Bounded-Depth Frege with Counting Principles Polynomially Simulates Nullstellensatz Refutations

Russell Impagliazzo[*] and Nathan Segerlind[†]
Department of Computer Science
University of California, San Diego
La Jolla, CA 92093
russell@cs.ucsd.edu, nsegerli@cs.ucsd.edu

Abstract

We show that bounded-depth Frege systems with counting principles modulo m can polynomially simulate Nullstellensatz refutations modulo m. This establishes new upper bounds for proofs of certain tautologies in bounded-depth Frege with counting axioms systems. When combined with another paper by the authors, this simulation establishes a size (as opposed to degree) separation between Nullstellensatz and polynomial calculus refutations.

1 Introduction

The central question of propositional proof complexity, as posed by Cook and Reckhow in [7], is "How can we prove lower bounds for the sizes of proofs of a given family of tautologies in a fixed propositional proof system?". Despite substantial breakthroughs in recent years, our understanding is limited to weak proof systems, systems far weaker than the textbook propositional proof systems, or Frege systems, let alone the general problem of NP versus coNP. Two subsystems of Frege which have received attention in recent yeanrs are bounded-depth Frege with counting axioms, as studied in [1], [2], [3], [10], [6], [4], and Nullstellensatz systems, as studied in [3], [6], [5].

In this paper we show that, under natural uniformity conditions on the polynomials, bounded-depth Frege with counting modulo m axioms can polynomially simulate Nullstellensatz refutations modulo m. This establishes upper bounds for bounded-depth Frege with counting axioms, and also gives *size* lower bounds for the Nullstellensatz system. In particular, a size separation between the polynomial calculus and Nullstellensatz refutations follows from the simulation and the results of [8].

Because lower bounds for bounded-depth Frege with counting axioms imply lower bounds for Nullstellensatz refutations, this simulation shows that the lower bound technique of reducing bounded-depth Frege with counting axiom proofs into Nullstellensatz refutations, as used in [3], [6], and [4], was not only sufficient but necessary:

By combining the simulation with the results of [8], we demonstrate a size separation between the polynomial calculus and Nullstellensatz refutations. Previously, the only Nullstellensatz *size* lower bounds we knew of followed from size lower bounds for the polynomial calculus, and as such were unable to give size separations between the polynomial calculus and Nullstellensatz refutations. Because the tautologies of [8] require large size to be proven by bounded-depth Frege with counting axioms also have small polynomial calculus refutations, we have a size separation between Nullstellensatz and polynomial calculus refutations.

Independently, in his work [9], Jan Krajicek made the aisde "that the Nullstellensatz over $\mathbb{Z}_p$ corresponds to an extension of $S_2^2(\alpha)$ by the so-called counting modulo p principle". Our results differ in some important ways. Our simulation is precise, and the details of the proof are given. Moreover, our results do not immediately follow from a simulation in bounded-arithmetic because the translation from bounded-arithmetic to bounded-depth Frege is quasi-polynomial not polynomial. Because the bounded-depth Frege with counting gates lower bound of [8] is barely su-

[*] Research Supported by NSF Award CCR-9734911, grant #93025 of the joint US-Czechoslovak Science and Technology Program, NSF Award CCR-0098197, and USA-Israel BSF Grant 97-00188

[†] Partially supported by NSF grant DMS-9803515

perpolynomial, this distinction is necessary to get the size separation between the Nullstellensatz and polynomial calculus modulo 2.

In section 2, we provide background information on the proof systems we use. In section 3, the outline of the proof of the simulation is provided. In section 4, it is shown how bounded-depth Frege with counting axioms can prove a needed auxiliary tautology. In section 5 we give the proof of the simulation. In section 6 we discuss the generality of the uniformity condition on the system of polynomials. In particular, we show that for any unsatisfiable propositional formula f, if there is a small size Nullstellensatz refutation of a certain algebraic translation of f, then there is a small refutation of f in bounded-depth Frege with counting axioms. In section 7 we show that the simulation can be applied to the induction on sums principles of [8], thereby establishing a size separation between Nullstellensatz and polynomial calculus, and we show that the simulation gives upper bounds for tautologies arising from systems of bounded-width linear equations.

