Multilinear Polynomials over Rings: Quantum Simulation and Solution Sets

Kenneth W. Regan[1] and Robert Surówka[1]

Department of CSE, University at Buffalo, Amherst, NY 14260 USA;
{regan,robertlu}@buffalo.edu

Abstract. We extend the quantum polynomial simulation of Dawson et al. [1] to work for quantum circuits with gates of almost any kind, using low-degree polynomials $q(x_1, \ldots, x_n)$ over the ring of integers modulo k where k is a power of 2. The simulations require computing the values $N_q[j] = |\{x \in \mathbb{Z}_k^n : q(x) = j\}|$ for all j, $0 \leq j \leq k-1$. For quadratic polynomials and fixed k this is doable in deterministic polynomial time by results of Cai, Chen, Lipton, and Lu [2, 3]. We observe that quantum *stabilizer circuits* involve such polynomials, thus yielding another proof that they can be simulated in classical polynomial time [4–8]. Our second main technical results show that the values $N_q[j]$ occurring in the expressions for the acceptance probability of quantum circuits are multiples of large powers of 2, thus limiting the extent to which probabilities in these circuits can be "amplified" at least when q is multilinear. These results are a first attempt at a Chevalley-Warning-Weil type theory (see [9]) for polynomials modulo composites rather than primes.

1 Introduction

Polynomials modulo composite numbers represent the frontier of what is known in computational complexity theory, and a step beyond the well worked-out theory of polynomials over fields. In complexity they correspond to the class ACC^0 of languages represented by constant-depth, polynomial-sized circuits of Boolean and mod-m gates. That this was only recently separated from the nondeterministic exponential time class NEXP [10] indicates how difficult they are to study. In mathematics there are strange behaviors even for univariate polynomials, for instance x "factors" as $(4x+3)(3x+4)$ over $\mathbb{Z}_6$. The presence of zero divisors nullifies regular notions such as degree and irreducibility. It is hard to find much evidence of a general theory of properties of their solution sets, analogous to the rich theory of varieties in algebraic geometry, because even when modules are used and polynomials are regarded as being over subrings, the coefficients and division relations are ultimately based on a field.

Quantum computation gives a new reason for caring about properties of polynomials over the rings $\mathbb{Z}_k$ for composite k, especially for k a power of 2. We describe a new rule for associating to a quantum circuit C a polynomial $q = q_C$ that quantifies the phase changes of the quantum state during its manipulation by gates of C. Provided all phase angles in the gates are integral multiples of $2\pi/k$, making them powers of a primitive k-th root of unity ω, we can define q over $\mathbb{Z}_k$. Then we associate to q the following *partition function* $Z(q)$ as in [8, 2], which can be expressed in two different ways as

$$Z(q) = \sum_{\mathbf{x}} \omega^{q(\mathbf{x})} = \sum_{i=0}^{k-1} \omega^i N_q[i].$$

Here and below, $N_q[i]$ denotes the number of arguments to the variables $\mathbf{x} = (x_1, \dots, x_n)$ for which $q(\mathbf{x}) = i$. The first form makes clear that this is an **exponential sum**, of the kind considered by Gauss two centuries ago. The second form expresses this in terms of the cardinalities of the solution sets of $q(\mathbf{x}) - i$ for all i, $0 \leq i \leq k-1$. The importance is magnified by a normal form for quantum circuits C in which $\frac{1}{R}|Z(q)|^2$ gives the acceptance probability of the circuit, where the normalizing constant R quantifies the amount of quantum nondeterminism (such as given by Hadamard gates) in the circuit.

The relation to acceptance was observed in the case $k = 2$ by Dawson et al. [1] for circuits of Hadamard and Toffoli gates. Although these gates have all-real-number entries, they are still universal for defining the bounded-error quantum polynomial time class, BQP. Dawson et al. suggested an extension for $k = 8$ using mixed-modulus arithmetic.

Our first main theorem shows how to do this for any $k = 2^r$ without mixed arithmetic, applicable to circuits C of gates whose phases are multiples of $2\pi/k$, where q may also use some auxiliary variables over $\mathbb{Z}_k$. Then we turn to the problem of the solution sets of $q(\mathbf{x}) - i$: what are their cardinalities $N_q[i]$, and what other properties do they have?

