$\mathrm{AC}^0[p]$-Frege Cannot Efficiently Prove That Constant-Depth Algebraic Circuit Lower Bounds Are Hard

Jiaqi Lu
Department of Computing, Imperial College London, UK

Rahul Santhanam
Department of Computer Science, Oxford University, UK

Iddo Tzameret
Department of Computing, Imperial College London, UK

Abstract

We study whether lower bounds against constant-depth algebraic circuits computing the Permanent over finite fields (Limaye–Srinivasan–Tavenas [J. ACM, 2025] and Forbes [CCC'24]) are hard to prove in certain proof systems. We focus on a DNF formula that expresses that such lower bounds are hard for constant-depth algebraic proofs. Using an adaptation of the diagonalization framework of Santhanam and Tzameret (SIAM J. Comput., 2025), we show *unconditionally* that this family of DNF formulas does not admit polynomial-size propositional $\mathrm{AC}^0[p]$-Frege proofs, infinitely often. This rules out the possibility that the DNF family is easy, and establishes that its status is either that of a hard tautology for $\mathrm{AC}^0[p]$-Frege or else unprovable (i.e., not a tautology). While it remains open whether the DNFs in question are tautologies, we provide evidence in this direction. In particular, under the plausible assumption that certain (weak) properties of multilinear algebra – specifically, those involving tensor rank – do not admit short constant-depth algebraic proofs, the DNFs *are* tautologies. We also observe that several weaker variants of the DNF formula are provably tautologies, and we show that the question of whether the DNFs are tautologies connects to conjectures of Razborov (ICALP'96) and Krajíček (J. Symb. Log., 2004).

Additionally, our result has the following special features:

(i) **Existential depth amplification**: the DNF formula considered is parameterised by a constant depth d bounding the depth of the algebraic proofs. We show that there *exists some fixed* depth d such that if there are no small depth-d algebraic proofs of certain circuit lower bounds for the Permanent, then there are no such small algebraic proofs in *a*ny constant depth.

(ii) **Necessity**: We show that our result is a necessary step towards establishing lower bounds against constant-depth algebraic proofs, and more generally against any sufficiently strong proof system. In particular, showing there are no short proofs for our DNF formulas, obtained by replacing "constant-depth algebraic circuits" with any "reasonable" algebraic circuit class $\mathcal{C}$, is *n*ecessary in order to prove any super-polynomial lower bounds against algebraic proofs operating with circuits from $\mathcal{C}$.

2012 ACM Subject Classification Theory of computation → Proof complexity; Theory of computation → Proof theory; Theory of computation → Algebraic complexity theory

Keywords and phrases Complexity, Lower bounds, Proof complexity, $\mathbf{AC^0[p]}$-Frege, Diagonalisation, Algebraic complexity

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.99

Related Version *Full Version*: `https://arxiv.org/pdf/2509.16824` [35]

Funding *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).

Rahul Santhanam: This project was partly funded by the EPSRC grant EP/Z534158/1, *Integrated Approach to Computational Complexity: Structure, Self-Reference and Lower Bounds.*
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, *Integrated Approach to Computational Complexity: Structure, Self-Reference and Lower Bounds.*

1 Introduction

Propositional proof complexity studies the sizes of proofs for propositional tautologies in *p*ropositional proof systems of interest [15, 7, 30]. In general, a propositional proof system Q is defined by a polynomial-time computable binary relation

R_Q such that a formula ϕ is a propositional tautology if and only if there is some y such that $R_Q(\phi, y)$ holds; any such y is called a *p*roof of ϕ. The R-proof size of ϕ is the size of the smallest y such that $R_Q(\phi, y)$ holds. For natural sequences of tautologies (such as the Pigeonhole Principle, Tseitin graph formulas, and formulas encoding circuit lower bounds) ϕ_n and propositional proof systems of interest (such as Resolution, Frege and Extended Frege), we would like to understand how the proof size of ϕ_n grows with the size of the formula $|\phi_n|$, and in particular whether the proof size is polynomially bounded or not as a function of the size of the formula.

In their seminal paper on propositional proof complexity, Cook and Reckhow [15] observed that $\mathsf{NP} = \mathsf{coNP}$ if and only if there is a propositional proof system in which every sequence of tautologies has polynomially bounded proof size. This is the basis of the "*Cook-Reckhow program*" [7], of which the ideal limit is the separation of NP from coNP (and hence also P from NP) by showing super-polynomial proof size lower bounds for progressively stronger propositional proof systems.

The Cook-Reckhow program can be seen as a dual, nondeterministic, analogue of the *c*ircuit complexity approach to P vs NP, which proceeds by showing super-polynomial circuit size lower bounds for progressively stronger circuit classes. This analogy is further strengthened by the fact that there is a close correspondence between Boolean circuit classes and inference-based propositional logic, i.e., Frege-style proof systems [7], in which new proofs are derived from axioms and previously derived proof lines using simple sound derivation rules. The basic Resolution proof system works with proof lines that are clauses; the Frege proof system with lines that are Boolean formulas; and the Extended Frege (EF) proof system with lines that are essentially Boolean circuits. The strength of these Frege-style proof systems is generally believed to grow as the proof lines get more expressive, just as the corresponding circuit classes are believed to increase in computational power as they grow more expressive.

1.1 Hard Formulas

We say that a sequence of formulas ϕ_n is *hard* if there is no proof of ϕ_n of polynomial size in $|\phi_n|$. One of the earliest steps in the Cook-Reckhow program – establishing a lower bound on the size of proofs – was taken by Haken [25]. He showed a super-polynomial lower bound for the Pigeonhole Principle formulas in Resolution. Soon after, Ajtai [1] showed a super-polynomial lower bound for the Pigeonhole Principle in AC^0-Frege, which is the Frege-style system where proof lines are constant-depth Boolean circuits. Since then, several improvements and extensions of Ajtai's result have been obtained [2, 6, 13], and the lower

bound techniques used in these works mirror the random restriction techniques used to prove lower bounds against the circuit class AC^0, further reinforcing the analogy between proof complexity lower bounds and circuit complexity lower bounds (cf. [39, 31]). In the circuit complexity setting, we also know lower bounds for the circuit class $\mathrm{AC}^0[p]$ of constant-depth Boolean circuits with prime modular gates, shown using the polynomial method of Razborov and Smolensky [47, 56]. Can the polynomial method or other techniques used to show proof complexity lower bounds for the corresponding Frege-style proof system $\mathrm{AC}^0[p]$-Frege?

Despite much effort, this question has remained open for more than three decades, and continues to be a frontier question in proof complexity. It is already highlighted as a key open problem in the 1998 survey of Beame and Pitassi [7], and the recent survey of Razborov re-iterates this [53]. Progress on the question has focused on restricted *algebraic* subsystems of $\mathrm{AC}^0[p]$-Frege such as the Nullstellensatz [6] and Polynomial Calculus [14] proof systems, which we discussed next.

1.2 Related Work on Algebraic Proof Systems

Much of the research on $\mathrm{AC}^0[p]$-Frege lower bounds has focused on subsystems such as Nullstellensatz and Polynomial Calculus, which encode a CNF and the Boolean constraints on its variables as polynomials and reduce the task of proving that the CNF has no satisfying Boolean assignments[1] to proving that these polynomials do not have a common zero [6, 13]. Nullstellensatz and Polynomial Calculus are propositional proof systems in the Cook-Reckhow sense [15], since the verification of proofs can be done in deterministic polynomial time.

Pitassi [38] proposed more powerful algebraic proof systems where verifying the correctness of a proof requires identity testing of algebraic circuits, i.e., checking whether a given algebraic circuit is identically zero. Identity testing is known to be doable in randomized polynomial time, but it remains a long-standing open question whether it can be done in deterministic polynomial time for general algebraic circuits. Thus, the more general algebraic systems proposed by Pitassi are not propositional proof systems in the traditional Cook-Reckhow sense, but they do have efficient *r*andomized verification.

Grochow and Pitassi [24] defined a strong algebraic proof system in this sense, called the *I*deal Proof System (IPS), where a single algebraic circuit acts as a *c*ertificate that a set of polynomial equations does not have a common zero. The size of an IPS proof is simply the size of the corresponding algebraic circuit which acts as a certificate. [24] showed that IPS is at least as strong as EF, and also that super-polynomial IPS lower bounds for *a*ny sequence of unsatisfiable formulas implies that the Permanent does not have polynomial-size algebraic circuits. This gives a long sought-after connection between proof complexity lower bounds for strong proof systems and (algebraic) circuit complexity lower bounds, but for an algebraic proof system with randomized verification rather than for a propositional proof system. In a more recent paper [54], the implication from proof complexity lower bounds to algebraic complexity lower bounds was strengthened to an *e*quivalence for a certain explicit sequence of formulas.

Given that a proof in IPS is a single algebraic circuit, we can define and study variants of IPS where this circuit is of a restricted form. This has been done in several works in the past decade [18, 5, 23, 26], which seek to show proof complexity lower bounds for subsystems of IPS or to find closer connections between IPS variants and propositional proof systems. Proof

[1] We will sometimes switch back and forth in our discussion between the tasks of refuting that a CNF formula is satisfiable and of proving that a DNF formula is a tautology, which are equivalent by De Morgan's laws.

complexity lower bounds in this setting are typically shown by adapting algebraic circuit lower bound techniques. One apparent drawback to this approach is that the hard candidates in these works are not propositional formulas, but rather purely algebraic instances (e.g., $x_1 + \cdots + x_n + 1 = 0$) that cannot be directly translated to propositional logic (cf. [16] for a discussion of this point).

In 2021, a breakthrough super-polynomial algebraic circuit lower bound against constant-depth algebraic circuits was shown by Limaye, Srinivasan and Tavenas [34] for large enough fields, and very recently has been extended by Forbes [17] to fields of characteristic p for any prime p. This motivates the question of whether a similar super-polynomial *p*roof size lower bound holds for constant-depth IPS, where the certificate is a constant-depth algebraic circuit. Some progress on this question has been made in recent work [5, 23, 26], but it remains open whether there are unsatisfiable CNF formulas (or propositional logic formulas more generally) requiring super-polynomial constant-depth IPS proofs.

1.3 Framework and Results

While most lower bounds in propositional proof complexity for concrete tautologies rely on combinatorial or algebraic techniques, one can also try to use logic – specifically, diagonalization – for this purpose. This is a natural idea, but in the propositional setting it faces an inherent obstacle: self-reference. Suppose that a formula Φ expresses a proof-complexity lower bound. Ideally, one would like Φ to encode the statement that "Φ itself has no short proofs." This, however, is impossible: any reasonable propositional encoding of Φ must use at least $|\Phi|$ symbols, so Φ would necessarily be longer than itself.[2]

One way to circumvent this problem, due to Krajíček, is to encode proofs implicitly, and hence more economically, via a circuit that computes the bits of the proof given their index (see [32]).

