Meta-Mathematics of Algebraic Complexity

Michal Garlík
Imperial College London, UK

Svyatolav Gryaznov
Imperial College London, UK

Jiaqi Lu
Imperial College London, UK

Rahul Santhanam
Oxford University, UK

Iddo Tzameret
Imperial College London, UK

Abstract

We initiate the study of the meta-mathematics of algebraic circuit lower bounds, aiming both to gain insight into the methods sufficient and necessary to prove algebraic circuit lower bounds, and to contribute to the study of bounded arithmetic as a logical foundation for complexity lower bounds. We demonstrate that while algebraic circuit lower bounds are hard for somewhat weak proof systems such as polynomial calculus resolution (PCR), contemporary lower bounds are efficiently provable in proof systems and bounded arithmetic theories corresponding to NC^2, such as VNC^2 and the corresponding class of propositional Frege proofs of quasipolynomial-size. Moreover, going below VNC^2 into algebraic constant-depth reasoning is likely insufficient to efficiently prove already constant-depth algebraic circuit lower bounds. Specifically, we show the following.

NC^2-reasoning and rank method. Algebraic circuit lower bounds are often proved via the "rank method", with recent prominent applications including the constant-depth lower bounds of Limaye, Srinivasan and Tavenas [27] and Forbes [10]. We show that these rank-based arguments can be formalized in the bounded arithmetic theory VNC^2, which captures reasoning with NC^2 concepts. This complements the work of Tzameret and Cook [47], who formalized structural *upper* bounds in this theory, and provides a unified framework for studying barriers to current algebraic complexity methods, complementing barriers studied by Efremenko, Garg, Makam, Oliveira, and Wigderson [9, 13].

Sparsity algebraic reasoning. We show that Polynomial Calculus Resolution (PCR) cannot efficiently prove superpolynomial algebraic circuit lower bounds for any family of polynomials. Moreover, PCR cannot efficiently prove exponential constant-depth circuit lower bounds for any family of polynomials.

Constant-depth algebraic reasoning. We introduce the Tensor Rank Principle and demonstrate it is hard for PCR. We show that if this principle is hard against constant-depth Ideal Proof System (IPS) then constant-depth IPS cannot efficiently prove constant-depth algebraic circuit lower bounds.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Complexity theory and logic; Theory of computation → Proof theory; Theory of computation → Proof complexity; Theory of computation → Circuit complexity

Keywords and phrases Complexity lower bounds, Bounded arithmetic, Feasible constructive mathematics, Algebraic complexity, Proof complexity, Meta-complexity, Algebraic circuit lower bounds, Polynomial Calculus Resolution, Barriers

Digital Object Identifier 10.4230/LIPIcs.LICS.2026.49

Funding *Michal Garlík*: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 101002742, *EPRICOT* project).

Svyatolav Gryaznov: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 101002742, *EPRICOT* project).
Jiaqi Lu: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 101002742, *EPRICOT* project). It was also supported by the Engineering and Physical Sciences Research Council (EPSRC) under grant EP/Z534158/1.
Rahul Santhanam: This project was partly funded by the EPSRC grant EP/Z534158/1.
Iddo Tzameret: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 101002742, *EPRICOT* project). It was also supported by the Engineering and Physical Sciences Research Council (EPSRC) under grant EP/Z534158/1.

Acknowledgements We are indebted to the anonymous reviewers of this paper for many important comments.

1 Introduction

The meta-mathematics of computational complexity asks questions about the nature and limits of efficient computation, with a central focus on *provability*: which proof systems or axiom systems are necessary or sufficient to establish hardness results, such as circuit-size lower bounds and complexity-class separations.

Beyond the formal provability of complexity lower bounds, one can also take a somewhat less formal approach by asking which "proof methods" can yield lower bounds, rather than in which formal proof system a given lower bound is provable. We call this direction *the barriers approach*, in contrast to the *meta-mathematical approach*.

In the *Boolean* setting, there has been extensive work on the barriers approach: developing tools for analysing which methods can yield strong Boolean circuit-size lower bounds, and which are ruled out by general obstacles. Classic examples include the *relativization* barrier [3] and the *natural proofs* barrier [43], both of which rule out broad families of standard approaches to proving superpolynomial lower bounds for NP.

These barriers have been highly instructive and influential, as they rule out large classes of lower-bound attempts. However, they can sometimes have an ad-hoc flavour, in that it is not always unambiguous whether a given lower-bound argument falls within their scope. For example, it is unclear what the relativization barrier says about low-depth circuit classes; similarly, in the natural proofs framework it can be difficult to identify the underlying "natural property", and to separate this identification from the task of proving that an explicit hard function satisfies the property.

In contrast, the meta-mathematical approach to complexity lower bounds goes through *formal logic* and specifically proof theory and independence results (namely, results showing that a theorem, and its negation, cannot be proved in a given formal theory of mathematics). One advantage of this approach is that barrier results that are formalised as logical independence results are more robust since they are closed under basic logical operations. For example, the natural-proofs barrier implies that there are no natural proofs of certain strong lower bounds. However, this does not exclude the following possibility: there is a natural proof of a statement A, and from A one can derive, by a non-natural argument, a strong lower bound B. Thus the barrier does not rule out proving B in this way. Hence, a natural argument could be helpful in proving lower bounds despite the barrier, as long it is only part of the proof. By contrast, logical barriers are formulated inside a fixed theory or

proof system, and therefore rule out not only direct proofs of B, but also proofs that derive B through intermediate statements such as A, provided that the implication $A \to B$ is itself provable in the theory.

When thinking of formal theories of interest in computational complexity theory, the natural choice is *Bounded Arithmetic* theories, which are weak fragments of Peano Arithmetic with their axioms and definable functions usually restricted to a prescribed complexity class. Razborov [36, 37] initiated a general investigation of the provability of Boolean circuit lower bounds in bounded arithmetic and propositional proof complexity, and proved strong unconditional limitations for restricted proof systems (e.g., the absence of efficient small-width DNF Resolution proofs of *any* superpolynomial Boolean circuit lower bound [41]; see also [39, 33] for preceding PC degree and resolution size lower bounds, respectively). More recent development in this direction appear in [26, 7, 32].

A central conjectural framework in this direction is due to Krajíček and Razborov [24, 38, 42]:[1]

Krajíček–Razborov Conjecture: Extended Frege cannot prove in polynomial size *any* superpolynomial Boolean circuit lower bound (for any Boolean function).

Similar to the development described above, the study of barriers against proving *algebraic* circuit lower bounds was also considered in the past, though it remains less developed than its Boolean counterpart. Two prominent frameworks for barriers have emerged. The *algebraic natural proofs* framework by Forbes, Shpilka and Volk, and independently Grochow, Kumar, Saks and Saraf [12, 15] develops algebraic analogues of natural properties. It is known that many[2] currently established algebraic lower bounds naturalise in this sense [12]. However, despite interesting recent work [6, 25] it remains open whether there is a compelling algebraic hardness assumption ruling out algebraic natural proofs against general algebraic circuits,[3] analogous to the cryptographic evidence that natural properties against general Boolean circuits do not exist [43]. A different line of work studies barriers for *rank-based* approaches by Efremenko, Garg, Oliveira, and Wigderson [9] and Garg, Makam, Oliveira, and Wigderson [13]. These works describe the limitations of techniques that proceed specifically by analysing matrix or tensor rank. The limitations shown in this direction are *unconditional*, and apply to a broad class of techniques. On the other hand these barriers apply only to tensor rank.

While barriers in algebraic circuit complexity have been investigated, its formal meta-mathematics remains unexplored, and in this work we initiate such a general study of "frontier" algebraic circuit lower bounds. The guiding question is:

[1] Razborov conjectured in [41] that Frege cannot efficiently prove superpolynomial circuit lower bounds for any Boolean function. More specifically, [41, Conjecture 1] with suitable parameters for the underlying combinatorial designs implies under some hardness assumptions that Frege cannot efficiently prove that $\mathsf{SAT} \notin \mathsf{P/poly}$. Further conjectures about the impossibility of *Extended* Frege to efficiently prove circuit lower bounds have been circulated in the proof complexity literature and discussions (cf. [34, 35, 23]).

[2] One example of an algebraic circuit lower bound technique that is not natural in the sense of algebraic natural proofs is the substitution method (see [5, Chapter 6]). Another is any lower bound technique that applies to tensor rank, but not border rank, since natural proofs necessarily prove lower bounds on border complexity. We thank the anonymous reviewer for pointing this out.

[3] The non-existence of algebraic natural properties against general algebraic circuits follows from the existence of *succinct* hitting set generators against algebraic circuits, but this is not an overly standard algebraic hardness assumption in any sense, and indeed is easily seen to be equivalent to the non-existence of natural properties.

What is the proof-theoretic (or propositional proof-complexity) strength needed to formalize and prove frontier lower bounds in algebraic complexity?

A natural test case is the family of rank-based lower bounds for constant-depth algebraic circuits computing the Permanent over finite fields, proved by Limaye–Srinivasan–Tavenas and extended by Forbes [27, 10]. These results are among the strongest unconditional lower bounds currently known for algebraic circuits, and their proofs use a robust and conceptually clean method (relative rank and set-multilinearization), making them particularly suitable for our analysis.

1.1 The rank method and constant-depth algebraic lower bounds

Following the terminology of Garg *et al.* [13, Definition 1.8], the essential feature of the rank method (which [13] calls "matrix-rank method" to distinguish it from objects of higher-order than matrices, e.g., tensors) is the use of a linear map $\phi\colon V \to \mathrm{Mat}_{p,q}$ and the associated subadditive measure $f \mapsto \mathrm{rank}(\phi(f))$. In the circuit lower-bound setting, such a measure yields a lower bound once it is shown to be small for every polynomial computed by small circuits in the model under consideration, and large for the target polynomial.

In particular, the arguments in Limaye, Srinivasan and Tavenas, and Forbes [27, 10] proceed by associating to a polynomial f a "relative rank" measure (defined with respect to an appropriate partition of variables and a set-multilinear structure), and then proving two complementary statements: (i) the Permanent has large relative rank, and (ii) every polynomial computed by a small constant-depth algebraic circuit has small relative rank. The second part requires turning a circuit into an explicit representation of the relevant coefficient vector (after suitable multilinearization), and then bounding the rank of this vector by structural properties of low-depth circuits.

From a proof-theoretic viewpoint, this raises concrete formalization tasks: one must define the rank measure inside a weak theory, prove its basic properties, and formalize the circuit-to-coefficient-vector transformation (together with the bounds needed in the rank argument). A priori, it is not obvious how much uniform reasoning is required, because the argument mixes algebraic manipulations, combinatorial counting bounds, and circuit-structured constructions.

1.2 Our results

In this work we study the efficient provability of algebraic circuit lower bounds. We consider this question in propositional and algebraic proof systems, as well as in bounded arithmetic. The latter are first-order theories that correspond to certain computational complexity classes and serve as a uniform counterpart for propositional proof systems (see [8, 22]). We discuss the consequences of our work in Section 1.4.

