Electronic Colloquium on Computational Complexity, Report No. 38 (2022)

Lower bounds for Polynomial Calculus with extension variables over finite fields

Russell Impagliazzo [*]

UC San Diego
russell@cs.ucsd.edu

Sasank Mouli [†]

UC San Diego
galivenk@ucsd.edu

Toniann Pitassi [‡]

Columbia University
tonipitassi@gmail.com

Abstract

For every prime $p > 0$, every $n > 0$ and $\kappa = O(\log n)$, we show the existence of an unsatisfiable system of polynomial equations over $O(n \log n)$ variables of degree $O(\log n)$ such that any Polynomial Calculus refutation over $\mathbb{F}_p$ with M extension variables, each depending on at most κ original variables requires size $\exp\left(\Omega(n^2/(\kappa^2 2^\kappa(M+n\log(n))))\right)$.

[*] Supported by the Simons Foundation and NSF grant CCF-1909634.

[†] Supported by the Simons Foundation and NSF grant CCF-1909634.

[‡] This material is based upon work supported by the National Science Foundation Grant No. CCF-1900460, and by the IAS School of Mathematics. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

ISSN 1433-8092

1 Introduction

Propositional proof complexity, started by the seminal work of Cook-Reckhow [CR79] is a field of study analogous to Boolean circuit complexity, and asks the following question: given a formal proof system dealing with propositional formulae, what Boolean tautologies are hard to prove in this system? The ultimate goal of this program is to come up with tautologies that are hard for any proof system that has a polynomial time verifier, hence showing that $\mathsf{coNP} \not\subseteq \mathsf{NP}$. So far progress has been made only for proof systems which are restricted in their capacity to reason, such as Resolution [Hak85],[BSW99] and Bounded-depth Frege [Ajt94], [PBI93],[KPW95].

The next frontier is to obtain lower bounds for the system $\mathsf{AC}^0[p]$-Frege. Since for the analogous circuit model, Razborov [Raz87] and Smolensky [Smo87] obtained lower bounds through connections to algebraic objects, this suggests the study of *Algebraic Proof Systems*. Beame et.al. [BIK$^+$96] introduced and showed lower bounds for the algebraic proof system *Nullstellensatz* where lines are low degree polynomials over a field. Clegg et. al [CEI96] introduced the algebraic system *Polynomial Calculus(*PC*)*, which is a dynamic generalization of Nullstellensatz. Lower bounds for Polynomial Calculus were obtained in many works (e.g., [Raz98, BGIP01, AR01, GL10, MN15]).

After what seemed to be reasonable progress with Algebraic Proof Systems, progress towards the frontier of $\mathsf{AC}^0[p]$-Frege is still stalled for various reasons. For one, the proof systems described above are not strong enough to simulate $AC^0[p]$-Frege. Also, the lower bound techniques used for the above lower bounds are based on random restrictions, and it is well known that modular counting gates are immune to such techniques. Therefore, we need to aim towards lower bounds for systems strong enough to simulate $AC^0[p]$-Frege. We also need lower bound techniques that are not just random-restriction based. On both fronts, there has been recent progress. Grigoriev and Hirsch [GH03] introduced the proof system constant-depth PC and showed that it simulates $\mathsf{AC}^0[p]$-Frege at a proportional depth. Raz and Tzameret [RT08] showed that constant-depth PC at depth 3 over the field of Rational numbers surprisingly simulates the semi-algebraic proof system Cutting Planes with bounded coefficients. [IMP20] obtained many more surprising results, and showed that Depth-43-PC (over a large enough extension of a finite field $\mathbb{F}_p$) simulates $AC^0[q]$-Frege for a different prime q, Cutting Planes with unbounded coefficients, and also the Sum-of-Squares proof system. They also showed that Depth-d-PC simulates TC^0-Frege at a proportional depth. It therefore makes sense to aim for lower bounds for the stronger system Depth-d-PC, for increasingly large constants d. In this direction, Sokolov [Sok20] obtained lower bounds for the system PC over $\mathbb{F}_3$ where extension variables of the form $z_i = 2x_i - 1$ are allowed to be introduced (hence making them take values in the set $\{+1, -1\}$).

In this work, we generalize the methods of Sokolov to show lower bounds for PC with up to $N^{2-\epsilon}$ extension variables which can depend on up to $\kappa = O(\log N)$ original variables (where N is the number of variables in the tautology). [Ale21] obtained stronger lower bounds for Polynomial Calculus with extension variables over the reals, but since we work over finite fields our results are incomparable. Also, their tautology is a variant of subset sum with large coefficients, which cannot be defined well over finite fields.

Theorem 1 (high-end)**.** *There is a family of CNF tautologies $\psi_{N,\kappa,M}$ on N variables with poly(N) clauses of width $O(logN)$ so that for any $M = Npolylog(N)$ and $\kappa \geq 1$,* *and prime p, there is a function $S(N) \in 2^{\Omega(N/polylog(N))}$ so that any* PC *refutation of $\psi_{N,\kappa,M}$ together with any M κ-local extensions over $\mathbb{F}_p$ requires size $S(N)$.*

Theorem 2 (low-end)**.** *For the same family of tautologies above, for any prime p, there are $0 < \alpha, \beta, \gamma < 1$, with $\gamma < 1 - \alpha - \beta$ so that, for $M = N^{1+\alpha}, \kappa = \beta logN$, and $S = exp(N^{\gamma})$, any* PC *refutation of Φ_N together with any M κ-local extensions over $\mathbb{F}_p$ requires size $S(N)$.*

1.1 Related Work

Our primary goal in this work is to prove lower bounds for low-depth IPS refutations for unsatisfiable CNF formulas, over finite fields, since this is the setting where algebraic lower bounds are closely connected to proving lower bounds for $AC^0[p]$-Frege systems, a major and longstanding open problem in proof complexity.

The work that inspired us and that is most related to our result is the recent paper by Sokolov [Sok20], proving exponential lower bounds on the size of PC refutations of CNF formulas over $\mathbb{F}_3$, where the variables take on values in $\{1, -1\}$. We generalize Sokolov's result to hold over any finite field, even with the addition of superlinear many extension variables, each depending arbitrarily on a small number of original variables. Thus our result can be alternatively viewed as making progress towards proving exponential lower bounds for depth-3 IPS, for a family of CNF formulas.

We note that for more general unsatisfiable polynomial equations that are *not* translations of CNF formulas, several recent papers prove much stronger results over the rationals (but are incomparable to our main result). First, [FSTW21] proved lower bounds for subsystems of IPS by restricted classes of circuits, including low-depth formulas, multilinear formulas and read-once oblivious branching programs. Secondly, Alekseev [Ale21] proved exponential lower bound on the bit complexity of constant-depth IPS proofs over the rationals, and a recent paper by Andrews and Forbes [AF21] proves quasipolynomial lower bounds on the circuit size of constant-depth IPS proofs for a different family of formulas, over the rationals. However, for a variety of reasons, all of these lower bounds do not imply nontrivial lower bounds in the propositional setting and thus they are incomparable to our main result. First, these results do not hold in the setting of finite fields. Secondly, the particular choice of hard polynomials are inherently nonboolean: [FSTW21, Ale21] use the subset sum principle which when translated to a propositional statement is no longer hard, and the hard polynomials in [AF21] have logarithmic depth.

1.2 Our Result: Proof Overview

The standard way of proving size lower bounds for PC for an unsatisfiable formula F for Boolean-valued variables dates back to the celebrated superpolynomial lower bounds for Resolution [Hak85, BSW99], where the basic tool is to reduce size lower bounds to degree lower bounds (or in the case of Resolution, size to clause-width) by way of either a general size-depth tradeoff, or by a more general random restriction argument. At a high level, both methods iteratively select a variable that occurs in a lot of high-degree terms, set this variable to zero (to kill off all high-degree terms containing it), while also ensuring (possibly by setting additional variables) that F remains hard to refute after applying the partial restriction. After applying this size-to-degree reduction, the main technical part is to prove degee lower bounds for the restricted version of F.

Unfortunately over the $\{-1, 1\}$ basis, the size to degree reduction breaks down. In fact, no generic reduction to degree can exist since random XOR instances over this basis require linear degree but have polynomial size PC refutations over GF_2. Moreover, we lacked *any* method for proving PC lower bounds for unsatisfiable CNFs over the basis $\{-1, 1\}$. and more generally over an arbitrary linear transformation of the variables. In [IMP20], we highlighted this as an open problem, noting that it is a necessary step toward proving superpolynomial $AC^0[2]$-Frege lower bounds, a major open problem in proof complexity.

Recently, Sokolov [Sok20] made significant progress by proving exponential lower bounds for PC (as well as for SOS) for random CNF formulas over the domain $\{-1, 1\}$, by developing new formula-specific techniques to reduce size to degree over this domain. As this is the starting point for our work, we begin by describing the main method in [Sok20] for reducing size to degree for certain families of formulas over $\{-1, 1\}$.

