

New Bounds for the Ideal Proof System in Positive Characteristic

Amik Raj Behera ✉ 🏠 


University of Copenhagen, Denmark

Nutan Limaye ✉ 🏠 

IT University of Copenhagen, Denmark

Varun Ramanathan ✉ 🏠 

Tata Institute of Fundamental Research, Mumbai, India

Srikanth Srinivasan ✉ 🏠 

University of Copenhagen, Denmark

Abstract

In this work, we prove upper and lower bounds over fields of positive characteristics for several fragments of the Ideal Proof System (IPS), an algebraic proof system introduced by Grochow and Pitassi (J. ACM 2018). Our results extend the works of Forbes, Shpilka, Tzameret, and Wigderson (Theory of Computing 2021) and also of Govindasamy, Hakoniemi, and Tzameret (FOCS 2022). These works primarily focused on proof systems over fields of characteristic 0, and we are able to extend these results to positive characteristic.

The question of proving general IPS lower bounds over positive characteristic is motivated by the important question of proving $AC^0[p]$ -Frege lower bounds. This connection was observed by Grochow and Pitassi (J. ACM 2018). Additional motivation comes from recent developments in algebraic complexity theory due to Forbes (CCC 2024) who showed how to extend previous lower bounds over characteristic 0 to positive characteristic.

In our work, we adapt the functional lower bound method of Forbes et al. (Theory of Computing 2021) to prove exponential-size lower bounds for various subsystems of IPS. In order to establish these size lower bounds, we first prove a tight degree lower bound for a variant of *Subset Sum* over positive characteristic. This forms the core of all our lower bounds.

Additionally, we derive upper bounds for the instances presented above. We show that they have efficient constant-depth IPS refutations. This demonstrates that constant-depth IPS refutations are stronger than the proof systems considered above even in positive characteristic. We also show that constant-depth IPS can efficiently refute a general class of instances, namely all symmetric instances, thereby further uncovering the strength of these algebraic proofs in positive characteristic.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Ideal Proof Systems, Algebraic Complexity, Positive Characteristic

Digital Object Identifier 10.4230/LIPIcs.ICALP.2025.22

Category Track A: Algorithms, Complexity and Games

Related Version *Full Version:* [Link to the full version](#)

Funding *Amik Raj Behera:* Supported by Srikanth Srinivasan's start-up grant from the University of Copenhagen.

Nutan Limaye: Supported by Independent Research Fund Denmark (grant agreement No. 10.46540/3103-00116B) and is also supported by the Basic Algorithms Research Copenhagen (BARC), funded by VILLUM Foundation Grant 54451.

Varun Ramanathan: Supported by the Department of Atomic Energy, Government of India, under project number RTI400112. A part of the work was done when the author was visiting the University of Copenhagen and was supported by the European Research Council (ERC) under grant agreement no. 101125652 (ALBA).



© Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan; licensed under Creative Commons License CC-BY 4.0

52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025).

Editors: Keren Censor-Hillel, Fabrizio Grandoni, Joël Ouaknine, and Gabriele Puppis

Article No. 22; pp. 22:1–22:20



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



Srikanth Srinivasan: Supported by the European Research Council (ERC) under grant agreement no. 101125652 (ALBA).

Acknowledgements We would like to thank Iddo Tzameret for his feedback and for sharing information about the independent work of Elbaz, Govindasamy, Lu, and Tzameret. NL thanks Tuomas Hakoniemi and Iddo Tzameret for several discussions on IPS proof systems.

1 Introduction

Propositional Proof Systems

A proof system consists of a set of axioms and inference rules. The goal is to start with the given set of axioms and apply the inference rules repeatedly to prove theorems (tautologies) within the proof system. A proof system is *sound* if it proves only true statements and it is *complete* if it proves all true statements. The area of *Propositional Proof Complexity* aims to understand the strength of different proof systems in the propositional setting. In a foundational work, Cook and Reckhow [10] showed that if we could prove that there exist tautologies such that they require exponential proof size (i.e., vaguely the number of times different inference rules are applied in the proof) in any proof system, then it would resolve the famous NP vs. coNP question in computational complexity theory.

Apart from the connection to this central question in complexity theory, understanding the power of different proof systems is also fundamental to mathematical reasoning. This has motivated a lot of research in the area for the last five decades. (See for instance these reference texts for more context [22, 9, 21].) There are many different kinds of propositional proof systems based on the set of axioms they start with and the kind of inference rules they are allowed to use. In this work, we will focus on algebraic proof systems. In algebraic proof systems, propositional tautologies are expressed as an unsatisfiable set of polynomial equations and the inference rules are algebraic, i.e. they involve reasoning based on polynomial arithmetic.

The study of algebraic proof systems originates from the work of Beame, Impagliazzo, Krajíček, Pitassi, and Pudlák [4] who introduced the Nullstellensatz proof system (based on Hilbert’s Nullstellensatz). Their work was followed by the work of Clegg, Edmonds, and Impagliazzo [8] who introduced Polynomial Calculus as a *dynamic* variant of the Nullstellensatz proof system. Over the years, substantial work on these proof systems has helped us get a good understanding of their power in terms of complexity measures such as sparsity and degree [4, 7, 29, 15, 20, 6, 1].

However, as noted in [13], sparsity and degree only roughly capture the complexity of algebraic proofs. More recently, Grochow and Pitassi [17] proposed the Ideal Proof System (IPS) as a natural generalization of these well-studied algebraic proof systems such as Polynomial Calculus and Nullstellensatz proof systems. In the last decade, several papers studied this proof system. (See for instance [17, 26, 13, 14, 19].) This has allowed us to understand many other aspects of algebraic proofs, such as proof size and proof depth.

In this paper, we extend this line of work. Specifically, we revisit some of the known upper and lower bounds for Ideal Proof Systems over characteristic 0 and show similar bounds over fields of any characteristic¹.

¹ In all the results mentioned here, when we say that a result holds over characteristic 0, it in fact holds over large enough characteristic as well.

1.1 Ideal Proof Systems

We start by describing the general setup for an algebraic (static²) proof system. Let \mathbf{x} denote the set of variables $\{x_1, x_2, \dots, x_n\}$. We are given a set of polynomial axioms $f_1(\mathbf{x}), f_2(\mathbf{x}), \dots, f_m(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ and the goal is to show that there is no 0-1 assignment to the variables such that it simultaneously satisfies $\{f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) = 0, \dots, f_m(\mathbf{x}) = 0\}$ over \mathbb{F} . To force a common Boolean solution, the set of axioms is appended with additional axioms, $\{x_i^2 - x_i = 0\}_{i \in [n]}$ for $i \in [n]$. These are called the *Boolean axioms*.

Based on Hilbert's Nullstellensatz, we know that if $\{f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) = 0, \dots, f_m(\mathbf{x}) = 0\} \cup \{x_i^2 - x_i = 0\}_{i \in [n]}$ are simultaneously not satisfiable, then such a refutation³ can be given by polynomials $A_1(\mathbf{x}), A_2(\mathbf{x}), \dots, A_m(\mathbf{x})$ and $B_1(\mathbf{x}), B_2(\mathbf{x}), \dots, B_n(\mathbf{x})$ such that

$$\sum_{i \in [m]} A_i(\mathbf{x}) \cdot f_i(\mathbf{x}) + \sum_{i \in [n]} B_i(\mathbf{x}) \cdot (x_i^2 - x_i) = 1. \quad (1)$$

The complexity of such a proof can be defined using complexity parameters of the polynomials $\{A_i(\mathbf{x})\}$ and $\{B_i(\mathbf{x})\}$. In the case of the Ideal Proof System, Grochow, and Pitassi proposed that we assume that $A_i(\mathbf{x}), B_i(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ are computed by algebraic circuits. (See Section 1.3 for the formal definition.) Based on this, they defined complexity measures such as circuit size and circuit depth of IPS.

This proof system in its full generality is known to be quite strong. Specifically, it can polynomially simulate Extended Frege [17], which is one of the most powerful among well-studied propositional proof systems. Additionally, the same work also showed that proving lower bounds for this proof system would also imply strong algebraic circuit lower bounds, which is also a very challenging problem.

In light of this (and other reasons explained below), many restricted variants of the IPS have been studied. Let \mathcal{C} be a class of polynomials. Then, a \mathcal{C} -IPS refutation is an IPS-refutation wherein $\{A_i(\mathbf{x})\}_{i \in [m]}$ and $\{B_i(\mathbf{x})\}_{i \in [n]}$ belong to the class \mathcal{C} . Forbes, Shpilka, Tzameret, and Wigderson [13], as well as Govindasamy, Hakoniemi, and Tzameret [14], considered different classes of polynomials, for example, the class of polynomials computed by read-once oblivious algebraic branching programs (roABPs), by multilinear formulas, or by constant-depth algebraic formulas. They proved upper and lower bounds on the size of (some variants of) \mathcal{C} -IPS refutations over characteristic 0.

1.2 Motivation

We extend these works and prove similar bounds in arbitrary characteristic. Our work is motivated by the following important strands of research in proof complexity.

IPS-refutations and $\text{AC}^0[p]$ -Frege

A long-standing open question in proof complexity, open for almost three decades [23], is to prove superpolynomial lower bounds against $\text{AC}^0[p]$ -Frege proof systems, i.e., a proof system in which the lines of the proof are constant-depth Boolean circuits that use modular gates. In the late 80s, Razborov [28] and Smolensky [33, 34] resolved the Boolean circuit lower bound question for $\text{AC}^0[p]$, but the corresponding proof complexity question has proved to be elusive.

