4-2/c}\right).$$

So, any formula computing g needs size at least $\Omega(n^{4-2/c})$. Hence, any $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation of $\left\{h = 0, X^2 - X = 0, Y^2 - Y = 0\right\}$ computed by a formula needs size at-least $\Omega(n^{4-2/c})$ by Proposition 2.15. Since both Lemma 3.3 and Proposition 3.1 is a characteristic independent statement, the set $\mathsf{TM}(\mathsf{coeff}_{X^{(k)}}(g))$ remains unchanged and algebraically independent. So, the proof follows when characteristic of the field is positive. □

4 Lower Bound Against Sum of ROABPs for $\mathsf{IPS}_{\mathsf{Lin}'}$ Proofs

We begin with an observation.

Observation 4.1. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a multilinear polynomial computed by an* ROABP *of size s. Then there is a multilinear* ROABP *of size at most s computing the same polynomial.*

Proof. Consider the ROABP, say $\mathcal{A}$, computing f. We get a multilinear ROABP computing f by simply removing non-multilinear terms from the label of every edge in $\mathcal{A}$. Since f is multilinear, the contribution of the non-multilinear monomials in the edge labels anyway cancel out at the end and therefore this does not affect the computation of f. □

We next state a couple of theorems from the work of Forbes, Shpilka, Tzameret, and Wigderson [FSTW21] that we will require.

Lemma 4.2. ([FSTW21, Lemma 3.7]) *Let $X = \{x_1, \ldots, x_n\}$ and $f \in \mathbb{F}[X]$ be a polynomial computed by an* ROABP *of width r. Then $r \geq \max_{i \in [n]} \{\mathrm{rank}(M_{Y_i,Z_i}(f))\}$ where $Y_i = \{x_1, \ldots, x_i\}$ and $Z_i = X \setminus Y_i$.*

Lemma 4.3. ([FSTW21, Proposition 4.5]) *Let $f \in \mathbb{F}[X]$ be a polynomial with individual degree of each variable being at most d. Further, suppose that f is computable by an* ROABP *of width r in some order. Then $\mathsf{mult}(f)$ can be computed by an* ROABP *of size $\mathrm{poly}(r, n, d)$ and width r that has the same order.*

Further there exist polynomials $h_1, \cdots, h_n \in \mathbb{F}[X]$ such that

- *for every $i \in [n]$, h_i has individual degree upper bounded by d;*
- *for every $i \in [n]$, h_i can be computed by an* ROABP *of size $\mathrm{poly}(r, n, d)$ and width r;*
- $f(\bar{x}) = \mathsf{mult}(f) + \sum_{i=1}^{n} h_i(x_i^2 - x_i)$.

We now use Lemma 4.3 to show a similar statement for a sum of ROABPs as well.

Proposition 4.4 (Multilinearization of Sum of ROABPs)**.** *Let $f \in \mathbb{F}[X]$ be a polynomial with individual degree at most d such that it is computable by a sum of t* ROABP*s, say $A_1, \ldots, A_t$, each with width at most r and potentially a different variable ordering. Let σ_i be the variable ordering of A_i. Then,*

- $\mathsf{mult}(f)$ *is computable by a sum of t multilinear* ROABP*s $B_1, \ldots, B_t$, where each B_i has width at most r, size $\mathrm{poly}(r, n, d)$ and variable ordering σ_i. Further, if f_i was the polynomial computed by A_i, then the polynomial computed by B_i is $\mathsf{mult}(f_i)$;*
- *there exist polynomials $h_1, \ldots, h_n$, each of individual degree at most d and computable by a sum of t* ROABP*s of size $\mathrm{poly}(r, n, d)$ and width at most r, such that*

$$f(\bar{x}) = \mathsf{mult}(f) + \sum_{i=1}^{n} h_i(x_i^2 - x_i).$$

Proof. We use Lemma 4.3 to prove the statement. By the assumption of the lemma, f is computable by $\sum_{i=1}^{t} A_i$ where each A_i is an ROABP of width at most r and variable ordering σ_i. Let f_i be the polynomial computed by A_i. Note that the individual degree of f_i is at most d.

Fix any i arbitrarily. Using Lemma 4.3, $\mathsf{mult}(f_i)$ has an ROABP of width at most r, order σ_i and size $\mathrm{poly}(r, n, d)$. Moreover, there exist polynomials $h_{i,1}, \ldots, h_{i,n}$ of individual degree at most d such that $f_i = \mathsf{mult}(f_i) + \sum_{j=1}^{n} h_{i,j}(x_j^2 - x_j)$. Here, for each $j \in [n]$, $h_{i,j}$ can be computed by an ROABP of width at most r, order σ_i and size $\mathrm{poly}(r, n, d)$. Hence,

$$\begin{aligned} f = \sum_{i=1}^{t} f_i &= \sum_{i=1}^{t} \mathsf{mult}(f_i) + \sum_{i=1}^{t} \sum_{j=1}^{n} h_{i,j}(x_j^2 - x_j) \\ &= \sum_{i=1}^{t} \mathsf{mult}(f_i) + \sum_{j=1}^{n} \left(\sum_{i=1}^{t} h_{i,j} \right) (x_j^2 - x_j). \end{aligned}$$

Clearly $\sum_{i=1}^{t} \mathsf{mult}(f_i) = \mathsf{mult}(f)$. Further, if we define $h_j = \sum_{i=1}^{t} h_{i,j}$, then each h_j is computable by a sum of t ROABPs that have the required properties. □

We additionally require the following lemma from the work of Forbes, Shpilka, Tzameret, and Wigderson [FSTW21].