We obtain results for $N_q[i]$ in case $q(x)$ is quadratic, and either over $\mathbb{Z}_4$ or multilinear over $\mathbb{Z}_{2^r}$. Such polynomials (specifically the former kind) arise as q_C for so-called *stabilizer circuits* C. It has long been known that these circuits, which include Hadamard but not Toffoli gates, can be simulated in classical deterministic polynomial time [4]. Successive modifications to the proof [5–8] have revealed connections to graph theory and Gauss sums, as well as enhancing the pretty theory already associated to stabilizer groups and Clifford algebra. Our work, combined with the polynomial-time algorithm for computing $Z(q)$ when q is quadratic by Cai et al. [2], furnishes yet another proof, but we argue greater significance in the reverse direction: this may enable the algebraic theory to inform issues about polynomials modulo 2^r.

The results for $N_q[i]$ in our other main theorems show that they are multiples of 2^m where $m = \Theta(nr)$. Thus the acceptance probability must be a multiple of $\frac{2^{2m}}{R}$. This limits how close to 1 it can be. We speculate that these observations can be extended to show a tradeoff between "amplification" of the success probability and the amount of quantum nondeterminism—such as the number of Hadamard gates—needed by the circuit.

When Toffoli gates are included, the degree of q becomes 3. (In the analogous setting of [8], the polynomial defined there goes from linear to quadratic.) Unfortunately our proof technique for degree 2 does not readily extend to degree 3 or higher, but we conclude with some conjectures for general degrees d. The general connection we establish in this paper may thereby explain some of the mathematical difficulty posed in studying solutions of cubic and higher degree polynomials modulo composites, supplemented by the results of [3] showing that computing $Z(q)$ becomes generally NP-hard, in fact $\#\mathsf{P}$-complete. Our side of the difficulty stems from Toffoli and Hadamard gates sufficing to build small quantum circuits for all problems in BQP, in particular the problem of factoring [11] which is commonly believed to lie outside of classical (randomized) polynomial time.

2 Quantum Circuit Simulation and Polynomials

Every quantum gate g has some bounded number m of incoming and outgoing *qubit wires*, and is specifiable by a $2^m \times 2^m$ unitary matrix U_g. The gate is *balanced* if all non-zero entries in U_g have the same magnitude r_g. This balance property carries over to arbitrary tensor products of U_g with identity matrices representing the (non-)action on qubit wires that re not involved in the gate. A quantum circuit is *balanced* if all of its gates are balanced. This is not a great restriction—in fact, it is hard to find examples of useful quantum circuits in the literature that aren't balanced, and many different kinds of universal quantum circuits are balanced.

The notion of balance suffices to well-define the normalizing constant $R = R_C$: it is the product of r_g over all gates g in C. Also define $k = k_C$ to be the least integer such that all angles θ in entries $re^{i\theta}$ of gates in C are integer multiples of $2\pi/k$. For example if C has only Hadamard, CNOT, and Toffoli gates then $k_C = 2$; if it adds the so-called T gate which has an entry $e^{\pi i/4}$, then $k_C = 8$. As is usual in talking about quantum circuits, we may suppose that the "input string" a is already packaged into an initial set of gates of C, and a final set of gates incorporates a string b that describes the final measurement process. Via the normal-form theorem proved in [1] (but previously folklore), the triple product aU_Cb yields a complex scalar whose norm-squared is the acceptance probability of C. Our theorem says that this scalar is described by the partition function of the polynomial q constructed in its proof.

The theorem itself involves counting 0-1 assignments, not all assignments in $\mathbb{Z}_k^n$. Accordingly we define $N'_q[\ell]$ to be the number of *Boolean* arguments $\mathbf{x}$ for which $q(\mathbf{x}) = \ell$. Our application to stabilizer circuits is an example where one can later extend the counting to all of $\mathbb{Z}_k^n$.

Theorem 1. *There is an efficient uniform procedure that transforms any balanced quantum circuit C with s gates of minimum phase $2\pi/k$ where $k = 2^r$ into a polynomial q over $\mathbb{Z}_k$ such that, with R and a, b as above,*

$$aU_Cb = \frac{1}{R}\sum_{\ell=0}^{k-1} \omega^\ell N'_q[\ell], \tag{1}$$

and both the size of q and the time needed to construct q are $O(2^{2m}ms)$ where m is the maximum arity of a gate in C.