² In the literature, the following type of proof system is often referred to as a static proof system. There are other algebraic proof systems, where the proof is presented line-by-line and those are known as dynamic proof systems. Here, we will only discuss static proof systems.

³ The words “proofs” and “refutations” are treated interchangeably in this paper. What we will be “proving” is a statement that “refutes” the existence of a common solution to a system of equations.

Over the years, several attempts have been made to resolve this question. The most relevant to our work is the result by Grochow and Pitassi [17, Theorem 3.5] which showed that constant-depth-IPS over characteristic p can efficiently simulate $\text{AC}^0[p]$ -Frege proofs. This means that proving superpolynomial lower bounds against constant-depth-IPS refutations will give superpolynomial lower bounds against $\text{AC}^0[p]$ -Frege. This gives a strong motivation to prove IPS lower bounds over small characteristics.

Functional lower bounds over any characteristic

Building on the work of [17], [13] further explored the power of IPS refutations. They proposed a concrete approach towards proving size lower bounds for IPS refutations via *functional lower bounds* (further explained in Section 1.4). Their method was inspired by the notion of functional lower bounds in Boolean circuit complexity [16, 12]. They demonstrated the promise of their method by proving several lower bounds for different fragments of IPS.

For example, the strong algebraic complexity lower bounds known for roABPs [25] and multilinear formulas [27] follow from understanding the *evaluation dimension* complexity measure in these models. Since this measure is essentially functional in nature, [13] used it to successfully prove lower bounds for \mathcal{C} -IPS when \mathcal{C} is a class of read-once branching programs or multilinear formulas. Their bounds are over characteristic 0.

This approach of [13] was further adapted by Govindasamy, Hakoniemi, and Tzameret [14] to prove superpolynomial lower bounds against (multilinear) constant-depth-IPS refutations. Their proof builds on some of the key components of the superpolynomial lower bound against constant-depth algebraic circuits by Limaye, Srinivasan, and Tavenas. The latter lower bound of [24] only worked over characteristic 0; for this and other reasons, the result of [14] was also limited to characteristic 0. In a recent paper, however, Forbes [11] improved the circuit lower bound result of [24] and proved the same⁴ lower bound over any characteristic.

In light of these results, the next obvious step is to prove the lower bounds of [13, 14] over any characteristic. We achieve that in this work.⁵

1.3 Our results

To describe our results, we start with the formal definitions of IPS refutations and its variants.

► **Definition 1** (IPS proof systems [17, 13]). *Let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ be a system of unsatisfiable polynomials over the Boolean cube $\{0, 1\}^n$. In other words, there is no Boolean assignment $\mathbf{a} \in \{0, 1\}^n$ to the variables x_1, \dots, x_n so that $f_i(\mathbf{a}) = 0$ for all $i \in [m]$.*

Given a class of algebraic circuits \mathcal{C} , a \mathcal{C} -IPS refutation of the system of equations defined by f_1, \dots, f_m is an algebraic circuit $C \in \mathcal{C}$ in variables $x_1, \dots, x_n, y_1, \dots, y_m, z_1, \dots, z_n$ such that

1. $C(\mathbf{x}, \mathbf{0}, \mathbf{0}) = 0$, and
2. $C(\mathbf{x}, f_1, \dots, f_m, x_1^2 - x_1, \dots, x_n^2 - x_n) = 1$.

The size of the refutation is the size of the circuit C .

⁴ Some parameters in the lower bound by [24] were subsequently improved by [5] and [11] achieves those improved parameters.

⁵ The subset-sum instances from [13, 14] are not always unsatisfiable over fields of positive characteristic; this requires that we tweak their instances to ensure unsatisfiability. Barring these changes, we qualitatively match their lower bounds over fields of positive characteristic.

Further, if the circuit C has individual degree at most 1 in the variables \mathbf{y} and \mathbf{z} , then we say that C is a $\mathcal{C}\text{-IPS}_{\text{LIN}}$ refutation. If the circuit C has individual degree at most 1 in the variables \mathbf{y} (but not necessarily in \mathbf{z}), then C is said to be a $\mathcal{C}\text{-IPS}_{\text{LIN}'}$ refutation.

Finally, we say that a circuit $C \in \mathcal{C}$ is a multilinear $\mathcal{C}\text{-IPS}_{\text{LIN}'}$ refutation if additionally $C(\mathbf{x}, \mathbf{y}, \mathbf{0})$ is a multilinear polynomial in the variables $\mathbf{x} \cup \mathbf{y}$.

► **Remark 2.** We mostly employ the above definition in the case that $m = 1$, i.e. the case when we have a single polynomial equation that is unsatisfiable over the Boolean cube. Further, while our upper bound results are proved in the more restrictive $\mathcal{C}\text{-IPS}_{\text{LIN}}$ proof system, our lower bounds results hold in the setting of the stronger $\mathcal{C}\text{-IPS}_{\text{LIN}'}$ proof systems.

We also recall some standard notions about polynomials and algebraic models of computation, which will be useful below.

Multilinear and symmetric polynomials

A polynomial $f(\mathbf{x}) \in \mathbb{F}[x_1, \dots, x_n]$ is a *multilinear* if the individual degree is at most 1. For a polynomial $f(\mathbf{x})$, the *multilinearization* operator, denoted by $\text{ml}[\cdot]$, changes for each variable x_j and any k , every occurrence of x_j^k in $f(\mathbf{x})$ to x_j .

A polynomial $f(\mathbf{x}) \in \mathbb{F}[x_1, \dots, x_n]$ is said to be a *symmetric polynomial* if the polynomial remains invariant under any permutation of the input variables. For a degree parameter $0 \leq d \leq n$, the d^{th} elementary symmetric polynomial $e_{n,d}(x_1, \dots, x_n)$ is defined to be the following multilinear polynomial $e_{n,d}(x_1, \dots, x_n) = \sum_{\substack{S \subseteq [n] \\ |S|=d}} \prod_{i \in S} x_i$. Whenever n is clear from the context, we will denote the d^{th} elementary symmetric polynomial by $e_d(\mathbf{x})$.

Algebraic models of computation

We recall definitions of some of the standard models of computation relevant to our results.

Algebraic circuits and formulas. An *algebraic circuit* is a directed acyclic graph in which each node either computes a sum (or a linear combination) of its inputs, or a product of its inputs. The leaf nodes are either variables or constants. The size of an algebraic circuit is the number of edges in the circuit, and the depth of an algebraic circuit is the longest path from the output node (a sink) to a leaf node (a source). An *algebraic formula* is an algebraic circuit where the output of each node feeds into at most another node; in other words, the underlying graph of an algebraic formula is a tree. An algebraic formula is a *multilinear formula* if every gate of the formula computes a multilinear formula.

Sparse polynomials and constant-depth circuits. The class $\sum \prod$ consists of depth-2 formulas with an addition gate in the top layer and multiplication gates in the bottom (second) layer. All the gates have unbounded fan-in. $\sum \prod$ formulas essentially compute polynomials in the *sparse* representation i.e. as a sum of monomials. In general, a constant-depth algebraic circuit has $O(1)$ alternating layers of additional and multiplication gates.

Read-Once Oblivious Algebraic Branching Programs. A read-once oblivious algebraic branching program in the variable-order $\pi \in \mathcal{S}_n$ ⁶ is a directed acyclic graph whose vertices are partitioned into n layers $V_0 = \{s\}, V_1, V_2, \dots, V_n = \{t\}$. For each $i \in \{1, 2, \dots, n\}$, there are edges directed from layer V_{i-1} to V_i that are labelled by univariate polynomials in the variable $x_{\pi(i)}$. For each s -to- t path p , the polynomial computed by p is defined to be product

⁶ \mathcal{S}_n denotes the set of all permutation of $[n]$.

of the edge labels on p . The polynomial computed by the roABP is defined as the sum of polynomials computed by all s -to- t paths. The *width* of an roABP is $\max_{0 \leq i \leq n} |V_i|$ i.e. the size of the largest layer of vertices.

For more background on these models of computation, please refer to one of the standard surveys in algebraic complexity ([32],[30]).

1.3.1 Lower bounds over positive characteristic

We start by stating our lower bound results.

► **Theorem 3** (Lower bounds for sparse-IPS_{LIN'} in positive characteristic). *The following holds for any large enough n . Let p be any prime number. Let $k \in \mathbb{N}$ such that $p^k > 2^{\Omega(n)}$. There exist $\alpha_i \in \mathbb{F}_{p^k}$ and $\beta \in \mathbb{F}_{p^{2k}} \setminus \mathbb{F}_{p^k}$ such that*

1. *The polynomial $f = \sum_{i \in [n]} \alpha_i x_i - \beta$ has no Boolean satisfying assignment.*
2. *Any sparse-IPS_{LIN'} refutation⁷ of f must have size at least $2^{\Omega(n)}$*

Note that the hard instance above is a sparse polynomial. We show that it has no small sparse refutation over positive characteristic.