2 The Proof Systems

2.1 Bounded-Depth Frege with Counting Principles Modulo m

Frege systems are sound, implicationally complete propositional proof systems with a finite number of axiom schemas and inference rules. The system we discuss will be over the basis of fan-in one NOT gates, and unbounded fan-in AND and OR gates. The size of a proof is the total number of symbols appearing in the proof. We say that a family of tautologies τ_n, each of size $s(n)$, has polynomially sized bounded-depth Frege proofs if there is are constants c and d so that for all n, there is a proof P_n of t_n so that each formula in P_n has depth at most d, and P_n has size size at most $\mathrm{O}\left(s^c(n)\right)$.

For an integer $m \geq 2$, we define a family of tautologies based on the fact it is impossible to partition a set of N elements into pieces of size m when $N \not\equiv_m 0$. For all $N \not\equiv_m 0$, let V be a fixed set of N elements. We associate a variable x_e with each m subset of V. The counting tautology asserts that it is impossible to partition a set of size N into pieces of size m.

$$\text{Count}_m^N := \bigvee_{v \in V} \bigwedge_{e \ni v} \neg x_e \;\vee\; \bigvee_{e \perp f} \left(x_e \wedge x_f\right)$$

Bounded-depth Frege systems with counting principles modulo m are just bounded-depth Frege systems which allow all substitution instances of Count_m^N as axioms.

For ease of comparison with algebraic systems, we will view bounded-depth Frege as a refutation system: we add an unsatisfiable formula as a hypothesis and derive 0.

2.2 Nullstellensatz Refutations

The Nullstellensatz system is a refutation system for showing that a system of polynomials has no common root by showing the ideal generated contains 1. Because we are interested in binary solutions, we add extra equations requiring that the variables be assigned $0, 1$ values. For an unsatisfiable system of polynomials, $f_1, \ldots f_k$, a Nullstellensatz refutation has the form

$$\sum_{i=1}^{k} P_i f_i + \sum_{j+1}^{n} R_j x_j \left(x_j - 1\right) = 1$$

The size of the refutation is the number of monomials appearing in the expansion of the left-hand side. The degree of the refutation is the maximum degree of the polynomials $P_i f_i$, $R_j x_j \left(x_j - 1\right)$. Hilbert's nullstellensatz coupled with the presence of the polynomials $x_j(x_j - 1)$ shows the completeness of this system, but nothing is said about the degree nor the size of the refutation.

2.3 Polynomial Calculus

Let $g_1, \ldots g_k$ be multivariate polynomials over $\mathbb{Z}_2$. A *polynomial calculus refutation of* $g_1, \ldots g_k$ *over* $\mathbb{Z}_2$ is a sequence of polynomials $f_1, \ldots f_l$ so that, for each $i \in \{1, \ldots l\}$, f_i is either one of the g_j's, ${x_i}^2 - x_i$ for a variable x_i, $af_j + bf_k$, with $j, k < i, a, b \in \mathbb{Z}_P$, or $x_i f_j$ with $j < i$.

The size of the proof is the number of monomials appearing in all of the polynomials, $f_1, \ldots f_l$. The degree of the proof is the maximum degree of a polynomial $f_1, \ldots f_l$.

3 Proof Sketch

The first issue that must be addressed is how we can compare the two systems when bounded-depth Frege with counting axioms works with propositional formulas and the

Nullstellensatz system works with polynomials. A term can be viewed as a conjunction of literals, and an assignment is a root to the polynomial modulo m if and only if there exists a partition of its satisfied terms into m-sets. The polynomial can be thought of as uniform if there are simple formulas which define a partition on its satisfied monomials.

We will show that if unsatisfiable formula f allows us to prove with short, constant depth proofs that some formulas θ^i_E form a partition on the satisfied terms of an unsatisfiable system of polynomials p_i, then there is a bounded-depth Frege with counting axioms refutation of f of size polynomially related to the size of the Nullstellensatz refutation of the p_i's, and the size of the proofs that the θ^i_E's form a partition on the satisfied terms of the p_i's.

The simulation of Nullstellensatz refutations works by partitioning the satisfied monomials in the expansion of the refutation in two contrary ways, thereby contradicting the Count$_m$ axioms.

The first partition is obtained from the Nullstellensatz refutation: after we expand the refutation and collect terms, the coefficients of the non-constant monomials are zero, therefore, if we group together the satisfied monomials of the expansion, we will will have an m-partition which leaves exactly one satisfied term uncovered.

On the other hand, if we work under the hypothesis that the θ^i_E's define a partition on the satisfied terms of the polynomials p_i's, we can extend that to a partition on the satisfied terms of the refutation. We take the "product partition" and place the terms of the expanded $f_i p_i$'s into groups according to their p_i components, and we have a partition that covers every satisfied term in the expansion.