Lemma 4.5. ([FSTW21, Proposition 5.13]) *Let $\mathbb{F}$ be a field of characteristic zero, $X = \{x_0, \ldots, x_{2n-1}\}$, $T = \{t_{i,j} : i, j \in [0, \ldots, 2n-1] \text{ with } i < j\}$ be two sets of variables and $\beta > \binom{2n}{2}$ be any number. Further, let g be the unique multilinear polynomial such that*

$$g(X,T) \equiv \frac{1}{\sum_{i<j} t_{i,j} x_i x_j - \beta} \pmod{X^2 - X,\ T^2 - T}.$$

Then for any balanced partition (Y,Z) of X, $\text{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] \geq 2^n$.

Finally, before we can prove our main theorem, we require a *weakness lemma* for a sum of multilinear ROABPs. The proof of this lemma is based on ideas which are implicitly present in the work of Chatterjee, Kush, Saraf, and Shpilka [CKSS24] (in the context of sums of ordered set-multilinear ABPs). However, we provide a detailed self-contained proof.

4.1 Weakness of a Sum of Multilinear ROABPs

Let $A = \sum_{i=1}^{t} A_i$ be a sum of ROABPs where each A_i is multilinear and computing some multilinear polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Without loss of generality, we can assume that each A_i has length n and say the maximum width is s. Since the polynomial is multilinear, the partial derivative matrix under any partition of variables (Y,Z) of X has dimension $2^{|Y|} \times 2^{|Z|}$ [5].

Fact 4.6. *Let (Y,Z) be some partition of the variable set X and $M_{Y,Z}(f)$ be the partial derivative matrix with respect to this partition. Then,*

$$\text{rank}[M_{Y,Z}(f)] \leq \min\{2^{|Y|}, 2^{|Z|}\} = 2^{\min\{|Y|,|Z|\}} \leq 2^{\frac{n-||Y|-|Z||}{2}}.$$

Next, we show that under any random balanced partition of the variables, the rank of any small size sum of multilinear ROABP reduces significantly with high probability.

Lemma 4.7 (Weakness Lemma)**.** *Let $q = r = \sqrt{n}$. Further, let $A = \sum_{i=1}^{t} A_i$ be a sum of multilinear* ROABP*s computing a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ and (Y,Z) be a partition of the variable set X chosen independently and uniformly at random. Then, there exist constants $\varepsilon', \varepsilon'' \in (0,1)$ such that*

$$\Pr_{(Y,Z)}\left[\text{rank}[M_{Y,Z}(A)] < t \cdot s^{q-1} \cdot 2^{\frac{n}{2} - \frac{\varepsilon' q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \geq 1 - t \cdot e^{-\varepsilon'' q}.$$

Proof. Since (Y,Z) is a partition chosen independently and uniformly at random, each variable in X is chosen to be a Y variable with probability $1/2$ and a Z variable with probability $1/2$. Let this

[5] The rows and columns are indexed by multilinear monomials over Y and Z variables respectively.

distribution on the partitions be $\mathcal{U}$. A partition (Y, Z) is balanced if $|Y| = |Z|$. It is a standard fact [CKSS24] that $\Pr_{(Y,Z)\sim\mathcal{U}}[(Y, Z) \text{ is balanced}] = \frac{\binom{n}{n/2}}{2^n} = \Theta\left(\frac{1}{\sqrt{n}}\right)$.

The idea is to first divide the ROABPs $\{A_i\}_{i\in[t]}$ into q parts each of length r. Fix $i \in [t]$ arbitrarily and let u_0, u_q be the source and sink node of A_i. Observe that

$$A_i = \sum_{u_1,\ldots,u_{q-1}} \prod_{j=1}^{q} g_{u_{j-1},u_j},$$

where the node u_j is in layer $j \in [q-1]$. Then the number of summands is upper bounded by s^{q-1}. This division of the ROABPs naturally partitions the variable set $X = X_1 \sqcup \cdots \sqcup X_q$ with each X_i containing r variables. (Y, Z) also gets further partitioned naturally into $\{(Y_j, Z_j)\}_{j\in[q]}$. We want to compute the rank of each product $\prod_{j=1}^{q} g_{u_{j-1},u_j}$ under any random partition.

$$\begin{aligned}\operatorname{rank}\left[M_{Y,Z}\left(\prod_{j=1}^{q} g_{u_{j-1},u_j}\right)\right] = \prod_{j=1}^{q} \operatorname{rank}\left[M_{Y_j,Z_j}(g_{u_{j-1},u_j})\right] &\leq \prod_{j=1}^{q} 2^{\frac{|Y_j|+|Z_j|}{2} - \frac{||Y_j|-|Z_j||}{2}} \\ &\leq 2^{\frac{n}{2} - \sum_{j=1}^{q} \frac{||Y_j|-|Z_j||}{2}}.\end{aligned}$$

Hence if we can lower bound the term $\sum_{j=1}^{q} \frac{||Y_j|-|Z_j||}{2}$, we would be able to upper bound the rank. Now, for any $j \in [q]$,

$$\Pr_{(Y_j,Z_j)}\left[\frac{||Y_j| - |Z_j||}{2} \leq \frac{\sqrt{r}}{4}\right] = \Pr_{(Y_j,Z_j)}\left[|Y_j| \in \left[\frac{r}{2} - \frac{\sqrt{r}}{4}, \frac{r}{2} + \frac{\sqrt{r}}{4}\right]\right] = \sum_{k=\frac{r}{2}-\frac{\sqrt{r}}{4}}^{\frac{r}{2}+\frac{\sqrt{r}}{4}} \frac{\binom{r}{k}}{2^r} < 1.$$

Let,

$$\varepsilon = \sum_{k=\frac{r}{2}-\frac{\sqrt{r}}{4}}^{\frac{r}{2}+\frac{\sqrt{r}}{4}} \frac{\binom{r}{k}}{2^r} \qquad \text{and for any } j \in [q], \text{ let} \qquad D_i = \begin{cases} 1 & \text{if } \frac{||Y_j|-|Z_j||}{2} \leq \frac{\sqrt{r}}{4} \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, if $D = \sum_j D_j$, then $\mathbb{E}[D] = \sum_j \mathbb{E}[D_j] = \varepsilon \cdot q$.