► **Theorem 4** (Lower bounds for fixed-order roABP in positive characteristic). *The following holds for any large enough n . Let p be any prime number. Let $k \in \mathbb{N}$ such that $p^k > 2^{\Omega(n)}$. There exist $\alpha_i \in \mathbb{F}_{p^k}$ and $\beta \in \mathbb{F}_{p^{2k}} \setminus \mathbb{F}_{p^k}$ such that*

1. *The polynomial $f = \sum_{i \in [n]} \alpha_i x_i y_i - \beta$ has no Boolean satisfying assignment.*
2. *Any roABP-IPS_{LIN'} refutation of f in any order of variables where \mathbf{x} variables come before \mathbf{y} variables, must have width $2^{\Omega(n)}$.*

To obtain lower bounds against more powerful models such as roABP-IPS_{LIN'} with respect to *any* order, or multilinear formulas, [13] used a slightly modified hard instance. We also use an instance the same as theirs up to the choice of coefficients.

► **Theorem 5** (Lower bounds for any order roABP-IPS_{LIN'} and multilinear-formula-IPS_{LIN'}). *The following holds for any large enough n . Let p be any prime number. Let $k \in \mathbb{N}$ such that $p^k > 2^{\Omega(n)}$. There exist $\alpha_{i,j} \in \mathbb{F}_{p^k}$ and $\beta \in \mathbb{F}_{p^{2k}} \setminus \mathbb{F}_{p^k}$ such that*

1. *The polynomial $f = \sum_{1 \leq i < j \leq n} \alpha_{i,j} z_{i,j} x_i x_j - \beta$ has no Boolean satisfying assignment.*
2. *Any roABP-IPS_{LIN'} refutation of f must have size at least $2^{\Omega(n)}$.*
3. *Moreover, any multilinear-formula-IPS_{LIN'} refutation of f must have size at least $n^{\Omega(\log n)}$ and for $\Delta = o(\log n / \log \log n)$, any product-depth⁸- Δ multilinear-formula-IPS refutation requires size $\geq n^{\Omega(\frac{1}{\Delta^2} (\frac{n}{\log n})^{1/\Delta})}$.*

Again notice that, f is a sparse polynomial and hence has a polynomial size roABP. It is also efficiently computable by a multilinear formula.

In general, in Boolean proof complexity, it is typical that the hard-to-refute instances are themselves easy to compute. In algebraic proof complexity, there are some lower bound results that do not have this property. That is, the instances that are hard to refute are also hard to compute. For example, the set of results obtained by the approach of multiples in [13, Theorem 1.18, Theorem 1.19, Theorem 1.20] and in a paper by Andrews and Forbes [3]. Additionally, in a recent work, Hakoniemi, Limaye, and Tzameret [19] presented instances

⁷ Note that sparse-IPS_{LIN} (a weaker system than sparse-IPS_{LIN'}) is equivalent to the Nullstellensatz proof system of [4].

⁸ The product-depth of a circuit is the maximum number of product gates appearing in any leaf-to-root path.

that were hard to refute for $\text{roABP-IPS}_{\text{LIN}'}$ and for multilinear-formula- $\text{IPS}_{\text{LIN}'}$ over any characteristics, i.e., similar to what we prove here. However, unfortunately, their instances were hard to compute and specifically, they could not be computed by roABP or by multilinear formulas. Hence, our result here have the best of both the worlds; the lower bounds hold over any characteristic and the hard instances are easy to compute.

► **Theorem 6** (Lower bounds for multilinear constant-depth- $\text{IPS}_{\text{LIN}'}$ in positive characteristic). *The following holds for any large enough n . Let p be any prime and let $k \in \mathbb{N}$ be large enough so that $p^k > 2^{\Omega((\log n)^2)}$. There exist $\alpha_{i,j,k,\ell} \in \mathbb{F}_{p^k}$ and $\beta \in \mathbb{F}_{p^{2k}} \setminus \mathbb{F}_{p^k}$ such that*

1. *The polynomial $f = \sum_{1 \leq i < j < k < \ell \leq n} \alpha_{i,j,k,\ell} z_{i,j,k,\ell} x_i x_j x_k x_\ell - \beta$ has no Boolean satisfying assignment.*
2. *Any multilinear constant-depth- $\text{IPS}_{\text{LIN}'}$ refutation of f must have size $n^{\omega(1)}$.*

The characteristic 0 (or large characteristic) version of the above theorem was presented in [14]. Their lower bound is a step towards constant-depth-IPS lower bounds. Our result above can thus be thought of as another step forward in the right direction. Moreover, our input instance is the same as the input instance in Theorem 1 [14] up to the choice of coefficients, and it is easy to compute (while being hard to refute). More specifically, it is computable by polynomial-sized constant-depth multilinear formulas.

► **Remark 7.** In all our results, the field characteristic is arbitrary, but the field size is quite large, i.e., p^k is either exponential or superpolynomial. This setting is non-trivial because the field elements have polynomial bit complexity. Other results in the area, such as the work of Alekseev, Grigoriev, Hirsch, and Tzameret [2] similarly use polynomial constraints with coefficients from exponentially large domains. Specifically [2] study a variant of the subset sum instance, called the Binary Value Principle, $\sum_{i \in [n]} 2^{i-1} x_i + 1 = 0$ in the context of IPS proof systems in fields of characteristic zero.

It is an interesting open question to prove similar IPS lower bounds over finite fields of small size. Unfortunately, as we show below, this forces the polynomial instances to become more complicated. See Section 1.5 for recent independent work that makes progress in this direction.

1.3.2 Upper bounds over positive characteristic

A natural question for hard instances above is: what is the weakest proof system in which they are efficiently refutable? In personal communication, Tzameret observed that the above instances were refutable by constant-depth- IPS_{LIN} hence showing that these proof systems can be exponentially more succinct than their multilinear counterpart. The theorem below shows that the above polynomials have efficient constant-depth- IPS_{LIN} refutations, even in the setting of positive characteristic.

► **Theorem 8** (Upper bounds for (non-multilinear) constant-depth- IPS_{LIN}). *Fix a prime number p . The following holds for any natural numbers n and k .*

Let $f \in \mathbb{F}[x_1, \dots, x_n]$ be any polynomial with sparsity s and degree D with coefficients from the field \mathbb{F}_{p^k} and let β be any element of $\mathbb{F} \setminus \mathbb{F}_{p^k}$ where \mathbb{F} is a field extension of \mathbb{F}_{p^k} .

Then,

1. *The polynomial $f(\mathbf{x}) - \beta$ has no satisfying assignment over the Boolean cube $\{0, 1\}^n$*
 2. *There is a constant-depth- IPS_{LIN} refutation of degree $O(k \cdot p \cdot D)$ and size $\text{poly}(s, p)$.*
- Note that since $\beta \notin \mathbb{F}_{p^k}$, the polynomial $f(\mathbf{x}) - \beta$ does not have a zero over $\{0, 1\}^n$ (in fact it does not have a solution over $\mathbb{F}_{p^k}^n$). So the first item of above follows immediately.

► **Remark 9.** Suppose the characteristic p is a fixed prime independent of the number of variables n .

1. Theorem 8 shows that the exponential field size in Theorem 3, Theorem 4 and Theorem 5 is not an artifact of the proofs.⁹ For fields of subexponential size, the polynomials in these theorems have refutations of degree $o(n)$ and in particular have $\text{roABP-IPS}_{\text{LIN}}$ refutations of size $2^{o(n)}$.¹⁰
2. Theorem 8 also shows that the multilinearity assumption in Theorem 6 is not an artifact of the proof. Non-multilinear proofs, even over large fields, allow efficient constant-depth refutations for sparse instances.

Our final result shows a constant-depth upper bound for multilinear and *symmetric* systems of polynomials, i.e. systems defined by polynomials $f(x_1, \dots, x_n)$ of the form $\sum_{d=1}^n \alpha_d e_{n,d} + \alpha_0$ where $e_{n,d}$ denotes the elementary symmetric polynomial of degree d in variables x_1, \dots, x_n . Such polynomial systems have been employed in [13] to prove lower bounds against restricted systems of constant-depth- IPS_{LIN} . Our results imply that general constant-depth circuit refutations can be exponentially more succinct than these restricted families, even for positive characteristic.

► **Theorem 10** (Upper bounds for multilinear symmetric systems). *Fix a field \mathbb{F} . Let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ be a family of multilinear and symmetric polynomials with no common Boolean solution i.e. there does not exist a $\mathbf{x} \in \{0, 1\}^n$ such that each $f_i(\mathbf{x}) = 0$. This system has a constant-depth- IPS_{LIN} refutation of size $\mathcal{O}(m^2 n^5 \log n)$ and depth 8.*

1.4 Proof techniques

Lower bounds

Our proof uses the functional lower bound method introduced by [13], which can be described as follows. We know that a $\mathcal{C}\text{-IPS}_{\text{LIN}'}$ refutation for $f(\mathbf{x})$ consists of $A(\mathbf{x}), B_i(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that

$$f(\mathbf{x}) \cdot A(\mathbf{x}) + \sum_{i \in [n]} (x_i^2 - x_i) \cdot B_i(\mathbf{x}) = 1,$$

where $A(\mathbf{x}), B_1(\mathbf{x}), \dots, B_n(\mathbf{x})$ belong to \mathcal{C} . As $f(\mathbf{x})$ is unsatisfiable over the Boolean hypercube, this implies that over the Boolean hypercube, $A(\mathbf{x})$ is a well-defined reciprocal of $f(\mathbf{x})$. Hence, to show that $A(\mathbf{x})$ cannot belong to \mathcal{C} , it is enough to show that any polynomial that agrees with $1/f(\mathbf{x})$ cannot be computed by \mathcal{C} . That is, the problem of proving a lower bound on the size of $\mathcal{C}\text{-IPS}_{\text{LIN}'}$ is reduced to proving a functional lower bound for $1/f(\mathbf{x})$.

