Linear Gaps Between Degrees for the Polynomial Calculus Modulo Distinct Primes

Sam Buss[1,2]
Department of Mathematics
Univ. of Calif., San Diego
La Jolla, CA 92093-0112
sbuss@ucsd.edu

Dima Grigoriev
Computer Science and Engineering
Pennsylvania State University
University Park, PA 16802-6106
dima@cse.psu.edu

Russell Impagliazzo[1,3]
Computer Science and Engineering
Univ. of Calif., San Diego
La Jolla, CA 92093-0114
russell@cs.ucsd.edu

Toniann Pitassi[1,4]
Computer Science
University of Arizona
Tucson, AZ 85721-0077
toni@cs.arizona.edu

Abstract

This paper gives nearly optimal lower bounds on the minimum degree of polynomial calculus refutations of Tseitin's graph tautologies and the mod p counting principles, $p \geq 2$. The lower bounds apply to the polynomial calculus over fields or rings. These are the first linear lower bounds for polynomial calculus; moreover, they distinguish linearly between proofs over fields of characteristic q and r, $q \neq r$, and more generally distinguish linearly the rings Z_q and Z_r where q and r do not have the identical prime factors.

1 Introduction

The problem of recognizing when a proposition formula is a tautology is dual to the satisfiability problem and is therefore central to computer science. A principal method of establishing that a formula is a tautology is to find a proof of it in a formal system such as resolution or (extended) Frege systems. In fact, many algorithms for establishing propositional validity are essentially a search for a proof in a particular formal system. In recent years, several algebraic proof systems, including the Nullstellensatz system and the polynomial calculus (also called the 'Gröbner' system) have been proposed: these systems are motivated in part by the desire to identify powerful proof systems which support efficient search algorithms and in part by the desire to extend lower bounds on proposition proof complexity to stronger proof systems.

The Nullstellensatz proof system is a propositional proof system based on Hilbert's Nullstellensatz and was introduced in [1]. The polynomial calculus (PC) is a stronger propositional proof system introduced first by [4]. (See [8] and [3] for subsequent, more general treatments of algebraic proof systems.) In the polynomial calculus, one begins with an initial set of polynomials and the goal is to prove that they cannot be simultaneously equal to zero over a field F. A polynomial calculus (PC) derivation of P_l from a set of polynomials Q is a sequence of polynomials $P_1, \ldots, P_l$ such that each polynomial is either an initial polynomial from Q, or follows from one of the following two rules: (i) If P_i and P_j are previous polynomials, then $cP_i + dP_j$ can be derived, where $c, d \in F$; (ii) if P_i is a previous polynomial, then xP_i can be derived. The *degree* of a PC derivation is the maximum degree of the P_i's. We identify polynomials P_i with the equations $P_i = 0$ and a PC refutation of Q (a proof that the equations $Q = 0$ are not solvable over F) is simply a PC derivation of 1 (i.e., of $1 = 0$).

The definition of the polynomial calculus depends implicitly on the choice of a field F such that all polynomials are over the field F. A number of authors also consider the polynomial calculus over rings ([3, 2]). The only difference in the definition of the PC system is that a PC refutation over a ring is a derivation of r (i.e., of $r = 0$) for some non-zero r in the ring. Our main results apply to both fields and rings.

The mod p counting principle can be formulated as a set MOD_p^n of constant-degree polynomials expressing the negation of the counting principle, and the present paper gives linear lower bounds on the degree of polynomial calculus refutations of MOD_p^n over fields of characteristic $q \neq p$. A couple lower bounds on the

[1]Supported in part by international grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic)
[2]Supported in part by NSF grant DMS-9803515
[3]Supported in part by NSF grant CCR-9734911, Sloan Research Fellowship BR-3311, and US-Israel BSF grant 97-00188.
[4]Supported in part by NSF grant CCR-9457783 and US-Israel BSF grant 95-00238.

degree of Nullstellensatz proofs of the mod p counting principles have been given in prior work: [1] gave non-constant lower bounds and [3] gave lower bounds of the form n^{ϵ}. For the polynomial calculus, the best lower bound on the degree of PC refutations of MOD_p^n was Krajíček's $\Omega(\log\log n)$ lower bound based on a general lower bound for symmetrically specified polynomials [7].

A couple polynomial calculus lower bounds have been obtained for other families of tautologies. Razborov [9] established $\sqrt{n}$ lower bounds on the degree of polynomial calculus proofs of the pigeon-hole principle. Krajíček [7] proves $\log\log n$ lower bounds for a wide variety of symmetric tautologies.

Recently, Grigoriev [5] succeeded in giving very simple linear lower bounds on the degree of Nullstellensatz refutations of the Tseitin mod 2 graph tautologies. The present work is motivated by this paper, and in particular by the idea of working in the Fourier basis which greatly simplifies the argument.

The present paper establishes linear lower bounds to the polynomial calculus by proving that over a field of characteristic $q \nmid p$, any PC refutation of the MOD_p^n polynomials requires degree $\delta \cdot n$, for a constant δ which depends on p and q. In section 8 we generalize this linear lower bound to the polynomial calculus over rings Z_q provided p and q are relatively prime.

As it is well-known to be easy to give constant degree polynomial calculus (and even Nullstellensatz) refutations of the MOD_p^n polynomials over F_p, our results imply that the MOD_p^n polynomials have a linear gap between proof complexity for the polynomial calculus over F_p and over F_q.

It follows from a result of Krajíček [6] that our linear lower bounds on the degree of PC refutations imply exponential lower bounds of $AC^0[q]$-Frege proofs of the mod p principles when Mod-q gates are present only at the top (root) of formulas.

2 Tseitin tautologies: polynomial version

Tseitin's (mod 2) graph tautologies are based on the following idea. Let G_n be a connected undirected graph on n vertices, where each node in the graph has an associated charge of either 0 or 1, and where the total sum of the charges is odd. Then it is impossible to choose a subset of the edges E' from E so that for every vertex $v \in V$, the number of E'-edges incident to v is equal mod 2 to the charge of v. This impossibility follows from a simple parity argument, since summing the degrees of all vertices in the subgraph counts each edge twice, and so is even, whereas it should also be the sum of all the charges, which is odd.

For an r-regular graph G_n with n odd, and charges all 1, we can express this principle as the inconsistency of the following system of polynomials over a finite field F of characteristic different from 2: There will be $rn/2$ underlying variables, one for each edge of G_n. We will denote the variable corresponding to the edge $e = \{i, j\}$ from i to j by $y_e = y_{\{i,j\}}$. For each variable y_e, we have the equation $y_e^2 - 1 = 0$; this forces the variables to take on values of either 1 or -1, with $y_e = -1$ corresponding to the presence of e in the subgraph E'. Secondly, corresponding to each vertex i in G_n, we will have the equation $1 + y_{\{i,j1\}} y_{\{i,j2\}} \cdots y_{\{i,jr\}} = 0$, where $j1, \ldots, jr$ are the neighbors of i in G_n. This corresponds to saying that the degree of i in the subgraph E' is odd. This set of equations, representing the Tseitin mod 2 graph formula, will be denoted by $TS_n(2)$.