Fix $\delta \in (0, 1)$ arbitrarily. Then, using Chernoff bound (Theorem 2.1), we know that

$$\Pr_{(Y,Z)\sim\mathcal{U}}[D \geq (1+\delta)\varepsilon q] \leq \exp\left(-\frac{\delta^2 \varepsilon q}{2+\delta}\right).$$

Thus,

$$\Pr_{(Y,Z)\sim\mathcal{U}}[D \geq (1+\delta)\varepsilon q] \mid (Y,Z) \text{ is balanced}] = \frac{\Pr_{(Y,Z)\sim\mathcal{U}}[D \geq (1+\delta)\varepsilon q]}{\Pr_{(Y,Z)\sim\mathcal{U}}[(Y,Z) \text{ is balanced}]} \leq \exp\left(-\frac{\delta^2\varepsilon q}{2+\delta}\right)\cdot\sqrt{n}$$

Choose $\varepsilon'' = \left(\frac{2\delta^2\varepsilon}{2+\delta}\right)$ and $\hat{\varepsilon} = \varepsilon(1+\delta)$. Then, we have that

$$\begin{aligned}
&\Pr_{(Y,Z)\sim\mathcal{U}}[D \geq \hat{\varepsilon}q] \mid (Y,Z) \text{ is balanced}] \leq \exp\left(-\varepsilon'' q\right) \\
&\qquad \implies \Pr_{(Y,Z)\sim\mathcal{U}}[D < \hat{\varepsilon}q \mid (Y,Z) \text{ is balanced}] \geq 1 - \exp\left(-\varepsilon'' q\right) \\
&\implies \Pr_{(Y,Z)\sim\mathcal{U}}\left[\sum_{j=1}^{q} \frac{||Y_j| - |Z_j||}{2} > \frac{(1-\hat{\varepsilon})q\sqrt{r}}{4} \mid (Y,Z) \text{ is balanced}\right] \geq 1 - \exp(-\varepsilon'' q) \\
&\implies \Pr_{(Y,Z)\sim\mathcal{U}}\left[\operatorname{rank}\left(M_{Y,Z}\left(\prod_{j=1}^{q} g_{u_{j-1},u_j}\right)\right) < 2^{\frac{n}{2}-\frac{(1-\hat{\varepsilon})q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \\
&\qquad\qquad \geq 1 - \exp(-\varepsilon'' q).
\end{aligned}$$

Recall that $A_i = \sum_{u_1,\ldots,u_{q-1}} \prod_{j=1}^{q} g_{u_{j-1},u_j}$. Thus, for every $i \in [t]$,

$$\Pr_{(Y,Z)\sim\mathcal{U}}\left[\operatorname{rank}\left(M_{Y,Z}\left(A_i\right)\right) < s^{q-1}\cdot 2^{\frac{n}{2}-\frac{(1-\hat{\varepsilon})q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \geq 1 - \exp(-\varepsilon'' q).$$

By union bound, this shows that

$$\begin{aligned}
&\Pr_{(Y,Z)\sim\mathcal{U}}\left[\exists i \in [t] \text{ s.t. } \operatorname{rank}\left(M_{Y,Z}\left(A_i\right)\right) \geq s^{q-1}\cdot 2^{\frac{n}{2}-\frac{(1-\hat{\varepsilon})q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \\
&\qquad\qquad \leq t\cdot\exp(-\varepsilon'' q) \\
&\implies \Pr_{(Y,Z)\sim\mathcal{U}}\left[\forall i \in [t],\ \operatorname{rank}\left(M_{Y,Z}\left(A_i\right)\right) < s^{q-1}\cdot 2^{\frac{n}{2}-\frac{(1-\hat{\varepsilon})q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \\
&\qquad\qquad \geq 1 - t\cdot\exp(-\varepsilon'' q).
\end{aligned}$$

Finally, using the sub-additivity of rank, we get that

$$\Pr_{(Y,Z)\sim\mathcal{U}}\left[\operatorname{rank}\left(M_{Y,Z}\left(A\right)\right) < t\cdot s^{q-1}\cdot 2^{\frac{n}{2}-\frac{(1-\hat{\varepsilon})q\sqrt{r}}{4}} \mid (Y,Z) \text{ is balanced}\right] \geq 1 - t\cdot\exp(-\varepsilon'' q).$$

Choosing $\varepsilon' = 1 - \hat{\varepsilon}$ completes the proof. □

We are now ready to prove an exponential lower bound against $\sum\mathsf{ROABP\text{-}IPS}_{\mathsf{Lin}'}$ proofs.