Summary of results

We shall demonstrate that while algebraic circuit lower bounds are hard for somewhat weak proof systems such as polynomial calculus resolution PCR they are provable (efficiently) in proof systems and theories corresponding to NC^2, such as the bounded arithmetic theory VNC^2 and the corresponding propositional proof system NC^2-Frege. We then show that "algebraic constant-depth" reasoning is plausibly insufficient to efficiently prove constant-depth algebraic circuit lower bounds. More precisely, we show that if a property of tensor rank is hard for algebraic proofs operating with constant-depth circuits (formally, constant-depth IPS), then so are constant-depth algebraic circuit lower bounds.

Table 1 Three proof-theoretic levels and the status of (constant-depth) algebraic circuit lower bounds.

Reasoning power	**What it can (efficiently) prove**	**What it cannot efficiently prove**
PCR	(Only limited algebraic reasoning.)	Algebraic circuit lower bounds are hard for PCR.
Constant-depth reasoning (polynomial-size constant-depth IPS)	(Constant-depth algebraic reasoning.)	Plausibly insufficient for constant-depth algebraic circuit lower bounds: conditionally, constant-depth algebraic circuit lower bounds are hard for constant-depth IPS.
NC^2 **reasoning** (VNC^2 and polynomial-size NC^2-Frege, equivalently quasipolynomial-size Frege proofs)	Constant-depth algebraic circuit lower bounds (e.g., rank-based lower bounds for Permanent over finite fields) admit efficient proofs; formalizable in VNC^2 and hence have polynomial-size NC^2-Frege proofs	(No lower-bound limitation shown here.)

This picture – depicted in Table 1 – aligns with the working assumption that rank arguments, and rank-based lower bounds specifically, sit proof-theoretically (or proof complexity-wise) in reasoning systems that operate with concepts in NC^2 (or more precisely, the complexity class DET, that is the AC^0-closure of the integer determinant; see [47] for a discussion and references).

1.2.1 VNC^2 and NC^2-Frege suffice

Our first contribution is to show that the entire rank-based lower bound argument against constant-depth algebraic circuits of Limaye *et al.* and Forbes [27, 10] can be carried out in the bounded arithmetic theory VNC^2. Using the standard translation between bounded arithmetic and propositional proofs (see, e.g., Cook–Nguyen [8]), we obtain the corresponding propositional upper bound.

▶ **Theorem 1** (Informal; Theorem 29 and Theorem 30)**.** *There are polynomial-size propositional* NC^2*-Frege proofs of the superpolynomial lower bound for the Permanent polynomial against constant-depth algebraic circuits over finite fields. Moreover, this lower bound is provable in the theory* VNC^2*.*

To establish this, we provide VNC^2-formal definitions and proofs for the key components of the rank-method framework in the parameter regime used by [27, 10]. In particular, we formalize:

- the definition of the relevant relative-rank measure and its basic algebraic properties;
- the fact that the specific "word polynomials" used in the argument have high rank;
- a uniform procedure that, given a constant-depth algebraic circuit of bounded syntactic-degree, computes the corresponding coefficient vector needed for the rank analysis;
- the set-multilinearization step in [10]: every constant-depth circuit can be converted into a set-multilinear circuit with depth preserved linearly with a moderate size blow-up;
- the final rank upper bound for constant-depth set-multlinear circuits, which implies a circuit size lower bound for the specific "word polynomials".

Conceptually, the theorem supports the informal correspondence between rank-based lower bounds and NC^2-level reasoning: the proof of [27, 10] does not require the strength of powerful systems such as Extended Frege.

Theorem 1 gives an upper bound for the proof complexity of the circuit lower bounds shown in [27, 10]. We believe that the upper bound is close to being tight (with respect to the proof system), which is consistent with the constant-depth algebraic analogues of the Krajíček–Razborov conjecture.

Proof overview for Theorem 1

We shall work with *first-order* theories of bounded arithmetic, which are translatable to polynomial-size propositional proofs. Specifically, we work with the theory VNC^2 as developed in Cook and Nguyen [8] and used in Tzameret and Cook [47] to formalize basic linear algebra in a seemingly minimal theory. Any formula of low logical complexity (formally, $\forall\Sigma^B_0$-formulas) that has a proof in VNC^2 translates naturally (by instantiating the universal variables in it by constants) to a family of propositional tautologies with polynomial-size propositional proofs in NC^2-Frege.

The formalization of the lower bound proceeds along the lines of [27] (which works over large characteristic), except where we use Forbes' idea for finite fields [10]. Specifically, this means that we use a direct set-multilinearization step using the Binet–Minc [29] identities. We note that for simplicity of presentation, the upper bound in NC^2-Frege we demonstrate is not precisely for $\mathsf{AlgCircuit}(\mathrm{perm}_n, s, \ell, \Delta))$ as is used in Theorem 2, but a slightly different formulation (though it can be made to match precisely our original propositional formula).

There are three main challenges in the formalization of the lower bounds in the theory, as follows.

Irrational numbers. We need to encode and reason about irrational numbers and functions on reals, such as exp and ln, as in [27], while the theory cannot do this directly. However, Jeřábek [20] has formalized these functions in the theory VTC^0 which is contained in VNC^2. Moreover, Jeřábek proved that VTC^0 can prove some properties about these functions, such as $\exp(z+w) = \exp(z)\exp(w)$ and $\exp(\log z) = z$, which is enough for our formalization.

Diophantine approximation. We need to use the following Diophantine approximation used in [27]: for $a, b \in Z$, $|a\alpha - b| \geq \frac{1}{4|a\alpha|+2}$, where $\alpha = 1/\sqrt{2}$. We show that to use the Diophantine approximation it is sufficient to prove the following statement in the theory: $x^2 = 2 \implies ax \neq b.$, which in itself expresses that x is irrational. This statement can be proved in the theory using the fact that the greatest common divisor of a and b is definable in VNC^2 using the number maximization axiom [17].

Properties of relative rank. The lower bound in [27] is a rank argument and hence uses several properties of matrix rank. Mulmuley [31] showed how to compute the rank of a matrix by using the determinant. Following [47] work on linear algebra in VNC^2, Ken and Koruda [21] used Mulmuley's algorithm to define in the theory the rank function. Using their rank function, the required properties of the rank function can be proved in VNC^2.

1.2.2 Polynomial Calculus Resolution lower bounds

We study the hardness of the statements $\mathsf{AlgCircuit}(f, s, \ell)$ stating that a polynomial f has an algebraic circuit of size s and syntactic-degree ℓ. We also study analogous statements $\mathsf{AlgCircuit}(f, s, \ell, \Delta)$, where the circuits are restricted to depth Δ. Similar formulas were considered for Boolean circuits [39, 33, 40, 24, 41, 14, 2] in the case of Resolution, Polynomial Calculus, Polynomial Calculus Resolution and Sum-of-Squares.

We define $\mathsf{AlgCircuit}(f, s, \ell)$ in a similar fashion to the lower bound statement from Razborov [41]. We prove its hardness against PCR over the two-element field by reducing (the negation of) the *rank principle* to $\mathsf{AlgCircuit}(f, s, \ell)$. Informally, the (weak) rank principle states that an $m \times m$ matrix A cannot be represented as a product of an $m \times n$ matrix and an $n \times m$ matrix when $m > n$ and the rank of A exceeds n. Garlík, Gryaznov, Ren and Tzameret [14] studied the complexity of different encodings of the rank principle, including its *iterated* variant, which is the variant we use in the reduction. This allows us to show that PCR cannot efficiently prove lower bounds on the algebraic circuit complexity of an n-variable polynomial f when $s \geq (\ell n)^{\Omega(1)}$.

Below we use $\mathsf{PCR}_{\mathbb{F}_2}$ to denote PCR refutations over $\mathbb{F}_2$.

▶ **Theorem 2** (PCR cannot efficiently prove algebraic circuit lower bounds; Theorem 20)**.** *There exists a constant $c > 0$ such that given any polynomial f of degree at most ℓ over $\mathbb{F}_2$ in n variables and $s \geq (\ell n)^c$, any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{AlgCircuit}(f, s, \ell)$ requires superpolynomially many monomials.*

This establishes a weaker version of an algebraic analogue of the Krajíček–Razborov conjecture by showing that there are no polynomial-size PCR proofs of superpolynomial algebraic circuit lower bounds for f, for *any* polynomial f.

As far as we are aware, Theorem 2 is the first result showing unconditional hardness of proving an algebraic circuit lower bound.

Constant-depth algebraic circuits form a strictly weaker computational model than general algebraic circuits. Consequently, establishing lower bounds against constant-depth algebraic circuits [27, 10] is expected to be easier than proving lower bounds against general algebraic circuits. It follows that proving proof-complexity lower bounds for formulas expressing lower bounds against constant-depth algebraic circuits is *stronger* than proving proof-complexity lower bounds for formulas expressing lower bounds against general algebraic circuits. By reducing to the rank principle, we obtain a superpolynomial lower bound for exponential constant-depth algebraic circuit lower-bound formulas against PCR:

▶ **Theorem 3** (PCR cannot efficiently prove exponential constant-depth algebraic circuit lower bounds;Theorem 21)**.** *For every constant $c > 0$, given a polynomial f of degree at most ℓ over $\mathbb{F}_2$ in n variables and $s \geq N^{1/c}$, where N is the number of monomials in n variables of degree at most ℓ, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{AlgCircuit}(f, s, \ell, O(c))$ requires superpolynomially many monomials.*

1.2.3 Conditional constant-depth IPS lower bounds

While in the previous section we discussed the relatively weak PCR proof system, here we shall deal with a stronger system: the Ideal Proof System (IPS) introduced by Grochow and Pitassi [16], and specifically its constant-depth fragment. Intuitively, one should think about it roughly as an algebraic proof system similar in strength to polynomial calculus in which each proof-line is written as an algebraic constant-depth circuit, instead of as a sum of monomial (like in PCR). Alternatively, one can consider constant-depth IPS over a finite constant field as constant Frege with counting gates modulo p (augmented with the ability to freely prove [arithmetized] polynomial identities).

We consider the generalization of the rank principle (see above), called the *tensor rank principle*, denoted $\mathsf{TRankP}_n^m(r, A)$. It states that an r-tensor $A \in \mathbb{F}^{m \times \cdots \times m}$ does not admit a tensor rank decomposition of some small rank n. When $r = 2$, this principle coincides with the rank principle. We show a conditional superpolynomial lower bound on $\mathsf{AlgCircuit}(f, s, \ell, \Delta)$ against Δ'-IPS (IPS refutations where the depth of refutation certificates is bounded by Δ'). This is done by reducing $\mathsf{AlgCircuit}(f, s, \ell, \Delta)$ to the tensor rank principle based on ideas from Raz [33].