It is impossible to have two m-partitions of a set, one which leaves no element out, and the other leaving out a number of elements non-divisible by m. This contradicts the axioms Count$_m$.

Therefore, bounded-depth Frege with counting axioms can derive a contradiction from the hypothesis that the θ^i_E's form a partition on the satisfied terms of the polynomials, and therefore a contradiction from the assumption f.

4 A Tautology on Contrary Partitionings of Satisfied Variables

For a fixed assignment to a set of underlying variables, it is not possible to to have two distinct partitions, one which perfectly covers the ones, and another which leaves exactly 1 satisfied variable uncovered. Similarly, for any k, $0 < k < m$, it is impossible to have one partition covering the ones perfectly, and another partitioning the satisfied variables, and an extra $m - k$ new points. These principles are what we call the contradictory partitions tautologies, CP$^{n,k}_m$.

Definition 4.1 *Let $u_1, \ldots u_n$ be a set of boolean variables, for each m-element subset $e \in [n]^m$, let y_e be a variable, and for each $e \in [n+m-k]^m$, let z_e be a variable.*

$CP^{n,k}_m(\vec{u}, \vec{y}, \vec{z})$ is the following formula:

$$\begin{array}{l}
\neg((\bigwedge_e y_e \Rightarrow \bigwedge_{i\in e} u_i) \\
\quad \wedge (\bigwedge_i u_i \Rightarrow \bigvee_{e\ni i} y_e) \\
\quad \wedge (\bigwedge_{e\perp f} \neg y_e \vee \neg y_f)) \\
\vee\neg((\bigwedge_e z_e \Rightarrow \bigwedge_{i\in e,\ i\le n} u_i) \\
\quad \wedge (\bigwedge_{i\le n} u_i \Rightarrow \bigvee_{e\ni i} z_e) \\
\quad \wedge (\bigwedge_{n+1<i\le n+m-k} \bigvee_{e\ni i} z_e) \\
\quad \wedge (\bigwedge_{e\perp f} \neg z_e \vee \neg z_f))
\end{array}$$

Proposition: The tautology CP$^{n,k}_m$ has a bounded-depth, polynomial size proof from Count$_m$.

Proof: Fix m, n and k. The proof of CP$^{n,k}_m$ is by contradiction. We make the assumption that the formula is false, and then give a collection of formulas which can be shown to define an m partition on a set of size $mn + (m-k)$, contradicting the axiom COUNT$^{mn+(m-k)}_m$.

We have m copies of each underlying variable, $\{(r,i) \mid 1 \le r \le m,\ 1 \le i \le n\}$, with $m-k$ many extra elements, $\{(0,i) \mid 1 \le i \le m-k\}$. If the variable x_i is set to 0, we group its copies together. For variables that are set to 1, within the first $m-1$ copies, we use the partition with no ones left over, and in the final copy we use the partition which also covers the extra elements. This gives a partition of a set of $mn + m - k$ elements into m sets, violating COUNT$^{mn+(m-k)}_m$.

Let $U = \{(r,i) \mid 1 \le r \le m,\ 1 \le i \le n\} \cup \{(0,i) \mid 1 \le i \le m-k\}$. (Think of (r,i) as the r'th copy of u_i.)

```
For each $e \in [U]^m$
    if there exists $i$, $1 \le i \le n$, so that $e = \{(r,i) \mid 1 \le r \le m\}$
        $\phi_e = \neg u_i$
    if $e \subseteq \{(r,i) \mid 1 \le i \le n\}$ for some $1 \le r < m$
```

```
        let $f = \{i \mid (r,i) \in e\}$
        $\phi_e = y_f$
    if $e \subseteq \{(m,i) \mid 1 \leq i \leq n\} \cup \{(0,i) \mid 1 \leq i \leq m-k\}$
        let $f = \{i \mid (m,i) \in e\} \cup \{n+i \mid (0,i) \in e\}$
        $\phi_e = z_f$
    otherwise, $\phi_e = 0$
```

The formula $\left(\neg\text{Count}_m^{mn+m-k}\right)[x_e \leftarrow \phi_e]$ is then constructed by brute force from the hypothesis $\neg\text{CP}_m^{mn+m-k}$.