4.2 Lower Bound over Fields of Characteristic Zero

Theorem 1.10. *For $X = \{x_0, \ldots, x_{2n-1}\}$, $T = \{t_{i,j} : i, j \in [0, \ldots, 2n-1] \text{ with } i < j\}$ and $\beta = 2\binom{2n}{2}$, let $f \in \mathbb{F}[X, T]$ be the polynomial defined as*

$$f = \left(\sum_{0 \le i < j \le 2n-1} t_{i,j} x_i x_j \right) - \beta$$

which is unsatisfiable over the Boolean hypercube. Then there exists $\gamma > 0$ such that the total width of any sum of ROABP *computing the linear proof of unsatisfiability ($\mathsf{IPS}_{\mathsf{Lin}'}$), for the system $\{f = 0, X^2 - X = 0, T^2 - T = 0\}$, is at-least $\exp(n^\gamma)$.*

Proof. Let g be the unique multilinear polynomial that proves the unsatisfiability of f. Then, by Lemma 4.5, for any balanced partition (Y, Z) of X, $\mathrm{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] \ge 2^n$. Thus,

$$\Pr_{(Y,Z)} \left[\mathrm{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] < 2^n \mid (Y, Z) \text{ is balanced} \right] = 0.$$

Suppose g is computable by a sum of t multilinear ROABPs, say $A_1, \ldots A_t$, of width at most s. Since the total number of variables is $2n$, by Lemma 4.7, we have that for any partition (Y, Z) of X chosen uniformly at random,

$$\Pr_{(Y,Z)} \left[\mathrm{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] < t \cdot s^{q-1} \cdot 2^{n - \frac{\varepsilon' q \sqrt{r}}{4}} \mid (Y, Z) \text{ is balanced} \right] \ge 1 - t \cdot e^{-\varepsilon'' q}.$$

for suitable constants $\varepsilon', \varepsilon'' \in (0, 1)$ and $q = r = \sqrt{2n}$.

Note that if $t > \exp(\varepsilon'' q)$, then we already have an $\exp(\Omega(\sqrt{n}))$ lower bound. Otherwise, there exists a balanced partition (Y, Z) such that $\mathrm{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] \le t \cdot s^{q-1} \cdot 2^{n - \frac{\varepsilon' q \sqrt{r}}{4}}$. However, we know that $\mathrm{rank}_{\mathbb{F}(T)}[M_{Y,Z}(g)] \ge 2^n$. Hence, it must be the case that $t \cdot s^{q-1} \ge 2^{\varepsilon' q \sqrt{r}}$, which would imply that $s \ge \exp(n^{1/4})$. Either way, we get that the size of the sum of ROABPs computing g is at least $\exp(n^\gamma)$ for some $\gamma > 0$.

Let $h \in \mathsf{IPS}_{\mathsf{Lin},}$ be any proof of unsatisfiability for f. Then $\mathsf{mult}(h) = g$. Assume, for sake of contradiction, that h can be computed by a sum of ROABPs, say $\sum A_i$, of size $\exp(o(n^\gamma))$.

$$h = \sum_i A_i \implies \mathsf{mult}(h) = \mathsf{mult}\left(\sum_i A_i \right) = \sum_i \mathsf{mult}(A_i)$$

Each ROABP $\mathsf{mult}(A_i)$ is a multilinear ROABP and using Proposition 4.4, $\sum_i \mathsf{mult}(A_i)$ is of size $\exp(o(n^{\gamma'}))$, but this contradicts the fact that any sum of multilinear ROABP computing $\mathsf{mult}(h) = g$ needs size at least $\exp(\Omega(n^\gamma))$. This completes the proof. □

4.3 Lower Bounds over Fields of Positive Characteristic of Large Size

Note that in Theorem 1.10, the characteristic of $\mathbb{F}$ is required to be zero even though the weakness lemma (Lemma 4.7) for sum of multilinear-ROABPs is characteristic independent. This is because we use Lemma 4.5. So, in order to prove a theorem analogous to Theorem 1.10 in the positive characteristic setting, we need a statement analogous to Lemma 4.5 in this setting.

The main idea for such a rank lower bound was recently shown in a work of Behera, Limaye, Ramanathan and Srinivasan [BLRS25]. We first state the main lemma from their work.

Lemma 4.8. ([BLRS25, Lemma 2.4]) *Let $\mathbb{F}, \mathbb{F}'$ be two fields such that $\mathbb{F} \subset \mathbb{F}'$, $n \in \mathbb{N}$ and X be the variable set. Fix $\beta \in \mathbb{F}' \setminus \mathbb{F}$ arbitrarily. Further, for any $\bar{\alpha} \in \mathbb{F}^n$ and a non-empty subset $S' \subseteq [n]$, let $g_{\bar{\alpha},S'}(\bar{x}) \in \mathbb{F}[X]$ be the unique multilinear polynomial that agrees with $\frac{1}{\sum_{i \in S'} \alpha_i \cdot x_i - \beta}$ over Boolean hypercube.*

For any $S \subseteq \mathbb{F}$ which is finite, if we choose $\bar{\alpha}$ uniformly at random from S^n, then the following is true.

$$\Pr_{\bar{\alpha} \sim S^n} \left[\exists \, \emptyset \neq S' \subseteq [n] \ : \ \deg(g_{\bar{\alpha},S'}(\bar{x})) < |S'| \right] < \frac{2^{2n}}{|S|}$$

We will also need the following lemma from the work of Forbes, Shpilka, Tzameret, and Wigderson [FSTW21].

Lemma 4.9. ([FSTW21, Lemma 5.12]) *Let $f \in \mathbb{F}[X, Y, Z]$ and $f_Z \in \mathbb{F}(Z)[X, Y]$ be the polynomial that symbolically equals f. That is, for any $\gamma \in \mathbb{F}^{|Z|}$, we have $f_\gamma(X, Y) = f(X, Y, \gamma) \in \mathbb{F}[X, Y]$.*

For any set of variables X, any field $\mathbb{F}$ and any $f \in \mathbb{F}[X]$, suppose $\mathsf{coeff}_X(f)$ is used to denote the coefficient vector of f. Then, for any $\gamma \in \mathbb{F}^{|Z|}$, $\dim_{\mathbb{F}(Z)}[\mathsf{coeff}_{X|Y}[f_Z(X, Y)]] \geq \dim_{\mathbb{F}}[\mathsf{coeff}_{X|Y}[f_\gamma(X, Y)]]$.