For any prime p, we can generalize the above principle to obtain a mod p version as follows. Again, we fix an underlying r-regular, undirected graph G_n, and then let G'_n be the corresponding directed graph where each undirected edge is replaced by two directed edges. Each vertex in G'_n will have an associated label, or charge in $[0, p-1]$ such that the sum of the vertex charges is congruent to 1 mod p. The mod p principle states that it is impossible to assign values in $[0, p-1]$ to each of the directed edges so that: (i) for any pair of complementary edges $\langle i, j\rangle$ and $\langle j, i\rangle$, $v(\langle i, j\rangle) + v(\langle j, i\rangle) \equiv 0 \pmod p$, and (ii) for every vertex i, the sum of the edge values coming out of vertex i is congruent to the charge of that vertex mod p. Again, this is impossible since if we sum the edges in pairs, we obtain 0 mod p, but summing them by vertices gives the total charge of 1 mod p.

Let F be a finite field with characteristic $q \neq p$ that contains a primitive p-th root of unity ω. Assume all charges of vertices are 1, and that $n \equiv 1 \pmod p$. We can express the mod p Tseitin principle for G'_n as the unsatisfiability of the following system of polynomials over F: We have rn underlying variables y_e, one for every directed edge e. For each variable y_e we have the equation $y_e^p - 1 = 0$; this forces variables to take on values in $1, \omega, \omega^2, \ldots, \omega^{p-1}$. (The power of ω corresponds to the value assigned to e.) Secondly, for each vertex i in G'_n, we will have the equation $y_{\langle i,j1\rangle} y_{\langle i,j2\rangle}, \ldots, y_{\langle i,jr\rangle} - \omega = 0$, where $j1, \ldots, jr$ are the neighbors of i. Third, for each edge $e = \langle i, j\rangle$ we have the equation $y_{\langle i,j\rangle} y_{\langle j,i\rangle} - 1 = 0$. This set of equations, representing the Tseitin mod p formula, will be denoted by $TS_n(p)$.

3 The mod p principle and low degree reductions

A related principle is the mod p counting principle. Intuitively, it states that it is not possible to partition a set of size n into groups of size p, if n is congruent to 1 mod p. We will express this by polynomial equations as follows. The underlying variables are x_e, where e ranges over all p element subsets of $[1, n]$. The degree 2

equations expressing the negation of the principle are: (1) $x_e^2 - x_e = 0$ for each e; (2) $x_e x_f = 0$, for each e, f such that $e \cap f \neq \emptyset$ and $e \neq f$; (3) $1 - \sum_{e, i \in e} x_e = 0$, for each $i \in [1, n]$. Let the above set of equations be denoted by MOD_p^n.

We want to show that a low degree PC refutation of the mod p counting principle implies a low degree PC refutation of the Tseitin mod p graph equations. To do this, we define the following general notion of a low degree reduction.

Definition. *Let $P(\overline{x})$, $Q(\overline{y})$ be two sets of polynomials over a field F. Then P is (d_1, d_2)-reducible to Q if: (1) For every y_i, there is a degree d_1 definition of y_i in terms of the x's. That is, for every i, there exists a degree d_1 polynomial r_i where y_i will be viewed as being defined by $r_i(x_1, \ldots, x_n)$; (2) there exists a degree d_2 PC derivation of the polynomials $Q(\overline{r}(x_1, \ldots, x_n))$ from the polynomials $P(\overline{x})$.*

Lemma 1 *Suppose that $P(x)$ is (d_1, d_2)-reducible to $Q(y)$. Then if there is a degree d_3 PC refutation of $Q(y)$, then there is a degree $max(d_2, d_3 d_1)$ PC refutation of $P(x)$.*

Lemma 2 *For all n and p, and for any field F of characteristic q, where $q \nmid p$, and F includes the primitive p-th root of unity, $TS_n(p)$ is (d_1, d_2)-reducible to MOD_p^m over F, where $m = n + nrp$, $d_1 = 2pr$ and $d_2 = 2pr$.*

Proof of Lemma 2. Let G'_n be a directed Tseitin graph on n vertices, where $n \equiv 1 \pmod p$. That is, the underlying G'_n is an r-regular graph; each vertex of G'_n has a charge of 1, and the edges of G'_n are labeled with values from $[0, p-1]$. Thus, the total number of directed edges of G'_n is rn. From G we will define a universe U of size m, and a corresponding p-partition of this universe, where $m = n + nrp$. In U, there will be one element corresponding to each vertex of G'_n, and there will also be p elements corresponding to each directed edge of G'_n. We will denote the element of U corresponding to vertex i in G'_n by (i), and the vector of p elements of U corresponding to the edge $\langle i, j \rangle$ in G'_n will be denoted by $(i, j, *) = \langle (i, j, 1), (i, j, 2), \ldots, (i, j, p) \rangle$.

Definition. *The elements in U associated with node i will be (i), plus all elements $(i, k, *)$. (That is, the rp elements corresponding to outgoing edges from i plus the element corresponding to node i.) The elements in U associated with the pair of nodes i, j will be the rp elements corresponding to the directed edge $\langle i, j \rangle$ plus the rp elements corresponding to the directed edge $\langle j, i \rangle$.*

The partition of U is defined as follows. We will consider node i in G'_n, and the r labeled edges, $(i, j_1), (i, j_2), \ldots, (i, j_r)$, leading out of i, where $j_1 < j_2 < \cdots < j_r$. Suppose that the values of these edges are: $a_1, a_2, \ldots, a_r$. Then for each ℓ, $1 \leq \ell \leq r$, we take the first a_ℓ elements in U from $(i, j_\ell, *)$, and group them with the first $(p - a_\ell)$ elements in U from $(j_\ell, i, *)$. (This gives us r p-partitions so far.) Note that the number of remaining, ungrouped elements associated with node i is $(p-a_1)+(p-a_2)+\cdots+(p-a_r)+1$, which is congruent to 0 mod p as long as $(a_1 + \cdots + a_r) \bmod p = 1$.

We then group these remaining, ungrouped elements associated with i, p at a time, in accordance with the following ordering. Ungrouped elements from $(i, j_1, *)$ are first, followed by ungrouped elements from $(i, j_2, *)$, and so on until we get to the ungrouped elements from $(i, j_r, *)$, and lastly the element (i).

It should be intuitively clear that if the values $y_{i,j}$ satisfy $TS_n(p)$, that is, if they are set so that the mod p sum coming out of each vertex in G'_n is congruent to 1 mod p, and $y_{i,j} y_{j,i} = 1$ and $y_{i,j}^p = 1$, then the corresponding partition of U is a proper p partition. We want to prove this now formally, with small-degree PC refutations. There are two steps to this reduction. First, for each variable x_e underlying MOD_p^m, we want to define a degree at most rp polynomial, call it $r_e(\overline{y})$, in the $y_{i,j}$ variables that corresponds to the above reduction. Secondly, we want to show that there is a small degree PC derivation of $MOD_p^m(\overline{r}_e)$ from $TS_n(p)$.

Step 1: Defining r_e. We will first describe the defining polynomial r_e for x_e. Recall that e is a particular p-set from U. In the above reduction, the valid p-partitions are of two types: (i) where the elements of e are a subset of the elements associated with a pair of nodes i, j in G'_n; (ii) where the elements of e are a subset of the elements associated with a node i. Thus, if the underlying p elements from e are not one of these two types, then x_e is just set to 0.