At the heart of such a functional lower bound lies a *degree lower bound*, i.e., a lower bound on the degree of $\tilde{f}(\mathbf{x})$, where $\tilde{f}(\mathbf{x})$ and $f(\mathbf{x})$ are related. In fact, $f(\mathbf{x})$ is a *lifted* version of $\tilde{f}(\mathbf{x})$. Once we have such a degree lower bound for $\tilde{f}(\mathbf{x})$, we can apply proof ideas from algebraic complexity theory such as the rank-based lower bound methods. These methods allow for the degree lower bounds for $\tilde{f}(\mathbf{x})$ to be lifted to size lower bounds for $f(\mathbf{x})$.

⁹ Suppose the field \mathbb{F}_{p^k} is not large enough, say, $k = o(n)$. Then there is a refutation of degree $d = \mathcal{O}(k \cdot p \cdot D)$, which is $o(n)$ when p and D are constants. In particular, the sparsity of the refutation is at most $\binom{n+d}{d}$, which is $2^{o(n)}$ when $d = o(n)$.

¹⁰ When the characteristic p is a growing function of n , this argument breaks down. It might be possible to get rid of the exponential field size.

For their machinery to work over positive characteristic, we prove a *positive characteristic* version of the degree lower bound (see Lemma 17 for the formal statement). In the case of the lower bound argument in [13], it was important to obtain a tight degree lower bound of exactly n . They needed it for the next step, i.e., *lifting*, to work. In our case, we show that such a degree lower bound holds with high probability (over the choice of coefficients of the hard instance). Once we have the degree lower bound, the rest of the lower bound proof works similar to the proof by [13]. Please refer to the full version for all the proofs.

Constant-depth upper bounds

We start by describing the main ideas in the proof of Theorem 8. Here, we proceed in two steps. First, we observe that for any sparse polynomial of degree d , we can *flatten* it to a linear polynomial by renaming the monomials by fresh variables. Our hard instance is indeed sparse, hence the observation can be used to rewrite the polynomial as a linear polynomial over a fresh set of variables.

Now, consider a linear polynomial $L(\mathbf{x}) - \beta$ such that $L(\mathbf{x}) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$, where $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{p^k}$ for some k and prime p and $\beta \in \mathbb{F} \setminus \mathbb{F}_{p^k}$ such that it is not satisfiable over 0-1 assignments.

To prove that the polynomial has a refutation over constant-depth circuits, we first prove that for every j , $L_j(\mathbf{x}) = \alpha_1^{p^j} x_1 + \alpha_2^{p^j} x_2 + \dots + \alpha_n^{p^j} x_n - \beta^{p^j}$ can be expressed as a multiple of $L(\mathbf{x})$ modulo the ideal $\mathbf{x}^p - \mathbf{x}$, which is a shorthand for the ideal generated by $\{x_i^p - x_i\}_{i \in [n]}$.

We then observe that for $j = k$, $L_k(\mathbf{x}) - L(\mathbf{x})$ is a non-zero constant and use this observation to construct small depth circuits for the refutation of $L(\mathbf{x}) - \beta$. Throughout, we use some standard but useful tricks available to positive characteristic fields. Please refer to the full version for all the proofs.

Upper bounds for symmetric polynomials

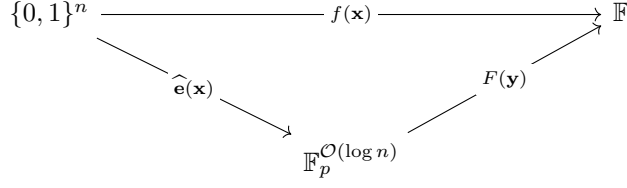
Now we discuss the proof outline for Theorem 10. For ease of exposition, we explain the ideas for the case of $m = 1$ in Theorem 10, i.e. there is one multilinear symmetric polynomial $f(\mathbf{x})$ that does not have a solution over the Boolean cube $\{0, 1\}^n$. Suppose \mathbb{F} has characteristic $p > 0$. Any symmetric polynomial is a polynomial of the n elementary symmetric polynomials¹¹ i.e. $e_1(\mathbf{x}), \dots, e_n(\mathbf{x})$. However, if we restrict to the Boolean cube $\{0, 1\}^n$, then any symmetric polynomial is a polynomial of just $\mathcal{O}(\log n)$ elementary symmetric polynomials. Let $\widehat{\mathbf{e}}(\mathbf{x})$ denotes the tuple of those $\mathcal{O}(\log n)$ elementary symmetric polynomials.

Let $F(\mathbf{y})$ be the $\mathcal{O}(\log n)$ variate polynomial such that $F(\mathbf{y}) \circ \widehat{\mathbf{e}}(\mathbf{x})$ agrees with $f(\mathbf{x})$ on the Boolean cube $\{0, 1\}^n$. The Boolean cube $\{0, 1\}^n$ is mapped to $\mathbb{F}_p^{\mathcal{O}(\log n)}$ under the map $\widehat{\mathbf{e}}(\mathbf{x})$ because $\text{char}(\mathbb{F}) = p$. The unsatisfiability of $f(\mathbf{x})$ over the Boolean cube $\{0, 1\}^n$ implies the unsatisfiability of $F(\mathbf{y})$ over $\mathbb{F}_p^{\mathcal{O}(\log n)}$. Applying Hilbert's Nullstellensatz Theorem (see Theorem 15) on the unsatisfiability¹² of $F(\mathbf{y})$ over $\mathbb{F}_p^{\mathcal{O}(\log n)}$, we get a *low-variate* Nullstellensatz certificate (it is a Nullstellensatz certificate in just $\mathcal{O}(\log n)$ variables)¹³. The coefficients of this low-variate Nullstellensatz certificate can be computed via $\text{poly}(n)$ -sized constant-depth circuits. This follows from the fact that we are working over constant characteristic. Refer to the diagram below for a schematic representation of what we discussed so far.

¹¹This follows from the Fundamental Theorem of Symmetric Polynomials.

¹²To capture the restriction of \mathbb{F}_p^n , we add n univariate polynomials, each of which vanishes on one coordinate of \mathbb{F}_p^n .

¹³Loosely speaking, one can imagine this as a “dimension reduction” of our problem. The symmetric structure of $f(\mathbf{x})$ led us to convert a problem in n variables to a problem in just $\mathcal{O}(\log n)$ variables.



Next we “lift” the Nullstellensatz back to the n variables (x_1, \dots, x_n) . To do so, we plug-in $\widehat{\mathbf{e}}(\mathbf{x})$ in place of \mathbf{y} . Observe that this substitution by $\widehat{\mathbf{e}}(\mathbf{x})$ preserves the size and the depth of the coefficients of the low-variate Nullstellensatz certificate because of the Ben-Or’s construction (see Theorem 12).

It remains to *prove* via constant-depth circuits that $F(\widehat{\mathbf{e}}(\mathbf{x}))$ agrees with $f(\mathbf{x})$ on the Boolean cube, i.e. $F(\widehat{\mathbf{e}}(\mathbf{x})) - f(\mathbf{x})$ lie in the ideal $(\mathbf{x}^2 - \mathbf{x})$. Here “to prove in constant-depth circuits” refers to giving a certificate for the ideal membership whose coefficients can be computed by constant-depth circuits. More precisely, we want to prove that there exists polynomials $B_j(\mathbf{x})$ ’s which have $\text{poly}(n)$ -sized constant-depth circuits such that

$$F(\widehat{\mathbf{e}}(\mathbf{x})) = f(\mathbf{x}) + \sum_{j=1}^n B_j(\mathbf{x}) \cdot (x_j^2 - x_j).$$

This is the key step in our proof. To prove this, it suffices to prove the following special case.

► **Lemma 11.** *Let $\ell = \mathcal{O}(\log n)$ and fix an arbitrary sequence $(\alpha_1, \dots, \alpha_\ell)$ where each $\alpha_i \in [n]$. There exist polynomials $B_j(\mathbf{x})$ ’s such that*

$$\prod_{i=1}^{\ell} e_{\alpha_i}(\mathbf{x}) = \text{ml} \left[\prod_{i=1}^{\ell} e_{\alpha_i}(\mathbf{x}) \right] + \sum_{j=1}^n B_j(\mathbf{x}) \cdot (x_j^2 - x_j),$$

and each polynomial $B_j(\mathbf{x})$ can be computed by a $\text{poly}(n)$ -sized constant-depth circuit.

Please refer to the full version for all the proofs.

1.5 Related work

In an independent work, Elbaz, Govindasamy, Lu, and Tzameret (personal communication) consider related questions. Using the recent lower bound of Forbes [11], which proves the positive characteristic version of the constant-depth formula lower bound of [24], they obtain lower bounds for fragments of the IPS over finite fields of *any* size.

1.6 Preliminaries

In this subsection, we present a few more definitions and standard facts on polynomials that will be used in our proofs later on.

For a polynomial $f(x_1, \dots, x_n)$, the individual degree of f is an integer D such that for all $i \in [n]$, the degree of f when viewed as a univariate polynomial in the variable x_i is at most D .

A classical and beautiful construction of Ben-Or shows that every elementary symmetric polynomial can be computed by $\text{poly}(n)$ -sized constant-depth circuits.