Using Lemma 4.8 and Lemma 4.9, Behera, Limaye, Ramanathan and Srinivasan [BLRS25] prove a rank bound analogous to Lemma 4.5 in positive characteristic.

Lemma 4.10. ([BLRS25, Lemma A.10]) *Let $n \in \mathbb{N}$ and $p \in \mathbb{N}$ be any prime. Say $\mathbb{F}'$ is a field of characteristic p with size p^{k+1}, where k is the smallest integer such that $p^k > \binom{2n}{n} 2^{2n}$ and that $\mathbb{F}$ is a field of size p^k (so that $\mathbb{F} \subset \mathbb{F}'$). Fix $\beta \in \mathbb{F}' \setminus \mathbb{F}$ arbitrarily and finally, for any $\alpha \in \mathbb{F}^{\binom{2n}{2}}$, let $g_\alpha(\bar{x}, \bar{t}) \in \mathbb{F}'[X, T]$ be the polynomial that agrees with $\frac{1}{\sum_{i<j} \alpha_{i,j} t_{i,j} x_i x_j - \beta}$ on the Boolean hypercube.*

Then there exists $\bar{\alpha}$ such that for any balanced partition (U, V) of X, $\mathrm{rank}_{\mathbb{F}'(T)}[M_{U,V}(g_\alpha)] \geq 2^n$.

We are now ready to prove an exponential lower bound for sum of ROABPs in positive characteristic.

Theorem 4.11. *Let $n \in \mathbb{N}$ and p be any prime. Further let $\mathbb{F}'$ be a field of characteristic p with size p^{k+1}, where k is the smallest integer such that $p^k > \binom{2n}{2} 2^{2n}$ and $\mathbb{F} \subset \mathbb{F}'$ be the subfield of size p^k. Also, arbitrarily fix $\beta \in \mathbb{F}' \setminus \mathbb{F}$.*

For $X = \{x_0, \ldots, x_{2n-1}\}$, $T = \{t_{i,j} \ : \ i, j \in \{0, \ldots, 2n-1 \text{ with } i < j\}\}$ and any $\bar{\alpha} \in \mathbb{F}^{\binom{2n}{2}}$, define

$$f = \left(\sum_{0 \leq i < j \leq 2n-1} \alpha_{i,j} t_{i,j} x_i x_j \right) - \beta$$

which is unsatisfiable over the Boolean hypercube. Then there exists $\bar{\alpha}$ and $\gamma > 0$, such that any sum of ROABP *computing the* $\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the system* $\{f = 0, X^2 - X = 0, T^2 - T = 0\}$ *must have total width at-least* $\exp(n^\gamma)$.

Proof. We combine Lemma 4.10 with the weakness lemma (Lemma 4.7) to get the required lower bound. The argument works in a similar manner given in the proof of Theorem 1.10. □

4.4 Lower Bound over Fields of Characteristic At Least Five

In Theorem 4.11 the field size needs to be large since we are using Lemma 4.8 to prove the rank lower bound. However, we can remove such a size requirement if we use the vector invariant polynomial from the work of Hakoniemi, Limaye, and Tzameret [HLT24]. We first state the rank lower bound from their work.

Lemma 4.12. ([HLT24, Lemma 43]) *Let $\mathbb{F}$ be a field of characteristic at least and $g(\bar{x}, \bar{t}) \in \mathbb{F}[X, T]$ be the polynomial defined in Theorem 4.13. Let $\hat{g}(\bar{x}, \bar{t}) \in \mathbb{F}[X, T]$ be any polynomial that satisfies*

$$\hat{g}(\bar{x}, \bar{t}) = \frac{1}{g(\bar{x}, \bar{t})} \bmod (X^2 - X, T^2 - T).$$

If $\hat{g}_T(\bar{x}) \in \mathbb{F}(T)[X]$ is the polynomial that symbolically equals $\hat{g}$, then for any balanced partition (U, V) of X, $\operatorname{rank}_{\mathbb{F}(T)}[M_{U,V}(\hat{g}_T(X)] \geq 2^n$.

We are now ready to prove an exponential lower bound against $\sum$ ROABPs for proofs in $\mathsf{IPS}_{\mathsf{Lin}'}$ model when the field size is not necessarily large.

Theorem 4.13. *Let $\mathbb{F}$ be a field of characteristic at least 5. Further, let $X = \{x_1, \ldots, x_{4n}\}$ and $T = \{t_{i,j,k,l} : i, j, k, l \in [4n]$ with $i < j < k < l\}$ be two sets of variables.*

Define $g \in \mathbb{F}[X, T]$ to be the polynomial

$$g = \left(\prod_{1 \leq i < j < k < l \leq 4n} 1 - t_{i,j,k,l} + t_{i,j,k,l}(x_i x_l - x_j x_k) \right) - \beta$$

which is unsatisfiable over Boolean hypercube as long as $\beta \neq \{-1, 0, 1\}$. Then there exists $\gamma > 0$ such that any sum of ROABP *computing a* $\mathsf{IPS}_{\mathsf{Lin}'}$ *refutation of the system $\{g = 0, X^2 - X = 0, T^2 - T = 0\}$ must have total width at-least $\exp(n^\gamma)$.*

The proof follows exactly along the lines of the one for Theorem 4.11 except that we use Lemma 4.7 combined with Lemma 4.12 instead of Lemma 4.10.