Santhanam–Tzameret [54] proposed a different approach: instead of referring to itself directly, a formula refers to a smaller version of itself. Concretely, they introduced the *iterated lower bound formulas*, which encode inductively the statement that "the previous-level formula has no short proof," thus avoiding direct self-reference. This yields diagonalization-based formulas that provably lack short proofs infinitely often. Specifically, if at level ℓ the formula

$$\varphi_\ell := \text{“there is no short proof of } \varphi_{\ell-1}\text{”}$$

has either a long proof or a short proof, then in both cases it establishes the truth of the no-short-proof claim for $\varphi_{\ell-1}$. If φ_ℓ has no proof at all, then in particular it has no short proof. Thus, we are done: either φ_ℓ or $\varphi_{\ell-1}$ has no short proof, and this holds for infinitely many ℓ.

By referring to a smaller (and therefore different) version of itself, the resulting formulas demonstrate that φ_ℓ has no short proofs infinitely often. However, this still leaves open whether these formulas are hard tautologies or not tautologies at all (and thus vacuously unprovable). Let us elaborate on the difference between showing that a statement is not easy, and showing that it is hard, i.e., that it is a tautology with no short proofs.

In general, given a proof system, every propositional formula φ falls into one of three categories: 1. a tautology with a short proof (easy), 2. a tautology without short proofs (hard), or 3. not a tautology (hence unprovable). This is depicted in Table 1.

[2] Friedman [19] and Pudlak [40, 41] show how to adapt the proof of Gödel's Second Incompleteness Theorem to give *s*ub-linear proof size lower bounds for strong enough propositional proof systems.

Table 1 A priori, every propositional formula falls into one of the cells labeled 1, 2, or 3.

Proof Complexity ↓ / Validity →	Tautology	Non-tautology
Easy	1. easy formula	**X**
Hard	2. hard formula	**X**
Unprovable	**X**	3. trivially unprovable

The standard aim in proof complexity is to establish hardness, i.e., to identify a formula in cell 2. For strong proof systems this remains open. Thus, a natural intermediate step is *ruling out that a formula is easy* (cell 1), while leaving open whether it belongs to cell 2 or 3. For this to be meaningful, one must consider sequences of formulas whose tautological status is unknown. A natural choice is formulas expressing open lower bounds in complexity theory. This viewpoint was emphasised by Razborov [52], who highlighted the importance of studying the proof complexity of natural statements whose validity is unknown. This approach was pursued in the 1990s by Razborov and others [48, 49, 51, 52] (see also Krajíček [33] and Raz [43]).[3]

In this work, as in [54], we follow this approach. We show that a family of DNF formulas of unknown validity has no short proofs. This situation is illustrated in Table 2.

Table 2 The DNF formula under consideration in this paper is shown to lie in either cell 2 or cell 3; in particular, we *rule out* the possibility that it is in cell 1 (with respect to the proof system $\mathrm{AC}^0[p]$-Frege).

Proof Complexity ↓ / Validity →	Tautology	Non-tautology
Easy	1. **X**	**X**
Hard	2. hard formula	**X**
Unprovable	**X**	3. trivially unprovable

There is another reason to consider statements of unknown validity when proving lower bounds for strong systems: very few plausible hard candidates are known for Frege and Extended Frege. The only compelling ones are random CNFs and circuit lower bound formulas, and for neither do we have effective methods for certifying validity. Indeed, confirming the validity of a fixed formula ϕ typically requires a proof, and existing proof methods can usually be captured in polynomial-size Frege or Extended Frege proofs – implying that ϕ is not a plausible hardness candidate for these systems.

As mentioned above, iterated lower bound formulas provide a simple way to show that a sequence of formulas is not easy. However, unlike formulas asserting SAT $\notin$ P/poly, it is unclear whether there is any reason to believe they are tautologies. What [54] demonstrated is that assuming some circuit lower bounds one can go beyond the iterated lower bound formulas: rule out that some formulas are easy for formulas that are *more likely to be tautologies* – specifically, formulas expressing that proving algebraic *circuit* lower bounds is hard. In particular, [54] combined the diagonalization framework with the [24] reduction from proof complexity to circuit lower bounds that showed that a proof-size lower bound implies an algebraic circuit-size lower bound (VP $\neq$ VNP). Hence, instead of stating recursively

[3] Typically, these propositional formulas are known unconditionally to be tautologies for random objects. For example, if a formula encodes a circuit lower bound for some Boolean function f, then for random f the lower bound holds. Thus, while the interesting candidate formula stating, say, SAT $\not\subseteq$ P/poly is not known to be a tautology, for a random f the statement $f \notin$ P/poly is.

that lower bounds are hard to prove, one formulates φ to be the statement "there are no short proofs of algebraic circuit lower bounds of the Permanent". This avoids the recursively defined statement of the iterated lower bound formulas, and is a statement whose validity is easier to assess and use. In this way we obtain:

$$\text{circuit lower bound} \;\Rightarrow\; \text{no short proof of } \overbrace{\text{`no short proof of the circuit lower bound'}}^{\varphi}.$$

However, this still leaves an extra conditional layer: we need to rely on VP $\neq$ VNP (the circuit lower bound) to rule out that φ is easy.

In the present work, we eliminate this conditionality in the constant-depth regime. Using the unconditional constant-depth algebraic circuit lower bound of Limaye, Srinivasan and Tavenas [34], we extend the diagonalization framework to constant-depth circuits.

We demonstrate formulas that *unconditionally* are not easy for AC^0[p]-Frege, such that:

- **Plausibly tautologies:** we give some evidence supporting the validity of these formulas;
- **Necessary (complete):** any hard instance for a sufficiently strong proof system must imply that our formulas are also not easy for that system;
- **Amplifying:** exhibiting a form of existential depth amplification: there exists a constant d, such that if our formulas are hard for depth-d proofs then they are hard for *every* constant-depth d' proofs.

▶ **Theorem 1** (Corollary of the more formal Theorem 2 below)**.** *For every prime p there is an explicit sequence $\{\phi_n\}$ of DNF formulas (of unknown validity) such that there are no polynomial-size* AC^0[p]*-Frege proofs of $\{\phi_n\}$.*

As mentioned above, Theorem 1 is shown via a diagonalization argument applied to the algebraic proof system IPS. It exploits the lower bound in [34] and Forbes' finite fields version [17], and the fact that Grochow-Pitassi [24] showed that constant-depth IPS over finite prime fields simulates AC^0[p]-Frege.

The formulas ϕ_n express proof size lower bounds for algebraic proof systems, and the evidence for their validity comes from several sources.

▶ Remark (Switching between DNF tautologies and unsatisfiable CNF formulas). Since we work with the *refutation* system IPS (whose constant-depth version simulates AC^0[p]-Frege), it is more natural to consider CNF formulas that are conjectured to be unsatisfiable, rather than DNF formulas that are conjectured to be valid. This is a matter of convenience, because of the trivial equivalence between showing that a CNF is unsatisfiable and showing that its complementary DNF is valid. We sometimes abuse notation and use "refutations" and "proofs" interchangeably; in all cases, the exact meaning should be clear from the context.

The CNF formulas we consider are related to the circuit lower bound formulas considered by Razborov [48, 49, 51, 52], but with two differences: we consider *a*lgebraic rather than Boolean circuits, and our formulas express lower bounds for *p*roving constant-depth algebraic lower bounds in constant-depth IPS, rather than express the circuit lower bounds directly. This allows us to adapt the diagonalization technique used to show an equivalence between circuit complexity and proof complexity in [54] to derive an *u*nconditional proof complexity lower bound in our setting.

To state our result more precisely we need the following notation. Let $\mathbb{F}$ be some underlying (finite) field. We let:

- $\mathrm{ckt}_d(\mathrm{perm}_n, s)$: a CNF formula expressing that the Permanent on $n \times n$ matrices has depth-d algebraic circuits of size s over $\mathbb{F}$.
- ref-$\mathrm{IPS}_d(\phi, t)$: a CNF formula expressing that ϕ has size-t IPS refutations of depth-d over $\mathbb{F}$.
- The ***diagonalizing CNF formula*** is:

$$\psi_{d,d',n} := \text{ref-IPS}_{d'}(\mathrm{ckt}_d(\mathrm{perm}_n, n^{O(1)}), N^{O(1)}),$$

where $N = |\mathrm{ckt}_d(\mathrm{perm}_n, n^{O(1)})|$ is $O(2^{n^{O(1)}})$, expressing that depth-d' IPS refutes in polynomial-size that the permanent is computed by a depth-d algebraic circuit of polynomial-size.

The use of $O(1)$ in the notation above is informal. We use it to avoid using more quantifiers that would make the statement below hard to parse.

▶ **Theorem 2** (Informal Statement; Theorem 32)**.** *For every constant prime p and for all positive integers d, there is a positive integer d' such that for all positive integers d'', there are no polynomial-size depth-d'' IPS refutations of the formula $\psi_{d,d',n}$, for infinitely many n over $\mathbb{F}_p$.*

Theorem 2 states the existence of no polynomial constant-depth IPS refutations for formulas that themselves express constant-depth IPS short refutation of constant-depth circuit upper bounds.

Here the size of a proof is always measured as a function of the length of the formula being proved. The result holds for any finite field, and further for sequence of prime fields of increasing size that are not too large, as we show below in Theorem 7.

Theorem 1 follows from Theorem 2 as follows: i) take the same p as in the statement of Theorem 2; ii) let the formulas ϕ_n in the former result to be the negation of $\psi_{d,d',n}$ in the latter result[4], where d (the stated depth of circuit computing Permanent) is chosen to be large enough and d' (the stated depth of IPS refutations) is chosen as a function of d so that Theorem 2 holds; iii) finally, use the fact that constant-depth IPS over fields of characteristic p simulates $\mathrm{AC}^0[p]$-Frege [24].

1.3.1 Implications and Several Important Aspects of Theorem 2

1.3.1.1 Supporting evidence for the unsatisfiability of the diagonalizing CNF formula

We describe three forms of supporting evidence that $\psi_{d,d',n}$ is unsatisfiable.

(I) Hardness of multilinear algebra for constant-depth proofs. To establish the unsatisfiability of $\psi_{d,d',n}$, it suffices to show that constant-depth algebraic circuit upper bound formulas do not admit small-size constant-depth IPS refutations.

The tensor rank principle denoted $\mathrm{TRankP}^r_{m,n}(A)$ and introduced in [20], states that an order-r tensor A of rank m can be written as the sum of n rank-1 tensors of order r. This principle is easily shown to be unsatisfiable when $m > n$.