Let Π be an alleged PC refutation of F of small size which includes the axioms $w^2 = 1$ for all variables w. The first step in Sokolov's argument is to show how to remove all high degree terms containing a particular variable w, provided that w is *irrelevant* – meaning that it does not occur in any of the initial polynomials other than the equation $w^2 = 1$. Intuitively, we want to show that if our unsatisfiable system of polynomial equations doesn't contain w, then we should be able to eliminate w altogether from the refutation. To show this, Sokolov writes each line q in the refutation as $q_0 + q_1 w$, and proves by induction that if we replace each line q by the pair of lines q_0, q_1, then it is still a valid refutation of F (and no longer contains w). While the split operation removes w from the proof, it doesn't kill off high degree terms. The crucial insight is that although this doesn't directly kill off high degree terms, a slightly different measure of degree (called quadratic degree) can be used instead, since removing w via the split operation removes all high quadratic degree terms that w contributed to, and secondly low quadratic degree implies low ordinary degree. The second and easier step in Sokolov's argument uses specific expansion properties of F to shows that for any variable w, there exists a small restriction ρ (to some of the other variables) such that w becomes irrelevant under ρ.

Our main theorem significantly generalizes Sokolov's lower bound by proving exponential lower bounds for an unsatisfiable CNF formulas F, even when we allow the axioms $\mathcal{P}$ to contain superlinear many extension axioms, provided that each has small support. Note that the variables of F are Boolean, but the extension variables are not restricted to being Boolean. In particular, they may be *nonsingular*, meaning that setting the variable to zero falsifies one of the initial polynomials. Intuitively, a nonsingular variable w cannot be set to 0, so we will handle them in a similar manner to Sokolov, by first isolating w, and then generalizing the split operation in order to kill off all large quadratic degree terms that contain w. However, dealing with a general set of extension axioms presents new technical challenges that we address next.

Our first idea is to design the unsatisfiable formula F carefully so that we can force variables to be irrelevant in a more modular way. Specifically, let $F'(x_1, \ldots, x_n)$ be an expanding unsatisfiable k-CNF formula with $m = O(n)$ clauses, such that any subset of $m' = \epsilon n$ clauses is unsatisfiable and requires proofs of large PC degree. We define an unsatisfiable formula F (based on F') that intuitively states that there is a subset

S of $m' = \epsilon m$ clauses of F' (as chosen by new selector variables y) that is satisfiable. We will prove lower bounds on the set of constraints $F \cup E$, where E is an arbitrary set of extension axioms satisfying the conditions mentioned earlier. In order to make a variable of F' irrelevant, we will simply make sure that our eventual assignment to the selector variables (y) avoids constraints of F' that contain this variable.

A second challenge that we face (that doesn't come up in Sokolov's proof) is that extension variables start off as either singular or nonsingular, but can change status after applying a restriction. For example, suppose E includes the extension axiom $z = x_1x_2 - x_1$. Then z is singular (since we can set $x_1 = x_2 = 0$), but if we set $x_1 = 1$, then z becomes nonsingular. In order to deal with this dynamically changing status of variables, our notion of quadratic degree must pay attention to which category each of the extension variables is in at any particular time, and make sure that we do not lose progress that was made earlier due to variables changing from singular to nonsingular. Fortunately we observe that variables can only change unidirectionally, from singular to nonsingular, and this is crucial for arguing that we can iteratively kill off large quadratic degree terms with respect to both types of variables in a particular order so that we continually make progress.

Finally, we also have to generalize Sokolov's split operation, which was previously defined only for $\{-1, 1\}$ variables. We give a generalization of how to do the split for arbitrary valued variables.

2 Preliminaries

Definition 1 (Polynomial Calculus). *Let $\Gamma = \{P_1 \ \cdots \ P_m\}$ be a set of polynomials in variables $\{x_1 \cdots x_n\}$ over a field $\mathbb{F}$ such that the system of equations $P_1 = 0 \cdots \ P_m = 0$ has no solution. A Polynomial Calculus refutation of Γ is a sequence of polynomials $R_1 \ \cdots \ R_s$ where $R_s = 1$ and for every ℓ in $\{1 \cdots s\}$, $R_\ell \in \Gamma$ or is obtained through one of the following derivation rules for $j, k < \ell$*

$$R_\ell = \alpha R_j + \beta R_k \textit{ for } \alpha,\ \beta \in \mathbb{F}$$

$$R_\ell = x_i R_k \textit{ for some } i \in \{1 \cdots n\}$$

The size of the refutation is $\sum_{\ell=1}^{s} |R_\ell|$, where $|R_\ell|$ is the number of monomials in the polynomial R_ℓ. The degree of the refutation is $\max_\ell deg(R_\ell)$.

Definition 2 (PC with extension variables). *Let $\Gamma = \{P_1 \ \cdots \ P_m\}$ be a set of polynomials in variables $\{x_1 \cdots x_n\}$ over a field $\mathbb{F}$ such that the system of equations $P_1 = 0 \ \cdots \ P_m = 0$ has no solution. Let $z_1 \cdots z_k$ be new variables defined over $\{x_1 \cdots x_n\}$ by $z_j = Q_j(x_1 \cdots x_n)$. A refutation of* PC *with extension variables $z_1 \cdots z_k$ of Γ is a Polynomial Calculus refutation of the set $\Gamma' = \{P_1 \cdots P_m, z_1 - Q_1, \cdots, z_k - Q_k\}$ of polynomials over $\{x_1 \cdots x_n\}$ and $\{z_1 \cdots z_k\}$.*

The size of such a refutation is the size of the Polynomial Calculus refutation of Γ'

Definition 3 (Refutation of a k-CNF in Polynomial Calculus). *Since we are working with Polynomial Calculus, a tautology in clausal form has to be translated into a set of polynomials over a field. We work over $\mathbb{F}_p$ for $p > 3$ and use the standard* PCR *translation of CNFs into polynomials: for each variable x occuring in the CNF, we have two associated variables x and $\bar{x}$ (representing x and its negation respectively). Each clause C is converted into an associated monomial in the natural way. For example, if*

$C = (x_1 \vee \neg x_2 \vee x_3)$, then the corresponding polynomial is $\bar{x}_1 x_2 \bar{x}_3 = 0$. In addition, for every variable $w, \overline{w}$, we include the boolean axioms $w^2 - w = 0$, $\overline{w}^2 - \overline{w} = 0$, as well as the axiom $w\overline{w} = 0$. .

3 The Hard Formulas

We distinguish between the case $p = 2$ and the case $p > 2$, and concentrate on the latter. This is because the case $p = 2$ does not require any new technical ideas, and we can pick from a large number of known hard tautologies for this case, such as random CNF's. Over $\mathbb{F}_2$, every extension variable is zero-one valued, and so standard size-degree tradeoffs pertain even with respect to extension variables. Also, k-local extension variables can change the degree by at most a factor of k. Since to use the size-degree tradeoffs , the degree must be at least the square root of the number of variables, this immediately gives a lower bound tolerating close to a quadratic number of local extension variables for any tautology requiring linear degree, giving us our claimed results.

Note, however, that over any field with $p > 2$, the Tseitin tautologies require linear degree but have polynomial sized proofs with a linear number of extension variables, so high degree is not sufficient when $p > 2$. So in this case, we need a new type of hard tautology. Below, we describe these tautologies.

We start with any unsatisfiable CNF formula such that

a) Any small set of variables appear in a small fraction of the axioms

b) Any large enough subset of axioms is unsatisfiable, and requires linear PC degree to refute.

For concreteness, we fix the following unsatisfiable CNF obtained by generating sufficiently many random parities.

First we'll show that a random regular bipartite graph has good boundary expansion. This has been used implicitly in other works ([CS88], [BKPS02]), but we could not find a clean statement to cite, so for completeness we state and prove it here. Let $G = (L, R, E)$ be a bipartite graph, and let $A \subseteq R$. The *boundary* for A, $\partial(A)$, is the set of vertices x in L so that $|N(x) \cap A| = 1$, i.e., vertices with a unique neighbor in A. A bipartite graph is (d, k) regular if every vertex in L has degree d and every vertex in R has degree k. In this case, for $n = |L|, m = |R|$, we have $dn = km$.

Theorem 3. *Let d, k, n, m be positive integers with $dn = km$, $k \geq 12$. Then with high probability for a random (d, k) regular bipartite graph with $|L| = n, |R| = m$, for all $A \subset R$, $|A| < n/(e^6k^2)$, we have $\partial(A) \geq k|A|/2$.*

Proof. Let $N(A)$ be all the neighbors of A. Since the total degrees of vertices in A is $k|A|$, and each element of $N(A) - \partial(A)$ is contingent on two such edges, $k|A| \geq 2(|N(A)| - |\partial(A)|) + |\partial(A)$, or $\partial(A) \geq 2|N(A)| - k|A|$. We will show that with high probability for all such A, $|N(A)| > 3k|A|/4$, and hence $\partial(A) \geq k|A|/2$.

If not, there are sets $A \subset R$ and $B \subset L$ so that $N(A) \subseteq B$ and $|B| = 3k|A|/4$. We will bound the probability that this is true for fixed sets A, B and then take a union bound. We can view picking a random (d, k) bipartite graph as picking a random matching between d half-edges adjacent to each $x \in L$ and k such half-edges adjacent to each $y \in R$; if a half edge for x is matched to a half-edge for y, it forms an edge between x and y.

We can form this matching by going through the half edges for nodes in R and for each randomly selecting an unmatched half-edge for some node in L. We start with the edges for A in an arbitrary order. If we condition on all previous neighbors for A being in B, the number of half-edges left still available for B is less than $d|B|$, whereas the number for $\overline{B}$ stays at exactly $d(n - |B|)$. Thus, the conditional probability that the next edge formed is also in B is at most $|B|/n$, and we do this for each of $k|A|$ edges, meaning the probability that all neighbors are in B is at most $(|B|/n)^{k|A|}$.