▶ **Theorem 4** (Constant-depth IPS cannot efficiently prove constant-depth algebraic circuit lower bounds conditionally; See Theorem 26 and Corollary 27)**.** *Suppose that* $\mathsf{TRankP}_n^m(r, A)$ *requires* Δ'-IPS *refutations of size* $2^{n^{\Omega(1)}}$*. Then* $\mathsf{AlgCircuit}(f, s, \ell, \Delta)$ *requires* $(\Delta' - 5)$-IPS *refutations of superpolynomial size.*

Tensor rank lower bounds are notoriously difficult to prove, and even basic mathematical questions about tensor rank remain poorly understood. Since tensors have been studied in mathematics for much longer than algebraic circuits, there is arguably stronger empirical evidence for the difficulty of proving tensor rank lower bounds than for the difficulty of proving algebraic circuit lower bounds. Thus, grounding the formal difficulty of reasoning about algebraic circuits in the difficulty of reasoning about tensors seems to provide meaningful evidence for the hardness of proving algebraic circuit lower bounds (this was pointed out by the anonymous reviewer).

To complement our lower bounds, we show an unconditional lower bound on the tensor rank formula $\mathsf{TRankP}_n^m(r, A)$ against $\mathsf{PCR}_{\mathbb{F}_2}$. This is achieved using a random restriction argument combined with a degree-reduction to the pigeonhole principle.

▶ **Theorem 5** (Theorem 25)**.** *Assume* m, n, r *to be positive integers with* $m > n$*. Let* $J \subseteq [m]$ *with* $|J| > n$ *and let* A *be the* r*-tensor defined as*

$$A_{i_1,\ldots,i_r} = \begin{cases} 1 & \text{if } i_1 = \cdots i_r \in J, \\ 0 & \text{otherwise.} \end{cases}$$

Then any $\mathsf{PCR}_{\mathbb{F}_2}$ *refutation of* $\mathsf{TRankP}_n^m(r, A)$ *requires* $2^{\Omega(n)}$ *monomials.*

1.3 Relation to other work

Santhanam and Tzameret [44], and later Lu *et al.* [28], investigated the proof complexity of statements asserting algebraic circuit lower bounds. However, these works did not directly study the hardness of the algebraic circuit lower-bound statements themselves. Instead, they considered a more meta-level question: whether one can prove lower bounds for the *statement* that there are no short proofs of algebraic circuit lower bounds. This meta-level lower bound was then used as an ingredient in a diagonalization argument.

Garlík, Gryaznov, Ren and Tzameret [14] studied two related questions. In the first, they established a $\mathsf{PCR}_{\mathbb{F}_2}$ lower bounds for noncommutative algebraic branching program (ncABP) lower bound statements. The model of ncABP is quite a weak model of computation, and further the result is specialized in the sense that the rank principle is intimately connected to the way ncABP are encoded. The second related question was the introduction of bounded arithmetic theories augmented with the rank principle as an axiom. They showed that *Boolean* complexity lower bounds such as Smolensky-Razborov [46] lower bounds against constant-depth Boolean circuits with mod p gates can be formalized in theories corresponding to $\mathsf{AC}^0[p]$-reasoning augmented with the weak rank principle. These theories seems prima facie close to the theory VNC^2 we use in this work.

Müller and Pich [30] and others showed that Extended Frege (which corresponds to a proof system operating with polynomial-size circuits) can prove known Boolean circuit lower bounds. Our results are analogous to theirs, as we show that NC^2-Frege, i.e., proofs operating with NC^2 circuits can prove known algebraic circuit lower bounds (where the class NC^2 corresponds to polynomial-size algebraic circuits, due to known depth reductions; i.e., a polynomial-size algebraic circuit computing a polynomial of polynomial degree, can be converted to a $\log^2(n)$ depth circuits of $\mathrm{poly}(n)$ size, for n the number of variables).

1.4 Discussion and conclusions

We conclude the introduction by explaining what our results suggest from the perspectives of algebraic and proof complexity.

First, from the perspective of algebraic complexity, our results show that known techniques, including frontier constant-depth algebraic circuit lower bounds such as those of Limaye, Srinivasan and Tavenas [27], can be formalised in a relatively weak theory corresponding to NC^2 reasoning, namely VNC^2. This should be contrasted with stronger bounded arithmetic theories, such as PV and S^1_2, which correspond to polynomial-time reasoning.

Thus, under an algebraic analogue of the Krajíček–Razborov conjecture, our results suggest a possible limitation of current methods. Suppose the algebraic analogue of Krajíček–Razborov conjecture holds, namely, VNC^2 reasoning cannot prove algebraic circuit lower bounds for NC^2 circuits, and hence, by depth reduction, for VP. Since we show that the present rank-based constant-depth lower bounds are provable already in VNC^2, any proof of substantially stronger algebraic circuit lower bounds would have to use ideas that are stronger, at least in their logical strength, than the concepts currently used in these arguments. In this sense, VNC^2 can prove the known constant-depth lower bounds, but, under the algebraic analogue of the Krajíček–Razborov conjecture, it should not be able to prove general algebraic circuit lower bounds.

Second, from the perspective of proof complexity, our results contribute to three objectives:

- We provide new hard instances for proof systems of interest, in the tradition of proof complexity lower bounds. In our case these are instances that are meta-mathematical statements by themselves (cf. Razborov and Raz [39, 33]). This can help to establish further new proof complexity lower bounds.
- Our instances are connected to the diagonalisation-based approach to proof complexity lower bounds. In the works of Santhanam and Tzameret [44] and Lu, Santhanam and Tzameret [28], strong proof complexity lower bounds were obtained for CNF formulas expressing the hardness of proving algebraic circuit lower bounds. A caveat in this approach is that it is not known, unconditionally, whether these CNF formulas are unsatisfiable. The present work identifies a condition under which such formulas are unsatisfiable: namely, the hardness of proving algebraic circuit lower bounds in constant-depth IPS. Combined with [28], this condition would imply lower bounds for $\mathsf{AC}^0[p]$-Frege, a longstanding open problem in proof complexity.
- Unprovability of lower bounds is a major effort in proof complexity, which helps to relate the strength of efficient computation and efficient provability, motivated by the goal to understand different proof systems and bounded arithmetic theories.

2 Preliminaries

To fix notation, we define Boolean circuits with fan-in two gates $\wedge, \vee$ and fan-in one gates $\neg$: for every $n \in \mathbb{N}$, an n-input, single-output Boolean circuit is a directed acyclic graph with n sources (vertices with no incoming edges) and one sink (a vertex with no outgoing edges). All non-source vertices are called gates or nodes and are labelled with one of $\wedge$, $\vee$ or $\neg$ (i.e., the logical operations OR, AND, and NOT). The vertices labelled with $\wedge$ and $\vee$ have fan-in (i.e., number of incoming edges) equal to 2, and the vertices labelled with $\neg$ have fan-in 1. The size of C, denoted by $|C|$, is the number of vertices in it. If C is a Boolean circuit and $x \in \{0,1\}^n$ is some input, then the output of C on x is denoted by $C(x)$.

2.1 Algebraic complexity

For standard definitions in algebraic complexity, we refer the reader to [45]. Let $\mathbb{F}$ be a field. Denote by $\mathbb{F}[\overline{x}]$ the ring of polynomials with coefficients from $\mathbb{F}$ and variables $\overline{x} = (x_1, \ldots, x_n)$. A polynomial is a formal linear combination of monomials, where a monomial is a product of variables. Two polynomials are identical if all their monomials have the same coefficients. The degree of a polynomial is the maximum total degree of a monomial in it.

▶ **Definition 6** (VAC^0). *Over a field $\mathbb{F}$, $\mathsf{VAC}^0_{\mathbb{F}}$ is the class of families $f = (f_n)_{n=1}^{\infty}$ of polynomials f_n such that f_n has $\mathrm{poly}(n)$ input variables, is of $\mathrm{poly}(n)$ degree, and can be computed by algebraic circuits over $\mathbb{F}$ of $\mathrm{poly}(n)$ size and depth $O(1)$.*

Notice that all VP,VNP and VAC^0 are non-uniform complexity classes.

▶ **Theorem 7** (Superpolynomial lower bounds against constant-depth circuits over a field with large characteristic [27]). *Assume $d \leq \frac{\log n}{100}$ and the characteristic of $\mathbb{F}$ is 0 or greater than d. For any product-depth $\Delta \geq 1$, any algebraic circuit C computing $\mathrm{IMM}_{n,d}$ of product-depth at most Δ must have size at least $n^{d^{\varepsilon}}$ where ε is $\exp(-O(\Delta))$.*

A recent result by Forbes [10] extended this result to *any* field, including finite fields. Lower bounds in [27] have been improved in [4], which has also been extended to any field by Forbes [10]. However, in this paper, we will focus on formalising proofs in [27] and [10].

▶ **Corollary 8** (Superpolynomial lower bounds on constant-depth circuits over any field [10]). *The lower bound of Theorem 7 holds over any field.*

Since $\mathrm{IMM}_{n,d}$ is a p-projection of the Permanent polynomial with $\mathrm{poly}(n,d)$ many variables, it follows that the Permanent does not have constant-depth polynomial-size circuits over any field, in the following sense. Recall that a *symbolic $n \times n$ matrix* is the $n \times n$ matrix with n^2 distinct indeterminates x_{ij}, for $i, j \in [n]$.

▶ **Theorem 9** (No polynomial-size constant depth circuits for the Permanent). *Let $\Delta \geq 1$ and let $\mathbb{F}$ be a field. There are no constants c_1, c_2, such that the Permanent polynomial $\mathrm{perm}(A)$ of the $n \times n$ symbolic matrix A over the field $\mathbb{F}$ is computable by an algebraic circuit of size $c_1 n^{c_2}$ and depth Δ where Δ is independent of n, for sufficiently large n.*

2.1.1 Encoding of algebraic circuit upper bound formulas

▶ **Definition 10** (Algebraic circuit upper bound formula). *Let $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ be a polynomial in n variables and with degree at most ℓ. The following set of polynomial equations $\mathsf{AUB}(f, s, \ell)$ (in the $\overline{w}$-variables only) expresses that the polynomial $f(\overline{x})$ can be computed by an algebraic circuit of size s:*

$$\left\{ \mathrm{coeff}_{M_i}(\widehat{U}(\overline{x}, \overline{w})) = b_i : 1 \leq i \leq N \right\},$$

where $\overline{b} = \mathrm{coeff}(f(\overline{x})) \in \mathbb{F}^N$ *is the coefficient vector of the polynomial* f *of dimension* N*,* $U(\overline{x}, \overline{w})$ *is the universal circuit for polynomials of degree at most* ℓ *and circuit size at most* s*,* $\overline{w}$ *are the* $K_{s,\ell}$ *edge variables,* $\{M_i\}_{i=1}^N$ *is the set of all possible* $\overline{x}$*-monomials of degree at most* ℓ*, and* $N = \Sigma_{j=0}^{\ell}\binom{n+j-1}{j} = 2^{O(n+\ell)}$ *is the number of monomials of total degree at most* ℓ *over* n *variables. Then, the size of the above set of polynomial equations is* $O(7^\ell \cdot s \cdot N)$*.*