[4] We take negation because we consider $\mathrm{AC}^0[p]$-Frege to be a *proof* system for DNF tautologies, while constant-depth IPS is a *refutation* system for unsatisfiable CNFs.

In [20], the tensor rank principle is used to derive the corresponding *constant-depth* algebraic circuit upper bound formulas within constant-depth IPS, showing that these upper bounds follow from the principle itself. As a result, proving super-polynomial-size lower bounds for the tensor rank principle against constant-depth IPS implies the unsatisfiability of the diagonalizing CNF formula:

▶ **Corollary 3** ([20]; informal, see Corollary 6.6 in the full version [35]). *If the sequence of CNF formulas $\psi_{d,d',n}$ are satisfiable then the tensor rank principle* $\mathrm{TRankP}^r_{m,n}(A)$ *admits polynomial-size refutations in depth-$O(d')$ IPS.*

It is known from [34, 17] that the determinant cannot be computed by polynomial-size constant-depth algebraic circuits over any field. Consequently, following the informal alignment between proof complexity and circuit complexity, one expects that proof systems operating with constant-depth algebraic circuits cannot efficiently prove statements expressing linear (or multilinear) algebraic properties (whose standard proofs use notions like rank and determinants). Therefore, it is reasonable to expect that $\mathrm{TRankP}^r_{m,n}(A)$ does not admit polynomial-size refutations in constant-depth IPS, and hence, that $\psi_{d,d',n}$ is unsatisfiable by the corollary.

(II) Weaker versions of the CNF that are provably unsatisfiable. To establish the unsatisfiability of $\psi_{d,d',n}$, it suffices to show that constant-depth algebraic circuit upper bound formulas do not admit small-size constant-depth IPS refutations. Here we mention two recent results that establish this for weaker variants of $\psi_{d,d',n} = \text{ref-IPS}_{d'}(\mathrm{ckt}_d(\mathrm{perm}_n, n^{O(1)}), N^{O(1)})$, namely when the proof system is Polynomial Calculus with Resolution (PCR) instead of depth-d' IPS (denoted "$\mathrm{IPS}_{d'}$" in $\psi_{d,d',n}$) and when the lower bound statement is against either algebraic circuits of unrestricted depth instead of general algebraic circuits (denoted "ckt_d" in $\psi_{d,d',n}$), or against noncommutative algebraic branching programs.

The refutation system PCR can be considered roughly as depth-2 IPS (see [24]). Note that when we increase the strength of the algebraic circuit model replacing ckt_d in $\psi_{d,d',n}$, we are actually *weakening* the statement, since proving lower bounds against stronger circuit model is *harder*, meaning that it is *easier* to show that such lower bounds are harder.

▶ **Corollary 4** ([20]; See Theorem 6.10 in the full version [35]). *Let f be any polynomial in n variables over $\mathbb{F}_2$. The CNF formula* $\text{ref-PCR}(\mathrm{ckt}(f, n^{O(1)}), N^{O(1)})$, *stating that* PCR *over $\mathbb{F}_2$ has a polynomial-size refutation of the statement that f is computable by polynomial-size algebraic circuits, is unsatisfiable.*

When the proof system in $\psi_{d,d',n}$ is weakened again to PCR instead of depth-d' IPS, while the algebraic circuit model is very weak (which *strengthens* the proof complexity lower bound statement), namely, noncommutative algebraic branching program (denoted ncABP), we have the following:

▶ **Corollary 5** ([21]). *Let f be any noncommutative polynomial in n variables over $\mathbb{F}_2$. The CNF formula* $\text{ref-PCR}(\mathrm{ncABP}(f, n^{O(1)}), N^{O(1)})$, *stating that* PCR *over $\mathbb{F}_2$ has polynomial-size refutations of the statement that f is computable by polynomial-size noncommutative algebraic branching programs, is unsatisfiable.*

Corollary 5 is proved via a reduction similar to the reduction from iterated proof complexity generators to Boolean circuit upper bound formulas in [52]. Since an algebraic branching program is characterized by iterated matrix multiplication, one can reduce the iterated rank principle to the ncABP upper bound formulas [21]. Thus, Corollary 5 follows by an exponential lower bound for the iterated rank principle.

(III) Algebraic analogues of proof complexity conjectures. Krajíček [33] and Razborov [50, 53] have conjectured the following:[5] Extended Frege cannot efficiently prove *a*ny super-polynomial Boolean circuit lower bound. Since Extended Frege is essentially a proof system that operates with Boolean circuits, this conjecture says that proof systems operating with Boolean circuits cannot efficiently prove Boolean circuit lower bounds. We raise the following analogous conjecture:

> **Constant-depth algebraic analogue of Krajíček-Razborov conjecture:** For every d, there is a d' such that there are no polynomial-size depth-d' IPS proofs of super-polynomial depth-d lower bounds for *a*ny polynomial f.

(Of course, the conjectured statement above depends on a natural encoding or formulation of the lower bound statement.)

The constant-depth algebraic analogue of the Krajíček-Razborov conjecture implies the unsatisfiability of the CNF formulas $\psi_{d,d',n}$ for arbitrary d and large enough d'.

The formulas $\psi_{d,d',n}$ assert this only for $f = \text{perm}$, and therefore follow trivially from the conjecture.

1.3.1.2 Diagonalizing formulas are necessary for lower bounds

We show that the diagonalizing formulas are not easy is *logically necessary* in order to prove super-polynomial lower bounds for $\mathcal{C}$-IPS for *any* "reasonable" algebraic circuit class $\mathcal{C}$. In other words, we show that the non-easiness of the diagonalizing formulas is implied by *a*ny super-polynomial lower bounds on tautologies for algebraic proofs operating with circuits from $\mathcal{C}$. To show this, we use the circuits-to-proofs connection of [24].

The notation $\mathcal{C}$-IPS stands for the IPS proof system in which an IPS refutation (i.e., certificate) is written as an algebraic circuit from the class $\mathcal{C}$ (for instance, depth-d circuits, for a constant d, algebraic formulas, etc.). A "reasonable" algebraic circuit class $\mathcal{C}$ is one for which the Grochow-Pitassi implication from $\mathcal{C}$-IPS lower bounds to $\mathcal{C}$ circuit lower bounds holds, and moreover this implication is efficiently provable in $\mathcal{C}$-IPS. Our methods in this paper imply that all the commonly studied algebraic circuit classes which contain the class of constant-depth algebraic circuits are reasonable.

▶ **Theorem 6** (Informal; Theorem 38; If algebraic proofs are not p-bounded then it is not easy to prove that circuit lower bounds are hard for algebraic proofs.)**.** *Let $\mathcal{C}$ be any "reasonable" algebraic circuit class. If there is a sequence $\{\phi_n\}_n$ of unsatisfiable CNF formulas that requires super-polynomial size $\mathcal{C}$-*IPS *proofs for infinitely many n, then the sequence $\{\psi_n\}_n$ of CNF formulas does not have polynomial size $\mathcal{C}$-*IPS *proofs for infinitely many n, where $\psi_n = \text{ref-}\mathcal{C}\text{-IPS}(\mathcal{C}\text{-ckt}(\text{perm}_n, n^{O(1)}), N^{O(1)})$, with $N = |\mathcal{C}\text{-ckt}(\text{perm}_n, n^{O(1)})|$.*

Theorem 6 is shown by abstracting the argument of Theorem 2 and combining the resulting generalization with the Grochow-Pitassi implication from proof complexity lower bounds to circuit complexity lower bounds [24].

[5] Razborov conjectured in [52] that Frege cannot efficiently prove super-polynomial circuit lower bounds for any Boolean function. More specifically, [52, Conjecture 1] with suitable parameters for the underlying combinatorial designs implies under some hardness assumptions that Frege cannot efficiently prove that SAT$\not\subseteq$ 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. [45, 46, 29]).

1.3.1.3 Existential depth amplification

The statements $\psi_{d,d',n}$ themselves refer to proof complexity lower bounds. Nevertheless, the lower bounds stated in the formulas and the lower bounds we get from our result are *different*.

First, the formulas state hardness of proving circuit lower bounds, while we get hardness of proving *proof complexity lower bounds*.

Second, notice the quantification over depths in Theorem 2: there is some *f*ixed depth d' such that if depth-d' IPS lower bounds on certain circuit lower bounds for the Permanent hold, then we get super-polynomial lower bounds for proofs of *a*ny constant depth. This shows that we can escalate the depth-d' IPS lower bounds stated in the formulas to *any* constant-depth IPS lower bounds. In other words, our result does not merely repeat the stated lower bound we assumed against depth-d' proofs of circuit lower bounds, but goes beyond it to rule out short proofs in *any* depth of proof complexity lower bounds.

1.3.2 Extension to Larger Fields

While [54] and Theorem 2 crucially use fields of constant size, and the ability to efficiently encode computation over finite fields of constant size by CNF formulas, we show further how to encode and reason about larger and growing fields. This technical contribution may be interesting on its own right.

Specifically, by reasoning about the bits of polynomial expressions with algebraic proofs, Theorem 2 can be extended to underlying fields of size polynomially bounded by $|\psi_{d,d',n}|$. Bit arithmetic in proof complexity was used before (cf. [22, 12, 4, 27]). We show how to reason about iterated addition, iterated multiplication and modular arithmetic in constant-depth IPS over polynomial-size fields.

▶ **Theorem 7** (Informal Statement; Corollary 39). *Let $\{p_n\}$ be any sequence of primes such that $p_n = O(2^n)$, and $\mathbb{F}_{p_n}$ be the field of size p_n. For all positive integers d, there is a positive integer d' such that for all positive integers d'', there are no polynomial-size depth-d'' IPS refutations of the formula $\psi_{d,d',n} = \text{ref-IPS}_{d'}(\text{ckt}_d(\text{perm}_n, n^{O(1)}), N^{O(1)})$ for infinitely many n over $\mathbb{F}_{p_n}$, where $N = |\text{ckt}_d(\text{perm}_n, n^{O(1)})|$ is $O(2^{n^{O(1)}})$.*

1.3.3 The Diagonalization Argument

Here we explain informally the idea behind the proof of Theorem 2, showing that the diagonalizing CNFs have no short refutations. This is where most of the nontrivial technical work lies. The key idea is to combine diagonalization with the known implication from proof complexity lower bounds to circuit complexity lower bounds [24].

The argument builds on the following three nontrivial technical points:

1. There is a reasonable CNF encoding expressing that the permanent polynomial can be computed by bounded-depth small-size algebraic circuits "VNP = VAC^0" (this is $\text{ckt}_d(\text{perm}_n, n^{O(1)})$ from before).[6]
2. There is a reasonable CNF encoding of the statement that there are constant-depth IPS refutations of size s for a CNF ϕ (this is ref-IPS$_d(\phi, t)$ from before).