Now, for a fixed $|A|$ and setting $|B| = 3k|A|/4$, we take the union bound over all subsets A and B. This gives a total probability of failure for some set A of size a as :

$$\binom{m}{a}\binom{n}{3ka/4}(3ka/4n)^{ka}$$

$$\leq (em/a)^a(4en/3ka)^{3ka/4}(3ka/4n)^{ka}$$

$$\leq (em/a)^a(e^3ka/n)^{ka/4} = (ekn/da)^a(e^3ka/n)^{ka/4} = (e^{3k/4+1}a^{k/4-1}k^{k/4+1}/dn^{k/4-1})^a$$

Since we are assuming $a < n/(e^6k^2)$, the base in the above expression is at most

$$e^{3k/4+1}(n/e^6k^2)^{k/4-1}k^{k/4+1}/dn^{k/4-1}$$

$$= e^{7-3k/4}k^{3-k/4}/d$$

which for $k \geq 12$ is bounded below e^{-2}, meaning the probability of such a bad set existing is exponentially small in a, and the probability of such a bad set existing for any a is less than 1/2.

□

Definition 4. *For a Boolean vector $X = \{x_1, \ldots, x_n\}$, we define $\mathcal{L}_{n,m,k_1,k}(X)$ to be a distribution over k-CNF formulas over n variables $X = \{x_1, \ldots, x_n\}$ obtained by selecting m parities, where each parity is represented by a node on the right of a bipartite graph $G(L, R)$ with left degree bounded by k_1 and right degree bounded by k chosen uniformly at random from all such graphs.*

Lemma 1. *Let $F_{n,k}$ be a tautology given by $AX = b$ over variables $X = \{x_1, \ldots, x_n\}$ where A is the adjacency matrix of a graph drawn at random from $\mathcal{L}_{n,m,k_1,k}$ where $m = 10n$, for large enough constants $k_1, k > 0$, and b is chosen randomly. Then the following hold with high probability for a small enough $\epsilon > 0$:*

a) Any subset of a $(1-\epsilon)$-fraction of the equations in $F_{n,k}$ is unsatisfiable

b) Any subset of a $(1-\epsilon)$-fraction of the equations in $F_{n,k}$ requires PC *degree $c_2(n)$ to refute, for some $c_2 > 0$.*

Proof. a) The probability that a set of $(1-\epsilon)10n$ random parities (i.e. for a random choice of b) is satisfiable is at most 2^{-9n} for a small enough ϵ. The probability that any such subset of $F_{n,k}$ is satisfiable is therefore at most $2^{(-n(9-10H(\epsilon)))}$, which is exponentially small for a small enough ϵ.

b) This follows directly from [AR01], Theorem 3.8 and Theorem 4.4, since by Theorem 3 the graph with adjacency matrix A has good expansion with high probability.

□

We now want to compose $F_{n,k}$ with a function we call SELECT, which encodes a complete bipartite graph such that nodes on the left represent equations of $F_{n,k}$ of which a large enough subset is selected by the nodes on the right. In order to eliminate an equation from being selected on the right, we add it to a running list of bad equations, and reduce the proof by the set of assertions stating that no node on the right can be assigned this equation. Conversely, by substituting a complete assignment for the variables of SELECT, we would like to be able to select sufficiently many equations from any large enough subset on the left.

We now define our tautology below.

Definition 5. *Let $F_{n,k}(X) = \{E_i \mid i \in [m]\}$ and ϵ be as in Lemma 1, $m = 10n$, $m' = (1 - \epsilon/2)m$ and Let $Y = \{y_{ij}, i \in [m'], j \in [\log m]\}$ and let Y_i be defined appropriately. For bits $b_1 \cdots b_{\log m}$ let $Y_i \neq b_1 \cdots b_{\log m}$ represent the formula $\prod_j (y_{ij} - b_j \oplus 1)$. Then $F^{SEL}_{n,k}$ is the following set of clauses in $O(n)$ variables $X \cup Y$.*

$$Y_i \neq b_1 \cdots b_{\log m} \vee E_{b_1 \cdots b_{\log m}}$$

$$Y_i \neq b_1 \cdots b_{\log m} \vee Y_{i'} \neq b_1 \cdots b_{\log m}$$

for $i \neq i'$

In the above definition, we refer to the variables $Y_i = y_{i1} \cdots y_{i \log m}$ as the i^{th} pigeon. Thus the axioms can be interpreted as the following two statements:

1. If the i^{th} pigeon maps to the string $b_1 \cdots b_{\log m}$ for any i, the equation $E_{b_1 \cdots b_{\log m}}$ is true.
2. For any $b_1 \cdots b_{\log m}$ and indices i, i', either the i^{th} pigeon does not map to it or the i'^{th} pigeon does not map to it.

Since we are working with Polynomial Calculus, the above CNF formula has to be translated into a set of polynomials, as described in Definition 3.

Definition 6. *A locality κ extension variable is a new variable z together with a single polynomial defining constraint $z = q(w_{i_1}, ..w_{i_k})$ for some polynomial q and κ original variables $w_{i_1}, \ldots, w_{i_k} \in X \cup Y$.*

Definition 7. *Let $\psi_{N,\kappa,M}(W)$ denote the unsatisfiable formula $F^{SEL}_{n,k}$ with M extension axioms Z of locality κ, and where $W = X \cup Y \cup Z$, and $|W| = N$.*

4 The Lower Bound

4.1 Technical Proof Overview.

We start with a PC refutation Π of $\psi_{N,\kappa,M}(W)$ over $\mathbb{F}_p$. Conventionally, proof size lower bounds are reduced to degree lower bounds, a single step of which involves finding a variable that occurs in a large fraction of high degree terms of the proof and setting it to zero. In our setting, if the latter turns out to be an extension variable, z with extension axiom $z = f(X, Y)$ it may be *nonsingular* meaning that setting $z = 0$ will falsify the extension axiom for z. In this case, we cannot simply eliminate the high degree terms containing z by setting $z = 0$. Sokolov [Sok20] introduced *quadratic degree* as a measure to be used instead of degree in such cases and showed that a refutation of low quadratic degree can be turned into one of low degree. Quadratic degree essentially measures the maximal degree of the *square* of each polynomial P occurring in the proof. Sokolov also introduced an operation *Split* that acts on a proof line by line in order to to reduce quadratic degree in the special case of nonsingular variables that always take on values in ± 1.

In our case, we have to deal with the case of both singular as well as nonsingular variables, and where the nonsingular variables can depend arbitrarily on a logarithmic number of original variables. To accomplish this, we give a procedure that reduces reduce both ordinary degree (for singular variables occurring in the proof) as well as quadratic degree (for nonsingular variables).

The first phase of our procedure deals with eliminating the set S of all high *singular* degree terms – that is, terms that contain many singular variables. This is handled in a standard way, by finding a singular variable w occurring in many terms of S, and applying the restriction σ which sets $w = 0$. Then in order to ensure that the properties of the tautology remain intact after applying σ, we maintain a list B of "bad" axioms and modify the formula and proof (using **X-cleanup**, **Y-cleanup** and Lemma 10) so that the selector variables cannot map to any axiom in B. In this case, we add to B any axiom that is affected by σ and modify the proof so that the Y-variables avoid mapping to any axiom in B.

In the second more difficult phase of our procedure deals with removing all terms of large quadratic degree from the proof. Assume that w is some *nonsingular* variable occuring in many terms of high quadratic degree. Since all variables in $X \cup Y$ are singular, w must be an extension variable z with corresponding extension axiom $z = f(X, Y)$. First, we apply a partial assignment σ to all but one X-variable of $f(X, Y)$ so that $f(X, Y)|_\sigma$ reduces to a linear function of a single X-variable, x (extension variables that only depend on the selector variables Y are inconsequential since we substitute a complete assignment to the variables Y at the end of our procedure). After applying σ (which sets a small number of both X and Y variables), we apply cleanup procedures to get rid of all axioms that were affected by σ, and also those that contain x. As in the first phase, this involves updating our list B of bad axioms, and as well as modifying the proof, using **X-cleanup**, **Y-cleanup** procedures together with Lemma 10.

Now that the axioms are free of both x and z, our main technical contribution (Lemma 9) significantly generalizes Sokolov's Split operation in order to eliminate z from the proof (thus making z irrelevant). This in turn yields a near-constant factor reduction in the number of large quadratic degree terms. By iterating this process, we obtain a refutation of a reduced version of $\psi_{N,\kappa,M}(X)$ of low quadratic degree. Crucially, our procedure for reducing quadratic degree does not increase the singular degree, and thus at the end of the second phase, we have extracted a proof (of a reduced but still hard formula) that has low singular degree as well as low quadratic degree. Then by Lemma 3, this in turn implies a proof of small overall degree.

Finally, we argue that we can substitute an assignment for the selector variables Y (since each step adds only a small number of axioms to the bad set B, and therefore the total size of B is at most a constant fraction of the original axioms) in order to obtain a low degree refutation of a large subset of $F_{n,k}$, which gives us a contradiction.