■

5 The Simulation

In order to use a Nullstellensatz refutation in a bounded-depth Frege proof, one must translate an algebraic hypothesis, that a system of polynomials simultaneously vanish, into a hypothesis in propositional logic. In the case of $\mathbb{Z}_m$, a polynomial vanishes if and only if there is an m-partition of its non-zero monomials. The simulation makes use of a family of formulas which define a partition on the satisfied monomials. For the sake of generality, we allow the system of polynomials to be in a different set of variables than the formulas defining the partition. That is, the polynomials can be in variables $\vec{y}$ and the partition definitions in variables $\vec{x}$. For this situation, we require, for each i, a propositional formula δ_i defining y_i from the x's.

Definition 5.1 *Let $p \in \mathbb{Z}_m[\vec{y}]$ be given, with $p = \sum_{I \subseteq \{1, \ldots n\}} c_I \prod_{i \in I} y_i$. The set of monomials of p is the following set:*

$$M_p = \{(c, I) \mid I \subseteq \{1, \ldots n\},\ 1 \leq c \leq a_I\}$$

Definition 5.2 *Let $\{x_i \mid i \in S_1\}$ and $\{y_i \mid i \in S_2\}$ be distinct, but not necessarily disjoint, sets of boolean variables.*

Let p be a polynomial in variables $\vec{y}$, $p = \sum_I a_I \prod_{i \in I} y_i$.

For each $i \in S_2$, let $\delta_i(\vec{x})$ be a propositional formula.

For each $E \in [M_p]^m$, let θ_e be a formula in $\vec{x}$.

We say that the θ's form a ones-partition the monomials of p with definitions $\vec{\delta}$ *if the following formula holds:*

$$\bigwedge_E \left(\theta_E \Rightarrow \bigwedge_{(c,I) \in E} \bigwedge_{k \in I} \delta_k\right) \wedge$$

$$\left(\bigwedge_{(c,I) \in M_p} \bigwedge_{k \in I} \delta_k \Rightarrow \bigvee_{E \ni (c,I)} \theta_E\right) \wedge \left(\bigwedge_{E \perp F} \neg\theta_E \vee \neg\theta_F\right)$$

Theorem 1 *Let $\{x_i \mid i \in S_1\}$ and $\{y_i \mid i \in S_2\}$ be distinct, but not necessarily disjoint, sets of boolean variables.*

Let $\Gamma(\vec{x})$ be a propositional formula. Let $p_1, \ldots p_k \in \mathbb{Z}_m[\vec{y}]$ be a system of polynomials with a Nullstellensatz refutation $f_1, \ldots f_k, r_1, \ldots r_n$ of size S. For each $i \in S_2$, let δ_i be a formula in $\vec{x}$.

Suppose there are formulas $\beta^i_E(\vec{x})$, $E \in [M_{p_i}]^m$, so that for each i, there is a size T, depth D Frege proof from $\Gamma(\vec{x})$ that the β^i's form ones-partitions on the monomials of p_i with definitions $\vec{\delta}$.

Then there is a depth $O(D)$ Frege refutation of $\Gamma(\vec{x})$ with size polynomial in m, $|\Gamma|$, T and S.

Proof:

We are going to obtain contrary partitionings of the the monomials that appear in the expansion of $\sum_{i=1}^k p_i f_i$ in which all polynomials are multiplied and multilinearized, but no terms are collected. Therefore, our index set is:

$$V := \bigcup_{i=1}^{k} \{((c, I), (d, J), i) \mid (c, I) \in M_{f_i},\ (d, J) \in M_{p_i}\}$$

The underlying "variables" will be the conjunctions of the definitions of the variables in each monomial: for $v \in V$, $v = ((c, I), (d, J), i)$, $\gamma_v = \bigwedge_{k \in I \cup J} \delta_k$.

For each $E \subseteq [V \cup \{1, \ldots m-1\}]^m$, we will give a formula θ_E. This family of formulas will be shown to define an m-partition on the satisfied monomials and $m-1$ extra points.

For each $E \subseteq [V]^m$, we will give a formula η_E. Using the hypothesis that the β^i's partition the satisfied monomials of p_i, we can show that these define an m-partition on the satisfied monomials.

This will contradict $\text{CP}_m^{|V|,1}[u_v \leftarrow \gamma_v,\ y_E \leftarrow \theta_E,\ z_E \leftarrow \eta_E]$, which is provable in bounded-depth Frege with counting axioms.

The Partition with 1 One Left Uncovered

When we collect terms after expanding $\sum_{i=1}^{k} p_i f_i$ and multilinearizing, the coefficient of every term of degree > 0 is 0 modulo m, and the constant term is 1 modulo m.