Conclusion

The construction of the axiom polynomials from the subset-sum axiom polynomial is particularly relevant in proof complexity although the subset-sum polynomial is not directly a translation of CNFs. More details regarding this can be found in [GHT22, Section 1.3]. Also, see [Raz00]. If the axiom polynomial is sparse, then it can be directly constructed from the subset-sum polynomial by substituting monomials for the variables. In this paper, all the axiom polynomials except the one used in Theorem 4.13 are sparse.

However, if one does not care about constructing sparse axiom polynomials, then the problem of proving polynomial-size quality lower bounds for formulas, ABPs, and circuits can be solved easily. This is noted in Observation A.5. As already mentioned above, it is more desirable if IPS lower bound results are shown for sparse axioms. This is also reflected if one compares the work of [AF22] with [GHT22].

Finally, we state a few open problems for further study.

1. Prove (nearly) quadratic-size $\mathsf{IPS}_{\mathsf{Lin}'}$ lower bounds for formulas for an axiom polynomial which is sparse.
2. Prove super-linear size $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ and $\mathsf{IPS}_{\mathsf{Lin}'}$ lower bounds for ABPs and circuits. Again, the axiom polynomials should be sparse.
3. Can we (re)-prove Theorem 4.13 for a sparse axiom polynomial?

References

[AF22] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: proving and using lower bounds for polynomial ideals. In *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 389–402. ACM, 2022.

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

[BCH94] Paul Beame, Stephen A. Cook, and H. James Hoover. Log Depth Circuits for Division and Related Problems. *SIAM Journal on Computing*, 23(4):740–751, 1994.

[BCS13] Peter Bürgisser, Michael Clausen, and Mohammad A Shokrollahi. *Algebraic complexity theory*, volume 315. Springer Science & Business Media, 2013.

[BDS25] C. S. Bhargav, Prateek Dwivedi, and Nitin Saxena. Lower bounds for the sum of small-size algebraic branching programs. *Theor. Comput. Sci.*, 1041:115214, 2025.

[BIK+94] Paul Beame, Russell Impagliazzo, Jan Krajícek, Toniann Pitassi, and Pavel Pudlák. Lower Bound on Hilbert's Nullstellensatz and propositional proofs. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 794–806. IEEE Computer Society, 1994.

[BLRS25] Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan. New Bounds for the Ideal proof System in Positive Characteristic. *Electron. Colloquium Comput. Complex.*, TR25-079, 2025. Pre-print available at `arXiv:TR25-079`.

[BO83] Michael Ben-Or. Lower Bounds for Algebraic Computation Trees. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing (STOC)*, pages 80–86. ACM, 1983.

[BPI92] Paul Beame, Toniann Pitassi, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. In *24th Annual ACM Symposium on Theory of Computing (STOC)*, pages 200–220. ACM, 1992.

[BS83] Walter Baur and Volker Strassen. The Complexity of Partial Derivatives. *Theor. Comput. Sci.*, 22:317–330, 1983.

[CKSS24] Prerona Chatterjee, Deepanshu Kush, Shubhangi Saraf, and Amir Shpilka. Lower Bounds for Set-Multilinear Branching Programs. In *39th Computational Complexity Conference, CCC 2024, July 22-25, 2024, Ann Arbor, MI, USA*, volume 300 of *LIPIcs*, pages 20:1–20:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[CKSV22] Prerona Chatterjee, Mrinal Kumar, Adrian She, and Ben Lee Volk. Quadratic Lower Bounds for Algebraic Branching Programs and Formulas. *Comput. Complex.*, 31(2):8, 2022.

[CKV24] Abhranil Chatterjee, Mrinal Kumar, and Ben Lee Volk. Determinants vs. Algebraic Branching Programs. *Comput. Complex.*, 33(2):11, 2024.

[CR79] Stephen A. Cook and Robert A. Reckhow. The Relative Efficiency of Propositional Proof Systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.

[EGLT25] Tal Elbaz, Nashlen Govindasamy, Jiaqi Lu, and Iddo Tzameret. Lower Bounds against the Ideal Proof System in Finite Fields. *arXive Preprint*, June 2025. Preprint. Pre-print available at `arXiv:2506.17210`.

[For24] Michael A. Forbes. Low-Depth Algebraic Circuit Lower Bounds over Any Field. In *39th Computational Complexity Conference, CCC 2024, July 22-25, 2024, Ann Arbor, MI, USA*, volume 300 of *LIPIcs*, pages 31:1–31:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[FS15] Michael A. Forbes and Amir Shpilka. Complexity Theory Column 88: Challenges in Polynomial Factorization1. *SIGACT News*, 46(4):32–49, 2015.

[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.

[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.

[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.

[HLT24] Tuomas Hakoniemi, Nutan Limaye, and Iddo Tzameret. Functional Lower Bounds in Algebraic Proofs: Symmetry, Lifting, and Barriers. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 1396–1404. ACM, 2024.

[HY09] Pavel Hrubes and Amir Yehudayoff. Monotone separations for constant degree polynomials. *Inf. Process. Lett.*, 110(1):1–3, 2009.

[Kal85] K. A. Kalorkoti. A Lower Bound for the Formula Size of Rational Functions. *SIAM Journal on Computing*, 14(3):678–687, 1985.

[KPW95] Jan Krajíček, Pavel Pudlák, and Alan Woods. Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995.

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*, volume 2 of *Springer-Verlag Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, Heidelberg, 2005.

[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.

[LTW18] Fu Li, Iddo Tzameret, and Zhengyu Wang. Characterizing Propositional Proofs as Noncommutative Formulas. *SIAM J. Comput.*, 47(4):1424–1462, 2018.