[6] We use VAC^0 to denote Valiant's analogue of AC^0, in the same way that VP and VNP correspond to P and NP. The class VAC^0 consists of families of polynomials computable by constant-depth, polynomial-size algebraic circuits.

3. If ϕ is unsatisfiable and there are short and constant-depth IPS refutations of "constant-depth IPS efficiently refutates ϕ", then there are short and constant-depth IPS refutations of "VNP = VAC^0".

The work of [54] formalized the Grochow-Pitassi implication from IPS lower bounds for CNFs to VNP $\neq$ VP within IPS. Assumption 3 above is a novel formalisation of a *constant-depth* version of the Grochow-Pitassi implication within constant-depth IPS.

According to [34], the permanent polynomial cannot be computed by constant-depth small-size algebraic circuits, which means "VNP = VAC^0" is an unsatisfiable CNF, using Assumption 1. Assume for the sake of contradiction that $\psi_{d,d',n}$, namely, ref-$\mathrm{IPS}_{d'}$("VNP = VAC^0", poly) (or more formally, ref-$\mathrm{IPS}_{d'}(\mathrm{ckt}_d(\mathrm{perm}_n, n^{O(1)}), N^{O(1)})$) has polynomial-size refutations in constant-depth IPS. Then by Assumption 3, "VNP = VAC^0" has polynomial-size constant-depth IPS refutations. But this contradicts the soundness of IPS, since IPS has (polynomial-size) refutations of the statement that "VNP = VAC^0" has polynomial-size IPS-refutations (formally, one has to account for instances of different sizes when following this argument, and we explain this more precisely below).

To clarify further the argument, we describe a slightly more detailed overview, highlighting the logic behind the argument. We show that infinitely often there are no polynomial-size constant-depth IPS refutations of the formula ref-$\mathrm{IPS}_{d'}(\mathrm{ckt}_d(\mathrm{perm}_n, n^c), n^{c'})$, expressing that there exists a constant c' such that $\mathrm{ckt}_d(\mathrm{perm}_n, n^c)$ has IPS refutations of size bounded from above by the polynomial $n^{c'}$ and depth bounded by d'.

Proof sketch of Theorem 2 (formally Theorem 32). Let i.o. abbreviate *infinitely often*, and let a.e. denote its converse *almost everywhere*, that is, "always except for finite many cases". Let $G \vdash_d^{f(n)} 1 = 0$ stands for an IPS refutation of G of refutation-size bounded by $f(n)$ and refutation-depth bounded by d. Our goal is to prove:

$$\forall\, c, d\ \exists\, c', d'\ \forall\, c'', d''\ \text{i.o.}\ \underbrace{\text{ref-IPS}_{d'}(\overbrace{\mathrm{ckt}_d(\mathrm{perm}_n, n^c)}^{\gamma}, |\gamma|^{c'})}_{\lambda} \nvdash_{d''}^{|\lambda|^{c''}} 1 = 0, \tag{1}$$

meaning that for all constants c, d there are constants c', d', such that for all constants c'', d'', λ does not have polynomial-size $|\lambda|^{c''}$ and constant depth d'' refutation, infinitely often.

Assume by way of contradiction that the converse holds, namely:

$$\exists\, c, d\ \forall\, c', d'\ \exists\, c'', d''\ \text{a.e.}\ \underbrace{\text{ref-IPS}_{d'}(\overbrace{\mathrm{ckt}_d(\mathrm{perm}_n, n^c)}^{\gamma}, |\gamma|^{c'})}_{\lambda} \vdash_{d''}^{|\lambda|^{c''}} 1 = 0, \tag{2}$$

Using the bounded-depth version of the argument of [24] (i.e., Item 3 above), we get that if VNP has polynomial-size depth-d circuits, then depth-d IPS is polynomially bounded, namely:

$$\exists c_1, d_1\ \underbrace{\mathrm{ckt}_d(\mathrm{perm}_{|\gamma|}, |\gamma|^c)}_{\gamma'} \vdash_{d_1}^{|\gamma'|^{c_1}} \text{ref-IPS}_d(\mathrm{ckt}_d(\mathrm{perm}_n, n^c), |\gamma|^c) \vdash_{d''}^{|\lambda|^{c''}} 1 = 0,$$

where $|\lambda|$ is polynomially bounded by $|\gamma'|$. The second part from left of the refutation above is given by the fact that ref-$\mathrm{IPS}_{d'}(\mathrm{ckt}_d(\mathrm{perm}_n, n^c), |\gamma|^{c'})$ can be efficiently refuted in bounded-depth IPS for any d' and c'. Hence, we take d' to be d and c' to be c, yielding the second part of the refutation above.

Therefore, in particular, by combining the two proofs into one, we get

$$\exists c_2, d_2 \ \mathrm{ckt}_d(\mathrm{perm}_{|\gamma|}, |\gamma|^c) \vdash_{d_2}^{|\gamma'|^{c_2}} 1 = 0.$$

Thus,

$$\exists c_2, d_2, \ \underbrace{\text{ref-IPS}_{d_2}(\mathrm{ckt}_d(\mathrm{perm}_{|\gamma|}, |\gamma|^c), |\gamma'|^{c_2})}_{\Lambda}$$

is a *satisfiable* CNF formula. Since Equation (2) holds almost everywhere, we can take n to be $|\gamma|$. Then, by taking d' to be d_2 and c' to be c_2 in Equation (2),

$$\exists C, D \ \underbrace{\text{ref-IPS}_{d_2}(\mathrm{ckt}_d(\mathrm{perm}_{|\gamma|}, |\gamma|^c), |\gamma'|^{c_2})}_{\Lambda} \vdash_D^{|\Lambda|^C} 1 = 0,$$

which means Λ is refutable. By the soundness of IPS, Λ is unsatisfiable which is a contradiction. ◀

1.4 Relation to Previous Work and Conclusion

Theorem 1 gives a first instance in which a formula whose validity is unknown is shown unconditionally to have no short proofs in AC^0[p]-Frege. Razborov [50] and Krajíček [33] *c*onjecture that all Boolean circuit lower bound formulas are hard for EF, but this is open even for AC^0-Frege and even when we relax hardness to being non-easy (as we do in our work). Our lower bound is for *p*roof complexity lower bound formulas rather than for circuit lower bound formulas, but our work is somewhat similar in spirit to [48].

From a technical point of view, our work is related to recent works by [54, 36], which also use diagonalization ideas. The main result of [54] is a *c*onditional existence of hard formulas for IPS, under the assumption that VNP $\neq$ VP. In contrast, our result ruling out easy formulas for constant-depth IPS, i.e., Theorem 2, is unconditional. One way to interpret our result is that it strengthens the equivalence between proof complexity lower bounds and circuit complexity lower bounds shown in [54] to hold for constant-depth circuits, and then applies the recent breakthroughs constant-depth algebraic circuit lower bounds [34, 17] to get unconditional proof complexity lower bounds.

Unconditional lower bounds for conjectured tautologies are also shown in [37] using a somewhat different diagonalization technique, however these are for highly non-explicit formulas[7], and do not seem directly relevant to progress on lower bounds for tautologies. In contrast, Theorem 6 shows that Theorem 2 is a *n*ecessary step toward super-polynomial lower bounds for constant-depth IPS.

One novel aspect in Theorem 1 is that a proof complexity lower bound for a propositional proof system is shown via *a*lgebraic circuit lower bounds. The theory of feasible interpolation in propositional proof complexity enables proof complexity lower bounds for weak systems such as Resolution and Cutting Planes to be derived from lower bounds on monotone circuit complexity [10, 28, 42]. However, there is cryptographic evidence against the applicability of feasible interpolation techniques to AC^0-Frege and stronger proof systems [11]. Implications from average-case circuit lower bounds to proof size lower bounds for strong systems were conjectured by Razborov [52] in the context of *p*roof complexity generators [3], but these conjectures are so far unproven.

[7] There are two sources of non-explicitness in [37]. First, they consider a *d*istribution on conjectured hard formulas rather than a fixed hard formula at every length. Second the formulas refer to a non-constructively defined proof system with non-uniform verification.

We note that the question of proving proof complexity lower bounds for constant-depth IPS has in itself been highlighted and studied in recent works [5, 23, 26, 16, 8]. Andrews and Forbes [5] show a super-polynomial constant-depth IPS lower bound for refuting certain sets of polynomial equations. However, their hard instances do not themselves have polynomial-size constant-depth circuits, and in particular are not CNFs. Govindasamy, Hakoniemi and Tzameret [23] give a super-polynomial multilinear constant-depth IPS lower bound for refuting polynomial equations expressible as small depth-2 algebraic circuits. Hakoniemi, Limaye and Tzameret [26] extend and strengthen these results from multilinear to low individual degree proofs [23]. However, they also show that the lower bound framework of [23, 26] is incapable of proving lower bounds for CNFs. Elbaz, Govindasamy, Lu and Tzameret [16] showed that any constant-depth IPS lower bounds over finite fields would lead to lower bounds for CNF formulas and thus $\mathrm{AC}^0[p]$-Frege lower bounds. Alas, the strongest constant-depth IPS lower bounds [26] are restricted to low individual degree refutations, for which the result of [16] do not hold. Proving lower bounds for CNFs is essential for the application to $\mathrm{AC}^0[p]$-Frege lower bounds, and none of the previous works achieve this. Our work provides an explicit CNF formula with no short refutations and with some evidence for its unsatisfiability.

2 Preliminaries

2.1 Algebraic Complexity

Let $\mathbb{F}$ be a field. Denote by $\mathbb{F}[\overline{x}]$ the field of polynomials with coefficients from $\mathbb{F}$ and variables $\overline{x} = [x_1, \cdots, x_n]$. 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. We assume some familiarity with algebraic complexity. Basic definition in algebraic complexity can be found in [55].

▶ **Definition 8** (Iterated Matrix Multiplication). *Let n and d be such that $N = dn^2$. The* Iterated Matrix Multiplication $\mathrm{IMM}_{n,d}$ *on $N = dn^2$ variables is defined as the following polynomial. The underlying variables are partitioned into d sets $X_1, \cdots, X_d$ of size n^2, each of which is represented as an $n \times n$ matrix with distinct variable entries. Then $\mathrm{IMM}_{n,d}$ is defined to be the polynomial that is the $(1,1)$th entry of the product matrix $X_1 \cdot X_2 \cdots X_d$.*

Iterated Matrix Multiplication is in VP.

▶ **Theorem 9** (Super-polynomial lower bounds against constant-depth circuits over large field [34]). *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 $n^{d^{\exp -O(\Delta)}}$.*

This lower bound for IMM against constant-depth circuits was improved in [9]. Let $\mu(\Delta) = 1/(F(\Delta) - 1)$, where $F(n) = \Theta(\varphi^n)$ is the nth Fibonacci number (starting with $F(0) = 1$, $F(1) = 2$) and $\varphi = (1 + \sqrt{5})/2$ is the golden ratio.

