Lower bounds on Hilbert's Nullstellensatz and propositional proofs

Paul Beame*  
Dept. of Computer Science and Engineering  
University of Washington  
beame@cs.washington.edu

Russell Impagliazzo †  
Dept. of Computer Science  
University of California at San Diego  
russell@cs.ucsd.edu

Jan Krajíček †  
Mathematical Institute  
Academy of Sciences, Praha  
krajicek@earn.cvut.cz

Toniann Pitassi‡  
Dept. of Computer Science and Mathematics  
University of Pittsburgh  
toni@cs.pitt.edu

Pavel Pudlák‡  
Mathematical Institute  
Academy of Sciences, Praha  
pudlak@earn.cvut.cz

Abstract

The weak form of the Hilbert's Nullstellensatz says that a system of algebraic equations over a field, $Q_i(\bar{z}) = 0$, does not have a solution in the algebraic closure of $F$ if and only if there exist polynomials $P_i(\bar{z})$ from $F[z]$ such that $\sum_i P_i(\bar{z})Q_i(\bar{z}) = 1$.

This result has the following application. The modular counting principle states that no finite set whose cardinality is not divisible by $q$ can be partitioned into $q$-element classes. For each fixed cardinality $N$, this principle can be expressed as a propositional formula $\text{Count}_N$. Ajtai [3] proved recently that, whenever $p, q$ are two different primes, the propositional formulas $\text{Count}_m$ do not have polynomial size, constant-depth Frege proofs from instances of $\text{Count}_m$, $m \neq 0 \pmod{p}$. We give a new proof of this theorem based on the lower bound for the Hilbert's Nullstellensatz. Furthermore our technique enables us to extend the independence results for counting principles to composite numbers $p$ and $q$. This results in an exact characterization of when $\text{Count}_p$ can be proven efficiently from $\text{Count}_q$, for all $p$ and $q$.

Introduction

The problem of solvability of a system of algebraic equations

$$Q_i(\bar{z}) = 0, \quad i \in I,$$

in a fixed finite field $F$ is one of the most natural $NP$-complete problems. If we look for solutions in the algebraic closure of $F$ the solvability is characterized by the basic result in algebraic geometry known as Hilbert's Nullstellensatz. Namely, the equations (1) do not have a solution in the algebraic closure of $F$, iff there exist polynomials $P_i(\bar{z})$ from $F[\bar{z}]$ such that

$$\sum_i P_i(\bar{z})Q_i(\bar{z}) = 1. \quad (2)$$

We can also use this to test solvability in the finite field $F$ itself by adding the equations $\{z_j^{|F|} - z_j = 0\}$ to (1) and we will usually assume that these equations have been included in (1).

The $NP$-completeness of the solvability problem for (1) in $F$ holds even if the degrees of the $Q_i$'s are bounded by a constant. Suppose there existed $P_i$'s of constant degree satisfying (2) for the extended system whenever (1) did not have a solution. Then, by solving linear equations which determine the coefficients of the monomials in the $P_i$'s, we could construct these polynomials in polynomial time. Thus $P \neq NP$ implies that there are instances such that the degree of $P_i$'s cannot be bounded by a constant. But the assump-
In a series of results, it has been shown that any constant-depth Frege proof of the *pigeonhole principle* (PHP) requires exponential size [12, 1, 13, 10, 17, 19]. These results were extended to show that even with the pigeonhole principle as an additional axiom constant-depth Frege systems require exponential size to prove the $\text{Count}_2$ tautologies [2, 17, 20]. (We use the notation $\text{Count}_q$ for the generic version of $\text{Count}_q!^m$ where $m \neq 0 \pmod{q}$.) Ajtai [3] studied the relationships among the various modular counting principles and showed that if $p, q$ are different primes then $\text{Count}_q$ does not admit polynomial size, constant-depth Frege proofs from instances of $\text{Count}_p$. Riis [20] also considered the same problem.

In this paper we give a new proof of this lower bound which also applies when $p$ and $q$ are not primes. We also give upper bounds that result in an exact characterization of when polynomial-size constant-depth Frege proofs exist. The lower bound proof consists of two parts. The first part is similar to the proof strategy of [6, 17, 19] and it is a universal method allowing us to reduce the lower bound problem to a combinatorial question about the existence of certain finite structures. This part employs ideas from boolean complexity (partial truth assignments, switching lemmas). The second part involves the lower bound for Hilbert’s Nullstellensatz.

## 1 Proof systems and counting principles

We confine ourselves to the following propositional language: atoms $x, y, \ldots$, constants 0 (falsity) and 1 (truth), negation $\neg$ and disjunction $\vee$ (binary). We use $\land$ as an abbreviation. The *depth* of a formula is the maximal number of alternations of $\neg$ and $\lor$ and its *size* is the number of occurrences of $\lor$. We shall use symbol $\bigvee_i \phi_i$ denoting the disjunction of unbounded arity as an abbreviation for the disjunction formed from binary $\lor$ with brackets distributed arbitrarily.

A *Frege system* [10] is a sound and implicationally complete proof system having a finite number of axiom schemes and inference rules. A typical Frege system is the usual calculus based on a finite number of axioms with modus ponens as the only rule of inference. The *size* of a proof in a Frege system is the number of distinct subformulas appearing in the proof where we do not distinguish $F$ and $\neg F$. We will also need a notion of the *size* of the inference rules and axiom schemes in a Frege system. For this we use the same notion of the number of distinct subformulas appearing in the axiom scheme or inference rule and we again identify
A depth $d$ Frege system is a Frege system allowing only formulas of depth at most $d$ in proofs. It is not complete but there is a constant $c$ such that any depth $d$ tautology has a depth $c+d$ proof in the Frege system.

**Definition 1.1** Let $N \geq r \geq 2$ and let $V$ be a set of cardinality $N$. $[V]^r$ denotes the set of $r$-element subsets of $V$.

Formula $\text{Count}_r^N$ is formed from atoms $x_e, e \in [V]^r$ and it is the formula:

$$\bigvee_{e \in [V]^r} \neg x_e \vee \bigvee_{e \in f} (x_e \land x_f)$$

where $e \perp f$ abbreviates the conjunction $e \cap f \neq \emptyset \land e \neq f$.

Denote by $\text{Count}_{r,s}$ the set of formulas $\text{Count}_r^N$ for $N \equiv i \pmod{r}$. For $R$ a set of pairs $(r,i)$ such that $0 < i < r$, $\text{Count}_{r,R}$ denotes the union of the sets of formulas $\text{Count}_{r,s}$ such that $(r,i) \in R$. Finally, $\text{Count}$ denotes the set of all formulas $\text{Count}_r^N$ for $N \not\equiv 0 \pmod{r}$; equivalently, $\text{Count}$ is $\text{Count}_r^N$ for $R = \{(r,i) \mid 0 < i < r\}$.

In the introduction we observed that if $r$ divides $s$ then are polynomial size constant-depth Frege proofs of $\text{Count}_r^s$ from $\text{Count}_r^r$.

**Problem** Assume $s,r \geq 2$ and assume $r$ does not divide $s$. Are there polynomial size, constant-depth Frege proofs of $\text{Count}_r^s$ from instances of formulas in $\text{Count}_r^r$? If so, under what circumstances do they exist?

This was solved in the negative by Ajtai [3] for the case when $r,s$ are two different primes. The following theorem is a strengthened version of Ajtai's result that gives a complete characterization of this problem. Let symbol $(a,b)$ denote the greatest common divisor of $a$ and $b$.