[PI94] Toniann Pitassi and Russell Impagliazzo. Exponential Lower Bounds for the Polynomial Calculus. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC)*, pages 129–135. ACM, 1994.

[Pit96] Toniann Pitassi. Algebraic Propositional Proof Systems. In *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. DIMACS/AMS, 1996.

[Raz00] Alexander A. Razborov. Lower Bounds for the Polynomial Calculus. *Computational Complexity*, 7(4):291–324, 2000.

[Rec76] Robert A. Reckhow. *On the lengths of proofs in the propositional calculus*. Ph.d. thesis, University of Toronto, 1976. Technical Report #87.

[Sap21] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. Manuscript online at https://github.com/dasarpmar/lowerbounds-survey/releases/download/v9.0.3/fancymain.pdf, 2021. A selection of lower bounds in arithmatic circuit complexity.

[SW01] Amir Shpilka and Avi Wigderson. Depth–3 Arithmetic Circuits Over Fields of Characteristic Zero. *Computational Complexity*, 10(1):1–27, November 2001.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5(3-4):207–388, 2010.

A Some Related Observations

In this section, we first sketch the non-multilinear formula refutations upper bounds. We start by defining the subset-sum polynomial.

Definition A.1. *Let $X = \{x_1, \ldots, x_n\}$ be a set of variables and β be a constant from $\mathbb{F}$. Then the subset-sum polynomial $f \in \mathbb{F}[X]$ is the following,*

Equation A.1.

$$f = \sum_{i=1}^{n} x_i - \beta \qquad \Diamond$$

When the characteristic of $\mathbb{F}$ is 0 and $\beta > n$, then the polynomial f is unsatisfiable over the Boolean hypercube (that is $\forall\, \bar{x} \in \{0,1\}^n \;\; f(\bar{x}) \neq 0$). The unsatisfiable system $\{f = 0, X^2 - X = 0\}$ is known to have a *linear*-IPS refutation computed by a $O(n^3)$ size constant depth formula (ABPs). The following lemma from [FSTW21] gives the upper bound.

Lemma A.2. ([FSTW21, Proposition B1]) *Let $\mathbb{F}$ be field of characteristic 0 and $g \in \mathbb{F}[X]$ be the unique multilinear polynomial such that $g \cdot (\sum_{i=1}^{n} x_i - \beta) \equiv 1 \pmod{X^2 - X}$. Then,*

$$g = \sum_{i=0}^{n} \frac{-i!}{\prod_{j=0}^{i}(\beta - i)} \sum_{S \subseteq [n] : |S| = i} \prod_{i \in S} x_i.$$

For any $n, d \in \mathbb{N}$ with $1 \leq d \leq n$, we denote the polynomial $\sum_{S \subseteq [n]:|S|=d} \prod_{i \in S} x_i$ by $\text{ESYM}_{n,d}$, which is the *elementary symmetric polynomial*. The lemma shows that the unique multilinear polynomial g is a *linear* combination of elementary symmetric polynomials. It is well known from the work of Ben-Or [BO83], that the polynomial $\text{ESYM}_{n,d}$ can be computed by a depth 3 formula ($\sum\prod\sum$) of size $O(n^2)$ (see for example [SW01]). Since we need to compute every elementary symmetric polynomial of degree $i \in [n]$, the formula complexity of g is $O(n^3)$. This clearly shows the $\mathsf{IPS}_{\mathsf{Lin}}$ proof complexity of the subset-sum axiom is $O(n^3)$ over characteristic zero fields. Moreover, it is well known that $\text{ESYM}_{n,i}$ can be computed by an ABP of size $O(ni)$. Hence, g also has an ABP of size $O(n^3)$. Using these, we give the following corollary.

Corollary A.3. *Consider the polynomials $f, h \in \mathbb{F}[X, Y]$ as described in Equation 1.2 and Equation 1.6 respectively and the unsatisfiable system described in Theorem 1.10. Then the following holds.*

- *If the characteristic of $\mathbb{F}$ is 0, then there exists a non-multilinear* IPS *refutation for the unsatisfiable systems $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ and $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$, which is computable efficiently by constant depth formulas.*
- *Similarly, over field of characteristic p, there exists a non-multilinear* IPS *refutation for the unsatisfiable systems $\{f = 0, X^2 - X = 0, Y^2 - Y = 0\}$ and $\{h = 0, X^2 - X = 0, Y^2 - Y = 0\}$, which is computable by constant depth formulas of size $\text{poly}(n, p)$.*
- *There is a non-multilinear* IPS *refutation for the unsatisfiable system given in Theorem 1.10 which has a $\text{poly}(n)$-size ABP, when the characteristic of field is 0.*

Proof. Since both the polynomials f (Equation 1.2) and h (Equation 1.6) are sparse polynomials, we can express them as subset-sum axiom polynomials using a distinct new variable for each distinct monomial. If the sparsity of the polynomial is s (for our case, it is $O(n^2)$), then we will have a subset sum axiom polynomial on s variables. In the case of characteristic 0 fields, we can use the upper bound construction described above to get a $O(s^3)$ size constant depth linear IPS refutation for the new system. Next, we substitute the variables by the monomials to get a non-multilinear constant depth refutation of size $O(n^6)$. We prove this formally for f. A similar proof can be shown for h.