▶ **Definition 11** (Bounded-depth algebraic circuit upper bound formula)**.** *Let* $f(\overline{x}) \in \mathbb{F}[\overline{x}]$ *be a polynomial with* n*-variables and degree at most* ℓ*. The following set of polynomial equations* $\mathsf{AUB}(f, s, \ell, \Delta)$ *(in the* $\overline{w}$*-variables only) expresses that the polynomial* $f(\overline{x})$ *can be computed by an algebraic circuit of size* s *and depth* Δ*:*

$$\left\{\mathrm{coeff}_{M_i}(\widehat{U}(\overline{x}, \overline{w})) = b_i : 1 \leq i \leq N\right\},$$

where $\overline{b} = \mathrm{coeff}(f(\overline{x})) \in \mathbb{F}^N$ *is the coefficient vector of the polynomial* f *of dimension* N*,* $U(\overline{x}, \overline{w})$ *is the bounded-depth universal circuit for polynomials of depth at most* Δ *and have circuits of size at most* s*,* $\overline{w}$ *are the* $K_{s,\Delta}$ *edge variables,* $\{M_i\}_{i=1}^N$ *is the set of all possible* $\overline{x}$*-monomials of degree at most* ℓ*, and* $N = \Sigma_{j=0}^{\ell}\binom{n+j-1}{j} = 2^{O(n+\ell)}$ *is the number of monomials of total degree at most* ℓ *over* n *variables. Then, the size of the above set of polynomial equations is* $O(2^{(t+\ell)\ell} \cdot \mathrm{poly}(s) \cdot N)$ *where* t *is the maximum multiplication fan-in in* $U(\overline{x}, \overline{w})$*.*

2.2 Proof complexity

▶ **Definition 12** (Polynomial Calculus with Resolution [1])**.** *Let* $\mathbb{F}$ *be a field.* Polynomial Calculus Resolution over $\mathbb{F}$ ($\mathsf{PCR}_\mathbb{F}$) *is a proof system whose lines are polynomials from* $\mathbb{F}[x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}]$*, where* $\overline{x_1}, \ldots, \overline{x_n}$ *are treated as new formal variables.* PCR *has Boolean axioms for all variables (including those that involve the variables* $\overline{x_i}$*) together with the additional axioms* $x_i + \overline{x_i} = 1 : i \in [n]$*. Each line is either an axiom or is derived from the previous lines using the following inference rules:*

$$\frac{f \qquad g}{\alpha f + \beta g} \quad \text{and} \quad \frac{f}{x \cdot f},$$

where $\alpha, \beta \in \mathbb{F}$ *are any scalars and* x *is a variable.*

For a clause C*, denote by* Γ_C *the monomial*

$$\Gamma_C \coloneqq \prod_{\overline{x} \in C} x \cdot \prod_{x \in C} \overline{x}$$

and for a CNF τ*, let* $\Gamma_\tau \coloneqq \{\Gamma_C : C \in \tau\}$*. Note that* τ *is unsatisfiable if and only if the polynomials* Γ_τ *have no common root in* $\{0,1\}^n$*. A* PCR refutation *of a CNF* τ *is a* PCR *proof of the contradiction* $1 = 0$ *from* Γ_τ*.*

The degree *of a* PCR *proof is defined as the maximum degree of a polynomial appearing in it, and its* size *is the number of different* monomials *in this proof.*

PC and PCR are equivalent with respect to the degree measure (via the affine transformation $\overline{x} \mapsto 1 - x$).

It is convenient to factorize all polynomials appearing in PCR proofs over the ideal generated by the Boolean axioms. This makes the proof lines multilinear and the resulting size and degree can only decrease.

We shall also use the system NC^2-Frege, which is an inference-based propositional proof system operating with NC^2-circuits. An NC^2-circuit is a depth-$O(\log^2 n)$ circuit, with n the number of input variables, and fan-in two, in the De Morgan language. We refer the reader to [18] for a formal definition of this system.

Ideal Proof Systems

Given $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ over some field $\mathbb{F}$, Hilbert's Nullstellensatz shows that the polynomial system $f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0$ is unsatisfiable (over the algebraic closure of $\mathbb{F}$) if and only if there are polynomials $g_1, \ldots, g_m \in \mathbb{F}[\overline{x}]$ such that $\sum_{j=1}^{m} g_j(\overline{x}) f_j(\overline{x}) = 1$ (as a formal identity), or equivalently, that 1 is in the ideal generated by $\{f_j\}_{j=1}^{m}$ (we use the notation from [11]).

▶ **Definition 13** ((Boolean) Ideal Proof System (IPS) [16]). *Let $f_1(\overline{x}), \ldots, f_m(\overline{x}), p(\overline{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ be a collection of polynomials. An* IPS *proof of $p(\overline{x}) = 0$ from $\{f_j(\overline{x})\}_{j=1}^{m}$, showing that $p(\overline{x}) = 0$ is semantically implied from the assumptions $\{f_j(\overline{x}) = 0\}_{j=1}^{m}$ over* 0-1 *assignments, is an algebraic circuit*

$$C(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{F}[\overline{x}, y_1, \ldots, y_m, z_1, \ldots, z_n],$$

such that (the equalities in what follows stand for formal polynomial identities[4]*)*

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

The size of the IPS *proof is the size of the circuit C. The variables $\overline{y}, \overline{z}$ are sometimes called the* placeholder variables *since they are used as placeholders for the axioms. An* IPS *proof $C(\overline{x}, \overline{y}, \overline{z})$ of $1 = 0$ from $\{f_j(\overline{x}) = 0\}_{j=1}^{m}$ is called an* IPS *refutation of $\{f_j(\overline{x}) = 0\}_{j=1}^{m}$. If C comes from a restricted class of algebraic circuits $\mathcal{C}$, then such a refutation is called a $\mathcal{C}$-*IPS *refutation. When $\mathcal{C}$ is the class of all algebraic circuits of depth at most Δ, we write Δ-*IPS *to denote $\mathcal{C}$-*IPS*.*

3 Hardness of Algebraic Circuit Lower Bounds from Hardness of Weak Rank Principle

We define the *polynomial system* $\mathsf{AlgCircuit}(f, s, \ell)$ as a formalization stating that a polynomial f can be computed by an algebraic circuit of size s and syntactic degree ℓ. Informally, this involves encoding the type of each gate (whether it is a variable, constant, + gate, or × gate), the inputs of the gate, and the polynomial it computes by specifying the coefficient vector over all possible monomials of degree at most ℓ. Additionally, it is convenient to introduce auxiliary variables to represent the polynomials computed by the inputs of + and × gates. The axioms of $\mathsf{AlgCircuit}(f, s, \ell)$ ensure the correctness of the encoded circuit. This definition closely resembles the lower bound formula from [41].

▶ **Definition 14** ($\mathsf{AlgCircuit}(f, s, \ell)$). *Let $f(\overline{u})$ be a polynomial in n variables. Let N be the number of $\overline{u}$-monomials of degree at most ℓ and $\{M_i\}_{i \in [N]}$ be all such monomials. The variables of $\mathsf{AlgCircuit}(f, s, \ell)$ together with their intended meaning are listed in Table 2.*

For every $v \in [s]$, the axioms of $\mathsf{AlgCircuit}(f, s, \ell)$ are the following polynomials:

$$(1 - \mathsf{InputType}_b(v))(1 - \mathsf{InputType}'_b(v))(\alpha_{1,v,b} - \mathsf{InputType}''_b(v)),$$

for all $b \in [s]$, making $\mathsf{InputType}''_b(v)$ consistent with $\alpha_{1,v,b}$ when the bth input of v is a constant,

$$(1 - \mathsf{InputType}_b(v))(1 - \mathsf{InputType}'_b(v))\alpha_{M_i,v,b},$$

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

Table 2 Variables of $\mathsf{AlgCircuit}(f, s, \ell)$, for every gate $v \in [s]$.

Variable	Meaning
$\alpha_{M_i,v} : i \in [N]$	the coefficient of M_i in the polynomial computed by the gate v.
$\alpha_{M_i,v,b} : i \in [N], b \in [s]$	the coefficient of M_i in the polymomial computed by the bth input of v.
$\mathsf{Type}(v)$	0 if v is a $+$ gate and 1 if v is a $\times$ gate.
$\mathsf{InputType}_b(v) : b \in [s]$	0 if the bth input of v is a variable or a constant and 1 if it is a gate.
$\mathsf{InputType}'_b(v) : b \in [s]$	when $\mathsf{InputType}_b(v) = 0$, it is 0 if the bth input of v is a constant and 1 if it is a variable.
$\mathsf{InputType}''_b(v) : b \in [s]$	when $\mathsf{InputType}_b(v) = \mathsf{InputType}'_b(v) = 0$, it is the constant value of the bth input of v.
$\mathsf{InputVar}_b(v, j) : b \in [s], j \in [n]$	when $\mathsf{InputType}_b(v) = 0$ and $\mathsf{InputType}'_b(v) = 1$, it is 1 iff the bth input of v is the x_j.
$\mathsf{InputNode}_b(v, v') : b \in [s], v' < v$	when $\mathsf{InputType}_b(v) = 1$, it is 1 iff the bth input of v is the gate v'.

for all $b \in [s], i \in [N], M_i \neq 1$, *setting* $\alpha_{M_i,v,b}$ *to* 0 *when the* b*th input of* v *is a constant,*

$$(1 - \mathsf{InputType}_b(v))\mathsf{InputType}'_b(v)\mathsf{InputVar}_b(v, j)\mathsf{InputVar}_b(v, j'),$$

for all $b \in [s], j \neq j' \in [n]$, *ensuring that at most one* $\mathsf{InputVar}_b(v, j)$ *is set to* 1 *when the* b*th input of* v *is a variable,*

$$(1 - \mathsf{InputType}_b(v))\mathsf{InputType}'_b(v)\left(\sum_{j \in [n]} \mathsf{InputVar}_b(v, j) - 1\right),$$

for all $b \in [s]$, *ensuring that at least one* $\mathsf{InputVar}_b(v, j)$ *is set to* 1 *when the* b*th input of* v *is a variable,*

$$(1 - \mathsf{InputType}_b(v))\mathsf{InputType}'_b(v)\mathsf{InputVar}_b(v, j)(\alpha_{x_j,v,b} - 1),$$

for all $b \in [s], j \in [n]$, *making* $\mathsf{InputVar}_b(v, j)$ *consistent with* $\alpha_{x_j,v,b}$ *when the* b*th input of* v *is a variable,*

$$(1 - \mathsf{InputType}_b(v))\mathsf{InputType}'_b(v)\mathsf{InputVar}_b(v, j)\alpha_{M_i,v,b},$$

for all $b \in [s], j \in [n], i \in [N], M_i \neq x_j$, *setting* $\alpha_{M_i,v,b}$ *to* 0 *when the* b*th input of* v *is a variable,*

$$\mathsf{InputType}_b(v)\mathsf{InputNode}_b(v, v')\mathsf{InputNode}_b(v, v''),$$