Now consider case (i); that is, the elements of e are a subset of the elements associated with the pair of nodes i, j. Suppose that e is the set $\{(i, j, 1), (i, j, 2), \ldots, (i, j, a_1), (j, i, 1), \ldots, (j, i, p - a_1)\}$. That is, e consists of an initial segment of size a_1 of the p elements associated with directed edge $\langle i, j \rangle$ and an initial segment of size $p - a_1$ of the p elements associated with $\langle j, i \rangle$. (If e is not of this form, then again x_e is just 0.) Then x_e should be 1 if $y_{i,j} = \omega^{a_1}$, $y_{j,i} = \omega^{p-a_1}$ and should be 0 otherwise. This is defined by the following polynomial:

$$\prod_{a \neq a_1} (\omega^{a_1} - \omega^a)^{-1} (y_{i,j} - \omega^a) \times \prod_{b \neq p - a_1} (\omega^{p-a_1} - \omega^b)^{-1} (y_{j,i} - \omega^b) \tag{1}$$

More generally, suppose that we want to define a 0-1 valued variable x so that $x = 1$ if $y_1 = \omega^{p_1}$ and $y_2 = \omega^{p_2}$ and ... and $y_k = \omega^{p_k}$, and otherwise $x = 0$. Then this is accomplished by the following degree kp polynomial:

$$\prod_i \prod_{p \neq p_i} (\omega^{p_i} - \omega^p)^{-1} (y_i - \omega^p) \tag{2}$$

Case (ii) is handled similarly but is somewhat more complicated. Now the elements of e are a subset of elements associated with i, and moreover we can assume without loss of generality that they must be end-segments of $(i, j_{l1}, *), (i, j_{l2}, *), \ldots, (i, j_{ll}, *)$ plus possibly either (i) or a consecutive segment of $(i, j_{ll+1}, *)$. (Otherwise, x_e is just set to zero.) Then x_e should be 1 if and only if there exists values $a_1, \ldots, a_r$ assigned to the outgoing edges $(i, j_1), \ldots, (i, j_r)$ such that the partition described in the reduction above groups the elements of e together. This is a big OR (translated as a sum) (of size at most p^r) over the good values of $a_1, \ldots, a_r$ that group e together. Thus, it is expressible by a polynomial in the variables $y_{i,j_1}, y_{i,j_2}, \ldots, y_{i,j_r}$ of degree at most pr.

Step 2: Deriving $MOD_p^m(r_e)$ from $TS_n(p)$. We will now describe how to give small degree PC derivations of the equations $MOD_p^m(r_e)$ from $TS_n(p)$. Recall that the equations in $MOD_p^m(r_e)$ are as follows.

1. $r_e^2 - r_e = 0$ for all p-sets e
2. $r_e r_f = 0$ for all e, f such that $e \cap f \neq 0$, $e \neq f$
3. $\sum_{e, u \in e} r_e - 1 = 0$, for all $u \in [m]$.

We want to show that for every equation E that we need to derive as described above, that E is a tautological consequence of a small, constant number of equations from $TS_n(p)$. Then, since each equation of $TS_n(p)$ involves only a constant number of variables, by completeness of PC it will follow that there is a small-degree derivation of each equation E.

Definition. *Let $f_1 = 0, \ldots, f_k = 0, g = 0$ be polynomial equations over a field F with underlying variables $x_1, \ldots, x_n$. Then g is a tautological consequence of $f_1, \ldots, f_k$ if for every assignment α to the underlying variables, if all of the equations $f_1, \ldots, f_k$ are satisfied by α, then $g = 0$ is also satisfied by α.*

By generalizing slightly the completeness result in [3], (Theorem 5.2 part 2), it can be shown that if g is a tautological consequence of $f_1, \ldots, f_k$, all with underlying variables $x_1, \ldots, x_n$, and if $f_1, \ldots, f_k$ includes the equations $x_i^p = 1$ for all variables x, then there is a degree pn derivation of g from $f_1, \ldots, f_k$.

In light of the above, it is just a matter of verifying that each of the above equations E is a tautological consequence of a small number of equations from $TS_n(p)$ involving a small number of variables. In particular, equations of type (1) require degree pr and equations of type (2) and (3) each require degree at most $2pr$.

This completes the proof of Lemma 2. □.

4 Intuition and an upper bound

In order to first give some intuition behind the lower bound for the Tseitin tautologies, it is helpful to think about the natural PC refutation for these equations. To be concrete, we consider the mod 2 case; the others are similar.

Initially, the equations say that the number of edges out of a single vertex v is odd. These equations have degree r. Then in degree at most $2r$, one can combine two of these equations to say that the number of edges out of a set of vertices of size 2 is even. Continuing in this way, if $S \subset V$, then one can derive an equation saying that the number of edges out of S, $E(S)$, has the same parity as the size of S. This equation is most naturally expressed as $m - 1 = 0$ if $|S|$ is even, and $m + 1 = 0$ if $|S|$ is odd, where m is the product of the variables corresponding to edges $E(S)$, that cross between S and its complement. Thus, the degree of this polynomial is equal to the size of $E(S)$. Proceeding this way, we eventually obtain two equations, one saying that the number of edges out of a set S_1 is odd, and the other one saying that the number of edges out of a set S_2 is even, where S_1 and S_2 are disjoint, and $S_1 \cup S_2 = V$. This will lead to a derivation of 1, since we have now derived $m + 1$ and $m - 1$ for some monomial m. If G_n is highly expanding, the degree of this refutation will be large since at some point we must pass through a relatively large set, and thus the polynomial expressing that the number of edges out of this set must have the same parity as the size of the set, will be large due to expansion.

We want to show that the above almost completely characterizes what can be done with the initial equations. Suppose we have derived $m - 1 = 0$, where m is the set of edges $E(S)$, such that $|E(S)| = d$, and $|S|$ is even. (Or similarly, we have derived $m + 1 = 0$ when m is the set of edges of $E(S)$ but now $|S|$ is odd.) However, now it is possible to rewrite this equation in a slightly different form so that it has smaller degree. In particular, we can divide up the edges of m into two halves, m_1 and m_2 and rewrite the equation $m - 1 = 0$ instead as $m_1 - m_2 = 0$. This is derived from $m - 1$ in degree d by multiplying $m - 1$ by edges of m_2, one at a time, thus transferring the edges of m_2 over to the second term, one at a time. This new equation, $m_1 - m_2 = 0$ has degree $d' = \lceil d/2 \rceil$, and in general is not derivable by a degree d' PC refutation. The (degree d) equations that interest us are this larger set of equations, which express the fact that the edges coming out of a set S are even (or odd) by a pair of monomials.

There are two key steps to making this intuition a proof. First, we must show that, although the PC proof can contain arbitrary polynomials, the important lines are equalities as above, or *binomials* if viewed as a difference. This is made formal in a very general way in section 5. Secondly, that the set of degree d equations described above, although not all provable

with degree d proofs, is more natural and thus easier to understand, and they span all of the degree d derivable PC polynomials. In contrast, an explicit construction of the exact set of degree d derivable PC polynomials (as done by Razborov [9] for pigeonhole principle) seems much more difficult.