4.2 Quadratic Degree, and Removing Irrelevant Variables

Definition 8 (Singular degree)**.** *For an extension variable z, we say that it is singular if it can take the value zero. Else we say that it is non-singular (any non-extension variable w is singular by default since $w^2 = w$ holds). By Lemma 2 below, a nonsingular variable implies $z^{p-1} = 1$. For a term t, let the singular degree $sing(t)$ denote the number of singular variables in t.*

Lemma 2. *For z non-singular, we can derive $z^{p-1} = 1$ from the extension axiom for z.*

Proof. Let q be any multi-linear polynomial in the original variables and let $z = q$ be the defining equation for z. Look at $q^{p-1}(X,Y)$. Since q is never $0 \mod p$ for Boolean inputs, this is always equal to 1 for Boolean inputs. But since every function from Boolean inputs to the field has a unique representation as a multi-linear function, when we make q^{p-1} multi-linear, it must be the identically 1 polynomial. Then $z^{p-1} = q^{p-1}$ is derivable from the defining axiom, which means $z^{p-1} - 1$ is derivable. □

Definition 9. *For a term t and a variable w (or its negated version $\bar{w}$),* $\deg(t, w)$ *is equal to the degree of w in t. Note that since we are over a finite field of characteristic p,* $\deg(t, w) \leq p$*. If w is nonsingular, then $w^{p-1} = 1(modp)$, so* $\deg(t, w) \leq p - 1$*. For a term t the overall degree of t,* $\deg(t)$*, equals* $\sum_{w\in W} \deg(t, w)$*.*

The next definition is a generalization/modification of Sokolov's definition of quadratic degree for the more general scenario where the proof contains both singular and non-singular variables.

Definition 10 (Quadratic degree)**.** *For a pair of terms t_1, t_2, and a variable w (or its negated version $\bar{w}$), we define the weight of w with respect to t_1 and t_2, $Qdeg(t_1, t_2, w)$ as follows. If $w \in X \cup Y$, then $Qdeg(t_1, t_2, w) = 1$ if w occurs in at least one of t_1 or t_2; if w is an extension variable, then $Qdeg(t_2, t_2, w) = 1$ if and only if* $\deg(t_1, w) \neq \deg(t_2, w)$*. The overall weight of the pair t_1, t_2, $Qdeg(t_1, t_2)$, is equal to $\sum_{w\in W} Qdeg(t_1, t_2, w)$. The weight of a polynomial P is equal to the maximum weight over all pairs (t_1, t_2) such that $t_1, t_2 \in P$. The quadratic degree of P is defined as the maximum weight of P. For a proof Π, the quadratic degree is the maximum quadratic degree over all polynomials $P \in \Pi$.*

Definition 11 ($\mathcal{Q}$)**.** *For a polynomial P, $\mathcal{Q}(P) = \{(t_1, t_2)|t_1, t_2 \in P\}$. For a pair of polynomials P_1 and P_2, $\mathcal{Q}(P_1, P_2) = \{(t_1, t_2)|t_1 \in P_1, t_2 \in P_2$ or vice versa$\}$. $\mathcal{Q}(\Pi) = \cup_{P\in\Pi}\mathcal{Q}(P)$.*

Definition 12 ($\mathcal{H}_d$)**.** *For a proof Π, $\mathcal{H}_d(\Pi)$ denote the set of pairs (t_1, t_2) of high quadratic degree. That is, $\mathcal{H}_d(\Pi)$ is the set of pairs of terms (t_1, t_2) such that t_1, t_2 both occur in P for some polynomial $P \in \Pi$, and $Qdeg(t_1, t_2) \geq d$.*

Observation 1. *Substitution does not raise the quadratic degree, i.e. if P is a polynomial, x is a variable occuring in it and $a \in \mathbb{F}_p$ then the quadratic degree of $P_{|x=a}$ is at most that of P.*

Proof. This follows from the fact that for any two terms $t_1, t_2 \in P$, $Qdeg(t_1, t_2, w)$ remains unchanged if w is different from x, and decreases if $w = x$. □

The following is a generalized version of the argument from [Sok20] that shows how to convert a proof with low quadratic degree to one with low degree.

Lemma 3. *If a set of unsatisfiable polynomials $\mathcal{F}$ of degree d_0 has a* PC *refutation of quadratic degree and singular degree at most d, then it has a* PC *refutation of degree $O(p \max(d, d_0))$.*

Proof. We first observe that for any two terms t_1, t_2, $deg(t_1 t_2^{p-2}) \leq p \cdot (Qdeg(t_1, t_2) + sing(t_1) + sing(t_2))$. This is due to the following. Note that any singular variable that appears in either t_1 or t_2 appears in $t_1 t_2^{p-2}$ with degree at most p. Thus, the degree of singular variables in $t_1 t_2^{p-2}$ is at most p times $sing(t_1) + sing(t_2)$. For a nonsingular extension variable z that occurs in t_1 and t_2 such that $deg(t_1, z) = deg(t_2, z)$, $deg(t_1 t_2^{p-2}, z) = Qdeg(t_1, t_2, z) = 0$. Any other nonsingular variable that occurs in at least one of t_1 and t_2 has $deg(t_1 t_2^{p-2}, x) \leq p - 1$ and $Qdeg(t_1, t_2, x) = 1$. Therefore the degree of nonsingular variables in $t_1 t_2^{p-2}$ is at most $p - 1$ times $Qdeg(t_1, t_2)$.

From the above observation, it suffices to prove the following: Let F be a set of unsatisfiable polynomials of degree d_0 with a PC refutation, Π, over $\mathbb{F}_p$. Further suppose that for every polynomial $P \in \Pi$, and for every pair of terms $t_1, t_2 \in P$, $\deg(t_1 t_2^{p-2}) < d$. Then F has a PC refutation of degree $\max(3pd, d_0)$. Since by our assumption the degree of singular variables is at most d, below we construct a refutation by multiplying each line of the original refutation by non-singular variables to lower their degree to at most $2pd$, which suffices to prove the statement.

For a term t in the proof, let $\mathcal{A}(t)$ denote the subterm consisting of only non-singular variables. Then clearly we have $\mathcal{A}(t)^{p-1} = 1$. Note that we also have $\deg(\mathcal{A}(t_1)^{p-2} t_2) \leq pd$ for any two terms t_1, t_2 by our assumption. For every line P_j in the refutation, we pick a term $t_j \in P_j$ and define $P'_j = \mathcal{A}(t_j)^{p-2} P_j$. Note that $\deg P'_j \leq pd$. We now show that each P'_j can be derived in degree $\max(2pd, d_0)$. If P_j is one of the axioms, we multiply by $\mathcal{A}(t_j)^{p-2}$ to get P'_j, and this takes degree $\max(pd, d_0)$. If $P_j = x_i P_{j_1}$ for $j_1 < j$, we choose t_j such that $t_j = x_i t_{j_1}$. Then we have P'_j is equal to $x_i P'_{j_1}$ if x_i is singular, and equal to P'_{j_1} otherwise. Finally, let $P_j = P_{j_1} + P_{j_2}$ for $j_1, j_2 < j$. We pick an arbitrary term $t_j \in P_j$. Then we have $P'_j = \mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_1}) P'_{j_1} + \mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_2}) P'_{j_2}$. We now show that $\deg(\mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_1})) \leq pd$ and $\deg(\mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_2})) \leq pd$ to conclude the proof. Since every term in P_j appears in one of P_{j_1}, P_{j_2}, let $t_j \in P_{j_1}$ without loss of generality. Then we have that t_j, t_{j_1} both appear in P_{j_1} and thus is $\deg(\mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_1})) \leq pd$. If $t_{j_2} \in P_j$ i.e. it is not canceled in the sum $P_{j_1} + P_{j_2}$, then we have t_j, t_{j_2} both appear in P_j and hence $\deg(\mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_2})) \leq pd$. If $t_{j_2} \notin P_j$, this implies that it was canceled in the sum $P_{j_1} + P_{j_2}$ and therefore $t_{j_2} \in P_{j_1}$ and $\deg(\mathcal{A}(t_j)^{p-2} \mathcal{A}(t_{j_2})) \leq d$. □

Lemma 4. *Let Π be a proof and let z be an extension variable such that the corresponding extension axiom implies the line $z^k - 1 = 0$ for some positive integer $k < p$. Let Π' be the proof obtained by reducing each line of Π by $z^k - 1 = 0$. Then we have $|\mathcal{H}_d(\Pi')| \leq |\mathcal{H}_d(\Pi)|$ for any $d \geq 0$.*

Proof. Since the extension axiom for z implies $z^k - 1$, z is nonsingular. Consider a polynomial $P \in \Pi$ and a pair of terms (t_1, t_2) that occur in P. If $wt(t_1, t_2, z) = 0$, then the weight will still be 0 after reducing by $z^k = 1$, and thus $|\mathcal{H}_d(\Pi')| \leq |\mathcal{H}_d(\Pi)|$. □

Lemma 5. *Let $a, b \in \mathbb{F}_p^*$ such that ℓ is the least positive integer less than p with $a^\ell = b^\ell$. Let P be a polynomial in $\mathbb{F}_p[X]$ and let z be an extension variable that occurs in P*

such that the corresponding extension axiom implies the line $(z-a)(z-b)=0$. Then, for any two distinct non-negative integers $\ell_1, \ell_0 < \ell$ there exists a unique polynomial $R = R_1 z^{\ell_1} + R_0 z^{\ell_0}$ such that $R = P \mod (z-a)(z-b)$.