for all $b \in [s], v' \neq v'' < v$, *ensuring that at most one* $\mathsf{InputNode}_b(v, v')$ *is set to* 1 *when the* b*th input of* v *is a gate,*

$$\mathsf{InputType}_b(v)\left(\sum_{v' < v} \mathsf{InputNode}_b(v, v') - 1\right),$$

for all $b \in [s]$, ensuring that at least one $\mathsf{InputNode}_b(v, v')$ *is set to* 1 *when the bth input of v is a gate,*

$$\mathsf{InputType}_b(v)\mathsf{InputNode}_b(v, v')(\alpha_{M_i,v,b} - \alpha_{M_i,v'}),$$

for all $b \in [s], v' < v, i \in [N]$, making $\alpha_{M_i,v,b}$ and $\alpha_{M_i,v'}$ consistent when the bth input of v is a gate,

$$(1 - \mathsf{Type}(v)) \left(\alpha_{M_i,v} - \sum_{b \in [s]} \alpha_{M_i,v,b} \right),$$

for all $i \in [N]$, making $\alpha_{M_i,v}$ equal to the sum of its children when v is a $+$ node,

$$\mathsf{Type}(v) \left(\alpha_{M_i,v} - \left(\sum_{\substack{i_1,\ldots,i_\ell \in [N] \\ \prod_{b\in[\ell]} M_{i_b} = M_i}} \prod_{b \in [\ell]} \alpha_{M_{i_b},v,b} \right) \prod_{b \in [s] \setminus [\ell]} \alpha_{1,v,b} \right),$$

for all $i \in [N]$, making $\alpha_{M_i,v}$ equal to the product of its children when v is a $\times$ node,

$$\mathsf{Type}(v) \prod_{b \in [\ell]} \alpha_{M_{i_b},v,b},$$

for all $i_1, \ldots, i_\ell \in [N]$ with $\deg(\prod_{b\in[\ell]} M_{i_b}) > \ell$, setting all high-degree monomials to 0*,*

$$\mathsf{Type}(v)\alpha_{M_i,v,b},$$

for all $b \in [s] \setminus [v], i \in [N], M_i \neq 1$, ensuring that only the first ℓ inputs of v are non-constant polynomials,

$$\alpha_{M_i,s} - \mathrm{coeff}_{M_i}(f),$$

for all $i \in [N]$, making $\alpha_{M_i,s}$ (the coefficient vector of the output gate) consistent with the coefficient vector of f.

The size of $\mathsf{AlgCircuit}(f, s, \ell)$ *is* $\mathrm{poly}(s, n, N^\ell)$.

▶ Remark 15. We limit the syntactic degree of the circuit to ℓ, thus every $\times$ node can have at most ℓ inputs computing non-constant polynomials. This allows us to assume that these input gates are among the first ℓ inputs, thus making the size of the encoding significantly smaller: it suffices to consider only N^ℓ tuples of monomials instead of $\binom{N}{s}$.

We demonstrate the hardness of $\mathsf{AlgCircuit}(f, s, \ell)$ by reducing it to the *weak rank principle* [14], which states that an $m \times m$ matrix of rank greater than n cannot be decomposed into the product of an $m \times n$ matrix and an $n \times m$ matrix when $m > n$. Given such a matrix A, we encode the negation of this principle as the following polynomial system $\mathsf{RankP}_n^m(A)$.

▶ **Definition 16** (The (Weak) Rank Principle [14])**.** *Let $\mathbb{F}$ be a field and m and n two positive integers with $m > n$. We denote by* $\mathsf{RankP}_n^m(A)$ *the system of degree-2 polynomial equations stating that the rank of an $m \times m$ matrix A is at most n over $\mathbb{F}$. More precisely,* $\mathsf{RankP}_n^m(A)$ *is defined over $2mn$ variables arranged into two matrices $X \in \mathbb{F}^{m\times n}$ and $Y \in \mathbb{F}^{n\times m}$. For every $i, j \in [m]$, there is an equation in* $\mathsf{RankP}_n^m(A)$ *stating that the (i, j)th entry of the product XY is equal to $A_{i,j}$. That is,* $\mathsf{RankP}_n^m(A)$ *consists of the polynomials*

$$\sum_{k \in [n]} x_{i,k} y_{k,j} - A_{i,j}, \qquad i, j \in [m].$$

By linear algebra, when the rank of A exceeds n, the system $\mathsf{RankP}_n^m(A)$ is unsatisfiable.

To perform the above reduction, we define an iterated version of $\mathsf{RankP}_n^m(A)$. Let L and n be positive integers and $\Sigma = \{0, \dots, L\}$ an alphabet of size $L+1$. We denote by $\Sigma^{\leq n}$ the set of strings over Σ of length at most n. Similarly, $\Sigma^{<n}$ denotes the set of all strings over Σ of length strictly less than n. Let K be a positive integer. For every string $\pi \in \Sigma^{\leq n}$, let $X^{(\pi)} = (x_{i,k}^{(\pi)})_{i\in[(L+1)K],k\in[K]}$ be an $(L+1)K \times K$ variable matrix. Let $Y = (y_{k,j})_{k\in[K],j\in[(L+1)K]}$ be a $K \times (L+1)K$ variable matrix. For every string $\pi \in \Sigma^n$, let $A^{(\pi)}$ be an $(L+1)K \times (L+1)K$ constant matrix.

▶ **Definition 17** (Iterated Rank Principle [14]). *Let L, n, K be positive integers, $\Sigma = \{0, \dots, L\}$, and let $\{A^{(\pi)} : \pi \in \Sigma^n\}$ be a set of $(L+1)K \times (L+1)K$ constant matrices. We define $\mathsf{IRankP}_{L,n,K}(\{A^{(\pi)}\})$ as the system of the following polynomial axioms:*

$$\sum_{k\in[K]} x_{i,k}^{(\pi)} y_{k,j} - x_{i,j-\lfloor\frac{j-1}{K}\rfloor K}^{(\pi*\lfloor\frac{j-1}{K}\rfloor)}, \qquad \forall \pi \in \Sigma^{<n}, i, j \in [(L+1)K],$$

$$\sum_{k\in[K]} x_{i,k}^{(\pi)} y_{k,j} - A_{i,j}^{(\pi)}, \qquad \forall \pi \in \Sigma^{n}, i, j \in [(L+1)K].$$

Namely, $\mathsf{IRankP}_{L,n,K}(\{A^{(\pi)}\})$ contains all the degree-2 polynomial equations in the following matrix multiplications:

$$X^{(\pi)}Y = \left[X^{(\pi*0)}\ X^{(\pi*1)}\ \cdots\ X^{(\pi*L)}\right], \qquad \forall \pi \in \Sigma^{<n},$$

$$X^{(\pi)}Y = A^{(\pi)}, \qquad \forall \pi \in \Sigma^{n}.$$

▶ **Definition 18** (Iterated Rank Principle with extension variables [14]). *Let L, n, K be positive integers, $\Sigma = \{0, \dots, L\}$ and let $\{A^{(\pi)} : \pi \in \Sigma^n\}$ be a set of $(L+1)K \times (L+1)K$ constant matrices. We define $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ as the polynomial system consisting of the axioms of $\mathsf{IRankP}_{L,n,K}(\{A^{(\pi)}\})$ together with the following axioms:*

$$z_{i,j,k}^{(\pi)} - x_{i,k}^{(\pi)} y_{k,j}, \qquad \forall \pi \in \Sigma^{\leq n}, i, j \in [(L+1)K], k \in [K].$$

We need these extension variables because the axioms of $\mathsf{IRankP}_{L,n,K}(\{A^{(\pi)}\})$ are inner products and thus require additional gates to be computed by an algebraic circuit. Namely, $z_{i,j,k}^{(\pi)}$ correspond to the $\times$ gates computing the products $x_{i,k}^{(\pi)} y_{k,j}$, which we later add by using a $+$ gate. The details of this construction are given in the proof of Theorem 20 below.

The monomial size lower bound on $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ against $\mathsf{PCR}_{\mathbb{F}_2}$ is given in [14].

▶ **Theorem 19** ([14]). *Every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ requires $2^{K^{\Omega(1)}}$ monomials.*

▶ **Theorem 20.** *There exists a constant $c > 0$ such that given a polynomial f of degree at most ℓ over $\mathbb{F}_2$ in n variables and $s \geq n^c$, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{AlgCircuit}(f, s, \ell)$ requires superpolynomially many monomials.*

Proof. We prove this theorem by construction a reduction from $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ to $\mathsf{AlgCircuit}(f, s, \ell)$ for some L and K that are polynomial in s and n. The reduction is done by substituting the variables of $\mathsf{AlgCircuit}(f, s, \ell)$ with *constants and variables* of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$, which does not increase the refutation size. Under this reduction, each axiom of $\mathsf{AlgCircuit}(f, s, \ell)$ is either satisfied or becomes a simple consequence of the axioms of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$.

The high level idea of the construction is as follows: we explicitly define a small algebraic circuit C that computes the given polynomial f. We proceed by embedding C into $\mathsf{AlgCircuit}(f, s, \ell)$ by fixing all the variables that are responsible for the topology of C (i.e., the variables that encode the type and inputs of each gate in C). This embedding satisfies all the axioms of $\mathsf{AlgCircuit}(f, s, \ell)$ except for those that describe the coefficent vectors of the gates in C. We show that they have simple derivations from the axioms of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$.

We construct a small circuit $C(\overline{u}) = C(u_1, \ldots, u_n)$ which purportedly computes f and uses variables of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ as constants. Let $L \leq \ell$ be the degree of f and let $\Sigma = \{0, \ldots, L\}$. The circuit uses gates $g_x[t, i, k]$ and $g_z[t, i, j, k, d]$, where $t \in \{0, \ldots, n\}$, $i, j \in [(L+1)K]$, $k \in [K]$, and $d \in \Sigma$. We also have a special output gate out. For each $\pi \in \Sigma^{\leq n}$, we write $\overline{u}^{\pi}$ to denote the monomial $u_1^{\pi_1} u_2^{\pi_2} \cdots u_{|\pi|}^{\pi_{|\pi|}}$.

Then for every $\pi \in \Sigma^n$, we define the matrix $A^{(\pi)}$ such that $A^{(\pi)}_{1,1} = \mathrm{coeff}_{\overline{u}^{\pi}(f(\overline{u}))}$ and is zero everywhere else. Assuming that $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$ is satisfied, we require that for each $\pi \in \Sigma^n$,

$$\mathrm{coeff}_{\overline{u}^{\pi}}(\widehat{C}_{\mathsf{out}}) = (X^{(\pi)}Y)_{1,1}. \tag{1}$$

We define $g_z[t, i, j, k, d] = g_x[t, i, k] y_{k,j} u_{t+1}^d$ for every $i, j \in [(L+1)K], k \in [K]$, $d \in \Sigma$ and $t \in \{0, \ldots, n-1\}$ and $g_z[n, 1, 1, k, 0] = g_x[n, 1, k] y_{k,1}$ (the other gates of the form $g_z[n, i, j, k, d]$ with $(i, j, d) \neq (1, 1, 0)$ are not used in the construction). The gates $g_x[t, i, k]$ are thus defined recursively on t, using g_z. For every $i \in [(L+1)K]$ and $k \in [K]$:

$$\begin{aligned} g_x[0, i, k] &= x^{()}_{i,k}, \\ g_x[t, i, k] &= \sum_{d \in \Sigma} \sum_{k' \in [K]} g_z[t-1, i, k + dK, k', d], && \forall t \in [n]. \end{aligned}$$

Here, () denotes the empty string. The output gate of $C(\overline{u})$ is $\mathsf{out} = \sum_{k' \in [K]} g_z[n, 1, 1, k', 0]$. It is easy to see that $C(\overline{u})$ is an algebraic circuit of size at most $2n(L+1)^3 K^3$.