5 Binomial systems and bounds for PC

In the previous section, we reduced the problem of proving lower bounds for the mod counting principles to that of proving lower bounds for the Tseitin graph tautologies. The reason this is progress is that the Tseitin graph tautologies are expressed as a system of polynomials of a very simple form: each polynomial is a *binomial*, the difference of two *terms* (i.e., the weighted sum of two monomials with coefficients over the field.) (This fact was earlier used by Grigoriev [5] in giving lower bounds for Nullstellensatz.) A binomial $a_1 m_1 - a_2 m_2$ can be viewed as the equation between two terms, $a_1 m_1 = a_2 m_2$. Intuitively, an algebraic proof for a binomial system should be expressible as a sequence of such equations. In the final paper, we shall formalize this intuition by giving a formal definition of the *Laurent* proof system on such equations, and showing equivalence to PC for binomial systems. However, we will only present the consequences of this characterization that we need for the lower bound in this version.

We use a general characterization of things provable in PC, and then show that this characterization can be refined for binomial systems. This characterization is from [4].

Definition. *A degree d* pseudo-ideal *I is a vector space of degree at most d polynomials so that if $p \in I$ and p has degree $\leq d-1$, then $xp \in I$ for every variable x.*

Theorem 3 *[4] Let P be a system of polynomials, and let $I_d(P)$ be the set of all polynomials q that have a degree d PC proof from P. Then $I_d(P)$ is a d-pseudo-ideal, and for any d-pseudo-ideal I containing P, $I_d(P) \subseteq I$.*

So pseudo-ideals capture provability in polynomial calculus. If equational reasoning is complete for polynomial calculus for binomial systems, it should follow that the pseudo-ideals for such systems are determined by which terms are "provably equal" from the system. In other words, pseudo-ideals should be determined by an equivalence relation on degree d terms with certain closure properties. This is formalized below.

Definition. *Let R be a ring and R^* a multiplicative subgroup of R, and let $x_1, \ldots, x_n$ be variables. (i.e., R^* consists only of invertible elements and is closed under products and inverses). An R^*-term is a term whose coefficient is from R^*. An R^*-binomial is the difference of two R^*-terms. A* d-Laurent relation *over R^*-terms is an equivalence relation $\equiv_d$ on R^*-terms of degree at most d with the following properties: Let t_1, t_2, be R^*-terms of degree at most d and let $r \in R^*$.*

(a) *$t_1 \equiv_d t_2$ iff $rt_1 \equiv_d rt_2$; and*

(b) *If t_1 and t_2 are degree at most $d-1$, and $t_1 \equiv_d t_2$ then $x_i t_1 \equiv_d x_i t_2$ for any variable x_i.*

If $\equiv_d$ is a d-Laurent relation, we define a corresponding set of binomials $B_{\equiv_d} = \{t_1 - t_2 | t_1 \equiv_d t_2\}$ and a set of polynomials $S_{\equiv_d} = SPAN_R(B_{\equiv_d})$, the set of linear combinations of binomials in $B_{\equiv_d}$.

R will usually be a field, but in section 8 we will need the more general version. Intuitively, $\equiv_d$ represents the set of pairs of terms that can be proved equal using equational-type reasoning, where we are allowed to multiply both sides of a known equation by a constant or variable, as long as we don't exceed degree d.

We now show that lower bounds on polynomial calculus proofs can be established by exhibiting a non-trivial d-Laurent relation.

Theorem 4 *Let Q be a set of R^* binomials. If $\equiv_d$ is a d-Laurent relation with $Q \subseteq B_{\equiv_d}$ and $1 \not\equiv_d a$ for any $a \in R^*, a \neq 1$, then Q has no degree d polynomial calculus refutation over R.*

The proof of this theorem follows from a sequence of lemmas that take up the rest of this section. Lemma 5 is the main technical lemma, and the other lemmas describe how to use it to prove the theorem.

Lemma 5 *Assume $\equiv_d$ is d-Laurent. Suppose $f \in S_{\equiv_d}$. Then f can be rewritten as a linear combination $f = \sum_{j=1}^{T} a_j(t_j - t'_j)$ of binomials from $B_{\equiv_d}$ such that no monomial completely cancels out, i.e., every monomial t_j, t'_j in the linear combination appears in f with non-zero coefficient.*

Proof. Let $f = \sum_j a_j(t_j - t'_j)$, where each pair of monomials in the above sum is a polynomial from $B_{\equiv_d}$. We prove the lemma by induction on the number of distinct monomials in the above sum. At each step, if cancellation of a monomial occurs, we will rewrite f by an equivalent sum of elements of R_d such that the number of monomials in the new sum is strictly smaller.

Assume m appears in the sum, without loss of generality in exactly the first T' differences, but has zero coefficient in f. Because each element $a_j \in R^*$, and so has an inverse, by factoring out the coefficient of m in each term, we can rewrite any elements that m appears in: $c_k(a_k m - a'_k m'_k) = c_k a_k (m - a'_k a_k^{-1} m'_k) = d_k(m - t_k)$ for some R^* term t_k. Also, by the closure properties of $\equiv_d$ for multiplication by constants from R^*, $m \equiv_d t_k$. Now, since m has coefficient 0 in f, $\sum_k d_k = 0$.

We claim that the sum of binomials containing m, $\sum_{k=1}^{T'} d_k(m - t_k)$, can be rewritten as $\sum_{k=2}^{T'} d_k(t_1 - t_k)$. This is because $\sum_{k=2}^{T'} d_k(t_1 - t_k) = (\sum_{k=2}^{T'} d_k)(t_1) -$

$\sum_{k=2}^{T'} d_k t_k = -d_1(t_1) - \sum_{k=2}^{T'} d_k t_k = -\sum_{k=1}^{T'} d_k t_k = (\sum_{k=1}^{T'} d_k)m - \sum_{k=1}^{T'} d_k t_k = \sum_{k=1}^{T'} d_k(m - t_k)$.

Since $\equiv_d$ is transitive, $t_1 \equiv t_k$ for all k. So this substitution rewrites f as a weighted sum of members of $B_{\equiv_d}$. The new sum is without m and without any monomial not in the previous sum, so contains one fewer monomial. □

Lemma 6 *If $\equiv_d$ is d-Laurent, and there is a $c \in R, c \neq 0$ with $c \in S_{\equiv_d}$, then there is an $a \in R^*, a \neq 1$ with $1 \equiv_d a$.*

Proof. If $c \in S_{\equiv_d}$, by Lemma 5, c can be written as a sum of equivalent terms which only have monomials that appear in c, i.e, are constants. Thus, at least two distinct constants $a \equiv_d a'$, and then $1 \equiv_d a'a^{-1}$. □

Lemma 7 *If $\equiv_d$ is d-Laurent, then $S_{\equiv_d}$ is a degree d pseudo-ideal.*

Proof. By definition, $S_{\equiv_d}$ is a vector space of polynomials of degree at most d, so we just need to show closure under multiplication by a variable, provided the total degree is at most d. Assume $f \in S_{\equiv_d}$ has degree at most $d-1$. By Lemma 5, we can write $f = \sum_{i=1}^{T} c_i(t_i - t_i')$, where $t_i \equiv_d t_i'$ and each t_i, t_i' comes from a monomial with non-zero coefficient in f. In particular, each t_i, t_i' has degree at most $d-1$. Therefore, $xt_i \equiv xt_i'$ by the second closure property in the definition of d-Laurent relation. So $xf = \sum_{i=1}^{T} c_i(xt_i - xt_i') \in S_{\equiv_d}$. □

Proof (of Theorem 4). Let $\equiv_d$ be a d-Laurent relation with $Q \subseteq B_{\equiv_d}$, and that $1 \not\equiv_d a$ for any $1 \neq a \in R^*$. Assume Q has a polynomial calculus refutation of degree d over R, i.e., proves some $c \neq 0$, $c \in R$. Then $c \in S_{\equiv_d}$, since the latter is a pseudo-ideal containing Q. But then $1 \equiv_d a$ for some $a \neq 1, a \in R^*$. This contradiction proves the theorem. □.