Proof. The polynomial q_C is a simple sum of polynomials q_g for every gate g in C. Each q_g has $2m$ basic variables labeled $\mathbf{y} = y_1, \ldots, y_m$ and $\mathbf{z} = z_1, \ldots, z_m$, plus some number of auxiliary variables w. Every possible 0-1 assignment i to $\mathbf{y}$ and j to $\mathbf{z}$ indexes a unique entry of U_g corresponding to (i, j). We can define an *indicator term* $T_{i,j}(\mathbf{y}, \mathbf{z})$ that is 1 when $\mathbf{y} = i$ and $\mathbf{z} = j$ and 0 otherwise.

If the entry $U_g(i, j)$ is non-zero, then after division by the balanced value r_g it has the form ω^e for some e, whereupon we give q_g the additive term $eT_{i,j}$. If it is zero, however, we allocate fresh variables $w_1, \ldots, w_r$ and include $(w_1 + 2w_2 + 4w_3 + \cdots 2^{r-1}w_r)T_{i,j}$ in the sum. In physical terms, the assignment $\mathbf{y} = i, \mathbf{z} = j$ violates the operation of the gate and is impossible. In our formula, its effect is to leave an additive term of w_b's where the variables w_b appear nowhere else. Since this term can take any value in $\mathbb{Z}_k$, all Boolean domain elements involving such an impossible assignment contribute equally to each $N_q[\ell]$ value, and hence cancel each other out in the expression for aU_Cb, i.e. in $Z(q)$.

The use of these extra w variables is the innovation that avoids the ad-hoc suggestion of mixed-modulus arithmetic in [1]. The remainder of the proof then follows by the technique used in that paper for $k = 2$ with Hadamard and Toffoli gates only. □

In many cases we can avoid introducing w-variables by substituting some or all z-variables for a gate by expressions in the y-variables. In particular, for a deterministic gate such as CNOT or Toffoli, we can substitute all of them and avoid introducing any w's. Note also that the $T_{i,j}$ terms are expressible as products of y_b or $1 - y_b$ and z_b or $1-z_b$ according to the values of the individual bits b of i and j. The different products of the former index the rows of U_g, and different products of the latter index the columns. For a general single-qubit gate g we have the indexing scheme

$$\left[\begin{array}{r|cc} & (1-z) & z \\ \hline (1-y) & a_{11} & a_{12} \\ y & a_{21} & a_{22}, \end{array}\right]$$

Writing a' when $a = \omega^{a'}$, and regarding $a' = w$ when the matrix entry is 0, the polynomial q_g is then given by

$$q_g = a'_{11}(1-y)(1-z) + a'_{12}(1-y)z + a'_{21}y(1-z) + a'_{22}yz.$$

The NOT gate, also called X, has $a_{11} = a_{22} = 0$ and $a_{12} = a_{21} = 1$, so it gives

$$q_g = (1-y)(1-z)w + (1-y)z \cdot 0 + y(1-z) \cdot 0 + yzw = w(2yz - y - z + 1).$$

Now when $z = y = 0$ or $z = y = 1$ the w is left alone as an additive term. Instead, we can substitute $z = 1-y$, and this dispenses with the w-variables leaving just $q'_g = 0$. We can always do substitution for any deterministic gate, even one with imaginary entries such as the *Phase Gate*:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \qquad q_g = w(y + z - 2yz) + \frac{k}{4}yz; \quad q'_g = \frac{k}{4}y^2.$$

For Hadamard gates we pull the balance factor $\sqrt{2}$ outside, and note that $-1 = \omega^{k/2}$.

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \qquad q_g = \frac{k}{2}yz.$$

Here there is no substitution, so we have added a variable, and there are no constraints on assignments either.

Multi-Qubit Gates

A 2-qubit gate with inputs y_1, y_2 has a 4×4 matrix with rows indexed $(1-y_1)(1-y_2)$, $(1-y_1)y_2$, $y_1(1-y_2)$, y_1y_2, and columns similarly for the outputs z_1, z_2. For example:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

The q-polynomial for CNOT has twelve terms multiplied by w's but nothing else. These terms are zeroed out by the substitution $z_1 = y_1$, $z_2 = y_1 + y_2 - 2y_1y_2$, which conveys this deterministic action having no effect on phase.

For CZ the bottom-right -1 entry contributes $\frac{k}{2}y_1y_2z_1z_2$ to q. The substitution $z_1 = y_1$, $z_2 = y_2$ is applicable, and leaves $\frac{k}{2}y_1^2y_2^2$, which is equivalent to $\frac{k}{2}y_1y_2$ for 0-1 assignments. It also has a similar w-multiplied term as for CNOT, which goes away for q'.