▶ **Theorem 10** ([9]). *Fixed a field $\mathbb{F}$ of characteristic 0 or greater than d. Let N, d, Δ be such that $d = O(\log / \log\log N)$. Then, any product-depth Δ circuit computing $\mathrm{IMM}_{n,d}$ on $N = dn^2$ variables must have size at least $N^{\Omega(d^{\mu(2\Delta)}/\Delta)}$.*

A recent result by Forbes [17] extended these results to *any* field, including finite fields.

▶ **Corollary 11** (Super-polynomial lower bounds on constant-depth circuits over any field [17]). *Let $\mathbb{F}$ be any field, and $d = o(\log n)$. Then the iterated matrix multiplication polynomial $\mathrm{IMM}_{n,d}$ where X_i requires*

$$n^{\Theta(d^{\mu(2\Delta)}/\Delta)}$$

size algebraic circuits of product depth Δ.

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.

▶ **Theorem 12** (No polynomial-size constant depth circuits for the Permanent [34, 17]). *Let $\Delta \geq 1$ and let $\mathbb{F}$ be any 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 with n, for sufficiently large n.*

2.2 Ideal Proof System

Given $f_1, \cdots, f_m \in \mathbb{F}[x_1, \cdots, x_n]$ over some field $\mathbb{F}$, Hilbert's Nullstellensatz shows that $f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0$ is unsatisfiable (over the algebraic closure of $\mathbb{F}$) if and only if there are polynomials $g_1, \cdots, g_m \in \mathbb{F}[\overline{x}]$ such that $\sum_j g_j(\overline{x}) f_j(\overline{x}) = 1$ (as a formal identity), or equivalently, that 1 is in the ideal generated by the $\{f_j\}_j$.

▶ **Definition 13** ((Boolean) Ideal proof system (IPS) [24]). *Let $f_1(\overline{x}), \cdots, f_m(\overline{x}), p(\overline{x}) \in \mathbb{F}[x_1, \cdots, x_n]$ 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 $C(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{F}[\overline{x}, y_1, \cdots, y_m, z_1, \cdots, z_n]$, such that (the equalities in what follows stand for formal polynomial identities[8])*

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

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 a placeholder 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 this is called a $\mathcal{C}$-*IPS *refutation.*

We shall also use the algebraic version of IPS(which does not use the Boolean axioms):

▶ **Definition 14** ((Algebraic) Ideal proof system (IPS$^{\mathrm{alg}}$) [24]). *Let $f_1(\overline{x}), \cdots, f_m(\overline{x}), p(\overline{x}) \in \mathbb{F}[x_1, \cdots, x_n]$ be a collection of polynomials. An* IPS$^{\mathrm{alg}}$ *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 assignments by field elements, is an algebraic circuit $C(\overline{x}, \overline{y}) \in \mathbb{F}[\overline{x}, y_1, \cdots, y_m]$, such that*

1. $C(\overline{x}, \overline{0}) = 0$.
2. $C(\overline{x}, f_1(\overline{x}), \cdots, f_m(\overline{x})) = p(\overline{x})$.

The size and refutation are defined similarly to Definition 13.

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

Now, we introduce some notation we will use in the following sections. Let $\overline{\mathcal{F}} = \{f_i(\overline{x}) = 0\}_{i=1}^m$ be a collection of circuit equations, namely the f_i's are written as algebraic circuits. We use $|\overline{\mathcal{F}}|$ to denote the total size of the circuit equations in $\overline{\mathcal{F}}$. We denote by $C : \overline{\mathcal{F}} \vdash_{\text{IPS}}^{s,\Delta} 1 = 0$ the fact that $\overline{\mathcal{F}}$ has an IPS refutation C of size at most s and depth at most Δ. If we do not care about the explicit size of the IPS refutation, we denote by $C : \overline{\mathcal{F}} \vdash_{\text{IPS}}^{*,\Delta} 1 = 0$ the fact that $\overline{\mathcal{F}}$ has an IPS refutation C of size polynomially bounded by $|\overline{\mathcal{F}}|$ and of depth Δ.

When we deal with algebraic IPS refutations, we will use the same notation as above, only using IPS^{alg} instead of IPS.

Polynomial identities are proved for free in IPS, which was observed in [4], and this also holds for constant-depth IPS proofs.

▶ **Proposition 15.** *If $C(\overline{x})$ is a Depth-Δ algebraic circuit in the variables $\overline{x}$ over the field $\mathbb{F}$ that computes the zero polynomial, then there is an Depth-Δ* IPS *proof of $C(\overline{x}) = 0$ of size $|F|$.*

The following theorem is from [24], and it already holds for IPS^{alg}.

▶ **Theorem 16** (Superpolynomial IPS lower bounds imply VNP $\neq$ VP [24])**.** *For any field $\mathbb{F}$, a superpolynomial lower bound on* IPS^{alg} *(also* IPS*) refutations over $\mathbb{F}$ for any family of* CNF *formulas implies* $\text{VNP}_{\mathbb{F}} \neq \text{VP}_{\mathbb{F}}$*. The same result holds if we assume that the* IPS^{alg} *(*IPS*) refutation size lower bound holds only infinitely often.*

▶ **Lemma 17** ([24])**.** *Every family of unsatisfiable* CNF *formulas (φ_n) has a family of* IPS^{alg} *(also* IPS*) certificates (C_n) in* $\text{VNP}_{\mathbb{F}}$*.*

2.3 Encoding in Fixed Finite Fields

In the section, we are working in the finite field $\mathbb{F}_q$ where q is a constant (independent of the size of the formulas and their number of variables). When we work with CNF formulas in IPS we assume that the CNF formulas are translated as follows:

▶ **Definition 18** (Algebraic translation of CNF formulas)**.** *Given a* CNF *formula in the variables $\overline{x}$, every clause $\bigvee_{i\in P} x_i \vee \bigvee_{j\in N} \neg x_j$ is translated into $\prod_{i\in P}(1-x_i)\cdot\prod_{j\in N} x_j = 0$. (Note that these terms are written as algebraic circuits as displayed, where products are not multiplied out.)*

Notice that a CNF formula is satisfiable by 0-1 assignment if and only if the assignment satisfies all the equations in the algebraic translation of the CNF.

The following definitions are taken from [54], and we supply them here for completeness.

▶ **Definition 19** (Algebraic extension axioms and unary bits [54])**.** *Given a circuit C and a node g in C, we call the equation*

$$x_g = \sum_{i=0}^{q-1} i \cdot x_{g_i}$$

the algebraic extension axiom of g, with each variables x_{g_i} being the ith unary-bit of g.

▶ **Definition 20** (Plain CNF encoding of a bounded-depth circuit equation $\text{cnf}(C(\overline{x}) = 0)$ [54])**.** *Let $C(\overline{x})$ be a circuit in the variables $\overline{x}$. The plain* CNF *encoding of the circuit equation $C(\overline{x}) = 0$ denoted $\text{cnf}(C(\overline{x}) = 0)$ consists of the following* CNF *encoding from the Plain*

CNF encoding of bounded-depth circuits (see definition 2.28 in the full version [35]) in the unary-bits variables of all the gates in C (and only in the unary-bit variables), together with the equations:

$$x_{g_{out}0} = 1 \quad \textit{and} \quad x_{g_{out}i} = 0, \quad \textit{for all } i = 1, \cdots, q-1,$$

which express that $g_{out} = 0$, where g_{out} is the output node of C.

▶ **Definition 21** (Extended CNF encoding of a circuit equation (circuit, *resp.*); $\mathrm{ecnf}(C(\overline{x}) = 0)$ ($\mathrm{ecnf}(C(\overline{x}))$, *resp.*) [54]). *Let $C(\overline{x})$ be a circuit in the variables $\overline{x}$ over the finite filed $\mathbb{F}_q$. The extended* CNF *encoding of the circuit equation $C(\overline{x}) = 0$ (circuit $C(\overline{x})$,* resp.*), in symbols* $\mathrm{ecnf}(C(\overline{x}) = 0)$ (ecnf$(C(\overline{x}))$, resp.*), is defined to be a set of algebraic equations over $\mathbb{F}_q$ in the variables x_g and $x_{g0}, \cdots, x_{gq-1}$ which are the unary-bit variables corresponding to the node g in C, that consist of:*

1. *the plain* CNF *encoding of the circuit equation $C(\overline{x}) = 0$ (circuit $C(\overline{x})$,* resp.*), namely,* $\mathrm{cnf}(C(\overline{x}) = 0)$ (cnf$(C(\overline{x}))$, resp.*); and*
2. *the algebraic extension axiom of g, for every gate g in C.*

Using results in [16], we could remove some extension axioms used in [54] when working over fixed finite fields. We use $\mathrm{UBIT}_j(x)$ to denote the following Lagrange polynomial:

$$\mathrm{UBIT}_j(x) := \frac{\prod_{i=0, i\neq j}^{q-1}(x-i)}{\prod_{i=0, i\neq j}^{q-1}(j-i)} \tag{3}$$

where x can be a single variable or an algebraic circuit. Hence, it is easy to observe that

$$\mathrm{UBIT}_j(x) = \begin{cases} 1, & x = j, \\ 0, & \text{otherwise.} \end{cases}$$

Also, suppose x has size $|x|$ and depth $\mathrm{depth}(x)$ (when x is a single variable, it has size 1 and depth 1), $\mathrm{UBIT}_j(x)$ can be computed by an algebraic circuit of size $O(|x|^{q-1})$ and depth $\mathrm{depth}(x) + 2$.

▶ **Definition 22** (Semi-CNF SCNF encoding of a bounded-depth circuit equation $\mathrm{SCNF}(C(\overline{x}) = 0)$). *Let $C(\overline{x})$ be a circuit in the variables $\overline{x}$. The semi-CNF encoding of the circuit equation $C(\overline{x}) = 0$ denoted $\mathrm{SCNF}(C(\overline{x}))$ is a substitution instance of the plain CNF encoding in Definition 20 where each unary-bits x_{uj} of all the gates and extra extension variables*[9] *u is substituted with $\mathrm{UBIT}_j(C_u)$ where C_u is the bounded-depth algebraic circuit computed by u.*[10]

We call $x^q - x = 0$ the *field axiom* for the variable x.