Now we verify that (1) holds for this construction. Before doing this, we start by verifying that for each $t \in \{0, \ldots, n\}$, $i \in [(L+1)K]$ and $k \in [K]$,

$$\widehat{C}_{g_x[t,i,k]} = \sum_{\pi \in \Sigma^{\leq t}} x^{(\pi)}_{i,k} \overline{u}^{\pi}, \tag{2}$$

can be derived using the axioms of $\mathsf{IRankPE}_{L,n,K}(\{A^{\pi}\})$. We prove the statement by induction on t. The base case holds by the definiton of $g[0, i, k]$. The inductive step is as follows:

$$\begin{aligned} \widehat{C}_{g_x[t,i,k]} &= \sum_{d \in \Sigma} \sum_{k' \in [K]} g_z[t-1, i, k + dK, k', d] && \text{(by definition)} \\ &= \sum_{d \in \Sigma} \left(\sum_{k' \in [K]} g_x[t-1, i, k'] y_{k', k+dK} \right) u_t^d && \text{(expanding } g_z\text{)} \\ &= \sum_{d \in \Sigma} \left(\sum_{k' \in [K]} \left(\sum_{\pi \in \Sigma^{\leq t-1}} x^{(\pi)}_{i,k'} \overline{u}^{\pi} \right) y_{k', k+dK} \right) u_t^d && \text{(by the induction hypothesis)} \\ &= \sum_{d \in \Sigma} \left(\sum_{\pi \in \Sigma^{\leq t-1}} \left(\sum_{k' \in [K]} x^{(\pi)}_{i,k'} y_{k', k+dK} \right) \overline{u}^{\pi} \right) u_t^d && \text{(switching the summation order)} \end{aligned}$$

$$= \sum_{d\in\Sigma}\left(\sum_{\pi\in\Sigma^{\le t-1}} x_{i,k}^{(\pi*d)}\overline{u}^{\pi}\right)u_t^d \qquad \text{(by the axioms of } \mathsf{IRankPE}_{L,n,K}(\{A^\pi\})\text{)}$$

$$= \sum_{\pi\in\Sigma^{\le t}} x_{i,k}^{(\pi)}\overline{u}^{\pi}. \qquad \text{(combining } \overline{u}^\pi \text{ and } u_t^d\text{)}$$

Similarly, we show that $\widehat{C}_{\mathsf{out}} = \sum_{\pi\in\Sigma^{\le n}} A_{1,1}^{(\pi)}\overline{u}^{\pi}$, which implies (1) due to the definition of $A^{(\pi)}$.

$$\widehat{C}_{\mathsf{out}} = \sum_{k'\in[K]} g_z[n,1,1,k',0] \qquad \text{(by definition)}$$

$$= \sum_{k'\in[K]} g_x[n,1,k']y_{k',1} \qquad \text{(expanding } g_z\text{)}$$

$$= \sum_{k'\in[K]}\left(\sum_{\pi\in\Sigma^{\le n}} x_{1,k'}^{(\pi)}\overline{u}^{\pi}\right)y_{k',1} \qquad \text{(by (2))}$$

$$= \sum_{\pi\in\Sigma^{\le n}}\left(\sum_{k'\in[K]} x_{1,k'}^{(\pi)}y_{k',1}\right)\overline{u}^{\pi} \qquad \text{(switching the summation order)}$$

$$= \sum_{\pi\in\Sigma^{\le n}} A_{1,1}^{(\pi)}\overline{u}^{\pi}. \qquad \text{(by the axioms of } \mathsf{IRankPE}_{L,n,K}(\{A^\pi\})\text{)}$$

Now, we present a substitution ρ, which embeds the circuit C into $\mathsf{AlgCircuit}(f,s,\ell)$. We begin by encoding the topology of the circuit by assigning all the Type, $\mathsf{InputType}$, $\mathsf{InputType}'$, $\mathsf{InputType}''$, $\mathsf{InputVar}$ and $\mathsf{InputNode}$ variables to the appropriate constants. Slightly abusing the notation, we proceed by setting for each $t\in\{0,\dots,n\}, i\in[(L+1)K], k\in[K], \pi\in\Sigma^{\le t}$, $d\in\Sigma$, $\rho(\alpha_{\overline{u}^\pi,g_x[t,i,k]}) = x_{i,k}^{(\pi)}$ and $\rho(\alpha_{M,g_x[t,i,k]}) = 0$ for the remaining monomials M. The values of $g_z[t,i,j,k]$ are defined similarly. Then the inputs of $g_x[t,i,k]$ are defined as the appropriate gates $g_z[t-1,i,k+dK,k',d]$ to satisfy the definition of C. The inputs of $g_z[t,i,j,k,d]$ are similarly defined as the gate $g_x[t,i,k]$, followed by d variables u_{t+1} and a constant $y_{k,j}$.

Observe that such a substitution replaces each variable with either a constant or another variable (possibly a negation). This preserves the PCR size of the refutation. It is follows from the definition that the axioms of $\mathsf{AlgCircuit}(f,s,\ell)\restriction\rho$ can be easily derived from the axioms of $\mathsf{IRankPE}_{L,n,K}(\{A^{(\pi)}\})$.

Now suppose that $\mathsf{AlgCircuit}(f,s,\ell))$ has a PCR refutation of polynomial size, specifically, $\mathrm{poly}(s,n,N^\ell) \le \exp((\ell n)^{O(1)})$. Then, $\mathsf{IRankPE}_{L,n,K}(\{A_\pi\})$ has a PCR refutation of size $\exp((\ell n)^{O(1)})$. By taking K to be sufficiently large (say, $(\ell n)^{\Omega(1)}$), this contradicts Theorem 19 since such a refutation must have size $\exp(K)$. ◀

Similarly to $\mathsf{AlgCircuit}(f,s,\ell)$, we can define $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ stating that an n-variable polynomial f has a depth-Δ algebraic circuit of size s and syntactic-degree ℓ. We can apply a similar idea to get a lower bound on the size of PCR refutations of $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ provided the rank principle does not hold.

▶ **Theorem 21.** *For every constant $c>0$, given a polynomial f of degree at most ℓ over $\mathbb{F}_2$ in n variables and $s\ge N^{1/c}$, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{AlgCircuit}(f,s,\ell,O(c))$ requires superpolynomially many monomials.*

Proof sketch. We construct the circuit C similarly to the one from the proof of Theorem 20 but instead of multiplying the $\overline{u}$-variables one-by-one, we multiply them by all monomials of degree at most ℓ in the subsequent n/c variables. This increases the size of the circuit since we are forced to choose L to be the number of such monomials, which is approximately $N^{1/c}$. However, this way, C only requires depth $O(c)$. ◀

▶ Remark 22. Observe that the above circuit constructions do not use the whole matrices $A^{(\pi)}$, but only their $(1,1)$th entry. We can construct some slightly more efficient circuits by using more entries of $A^{(\pi)}$ to store the coefficients by computing the polynomials

$$\sum_{\pi\in\Sigma^{\leq n-2},d,d'\in\Sigma} A^{(\pi)}_{d,d'}u^{(\pi)}u^d_{n-1}u^{d'}_n.$$

This can be done by introducing gates $\alpha[k]$ computing the polynomials

$$\sum_{d\in\Sigma}\sum_{\pi\in\Sigma^{\leq n-2}} x^{(\pi)}_{d,k}u^{(\pi)}u^d_{n-1}$$

and gates $\beta[d'+dK]$ computing $y_{d'+dK}u^{d'}_n$. Then, the output gate can be defined as the inner product of α and β.

A similar idea can be applied to the proof for $\mathsf{AlgCircuit}(f,s,\ell,O(c))$.

▶ Remark 23. Note that we can also view $\mathsf{AlgCircuit}(f,s,\ell)$ as a **proof complexity generator** in the algebraic setting: treating the coefficient vector of f as an output vector $\overline{b}\in\mathbb{F}^N$ (where N is the number of monomials of degree at most ℓ over n variables) of a function $\tau(s,\ell)$, we can view $\mathsf{AlgCircuit}(f,s,\ell)$ as an encoding of the statement $\tau(s,\ell)=\overline{b}$. Thus, Theorem 20 shows that $\mathsf{AlgCircuit}(f,s,\ell)$ is a proof complexity generator against PCR.

Similarly, $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ can be viewed as $\tau(s,\ell,\Delta)=\overline{b}$, where $\overline{b}\in\mathbb{F}^N$ and N is the number of monomials of degree at most ℓ over n variables, and is a proof complexity generator against PCR.

4 Hardness of Bounded-Depth Algebraic Circuit Lower Bounds from Hardness of Weak Tensor Rank Principles

In this section, we need a generalization of the rank principle, which we call the *tensor rank principle*.

▶ **Definition 24** (Tensor Rank Principle). *Let $\mathbb{F}$ be a field and m,n two positive integers with $m>n$. We denote $\mathsf{TRankP}^m_n(r,A)$ the system of degree-r polynomial equations stating that the tensor rank of an r-tensor $A\in\mathbb{F}^{\overbrace{m\times\cdots\times m}^{r\text{ times}}}$ is at most n over $\mathbb{F}$. More precisely, $\mathsf{TRankP}^m_n(r,A)$ is defined over rmn variables arranged into rn vectors $\mathbf{x}_{j,k}\in\mathbb{F}^m : j\in[r],k\in[n]$.*

For every $i_1,\ldots,i_r\in[m]$ (which are not necessarily distinct), there is an equation in $\mathsf{TRankP}^m_n(r,A)$ stating that the $(i_1,\ldots,i_r)$th entry in the summation of the tensor product $\bigotimes_{j=1}^r\mathbf{x}_{j,k}$ is equal to $A_{i_1,\ldots,i_r}$. That is, $\mathsf{TRankP}^m_n(r,A)$ consists of the polynomials

$$\sum_{k\in[n]}\prod_{j\in[r]}x_{j,k,i_j}-A_{i_1,\ldots,i_r},\qquad i_1,\ldots,i_r\in[m],\tag{3}$$

where x_{j,k,i_j} denotes the (i_j)th entry of the vector $\mathbf{x}_{j,k}$.