6 PC lower bound for mod 2

We first prove linear lower bounds for the Tseitin principle $TS_n(2)$ for polynomial calculus over fields of characteristic $q > 2$, provided the underlying graph is an expander graph.

Definition. *Let $G = (V, E)$ be an undirected graph. G has* expansion ϵ *if for any subset S of vertices with $|S| \leq |V|/2$, $|N(S)| \geq (1+\epsilon)|S|$, where $N(S)$ is the set of nodes adjacent to nodes in S.*

Theorem 8 *Let F be a field and let G_n have expansion ϵ. For all $d < \epsilon n/8$, there is no degree d PC refutation of $TS_n(2)$ over F.*

Note that there is no restriction on the characteristic q of the field F. When q is an odd prime or zero, then the $TS_n(2)$ polynomials are unsatisfiable and therefore have a PC refutation over F, of degree which is necessarily linear by the theorem. When $q = 2$, then the $TS_n(2)$ polynomials are easily seen to be satisfiable (trivially, since $1 = -1$), and there is no PC-refutation of $TS_n(2)$ at all.

It is an easy corollary of Theorem 8 and Lemmas 1 and 2 that over a field of characteristic $q \neq 2$, PC-refutations of the MOD_2^n polynomials require size linear in n: this is established as Corollary 18 below for general p in place of 2.

Preparatory to proving Theorem 8, we establish some definitions and lemmas. In what follows, we will reduce all polynomials by $y_{i,j}^2 = 1$ for all variables, thus obtaining only multilinear polynomials.

Definition. *For a monomial $m = \prod_i y_i^{f_i}$, define the* multilinearization $\overline{m}$ *of m to be $\prod_i y_i^{f_i \bmod 2}$. For a multilinear monomial m we define E_m to be the set of edges e such that y_e is a factor of m.*

Definition. *For two sets A, B, $A +_2 B$ denotes the disjoint union of A and B.*

Definition. *Let $S \subseteq V$, where V is the set of vertices in G_n. Then $E(S)$ is defined to be the set of edges with exactly one endpoint in S and one endpoint outside of S.*

Proposition 9 *Let G_n be an expander graph with expansion ϵ. If $S \subseteq V$, $|S| \leq n/2$, then $|E(S)| \geq \epsilon|S|$.*

Proof Since $|S| \leq n/2$, $|N(S)| \geq (1+\epsilon)|S|$ by the definition of expansion. Then $|N(S) - S| \geq \epsilon|S|$, and each node in $N(S) - S$ is the endpoint of at least one edge in $E(S)$.

We shall prove Theorem 8 as a corollary to Theorem 4: for this, we let $R = F$ and $R^* = \{-1, 1\}$. The R^*-terms are thus just the terms m and $-m$ where m is a monomial.

Definition. *We define an equivalence relation $\equiv_d$ on the R^*-terms of degree at most d multilinear monomial, as follows. Let $b_1, b_2 \in \{0, 1\}$, $(-1)^{b_1} m_1 \equiv_d (-1)^{b_2} m_2$ if there exists a set $S \subset V$ such that*

1. *$E_{\overline{m_1 m_2}} = E(S)$.*
2. *$|S| < n/2$; and*
3. *$|S| \equiv b_2 - b_1 \pmod 2$.*

We will show that there is no degree $d < \epsilon n/8$ PC refutation of $TS_n(2)$ by showing that that $\equiv_d$ is a d-Laurent relation.

Lemma 10 *If $d < \epsilon n/8$, then the relation $\equiv_d$ is an equivalence relation.*

Proof. It is easy to see from the definitions that $(-1)^b m \equiv_d (-1)^b m$ and that $(-1)^{b_1} m_1 \equiv_d (-1)^{b_2} m_2$ iff $(-1)^{b_2} m_2 \equiv_d (-1)^{b_1} m_1$. We need to show that if $(-1)^{b_1} m_1 \equiv_d (-1)^{b_2} m_2$ and $(-1)^{b_2} m_2 \equiv_d (-1)^{b_3} m_3$, then $(-1)^{b_1} m_1 \equiv_d (-1)^{b_3} m_3$. Let S_1 be the set of vertices such that $E(S_1) = E_{\overline{m_1 m_2}}$, $|S_1| \equiv b_2 - b_1 \pmod 2$, $|S_1| < n/2$, and similarly let S_2 be the set of vertices such that $E(S_2) = E_{\overline{m_2 m_3}}$, $|S_2| \equiv b_3 - b_2 \pmod 2$,

$|S_2| < n/2$. We want to show that $S' = S_1 +_2 S_2$ is a set of vertices such that $E(S') = E_{\overline{m_1 m_3}}$, $|S'| = b_3 - b_1$, and $|S'| < n/2$. Intuitively, this is saying that if S_1 has parity $b_2 - b_1$ which equals the parity of $|E(S_1)|$, and S_2 has parity $b_3 - b_2$, which equals the parity of $|E(S_2)|$, then $S_1 +_2 S_2$ has parity $b_3 - b_1$, which equals the parity of $|E(S_1 +_2 S_2)|$. And furthermore, $|S_1 +_2 S_2|$ is not too large.

Clearly, $|S'| \bmod 2 = |S_1| \bmod 2 + |S_2| \bmod 2 = b_2 - b_1 + b_3 - b_2 = b_3 - b_1$. Also we have: $E(S_1 +_2 S_2) = E(S_1) +_2 E(S_2) = E_{\overline{m_1 m_2 m_2 m_3}} = E_{\overline{m_1 m_3}}$.

It is left to show that $|S'| < n/2$. Since $|m_1|, |m_2| \leq d$, it follows that $|E(S_1)| \leq |m_1 m_2| \leq 2d$. Since G_n is an expander graph, Proposition 9 implies that $|E(S_1)| \geq \epsilon |S_1|$, and thus it follows that $|S_1| \leq 2d/\epsilon < n/4$. Similarly, $|S_2| \leq n/4$. Thus, $|S'| \leq |S_1| + |S_2| < n/2$. In fact, since $|E(S')| \leq |m_1 m_3| \leq 2d$, Proposition 9 further implies that $|S'| \leq n/4$. □

Lemma 11 *For $d \leq \epsilon n/8$, $\equiv_d$ is a d-Laurent relation.*

Proof. Let $d \leq \epsilon n/8$. We just established that $\equiv_d$ is an equivalence relation. Condition (a) of the definition of d-Laurent is trivially satisfied from the definition of $\equiv_d$. Also, the fact that $(-1)^{b_1} m_1 \equiv_d (-1)^{b_2} m_2$ is defined in terms of the linearization of $m_1 m_2$ means that condition (b) of the definition of d-Laurent is also satisfied. □.