▶ **Lemma 23** (Translate semi-CNFs from circuit equations in Fixed Finite Fields, [16]). *Let $\mathbb{F}_q$ be a finite field, and let $C(\overline{x})$ be a circuit of depth Δ in the $\overline{x}$ variables over $\mathbb{F}_q$. Then, the following hold*

$$\{x^q - x = 0 : x \textit{ is a variable in } C\}, C(\overline{x}) = 0 \vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} \mathrm{SCNF}(C(\overline{x}) = 0)$$

[9] These extension variables are used in Item 3 of the Plain CNF encoding of bounded-depth circuits (see definition 2.28 in the full version [35]) to help encode the circuit.

[10] This C_u can be constructed from the straight line program encoding (see Definition 2.31 in the full version [35])easily.

▶ **Lemma 24** (Translate circuit equations from semi-CNFs in fixed finite fields, [16]). *Let $\mathbb{F}_q$ be a finite field, and let $C(\overline{x})$ be a circuit of depth Δ in the $\overline{x}$ variables over $\mathbb{F}_q$. Then, the following hold*

$$\{x^q - x = 0 : x \text{ is a variable in } C\}, \mathrm{SCNF}(C(\overline{x}) = 0) \vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} C(\overline{x}) = 0$$

We will use our new translation lemma for the next section, which is our main result in fixed finite fields. For polynomial-size finite fields, we have a different translation lemma.

3 Universal Algebraic Circuits for Bounded-Depth

Here, we develop the necessary technical information regarding universal circuits. This is a novel adaptation of the work of Raz [44] to the bounded-depth setting, in which both the universal circuit and the circuits it encodes are of bounded depth.

In this section, we will work with algebraic circuits whose edges can be labelled by field elements. This does not make too much difference, as we can easily replace them with a multiplication, which only increases the depth and size of a circuit up to a factor of 2.

▶ **Theorem 25** (Existence of bounded-depth universal circuits for polynomials computed by bounded-depth circuits). *Let $\mathbb{F}$ be a field and $\overline{x}$ be n variables, and let $\mathrm{VAC}^0_{s,\Delta}$ denote the class of all polynomials in $\mathbb{F}[\overline{x}]$ that have algebraic circuits of size at most s and depth at most Δ, where Δ is a constant. Then there is a circuit $U(\overline{x}, \overline{w}) \in \mathbb{F}[\overline{x}, \overline{w}]$ of size $\mathrm{poly}(s)$ and depth $\mathrm{poly}(\Delta)$ such that $\overline{w}$ are $K_{s,d}$ variables that are disjoint from $\overline{x}$, that is universal for $\mathrm{VAC}^0_{s,\Delta}$ in the following sense: if $f(\overline{x}) \in \mathrm{VAC}^0_{s,\Delta}$, then there exists $\overline{a} \in \mathbb{F}^{K_{s,d}}$ such that $U(\overline{x}, \overline{a}) = f(\overline{x})$. Notice that given s and d, $K_{s,d}$ can be computed efficiently and is bounded by $\mathrm{poly}(s)$. Also, the universal circuit preserves the maximum multiplication fan-in.*

See the full version [35] for the proof of Theorem 25.

4 Extracting Coefficients and IPS Refutation Formula

Let $f(\overline{x}, \overline{w}) \in \mathbb{F}[\overline{x}, \overline{w}]$ be a polynomial, and let $M = \prod_{i \in I} x_i^{\alpha_i} \cdot \prod_{j \in J} w_j^{\beta_j}$ be a monomial in $f(\overline{x}, \overline{w})$, for some $\alpha_i, \beta_i \in \mathbb{N}$ (where $0 \in \mathbb{N}$). Then, we call $\Sigma_{i \in I} \alpha_i$ the $\overline{x}$-degree of M.

▶ **Definition 26** ($\mathrm{coeff}_M(\cdot)$ [54]). *Let $f(\overline{x}, \overline{w})$ be a polynomial in $\mathbb{F}[\overline{x}, \overline{w}]$ in the disjoint sets of variables $\overline{x}, \overline{w}$. Let M be an $\overline{x}$-monomial. Then, $\mathrm{coeff}_M(f(\overline{x}, \overline{w}))$ is the (polynomial) coefficient in $\mathbb{F}[\overline{w}]$ (that is, in the $\overline{w}$-variables only) of M in $f(\overline{x}, \overline{w})$.*

Note that $f(\overline{x}, \overline{w}) = \Sigma_{M_i} M_i \cdot \mathrm{coeff}_{M_i}(f(\overline{x}, \overline{w}))$, where the M_i's are all possible $\overline{x}$-monomials of degree at most d, for d the maximal $\overline{x}$-degree of a monomial in $f(\overline{x}, \overline{w})$.

While [54] gave the proposition about the computation of the coefficient of an $\overline{x}$-monomial in general algebraic circuits, we present the computation of the coefficient of an $\overline{x}$-monomial in *bounded-depth* circuits.

Since we can decrease the maximum multiplication fan-in to n in each polynomial-size bounded-depth circuit with at most a polynomial-size blow up and depth blowing up by at most a constant factor, we can assume that the maximum multiplication fan-in in each polynomial-size bounded-depth circuit is n.

▶ **Proposition 27** (Computation of coefficients in bounded-depth circuits). *Let $f(\overline{x}, \overline{w}) \in \mathbb{F}[\overline{x}, \overline{w}]$ be a polynomial in $\mathbb{F}[\overline{x}, \overline{w}]$ in the disjoint sets of variables $\overline{x}, \overline{w}$. Suppose that M is an $\overline{x}$-monomial of degree d, and assume that there is an algebraic circuit $C(\overline{x}, \overline{w})$ computing $f(\overline{x}, \overline{w})$ of maximum multiplication fan-in t, size s, syntactic-degree l and depth Δ where Δ is a constant such that*

1. *All edges from the leaves are to + nodes.*
2. *All output-nodes are + nodes.*
3. *The nodes of G are alternating. That is, if v is a + node and (u,v) is an edge, then u is a $\times$ node, and if v is a $\times$ node and (u,v) is an edge then u is either a leaf or a + node.*

Then, there is a bounded-depth algebraic circuit of depth Δ, size $O(2^{(t+d)d}\cdot s)$ computing $\mathrm{coeff}_M(f(\overline{x},\overline{w}))$ *of syntactic-degree $l^{O(1)}$.*

See the full version [35] for the proof of Proposition 27.

▶ **Definition 28** (Bounded-depth IPS refutation predicate $\mathrm{IPS}_{\mathrm{ref}}(s,\Delta,l,\overline{\mathcal{F}})$)**.** *Let $\overline{\mathcal{F}}$ be a* CNF *formula with m clauses and n variables $\overline{x}$ written as a set of polynomial equations according to Definition 18. Let $U(\overline{x},\overline{y},\overline{w})$ be the bounded-depth universal circuit for depth Δ and size s circuits in the $\overline{x}$ variables and the m placeholder variables $\overline{y}$, and the $K_{s,\Delta}$ edge label variables $\overline{w}$. We formalize the existence of a size s, depth Δ circuit that computes the* IPS *refutation of $\overline{\mathcal{F}}$ in degree at most l, denoted* $\mathrm{IPS}_{\mathrm{ref}}(s,\Delta,l,\overline{\mathcal{F}})$*, with the following set of circuit equations (in the $\overline{w}$ variables only):*

$$\mathrm{coeff}_{M_i}(U(\overline{x},\overline{0},\overline{w}))=0$$

$$\mathrm{coeff}_{M_i}(U(\overline{x},\overline{\mathcal{F}},\overline{w}))=\begin{cases}1, & M_i=1 \text{ (i.e., } \textit{the constant 1 monomial}\text{)};\\ 0, & \textit{otherwise},\end{cases}$$

where $i\in[N]$ so that $\{M_i\}_{i=1}^N$ are the set of all possible $\overline{x}$-monomials of degree at most l, and $N=\sum_{j=0}^{l}\binom{n+j-1}{j}=2^{O(n+l)}$ is the number of monomials of total degree at most l over n variables, and $\overline{0}$ is the all-zero vector of length m.

The size of $\mathrm{IPS}_{\mathrm{ref}}(s,\Delta,l,\overline{\mathcal{F}})$ *is $O(2^{(t+l)l}\cdot|U(\overline{x},\overline{y},\overline{w})|\cdot|\overline{\mathcal{F}}|\cdot N)$ where t is maximum multiplication fan-in in $U(\overline{x},\overline{y},\overline{w})$.*

▶ **Definition 29** (Formalization of VNP $=$ VAC^0)**.** *The formalization of* VNP $=$ $\mathrm{VAC}^0(n,s,l,\Delta)$ *denoted "*VNP $=$ $\mathrm{VAC}^0(n,s,l,\Delta)$*", expressing that there is a bounded-depth universal circuit for size s and depth Δ circuits that compute the Permanent polynomial of dimension n (with $\overline{x}$ being the n^2 variables of the Permanent), is the following set of polynomial equations (in the $\overline{w}$-variables only):*

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

where $\overline{b}=\mathrm{coeff}(\mathrm{perm}(\overline{x}))\in\mathbb{F}^N$ is the coefficient vector of the polynomial $\mathrm{perm}(\overline{x})$ *of dimension n, $U(\overline{x},\overline{w})$ is the constant-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 $N=\Sigma_{j=0}^{l}\binom{n^2+j-1}{j}=2^{O(n^2+l)}$ is the number of monomials of total degree at most l over n^2 variables. Then, the size of the above set of polynomial equations is $O(2^{(t+l)l}\cdot|U(\overline{x},\overline{w})|\cdot N)$ where t is maximum multiplication fan-in in $U(\overline{x},\overline{w})$.*

5 No Short AC$^0[p]$-Frege Proofs for Diagonalizing DNF Formulas

This section presents our main result. we show unconditionally that constant-depth IPS cannot efficiently refute certain constant-depth IPS upper bounds. As a corollary, we obtain the same result for AC$^0[p]$-Frege, since this proof system is simulated by constant-depth IPS over $\mathbb{F}_p$ (Theorem 34). More precisely, we prove that constant-depth IPS does not admit

polynomial-size refutations of the diagonalizing CNF formulas $\Phi_{t,l,\Delta',n,s,\Delta}$, infinitely often. These formulas express the existence of size-t, depth-Δ' IPS refutation of the statement that the Permanent polynomial is computable by size-s, depth-Δ algebraic circuits.

In addition, this section contains the proof of Theorem 6, which shows that ruling out short proofs for the diagonalizing formulas is a necessary step towards constant-depth IPS lower bounds. We begin by introducing the formulas that will be used throughout the argument.

Let $N = \sum_{j=0}^{l} \binom{n^2+j-1}{j} = 2^{O(n^2+l)}$ be the number of monomials of total degree at most l over n^2 variables. We shall work over a finite field $\mathbb{F}_q$ here to enable the encoding of circuit equations as CNF formulas.