**Theorem 1.2** Let $q \geq 2$ and $0 < i < q$. Let $R$ be a set of pairs of integers $(p,j)$ such that $0 < j < p$. Then there are constant-depth, polynomial size Frege proofs of formulas from $\text{Count}_{q,i}^N$ from instances of $\text{Count}_R$ if and only if there is a $(p,j) \in R$ such that all prime divisors of $(q/j)$ also divide $\frac{q}{(q,j)}$.

**Corollary 1.3** Let $p,q \geq 2$ and assume that there is a prime factor of $q$ which does not divide $p$. Then there is an infinite set of $N \not\equiv 0 \pmod{q}$ such that there are no constant-depth, polynomial size Frege proofs of $\text{Count}_r^N$ from instances of $\text{Count}_p$. In particular, this holds for all sufficiently large $N$ such that $\frac{q}{(q,N)} = 1$.

On the other hand, if all prime factors of $q$ also divide $p$ then for every infinite set of $N \not\equiv 0 \pmod{q}$ there are constant-depth, polynomial size Frege proofs of $\text{Count}_q^N$ from instances of $\text{Count}_p$.

**Proof of Corollary 1.3 from Theorem 1.2:** For the first part, if $r$ is a prime factor of $q$ which does not divide $p$ then for $N \equiv q/r \pmod{q}$ we have $(p, \frac{q}{(q,N)}) = (p,r) = 1$. It follows that for all $j$, $0 < j < p$, $(p, \frac{q}{(q,N)}) = 1$. Thus for each $j$, $0 < j < p$, there is some prime factor of $(\frac{p}{j})$ that is not a factor of $\frac{q}{(q,N)}$. Applying Theorem 1.2 we obtain our desired result.

For the second part, assume that all prime factors of $q$ also divide $p$. For $N \equiv 0 \pmod{q}$, let $s$ be any prime factor of $\frac{q}{(q,N)}$. By assumption $s$ also divides $p$. Thus for $j = p/s$ all prime factors of $\frac{p}{j}$ also divide $\frac{q}{(q,N)}$ and applying Theorem 1.2 we are done. □

The bulk of our arguments are concerned with our extension of Ajtai's lower bounds but we deal with the upper bounds first. These are extensions of upper bounds due to Riis [20]. The informal arguments given below can be easily formalized by polynomial size, constant-depth Frege proofs.

**Lemma 1.4** Assume that $r \geq 2$, $0 < i < r$, and $k$ is a positive integer. Then

(a) there are polynomial size constant-depth Frege proofs of $\text{Count}_{r,s}$ from instances of $\text{Count}_{r,k}$.

(b) if $ik \not\equiv 0 \pmod{r}$, there are polynomial size constant-depth Frege proofs of $\text{Count}_{r,s}$ from instances of $\text{Count}_{r,k}$ mod $r$.

**Proof:** Suppose that we have an $r$-partition of $N$, $N \equiv i \pmod{r}$. We can make $k$ copies of each point to create a new set of size $N' = Nk$. Part (a) follows by creating an $rk$-partition of $N'$ where each new class contains all $k$ copies of the elements of each class from the partition of $N$. Part (b) follows instead by creating an $r$-partition of $N'$ by making each class in the partition of $N$ into $k$ classes in the new partition. □

The proof of the following lemma is more interesting but too long to include here. The main idea in its proof, which we borrow from a similar construction due to Riis [20], is to use a property of a set $N$ (existence of an $rk$-partition of $N$) to obtain a property of the set $M$ of $k$-element subsets of $N$ (existence of an $r$-partition) and to use the fact that the size of $M$ modulo $r$ depends on the size of $N$ in a nice way.
Lemma 1.5 Let \( r \geq 2 \) and \( k \) be a positive integer. There are polynomial size constant-depth Frege proofs of \( \text{Count}_{r,k} \) from instances of \( \text{Count}_{r,1} \).

Corollary 1.6 Let \( p \geq 2 \) and \( 0 < j < p \).

(a) There are polynomial size constant-depth Frege proofs of \( \text{Count}_{p,j} \) from instances of \( \text{Count}_{p,j+1} \), and

(b) There are polynomial size constant-depth Frege proofs of \( \text{Count}_{p,j} \) from instances of \( \text{Count}_{p,j+1} \).

Proof: For (a) part, we start with instances of \( \text{Count}_{p,j+1} \). By Lemma 1.5 we obtain \( \text{Count}_{p,p,j} \). By definition there are integers \( k, l \) such that \( (p, j) = kj + lp \). Applying Lemma 1.4 part (b) with this value of \( k, r = p \) and \( i = j \) we obtain \( \text{Count}_{p,j} \). For (b) part, starting with instances of \( \text{Count}_{p,j} \) and applying Lemma 1.4 part (a) with \( r = p, i = j, k = (p, j) \) we obtain \( \text{Count}_{p,j} \). Then, applying Lemma 1.4 part (b) with \( r = p, i = j, k = (p, j) \) we obtain \( \text{Count}_{p,j+1} \).

Lemma 1.7 Let \( p, q \geq 2 \). If all prime factors of \( p \) also divide \( q \) then there are polynomial size constant-depth Frege proofs of \( \text{Count}_{q,1} \) from instances of \( \text{Count}_{p,1} \).

Proof: If all prime factors of \( p \) also divide \( q \) then there is some integer \( k \) such that \( p \mid q^k \). By splitting the classes of size \( p \) into pieces of size \( q^k \), we can obtain polynomial size constant-depth Frege proofs of \( \text{Count}_{q,1} \) from instances of \( \text{Count}_{p,1} \). We will show how to obtain \( \text{Count}_{q,1} \) from instances of \( \text{Count}_{p,1} \).

Suppose that there is some \( q \)-partition \( E \) of \( N \equiv 1 \pmod{q} \). The Fermat-Euler Theorem implies that \( N^m \equiv 1 \pmod{q^k} \) where \( m \) is any multiple of \( \phi(q^k) \). Fix some such multiple \( m \) with \( m \geq k \). Define a \( q \)-partition \( E' \) of \( N^m \) by taking the \( m \)-th Cartesian power of \( E \) i.e. the classes of \( E' \) have the form: \( e_1 \times \ldots \times e_m \) where \( e_i \) are classes of \( E \). \( E' \) is a \( q \)-partition of \( N^m = N \times \ldots \times N \). Decompose each class of \( E' \) into \( q \)-subclasses of size \( q^k \). This yields a partition violating \( \text{Count}_{q,1} \).

We are now ready to prove the forward direction of Theorem 1.2. Assuming that all prime divisors of \( \text{Count}_{p,j} \) divide \( \frac{q}{q^k} \), we want to show that we can prove \( \text{Count}_{q,1} \) from \( \text{Count}_{p,j} \). By Corollary 1.6 part (b), we can prove \( \text{Count}_{p,j} \) from \( \text{Count}_{p,j+1} \). Then by Lemma 1.7, we can prove \( \text{Count}_{q,1} \) from \( \text{Count}_{p,j+1} \). Lastly, by Corollary 1.6 part (a), we can derive \( \text{Count}_{q,1} \) from \( \text{Count}_{p,1} \).

2 Reducing the lower bound to a combinatorial problem

In this section we reduce the lower bound that we are after to a purely combinatorial problem concerning generic systems. This section is a modification of very similar arguments that can be found in [7] and [20] (the name generic systems was introduced in [20] for similar objects). For the rest of the paper we shall fix two different numbers \( p, q \geq 2 \) and a set \( V \) of cardinality \( N \) such that \( N \not\equiv 0 \pmod{q} \). We will sometimes find it convenient to identify an integer \( N \) with a canonical set of size \( N \). We will first state some important definitions.