Namely, $\mathsf{TRankP}_n^m(r, A)$ *is the set of polynomial equations stating that*

$$\sum_{k\in[n]} \bigotimes_{j=1}^{r} \mathbf{x}_{j,k} = A.$$

By definition, $\sum_{k\in[n]} \bigotimes_{j=1}^{r} \mathbf{x}_{j,k}$ is the tensor rank decomposition of rank at most n. Thus, when the tensor rank of A exceeds n, $\mathsf{TRankP}_n^m(r, A)$ is unsatisfiable. This principle can be viewed as a generalization of the rank principle, and coincides with it when $r = 2$.

▶ **Theorem 25.** *Assume m, n, r to be positive integers with $m > n$. Let $J \subseteq [m]$ with $|J| > n$ and let A be the r-tensor defined as*

$$A_{i_1,\dots,i_r} = \begin{cases} 1 & \text{if } i_1 = \cdots i_r \in J, \\ 0 & \text{otherwise.} \end{cases}$$

Then every $\mathsf{PCR}_{\mathbb{F}_2}$ *refutation of* $\mathsf{TRankP}_n^m(r, A)$ *requires* $2^{\Omega(n)}$ *monomials.*

Proof. Without loss of generality assume that $A = I_m$ (and thus $J = [m]$): we can set all $x_{j,k,i}$ to 0 for all $j \in [r]$, $k \in [n]$ and $i \notin J$. This reduces $\mathsf{TRankP}_n^m(r, A)$ to $\mathsf{TRankP}_n^{|J|}(r, I_{|J|})$.

The idea of the proof is analogous to the proof of the lower bound for RankP in [14].

We say that a term t *mentions* an index $k \in [n]$ if there exist $j \in [r]$ and $i \in [m]$ such that $x_{j,k,i}$ or $\overline{x}_{j,k,i}$ appears in t. We start by proving a lower bound on the number of different indices $k \in [n]$ each term mentions by reducing PHP_n^m to $\mathsf{TRankP}_n^m(r, A)$. The axioms of PHP_n^m are the *pigeon axioms*

$$\sum_{k\in[n]} x_{i,k} - 1, \qquad \forall i \in [m],$$

and the *hole axioms*

$$x_{i,k}x_{j,k}, \qquad \forall i \neq j \in [m], k \in [n].$$

It follows from [39, 19] that any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of PHP_n^m must have a term that mentions at least $n/2 + 1$ different holes $k \in [n]$ (in fact, it must contain a term that correspond to a *matching* of this size).

Let $X = (x_{i,k})_{i\in[m],k\in[n]}$ be fresh variables and define the restriction ρ as

$$\rho(x_{j,k,i}) = x_{i,k}, \qquad \forall j \in [d], k \in [n], i \in [m].$$

Under ρ, the axioms of $\mathsf{TRankP}_n^m(r, A)$ become[5]

$$\sum_{k\in[n]} x_{i,k} - 1, \tag{4}$$

when $i_1 = \cdots = i_r = i$ and

$$\sum_{k\in[n]} \prod_{j\in[r]} x_{i_j,k}, \tag{5}$$

[5] Recall that proof lines are *multilinear* polynomials.

where at least two i_j and $i_{j'}$ are different. Observe that (4) is precisely the pigeon axiom of PHP_n^m and (5) can be derived easily from the hole axioms $x_{i_j,k}x_{i_{j'},k}$. Thus, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{TRankP}_n^m(r,A)$ must contain a term involving at least $n/2+1$ variables $x_{j,k,i}$ (or their negations) with different k.

Now let σ be a partial restriction defined as follows. Choose a random subset $K \subseteq [n-1]$ of size $n/2-1$ uniformly and for each $k \in K$ independently choose $c_k \in \{0,1\}$ at random. Define $c_n = 1$ if $\sum_{k\in K} c_k$ is odd and $c_n = 0$ otherwise. This guarantees that $\sum_{k\in K\cup\{n\}} c_k$ is even. Then assign

$$\sigma(x_{j,k,i}) = \begin{cases} c_k & \text{if } k \in K \cup \{n\}, \\ * & \text{if } k \notin K \cup \{n\}. \end{cases}$$

Under σ, $\mathsf{TRankP}_n^m(r,A) \restriction \sigma$ becomes $\mathsf{TRankP}_{n/2}^m(r,A)$ (up to the variable renaming). Moreover, each term that mentions at least $n/2+1$ different $k \in [n]$, becomes zero with probability $1-\exp(-\Omega(n))$ by the Chernoff bound. Applying the union bound, we can eliminate all such terms in a proof of size at most $\exp(\epsilon n)$ for a sufficiently small constant $\epsilon > 0$, contradicting the above degree bound. ◀

▶ **Theorem 26.** *Suppose that* $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ *admits a* Δ'-IPS *refutation of size* s*, where* $\Delta > 4$ *and* $s > n2\ell^4$*. Then* $\mathsf{TRankP}^N_{\sqrt{s}}(n,A)$ *admits a* $(\Delta'+5)$-IPS *refutation of size*

$$O(Nn\cdot s + NK\cdot|\mathsf{AlgCircuit}(f,s,\ell,\Delta)|), \text{ where}$$

- $N = \binom{n+\ell}{\ell}$ *is the number of monomials in* n *variables of total degree at most* ℓ*;*
- A *is the* n*-tensor such that the* $(M,\dots,M)$*th entry of* A *is* $\operatorname{coeff}_M(f)$*, for every monomial* M *in* n *variables and total degree at most* ℓ*, and the rest of* A *is all zero.*

The proof of this theorem is analogous to the proof of Theorem 20. We construct a circuit C that is parametrized by the variables of $\mathsf{TRankP}^N_{\sqrt{s}}(n,A)$ such that after we embed this circuit into $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$, we obtain a refutation of a polynomial system that can be easily derived from the axioms of $\mathsf{TRankP}^N_{\sqrt{s}}(n,A)$.

Proof. We show how to reduce the bounded-depth algebraic circuit upper bound formulas to $\mathsf{TRankP}^N_K(n,A)$, where $T_f \coloneqq \{M : M \text{ is a monomial in } f \text{ with a non-zero coefficient}\}$ and K is bounded by $\sqrt{s}$. We use the notation $\deg_{u_j}(M)$ to denote the individual degree of u_j in the monomial M.

Consider the depth-4 algebraic circuit $C(u_1,\dots,u_n) \coloneqq \sum_{k\in[K]}\prod_{j\in[n]}\sum_{d\in[\ell+1]}\alpha_{j,k,d}u_j^d$, where $\alpha_{j,k,d}$ are placeholder variables defined as $\alpha_{j,k,d} \coloneqq \sum_{\substack{M\in T_f,\\ \deg_{u_j}(M)=d}} x_{j,k,M}$.

For every monomial $M = u_1^{d_1}\cdots u_n^{d_n} \in T_f$, we have

$$\begin{aligned}
\operatorname{coeff}_M(\widehat{C}) &= \operatorname{coeff}_M\left(\sum_{k\in[K]}\prod_{j\in[n]}\sum_{d\in[\ell+1]}\alpha_{j,k,d}u_j^d\right) && \text{(by definition)}\\
&= \sum_{k\in[K]}\operatorname{coeff}_M\left(\prod_{j\in[n]}\sum_{d\in[\ell+1]}\alpha_{j,k,d}u_j^d\right) && \text{(since coefficients add termwise)}\\
&= \sum_{k\in[K]}\prod_{j\in[n]}\alpha_{j,k,d_j} && \text{(computing the coefficient for } M)
\end{aligned}$$

$$= \sum_{k\in[K]} \left(\prod_{j\in[n]} x_{j,k,M} + X_k \right) \qquad \text{(using } X_k \text{ to denote the summation of monomials in involving at least two variables } x_{j,k,M} \text{ and } x_{j',k',M'} \text{ with } M \neq M' \text{ and rearranging the terms)}$$

$$= \sum_{k\in[K]} \prod_{j\in[n]} x_{j,k,M} \qquad \text{(by the off-diagonal axioms of } \mathsf{TRankP}^N_K(n,A))$$

$$= A_{M,\dots,M} \qquad \text{(by the axioms of } \mathsf{TRankP}^N_K(n,A))$$

$$= \mathrm{coeff}_M(f). \qquad \text{(by the definition of } A)$$

For a monomial $M \notin T_f$, we have

$$\mathrm{coeff}_M(\widehat{C}) = \sum_{k\in[K]} \mathrm{coeff}_M \left(\prod_{j\in[n]} \sum_{d\in[\ell+1]} \alpha_{j,k,d} u_j^d \right) \qquad \text{(since coefficients add termwise)}$$

$$= \sum_{k\in[K]} X_k \qquad \text{(by computing the coefficient for } M)$$

$$= 0. \qquad \text{(by the axioms of } \mathsf{TRankP}^N_K(n,A))$$

We construct a substitution ρ that embeds C into $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$. Note that C is a depth-4 algebraic circuit having size at most $2Kn(\ell+1)^2$. The formal variables $\alpha_{j,k,d}$ are replaced with $\sum_{M\in T_f,\ \deg_{u_j}(M)=d} x_{j,k,M}$ of size at most N.

Under this substitution, every axiom in $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$, where $s \geq 2Kn(\ell+1)^2$, is transformed into a formula derivable from $\mathsf{TRankP}^N_K(n,A)$ with size at most $O(NK)$ and depth at most 4. Consequently, if $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ admits a Δ'-IPS refutation of size s, then $\mathsf{TRankP}^N_K(n,A)$ admits a $(\Delta'+5)$-IPS refutation of size

$$O(Nns + NK \cdot |\mathsf{AlgCircuit}(f,s,\ell,\Delta)|)\,.$$

Finally, since K is the maximum fan-in of the circuit C, we may set $K = \sqrt{s}$. ◀

▶ **Corollary 27.** *Suppose that* $\mathsf{TRankP}^m_n(r,A)$ *requires* Δ'-IPS *refutations of size* $2^{n^{\Omega(1)}}$. *Then* $\mathsf{AlgCircuit}(f,s,\ell,\Delta)$ *requires* $(\Delta'-5)$-IPS *refutations of size at least* $|\mathsf{AlgCircuit}(f,s,\ell,\Delta)|^{\omega(1)}$.

▶ Remark 28. In Theorem 26 we only consider the unit tensor, but it is plausible that it should be hard for constant-depth IPS. By definition, $\mathsf{TRankP}^m_n(r,I)$ is a generalization of $\mathsf{RankP}^m_n(I)$. For sufficiently strong proof systems, $\mathsf{RankP}^m_n(I)$ and $\mathsf{RankP}^m_n(A)$, for an arbitrary high-rank matrix A, are equivalent since they can perform the linear transformation that transforms one formula into the other. Because the determinant is hard for constant-depth circuits [27], the rank principle – and, by extension, the tensor rank principle – is likely hard for constant-depth IPS.

5 Short NC^2-Frege Proofs for Constant-Depth Algebraic Circuit Lower Bounds

In this section we show that NC^2-Frege (see [18] for the definition) admits short proof of [27] and [10], namely, of constant depth algebraic circuit lower bounds for the permanent and determinant.