- $\mathrm{VNP} = \mathrm{VAC}^0(n, s, l, \Delta)$: circuit equations expressing that there is an algebraic circuit of size s and depth Δ that *agrees* with the Permanent polynomial of dimension n on all the coefficients of monomials of degree at most l (i.e., every monomial M computed by the algebraic circuit has the same coefficient as
- $\varphi^{\mathrm{cnf}}_{n,s,l,\Delta}$: the CNF encoding of $\mathrm{VNP} = \mathrm{VAC}^0(n, s, l, \Delta)$ based on Definition 20.
- $\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}$: the SCNF encoding of $\mathrm{VNP} = \mathrm{VAC}^0(n, s, l, \Delta)$ based on Definition 22 together with the field axioms $(x^q - x = 0)$ for all variables.
- $\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \overline{\mathcal{F}})$: circuit equations expressing that there exists an algebraic circuit for size t and depth Δ that agrees with the IPS refutation of $\overline{\mathcal{F}}$ on all the coefficients of monomials of degree at most l.
- $\Phi_{t,l,\Delta',n,s,\Delta}$: *The diagonalizing CNF formula.* More precisely, the CNF encoding of $\mathrm{IPS}_{\mathrm{ref}}(t, \Delta', l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})$ expressing that there is an algebraic circuit (the purported IPS refutation) of size t and depth Δ' that agrees with the IPS refutation of $\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}$ on all the coefficients of monomials of degree at most l.

The following lemma easily follows from Lemma 17.

▶ **Lemma 30.** *Every family of unsatisfiable formulas (φ_n), which contains a set of unsatisfiable* CNF *formulas, has a family of* $\mathrm{IPS}^{\mathrm{alg}}$ *(also* IPS*) certificates (C_n) in* $\mathrm{VNP}_{\mathbb{F}}$.

Since Semi-CNFs are substitution instances of CNFs, we get the following lemma by substituting the occurrence of Boolean variables with their corresponding UBIT.

▶ **Lemma 31.** *$\{\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}\}_n$ is a family of unsatisfiable* SCNF *formulas and has a family of* $\mathrm{IPS}^{\mathrm{alg}}$ *(also* IPS*) certificates (C_n) in* $\mathrm{VNP}_{\mathbb{F}}$.

We fix $l : \mathbb{N} \to \mathbb{N}$ to be a (monotone) size function $l(r) = \lceil r^{\epsilon} \rceil$ for some constant ϵ.
The main result of this section is the following.

▶ **Theorem 32** (Main; no short proofs over fixed finite field)**.** *Let q be a constant prime. The* CNF *family $\{\Phi_{t,l,\Delta',n,s,\Delta}\}$ does not have constant-depth polynomial-size* IPS *refutations infinitely often over $\mathbb{F}_q$, in the following sense: for every constant Δ there exist constants c_1 and Δ', such that for every sufficiently large constant c_2 and every constants Δ'' and c_0, for infinitely many $n, t(n), s(n) \in \mathbb{N}$, such that $t(n) > |\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}|^{c_1}$ and $n^{c_1} < s(n) < n^{c_2}$, $\Phi_{t,l,\Delta',n,s,\Delta}$ has no* IPS *refutation of size at most $|\Phi_{t,l,\Delta',n,s,\Delta}|^{c_0}$ and depth at most Δ''.*

We provide an overview of its proof.

Proof overview. By way of contradiction, we assume that there exists a constant Δ such that for every constant Δ', for every sufficiently large n, and for every $t(n), s(n) \in \mathbb{N}$, such that $t(n) > |\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}|^{c_1}$ and $n^{c_1} < s(n) < n^{c_2}$, $\Phi_{t,l,\Delta',n,s,\Delta} := \mathrm{cnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta', l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ has a

small depth-$O(1)$ refutation. Then, by substituting the occurrences of Boolean variables with the correspondence UBITs, we can assume that $\mathrm{scnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta', l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ has a small and depth-$O(\Delta')$ refutation.

1. By applying Lemma 24, from $\varphi^{\mathrm{scnf}}_{m,t,l,\Delta}$ where m, t, l are parameters, that meet the conditions in Theorem 32, we can derive the circuit equations

   $$\mathrm{VNP} = \mathrm{VAC}^0(m, t, l, \Delta),$$

   in $O(\Delta)$ depth and polynomial-size IPS. Recall that $\mathrm{VNP} = \mathrm{VAC}^0(m, t, l, \Delta)$ is the set of circuit equations expressing that there is an algebraic circuit of size t and depth Δ that agrees with the Permanent polynomial of dimension m on all the coefficients of monomials of degree at most l.
2. In Lemma 33 we prove (the contrapositive of) the bounded-depth version of Theorem 16 *within bounded-depth* IPS. The contrapositive of the bounded-depth version of Theorem 16 expresses that if the Permanent polynomial can be computed by bounded-depth polynomial-size circuits, then bounded-depth IPS can efficiently refute any family of CNF formulas. To be more specific, from $\mathrm{VNP} = \mathrm{VAC}^0(m, t, l, \Delta)$ we derive $\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})$ in depth $O(\Delta)$ and polynomial size. Note that $\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})$ is the set of circuit equations expressing that IPS can refute $\varphi^{\mathrm{scnf}}_{n,s,l,\Delta}$ in size t and depth Δ.
3. Applying Lemma 23, we can derive $\mathrm{scnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ from $\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})$ in depth $O(\Delta)$ polynomial size IPS. Since we assumed that for any constant Δ', $\mathrm{scnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta', l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ has a small and bounded-depth refutation, it follows that $\mathrm{scnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ has a small and bounded-depth refutation, particularly when we take $\Delta' = \Delta$.

Hence, we get a small and bounded-depth refutation of $\varphi^*_{m,t,l,\Delta}$, as follows:

$$\begin{aligned}
\varphi^*_{m,t,l,\Delta} &\vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} \mathrm{VNP} = \mathrm{VAC}^0(m, t, l, \Delta) && \text{Lemma 24 (see Item 1)}\\
&\vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} \mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}) && \text{Lemma 33 (see Item 2)}\\
&\vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} \mathrm{scnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta, l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})) && \text{Lemma 23 (see Item 3)}\\
&\vdash^{*,O(\Delta)}_{\mathrm{IPS}^{\mathrm{alg}}} 1 = 0 && \text{by assumption.}
\end{aligned}$$

Then we know that for some constant Δ''' and large enough w, the system of circuit equations $\mathrm{IPS}^{\mathrm{alg}}_{\mathrm{ref}}(w, \Delta''', l, \varphi^*_{m,t,l,\Delta})$ is satisfiable. Hence, $\mathrm{cnf}(\mathrm{IPS}^{\mathrm{alg}}_{\mathrm{ref}}(w, \Delta''', l, \varphi^*_{m,t,l,\Delta}))$ is satisfiable.

By assumption, for any constant Δ', for all sufficiently large n, for all proper $t(n), s(n) \in \mathbb{N}$, $\Phi_{t,l,\Delta',n,s,\Delta} := \mathrm{cnf}(\mathrm{IPS}_{\mathrm{ref}}(t, \Delta', l, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta}))$ has a small and depth-$O(1)$ refutation. Taking $t = w$, $\Delta' = \Delta'''$, $n = m$, $s = t$, we know that $\mathrm{cnf}(\mathrm{IPS}^{\mathrm{alg}}_{\mathrm{ref}}(w, \Delta''', l, \varphi^{\mathrm{scnf}}_{m,t,l,\Delta}))$ is refutable which implies it is not satisfiable. This is a contradiction. ◀

▶ **Lemma 33** (Constant-depth version of Grochow-Pitassi formalization in IPS$^{\mathrm{alg}}$)**.** *There are constants c_3 and Δ''' such that under the above notation and parameters:*

$$\overbrace{\varphi^{\mathrm{scnf}}_{m,t,l,\Delta}}^{\gamma} \vdash^{|\gamma|^{c_3},\Delta'''}_{\mathrm{IPS}^{\mathrm{alg}}} \mathrm{scnf}(\mathrm{IPS}^{\mathrm{alg}}_{\mathrm{ref}}(t, l, \Delta, \varphi^{\mathrm{scnf}}_{n,s,l,\Delta})).$$

We omit the proof of Theorem 32; it can be found in the full version [35].

Theorem 2 in the introduction which uses a fixed prime field of size p follows from Theorem 32 by setting $\psi_{d,d',n} = \Phi_{t,l,\Delta',n,s,\Delta}$, where $d = \Delta, d' = \Delta'$ and s and t are chosen to be appropriate polynomially bounded functions as in the statement of Theorem 32.

To get the no-short proof result against $\mathrm{AC}^0[p]$-Frege we use the following simulation:

▶ **Theorem 34** (Depth-preserving simulation of Frege systems by the Ideal proof system [24]). *Let p be prime and $\mathbb{F}$ any field of characteristic p. Then $\mathrm{IPS}_{\mathbb{F}}$ p-simulates $\mathrm{AC}^0[p]$-Frege in such a way that depth-d $\mathrm{AC}^0[p]$-Frege proofs are simulated by depth-$O(d)$ $\mathrm{IPS}_{\mathbb{F}}$ proofs. In particular, $\mathrm{AC}^0[p]$-Frege is p-simulated by bounded-depth $\mathrm{IPS}_{\mathbb{F}}$.*

Therefore, a corollary of Theorem 32 is (see the argument in Section 1.3 that comes after Theorem 2):

▶ **Corollary 35.** *For every prime p there is an explicit sequence $\{\phi_n\}$ of DNF formulas (of unknown validity) such that there are no polynomial-size $\mathrm{AC}^0[p]$-Frege proofs of $\{\phi_n\}$.*

6 Ruling Out Easiness for Diagonalizing CNFs is Necessary

We now turn to establishing Theorem 6. We first define the notion of a "reasonable" circuit class.

▶ **Definition 36.** *We say $\mathcal{C}$ is a* reasonable *algebraic circuit class if $\mathcal{C}$-IPS can efficiently prove the $\mathcal{C}$-IPS analogue of Lemma 33, i.e., that $\mathcal{C}$ lower bounds for Permanent follow from $\mathcal{C}$-IPS lower bounds for* CNF *formulas.*

The main result of [54] can be seen as showing that the class of general algebraic circuits is reasonable, and Theorem 32 shows that the class of constant-depth algebraic circuits is reasonable as well. The proof of Theorem 32 establishes that every natural algebraic class intermediate in power between constant-depth circuits and general circuits is reasonable as well.

We observe that Lemma 17 can be generalised for an arbitrary algebraic circuit class $\mathcal{C}$.