► **Theorem 12** (Ben-Or’s construction for elementary symmetric polynomials). (See [31, Theorem 5.1]). Let \mathbb{F} be a field with $|\mathbb{F}| > n$. Then for every $d \in [n]$, the d^{th} elementary symmetric polynomial $e_d(x_1, \dots, x_n)$ has a circuit of size $\mathcal{O}(n^2)$ and depth 3 (a $\Sigma\Pi\Sigma$ circuit). More particularly, for any choice of $(n+1)$ distinct elements $\gamma_1, \dots, \gamma_{n+1} \in \mathbb{F}$ and for every $k \in [n]$, there exists coefficients $c_{k,i}$ ’s such that

$$e_k(\mathbf{x}) = \sum_{i=1}^{n+1} c_{k,i} \prod_{j=1}^n (1 + \gamma_i x_j)$$

► **Theorem 13** (Polynomial Identity Lemma). (See [18, Lemma 9.2.2]). Let \mathbb{F} be an arbitrary field. Let $f(\mathbf{x})$ be a nonzero polynomial of degree at most d and let $S \subseteq \mathbb{F}$. If we choose $\mathbf{a} \sim S^n$ uniformly at random, then:

$$\Pr_{\mathbf{a} \sim S^n} [f(\mathbf{a}) = 0] \leq \frac{d}{|S|}$$

For a natural number k and variables (z_1, \dots, z_n) , we will use $(\mathbf{z}^k - \mathbf{z})$ to denote the following ideal $(\mathbf{z}^k - \mathbf{z}) := (z_1^k - z_1, \dots, z_n^k - z_n) \subseteq \mathbb{F}[z_1, \dots, z_n]$.

Next we recall the definition of an ideal and a variety, and then we state Hilbert’s Nullstellensatz.

► **Definition 14** (Ideal and Variety). Fix any field \mathbb{F} and consider the commutative ring $\mathbb{F}[x_1, \dots, x_n]$. For a set of polynomials $f_1, \dots, f_m \in \mathbb{F}[\mathbf{x}]$, the ideal generated by f_i ’s, denoted by (f_1, \dots, f_m) is defined as:

$$(f_1, \dots, f_m) = \left\{ h \in \mathbb{F}[\mathbf{x}] \mid \exists g_1, \dots, g_m \in \mathbb{F} \text{ such that } h = \sum_{i=1}^m g_i f_i \right\}.$$

For a set of polynomials $f_1, \dots, f_m \in \mathbb{F}$, their variety, denoted by $\mathbb{V}(f_1, \dots, f_m)$ is a subset of the algebraic closure of \mathbb{F}^n , defined as:

$$\mathbb{V}(f_1, \dots, f_m) = \{ \mathbf{a} \in \bar{\mathbb{F}}^n \mid f_1(\mathbf{a}) = \dots = f_m(\mathbf{a}) = 0 \}.$$

Now we state Hilbert’s Nullstellensatz which essentially says that if a set of polynomials do not have a common zero, then there exists “witness” for this, i.e. one can express 1 as a polynomial combination of f_i ’s.

► **Theorem 15** (Hilbert’s Nullstellensatz). Fix any field \mathbb{F} . Let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ be a set of multivariate polynomials such that they do not have any common zeros over the algebraic closure of \mathbb{F} . Then the constant 1 lies in the ideal $(f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$. In other words, there exists polynomials $A_1, \dots, A_m \in \mathbb{F}[x_1, \dots, x_n]$ such that

$$A_1(\mathbf{x}) \cdot f_1(\mathbf{x}) + \dots + A_m(\mathbf{x}) \cdot f_m(\mathbf{x}) = 1.$$

Strictly speaking, Hilbert’s Nullstellensatz guarantees that the polynomials A_i ’s are in $\bar{\mathbb{F}}[\mathbf{x}]$ ($\bar{\mathbb{F}}$ is the algebraic closure of \mathbb{F}). However, the above statement also follows easily by observing that we can solve for A_i ’s by solving a system of linear equations over \mathbb{F} . Throughout this article, we will refer to $(A_1(\mathbf{x}), \dots, A_m(\mathbf{x}))$ as a *Nullstellensatz certificate*¹⁴ for the system $\{f_1(\mathbf{x}), \dots, f_m(\mathbf{x})\}$. We will also refer to A_i ’s as *coefficients* because if we take a polynomial combination of f_i ’s with A_i ’s being the coefficients, then we can generate 1.

¹⁴ There are infinitely many Nullstellensatz certificates for a system $\{f_1, \dots, f_m\}$. To see this, suppose $m = 2$ and let (A_1, A_2) be a Nullstellensatz certificate. Then for any polynomial $g \in \mathbb{F}[\mathbf{x}]$, $(A_1 + g f_2, A_2 - g f_1)$ is also a Nullstellensatz certificate.

2 Lower bounds in large fields of positive characteristic

In this section, we will prove size lower bounds for several fragments of IPS over positive characteristic. As explained in Section 1.3.1, we start by proving a tight degree lower bound (Lemma 17) over positive characteristic. Using our positive characteristic variant of the degree lower bound, we then recover the lower bound results from [13] and [14] over positive characteristic.

2.1 Degree lower bounds over large fields of arbitrary characteristic

For any $\mathbf{a} \in \{0, 1\}^n$, we use $|\mathbf{a}|$ to denote its Hamming weight. For any $\mathbf{a} = (a_1, \dots, a_n) \in \{0, 1\}^n$ and any subset of indices $S \subseteq [n]$, we use \mathbf{a}_S to denote $\prod_{i \in S} a_i$. All the statements in this section work over fields of arbitrary characteristic.

First, we state a standard fact about multilinear polynomials, which will be useful in the main lemma.

► **Fact 16.** *Let $f(\mathbf{x}) = \sum_{S \subseteq [n]} \lambda_S \mathbf{x}_S$ be a multilinear polynomial on n variables. Then,*

$$\lambda_{[n]} = \sum_{\mathbf{a} \in \{0, 1\}^n} (-1)^{|\mathbf{a}|} f(\mathbf{a})$$

The next lemma is our main degree lower bound which shows that a multilinear polynomial for the inverse of a random linear form will have maximal degree. While similar statements have been observed in the literature (e.g. [15, Proposition 2]), we give an explicit proof for the sake of completeness.

► **Lemma 17.** *Let \mathbb{F} and \mathbb{F}' be fields such that \mathbb{F} is a strict subfield of \mathbb{F}' . Let $n \in \mathbb{N}$ be a natural number and let \mathbf{x} denote the tuple of variables (x_1, \dots, x_n) . Fix any $\beta \in \mathbb{F}' \setminus \mathbb{F}$. For any $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}^n$, let $f_\alpha(\mathbf{x})$ be the unique multilinear polynomial that agrees with the function*

$$\frac{1}{\sum_{i=1}^n \alpha_i x_i - \beta}$$

on the Boolean cube $\{0, 1\}^n$. Let $S \subseteq \mathbb{F}$ be any finite subset of the field. Then, for a uniformly random $\alpha \sim S^n$:

$$\Pr_{\alpha \sim S^n} [\deg f_\alpha(\mathbf{x}) = n] \geq 1 - \frac{2^n - 1}{|S|}$$

Proof. By Fact 16, the coefficient of $\mathbf{x}_{[n]}$ in $f_\alpha(\mathbf{x})$ is $\sum_{\mathbf{a} \in \{0, 1\}^n} (-1)^{|\mathbf{a}|} f_\alpha(\mathbf{a})$, or equivalently,

$$\sum_{V \subseteq [n]} (-1)^{|V|} \frac{1}{(\sum_{i \in V} \alpha_i) - \beta}$$

Based on the above expression, we define the rational function $\lambda_{[n]}(\mathbf{z})$ as follows.

$$\lambda_{[n]}(\mathbf{z}) := \sum_{V \subseteq [n]} (-1)^{|V|} \frac{1}{(\sum_{i \in V} z_i) - \beta}$$

We will use $N(\mathbf{z})$ and $D(\mathbf{z})$ to denote the numerator and denominator of $\lambda_{[n]}(\mathbf{z})$. For any $S \subseteq [n]$, we will use $L_S(\mathbf{z})$ to denote $\sum_{i \in S} z_i$. It follows that

$$\begin{aligned} N(\mathbf{z}) &= \sum_{V \subseteq [n]} (-1)^{|V|} \prod_{T \subseteq [n]: T \neq V} (L_T(\mathbf{z}) - \beta) \\ D(\mathbf{z}) &= \prod_{V \subseteq [n]} (L_V(\mathbf{z}) - \beta) \end{aligned}$$

Since $\beta \in \mathbb{F}' \setminus \mathbb{F}$, $D(\alpha) \neq 0$ for any $\alpha \in \mathbb{F}$. If we prove that $N(\mathbf{z})$ is a non-zero polynomial, then by the Polynomial Identity Lemma (Theorem 13), for any finite subset $S \subseteq \mathbb{F}$, $\Pr_{\alpha \sim S^n}[N(\alpha) \neq 0] \geq 1 - \frac{2^n - 1}{|S|}$, which implies that $\Pr_{\alpha \sim S^n}[\lambda_{[n]}(\alpha) \neq 0] \geq 1 - \frac{2^n - 1}{|S|}$, and thus proves the theorem. Thus, it is enough to prove that some monomial in $N(\mathbf{z})$ has non-zero coefficient.