2.1 \( q \)-decision trees and \( k \)-evaluations

Definition 2.1 A \( q \)-decision tree \( T \) over \( V \) is a finite directed tree whose vertices other than leaves are labelled by elements \( v \in V \), whose edges are labelled by classes \( e \in [V]^q \), whose leaves are labelled from a fixed set \( L \) of values, (usually \( L \) will be the set \( \{0, 1\} \)) and which satisfies two conditions:

1. if the label of the root of \( T \) is \( v \) then for any \( e \in [V]^q, v \in e \), there is exactly one edge outgoing from the root and labelled by \( e \), and there are no other edges.

We shall identify the edges by their labels.

2. Let \( T^* \) be the proper subtree of \( T \) whose root is the end-point of edge \( e \) outgoing from the root. Then \( T^* \) is a \( q \)-decision tree over \( V \setminus \{e\} \).

The height of tree \( T \) is the maximum number of edges on a path from the root to a leaf. Let \( \text{br}(T) \) denote the set of branches of \( T \) and \( \text{br}_1(T) \) denote the set of branches of \( T \) with leaf label \( i \in L \). We shall also identify a branch with the conjunction of the variables indexed by its edges.

We would like to prove the main theorem by finding an assignment making all formulas from \( \text{Count}_R \) true but \( \text{Count}_q \) false, demonstrating thus that \( \text{Count}_q \) cannot be proved from \( \text{Count}_R \). This is, of course, impossible as all formulas in \( \text{Count}_q \) are tautologies. So we must find another way of 'evaluating' formulas which would permit such argument. A possible evaluation is to assign to each formula \( \phi \) a usual decision tree deciding the value of the formula and consider the set of all branches of the tree for \( \phi \) with leaf label 1. Thus \( \phi \) is a tautology iff all branches in this decision tree have leaf label 1 (\( \text{br}(T \phi) = \text{br}_1(T \phi) \) in future terminology).
We shall approximate this idea by the following definition. To each formula \( \phi \) we assign a q-decision tree \( T_\phi \). Intuitively, a formula \( \phi \) is approximately true iff all branches in \( T_\phi \) have leaf label 1. Furthermore, condition (1) of Definition 2.1 corresponds to the first conjunct in \( \neg \text{Count}^N_q \) (i.e. every \( v \in V \) is in some class \( e \) of the partition violating \( \text{Count}^N_q \)) while condition (2) corresponds to the second one (that any two classes in the partition are disjoint). Hence we expect that all leaves of \( T_\phi \) have leaf label 1 and thus get a notion of evaluation in which \( \text{Count}^N_q \) is false. The following is a reinterpretation of the definition in [17].

**Definition 2.2** Let \( \Gamma \) be a set of formulas formed from atoms of \( \text{Count}^N_q \) (we shall not repeat this condition as we do not consider formulas formed from other atoms) and closed under subformulas.

A k-evaluation of \( \Gamma \) is a map \( T : \phi \mapsto T_\phi \), defined on \( \Gamma \) such that:

1. The set of leaf labels \( L \) of \( T_\phi \) is \( \{0, 1\} \).
2. \( T_\phi \) is a q-decision tree over \( V \) of height at most \( k \).
3. \( T_0 \) and \( T_1 \) are q-decision trees of height 0,
   \( br_1(T_0) = 0 \) and \( br_1(T_1) = br(T_1) \).
4. \( T_{\phi \lor \psi} \) is a q-decision tree having the property that every non-leaf vertex of \( T_{\phi \lor \psi} \) is labelled by some \( v \in e \), and \( br_1(T_{\phi \lor \psi}) \) is the unique branch of length 1 consisting of the edge labelled by \( e \).
5. \( br(T_{\phi \land \psi}) = br(T_\phi) \land br(T_\psi) \) and \( br(T_{\phi \lor \psi}) = br(T_\phi) \lor br(T_\psi) \).
6. if \( \phi = \bigvee_1 \phi_1 \) then \( T_\phi \) refines and represents \( \bigvee H \) where \( H := \bigcup_i br(T_{\phi_i}) \), i.e.:
   (a) \( br(T_\phi) \) refines \( H \), i.e. every \( E \in br(T_\phi) \) either is a superset of some \( F \in H \) or \( E \subseteq F \) for all \( F \in H \) where \( E \perp F \) iff \( e \perp f \) for some \( e \in E \) and \( f \in F \).
   (b) \( br(T_\phi) = \{ E \in br(T_\phi) \mid \exists F \in H, F \subseteq E \} \).

The following lemma is completely analogous to a lemma from [17] treating the case of PHP, in place of \( \text{Count}^N_q \) and we shall not reprove it here.

**Lemma 2.3** Assume \( \Gamma \) is a set of formulas closed under subformulas. Let \( T \) be its k-evaluation and assume \( kq^s < N \). Then

1. if \( \phi \in \Gamma \) is an axiom scheme of size at most \( s \) then \( br_1(T_\phi) = br(T_\phi) \).
2. equality \( br_1(T_\phi) = br(T_\phi) \) is preserved by any sound inference rule of size at most \( s \); for example if \( 3kq < N \), \( br_1(T_\phi) = br(T_\phi) \) and \( br_1(T_{\alpha \lor \beta}) = br(T_{\alpha \lor \beta}) \).
3. if \( \phi = \text{Count}^N_q \in \Gamma \) then \( br_1(T_\phi) = 0 \neq br(T_\phi) \).

Assume now that \( \Pi \) is a short constant-depth Frege proof of \( \text{Count}^N_q \) from some instances of \( \text{Count}_R \); that is from some formulas

\[
\text{Count}^N_q(y, q, \psi_1, \psi_2),
\]

where \( M = j \mod p \), \( 0 < j < p \) and \( (p, j) \in R \), \( g \in [M]^p \) and \( \psi_g \) are formulas in atoms \( \pi_e \) of \( \text{Count}^N_q \). Other than the \( \text{Count}_R \) axioms, there is a constant \( s \) such that all axiom schemes and inference rules used in \( \Pi \) are of size at most \( s \). Suppose that there is a k-evaluation \( T \) of all subformulas in \( \Pi \) such that

1. \( kqs < N \) and
2. for all instances \( \phi \) of a \( \text{Count}_R \) axiom in \( \Pi \), \( br_1(T_\phi) = br(T_\phi) \).

That would give a contradiction with Lemma 2.3 as \( br_1(T_\phi) = br(T_\phi) \) would hold for all axioms and all inferences in \( \Pi \) but not for the final formula.

This motivates the structure of our argument. More precisely, we first show that if \( \Pi \) is a short proof of \( \text{Count}^N_q \) then there is a k-evaluation of all subformulas of \( \Pi \) satisfying (1) but not (2) and thus derive in Theorem 2.5 that a particular combinatorial object (a generic system) must exist. We then derive a contradiction in Lemma 2.10 by showing that this combinatorial object cannot exist.

**Definition 2.4** A \( (p, q, \ell, M) \)-generic system over \( V \) is a collection of q-decision trees over \( V \), \( T_i, i \leq M \), with leaf labels from \( [M]^{p} \) such that:

1. each \( T_i \) has height at most \( \ell \);
2. each branch in \( T_i \) with leaf label \( g \) has \( i \in g \);
3. for all \( g \in [M]^{p} \), \( br(g(T_i)) = br(T_i) \) for all \( i, j \in g \).