For each $S \subseteq [n]$, let $V_S = \{((c, I), (d, J), i)) \in V \mid I \cup J = S\}$. When S is a nonempty subset of $\{1, \ldots n\}$, there is an m-partition $\mathcal{P}_S$ on V_S. Likewise, there is an m-partition $\mathcal{P}_\emptyset$ on $V_\emptyset \cup \{1, \ldots m-1\}$.

We define formulas θ_E, for $E \in ([V] \cup [1, \ldots m-1])^m$, as follows:

If $E \notin \bigcup_{S \subseteq [n]} \mathcal{P}_S$
    then $\theta_E = 0$
Otherwise, for $E \in \mathcal{P}_S$
    $\theta_E = \bigwedge_{j \in S} \delta_j$

Bounded-depth Frege can prove that this is a m-partition of $V \cup \{1, \ldots m-1\}$ by brute-force with a proof of size $O(|V|^m)$. It is trivial from the definition of θ_E that the edges cover only satisfied monomials. That every satisfied monomial $\bigwedge_{k \in S} \delta_k$ is covered is also trivial: the edge from $\mathcal{P}_S$ is used if and only if the term δ_S is satisfied. Finally, it easily shown that the formulas for two overlapping edges are never both satisfied: only edges from $\mathcal{P}_S$ are ever used (regardless of the values of the x's), and for any pair of overlapping edges, one of the two formulas is identically 0.

The Partition with No Ones Left Uncovered

The partition which we use simply groups the pairs of monomials according to their p_i component using the partition defined by the β^i's.

We consider only edges in which the contribution from a term of an f_i is fixed. For each $E \in [V]^m$, if there exists i, $1 \leq i \leq k$, $(c, I) \in M_{f_i}$ so that $E = \{((c, I), (d_l, J_l), i) \mid 1 \leq l \leq m\}$, let $E_0 = \{(d_l, J_l) \mid 1 \leq l \leq m\}$.

For each $E \in [V]^m$, define η_E as follows:

If there exists i, $(c, I) \in M_{f_i}$
    so that $E = \{((c, I), (d_l, J_l), i) \mid 1 \leq l \leq m\}$
then
    let $\eta_E = \bigwedge_{k \in I} \delta_k \wedge \beta_{E_0}$
Otherwise, $\phi_E = 0$

Every satisified monomial is covered. Let $((c, I), (d, J), i) \in V$ be given. If $\bigwedge_{k \in I \cup J} \delta_k$ holds, then so do $\bigwedge_{k \in I} \delta_k$ and $\bigwedge_{k \in J} \delta_k$. Because the β^i's form a ones-partition on the monomials of p_i, there is an $E_0 \ni (d, J)$ so that $\eta^i_{E_0}$ holds. Set $E = \{((c, I), (d', J'), i) \mid (d', J') \in E_0\}$. derive $\eta_{E_0} \wedge \bigwedge_{k \in I} \delta_k = \theta_E$.

Every monomial covered is satisfied. Let $v = ((c, I), (d, J), i) \in V$ be given. Suppose $v \in E$ and θ_E holds. By definition, the monomial is $\bigwedge_{k \in I \cup J} \delta_k$ and $\theta_E = \bigwedge_{k \in I} \delta_k \wedge \eta^i_{E_0}$. Therefore $\bigwedge_{k \in I} \delta_k$ holds. Because the η^i's form a ones-partition on the monomials of p_i, $\bigwedge_{k \in J} \delta_k$ holds. Therefore $\bigwedge_{k \in I \cup J} \delta_k$ holds.

No two overlapping edges E and F can have θ_E and θ_F simultaneously satisfied. If $E \perp F$, and neither θ_E nor θ_F is identically 0, then they share the same (constant) f_i component. That is, there exists i, $(c, I) \in M_{f_i}$ so that $E = \{((c, I), (d_l, J_l), i) \mid 1 \leq l \leq m\}$, and $F = \{((c, I), (d'_l, J'_l), i) \mid 1 \leq l \leq m\}$. Because $E \perp F$, we also have $E_0 \perp F_0$. Because the β^i's form a ones-partition on the monomials of p_i, we can derive $\neg\beta^i_{E_0} \vee \neg\beta^i_{F_0}$ and thus $\neg\left(\bigwedge_{k \in I} \delta_k \wedge \beta^i_{E_0}\right) \vee \neg\left(\bigwedge_{k \in I} \delta_k \wedge \beta^i_{F_0}\right) = \neg\theta_E \vee \neg\theta_F$.