Lemma 12 *Every polynomial of $TS_n(2)$ is a binomial from $B_{\equiv_d}$.*

Proof. There are two kinds of polynomials in $TS_n(2)$. For the equations $y_e^2 - 1$, we must show that $y_e^2 \equiv_d 1$. This is easily done by taking $S = \emptyset$ and noting that since $\overline{y_e^2 1} = 1$, the three conditions of the definition of $\equiv_d$ are trivially satisfied. For the equations of the form $1 + y_{\{i,j1\}} y_{\{i,j2\}} \cdots y_{\{i,jr\}} = 0$, we must show that $1 \equiv_d (-1) y_{\{i,j1\}} y_{\{i,j2\}} \cdots y_{\{i,jr\}}$. This is easily seen to hold with $S = \{i\}$. □

Proof of Theorem 8. This is a consequence of Theorem 4. First, Lemma 11 shows $\equiv_d$ is d-Laurent. Second, Lemma 12 shows $TS_n(2) \subset B_{\equiv_d}$. It remains to show that $1 \not\equiv_d (-1)$. To prove this suppose $1 \equiv_d (-1)$ holds with some set S satisfying the conditions of the definition $\equiv_d$. Now we must have $E(S) = \emptyset$. But on the other hand, $|S| < n/2$, so Lemma 9 implies $E(S)$ is non-empty — a contradiction. Therefore, the hypotheses of Theorem 4 hold, and there is no PC refutation of $TS_n(2)$ over F of degree d. □

7 PC lower bound for the general case

This section proves the following theorem giving linear lower bounds on the degree of PC refutations of $TS_n(p)$ over a field F of characteristic q.

Theorem 13 *Let F be a field of characteristic q, and let G_n be an r-regular graph with expansion ϵ. Then, for all $d < \epsilon n/8$, there is no degree d PC refutation of $TS_n(p)$ over F.*

As a corollary to this theorem and Lemmas 1 and 2, we shall prove (as Corollary 18) that when $q \nmid p$, any PC refutation of the MOD_p^n polynomials over F requires linear degree.

In order to express the $TS_n(p)$ polynomials, F must contain a p-th primitive root of unity, ω. We let $R = F$ and R^* be the powers of the root of unity, i.e., $R^* = \{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$. For the rest of this section, it is sufficient to assume only that R is a ring (rather than a field). See section 8 for more explanation of what it means for a ring to have a p-th root of unity.

Definition. *Let A and B be two multisets sets. Then $A +_p B$ denotes the multiset, where if x occurs in A with multiplicity $a \bmod p$, and in B with multiplicity $b \bmod p$, then x occurs in $A +_p B$ with multiplicity $(a + b) \bmod p$. Note that when A and B are ordinary sets and $p = 2$, then $A +_2 B$ is simply the disjoint union of A and B.*

Definition. *Let $S = \{s_1, \ldots, s_n\}$, where each $s_i \in [0, p-1]$. We will think of S as a multiset over the vertices V in G, where vertex i occurs in the set with multiplicity s_i. $E(S)$ will denote a multiset of edges from G'_n as follows. Edge $\langle i, j \rangle$ occurs with multiplicity 0 if $s_i - s_j$ is negative, and occurs with multiplicity $s_i - s_j$ otherwise.*

The *size* of S, $|S|$, will be k if and only if the number of nonzero elements in S is k. In other words, the size of a multiset is the number of elements that appear at least once in the multiset. The size of $E(S)$ is defined similarly.

Proposition 14 *Let G_n be an expander graph with expansion ϵ. If $|S| \leq n/2$, then $|E(S)| \geq \epsilon |S|$.*

Proof. Even though S and $E(S)$ are multisets and the definition of 'size' is correspondingly modified, the proof of Proposition 9 still applies word-for-word. (In fact, when members of S have different non-zero multiplicities, it only makes the size of $E(S)$ increase.) □

Definition. *We define the binary relation $\equiv_d$ on the R^*-terms $\omega^b m$ where m is a degree at most d monomial and $0 \leq b < p$. $\omega^{b_1} m_1 \equiv_d \omega^{b_2} m_2$ if there exists a multiset S of vertices such that (i) The multiset of edges in $m_1 m_2^{-1}$ (after applying $y_{i,j}^p = 1$, and $y_{i,j} y_{j,i} = 1$) equals $E(S)$; (ii) $|S| < n/2$; and (iii) $\sum_i s_i \equiv b_2 - b_1 \pmod p$.*

The next three lemmas are proved exactly analogously to Lemmas 10-12.

Lemma 15 *For $d \leq \epsilon n/8$, the relation $\equiv_d$ is an equivalence relation.*

Lemma 16 *For $d \leq \epsilon n/8$, $\equiv_d$ is a d-Laurent relation.*

Lemma 17 *Every polynomial of $TS_n(2)$ is a binomial from $B_{\equiv_d}$.*

Proof of Theorem 13. Exactly as argued in the proof of Theorem 8, we have that $1 \not\equiv_d a$ for any $a \in R^*$ distinct from 1, i.e., $1 \not\equiv_d \omega^i$ for all $0 < i < p-1$. Thus Theorem 13 follows from Theorem 4 using Lemmas 16 and 17. □

Corollary 18 *Let $q \geq 2$ be a prime such that $q \nmid p$ and let F be a field of characteristic q. Any PC-refutation of the MOD_p^n polynomials requires degree $> \delta n$, for some constant $\delta > 0$.*

Proof. Choose constants ϵ and r so that there are r-regular graphs G_n of expansion ϵ for all n. Let $d_1 = d_2 = 2pr$. Suppose MOD_p^m has a degree d_3 PC refutation, where $m = n + nrp$. By Lemmas 1 and 2 $TS_n(p)$ has a degree $d_3 d_1$ PC refutation, so by Theorem 13, $d_3 d_1 > \epsilon n/(8pr)$. Thus, $d_3 > \epsilon m/(16p^2r^2(1+rp))$. Since ϵ, r, p, d are constants, this proves the Corollary. □

8 Polynomial calculus over rings

We now consider the polynomial calculus over rings instead of over fields. For this, we consider a fixed ring R and the polynomials have coefficients from R. (By 'ring' we always mean 'commutative ring'.) Since the definition of the polynomial calculus did not use any field-specific properties, e.g., since the definition did not depend on the existence of inverses, it is completely natural to consider the polynomial calculus over rings. As before, we define a PC derivation to be a sequence of polynomials $\langle P_i \rangle_i$ with the same rules of addition and multiplication. However, we modify the definition of a PC refutation of Q to be a PC derivation that ends with a constant polynomial m where $m \in R$ is non-zero (and its derivation thus corresponds to a derivation of the contradiction $m = 0$).