Proof. Since $R = P \mod (z-a)(z-b)$, we have $R(a) = P(a)$ and $R(b) = P(b)$, and therefore it is sufficient to show that there is a unique solution to this pair of equations. Suppose that $\ell_0 < \ell_1$. We have $\begin{vmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{vmatrix} = a^{\ell_0} b^{\ell_0} (b^{\ell_1-\ell_0} - a^{\ell_1-\ell_0})$. Since $\ell_1 - \ell_0 < \ell$, this matrix is non-singular over $\mathbb{F}_p$ and therefore the system of equations

$$R_1 a^{\ell_1} + R_0 a^{\ell_0} = P(a)$$

$$R_1 b^{\ell_1} + R_0 b^{\ell_0} = P(b)$$

has a unique solution. □

Definition 13 ($Split_{z,\ell_1,\ell_0}$)**.** *For a polynomial P and a variable z such that the identity $(z-a)(z-b)=0$ holds, and integers ℓ_1, ℓ_0 such that $\ell_0 < \ell_1$ and $a^{\ell_1-\ell_0} \neq b^{\ell_1-\ell_0}$, let $R = R_1 z^{\ell_1} + R_0 z^{\ell_0}$ be the unique polynomial given by the previous lemma such that $R = P \mod (z-a)(z-b)$. $Split_{z,\ell_1,\ell_0}(P)$ is defined as the pair of polynomials $\{R_1, R_0\}$. For a proof Π, we define $Split_{z,\ell_1,\ell_0}(\Pi)$ to be the set of lines $Split_{z,\ell_1,\ell_0}(P)$ for all $P \in \Pi$.*

Lemma 6. *Let P be a polynomial of the form $P_{\ell-1} z^{\ell-1} + \cdots + P_0$. Then for $\ell_0 < \ell_1 < \ell$, $Split_{z,\ell_1,\ell_0}(P) = \{R_1, R_0\}$ where*

$$R_1 = P_{\ell_1} + \sum_{i<\ell, i\neq \ell_0} c_{1i} P_i$$

$$R_0 = P_{\ell_0} + \sum_{i<\ell, i\neq \ell_1} c_{0i} P_i$$

for some constants $c_{1i}, c_{0i} \in \mathbb{F}_p$.

Proof. This is easily verified from the definition of $Split_{z,\ell_1,\ell_0}$. □

Lemma 7. *Let z be a variable that occurs in a proof Π but does not occur in any axioms except for $(z-a)(z-b)=0$. Then, for any ℓ_1 and ℓ_0 such that $\ell_0 < \ell_1$ and $a^{\ell_1-\ell_0} \neq b^{\ell_1-\ell_0}$, $Split_{z,\ell_1,\ell_0}(\Pi)$ is a valid refutation and can be derived without increasing the size of $\mathcal{H}_d(\Pi)$ or the singular degree of Π.*

Proof. Let $P_j = P_{j(k-1)} z^{k-1} + \cdots + P_{j2} z^2 + P_{j1} z + P_{j0}$ be the j^{th} line in the refutation Π, where k is the least integer such that the identity $z^k - 1 = 0$ holds (this is without loss of generality by Lemma 4). We view P_j as a univariate polynomial in z over the appropriate ring. Let $R_j(z) = R_{j1} z^{\ell_1} + R_{j0} z^{\ell_0}$ be a polynomial such that $P_j(z) = R_j(z) \mod (x-a)(x-b)$. Then we have $P_j(a) = R_j(a)$ and $P_j(b) = R_j(b)$, thus by Lemma 5 $R_j(z)$ is uniquely given by

$$\begin{pmatrix} R_{j1} \\ R_{j0} \end{pmatrix} = \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix}^{-1} \begin{pmatrix} P_j(a) \\ P_j(b) \end{pmatrix}$$

We now proceed to show by induction that the set of lines $\{R_{j1}, R_{j0}\}$ is a valid derivation. For the base case, note that all of the axioms of $\mathit{\Phi}$ are either free of z or eliminated as a result of reducing by $(z-a)(z-b)$, and hence their Split versions are derivable, Now for a line $P_j = \alpha P_{j_1} + \beta P_{j_2}$ for some j_1 and j_2 less than j and $\alpha, \beta \in \mathbb{F}_p$, then we have that $R_{j1} = \alpha R_{j_1 1} + \beta R_{j_2 1}$ and therefore by induction we have a proof of R_{j1} (similarly for R_{j0}). If $P_j = wP_{j'}$ for some $j' < j$ and some variable w distinct from z, we have that $R_{j1} = wR_{j'1}$ (similarly for R_{j0}). Lastly, if $P_j = zP_{j'}$, we have

$$\begin{pmatrix} R_{j'1} \\ R_{j'0} \end{pmatrix} = \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix}^{-1} \begin{pmatrix} P_{j'}(a) \\ P_{j'}(b) \end{pmatrix}$$

from which we need to derive

$$\begin{aligned} \begin{pmatrix} R_{j1} \\ R_{j0} \end{pmatrix} &= \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix}^{-1} \begin{pmatrix} P_j(a) \\ P_j(b) \end{pmatrix} \\ &= \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix}^{-1} \begin{pmatrix} aP_{j'}(a) \\ bP_{j'}(b) \end{pmatrix} \\ &= \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix}^{-1} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} a^{\ell_1} & a^{\ell_0} \\ b^{\ell_1} & b^{\ell_0} \end{pmatrix} \begin{pmatrix} R_{j'1} \\ R_{j'0} \end{pmatrix}. \end{aligned}$$

□

Lemma 8. *Let Π be a proof and let z be an extension variable that does not occur in any of the axioms except the identity $(z-a)(z-b) = 0$ for some $a, b \in \mathbb{F}_p^*$ and occurs*[1] *in at least an ϵ fraction of pairs (t_1, t_2) in $\mathcal{H}_d(\Pi)$ for an arbitrary integer $d \geq 0$. Then there exist integers $\ell_1, \ell_0 < p$ such that the size of $\mathcal{H}_d(Split_{z,\ell_1,\ell_0}(\Pi))$ is at most $(1 - \epsilon/p^2)$ times the size of $\mathcal{H}_d(\Pi)$.*

Proof. The arguments below hold for $\mathcal{H}_d(\Pi)$ for any d, so for simplicity we show the proof for $\mathcal{H}_0(\Pi) = \mathcal{Q}(\Pi)$. For a line $P \in \Pi$, let $\mathcal{Q}_z(P)$ and $\mathcal{Q}_{\neg z}(\Pi)$ be subsets of $\mathcal{Q}(P)$ with $wt(t_1, t_2, z) = 1$ and $wt(t_1, t_2, z) = 0$ for all $(t_1, t_2) \in \mathcal{Q}_z(P)$ and $(t_1, t_2) \in \mathcal{Q}_{\neg z}(P)$ respectively. By Lemma 4, we assume without loss of generality that Π is reduced by $z^\ell - 1 = 0$ where $\ell > 0$ is the least such integer. Let $P = P_{\ell-1}z^{\ell-1} + \cdots + P_2 z^2 + P_1 z + P_0$ and $\mathcal{Q}_{ij}(P) = \mathcal{Q}(P_i z^i, P_j z^j)$ for $i, j < \ell$. Then we have

$$\mathcal{Q}_z(P) = \sqcup_{i<j} \mathcal{Q}_{ij}(P)$$
$$\mathcal{Q}_{\neg z}(P) = \cup_i \mathcal{Q}(P_i)$$

where $\sqcup$ denotes disjoint union. This is because by the definition of $\mathcal{Q}_{ij}(P)$, for any pair $(t_1, t_2) \in \mathcal{Q}_{ij}(P)$ we have that $z^i \in t_1$ and $z^j \in t_2$ or vice versa. Therefore, for two pairs (i_1, j_1) and (i_2, j_2) such that $i_1 \neq j_1$ and $i_2 \neq j_2$ and $\{i_1, j_1\} \neq \{i_2, j_2\}$, we have that $\mathcal{Q}_{i_1 j_1}(P) \cap \mathcal{Q}_{i_2 j_2}(P) = \emptyset$. Note that this property also extends to $\cup_P \mathcal{Q}_{ij}(P)$. Since $\mathcal{Q}(\Pi) = \cup_{P \in \Pi} \mathcal{Q}(P)$, we have

$$\mathcal{Q}_z(\Pi) = \cup_P \sqcup_{i<j} \mathcal{Q}_{ij}(P) = \sqcup_{i<j} \cup_P \mathcal{Q}_{ij}(P) \tag{1}$$
$$\mathcal{Q}_{\neg z}(\Pi) = \cup_P \cup_i \mathcal{Q}(P_i)$$

and therefore

[1] We say that a variable z occurs in a pair (t_1, t_2) if $wt(t_1, t_2, z) \neq 0$.

$$\mathcal{Q}(\Pi) = \big(\sqcup_{i<j} \cup_P \mathcal{Q}_{ij}(P) \big) \sqcup \big(\cup_P \cup_i \mathcal{Q}(P_i) \big)$$

$$|\mathcal{Q}(\Pi)| = \sum_{i<j} | \cup_P \mathcal{Q}_{ij}(P)| + | \cup_P \cup_i \mathcal{Q}(P_i)| \tag{2}$$