▶ **Theorem 37** (Grochow-Pitassi for $\mathcal{C}$). *Let $\mathcal{C}$ be any algebraic circuit class. For any field $\mathbb{F}$, if $\mathcal{C}$-IPS is not p-bounded, namely there exists a super-polynomial lower bound on algebraic $\mathcal{C}$-IPS refutations (hence also on $\mathcal{C}$-IPS refutations) over $\mathbb{F}$ for a family of unsatisfiable* CNF *formulas $\{\phi_n\}_n$, then $\mathrm{VNP}_{\mathbb{F}} \neq \mathcal{C}_{\mathbb{F}}$.*

Now, we show that the $\mathcal{C}$-analogue of Theorem 2 is necessary to prove $\mathcal{C}$-IPS lower bounds for unsatisfiable CNFs, when $\mathcal{C}$ is a reasonable algebraic circuit class.

We use $\{\Phi_n^{\mathcal{C}}\}$ to denote the $\mathcal{C}$ analogue of $\{\Phi_{t,l,\Delta',n,s,\Delta}\}$ from Theorem 32.

▶ **Theorem 38** (Necessity of the main theorem). *Let $\mathcal{C}$ be any reasonable algebraic circuit class. Let p be a sequence of primes, and $\mathbb{F}_p$ be the prime field. If $\mathcal{C}$-IPS is not p-bounded over $\mathbb{F}_p$, which means there is a super-polynomial lower bound on algebraic $\mathcal{C}$-IPS refutations (hence also on $\mathcal{C}$-IPS refutations) over $\mathbb{F}_p$ for a family of unsatisfiable* CNF *formulas $\{\phi_n\}_n$, then the* CNF *family $\{\Phi_n^{\mathcal{C}}\}$ does not have polynomial-size $\mathcal{C}$-IPS refutations infinitely often over $\mathbb{F}_p$ in the following sense: there exists a constant c_1 such that for every sufficiently large constant c_2 and every constant c_0, for infinitely many $n, t(n), s(n) \in \mathbb{N}$, $t(n) > 2^{(n^{c_1})}$ and $n^{c_1} < s(n) < n^{c_2}$, $\Phi_n^{\mathcal{C}}$ has no $\mathcal{C}$-IPS refutation over $\mathbb{F}_p$ of size at most $|\Phi_n^{\mathcal{C}}|^{c_0}$.*

Theorem 38 is the formal version of Theorem 6 in the Introduction.

7 No Short Bounded-Depth IPS Refutations for Diagonalizing CNF Formulas: the Polynomial-Size Fields Case

In this section, we work over finite fields whose characteristic is polynomially bounded by the instance size, in order to obtain a more general result. This contrasts with the previous section, where the characteristic of the finite field was a fixed global constant, independent of the instance size. Here we encode binary string arithmetic – including addition, multiplication, and modular computation into CNF formulas. Within this setting, we also establish the translation lemma, which yields a version of Theorem 32 over finite fields of polynomially bounded characteristic. In other words, we show that no efficient provability result holds against constant-depth IPS over polynomial-size finite fields. Since Forbes [17] extended [34] to arbitrary fields, the results of this section generalize Theorem 32. The techniques here, however, are somewhat more involved.

We will continue to use notations such as $\mathrm{cnf}(C(\overline{x}) = 0)$ and $\mathrm{ecnf}(C(\overline{x}) = 0)$ from the fixed-field setting, but with a different interpretation: in this section they refer to the CNF and Extended CNF encodings of $C(\overline{x}) = 0$ obtained via bit-level arithmetic, which we can be found in the full version [35].

▶ **Corollary 39** (Main theorem in polynomial-size finite fields). *The* CNF *family* $\{\Phi_{t,l,\Delta',n,s,\Delta}\}_n$ *does not have polynomial-size* IPS *refutations infinitely often over* $\mathbb{F}_q$*, for every prime* q *such that* $q < (|\varphi^*_{n,s,l,\Delta}| + 1)^3$*, in the following sense: for every constant* Δ *there exists a constant* c_1*, a constant* Δ' *such that for every sufficiently large constant* c_2 *and every constant* Δ'' *and every constant* c_0*, for infinitely many* $n, t(n), s(n) \in \mathbb{N}$*,* $t(n) > |\varphi^*_{n,s,l,\Delta}|^{c_1}$ *and* $n^{c_1} < s(n) < n^{c_2}$*,* $\Phi_{t,l,\Delta',n,s,\Delta}$ *has no* IPS *refutation of size at most* $|\Phi_{t,l,\Delta',n,s,\Delta}|^{c_0}$ *and depth at most* Δ''*.*

Corollary 39 is a formal statement of Theorem 7 in the Introduction, which can be obtained from it by setting l, s, t to appropriate polynomial functions of n, and by setting $d = \Delta, d' = \Delta', d'' = \Delta''$.

References

1 Miklós Ajtai. The complexity of the pigeonhole principle. In *Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science*, pages 346–355, 1988. doi:10.1109/SFCS.1988.21951.

2 Miklós Ajtai. The independence of the modulo p counting principles. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 402–411, 1994.

3 Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM J. Comput.*, 34(1):67–88, 2004. (A preliminary version appeared in Proceedings of the 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)). doi:10.1137/S0097539701389944.

4 Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semialgebraic proofs, IPS lower bounds, and the τ-conjecture: Can a natural number be negative? *SIAM J. Comput.*, 53(3):648–700, 2024. doi:10.1137/20M1374523.

5 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.

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

7 Paul Beame and Toniann Pitassi. Propositional proof complexity: Past, present and future. *Bulletin of the EATCS*, 65:66–89, 1998.

8 Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan. New bounds for the ideal proof system in positive characteristic. In *52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025)*, Aarhus, Denmark, July 2025. To appear.

9 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.

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

11 Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. *SIAM J. Comput.*, 29(6):1939–1967, 2000. doi:10.1137/S0097539798353230.

12 Samuel R Buss. Polynomial size proofs of the propositional pigeonhole principle. *The Journal of Symbolic Logic*, 52(4):916–927, 1987. doi:10.2307/2273826.

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

14 Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 174–183, New York, 1996. ACM. doi:10.1145/237814.237860.

15 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979. doi:10.2307/2273702.

16 Tal Elbaz, Nashlen Govindasamy, Jiaqi Lu, and Iddo Tzameret. Lower bounds against the ideal proof system in finite fields. *arXiv preprint arXiv:2506.17210*, 2025. doi:10.48550/arXiv.2506.17210.

17 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.

18 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.

19 Harvey Friedman. On the consistency, completeness and correctness problems. Unpublished, 1979.

20 Michal Garlik, Svyatoslav Gryaznov, Jiaqi Lu, Rahul Santhanam, and Iddo Tzameret. Metamathematics of algebraic circuit lower bounds. Manuscript, 2025.

21 Michal Garlik, Svyatoslav Gryaznov, Hanlin Ren, and Iddo Tzameret. The weak rank principle: Lower bounds and applications. Manuscript, 2025.

22 Andreas Goerdt. Cutting plane versus Frege proof systems. In Egon Börger, Hans Kleine Büning, Michael M. Richter, and Wolfgang Schönfeld, editors, *Computer Science Logic, 4th Workshop, CSL '90, Heidelberg, Germany, October 1-5, 1990, Proceedings*, volume 533 of *Lecture Notes in Computer Science*, pages 174–194. Springer, 1991. doi:10.1007/3-540-54487-9_59.

23 Nashlen Govindasamy, Tuomas Hakoniemi, and Iddo Tzameret. Simple hard instances for low-depth algebraic proofs. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 188–199. IEEE, 2022. doi:10.1109/FOCS54457.2022.00025.

24 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.

25 Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985. doi:10.1016/0304-3975(85)90144-6.

26 Tuomas Hakoniemi, Nutan Limaye, and Iddo Tzameret. Functional lower bounds in algebraic proofs: Symmetry, lifting, and barriers. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, pages 1396–1404, New York, NY, USA, 2024. Association for Computing Machinery. Full version in ECCC https://eccc.weizmann.ac.il/report/2024/079/. doi:10.1145/3618260.3649616.

27 Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. The surprising power of constant depth algebraic proofs. In Holger Hermanns, Lijun Zhang, Naoki Kobayashi, and Dale Miller, editors, *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, pages 591–603. ACM, 2020. doi:10.1145/3373718.3394754.

28 Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997. doi:10.2307/2275541.

29 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.

30 Jan Krajíček. *Proof complexity*, volume 170. Cambridge University Press, 2019.

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

32 Jan Krajíček. Diagonalization in proof complexity. *Fundamenta Mathematicae*, 182:181–192, 2004.

33 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.

34 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.

35 Jiaqi Lu, Rahul Santhanam, and Iddo Tzameret. Ac^0[p]-frege cannot efficiently prove that constant-depth algebraic circuit lower bounds are hard. *arXiv preprint arXiv:2509.16824*, 2025. doi:10.48550/arXiv.2509.16824.

36 Jan Pich and Rahul Santhanam. Why are proof complexity lower bounds hard? In *60th Annual IEEE Symposium on Foundations of Computer Science FOCS 2019, November 9-12, 2019, Baltimore, Maryland USA*, 2019.

37 Ján Pich and Rahul Santhanam. Learning algorithms versus automatability of frege systems. *Journal of Mathematical Logic*, 2024. doi:10.1142/S0219061325500023.

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

39 Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *computational complexity*, 3(2):97–140, 1993. doi:10.1007/BF01200117.

40 Pavel Pudlak. On the length of proofs of finitistic consistency statements in first order theories. *Studies in Logic and the Foundations of Mathematics*, 120:165–196, 1986.

41 Pavel Pudlak. Improved bounds to the length of proofs of finite consistency statements. *Contemporary Mathematics*, 65:309–331, 1987.

42 Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, September 1997. doi:10.2307/2275583.

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

44 Ran Raz. Elusive functions and lower bounds for arithmetic circuits. *Theory of Computing*, 6(1):135–177, 2010. doi:10.4086/toc.2010.v006a007.

45 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.

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

47 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(4):333–338, 1987. doi:10.1007/BF01137685.

48 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.

49 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.

50 Alexander A. Razborov. Lower bounds for propositional proofs and independence results in bounded arithmetic. In Friedhelm Meyer auf der Heide and Burkhard Monien, editors, *Automata, Languages and Programming, 23rd International Colloquium, ICALP96, Paderborn, Germany, 8-12 July 1996, Proceedings*, volume 1099 of *Lecture Notes in Computer Science*, pages 48–62. Springer, 1996. doi:10.1007/3-540-61440-0_116.

51 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998. doi:10.1007/S000370050013.

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

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

54 Rahul Santhanam and Iddo Tzameret. Iterated lower bound formulas: A diagonalization-based approach to proof complexity. *SIAM Journal on Computing*, pages 313–349, 2025. Preliminary version appeared in Proceedings of the *53rd Annual ACM Symposium on Theory of Computing (STOC 2021)*.

55 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.

56 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.