Informally, a \( (p, q, \ell, M) \)-generic system over \( V \) specifies locally consistent pieces of a perfect p-partition of \( M \) as partial functions of \( \{z_e\}, e \in [V]^{p} \). (Say that \( E \) and \( F \) are compatible if \( E \perp F \). By locally consistent, we mean that any mutually compatible set of branches in the trees of the generic system have leaf labels that are themselves mutually compatible.) When \( M \) is congruent to 0 mod \( p \), \( (p, q, 1, M) \)-generic systems exist (take any system of height 1 q-decision trees \( \{T_i\} \) and a p-partition \( \pi \) of \( M \) and label...
all leaves of $T_i$ by the $p$-class $e \in \pi$ such that $i \in e$.

Even when $M$ is not congruent to $0 \mod p$, the existence of a $(p, q, \ell, M)$-generic system is not inconceivable since there need not be any mutually compatible set of branchings that contains a branch from each $T_i$.

**Theorem 2.5** Let $0 < i < q$ and $R$ be a set of pairs of integers $(p, j)$ such that $0 < j < p$. Let $d$ be a constant and $k(N)$ a function of $N$ with $k(N) = N^{O(1)}$, and assume that for sufficiently large $N$, $N \equiv i \mod q$, there are depth $d$ size $N^{k(N)}$ Frege proofs of Count$_N^*$ from instances of Count$_R$.

Then for sufficiently large $N \equiv i \mod q$ there is a $(p, j) \in R$, an $N' \leq N$, $N' = N^{O(1)}$ and $N' \equiv i \mod q$, an $\ell = O(k(N))$ and a number $M = N^{O(\ell)} = (N')^{O(\ell)}$, $M \equiv j \mod p$, such that there exists a $(p, q, \ell, M)$-generic system over a set $V$ of size $N'$.

For the proof we need to use restrictions.

**Definition 2.8** A restriction $\rho$ is given by a set of disjoint $q$-element sets on a domain $V$. It determines an assignment to the variables over $V$ as follows:

\[
(x_e)^\rho = \begin{cases} 
1 & \text{if } e \in \rho, \\
0 & \text{if } e \notin \rho \text{ but } e \cap f \neq \emptyset \text{ for some } f \in \rho, \\
\text{otherwise} & 
\end{cases}
\]

We shall denote by $V^\rho$ the set of vertices not covered by $q$-element sets of $\rho$. Denote by $F^\rho$ the effect of applying the assignment to a Boolean formula $F$; we use similar notation for the effect of $\rho$ on proofs, functions etc. Also, we can apply a restriction $\rho$ to a $q$-decision tree $T$ over $V$ in the obvious way to obtain a $q$-decision tree $T^\rho$ over $V^\rho$. Note that after applying $\rho$, we get essentially the same modulus $q$ counting principle on $V^\rho$ and that $|V^\rho| \equiv |V| \mod q$.

**Proof:** Assume that $\Pi$ is a depth $d$, size $N^{k(N)}$ Frege proof of Count$_N^*$ from instances of some Count$_R$, and thus $M_i = N^{O(k(N))}$ automatically. We begin by applying a restriction $\rho$ to each formula in $\Pi$ to get a new proof, $\Pi'$ over a smaller universe $N' < N$ with the property that $\Pi'$ has a $k$-evaluation—this is the content of the following lemma.

**Lemma 2.7** Let $\Pi$ be a depth $d$, size $N^{k(N)}$ Frege proof of Count$_N^*$ from instances of Count$_R$. For some $c_d \leq 5kq^2d^4$, if $k(N) \leq N^{1/c_d}$, then there exists a restriction $\rho$ such that:

1. $N' = |V^\rho| \geq N^{3/c_d},$

2. $N' \equiv N \mod q$, (3) $\Pi$ restricted by $\rho$ is a proof (over $N'$) of Count$_N^*$ from instances of Count$_R$, and

4. there exists an $k'$-evaluation, $T$, of the subformulas in $\Pi'$ for $k' \leq c_d k(N)$.

The above lemma is proven by inductively generating $k_d$-evaluations (for some appropriate sequence of values $k_d$) for the set of subformulas appearing at the $\ell$ bottom levels of every formula in $\Pi$. It is trivial to do this for the literals and constants on the leaves of the formulas. This $k_d$-evaluation is extended to a $k_{d+1}$-evaluation of the set of subformulas in $\Pi$ one level higher by applying a Håstad-style switching lemma [13] on an appropriate class of restrictions. The restrictions that are needed, together with the corresponding switching lemma, are stated below. A complete proof of this switching lemma and a sketch of how to apply it to obtain the above lemma can be found in [5].

**Definition 2.8** Define the set of restrictions $M'_{N'}$ to be the set of all partial $q$-partitions $\rho$ of $V$ which cover all but $qm + j$ nodes of $V$ where $j = |V| \mod q$.

**Lemma 2.9** Fix some set $V$ of vertices and integers $m, \ell$, and $s \geq 0$. Let $T_0$ be any set of $q$-decision trees over $V$ of height at most $r$, let $n = \lfloor |V|/q \rfloor$ and let $u = m/n$. If $\rho$ is a restriction chosen uniformly at random from $M'_{N'}$, then with probability at least $1 - (4e^2r^{-1/3}uq^{n-1/3})^s$, there is a $q$-decision tree over $V^\rho$ of depth at most $s$ refining and representing $\bigvee_{\ell} br(T_0^\rho)$.

If $S$ is a set of Boolean formulas closed under subformulas and $T$ is a $k$-evaluation of $S$ over $V$ then it is easy to check that the map $T'$ that sends $\phi^\rho \rightarrow T_{\phi^\rho}$ is a $k$-evaluation of $S^\rho$ over $V^\rho$. With this observation and the appropriate choice of parameters we obtain Lemma 2.7 from repeated applications of Lemma 2.9.

After applying Lemma 2.7, we are left with a new proof of Count$_{N'}^*$ from instances of Count$_R$: Count$_{M'_N}(\psi)$ such that $M_i \equiv j_i \mod (p_i)$ where $(p_i, j_i) \in R$, together with a $k'$-evaluation, $T'$, for all subformulas in the proof, where $N' = N/e$, $e > 0$, and $M_i \leq (N')^{k'/4}$ for $k' = O(k(N))$.

Lemma 2.3 implies (as $br(T_{\phi}) \neq br(T_{\phi'})$ holds for the final formula $\eta$ of $\Pi'$) that $bt_0(T_{\phi}) \neq 0$ for all one Count$_R$ axiom $\phi$ in $\Pi'$. Take one such $\phi$, and any $G \in bt_0(T_{\phi})$ and restrict $\Pi'$ further by $G$. In particular, $\phi$ is reduced to some instance $\phi^G = Count_{M'_N}(\psi)$ for which $br(T_{\phi^G}) = br_0(T_{\phi})$. To simplify further notation we shall assume that already $G \subseteq \rho$; hence
For all incompatible $g, h \in [M]^p$, if $E$ is a branch of $T_{\phi_g}$ labelled by 1, and $F$ is a branch of $T_{\phi_h}$ labelled by 1, then $E \cap F$. Thus, the decision trees $T_i$, $i \in [M]$ induce a Frege proof $T_i$ over $\mathcal{L}_F$. We will show that the set of $q$-partition decision trees $T_i$, $i \in [M]$ form a $(p, q, \ell, M)$-generic system for $\ell = O(k(N))$. By construction, the trees $T_i$ have height $O(pk'/\epsilon) = O(k(N))$ and the $T_i$ are defined over a set of size $N'' = N^{4k}$. Also by construction, each branch in $T_i$ with leaf label $g$ has $i \in g$. Finally, by the above argument, we have shown that for every $g$, and every $i, j \in g$, the set of branches in $\text{br}(T_i)$ with leaf label $g$ is equal to the set of branches in $\text{br}(T_j)$ with leaf label $g$. Thus, the decision trees $T_i$, $i \in [M]$ is a $(p, q, \ell, M)$-generic system as required by Theorem 2.5.