For $V \neq \emptyset$, $\prod_{T \subseteq [n]: T \neq V} (L_T(\mathbf{z}) - \beta)$ has degree at most $2^n - 2$ since $L_\emptyset(\mathbf{z}) - \beta$ will not increase the degree. The term $\prod_{T \neq \emptyset} (L_T(\mathbf{z}) - \beta)$ syntactically contributes monomials of degree $2^n - 1$ from $\prod_{T \neq \emptyset} L_T(\mathbf{z})$, but is possible that these coefficients vanish if the field \mathbb{F} is of positive characteristic. We will show that there is a monomial of degree $2^n - 1$ with coefficient 1, and thus this monomial will survive over any field.

▷ **Claim 18.** The coefficient of the monomial¹⁵ $\prod_{i=1}^n z_i^{2^{i-1}}$ in $\prod_{T \neq \emptyset} (L_T(\mathbf{z}) - \beta)$ is 1.

Proof sketch. We would like to count the number of ways of collecting variables from each $L_T(\mathbf{z})$ to construct the required monomial. We first observe (via a simple counting argument) that for every $i \in [n]$, the number of subsets $T \subseteq [n]$ such that $\{j \in [n] : j > i\} \cap T = \emptyset$, and $i \in T$, is 2^{i-1} . Moreover, for each $i \in [n]$, if \mathcal{T}_i is the collection of subsets with the above properties, then we observe that $\mathcal{T}_i \cap \mathcal{T}_j = \emptyset$ for all $i \neq j$, $i \in [n]$, $j \in [n]$.

With these observations, it inductively follows that for each $i \in [n]$, conditioned on the degree of variables z_n, \dots, z_{i+1} being correct (i.e. $z_j^{2^{j-1}}$), there is exactly one way of ensuring that the degree of z_i is 2^{i-1} : for each T that is one of the 2^{i-1} subsets satisfying the properties of the above observation, select the z_i 's from $L_T(\mathbf{z})$. ◁

◀

The next lemma proves a stronger version of the previous lemma: for a random linear form, the inverse of *every* restriction of the linear form (by setting some variables to 0) will have maximal degree. It follows from the previous lemma and an union bound.

► **Lemma 19.** Let \mathbb{F} and \mathbb{F}' be fields such that \mathbb{F} is a strict subfield of \mathbb{F}' . Let $n \in \mathbb{N}$ be a natural number and let \mathbf{x} denote the tuple of variables (x_1, \dots, x_n) . Fix any $\beta \in \mathbb{F}' \setminus \mathbb{F}$. For any $\emptyset \neq U \subseteq [n]$, let $f_{\alpha, U}(\mathbf{x})$ be the unique multilinear polynomial that agrees with the function

$$\frac{1}{\sum_{i \in U} \alpha_i x_i - \beta}$$

on the Boolean cube $\{0, 1\}^n$. Let $S \subseteq \mathbb{F}$ be a finite subset of the field. Then, for an $\alpha \sim S^n$ chosen uniformly at random:

$$\Pr_{\alpha \sim S^n}[\exists \text{ a non-empty } U \subseteq [n] : \deg f_{\alpha, U}(\mathbf{x}) < |U|] \leq \sum_{\emptyset \neq U \subseteq [n]} \frac{2^{|U|} - 1}{|S|} < \frac{2^{2n}}{|S|}$$

In particular, with probability at least $1 - (2^{2n}/|S|)$ over the choice of $\alpha \sim S^n$, for every $U \subseteq [n]$, the leading monomial of $f_{\alpha, U}(\mathbf{x})$ is $c \cdot \prod_{i \in U} x_i$ for some $c \in \mathbb{F} \setminus \{0\}$.

¹⁵The same proof works for any monomial $\prod_{i=1}^n z_{\sigma(i)}^{2^{i-1}}$, where σ is an arbitrary permutation on $[n]$.

2.2 Constant-depth multilinear $\text{IPS}_{\text{LIN}'}$ lower bounds over large fields of arbitrary characteristic

In [14], Govindasamy, Hakoniemi, and Tzameret prove super polynomial lower bounds against constant-depth multilinear $\text{IPS}_{\text{LIN}'}$ refutations of the subset sum variant

$$\sum_{i,j,k,l \in [n]} z_{i,j,k,l} x_i x_j x_k x_l - \beta$$

In particular, they prove the following theorem.

► **Theorem 20** (Constant-depth functional lower bounds [14]). *Let $n, \Delta \in \mathbb{N}_+$ with $\Delta \leq \mathcal{O}(\log \log \log n)$ and assume that $\text{char}(\mathbb{F}) = 0$. Let f be the multilinear polynomial such that*

$$f = \frac{1}{\sum_{i,j,k,l \in [n]} z_{i,j,k,l} x_i x_j x_k x_l - \beta}$$

over the Boolean cube. Then, any circuit of product-depth Δ computing f has size at least

$$n^{(\log n)^{\exp(-\mathcal{O}(\Delta))}}$$

We prove the same statement for large fields of arbitrary characteristic. Our proof exactly follows the structure of [14]. Their proof requires the $\text{char } \mathbb{F} = 0$ condition for two reasons:

1. They use the results of Limaye, Srinivasan, and Tavenas [24], which gave superpolynomial lower bounds against constant-depth circuits over any field \mathbb{F} with $\text{char}(\mathbb{F}) = 0$ or greater than the degree d of the hard polynomial. In particular, they use the result that over fields with $\text{char}(\mathbb{F}) = 0$ or greater than d , any low-degree set-multilinear polynomial computed by a constant-depth circuit can also be computed by a set-multilinear constant-depth circuit.¹⁶
2. They use the degree lower bound for the multilinear representation of $1/(\sum_{i \in [n]} x_i - \beta)$, proved by Forbes, Shpilka, Tzameret, and Wigderson [13].

To deal with the first requirement, we use the recent beautiful result of Forbes [11], which extends the results of [24] to arbitrary fields. In particular, we will use the following statement from [11], which says that the set-multilinear projection of a constant-depth circuit can be efficiently computed by a constant-depth circuit over arbitrary fields.

► **Theorem 21.** [11, Corollary 27]. *Let \mathbb{F} be an arbitrary field. Let $\mathbf{x} = \mathbf{x}_1 \sqcup \mathbf{x}_2 \sqcup \dots \sqcup \mathbf{x}_d$ be a partition of the variables \mathbf{x} . Suppose f can be computed by a size s product-depth Δ arithmetic circuit. Then the set-multilinear projection of f (the restriction of f to monomials that are set-multilinear with respect to the specified partition) can be computed by a size $\text{poly}(s, \Theta(\frac{d}{\log d})^d)$ -size circuit of product-depth 2Δ .*

To deal with the second requirement, we use our degree lower bound from Lemma 19, which works for arbitrary fields of exponential size i.e. there is no restriction on the characteristic of the field.

¹⁶They also use other ideas from [24] such as relative rank, word polynomial, etc., but those ideas do not require any restrictions on the characteristic of the underlying field.

Overview of [14]

1. Using the *word polynomials* framework of [24], construct a *knapsack polynomial* $\text{ks}_{\mathbf{w}}$ (for a partition given by a word $w \in \mathbb{Z}^d$) with the property that the set-multilinear projection of $\frac{1}{\text{ks}_{\mathbf{w}}}$ over the Boolean cube requires superpolynomially large set-multilinear constant-depth circuits.
2. Consider a degree-4 subset-sum variant $f(\mathbf{z}, \mathbf{x}) := \sum_{i,j,k,l} z_{i,j,k,l} x_i x_j x_k x_l - \beta$ so that for the word $w \in \mathbb{Z}^d$ that will be used to instantiate the previous point, there exists an assignment of some of the variables in \mathbf{z}, \mathbf{x} that maps $f(\mathbf{z}, \mathbf{x})$ to $\text{ks}_{\mathbf{w}}$ (upto a renaming of variables).
3. If there is a multilinear polynomial computing $1/f(\mathbf{z}, \mathbf{x})$ over $\{0, 1\}^n$ that has a small constant-depth circuit, then there is a multilinear polynomial computing $1/\text{ks}_{\mathbf{w}}$ over $\{0, 1\}^n$ that has a small constant-depth circuit. Moreover by the set-multilinearization of [24], there is a small set-multilinear constant-depth circuit computing the set-multilinear projection of $1/\text{ks}_{\mathbf{w}}$.
4. Combining the first point with the contrapositive of the third point, conclude that any multilinear polynomial computing $1/f(\mathbf{z}, \mathbf{x})$ over $\{0, 1\}^n$ requires superpolynomially large constant-depth circuits. The multilinear constant-depth IPS_{LIN} lower bound follows.

In [14], the proof for the hardness of $\frac{1}{\text{ks}_{\mathbf{w}}}$ requires the underlying field to be of large characteristic essentially because it requires the degree lower bound from [13], which requires large characteristic. To make Theorem 20 work over fields of positive characteristic, we will employ our degree lower bound from Lemma 19 with a variant of the knapsack polynomial; the rest of the proof remains the same as that of Theorem 20. To provide the necessary details, we first describe the construction of the knapsack polynomial. Then, we state the particular claim from [14] that uses the degree lower bound from [13]. Finally, we show how our degree lower bound Lemma 19 fits into the rest of the proof.

Constructing the knapsack polynomial

We shall now recall the definitions required for defining the hard polynomial in [14] via the word polynomials template of [24].