■

6 Generality of the Uniformity Condition

The uniformity condition of the 1 may strike the reader as somehwat unnatural. However, if we begin with a propositional formula and translate it into a system of polynomials in a standard way, we can show that the system of polynomials admits a definition of partitions on its monomials with proofs of size polynomial in $|f|$.

Definition 6.1 *Let f be a formula in the variables $X_1, \ldots X_n$ and the connectives $\{\bigvee, \neg\}$.*

For each subformula g of g, let there be a variable Y_g. For each pair of subformulas of f, g_1 and g_2, with g_1 an input to g_2 let there be a variable Z_{g_1, g_2}.

Canonically order the subformulas of f, and write $g_1 < g_2$ if g_1 precedes g_2 in this ordering.

The polynomial translation of f, poly(f), *is the following set of polynomials:*

for each subformula g_1 whose top connective is an $\bigvee$

$\sum_{g_2 \to g_1} Z_{g_2,g_1} - Y_{g_1}$

For each triple of subformulas g_1, g_2, g_3 with the top connective of g_1 an $\bigvee$, $g_2 \to g_1$, $g_3 \to g_1$ and $g_2 < g_3$

$Y_{g_2} Z_{g_3,g_1}$

For each pair of subformulas g_1, g_2, with the top connective of g_1 an $\bigvee$ and $g_2 \to g_1$

$Z_{g_2,g_1} Y_{g_2} - Z_{g_2,g_1}$

For each subformula g_1 whose top connective is a $\neg$, with g_2 the unique input of g_1

$Y_{g_1} Z_{g_2,g_1} - Y_{g_1}$

$Y_{g_2} Z_{g_2,g_1}$

Finally, we stipulate that the formula is satisfied:

$Y_f - 1$

One can easily show by induction that f is satisfiable if and only if poly(f) has a common root.

Theorem 2 *Suppose that f is an unsatisfiable formula in the variables $X_1, \ldots X_N$ and the connectives $\{\bigvee, \neg\}$. If poly(f) has a size S Nullstellensatz refutation, the f has a Frege refutation of depth $\mathrm{O}(depth(f))$, and size polynomial in $|f|$, S.*

Proof:

We define the variable Y_g by the formula $g(\vec{x})$, and the formula Z_{g_2,g_1} by $g_2(\vec{x}) \wedge \bigwedge_{\substack{g_3 < g_2 \\ g_3 \to g_1}} \neg g_3(\vec{x})$.

We use the subformulas of f to define a partition on the monomials of each polynomials.

For polynomials of the form $\sum_{g_2 \to g_1} Z_{g_2,g_1} - Y_{g_1}$, where g_1 is a polynomial whose top connective is an $\bigvee$, we pair up the monomials Z_{g_2,g_1} and Y_{g_1} if and only if $g_2 \wedge \bigwedge_{\substack{g < g_2 \\ g \to g_1}} \neg g$.

For polynomials $Y_{g_2} Z_{g_3,g_1}$, with the top connective of g_1 an $\bigvee$, $g_2 \to g_1$, $g_3 \to g_1$ and $g_2 < g_3$, it is quickly shown that these monomials (under our definitiions) cannot be satisfied. Y_{g_2} is defined by $g_2(\vec{x})$ and Z_{g_3,g_1} is defined by $g_3(\vec{x}) \wedge \bigwedge_{\substack{g < g_3 \\ g \to g_1}} \neg g(\vec{x})$. Because $g_2 < g_3$, these definitions contain g_2 and $\neg g_2$ as conjuncts, respectively.

For $Z_{g_2,g_1} Y_{g_2} - Z_{g_2,g_1}$, we pair the two monomials if and only if $g_2 \wedge \bigwedge_{\substack{g_3 < g_2 \\ g_3 \to g_1}} \neg g_3$.

For polnynomials of the form $Y_{g_1} Z_{g_2,g_1} - Y_{g_1}$, where g_1 is a subformula of f whose top connective is a $\neg$ and g_2 is the unique input of g_1, we pair the monomials if and only if $\neg g_2$.

For polynomials of the form $Y_{g_2} Z_{g_2,g_1}$, where g_1 is a subformula of f whose top connective is a $\neg$ and g_2 is the unique input of g_1, it is easily shown from the definitions that the monomial is never satisfied.

For the polynomial $Y_f - 1$, because Y_f is defined as f, from the hypothesis f we can quickly show that the pairing of these monomials forms a ones-partition. ■

7 Applications

7.1 A Size Separation Between the Nullstellensatz System and the Polynomial Calculus

In [8], a family of tautologies, the "induction sums principles", is presented. This principle is shown to require super-polynomial size refutations in bounded-depth Frege with counting axioms modulo two. A natural algebraic translation of the principle is shown to have constant-degree, polynomial-size refutations in the polynomial calculus.