The Toffoli gate is similar for three inputs/outputs and an 8×8 matrix. The main difference is that the substitution for the third qubit is

$$z_3 = y_1y_2 + y_3 - 2y_1y_2y_3,$$

which is a cubic polynomial. Of particular import, there is no linear or quadratic substitution that has the same parity. Thus these gates, which are needed for efficient universality to define BQP, introduce cubic terms into the partition polynomials, making the additive ones over $\mathbb{Z}_k$ cubic overall. (Compare also the notation scheme of [8], in which this case comes out quadratic.)

Simulations

A *stabilizer circuit* can be characterized by having only Hadamard, CZ, and S-gates, giving $k = 4$.

Theorem 2. *There is an efficient translation of a stabilizer circuit C into a quadratic polynomial q over $\mathbb{Z}_4$ such that with a, b as above and $R' = 2^n R$,*

$$aU_Cb = \frac{1}{R'}Z(q),$$

and so that q is invariant under replacing any argument y by $y + 2$ modulo 4.

The proof is by inspection, since q is composed of terms y^2 and $2yz$ which have the invariance property. This enables a correspondence between Boolean arguments and those over $\mathbb{Z}_4^n$, whose double-counting is absorbed by going from R to R'. The following known theorem then provides another proof that stabilizer circuits can be simulated in classical polynomial time:

Theorem 3 ([2, 3]). *There is a $\mathsf{poly}(n, r)$-time algorithm to compute $Z(q)$ given any quadratic polynomial q over $\mathbb{Z}_{2^r}$.*

The running times appear to have the same order as in earlier algorithms for stabilizer circuits [5–7], skirting the issue of repeated measurements which most concerns these papers.

The main issue going forward is, what further properties are possessed by the sets of solutions to $q(\mathbf{x}) = j$ for the different values of j? The cardinality of these sets affects the granularity of the sums of powers of ω, and hence the set of possible amplitudes of the expression for the acceptance probability. It would also be nice to learn other structural properties of the respective solution sets, but it is already enough of an issue to begin with their cardinalities.

3 Solution Set Cardinalities

The notation for this part of the paper switches to using w for the modulus, k for a value modulo w, and P for polynomials. We write $N_P[k \mid \text{some constraints}]$ to denote the number of assignments to **x** that fulfill the constraints and for which still $P(\mathbf{x}) \equiv k \bmod w$. Also T_k denotes a generic integer depending on k, and implicitly also depending on P and w.

Theorem 4. *For any multivariate polynomial $P(\boldsymbol{x})$ of n variables over $\mathbb{Z}_4$ of degree up to 2 without square terms, and any $k \in \{0, 1, 2, 3\}$, it holds that $N_P[k] = T_k 2^{n-1}$. Furthermore, $N_P[k]$ + $N_P[k + 2]$ is divisible by 2^n.*

Proof. The proof is by induction on number of variables. It can be easily checked to be true for $n = 1$ and $n = 2$ through exhaustive iteration.

Assuming the theorem holds for all polynomials over at most n variables, we would like to show that it holds for any polynomial of the form

$$Q_{n+1}(\mathbf{x}, z) = P_n(\mathbf{x}) + L_n(\mathbf{x})z,$$

where Q_{n+1} is over $n + 1$ variables and has degree up to 2, P_n is over n variables and also has degree up to 2, and L_n is an affine linear form over n variables. Then:

$$\begin{aligned}
&N_Q[0 \mid z = 0] = N_P[0]\\
&N_Q[0 \mid z = 1] = N_P[0 \mid L(\mathbf{x}) = 0] + N_P[3 \mid L(\mathbf{x}) = 1] + N_P[2 \mid L(\mathbf{x}) = 2] + N_P[1 \mid L(\mathbf{x}) = 3]\\
&N_Q[0 \mid z = 2] = N_P[0 \mid L(\mathbf{x}) = 0] + N_P[2 \mid L(\mathbf{x}) = 1] + N_P[0 \mid L(\mathbf{x}) = 2] + N_P[2 \mid L(\mathbf{x}) = 3]\\
&N_Q[0 \mid z = 3] = N_P[0 \mid L(\mathbf{x}) = 0] + N_P[1 \mid L(\mathbf{x}) = 1] + N_P[2 \mid L(\mathbf{x}) = 2] + N_P[3 \mid L(\mathbf{x}) = 3].
\end{aligned}$$