Let $\mathbf{w} \in \mathbb{Z}^d$ be an arbitrary word. For any $S \subseteq [d]$, let $w|_S$ denote the subword of w indexed by the set S . Consider the sequence $\bar{X}(w) = (X(w_1), \dots, X(w_d))$ of sets of variables. Define the *positive indices* and *negative indices* of \mathbf{w} as:

$$P_{\mathbf{w}} := \{i \in [d] : w_i \geq 0\} \quad \text{and} \quad N_{\mathbf{w}} := \{i \in [d] : w_i < 0\}$$

Let any $i \in P_{\mathbf{w}}$, the variables of $X(w_i)$ will be of the form $x_{\sigma}^{(i)}$, where σ is a binary string indexed by the set:

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

We will call these sets *positive indexing sets*. The size of each $A_{\mathbf{w}}^{(i)}$ is $|w_i|$. The number of strings in $A_{\mathbf{w}}^{(i)}$ is $2^{|w_i|}$.

For $i \in N_{\mathbf{w}}$, we similarly define the *negative indexing sets* $B_{\mathbf{w}}^{(i)}$ that will be used to index the variables of $X(w_i)$ for $i \in N_{\mathbf{w}}$.

A word $w \in \mathbb{Z}^d$ is *balanced* if:

1. $\forall i \in P_{\mathbf{w}} \exists j \in N_{\mathbf{w}}$ such that $A_{\mathbf{w}}^{(i)} \cap B_{\mathbf{w}}^{(j)} \neq \emptyset$ (i.e. $j \in N_{\mathbf{w}}$ is a *witness* that \mathbf{w} is balanced at $i \in P_{\mathbf{w}}$)
2. $\forall j \in N_{\mathbf{w}} \exists i \in P_{\mathbf{w}}$ such that $A_{\mathbf{w}}^{(i)} \cap B_{\mathbf{w}}^{(j)} \neq \emptyset$ (i.e. $i \in P_{\mathbf{w}}$ is a *witness* that \mathbf{w} is balanced at $j \in N_{\mathbf{w}}$)

For any $i \in P_{\mathbf{w}}, \sigma \in \{0, 1\}^{A_{\mathbf{w}}^{(i)}}$, define:

$$f_{\sigma}^{(i)} := \prod_{\substack{j \in N_{\mathbf{w}} \\ A_{\mathbf{w}}^{(i)} \cap B_{\mathbf{w}}^{(j)} \neq \emptyset}} \sum_{\substack{\sigma_j \in \{0, 1\}^{B_{\mathbf{w}}^{(j)}} \\ \sigma_j(k) = \sigma(k) \forall k \in A_{\mathbf{w}}^{(i)} \cap B_{\mathbf{w}}^{(j)}}} y_{\sigma_j}^{(j)} \quad (2)$$

The product ranges over each $j \in N_{\mathbf{w}}$ that witnesses the fact that \mathbf{w} is balanced at i . The sum ranges over each σ_j that is consistent with σ on $A_{\mathbf{w}}^{(i)} \cap B_{\mathbf{w}}^{(j)}$. Now, we define the knapsack polynomial as

$$\text{ks}_{\mathbf{w}} := \left(\sum_{i \in P_{\mathbf{w}}} \sum_{\sigma \in \{0, 1\}^{A_{\mathbf{w}}^{(i)}}} x_{\sigma}^{(i)} f_{\sigma}^{(i)} \right) - \beta \quad (3)$$

where $\beta \in \mathbb{F}$ is any field element such that $\text{ks}_{\mathbf{w}}$ has no Boolean roots. To make the proof work over fields of positive characteristic, we define a variant of $\text{ks}_{\mathbf{w}}$ as:

$$\text{ks}_{\mathbf{w}, \alpha} := \left(\sum_{i \in P_{\mathbf{w}}} \alpha_i \sum_{\sigma \in \{0, 1\}^{A_{\mathbf{w}}^{(i)}}} x_{\sigma}^{(i)} f_{\sigma}^{(i)} \right) - \beta \quad (4)$$

where $\alpha = (\alpha_i)_{i \in P_{\mathbf{w}}} \in \mathbb{F}^{|P_{\mathbf{w}}|}$, and β will be chosen from an extension field $\tilde{\mathbb{F}} \supset \mathbb{F}$ so that $\text{ks}_{\mathbf{w}, \alpha}$ has no Boolean roots.

For any word $\mathbf{w} \in \mathbb{Z}^d$, $M_{\mathbf{w}}(f)$ denotes the matrix with rows indexed by all monomials m that are set-multilinear over $\mathbf{w}|_{P_{\mathbf{w}}}$, and columns indexed by all monomials m' that are set-multilinear over $\mathbf{w}|_{N_{\mathbf{w}}}$. For each such pair of monomials (m, m') , the corresponding entry in $M_{\mathbf{w}}(f)$ carries the coefficient of mm' in f . To show that the set-multilinear projection of any multilinear polynomial f computing $1/\text{ks}_{\mathbf{w}}$ over $\{0, 1\}^n$ requires superpolynomially large set-multilinear constant-depth circuits, [14] shows that $M_{\mathbf{w}}(f)$ is full-rank.

► **Lemma 22** (Rank lower bound lemma (Lemma 6 [14])). *Let $\mathbf{w} \in \mathbb{Z}^d$ be a balanced word, and let f be the multilinear polynomial such that $f = \frac{1}{\text{ks}_{\mathbf{w}}}$ over $\{0, 1\}^n$. Then, $M_{\mathbf{w}}(f)$ is full-rank.*

With this lemma, the lower-bound follows via the arguments from [24]. Importantly for us, this lemma uses the degree lower bound from [13]; we describe a sketch of the same.

The use of degree lower bound in [14]

Suppose $f = \sum_m g_m(\mathbf{x})m$, where the sum runs over all multilinear monomials m in the \mathbf{y} variables, and $g_m(\mathbf{x})$ is some multilinear polynomial in the \mathbf{x} variables. They show that for any m which is set-multilinear on $\mathbf{w}|_{N_{\mathbf{w}}}$, the leading monomial of $g_m(\mathbf{x})$ is the set-multilinear monomial m' on positive variables such that $\sigma(m')$ is consistent with $\sigma(m)$ ([14] describes this formally). For each monomial m that is set-multilinear on $\mathbf{w}|_{N_{\mathbf{w}}}$, the leading monomial of $g_m(\mathbf{x})$ turns out to be a different set-multilinear monomial on the positive variables, and together, these leading monomials span the space of all set-multilinear monomials on the positive variables. This makes $M_{\mathbf{w}}(f)$ full-rank. To get a handle on $g_m(\mathbf{x})$ (for m being

a monomial on $\mathbf{w}|_{N_{\mathbf{w}}}$, consisting only of \mathbf{y} variables), [14] sets all the variables in m to 1 and all the \mathbf{y} variables outside m to 0. They call this transformation τ_m . For the proof of Lemma 22, an important requirement is that:

For every $T \subseteq N_{\mathbf{w}}$ and for every set-multilinear monomial m on $\mathbf{w}|_T$, the leading monomial of $\tau_m(f)$ is $\prod_{i \in U_T} x_{\sigma(i)}^{(i)}$, which is the product of all the variables that show up in the denominator of

$$\frac{1}{\tau_m(\text{ks}_{\mathbf{w}})} = \frac{1}{\sum_{i \in U_T} x_{\sigma(i)}^{(i)} - \beta}$$

where $U_T = \{i \in P_{\mathbf{w}} : A_{\mathbf{w}}^{(i)} \subseteq B_{\mathbf{w}}^T\}$, and for each $i \in P_{\mathbf{w}}$, $\sigma(i)$ is the unique indexing string that agrees with $\sigma(m)$ on $A_{\mathbf{w}}^{(i)}$, the i^{th} positive indexing set.

This requirement is satisfied due to the degree lower bound from [13], which requires the field to be of characteristic 0. The proof in [14] includes helpful figures and the reader is encouraged to refer to the paper.

Let us recall our variant of $\text{ks}_{\mathbf{w}}$:

$$\text{ks}_{\mathbf{w}, \alpha} := \left(\sum_{i \in P_{\mathbf{w}}} \alpha_i \sum_{\sigma \in \{0,1\}^{A_{\mathbf{w}}^{(i)}}} x_{\sigma}^{(i)} f_{\sigma_i} \right) - \beta \quad (5)$$

where $\alpha = (\alpha_i)_{i \in P_{\mathbf{w}}} \in \mathbb{F}^{|P_{\mathbf{w}}|}$. To prove Theorem 20 in positive characteristic, we use the following lemma that follows by a union bound over all $T \subseteq N_{\mathbf{w}}$ and all set-multilinear monomials on $\mathbf{w}|_T$, on top of Lemma 17.