Here we show that that the algebraic translations of the induction on sums principles satisfy the uniformity condition of our simulation. Therefore, there is a superpolynomial size separation between the polynomial calculus and Nullstellensatz refutations for this principle.

We recap the tautologies below:

Let M and N be positive integers. Suppose that we have M rows of N boolean variables. There is no assignments to these variables with the following properties:

1. The parity of the first row is 0.
2. The parity of the final row is 1.
3. For each r from 2 to M, the parity of row r is equal to the parity of row r times the parity of row $r - 1$.

Let M and N be integers. Let $R_1, \ldots R_M$ be disjoint sets of size N (view each R_i as a row of N variables).

For $r \in \{0, \ldots M\}$, the "set of monomials for equation r", U_r, is the set of monomials appearing in E_r, represented as sets of indices (this suffices because we are working modulo 2).

$$U_0 = \{\{i\} \mid i \in R_1\}$$

$$U_r = \{\{i, j\} \mid i \in R_r,\ j \in R_{r+1}\} \cup \{\{j\} \mid j \in R_{r+1}\}$$

$$U_M = \{\{i\} \mid i \in R_M\} \cup \{\emptyset\}$$

We express that each equation is satisfied by partitioning the satisfied monomials into groups of two.

Definition 7.1 *For each* $r,\ 0 \leq r \leq M$, *there are partition variables* Y_e *for each* $e \in [U_r]^2$.

The formula IS(M, N) *is the negation of the conjunction of the following clauses:*

for each $r,\ 0 \leq r \leq M$, *each* $I \in U_r$,
$\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$
for each $r,\ 0 \leq r \leq M$, *each* $I \in U_r$, *each* $i \in I$, *and each* $e \in [U_r]^2$, $e \ni I$,
$\neg Y_e \vee X_i$
for each $r,\ 0 \leq r \leq M$,, *each* $e, f \in [U_r]^2$, $e \perp f$,
$\neg Y_e \vee \neg Y_f$

Definition 7.2 *For each* $r,\ 0 \leq r \leq M$, *there are partition variables* Y_e *for each* $e \in [U_r]^2$.

The formula AIS(M, N) *is set of the following equations:*

for each $r,\ 0 \leq r \leq M$, *each* $I \in U_r$,
$\prod_{i \in I} X_i \left(\sum_{e \ni I} Y_e - 1\right)$
for each $r,\ 0 \leq r \leq M$, *each* $I \in U_r$, *each* $i \in I$, *and each* $e \in [U_r]^2$, $e \ni I$,
$Y_e X_i - Y_e$
for each $r,\ 0 \leq r \leq M$,, *each* $e, f \in [U_r]^2$, $e \perp f$,
$Y_e Y_f$

Lemma 3 *If there is a size* S *Nullstellensatz refutation of AIS*(M, N), *then there is a size poly*(M, N, S), *depth* $O(1)$ *Frege proof of IS*(M, N).

Proof:

To define a ones partition on the monomials of $\prod_{i \in I} X_i \left(\sum_{e \ni I} Y_e - 1\right)$, we use the formula $Y_e \wedge \bigwedge_{i \in I}$ for $\{I \cup \{e\}, I\}$, the edge which pairs the monomials $\prod_{i \in I} X_i Y_e$ and $\prod_{i \in I} X_i$. From the hypotheses $\bigvee_{i \in I} \neg X_i \vee \bigvee_{e \ni I} Y_e$ and $Y_e Y_f$ (for all $e \perp f$), there is a proof of size $O()$ that these formulas define a ones-partition on the monomials of $\prod_{i \in I} X_i \left(\sum_{e \ni I} Y_e - 1\right)$.

To define a ones partition on the monomials of an equation $Y_e X_i - Y_e$, we simply pair the monomials if and only if Y_e is satisfied. The hypothesis $\neg Y_e \vee X_i$ shows that this is a ones-partition of the monomials.

Defining a ones partition on the monomials of $Y_e Y_f$ is an exercise in vacuity. On one hand, because there is only one monomial, there are no edge variables. On the other hand, the hypothesis $\neg Y_e \vee \neg Y_f$ ensures that the monomial is never satisfied, so the empty partition indeed forms a ones-partition.