We shall apply Theorem 2.5 only for $k(N)$ a constant because we are able to prove the next lemma only for $\ell$ a constant independent of $N$. It is our main combinatorial result and its proof occupies sections 3 and 4.

**Lemma 2.10** Let $\ell > 0$. For all sufficiently large $N$ such that $(p(\ell - 1)^{\ell+1}, q) \mid N$, there does not exist a $(p, q, \ell, M)$-generic system over $\mathcal{L}_F$, with $M \not\equiv 0 \pmod{p}$.

**Proof of Theorem 1.2:**
Let $q' = (\frac{2}{M})$ and $R' = \{ (p, j) \mid (p, j) \in R \}$. By Corollary 1.6 it suffices to show that there are polynomial size constant-depth Frege proofs of $\text{Count}_{q', 1}$ from instances of $\text{Count}_{q', 1}$, $p' \in R'$, and if only if there is some $p' \in R'$ such that all prime factors of $p'$ also divide $q'$.

In the case that some such $p'$ exists, the statement follows immediately from Lemma 1.7.

Now suppose instead that for every $p' \in R'$ there is some prime factor of $p'$ that does not divide $q'$. Let $k$ be a constant. Assume that, for sufficiently large $N \equiv 1 \pmod{q'}$, there are depth $d$ size $N^k$ Frege proofs of $\text{Count}_{q'}$ from instances of $\text{Count}_{q', 1}$. Then by Theorem 2.5 for some $p' \in R'$ there is a $(p', q', \ell, M)$-generic system over $N' \equiv 1 \pmod{q'}$ for constant $\ell$, $M \equiv 1 \pmod{p'}$, and $N'$ arbitrarily large.

Let $r$ be the prime factor of $p'$ that does not divide $q'$. From the $(p', q', \ell, M)$-generic system over $N'$ we can derive an $(r, q', \ell, M)$-generic system over $N'$ by splitting sets of size $p'$ in a canonical way into $p'/r$ sets each of size $r$. More precisely, for each $i \in M$ and
We note that, although \( x_e^{|F|} - x_e \) is not present explicitly in the system of polynomials, \( Q_e, Q_{e,f} \), it is easily derived since \( x_e^2 - x_e \) is obtainable as a linear combination \( x_e \cdot Q_e - \sum_{v \in \epsilon', e' \neq e} Q_e, e' \) for any \( v \in \epsilon \). Thus a non-constant degree lower bound on the \( P_e \) and \( P_{e,f} \) in the above linear combination also implies such a non-constant lower bound for an extended system of the type considered in the introduction.

We shall study linear combinations of polynomials \( Q_e, Q_{e,f} \) also for the ring \( \mathbb{Z}_p \) of counting modulo \( p \), where we do not assume that \( p \) is prime. Henceforth a linear combination \( L \) means a polynomial of the form:

\[
\sum_v P_v \cdot Q_v + \sum_{e \perp f} P_{e,f} \cdot Q_{e,f}
\]

and the degree of \( L \) is the maximum degree of the polynomials \( P_v, P_{e,f} \).

For a non-empty \( q \)-partition \( E = \{ e_1, \ldots, e_t \} \) of \( V \) denote by \( x_E \) the monomial \( x_{e_1} \cdots x_{e_t} \) and put \( x_\emptyset := 1 \).

**Lemma 3.3** Let \( T \) be a \( q \)-decision tree of height \( \ell \) and assume \( \ell q < N \). Then the polynomial

\[
\omega_T := ( \sum_{E \in br(T)} x_E ) - 1
\]

can be expressed as a linear combination of degree at most \( \ell - 1 \).

(This means that \( \omega_T \) is equal to 1 modulo the ideal generated by polynomials \( Q_v, Q_{e,f} \), but the bound on the degrees is also important for us.)

**Proof:** Proceed by induction on \( \ell \). For \( \ell = 1 \)

\[
\omega_T = \sum_{v \in V} x_v - 1
\]

for some \( v \in V \) which is just the polynomial \( Q_v \) itself. Hence \( \omega_T \) is a linear combination of degree 0.

Assume \( \ell > 1 \) and let \( v \) be the label of the root of \( T \). Then:

\[
\omega_T = \sum_{E \in br(T)} x_E - 1 = \sum_{v \in \epsilon} ( \sum_{P \in br(T^v)} x_P ) - 1
\]

By the induction hypothesis there are linear combinations \( L_e \) of degree at most \( \ell - 2 \) such that:

\[
L_e = \sum_{F \in br(T^v)} x_F - 1
\]

and so

\[
\omega_T = \sum_{v \in \epsilon} (x_e (L_e + 1) - 1 = \sum_{v \in \epsilon} x_e \cdot L_e + \sum_{v \in \epsilon} x_e - 1
\]
The quantity \( \sum_{x \in x} x \cdot L_x \) is a linear combination of degree at most \( \ell - 1 \) and the remaining quantity is just the polynomial \( Q_0 \); hence \( u_i \) is also a linear combination of degree at most \( \ell - 1 \).

The next lemma is an important property of generic systems.

**Lemma 3.4** Let \( T_i, i \in [M] \) be a \( (p, q, \ell, M) \)-generic system. Then in the ring \( \mathbb{Z}_p[\bar{x}_e] \) we have

\[
\sum_{i \in [M]} \sum_{E \in \text{br}(T_i)} x_E = 0.
\]

**Proof:** Let \( g \in [M]^p \) and \( S_g = \bigcup_{i \in [M]} \text{br}_g(T_i) \). By the definition of a generic system, for each \( i \in g \), \( \text{br}_g(T_i) = S_g \) and for each \( i \not\in g \), \( \text{br}_g(T_i) = \emptyset \). Thus for each \( g \), each branch in \( S_g \) occurs \( p \) times in \( \bigcup_{i \in [M]} \text{br}(T_i) \), once for each of the elements \( i \in g \), and hence

\[
\sum_{i \in [M]} \sum_{E \in \text{br}(T_i)} x_E \equiv 0 \pmod{p}.
\]  

The lemma below follows from the previous two lemmas.

**Lemma 3.5** If there is a \( (p, q, \ell, M) \)-generic system \( T_i, i \in [M] \), such that \( \ell \cdot q < N \), then there is a linear combination \( L \) of degree at most \( \ell - 1 \) such that \( L + M = 0 \) in the ring \( \mathbb{Z}_p[\bar{x}_e] \).

**Proof:** By Lemma 3.3, we can write the sum

\[
\sum_{i \in [M]} \sum_{E \in \text{br}(T_i)} x_E
\]

as:

\[
\sum_{i \in [M]} (L_i + 1) = \sum_{i \in [M]} L_i + M
\]

where \( L_i \) are linear combinations of degree at most \( \ell - 1 \). But by Lemma 3.4,

\[
\sum_{i \in [M]} \sum_{E \in \text{br}(T_i)} x_E = 0
\]

and thus we have \( \sum_{i \in [M]} L_i + M = 0 \).