► **Lemma 23.** *Let $d \in \mathbb{N}$ be a natural number and $\mathbf{w} \in \mathbb{Z}^d$ be a balanced word. Let $m = |P_{\mathbf{w}}|$. For any $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}^m$, $T \subseteq N_{\mathbf{w}}$ and any m_T that is a set-multilinear monomial on $\mathbf{w}|_T$, let $f_{\alpha, T, m_T}(\mathbf{x})$ be the unique multilinear polynomial that agrees with the function*

$$\tau_{m_T} \left(\frac{1}{\text{ks}_{\mathbf{w}, \alpha}} \right) = \frac{1}{\sum_{i \in U_T} \alpha_i x_{\sigma(i)}^{(i)} - \beta}$$

on the Boolean cube, where $\beta \in \mathbb{F}$ is chosen so that $\text{ks}_{\mathbf{w}, \alpha}$ has no Boolean roots, and $U_T = \{i \in P_{\mathbf{w}} : A_{\mathbf{w}}^{(i)} \subseteq B_{\mathbf{w}}^T\}$. Let $S \subseteq \mathbb{F}$ be a finite subset of the field. Let $\gamma := |N_{\mathbf{w}}| + \sum_{i \in N_{\mathbf{w}}} |w_i|$. Then, for an $\alpha \in S^m$ chosen uniformly at random:

$$\Pr_{\alpha \sim S^m} [\exists T \subseteq N_{\mathbf{w}}, m_T : \deg f_{\alpha, T, m_T}(\mathbf{x}) < |U_T|] < \frac{2^{\gamma+m}}{|S|}$$

In particular, with probability at least $1 - (2^{\gamma+m}/|S|)$ over the choice of $\alpha \in S^m$, for every choice of $T \subseteq N_{\mathbf{w}}$ and set-multilinear monomial m_T over $\mathbf{w}|_T$, the leading monomial of $f_{\alpha, T, m_T}(\mathbf{x})$ is $c \cdot \prod_{i \in U_T} x_{\sigma(i)}^{(i)}$ for some $c \in \mathbb{F} \setminus \{0\}$.

Proof. The number of $T \subseteq N_{\mathbf{w}}$ is $2^{|N_{\mathbf{w}}|}$. The number of set-multilinear monomials on $\mathbf{w}|_T$ for any $T \subseteq N_{\mathbf{w}}$ is $2^{\sum_{i \in T} |w_i|}$, which is at most $2^{\sum_{i \in N_{\mathbf{w}}} |w_i|}$. For any fixed $T \subseteq N_{\mathbf{w}}$ and m_T that is a set-multilinear monomial on $\mathbf{w}|_T$, Lemma 17 implies that for an $\alpha \in S^m$ chosen uniformly at random:

$$\Pr_{\alpha \in S^m} [\deg f_{\alpha, T, m_T}(\mathbf{x}) < |U_T|] < \frac{2^m}{|S|}$$

Applying a union bound over all $T \subseteq N_{\mathbf{w}}$ and m_T implies that for an $\alpha \in S^m$ chosen uniformly at random:

$$\Pr_{\alpha \in S^m} [\exists T \subseteq N_{\mathbf{w}}, m_T : \deg f_{\alpha, T, m_T}(\mathbf{x}) < |U_T|] < \sum_{T \subseteq N_{\mathbf{w}}, m_T} \frac{2^m}{|S|} \leq \frac{2^{\gamma+m}}{|S|}$$

◀

With this lemma, the rest of the proof of [14] works out verbatim. We state the final theorem, which is a version of Theorem 20 for finite fields of positive characteristic.

► **Theorem 24** ([14] over positive characteristic). *Let $n, \Delta \in \mathbb{N}_+$ with $\Delta \leq O(\log \log \log n)$. Let $p \in \mathbb{N}$ be any prime. Let $\tilde{\mathbb{F}}$ be a field of characteristic p and size p^{2^k} , where k is the smallest integer that satisfies $p^k > 2^{C(\log n)^2}$ for an absolute constant $C \geq 1$ ¹⁷. Let β be an arbitrary element in $\tilde{\mathbb{F}} \setminus \mathbb{F}$, where \mathbb{F} denotes the subfield of size p^k . For any $\alpha \in \mathbb{F}^{n^4}$, Let f_{α} be the multilinear polynomial such that*

$$f = \frac{1}{\sum_{i,j,k,l \in [n]} \alpha_{i,j,k,l} z_{i,j,k,l} x_i x_j x_k x_l - \beta}$$

over the Boolean cube. Then, there exists an $\alpha \in \mathbb{F}^{n^4}$ such that any circuit of product-depth Δ computing f_{α} has size at least

$$n^{(\log n)^{\exp(-O(\Delta))}}$$

The reason for $|\mathbb{F}| > 2^{\Omega((\log n)^2)}$ in Theorem 24.

When we instantiate Lemma 23 inside the proof of Theorem 24, the parameter d , which is the number of variable sets, will be $O(\log n)$, and the word $\mathbf{w} \in \mathbb{Z}^d$ will also be chosen so that for each $i \in [d]$, $|w_i| \leq O(\log n)$. Thus, $\sum_{i \in N_{\mathbf{w}}} |w_i| = O((\log n)^2)$, and the union bound in Lemma 23 will require the field to be larger than $2^{O((\log n)^2)}$.

References

- 1 M. Alekhovich and A.A. Razborov. Lower bounds for polynomial calculus: non-binomial case. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 190–199, 2001. doi:10.1109/SFCS.2001.959893.
- 2 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, pages 54–67, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3357713.3384245.
- 3 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, pages 389–402, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3519935.3520025.
- 4 Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on hilbert’s nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, s3-73(1):1–26, 1996. doi:10.1112/plms/s3-73.1.1.

¹⁷This C is a fixed constant that depends on the exact choice of parameters in the proof of [14]

- 5 C.S. Bhargav, Sagnik Dutta, and Nitin Saxena. Improved lower bound, and proof barrier, for constant depth algebraic circuits. *ACM Trans. Comput. Theory*, 16(4), November 2024. doi:10.1145/3689957.
- 6 Sam Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62(2):267–289, 2001. doi:10.1006/jcss.2000.1726.
- 7 Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiri Sgall. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Comput. Complex.*, 6(3):256–298, 1997. doi:10.1007/BF01294258.
- 8 Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 174–183, New York, NY, USA, 1996. Association for Computing Machinery. doi:10.1145/237814.237860.
- 9 Peter Clote and Evangelos Kranakis. *Boolean Functions and Computation Models*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2002. doi:10.1007/978-3-662-04943-3.
- 10 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979. doi:10.2307/2273702.
- 11 Michael A. Forbes. Low-Depth Algebraic Circuit Lower Bounds over Any Field. In Rahul Santhanam, editor, *39th Computational Complexity Conference (CCC 2024)*, volume 300 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:16, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2024.31.
- 12 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. doi:10.4230/LIPIcs.CCC.2016.33.
- 13 Michael A. Forbes, Amir Shpilka, Iddo Zameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. *Theory Comput.*, 17:1–88, 2021. doi:10.4086/TOC.2021.V017A010.
- 14 Nashlen Govindasamy, Tuomas Hakoniemi, and Iddo Zameret. Simple hard instances for low-depth algebraic proofs. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 188–199, 2022. doi:10.1109/FOCS54457.2022.00025.
- 15 D. Grigoriev. Tseitin’s tautologies and lower bounds for nullstellensatz proofs. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 648–652, 1998. doi:10.1109/SFCS.1998.743515.
- 16 Dima Grigoriev and Alexander A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 10:465–487, 2000. doi:10.1007/S002009900021.
- 17 Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6), November 2018. doi:10.1145/3230742.
- 18 Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. *Essential Coding Theory*. 2023. Available online: <https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/web-coding-book.pdf>. URL: <https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/web-coding-book.pdf>.
- 19 Tuomas Hakoniemi, Nutan Limaye, and Iddo Zameret. Functional lower bounds in algebraic proofs: Symmetry, lifting, and barriers. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, pages 1396–1404, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3618260.3649616.

- 20 Russell Impagliazzo, Pavel Pudlák, and Jirí Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Comput. Complex.*, 8(2):127–144, 1999. doi:10.1007/s000370050024.
- 21 J. Krajíček. *Proof Complexity*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019. URL: <https://books.google.dk/books?id=u0yKuQEACAAJ>.
- 22 Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, 1995. doi:10.1017/CB09780511529948.
- 23 Jan Krajíček. A reduction of proof complexity to computational complexity for $AC^0[p]$ frege systems. *Proceedings of the American Mathematical Society*, 143(11):4951–4965, 2015. URL: <http://www.jstor.org/stable/24507779>.
- 24 Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 804–814, 2021. doi:10.1109/FOCS52979.2021.00083.
- 25 Noam Nisan. Lower bounds for non-commutative computation. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, STOC '91*, pages 410–418, New York, NY, USA, 1991. Association for Computing Machinery. doi:10.1145/103418.103462.
- 26 Toniann Pitassi and Iddo Zameret. Algebraic proof complexity: progress, frontiers and challenges. *ACM SIGLOG News*, 3(3):21–43, August 2016. doi:10.1145/2984450.2984455.
- 27 Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, 56(2), April 2009. doi:10.1145/1502793.1502797.
- 28 Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical notes of the Academy of Sciences of the USSR*, 41:333–338, 1987. URL: <https://api.semanticscholar.org/CorpusID:121744639>.
- 29 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complex.*, 7(4):291–324, 1998. doi:10.1007/s000370050013.
- 30 Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. *Github survey*, 2021. URL: <https://github.com/dasarpmar/lowerbounds-survey/releases/tag/v9.0.3>.
- 31 Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complex.*, 10(1):1–27, 2001. doi:10.1007/PL00001609.
- 32 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. doi:10.1561/04000000039.
- 33 Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, 1987. URL: <https://api.semanticscholar.org/CorpusID:2214101>.
- 34 Roman Smolensky. On representations by low-degree polynomials. *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 130–138, 1993. doi:10.1109/SFCS.1993.366874.