Therefore, by theorem 1, if there is a size S Nullstellensatz refutation of AIS(M, N), then there is a size poly(M, N, S), depth $O(1)$ Frege proof of IS(M, N). ■

However, the constant-depth Frege systems have no polynomial size proofs of IS(M, N).

Theorem 4 *[8] Let* c, d *be positive constants. For sufficiently large values of* M, N, *there is no depth* d *refutation* $\mathcal{P}$ *of IS*$(\mathcal{U})$ *of size* $\leq N^c$.

The polynomial calculus has polynomial size refutations of AIS(M, N):

Theorem 5 *([8]) Let* M, N *be given, and let* $\mathcal{U}$ *be an* (M, N) *universe. AIS*$(\mathcal{U})$ *system of polynomials has degree* 3, *size* $O(MN^3)$ *polynomial calculus refutation.*

Corollary 6 *The Nullstellensatz system modulo two does not polynomially simulate the polynomial calculus modulo two.*

7.2 An Upper Bound: Unsatisfiable Systems of Bounded-Width Linear Equations

Consider an inconsistent system of N linear equations in variable $\vec{x}$ over $\mathbb{Z}_p$, in which no equation contains more than C variables. Such systems have small Nullstellensatz refutations (given by Gaussian elimination). Moreover, each equation can be described by a depth two formula of size $O(2^C)$ in the variables $\vec{x}$, so the system can be expressed as a depth three propositional formula F of size $O(N 2^C)$, in the variables $\vec{x}$.

To define the ones-partitions on the sets of monomials of each polynomial, p_i, we choose a partition on the satisfied monomials for each root of p_i. Then, for each $E \in [M_{p_i}]^p$, we simply let β^i_E be a case-analysis of the $\leq C$ variables involved in p_i. From the hypothesis F, which explicitly states that each polynomial vanishes, we can provide constant depth proofs that these definitions form a ones-partitions on the monomials.

8 Conclusions and Future Work

We have shown that bounded-depth Frege with counting axioms can polynomially simulate Nullstellensatz refutations whenever the polynomials are sufficiently uniform. In particular, polynomials which arise as translations of propositional formulas satisfy this uniformity condition. Therefore, in most cases that have arisen in study, Nullstellensatz upper bounds yield bounded-depth Frege with counting axioms upper bounds, and size lower bounds for bounded-depth Frege with counting axoims yield size lower bounds for Nullstellensatz refutations. In particular, this enables to show that a large class of tautologies has small bounded-depth Frege with counting axioms proofs, and that Nullstellensatz refutations modulo two do not polynomiall simulate polynomical calculus refutations modulo two.

The primary questions left open are those left open by [8]: to generalize the lower bound for $IS(M,N)$ from bounded-depth Frege with counting axioms modulo two to bounded-depth Frege with counting axioms of an arbitrary modulus, and to finda tautology which improves the separation from superpolynomial to exponential. Both improvements would improve the size separation between the Nullstellensatz and polynomial calculus systems.

References

[1] Ajtai. Parity and the pigeonhole principle. In *FEASMATH: Feasible Mathematics: A Mathematical Sciences Institute Workshop*. Birkhauser, 1990.

[2] M. Ajtai. The independence of the modulo p counting principles. In *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, pages 402–411, Montréal, Québec, Canada, 23–25 May 1994.

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

[4] Paul Beame and Søren Riis. More one the relative strength of counting principles. In Paul Beame and Sam Buss, editors, *Proof Complexity and Feasible Arithmetics*, pages 13–35. American Mathematical Society, 1998.

[5] Josh Buresh-Oppenheim, Matt Clegg, Russell Impagliazzo, and Toniann Pitassi. Homogenization and the polynomial calculus. Submitted for publication., 1999.

[6] Buss, Impagliazzo, Krajíčcek, Pudlák, Razborov, and Sgall. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Computational Complexity*, 6, 1997.

[7] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36 – 50, March 1979.

[8] Russell Impagliazzo and Nathan Segerlind. Counting axioms do not polynomially simulate counting gates (extended abstract). In *Proceedings of the Forty-Second Annual Symposium on Foundations of Computer Science*, pages 200–209. IEEE Computer Society, 2001.

[9] Jan Krajicek. Uniform families of polynomial equations over a finite field and structures admitting and euler characteristic of definable sets. *Proc. London Mathematical Society*, 3(81):257–284, 2000.

[10] Søren Riis. Count(q) does not imply Count(p). *Annals of Pure and Applied Logic*, 90(1–3):1–56, 15 December 1997.