Let us now evaluate a similar expression for $\mathcal{Q}(Split_{z,\ell_1,\ell_0}(\Pi))$. Let $\mathcal{Q}^0_{ij}(P) = \mathcal{Q}(P_i, P_j)$. Note that $|\cup_P \mathcal{Q}^0_{ij}(P)| \leq |\cup_P \mathcal{Q}_{ij}(P)|$. Then since by Lemma 6 $Split_{z,\ell_1,\ell_0}(P)$ consists of lines of the form

$$R_1(P) = P_{\ell_1} + \sum_{i<\ell, i\neq \ell_0} c_{1i} P_i$$

$$R_0(P) = P_{\ell_0} + \sum_{i<\ell, i\neq \ell_1} c_{0i} P_i$$

for some constants $c_{1i}, c_{0i} \in \mathbb{F}_p$, we have

$$\begin{aligned}
\mathcal{Q}(Split_{z,\ell_1,\ell_0}(\Pi)) &= \cup_P \mathcal{Q}(Split_{z,\ell_1,\ell_0}(P)) \\
&= \cup_P (\mathcal{Q}(R_1(P)) \cup \mathcal{Q}(R_0(P))) \\
&\subseteq \cup_P \big(\cup_{\ell_0 \neq i<j \neq \ell_1} \mathcal{Q}^0_{ij}(P) \big) \cup \big(\cup_i \mathcal{Q}(P_i) \big) \\
&= \big(\cup_{\ell_0 \neq i<j \neq \ell_1} \cup_P \mathcal{Q}^0_{ij}(P) \big) \cup \big(\cup_P \cup_i \mathcal{Q}(P_i) \big)
\end{aligned}$$

Therefore, we have that

$$\begin{aligned}
|\mathcal{Q}(Split_{z,\ell_1,\ell_0}(\Pi))| &\leq \sum_{\ell_0 \neq i<j \neq \ell_1} | \cup_P \mathcal{Q}^0_{ij}(P)| + | \cup_P \cup_i \mathcal{Q}(P_i)| &(3) \\
&\leq \sum_{\ell_0 \neq i<j \neq \ell_1} | \cup_P \mathcal{Q}_{ij}(P)| + | \cup_P \cup_i \mathcal{Q}(P_i)| &(4) \\
&\leq |\mathcal{Q}(\Pi)| - | \cup_P \mathcal{Q}_{\ell_0 \ell_1}(P)| &(5)
\end{aligned}$$

where the last bound follows from equation 2. Now, by our assumption, since $\mathcal{Q}_z(\Pi)$ is at least an ϵ fraction of $\mathcal{Q}(\Pi)$ we have from equation 1 by an averaging argument that for some $\ell_0 < \ell_1 < \ell$, $\cup_P \mathcal{Q}_{\ell_0 \ell_1}(P)$ is at least a ϵ/p^2 fraction of $\mathcal{Q}(\Pi)$. For such ℓ_0, ℓ_1 from equation 5 we have $|\mathcal{Q}(Split_{z,\ell_1,\ell_0}(\Pi))| \leq (1 - \epsilon/p^2)|\mathcal{Q}(\Pi)|$.

□

Below we prove a slightly more complex version of the previous lemma.

Lemma 9. *Let Π be a proof, $x \in X$ and let $z = \alpha x + \beta$ be a variable such that x, z do not occur in any other axioms except $x^2 = x$, with z occurring in at least an ϵ fraction of the vectors in $\mathcal{H}_d(\Pi)$, for some $\alpha, \beta \in \mathbb{F}^*_p$ and any integer $d \geq 0$. Then there exist a refutation Π' such that the size of $\mathcal{H}_d(\Pi')$ is at most $(1 - \epsilon/3p^2)$ times the size of $\mathcal{H}_d(\Pi)$.*

Proof. The proof is by a simple case analysis followed by appealing to the previous lemma. Once again we only show the case of $\mathcal{H}_0(\Pi) = \mathcal{Q}(\Pi)$. Let $\mathcal{Q}_z(P)$ be the subset of $\mathcal{Q}(P)$ with $wt(t_1, t_2, z) = 1$ for all $(t_1, t_2) \in \mathcal{Q}_z(P)$. Firstly, note that substituting $x = \alpha^{-1}(z - \beta)$ in the identity $x^2 = x$ we get $(z - a)(z - b) = 0$ for some $a, b \in \mathbb{F}_p$. If either a or b is zero, then we can set $z = 0$ by setting x appropriately to eliminate all terms in $\mathcal{Q}(\Pi)$ containing z. Therefore we assume that $a, b \in \mathbb{F}_p^*$, i.e. z is not singular. By Lemma 4, we assume without loss of generality that Π is reduced by $z^\ell - 1 = 0$ where $\ell > 0$ is the least such integer. Then each line P of Π is of the form

$$\begin{aligned} P = (P'_{\ell-1}z^{\ell-1} + \cdots + P'_2z^2 + P'_1z + P'_0) + x(P''_{\ell-1}z^{\ell-1} + \cdots + P''_2z^2 + P''_1z + P''_0) \\ + \bar{x}(P'''_{\ell-1}z^{\ell-1} + \cdots + P'''_2z^2 + P'''_1z + P'''_0) \end{aligned}$$

We define the following subsets of $\mathcal{Q}(\Pi)$: (note that since $x \in X$, $Qdeg(x, x, x) = 1$)

$$\mathcal{Q}_{zx} = \cup_P \sqcup_{i<j} \mathcal{Q}(P'_iz^i, xP''_jz^j) \cup \mathcal{Q}(xP''_iz^i, P'_jz^j) \cup \mathcal{Q}(xP''_iz^i, xP''_jz^j)$$

$$\mathcal{Q}_{z\bar{x}} = \cup_P \sqcup_{i<j} \mathcal{Q}(P'_iz^i, \bar{x}P'''_jz^j) \cup \mathcal{Q}(\bar{x}P'''_iz^i, P'_jz^j) \cup \mathcal{Q}(\bar{x}P'''_iz^i, \bar{x}P'''_jz^j)$$

$$Q_{zx\bar{x}} = \cup_P \sqcup_{i<j} \mathcal{Q}(xP''_iz^i, \bar{x}P'''_jz^j) \cup \mathcal{Q}(\bar{x}P'''_iz^i, xP''_jz^j)$$

$$\mathcal{Q}_z = \cup_P \sqcup_{i<j} \mathcal{Q}(P'_iz^i, P'_jz^j)$$

and observe that

$$\mathcal{Q}_z(\Pi) = \mathcal{Q}_{zx} \sqcup \mathcal{Q}_{z\bar{x}} \sqcup \mathcal{Q}_{zx\bar{x}} \sqcup \mathcal{Q}_z \tag{6}$$

Now, if $|\mathcal{Q}_{zx} \sqcup \mathcal{Q}_{zx\bar{x}}(\Pi)| \geq \epsilon|\mathcal{Q}(\Pi)|/3$, then we set $x = 0$ to obtain a refutation Π_1, for which it is easy to see that

$$\mathcal{Q}_z(\Pi_1) = \mathcal{Q}_{z\bar{x}} \sqcup \mathcal{Q}_z$$

$$\mathcal{Q}_{\neg z}(\Pi_1) \subseteq \mathcal{Q}_{\neg z}(\Pi)$$

and therefore $|\mathcal{Q}(\Pi_1)| \leq (1-\epsilon/3)|\mathcal{Q}(\Pi)|$. Otherwise, if $|\mathcal{Q}_{z\bar{x}} \sqcup \mathcal{Q}_{zx\bar{x}}(\Pi)| \geq \epsilon|\mathcal{Q}(\Pi)|/3$ then we similarly set $x = 1$ and obtain a refutation Π_1 with $|\mathcal{Q}(\Pi_1)| \leq (1-\epsilon/3)|\mathcal{Q}(\Pi)|$.

If both of the above don't hold, then we have $|\mathcal{Q}_{zx} \sqcup \mathcal{Q}_{z\bar{x}} \sqcup \mathcal{Q}_{zx\bar{x}}(\Pi)| \leq 2\epsilon|\mathcal{Q}(\Pi)|/3$ and from equation 6 and our assumption we have $|\mathcal{Q}_z| \geq \epsilon|\mathcal{Q}(\Pi)|/3$. Let $\ell_0 < \ell_1$ be indices (that exist by an averaging argument) such that $\cup_P \mathcal{Q}(P'_{\ell_0}z^{\ell_0}, P'_{\ell_1}z^{\ell_1})$ is of size at least $\epsilon|\mathcal{Q}(\Pi)|/3p^2$. We now substitute $x = \alpha^{-1}(z - \beta)$ in Π and apply $Split_{z,\ell_0,\ell_1}$. It is easy to see that this replaces each line P of Π with two lines of the form

$$R_1(P) = P'_{\ell_1} + \sum_{i<\ell, i\neq\ell_0} c'_{1i}P'_i + \sum_{i<\ell} c''_{1i}P''_i$$

$$R_0(P) = P'_{\ell_0} + \sum_{i<\ell, i\neq\ell_1} c'_{0i}P'_i + \sum_{i<\ell} c''_{1i}P''_i$$

for some constants $c'_{1i}, c'_{0i}, c''_{1i}, c''_{0i} \in \mathbb{F}_p$. By an analysis similar to the previous lemma we can show that

$$\begin{aligned} |\mathcal{Q}(Split_{z,\ell_0,\ell_1}(\Pi))| &\leq |\mathcal{Q}(\Pi)| - |\cup_P \mathcal{Q}(P'_{\ell_0}z^{\ell_0}, P'_{\ell_1}z^{\ell_1})| \\ &\leq (1 - \epsilon/3p^2)|\mathcal{Q}(\Pi)|. \end{aligned}$$