For this purpose, we use a formalization in VNC^2, which is a first-order theory whose (low logical complexity) theorems translate to polynomial-size proofs in NC^2-Frege. We shall demonstrate a formalization of the proof of the superpolynomial lower bound of the Permanent polynomial against constant-depth algebraic circuits over any field. This is an adaptation of the proof of [27] and [10]. The work in [27] presented a superpolynomial lower bound against constant-depth algebraic circuit lower over fields with large characteristic. Forbes extended this result to any field by replacing the original set-multilinearization argument in [27], which works only in fields with large characteristic, with a new set-multilinearization argument over any field.

In previous sections all we studied were lower bounds (or unprovability) results for constant-depth algebraic circuit lower bound statements. In this section, we present an *upper bound* on proving constant-depth algebraic circuit lower bounds. Due to space constraints, the proofs are deferred to the full version of this paper.

▶ **Theorem 29** (Provability of superpolynomial lower bound for the Permanent polynomial against constant-depth algebraic circuits)**.** *Let $s(n)$ be a polynomial in n, Δ be a constant. The following $\forall\Sigma^B_0$-formula stating a superpolynomial lower bound for the Permanent polynomial against constant-depth algebraic circuits is provable in VNC^2:*

$$\begin{aligned}
&\forall n \in Log, d = c\lfloor \log n \rfloor,\ k = 10d,\\
&\forall w \in A^d,\ \forall |V|, |G|, |I|, |E| < s(n), N = \binom{n+d}{d},\\
&\quad \mathbf{unbiased}(w, d, k) \wedge \mathbf{Depth}_{2\Delta}(V, G, I, E) \rightarrow\\
&\quad \mathbf{Coeff}(V, G, I, E, N) \neq \mathbf{Perm}(\sum_{i\in[d]} 2^{|w_{[i]}|_1}, \sum_{i\in[d]} 2^{|w_i|_1}).
\end{aligned}$$

The above formula is in $\forall\Sigma^B_0$. The length of every string in the proof is polynomially bounded by n^d, which is the length of the coefficient vectors of n variables and degree d. Moreover, n is logarithmically small and d, which is equal to $c\lfloor \log n \rfloor$, is even logarithmically smaller than n.

Using the translation between bounded arithmetic theories and propositional proofs as shown in [8], we get the following theorem.

▶ **Theorem 30.** *There are polynomial-size propositional NC^2-Frege proofs of the superpolynomial lower bound for the Permanent polynomial against constant-depth algebraic circuits over finite fields $\mathbb{F}_q$.*

References

1 Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM J. Comput.*, 31(4):1184–1211 (electronic), 2002.

2 Per Austrin and Kilian Risse. Sum-of-squares lower bounds for the minimum circuit size problem. In *38th Computational Complexity Conference, CCC'23*, pages 31:1–31:21, 2023. doi:10.4230/LIPIcs.CCC.2023.31.

3 Theodore P. Baker, John Gill, and Robert Solovay. Relativizations of the P =? NP question. *SIAM J. Comput.*, 4(4):431–442, 1975. doi:10.1137/0204037.

4 CS Bhargav, Sagnik Dutta, and Nitin Saxena. Improved lower bound, and proof barrier, for constant depth algebraic circuits. *ACM Transactions on Computation Theory*, 16(4):1–22, 2024. doi:10.1145/3689957.

5 Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.

6 Prerona Chatterjee, Mrinal Kumar, C. Ramya, Ramprasad Saptharishi, and Anamay Tengse. On the existence of algebraically natural proofs. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS '20*, pages 870–880. IEEE, 2020. doi:10.1109/FOCS46700.2020.00085.

7 Lijie Chen, Jiatu Li, and Igor Oliveira. Reverse mathematics of complexity lower bounds. *SIAM Journal on Computing*, pages FOCS24–316, 2026.

8 Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. ASL Perspectives in Logic. Cambridge University Press, 2010.

9 Klim Efremenko, Ankit Garg, Rafael Mendes de Oliveira, and Avi Wigderson. Barriers for rank methods in arithmetic complexity. In *9th Innovations in Theoretical Computer Science Conference, ITCS'18*, pages 1:1–1:19, 2018. doi:10.4230/LIPIcs.ITCS.2018.1.

10 Michael A. Forbes. Low-Depth Algebraic Circuit Lower Bounds over Any Field. In *39th Computational Complexity Conference (CCC 2024)*, volume 300 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:16. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.CCC.2024.31.

11 Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. *Theory Comput.*, 17:1–88, 2021. doi:10.4086/TOC.2021.V017A010.

12 Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving lower bounds for algebraic circuits. *Theory of Computing*, 14(1):1–45, 2018. doi:10.4086/toc.2018.v014a018.

13 Ankit Garg, Visu Makam, Rafael Mendes de Oliveira, and Avi Wigderson. More barriers for rank methods, via a "numeric to symbolic" transfer. In *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS '19*, pages 824–844, 2019. doi:10.1109/FOCS.2019.00054.

14 Michal Garlík, Svyatoslav Gryaznov, Ren Hanlin, and Iddo Tzameret. The weak rank principle: Lower bounds and applications. In *Proceedings of the 58th Annual ACM Symposium on the Theory of Computing (STOC)*, 2026.

15 Joshua A. Grochow, Mrinal Kumar, Michael E. Saks, and Shubhangi Saraf. Towards an algebraic natural proofs barrier via polynomial identity testing. *CoRR*, abs/1701.01717, 2017. arXiv:1701.01717.

16 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. doi:10.1145/3230742.

17 Joel David Hamkins and Emil Jeřabek. Can the induction axiom in the peano arithmetic be replaced by the irrationality of $\sqrt{2}$? MathOverflow (2018). URL: https://mathoverflow.net/q/306860.

18 Pavel Hrubes and Iddo Tzameret. Short proofs for the determinant identities. *SIAM J. Comput.*, 44(2):340–383, 2015. doi:10.1137/130917788.

19 Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. doi:10.1007/s000370050024.

20 Emil Jeřábek. Elementary analytic functions in VTC^0. *Annals of Pure and Applied Logic*, 174(6):103269, 2023.

21 Eitetsu Ken and Satoru Kuroda. On matrix rank function over bounded arithmetics. *arXiv preprint arXiv:2310.05982*, 2023. doi:10.48550/arXiv.2310.05982.

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/CBO9780511529948.

23 Jan Krajíček. On the proof complexity of the Nisan-Wigderson generator based on a hard NP ∩ coNP function. *J. Math. Log.*, 11(1):11–27, 2011. doi:10.1142/S0219061311000979.

24 Jan Krajíček. Dual weak pigeonhole principles, pseudo-surjective functions, and provability of circuit lower bounds. *Journal of Symbolic Logic*, 69(1):265–286, 2004. doi:10.2178/JSL/1080938841.

25 Mrinal Kumar, C. Ramya, Ramprasad Saptharishi, and Anamay Tengse. If VNP is hard, then so are equations for it. In *39th International Symposium on Theoretical Aspects of Computer Science, STACS'22*, pages 44:1–44:13, 2022. doi:10.4230/LIPIcs.STACS.2022.44.

26 Jiatu Li and Igor C Oliveira. Unprovability of strong complexity lower bounds in bounded arithmetic. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1051–1057, 2023. doi:10.1145/3564246.3585144.

27 Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Journal of the ACM*, 72(4):1–35, 2025. doi:10.1145/3734215.

28 Jiaqi Lu, Rahul Santhanam, and Iddo Tzameret. $\mathrm{AC}^0[p]$-frege cannot efficiently prove that constant-depth algebraic circuit lower bounds are hard. In *17th Innovations in Theoretical Computer Science Conference, ITCS '26*, 2026. arXiv preprint arXiv:2509.16824. doi:10.48550/arXiv.2509.16824.

29 Henryk Minc. Evaluation of permanents. *Proceedings of the Edinburgh Mathematical Society*, 22(1):27–32, 1979.

30 Moritz Müller and Ján Pich. Feasibly constructive proofs of succinct weak circuit lower bounds. *Annals of Pure and Applied Logic*, 171(2):102735, 2020. doi:10.1016/j.apal.2019.102735.

31 Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 338–339, 1986. doi:10.1145/12130.12164.

32 Igor C Oliveira. Sigact news complexity theory column 124 meta-mathematics of computational complexity theory. *ACM SIGACT News*, 56(1):41–68, 2025. doi:10.1145/3726856.3726862.

33 Ran Raz. Resolution lower bounds for the weak pigeonhole principle. *J. ACM*, 51(2):115–138, 2004. doi:10.1145/972639.972640.

34 Alexander Razborov. Propositional proof complexity: Fifteen (or so) years after. Talk at "A Celebration of Mathematics and Computer Science. Celebrating Avi Wigderson's 60th Birthday October 5 - 8, 2016". https://youtu.be/7LfW6VTW8zo?t=2722, 2016.

35 Alexander Razborov. P, NP and proof complexity. Talk at "SAT and Foundations of Mathematics", Simons Institute. https://youtu.be/xx4mxcqAl5A?t=2333, 2021.

36 Alexander A. Razborov. Bounded arithmetic and lower bounds in boolean complexity. In *Clote, P., Remmel, J., eds. Feasible Mathematics II. Progress in Computer Science and Applied Logic*, volume 13, pages 344–86. Birkhauser, 1995.

37 Alexander A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izv. Ross. Akad. Nauk Ser. Mat.*, 59(1):201–224, 1995.

38 Alexander A. Razborov. Lower bounds for propositional proofs and independence results in bounded arithmetic. In *Automata, Languages and Programming, 23rd International Colloquium, ICALP '96*, pages 48–62. Springer, 1996. doi:10.1007/3-540-61440-0_116.

39 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998. doi:10.1007/s000370050013.

40 Alexander A. Razborov. Resolution lower bounds for perfect matching principles. *Journal of Computer and System Sciences*, 2004.

41 Alexander A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics*, 181:415–472, 2015.

42 Alexander A. Razborov. Guest column: Proof complexity and beyond. *SIGACT News*, 47(2):66–86, 2016. doi:10.1145/2951860.2951875.

43 Alexander A. Razborov and Steven Rudich. Natural proofs. *J. Comput. System Sci.*, 55(1, part 1):24–35, 1997. doi:10.1006/JCSS.1997.1494.

44 Rahul Santhanam and Iddo Tzameret. Iterated lower bound formulas: A diagonalization-based approach to proof complexity. *SIAM Journal on Computing*, 0(0):STOC21–313–STOC21–349, 0. doi:10.1137/21M1447519.

45 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:10.1561/0400000039.

46 Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the Annual ACM Symposium on the Theory of Computing 1987*, pages 77–82, 1987. doi:10.1145/28395.28404.

47 Iddo Tzameret and Stephen A Cook. Uniform, integral, and feasible proofs for the determinant identities. *Journal of the ACM (J. ACM)*, 68(2):1–80, 2021. doi:10.1145/3431922.