The following is the main technical result of this paper.

**Lemma 3.6 (main)** Let \( d \) be a constant, let \( N \) be sufficiently large and suppose that \( N \) satisfies \( (pd^{d+1}, q) \mid N \). Then every linear combination \( L \) such that \( L = M \) in \( \mathbb{Z}_p[\bar{x}_e] \) must have degree larger than \( d \).

Put otherwise, linear combinations expressing a constant other than 0 cannot have a constant degree.

We shall prove the main lemma in the next section, now we infer Lemma 2.10 from it.

**Proof of Lemma 2.10 from Lemma 3.6**

Assume that for some constant \( \ell \) there exists a \( (p, q, \ell, M) \)-generic system \( T_i, i \in [M], M \not\equiv 0 \pmod{p} \), over some \( N \) such that \( (pd^{d+1}, q) \mid N \).

If \( N \equiv 0 \pmod{q} \) then there is some perfect \( q \)-partition \( \pi \) of \( N \). For each \( q \)-decision tree \( T_i \), there is some branch \( E_i \) in \( T_i \) such that \( E_i \subseteq \pi \). By the definition of generic systems, the leaf labels of these branches form a perfect \( p \)-partition of \( M \) which is impossible since \( M \not\equiv 0 \pmod{p} \).

Suppose now that \( N \not\equiv 0 \pmod{q} \). By Lemma 3.5 the existence of this \( (p, q, \ell, M) \)-generic system over \( N \) implies the existence of a linear combination, \( L \), of degree at most \( \ell - 1 \) such that \( L = -M \) in the ring of polynomials \( \mathbb{Z}_p[\bar{x}_e] \). But this contradicts Lemma 3.6 because \( -M \) is not congruent to 0 mod \( p \).

\[ \square \]

### 4 Proof of the lower bound on the degree of the polynomials

In this section we prove main Lemma 3.6. It is an immediate corollary of the following lemma.

**Lemma 4.1** Let \( d \) be a constant, let \( N \) be sufficiently large and suppose that \( N \) satisfies \( (pd^{d+1}, q) \mid N \). If \( P_e, v \in V, |V| = N \), are of degree \( \leq d \), then there exists a 0-1 assignment \( a \) such that for every \( e \perp f \)

\[
Q_{e,f}(a) = 0,
\]

and

\[
\sum_{v \in V} P_v(a)Q_v(a) = 0,
\]

where we count in \( \mathbb{Z}_p \).

The rest of the section is devoted to outlining the proof of this lemma. We first need some preliminary concepts.

A 0-1 assignment corresponds to a set of \( q \)-element sets (those for which \( x_e(a) = 1 \)). For this to satisfy (3) these \( q \)-element sets must be disjoint, so without loss of generality we restrict ourselves to such assignments. Also, since we shall evaluate polynomials on 0-1 inputs, we can replace any \( x_e^d \) with \( d > 1 \) by \( x_e \). Thus we shall assume that all polynomials are multilinear. (This assumption could also easily have been justified by the fact that for any \( e, x_e^2 - x_e \) is obtainable as a linear combination of degree 1.)

Let \( \Xi = x_{e_1}, \ldots, x_{e_d} \) be a monomial of \( P_e \). If \( v \in e_j \), for some \( j \), then \( \Xi(a)Q_v(a) \) is always 0, since if
Proof: Take $t \geq 0$ such that

$$N - qt \geq 0 \text{ and } N - qt \equiv 0 \pmod{p^{k+1}}.$$ 

Let $a$ consist of a $q$-partition of the last $qt$ elements of $V$, the rest being uncovered. Then for $v > N - qt$, $P_r(a)Q_s(a) = 0$, since $Q_s(a) = 0$ already. For $1 \leq v \leq N - qt$ we have $Q_s(a) = -1$ and all monomials $\Xi$ in $V$, that are non-zero under $a$ have support contained in the last $qt$ elements of $V$. Thus, the choice of $v \leq N - qt$ does not affect the type $(v, \Xi)$ for any monomials $\Xi$ that are non-zero under $a$. By $p^k$-symmetry, for any two $v, v' \leq N - qt$ that agree modulo $p^k$, the coefficients of all monomials with support among the last $qt$ elements of $V$ are the same in $P_r$ and $P_{r'}$. Since $p^{k+1}$ divides $N - qt$ the number of $v \leq N - qt$ congruent to $i$ modulo $p^k$ is divisible by $p$ for each fixed $0 \leq i < p^k$. Thus $p^k$-symmetry implies that for every $i$

$$\sum_{v \leq N - qt, v \equiv i \pmod{p^k}} P_r(a)Q_s(a) \equiv 0 \pmod{p},$$

whence the lemma follows. \hfill \Box

We note that in the argument above we actually used relatively little of the properties of $p^k$-symmetry. However, the notion of $p^k$-symmetry is more natural for the application of Ramsey's theorem and it facilitates the inductive nature of the argument.

To apply Ramsey's theorem we employ restrictions as described in section 2. When we try to apply Ramsey's theorem to get a $p^k$-symmetric system of polynomials after applying some restriction $\rho$ we encounter two problems: First, a single application of Ramsey's theorem will only allow us symmetrize with respect to monomials of some particular degree (since the signatures of monomials of different degrees are different.) When we symmetrize with respect to the monomials of some degree $c$, we apply a restriction and this restriction may also create new monomials of degree $c$ from monomials of larger degree. Thus it makes sense to symmetrize starting with monomials of large degree first in the hope that the newly created monomials will occur symmetrically. However, the second problem is that if the monomials of degree $d$ are $p^k$-symmetric then it turns out (an example can be given) that it is not possible to achieve $p^k$-symmetry for monomials of smaller degree. This is resolved by starting with $p^r$-symmetry for $r < k$ (a stricter notion) for the large degrees and then relaxing it as the smaller degrees are handled and being careful about the exact details of constructing the restriction.

Suppose that $|V| = N, \quad V^p = \{v_1, \ldots, v_m\}, \quad v_1 < \ldots < v_m$ for some restriction $\rho$ and that $\mathcal{P}$ has
been made $p'$-symmetric over $V$ with respect to monomials of degree greater than $d'$. To argue that the contribution to monomials of degree $d'$ from monomials in $P$ of larger degree is $p'$-symmetric over $V'$ for some $s > r$, we argue that for any $p'$-type $T'$ over $V'$ of degree $d'$, the contribution (modulo $p$) to the coefficient of any $(v, \Xi_1)$ of $p'$-type $T'$ over $V'$ from the restriction of monomials of $p'$-type $T$ over $V$ of degree $d'$ over $V$ we need only count the number of $(v, \Xi_1 \in \Xi_2)$ of $p'$-type $T'$ over $V'$ that contribute to the coefficient of a given $(v, \Xi_1)$ of $p'$-type $T'$ over $V'$. By the $p'$-symmetry of the larger degree terms over $V$ we argue that for any $p'$-type $T$ over $V$ that contribute to the coefficient of a given $(v, \Xi_1)$ of $p'$-type $T'$ over $V'$.

We note that for a given $(v, \Xi_1)$, the number of $\Xi_2$ such that $\Xi_2' = 1$ and $(v, \Xi_1 \Xi_2)$ is of a given $p'$-symmetry of degree $d'$ over $V$ is affected by the relative order of $(v) \cup \text{supp}(\Xi_1)$ among the elements of the $q$-sets in $\rho$. Thus, after we choose the set $V'$ using Ramsey's theorem, we have to be careful, when we choose $\rho$ such that $V' = V^\rho$, to consider how the $q$-element sets in $\rho$ cover the nodes in $V \setminus V'$ that are between elements of $V'$; we say any such $q$-element set interleave the set $V'$.