□

Lemma 10. *Let Π be a refutation and let $Y_i \neq b_1 \dots b_{\log m} \vee E_{b_1 \dots b_{\log m}}$ be one of its axioms. Then there exists another valid refutation Π' with the latter axiom replaced by the axiom $Y_i \neq b_1 \dots b_{\log m} \equiv \prod_j (y_{ij} - b_j \oplus 1) = 0$, such that the quadratic degree and singular degree of Π' are at most those of Π.*

Proof. Note that the axiom $Y_i \neq b_1 \dots b_{\log m} \vee E_{b_1 \dots b_{\log m}}$ can be derived from the axiom $\prod_j (y_{ij} - b_j \oplus 1) = 0$. We construct Π' as follows. We first derive the former axiom from the latter in Π'. Besides this derivation, Π' involves the same steps as Π'. Note that since this derivation only involves PCR monomials, this does not raise the quadratic degree of Π'. Also, its singular degree is not more than that of Π. □

4.3 Proof of Main Theorem

Theorem 4. *Any* PC *refutation of $\psi_{N,\kappa,M}(W)$ is of size at least $2^{\Omega\left(\frac{n^2}{\kappa^2 2^\kappa (M+n\log(n))}\right)}$.*

Proof. Let Π be a refutation of $\psi_{N,\kappa,c}(W)$ of size at most $2^{\gamma n^2/(\kappa^2 2^\kappa (M+n\log(n)))}$ for a small enough constant γ. Given an alleged PC refutation Π, Algorithm 1 (defined below) will apply a sequence of restrictions and cleanup steps in order to produce a refutation Π'' of a restricted version of $\psi_{N,\kappa,c}(W)$ with the property that both the singular as well as the quadratic degree of Π'' are at most d. The algorithm contains two while loops, the first of which iteratively removes all terms of high singular degree, and the second iteratively removes all pairs of terms of high quadratic degree. From Π'', we will apply a further restriction to all of the remaining unset Y variables, to extract a refutation of a subset of m' equations from $F_{n,k}$ of low degree, contradicting the degree lower bound given in Lemma 1. Recall that $F_{n,k}$ is defined over variables X and we pick a subset of these equations by matching pigeons Y_i to equations in $F_{n,k}$ through a complete bipartite graph. We initialize a bad list B of bit strings $b_1 \dots b_{\log m}$ to empty (where each such bit string indexes an equation $E_{b_1 \dots b_{\log m}}$ of $F_{n,k}$). This bad list will contain all of the equations that were affected by either of the above while loops.

We will first analyze the first while loop (lines 5-15). Initially S is initialized to the set of all terms in the proof of singular degree greater than d. Let $M' = M + n\log(n)$. This loop kills off terms in S until S is empty, by iteratively picking a variable w that, by an averaging argument, occurs in at least a d/M' fraction of terms in S. There are two cases depending on whether $w \in X \cup Y$ (the first case) or whether $w \in Z$. In the first case, we apply the restriction $w = 0$ and call **X-cleanup**$(w = 0)$ or **Y-cleanup**$(w = 0)$ depending on whether $w \in X$ or $w \in Y$. This eliminates the contribution to high singular degree from terms containing w, and hence obtains a $(1 - d/M')$-factor reduction in the size of S. In the second case, w is an extension variable, defined by $w = f(X, Y)$ for some polynomial f that depends on at most κ variables from $X \cup Y$. Since w is singular, there exists an assignment $\sigma = \sigma_X \cup \sigma_Y$ such that $f(\sigma) = 0$. We apply the restriction σ to the proof, thus eliminating all terms containing w, which causes a $(1 - d/M')$-factor reduction in the number of high singular degree terms. Next, we run subroutines **X-cleanup**(σ_X) and **Y-cleanup**(σ_Y) (described below) to get rid of all axioms that were affected by the restriction σ. without affecting the other axioms. By repeating the above for $-\log|S|/\log(1-d/M')$ $\approx M'\log|S|/d \leq O(\gamma)n/\kappa 2^\kappa$ iterations (where $|S| = 2^{\gamma n^2/\kappa^2 2^\kappa M'}$), we eliminate all terms in S from the proof and thus obtain a refutation of singular degree less than d.

```
Input: A refutation $\Pi$ of $\psi_{N,\kappa,M}$
Output: A refutation $\Pi'$ with quadratic and singular degree less than $d$
$d \leftarrow \nu n/\kappa$, where $\nu$ is a sufficiently small constant.
$M' \leftarrow M + n\log(n)$.
$S \leftarrow$ the set of all terms in the proof of singular degree greater than $d$
$B \leftarrow \emptyset$.
while $S$ is non empty do
    Pick a variable $w$ that, by an averaging argument, occurs in at least $d/M'$
      fraction of terms in $S$
    if $w \in X \cup Y$ then
        Substitute $w = 0$
        Call X-cleanup($w = 0$) or Y-cleanup($w = 0$) depending on whether $w \in X$
          or $w \in Y$
    end
    if $w$ is an extension variable, defined by $w = f(X, Y)$ then
        Let $\sigma = \sigma_X \cup \sigma_Y$ be an assignment to the variables of $f$ such that $f(\sigma) = 0$
        Substitute $\sigma$
        Call X-cleanup($\sigma_X$) and Y-cleanup($\sigma_Y$)
    end
end
$H \leftarrow$ the set of all pairs of terms in the proof of quadratic degree greater than $d$
while $H$ is non empty do
    Pick a variable $w$ that, by an averaging argument, occurs in at least $d/M'$
      fraction of terms in $H$
    if $w \in X \cup Y$ then
        Substitute $w = 0$
        Call X-cleanup($w = 0$) or Y-cleanup($w = 0$) depending on whether $w \in X$
          or $w \in Y$
    end
    if $w$ is an extension variable, defined by $w = f(X, Y)$ then
        Let $\sigma = \sigma_X \cup \sigma_Y$ be an assignment to the variables of $f$ such that
          $f(\sigma) = \alpha x + \beta$ for some $x \in X$ (exists since we substitute a complete
          assignment for $Y$ eventually and hence extension variables that depend only
          on $Y$ are inconsequential)
        Substitute $\sigma$
        Call X-cleanup($\sigma_X \cup \{x = 0\}$) and Y-cleanup($\sigma_Y$)
        Split on $w$ using Lemma 9
    end
end
```

Algorithm 1: Eliminating high quadratic and singular degree terms from the proof

The processes **X-cleanup**(σ_X) and **Y-cleanup**(σ_Y) increase the size of the bad list B by only $O(|\sigma|) = O(\kappa)$ per call, since each X-variable occurs in at most $k_1 = O(1)$ clauses, and each clause has size $k = O(1)$). Therefore the total size of B at the end of the first while loop is at most $O(\gamma)n/2^\kappa$.

Let Π' be the (modified) proof after exiting the first while loop. Before entering the second while loop (lines 18-29), we initialize H to be equal to $\mathcal{H}_d(\Pi')$, the set of all pairs of terms of Π' of quadratic degree greater than d. Note that H may be different than the original set of bad pairs, since during the execution of the first while loop, some extension variables that were originally singular may become nonsingular. In this second loop, we will kill off all pairs from H by iteratively picking a variable w that contributes to the weight of at least a d/M' fraction of pairs in H.

There are two cases depending on whether $w \in X \cup Y$ or $w \in Z$. In the first case ($w \in X \cup Y$), we apply the restriction $w = 0$ and call **X-cleanup**$(w = 0)$ or **Y-cleanup**$(w = 0)$ depending on whether $w \in X$ or $w \in Y$ respectively. This eliminates the contribution to high quadratic degree from terms containing w, and hence obtains a $(1 - d/M')$-factor reduction in the size of H. In the second case, w is an extension variable defined by extension axiom $w = f(X, Y)$ where f depends on at most κ variables from $X \cup Y$. We can assume that z depends on at least one X-variable since at the end of the procedure we will set all Y-variables to constants, and therefore extension variables that only depend on Y variables will be inconsequential. Thus, there there exists an assignment $\sigma = \sigma_X \cup \sigma_Y$ such that $f(\sigma) = \alpha x + \beta$ for some $\alpha, \beta \in \mathbb{F}_p$ and $x \in X$. We apply σ to the proof, and then call the subroutines **X-cleanup**$(\sigma_X \cup \{x = 0\})$ and **Y-cleanup**(σ_Y) to get rid of all axioms that were affected by σ and also those that contain x. Now that the axioms are free of x and w, we Split on w using Lemma 9, which causes a $(1 - d/3p^2M')$-factor reduction in the number of high quadratic degree terms. By repeating the above for $-\log|H|/\log(1 - d/3p^2M')$ $\approx p^2M'\log|H|/d \leq O(\gamma)n/\kappa 2^\kappa$ iterations (where $|H| = 2^{2\gamma n^2/\kappa^2 2^\kappa M'}$), we eliminate all terms in H from the proof and thus obtain a refutation of quadratic degree less than d. Since one call to **X-cleanup**(σ_X) and **Y-cleanup**(σ_Y) increases the size of the bad list B by only $O(|\sigma|) = O(\kappa)$ per call, the total size of B upon termination of Algorithm 1 is at most $O(\gamma)n/2^\kappa$.