Recall that $f = f' + 1$, where

Equation 1.1.

$$f'(\bar{x}, \bar{y}) = \sum_{i=1}^{N} \sum_{S \subseteq X_i} \left(\prod_{j \in S} x_j \cdot y_{t(S)} \right). \tag{1.1}$$

Let sparsity of f' be $s = O(\frac{n^2}{\log n})$. Further, let $Z = \{z_1, \ldots, z_s\}$ be a set of variables and define $\tilde{f}(\bar{z}) = \sum_{i=1}^{s} z_i + 1$, such that $\tilde{f}(m_1, \ldots, m_s) = f(\bar{x})$ where $m_i \in \text{supp}(f')$. Clearly, $\tilde{f}(\bar{z})$ is unsatisfiable over the Boolean cube. Using Lemma A.2, there is a multilinear polynomial $\tilde{g}(\bar{z})$ such that

$\tilde{g}(\bar{z}) \cdot \tilde{f}(\bar{z}) \equiv 1 \pmod{Z^2 - Z}$. That is, there exists polynomials $h_1, \ldots, h_s \in \mathbb{F}[\bar{z}]$ such that the following identity holds,

$$\tilde{g}(\bar{z}) \cdot \tilde{f}(\bar{z}) + \sum_{i=1}^{s} h_i(z_i^2 - z_i) = 1.$$

Substituting back the monomials in place of z variables we get

$$\tilde{g}(\bar{m})\tilde{f}(\bar{m}) + \sum_{i=1}^{s} h_i(\bar{m})(m_i^2 - m_i) = 1,$$

where $\bar{m}$ denotes the monomials in $\mathsf{supp}(f)$. Therefore, there exist $\{h'_i\}_{i\in[n]}$ such that

$$\tilde{g}(\bar{m}) \cdot f(\bar{x}) + \sum_{i=1}^{n} h'(i)(x_i^2 - x_i) = 1$$

The existences of such h'_i follows from [BLRS25, Claim 3.4]. This equation clearly gives the require upper bound of $O(n^6)$. Similar arguments work for the unsatisfiable system given in Theorem 1.10. Here we get a non-multilinear IPS refutation computed by a $\mathrm{poly}(n)$-size ABP.

In the case of positive characteristic, we can use the upper bound from the work of Behera, Limaye, Ramanathan, Srinivasan [BLRS25, Theorem 1.8]. □

Now we sketch a few details which are noted in the conclusion. We start with the following fact, which is given in [FSTW21, HLT24].

Fact A.4. *Let $n \geq d \in \mathbb{N}$ and $f = \mathrm{ESYM}_{n,d} - \beta$ for some $\beta \geq \binom{n}{d} \in \mathbb{F}$. Let $g(\bar{x})$ be the unique multilinear polynomial that agrees with $\frac{1}{f}$ over the Boolean hypercube. Then there exists $\beta' \neq 0$ and non-zero field elements $\alpha_d, \alpha_{d+1}, \ldots, \alpha_n$ such that $g(\bar{x}) = \sum_{i=d}^{n} \alpha_i \,\mathrm{ESYM}_{n,i} + \beta'$*

Since the polynomial $f(\bar{x})$ is symmetric and the multilinear polynomial $g(\bar{x})$ agrees with $\frac{1}{f(\bar{x})}$ over the Boolean hypercube, it must be the case that $g(\bar{x})$ is a symmetric multilinear polynomial. Hence, it can be expressed as a linear combination of elementary symmetric polynomials $\mathrm{ESYM}_{n,i}$. The fact that the coefficients of $\mathrm{ESYM}_{n,i}$ for $i < d$ are 0 follows from Lemma 3.3. Moreover, to the best of our knowledge, the best known formula upper bound for $g(\bar{x})$ is $O(dn^2)$. This follows by computing each $\mathrm{ESYM}_{n,i}$ (for every $i \in [d, n]$) by a $O(n^2)$ size formula using Ben-Or's construction [BO83]. The circuit complexity of $g(\bar{x})$ is $O(n \log^2 n)$ [BCS13] and ABP complexity of $g(\bar{x})$ is $O(n^2)$ (using Ben-Or's construction).

Observation A.5. *Consider the polynomial $g(\bar{x})$ defined in Fact A.4 with $d = \frac{n}{10}$. Then the following statements are true.*

- *Any formula computing a $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation of the system $\{g = 0, X^2 - X = 0\}$ must have size at least $\Omega(n^2)$.*

- *Any ABP computing a* $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ *refutation of the system* $\{g = 0, X^2 - X = 0\}$ *must have size at least* $\Omega(n^2)$.
- *Any circuit computing a* $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ *refutation of the system* $\{g = 0, X^2 - X = 0\}$ *must have size least* $\Omega(n \log n)$.

Proof. By Proposition 2.15, if we show a $\Omega(n^2)$ formula (ABP) lower bound for the unique multilinear polynomial $f(\bar{X})$ that agrees with $\frac{1}{g(\bar{X})}$ over the Boolean hypercube, we get our $\mathsf{mult\text{-}IPS}_{\mathsf{Lin}'}$ refutation lower Bound. By the Fact A.4, here $f(\bar{X}) = \text{ESYM}_{n,\frac{n}{10}}$ which has a $\Omega(n^2)$ formula (ABP) lower bound from [CKSV22]. Note that, there is a crucial condition on characteristic of field $\mathbb{F}$, $\text{Char}(\mathbb{F}) \nmid n$ in order to hold the lower bound. We do not know yet how to remove this condition. So, it is fair to assume $\text{Char}(\mathbb{F}) = 0$. For circuit we refer to the work [BS83], which shows any circuit computing $\text{ESYM}_{n,\frac{n}{10}}$ needs size at least $\Omega(n \log n)$. Here also the size of $\mathbb{F}$ need to be either large enough or $\text{Char}(\mathbb{F}) = 0$ for the lower bound. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il