Therefore:

$$\begin{aligned}
N_Q[0] = {} & 4N_P[0 \mid L(\mathbf{x}) = 0] + 2(N_P[0 \mid L(\mathbf{x}) = 2] + N_P[2 \mid L(\mathbf{x}) = 2])\\
& + N_P[0 \mid L(\mathbf{x}) = 1] + N_P[1 \mid L(\mathbf{x}) = 1]) + N_P[2 \mid L(\mathbf{x}) = 1] + N_P[3 \mid L(\mathbf{x}) = 1])\\
& + N_P[0 \mid L(\mathbf{x}) = 3] + N_P[1 \mid L(\mathbf{x}) = 3]) + N_P[2 \mid L(\mathbf{x}) = 3] + N_P[3 \mid L(\mathbf{x}) = 3])
\end{aligned}$$

Let us note that for any k and ℓ, $N_P[k \mid L(\mathbf{x}) = \ell]$ takes on one of three forms. Either it equals $N_G[k]$ for a certain polynomial G over $n - 1$ variables, the sum of

$N_{G_i}[k]$ for some such polynomials over $n-1$ variables, or is 0 (note that because L is affine-linear, we can always solve it for one variable and replace that variable in P). In any case we can always say that $N_P[k \mid L(\mathbf{x}) = \ell] = t2^{n-2}$ for some t. Using the induction hypothesis we write:

$$N_Q[0] = 4t_0 2^{n-2} + 2t_2 2^{n-1} + t_1 4^{n-1} + t_3 4^{n-1} = T_0 2^n,$$

noting $N_P[0 \mid L(\mathbf{x}) = 2] + N_P[2 \mid L(\mathbf{x}) = 2] = t_2 2^{n-1}$. Analogously as for $N_Q[0]$ we obtain:

$$\begin{aligned} N_Q[1] = 4N_P[1 \mid L(\mathbf{x}) = 0] &+ 2(N_P[1 \mid L(\mathbf{x}) = 2] + N_P[3 \mid L(\mathbf{x}) = 2]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 1] + N_P[1 \mid L(\mathbf{x}) = 1]) + N_P[2 \mid L(\mathbf{x}) = 1] + N_P[3 \mid L(\mathbf{x}) = 1]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 3] + N_P[1 \mid L(\mathbf{x}) = 3]) + N_P[2 \mid L(\mathbf{x}) = 3] + N_P[3 \mid L(\mathbf{x}) = 3]) \end{aligned}$$

$$\begin{aligned} N_Q[2] = 4N_P[2 \mid L(\mathbf{x}) = 0] &+ 2(N_P[0 \mid L(\mathbf{x}) = 2] + N_P[2 \mid L(\mathbf{x}) = 2]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 1] + N_P[1 \mid L(\mathbf{x}) = 1]) + N_P[2 \mid L(\mathbf{x}) = 1] + N_P[3 \mid L(\mathbf{x}) = 1]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 3] + N_P[1 \mid L(\mathbf{x}) = 3]) + N_P[2 \mid L(\mathbf{x}) = 3] + N_P[3 \mid L(\mathbf{x}) = 3]) \end{aligned}$$

$$\begin{aligned} N_Q[3] = 4N_P[3 \mid L(\mathbf{x}) = 0] &+ 2(N_P[1 \mid L(\mathbf{x}) = 2] + N_P[3 \mid L(\mathbf{x}) = 2]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 1] + N_P[1 \mid L(\mathbf{x}) = 1]) + N_P[2 \mid L(\mathbf{x}) = 1] + N_P[3 \mid L(\mathbf{x}) = 1]) \\ &+ N_P[0 \mid L(\mathbf{x}) = 3] + N_P[1 \mid L(\mathbf{x}) = 3]) + N_P[2 \mid L(\mathbf{x}) = 3] + N_P[3 \mid L(\mathbf{x}) = 3]) \end{aligned}$$

Note that for any $N_Q[k]$, assignments for ℓ from $N_P[\ell \mid \ldots]$ are just shifted by k from those for $N_Q[0]$. It is easy to observe that for any k: $N_Q[k] + N_Q[k+2] = t2^{n+1}$ for some t. $\square$

Theorem 5. *For any multivariate polynomial $P(\boldsymbol{x})$ of $n \geq 2$ variables over $\mathbb{Z}_{2^r}$ of degree up to 2 without square terms, and any integer k, there is an integer T_k such that $N_P[k] = T_k 2^{\lceil \frac{rn}{2} \rceil - 1}$. Furthermore,*

$$\sum_{i=0}^{2^q-1} N_P[k + 2^{r-q} i] = T_{k,q} 2^{\lceil \frac{rn}{2} \rceil + q - 1}$$

for a certain integer $T_{k,q}$.