It is known that the polynomial calculus over rings is complete with respect to Boolean reasoning, i.e., if the initial polynomials include $x^2 - x = 0$ for each variable x then any unsatisfiable set of polynomials has a PC refutation. However, the polynomial calculus over rings is not complete for general derivations, see the examples in [2]. In this respect the polynomial calculus over a field is stronger than the polynomial calculus over a ring. On the other hand, if the ring R is $\mathbb{Z}_m$ where $m = p_1 \cdot p_2$ for distinct primes p_1, p_2, then it is well-known that there are constant-degree polynomial calculus proofs of $MOD_{p_1}^n$ and $MOD_{p_2}^n$. But Theorem 13 implies that there is no single field for which the polynomial calculus has constant degree proofs of both these principles.

The situation is a little analogous to an important open problem in circuit complexity. Namely, Smolensky [10] showed that polynomial size constant-depth circuits with mod-q gates cannot compute the mod-p function for distinct primes p, q. However, it is open whether this is true for composite values of q where $p \nmid q$.

We prove below that if p and q are relatively prime, then over the ring Z_q, any PC refutation of MOD_p^n requires degree $\geq \delta n$ for some constant δ. The general outline of the proof is similar to the approach used for the proof of Theorem 13.

In the next section, we do some preliminary work introducing rings with roots of unity. Following that, we discuss the reduction of the Tseitin principle to the mod p counting principle and then discuss the lower bound for Tseitin principle.

8.1 Rings with roots of unity

We are mostly interested in lower bounds on the degree of polynomial calculus refutations over rings $R = \mathbb{Z}_q$; however, our method of proof depends strongly on the use of p-th roots of unity, and on the existence of inverses of certain terms involving the p-th root of unity. In this section, we prove that there exist rings containing $\mathbb{Z}_q$ with the desired p-th roots of unity.

Theorem 19 *Let $p, q > 1$ be relatively prime. Then there is a finite ring $R \supset Z_q$ which contains a p-th root of unity ω such that*

(a) *p is the least positive integer i such that $\omega^i = 1$,*

(b) *For all $0 \leq j < k < p$, $(\omega^k - \omega^j)$ has an inverse in R.*

Proof. First we shall give a simple proof for the case where q is a product of *distinct* primes $q = r_1 \cdot r_2 \cdots r_m$. For this, let GF_r be the field of order r and let $F_i = GF_r[\sqrt[p]{1}]$ be the extension of GF_r obtained by adjoining a p-th root of unity. We use ω_i to denote a p-th root of unity in F_i. Define R to be the ring with domain $\prod_i F_i$ and component-wise addition and multiplication. An element of R is an m-tuple $\langle a_1, \ldots, a_m \rangle$ with $a_i \in F_i$. By the Chinese remainder theorem, a copy of Z_q is embedded in R by $n \mapsto \langle n \bmod r_1, \ldots, n \bmod r_m \rangle$. The element $\langle a_1, \ldots, a_m \rangle$ has an inverse in R iff each $a_i \neq 0$. Letting $\omega = \langle \omega_1, \ldots, \omega_m \rangle$, it is easy to see that ω is a p-th root of unity in R and satisfies property (a). Likewise, $\omega_i^k - \omega_i^j \in F_i$ is non-zero for all i and thus $(\omega^k - \omega^j)^{-1}$ exists in R.

Now consider the general case, where q is not a product of distinct primes. (We don't use any special properties of Z_q beyond the fact that p^{-1} exists in Z_q, which follows from the fact that p and q are relatively prime.) Consider a primitive p-th root of unity, ν, over the field of rationals. As a root of unity, ν is a root of the polynomial $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$. Likewise, for any $\ell < p$ dividing p, $\nu^{p/\ell}$ is a primitive ℓ-th root of unity, so ν is a root of $x^{(\ell-1)p/\ell} + x^{(\ell-2)p/\ell} + \cdots + x^{p/\ell} + 1$. It follows that there is a

non-constant polynomial $Q(x)$ which is the greatest common divisor of each of these polynomials which has ν as a root. Furthermore, by Gauss's lemma, we may choose the polynomial $Q(x)$ with leading coefficient 1 and integer coefficients. We define R to be the extension ring $Z_q[\omega]/(Q(\omega))$. Formally, this means we define an equivalence relation on the set $Z_q[\omega]$ of univariate polynomials over Z_q by

$$f \sim g \quad \leftrightarrow \quad \exists h \in Z_q[\omega],\, f(\omega) - g(\omega) = h(\omega) \cdot Q(\omega).$$

Clearly this is an equivalence relation, and addition and multiplication respect $\sim$. The ring $R = Z_q[\omega]/(Q(\omega)) =_{df} Z_q[\omega]/\sim$ has domain the set of $\sim$-equivalence classes (but we generally abuse notation by writing $f \in R$ instead of $[f] \in R$, etc.) Clearly R is a ring. In R, each polynomial $x^{(\ell-1)p/\ell} + x^{(\ell-2)}p/\ell + \cdots + x^{p/\ell} + 1$ is equal to zero, since it is a multiple of Q. Therefore $\omega^p = 1$ in R (i.e., $w^p \sim 1$) since

$$(\omega - 1) \cdot (\omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1) \;=\; \omega^p - 1.$$

Also note that no constant of Z_q becomes equal to zero in R: this is immediate from the fact that Q is a non-constant, monic polynomial over Z_q.

It remains to prove that if $k \neq \ell$, $0 \leq k, \ell < p$, then $(\omega^k - \omega^\ell)$ has a (multiplicative) inverse in R. Since $(\omega^k - \omega^l) = \omega^\ell(\omega^{k-\ell} - 1)$ and ω^ℓ has inverse in R, it will suffice to prove that $(\omega^k - 1)$ has an inverse in R for all $1 \leq k < p$.

Define $i_0 = 0$ and $i_{n+1} = i_n + k \bmod p$. Let ℓ be the least value such that $i_\ell = 0$; of course ℓ divides p. Therefore the values $i_0, \ldots, i_{\ell-1}$ are distinct and enumerate all the values in $\{0, p/\ell, 2p/\ell, \ldots, (\ell-1)p/\ell\}$. For $0 \leq j < \ell$, let $v(j)$ be the value such that $i_{v(j)} = j$, $0 \leq v(j) < \ell$. Define

$$f(\omega) \;=\; \sum_{j=0}^{\ell-1} v(j)\omega^j \;=\; \sum_{n=0}^{\ell-1} n \cdot \omega^{i_n}.$$

Claim: $(\omega^k - 1)f(\omega) = \ell$ holds in R.

Since ℓ has an inverse in Z_q, the claim immediately implies that $(\omega^k - 1)$ has in inverse in R, namely, $\ell^{-1}f(\omega)$.

In R we have

$$\begin{aligned}
(\omega^k - 1) \cdot f(\omega) &= \sum_{n=0}^{\ell-1} n\omega^{i_n+k} - \sum_{n=0}^{\ell-1} n\omega^{i_n} \\
&= \sum_{n=1}^{\ell} (n-1)\omega^{i_n} - \sum_{n=1}^{\ell-1} n\omega^{i_n} \\
&= (\ell-1) \cdot \omega^{i_\ell} - \sum_{n=1}^{\ell-1} \omega^{i_n} \\
&= (\ell-1) \cdot 1 + 1 - \sum_{n=0}^{\ell-1} \omega^{i_n} \\
&= \ell - \sum_{n=0}^{\ell-1} \omega^{i_n} \;=\; \ell - \sum_{n=0}^{\ell-1} \omega^{np/\ell} \\
&= \ell - 0 \;=\; \ell.
\end{aligned}$$

That completes the proof of the claim and of Theorem 19 □

For the next two sections, we shall consider p and q to be fixed and let R be as in Theorem 19.