The next lemma whose proof is in the full paper formalizes the base case of the proof of Lemma 4.1.

Lemma 4.5 For every $m, d', k' > 0$ there exists an $N_0$ such that for any $N \geq N_0$ with $N \equiv m \pmod{q}$ and every $P$ over any $V$, $|V| = N$, there exists a restriction $\rho$ such that

1. the monomials of degree $d'$ in $P$ in variables over the set $V^\rho$ form a symmetric system;
2. $|V^\rho| = m$;
3. for every $u, v' \in V^\rho$, $v \equiv v' \pmod{k'}$;
4. if we let $U = \{u_1, \ldots, u_z\} \subseteq V \setminus V^\rho$ be the set of elements that are between elements of $V^\rho$ then $\rho$ contains the sets $\{u_i, u_i^{(1)}, \ldots, u_i^{(q-1)}\}$ for $i = 1, \ldots, z$ where we take disjoint sets $\{u_i^{(1)}, \ldots, u_i^{(q-1)}\}$ consecutively, either starting from the largest element of $V^\rho$ and working upwards, or starting from the smallest element of $V^\rho$ working downwards.

Lemma 4.6 For every $m > 0$ and $d' < d$, there exists $N_0$ such that for every $N \geq N_0$ with $N \equiv m \pmod{q}$ and every $P$ of degree $d$ over $V$, $|V| = N$, if the monomials of $P$ of degrees $d'+1, \ldots, d$ form a $k'$-symmetric system of polynomials, then there is a restriction $\rho$ such that $|V^\rho| = m$ and the monomials of degree $d', d'+1, \ldots, d$ of $P^\rho$ form a $kp'$-symmetric system over $V^\rho$.

To prove this we need:

**Lemma 4.7** Let $0 \leq i_1, \ldots, i_l < k$ be fixed and consider all $n \geq 0$. Let $C$ be the number of possible choices of $(b_1, \ldots, b_l)$ with $0 \leq b_1 < \ldots < b_l < n$ satisfying the condition

$$b_1 \equiv i_1 \pmod{k}$$

$$\vdots$$

$$b_l \equiv i_l \pmod{k}.$$

Then the residue class modulo $p$ of $C$ is determined by $n \pmod{kp}$.

**Proof of Lemma 4.6.** By Lemma 4.5 there is an $N_0$ such that for any $V$, $|V| \geq N_0$ and $|V| = N \equiv m \pmod{q}$, and every $P$ over $V$, there is a restriction $\rho$ satisfying conclusions 1-4 of Lemma 4.5 with $k' = kp$. Choose this $N_0$ and $\rho$. By conclusion 1 of Lemma 4.5, the monomials of degree $d'$ in $P$ over $V^\rho$ appear symmetrically. Thus, since the monomials of degree $d$ in $P'$ over $V'$ appear symmetrically, it is sufficient to show that if $P'$ is any $k'$-symmetric system of monomials of degree at most $d$ over $V$ then $P^\rho$ is $kp'$-symmetric over $V^\rho$.

Let $V' = V^\rho = \{v_1, \ldots, v_m\}$ and write $\rho = \rho_1 \rho_2$ where $\rho_1$ is the portion of $\rho$ that interleaves $V'$. Consider first $P^\rho$ over $V^\rho$. Note that $V^\rho$ is a consecutive sequence of elements of $V$. Thus, for any two $(v, \Xi_1)$ and $(v', \Xi_1)$ of $k$-type $T$ over $V^\rho$, if $(v, \Xi_1 \Xi_2)$ is of $k'$-type $T'$ over $V$ of degree $d'$ then so is $(v', \Xi_1 \Xi_2)$. Thus $P^\rho$ is $k'$-symmetric over $V^\rho$.

It remains to see what happens with monomials after applying $\rho_1$. Since $P^\rho$ is $k'$-symmetric over $V^\rho$ and the elements of $V^\rho$ are consecutive we can ignore the difference between $P^\rho$ and $P'$ and between $V^\rho$ and $V$. Thus we want to show for an arbitrary $k$-symmetric system $P'$ over $V$ of degree at most $d$ such that $V^\rho = V'$, $P^\rho$ is $kp'$-symmetric over $V'$.

Claim. Suppose that $T$ is a $k$-type of degree at most $d$ over $V$ and $T'$ is a $kp'$-type over $V'$ of degree $c < d$. For any $(v, \Xi_1)$ of $kp'$-type $T'$ over $V'$, the number (modulo $p$) of $\Xi_2$ such that $(v, \Xi_1 \Xi_2)$ has $k$-type $T$ over $V$ and $\Xi_2_1 = 1$ is the same.

Let $\{v\} \cup \text{supp}(\Xi_1) = \{u_1, \ldots, u_{n'}\}$ in increasing order ($c$ is the degree of $\Xi_1$). Consider possible monomials $\Xi_2$ of degree $b$ such that $b + c < d$ and $\Xi_2_1 = 1$. Each $q$-set fixed by $\rho_1$ is determined by a single representative $u \in [v_1, v_{n'}] \setminus V'$. Thus consider the representatives $u_{j_1}, \ldots, u_{j_l}$ in $[v_1, v_{n'}] \setminus V'$ which determine the monomial $\Xi_2$. Since $\Xi_1$ is fixed, by construction of $\rho_1$, the $k$-type of $(v, \Xi_1 \Xi_2)$ over $V$ depends only on two properties:
(A) the position of \(u_{j_1}, \ldots, u_{j_t}\) w.r.t. \(u_0, u_1, \ldots, u_n\) (which fixes the type of \((v, \Xi, \Xi_2)\) since the order of the least elements in the q-sets containing the \(u_{j_i}\) is either always the order of the \(u_{j_i}\) or always the reverse);

(B) the residue classes of \(\{u_{j_1}, u_{j_1}^{(1)}, u_{j_1}^{(2)}, \ldots, u_{j_1}^{(q-1)}\}, \ldots, \{u_{j_t}, u_{j_t}^{(1)}, u_{j_t}^{(2)}, \ldots, u_{j_t}^{(q-1)}\}\) modulo \(k\).

The key observation for (B) is that the residue classes of \(\{u_{j_1}, u_{j_1}^{(1)}, u_{j_1}^{(2)}, \ldots, u_{j_1}^{(q-1)}\}\) are precisely determined by the residue class modulo \(k\) of \(u_{j_1}\) and the residue class modulo \(k\) of the number of vertices in \(V'\) less than \(u_{j_1}\). This is because the residue classes of \(\{u_{j_1}, u_{j_1}^{(1)}, u_{j_1}^{(2)}, \ldots, u_{j_1}^{(q-1)}\}\) are determined just by \(j_1\) modulo \(k\) and the difference between the residue classes of \(u_{j_1}\) and \(j_1\) depends on the number of vertices in \(V'\) less than \(u_{j_1}\). (The difference is either positive or negative depending upon whether \(\rho_1\) matches the elements \([u_1, v_m] \setminus V'\) above or below \([u_1, v_m]\).)