Let Π'' denote the modified proof upon termination of Algorithm 1. We claim that the singular degree as well as the quadratic degree of Π'' is at most d. This is because the first while loop gets rid of all terms of high singular degree, and neither the first or second subroutine creates new variables of high singular degree since substitution can only turn singular variables to nonsingular and not the other way around. Similarly, the second while loop gets rid of all pairs of terms of high quadratic degree, and this second while loop does not create new terms of high quadratic degree, since by Observation 1 substitution does not increase the quadratic degree.

Note that out of the $m' = (1 - \epsilon/2)m$ pigeons, there are at least a $m' - O(\gamma)n/2^\kappa$ pigeons still alive (i.e. not removed by the operations **Y-cleanup**), since we run for $O(\gamma)n/\kappa 2^\kappa$ many iterations, and in each iteration at most κ pigeons are affected by any extension variable. Since $|B| \leq O(\gamma)n/2^\kappa$, the number of untouched equations available for the pigeons to map to is $m - O(\gamma)n/2^\kappa$. We now substitute for the remaining pigeons Y_i so that we select a subset of at least $(1 - \epsilon)m$ unsatisfiable equations φ not in B from $F_{n,k}$ and obtain a refutation of them of quadratic degree at most d and singular degree at most d (assuming γ is small enough). By Lemma 3, this implies a refutation of φ of degree at most $O(p)d$. Now, for all surviving extension variables we substitute them with their definitions in terms of the variables X. Note that since the extension variables are degree κ polynomials this raises the degree to at most $O(p)\kappa d$. Since $d = \nu n/\kappa$, for sufficiently small ν, we end up with a refutation of φ of degree less than $c_2 n$, contradicting Lemma 1.

For the cleanup operations to work properly, recall that $|B| = O(\gamma)n/2^\kappa$ always holds conditioned on each cleanup operation increasing B only by $O(\kappa)$ (for a small enough constant γ).

```
Input: A partial assignment $\sigma$ to the variables $X$
for Every $x \in X$ that occurs in $\sigma$ do
    for Every equation $E_{b_1 \ldots b_{\log m}}$ from $F_{n,k}$ that $x$ occurs in do
        Add $E_{b_1 \ldots b_{\log m}}$ to the list $B$
        for Every $i \in [m']$ do
            Use Lemma 10 to replace the axiom $Y_i \neq b_1 \ldots b_{\log m} \vee E_{b_1 \ldots b_{\log m}}$ by
              $Y_i \neq b_1 \ldots b_{\log m} \equiv \prod_j (y_{ij} - b_j \oplus 1) = 0$
        end
    end
end
```

Algorithm 2: X-cleanup

X-cleanup(σ) Correctness. Suppose $x \in X$ is a variable that occurs in σ. We first add all the equations in $F_{n,k}$ that x occurs in to the list B. By Lemma 1 this is k_1 many equations. We now proceed to eliminate all axioms that contain x. For every such equation $E_{b_1 \ldots b_{\log m}}$ from $F_{n,k}$, which appears in the axiom $Y_i \neq b_1 \ldots b_{\log m} \vee E_{b_1 \ldots b_{\log m}}$ for every i, we use Lemma 10 to replace the latter by $Y_i \neq b_1 \ldots b_{\log m} \equiv \prod_j (y_{ij} - b_j \oplus 1) = 0$ for every i. That is, we assert that no pigeon maps to the equation $E_{b_1 \ldots b_{\log m}}$ and hence it stands eliminated. By Lemma 10 this does not raise the quadratic/singular degree of the proof. We do this for all such x. Note that we have maintained the property that one call to this process adds $O(|\sigma|)$ entries to the bad list B.

```
Input: A partial assignment $\sigma$ to the variables $Y$
for Each $i$ such that $y_{ij} \in Y_i$ is a variable that appears in $\sigma$ for some $j$ do
    Pick an assignment $b_1 \ldots b_{\log m}$ to $y_{i1} \cdots y_{i \log m}$ such that the variables that
      appear in $\sigma$ are set consistently, and $b_1 \ldots b_{\log m}$ does not appear in the bad list
      $B$ (this is possible since the size of $B$ is small enough; see paragraph below)
    Apply $b_1 \ldots b_{\log m}$ to $y_{i1} \cdots y_{i \log m}$; this turns the axiom
      $Y_i \neq b_1 \cdots b_{\log m} \vee E_{b_1 \cdots b_{\log m}}$ into $E_{b_1 \cdots b_{\log m}} = 0$
    Let $\sigma_X$ be a partial assignment to the $X$-variables such that $\sigma_X$ satisfies $E_{b_1 \cdots b_{\log m}}$
    Substitute $\sigma_X$ and add any equation that contains a variable from $\sigma_X$ to the bad
      list $B$
    Add $b_1 \ldots b_{\log m}$ to the bad list $B$
end
```

Algorithm 3: Y-cleanup

Y-cleanup(σ) Correctness. Let i be an index such that $y_{ij} \in Y_i$ is a variable that appears in σ for some j. For each such index i, our plan is to map the i^{th} pigeon comprising of variables $y_{i1} \cdots y_{i \log m}$ to some equation $E_{b_1 \cdots b_{\log m}}$ that is not on the bad list B, and then satisfy the latter. Firstly, note that only κ variables from Y_i can appear in σ (since extension variables that **Y-cleanup** is called on depend on only κ variables and hence the size of σ is bounded by κ). Therefore, there are at least $m/2^\kappa$ values that the binary string $y_{i1} \cdots y_{i \log m}$ can be set to, given that some of these variables are already set by σ. Since the size of the set B is always $O(\gamma)n/2^\kappa$, there exists an assignment $b_1 \dots b_{\log m}$ to $y_{i1} \cdots y_{i \log m}$ such that the variables that appear in σ are set consistently, and $b_1 \dots b_{\log m}$ does not appear in the bad list B. We apply the assignment $b_1 \dots b_{\log m}$ to $y_{i1} \cdots y_{i \log m}$. Note that this turns the axiom $Y_i \neq b_1 \cdots b_{\log m} \vee E_{b_1 \cdots b_{\log m}}$ into $E_{b_1 \cdots b_{\log m}} = 0$ (i.e. selects the equation $E_{b_1 \cdots b_{\log m}}$). We now get rid of it as follows. Since $b_1 \cdots b_{\log m}$ is not on the bad list B, the equation $E_{b_1 \cdots b_{\log m}}$ is untouched, i.e. none of its variables have been set before. Let σ_X be a partial assignment to the X-variables such that σ_X satisfies $E_{b_1 \cdots b_{\log m}}$. We substitute σ_X and add any equation that contains a variable from σ_X to the bad list B. Finally, we add $b_1 \dots b_{\log m}$ to the bad list B. Note that we have maintained the property that one call to this process adds only a $O(|\sigma|)$ number of entries to the bad list B since the equations $F_{n,k}$ contain only k variables per equation.

□

Acknowledgments

The authors would like to thank Paul Beame and Dmitry Sokolov for helpful discussions.

References

[AF21] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: Proving and using lower bounds for polynomial ideals. *CoRR*, abs/2112.00792, 2021.

[Ajt94] Miklós Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[Ale21] Yaroslav Alekseev. A lower bound for polynomial calculus with extension rule. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 21:1–21:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[AR01] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 190–199. IEEE Computer Society, 2001.

[BGIP01] Sam Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62(2):267–289, 2001.

[BIK$^+$96] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on hilbert's nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 3(1):1–26, 1996.

[BKPS02] Paul Beame, Richard Karp, Toniann Pitassi, and Michael Saks. The efficiency of resolution and davis–putnam procedures. *SIAM Journal on Computing*, 31(4):1048–1075, 2002.

[BSW99] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – resolution made simple. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 517–526, 1999.

[CEI96] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 174–183, 1996.

[CR79] Stephen A Cook and Robert A Reckhow. The relative efficiency of propositional proof systems. *The journal of symbolic logic*, 44(1):36–50, 1979.

[CS88] Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *Journal of the ACM (JACM)*, 35(4):759–768, 1988.

[FSTW21] Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. *Theory Comput.*, 17:1–88, 2021.

[GH03] Dima Grigoriev and Edward A Hirsch. Algebraic proof systems over formulas. *Theoretical Computer Science*, 303(1):83–102, 2003.

[GL10] Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Trans. Comput. Log.*, 12(1):4:1–4:22, 2010.

[Hak85] Armin Haken. The intractability of resolution. *Theoretical computer science*, 39:297–308, 1985.

[IMP20] Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. The surprising power of constant depth algebraic proofs. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 591–603, 2020.

[KPW95] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random structures & algorithms*, 7(1):15–39, 1995.

[MN15] Mladen Miksa and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. In David Zuckerman, editor, *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, volume 33 of *LIPIcs*, pages 467–487. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.

[PBI93] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational complexity*, 3(2):97–140, 1993.

[Raz87] Alexander A Razborov. Lower bounds for the size of circuits of bounded depth with basis fˆ; g. *Math. notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

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

[RT08] Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Annals of Pure and Applied Logic*, 155(3):194–224, 2008.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82, 1987.

[Sok20] Dmitry Sokolov. (semi) algebraic proofs over $\{\pm 1\}$ variables. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 78–90, 2020.