8.2 Low degree reductions

Lemma 1 clearly still applies to the polynomial calculus over rings, but Lemma 2 needs to be reproved for rings. Let q, p, R be as in the previous theorem.

Lemma 20 *Over the ring R, $TS_n(p)$ is (d_1, d_2)-reducible to MOD_p^m, where $m = n + nrp$, $d_1 = 2pr$ and $d_2 = 2pr$.*

Proof. The reduction is exactly the same as the reduction used for the proof of Lemma 2. Examination of the definition of r_e in Step 1 of that proof reveals that the only place where inverses were used was in the polynomials (1) and (2) and these were inverses of elements of the form $\omega^{a_1} - \omega^a$ which do exist in R. So it remains to re-do Step 2 of the proof of Lemma 2.

Recall that we must find small degree PC derivations of $MOD_p^m(r_e)$ equations:

1. $r_e^2 - r_e = 0$ for all p-sets e
2. $r_e r_f = 0$ for all e, f such that $e \cap f \neq 0$, $e \neq f$
3. $\sum_{e, u \in e} r_e - 1 = 0$, for all $u \in [m]$.

As discussed before, each single equation is a tautological consequence of a constant number of equations of $TS_n(p)$. We now need to extend the completeness theorem of [3], Theorem 5.2, to apply to the polynomial calculus over R.

Lemma 21 *Let $z_1, \ldots, z_k$ be variables, and $f(\vec{z})$ be a polynomial. Suppose that in the ring R, $f(z_1, \ldots, z_k) = 0$ for all values of $z_1, \ldots, z_k \in \{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$. Then there is PC derivation of $f(\vec{z})$ from the polynomials $z_i^p - 1$, of degree $\leq pk \cdot \deg(f)$.*

Proof. We give the proof for the case $k = 1$ and leave it the reader to formulate the proof by induction for the case $k > 1$. (All the essential difficulties arise already in the case $k = 1$.) Let P_a be the polynomial

$$(z_1 - \omega^0)(z_1 - \omega^1) \cdots (z_1 - \omega^{a-1})(z_1 - \omega^{a+1}) \cdots (z_1 - \omega^{p-1}).$$

Note that $P_a \cdot (z_1 - \omega^a)$ is the polynomial $z_1^p - 1$ (this is immediate from the fact that they are the same polynomial in each field F_{q_i}).

Claim: Let $c = f(\omega^a) \in R$. The polynomial $P_a \cdot (f(z_1) - c)$ is PC derivable from $z_i^p - 1$ in degree $(p-1)\cdot\deg(f)$.

The claim is proved by induction on the size of the polynomial f. The base case where f is a constant is trivial. The second base case where $f(z_1)$ is just z_1 is immediate from the observation above that $P_a \cdot (z_1 - \omega^a) = z_1^p - 1$. The induction steps of addition and multiplication are handled by the following two constructions:

$$\frac{P_a\cdot(f-c) \qquad P_a\cdot(g-d)}{P_a\cdot((f+g)-(c+d))}$$

and

$$\frac{\dfrac{P_a\cdot(f-c)}{P_a\cdot(fg-cg)} \qquad \dfrac{P_a\cdot(g-d)}{P_a\cdot(cg-cd)}}{P_a\cdot(fg-cd)}$$

and this proves the claim.

Now let P_a^ℓ be the polynomial $\prod_{\substack{i\geq\ell\\ i\neq a}}(z_1-\omega^i)$. We only use this polynomial when $a \geq \ell$.

Claim: Let $\ell \geq 0$ and let $c = f(\omega^a) \in R$. The polynomial $P_a^\ell \cdot f(z_1)$ is PC derivable from $z_i^p - 1$ in degree $(p-1)\deg(f)$.

The second claim is proved by induction on ℓ. The base case, where $\ell = 0$ is already established by the first claim, since $P_a^0 = P_a$. For the induction step, let $a \geq \ell + 1$. The induction hypothesis tells us that $P_\ell^\ell f(z_1)$ and $P_a^\ell \cdot f(z_1)$ are both PC derivable. Subtracting these gives

$$(\omega^\ell - \omega^a) P_a^{\ell+1} \cdot f(z_1).$$

Since $(\omega^\ell - \omega^a)$ is invertible in R, we may multiply by $(\omega^\ell - \omega^a)^{-1}$ to derive $P_a^{\ell+1} \cdot f(z_1)$, and the claim is proved.

The base case $k = 1$ of Lemma 20 is immediate from the second claim, with $\ell = p$. The argument for the induction step is similar and is left to the reader. □

8.3 PC lower bound for rings

We now prove the main theorems giving lower bounds the degrees of of PC derivations over $\mathbb{Z}_q$. Fix p, q,R as above.

Theorem 22 *Let G_n be an r-regular graph with expansion ϵ. Then, for all $d < \epsilon n/4$, there is no degree d PC refutation of $TS_n(p)$ over R.*

This plus Lemmas 1 and 20 immediately imply:

Corollary 23 *Let $p, q \geq 2$ be relatively prime. Any PC-refutation over Z_q of the MOD_p^n polynomials requires degree $> \delta n$, for some constant $\delta > 0$.*

The constant δ depends on p and q. To prove Theorem 22, we need merely note that the proof of Theorem 13 still applies: We take $R^* = \{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$ and then, as already noted near the beginning of section 7, the proof of Theorem 13 establishes Theorem 22.

Acknowledgement. We thank A. Wadsworth for discussions about ring extensions.

References

[1] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs*, Proceedings of the London Mathematical Society, 73 (1996), pp. 1–26.

[2] S. R. Buss, *Lower bounds on Nullstellensatz proofs via designs*, in Proof Complexity and Feasible Arithmetics, P. Beame and S. Buss, eds., American Mathematical Society, 1998, pp. 59–71.

[3] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall, *Proof complexity in algebraic systems and bounded depth Frege systems with modular counting*, Computational Complexity, 6 (1996/1997), pp. 256–298.

[4] M. Clegg, J. Edmonds, and R. Impagliazzo, *Using the Groebner basis algorithm to find proofs of unsatisfiability*, in Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing, 1996, pp. 174–183.

[5] D. Grigoriev, *Nullstellensatz lower bounds for Tseitin tautologies.* To appear, *39th Annual IEEE Symp. on Foundations of Computer Science*, 1998.

[6] J. Krajíček, *Lower bounds for a proof system with an exponential speed-up over constant depth Frege systems and over polynomial calculus.* Typeset manuscript, 1997.

[7] ——, *On the degree of ideal membership proofs from uniform families of polynomials over a finite field.* Typeset manuscript, 1998.

[8] T. Pitassi, *Algebraic propositional proof systems*, in Descriptive Complexity and Finite Models, N. Immerman and P. Kolaitis, eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Science #31, American Mathematics Society, 1996, pp. 215–244.

[9] A. A. Razborov, *Lower bounds for the polynomial calculus.* Typeset manuscript, 1996.

[10] R. Smolensky, *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, in Proceedings of the Nineteenth Annual ACM Symposium on the Theory of Computing, ACM Press, 1987, pp. 77–82.