Since we only consider \(\Xi_2\) such that \((v, \Xi_2, \Xi_3)\) has some fixed \(k\)-type \(T\) over \(V_1\) for each \(\alpha, 0 \leq \alpha \leq q\), we have fixed the indices \(\beta, \ldots, \gamma\) such that \(\alpha_0 < \alpha_2 < \ldots < \alpha_j < \nu_{s+1}\), where \(\beta, \gamma\) depend only on \(\alpha\). We shall handle each such interval \(\alpha_0 < \nu_{s+1}\) separately and show that (modulo \(p\)) the number of choices of \(u_{j_1}, \ldots, u_{j_t}\) between \(u_0\) and \(u_{\alpha_1}\) such that \(\{u_{j_1}, u_{j_1}^{(1)}, u_{j_1}^{(2)}, \ldots, u_{j_1}^{(q-1)}\}\) and \(\{u_{j_2}, u_{j_2}^{(1)}, u_{j_2}^{(2)}, \ldots, u_{j_2}^{(q-1)}\}\) belong to particular residue classes modulo \(k\) depends only on the residue classes of \(\nu_{s}\) and \(\nu_{s+1}\) modulo \(kp^d\). This will be sufficient since the total number of choices of \(\Xi_2\) is the product of the number of choices in each of these intervals and the \(kp^d\)-type \((v, \Xi_1)\) over \(V^p\) determines these residue classes.

By the key observation, the only further condition that the \(k\)-type \(T\) places on \(u_{j_1}, \ldots, u_{j_t}\) is given by a sequence of pairs \((k_0, k_0'), \ldots, (k_t, k_t')\) such that, for \(0 \leq \gamma \leq \gamma, 0 \leq \gamma \leq k, k_0' < k\)

\[u_{j_1} \equiv k_1 (mod \ k); \quad \text{and} \quad \ell_t \equiv k_t' (mod \ k),\]

where \(\ell_t\) is the index such that \(u_{\ell_t} < u_{j_t} < u_{\ell_t+1}\).

We would like to apply Lemma 4.7 to the equations for \(u_{j_t}\) and \(\ell_t\) above and argue that the number of solutions only depends on \(\nu_{s}\) and \(\nu_{s+1}\) modulo \(kp^d\).

We cannot do so immediately since it is possible, if \(k_t' = k_t'-1\), that \(\ell_t = \ell_t+1\) and Lemma 4.7 does not apply in this case. Instead we break up the cases into the possible partitions \(\pi\) of the interval \([\beta, \gamma]\) into intervals \([\mu_1, \nu_1], \ldots, [\mu_t, \nu_t]\) so that for \(t, t'\) in the same interval \(\ell_t = \ell_{t'}\) and for \(t, t'\) in different intervals \(\ell_t \neq \ell_{t'}\). It is now sufficient to argue two things for each fixed partition \(\pi\):

- The number of choices (modulo \(p\)) of the sequence \(u_{j_t}\) consistent with the \(k\)-type \(T\) and the partition \(\pi\) depends only on \(\nu_{s}\) and \(\nu_{s+1}\) modulo \(kp^d\).
- The number of choices (modulo \(p\)) of \(u_{j_t}, \ldots, u_{j_{t'}}, \ldots, u_{j_t}\) consistent with \(k\)-type \(T\) and a fixed sequence of \(\ell_t\) that is consistent with \(T\), is independent of the choice of \((v, \Xi_1)\).

Given the fixed partition \(\pi\), the sequence of \(\ell_t\) for \(t \in [\beta, \gamma]\) is precisely determined by \(\ell_{\mu_1}, \ldots, \ell_{\mu_t}\) where \(i_0 < \ell_{\mu_1} < \ldots < \ell_{\mu_t} = i_{\mu_{t+1}}\) and \(\nu_{\mu_t} \equiv k_1 (mod k)\) for \(i = 1, \ldots, \xi\). By Lemma 4.7 the number of such solutions depends only on \(\nu_{s+1} - \nu_{s}\) modulo \(kp^d\) which is determined by \(\nu_{s+1} - \nu_{s}\) modulo \(kp^d\) since \(\ell_t \leq d\).

Now consider the fixed sequence \(\ell_t\) and its associated partition \(\pi\). For each interval \([\mu_t, \nu_t]\) in \(\pi\) we count the number of choices of \(u_{j_t}, \ldots, u_{j_{t'}}\), consistent with the \(k\)-type \(T\). The solutions \(u_{j_t}, \ldots, u_{j_{t'}}\) precisely satisfy \(u_{t}, u_{t'} \in \{v_{i_{t}}, \ldots, v_{s+1}\}\) and \(u_{t+1} \equiv k_t (mod k)\) for \(t \in [\beta, \gamma]\). By Lemma 4.7 the number of such choices modulo \(p\) depends only \(u_{\nu_{s+1}} - (u_{\nu_{s+1}} + 1)\) modulo \(kp^d\). Since all elements of \(V^p\) are equivalent modulo \(kp^d\) and \(d \geq s > 1\), \(\nu_{s+1} - (\nu_{s+1} + 1)\) is always congruent to \(-1\) modulo \(kp^d\) and thus the number of choices modulo \(p\) in each interval of \(\pi\) is independent of the choice of \((v, \Xi_1)\).

Therefore the number of choices modulo \(p\) of \(u_{j_t}, \ldots, u_{j_{t'}}\), consistent with the sequence of \(\ell_t\) and the \(k\)-type \(T\) is independent of \((v, \Xi_1)\) as required.

Thus we have proved the claim and hence the system \(P^p\) is \(kp^d\)-symmetric, which finishes the proof of Lemma 4.6.

\[\boxtimes\]

**Proof of Lemma 4.1.** Let \(m \geq p^{d^2+1} q\) and \((p^{d^2+1}, q), \mod \ m\). Choose \(V_1, |V_1| = N \equiv m (\mod q)\), large enough to apply Lemma 4.6 for \(d' = d, d - 1, \ldots, 1\), in order, to a system \(\mathcal{P} = \{P_0, \ldots, P_{d-1}\}\) of degree \(d\) and still have the combined restriction constructed have \(|V^p| = m\). Choose any system \(\mathcal{P}\) and note that Lemma 4.6 implies that there is a restriction \(\rho\) with \(|V^p| = m \quad \text{and} \quad \mathcal{P}^\rho\) is \(pd\)-symmetric over \(V^p\). By Lemma 4.4 there is an assignment \(a\) on which \(\mathcal{P}^\rho\) vanishes. Combining \(\rho\) with \(a\), we get an assignment on which \(\mathcal{P}\) vanishes. Finally, recall that all \(Q_{(t')\}^\rho's\) vanish too, due to the fact that \(\rho\) and \(a\) are partial partitions. 

805
5 Remarks

We have introduced a natural approach to proving lower bounds for propositional proof systems that is based on studying the complexity of the Nullstellensatz polynomials witnessing the unsolvability of a system of equations.

One important open question is whether or not our main theorem can be improved. We conjecture that the degree lower bound is nearly linear, although the techniques of this paper only succeed in proving a non-constant lower bound. Note that an exponential lower bound on the size of constant-depth Frege proofs of $Count^N$ from $Count_p$ instances would follow from an improvement of the degree lower bound to $n^e$ for some $e > 0$.

We note that, at the same time as Ajtai's proof of the separation of the counting principles appeared [3], Riis [20] also announced a more detailed separation but its proof was incomplete. More recently [21], he has developed another proof of the separation using a Ramsey theory argument but not the Nullstellensatz polynomials that we use here.

Finally, Edmonds, Impagliazzo, and Pitassi [11] have recently shown a lower bound of $\Omega(n^{1/4})$ on the degree of the witnessing polynomials for a different unsolvable system of polynomial equations.

References