Proof. The proof is by induction on the number of variables. The base cases are $n = 2$ and $n = 3$; in this extended abstract we omit their lengthy consideration, and present the general induction step as our theorem. Assuming the theorem is true for all polynomials over $n \geq 2$ variables, we would like to show that it holds for any

$$Q_{n+1}(\mathbf{x}, z) = P_n(\mathbf{x}) + L_n(\mathbf{x}) z.$$

where Q_{n+1} is over $n+1$ variables and has degree up to 2, P_n is over n variables and also has degree up to 2, while L_n is an affine linear form over n variables. Let us notice that:

$$N_Q[k] = \sum_{\ell=0}^{2^r-1} \sum_{z=0}^{2^r-1} N_P[k - \ell z \mid L(\mathbf{x}) = \ell] = \sum_{\ell=0}^{2^r-1} \sum_{z=0}^{2^r-1} N_P[k + \ell z \mid L(\mathbf{x}) = \ell].$$

If we divide this sum into components with identical value ℓ, we will see that each of them has the form

$$2^f \sum_{j=0}^{2^{r-f}-1} N_P[k + 2^f j | L(\mathbf{x}) = \ell],$$

where for any given ℓ, $f = max_m\{m \leq r : 2^m \mid \ell\}$.

Let us note that for any k, ℓ: $N_P[k \mid L(\mathbf{x}) = \ell]$ is equal either to $N[k]$ for some polynomial over $n-1$ variables, the sum of $N[k]$-s over some polynomials over $n-1$ variables, or to 0 (again because L is affine-linear, we can solve it for one variable and replace that variable in P). Using the induction hypothesis for $n-1$ variables, we can write now:

$$2^f \sum_{j=0}^{2^{r-f}-1} N_P[k + 2^f j \mid L(\mathbf{x}) = \ell] = 2^f T_{k,f} 2^{\lceil \frac{r(n-1)}{2} \rceil + r - f - 1} = T_{k,f} 2^{\lceil \frac{r(n+1)}{2} \rceil - 1}.$$

Because all of the components of the sum are divisible by $2^{\lceil \frac{r(n+1)}{2} \rceil - 1}$, therefore the whole sum is divisible by this value too. Finally, let us notice that

$$\begin{aligned}\sum_{i=0}^{2^q-1} N_Q[k + 2^{r-q} i] &= \sum_{i=0}^{2^q-1} \sum_{\ell=0}^{2^r-1} \sum_{z=0}^{2^r-1} N_P[k + 2^{r-q} i + \ell z \mid L(\mathbf{x}) = \ell] \\ &= \sum_{\ell=0}^{2^r-1} \sum_{i=0}^{2^q-1} \sum_{z=0}^{2^r-1} N_P[k + 2^{r-q} i + \ell z \mid L(\mathbf{x}) = \ell].\end{aligned}$$

We can divide this sum, as we did earlier (defining f in the same way), into components with identical value of ℓ, and therefore obtain components of the form:

$$\begin{aligned}&\sum_{i=0}^{2^q-1} 2^f \sum_{j=0}^{2^{r-f}-1} N_P[k + 2^{r-q} i + 2^f j \mid L(\mathbf{x}) = \ell] \\ &= 2^f 2^{\min(q,r-f)} \sum_{i=0}^{2^{\max(q,r-f)}-1} N_P[k + 2^{r-\max(q,r-f)} i \mid L(\mathbf{x}) = \ell] \\ &= 2^{f+\min(q,r-f)} T_{k,f} 2^{\lceil \frac{r(n-1)}{2} \rceil + \max(q,r-f) - 1} = T_{k,f} 2^{\lceil \frac{r(n+1)}{2} \rceil + q - 1}. \square\end{aligned}$$

4 Conclusions and Further Work

We have first extended the method of [1] to prove a general algebraic simulation of quantum circuits, one that directly connects the minimum phase angle of the quantum gates to the modulus of polynomials. We observed that for stabilizer circuits, the resulting n-variable polynomials $q(\mathbf{x})$ over $\mathbb{Z}_4$ are quadratic and multilinear. We then proved that the number of solutions to $q(\mathbf{x}) = i$ is always a multiple of 2^{n-1}. We extended this over Z_{2^r} for $r > 2$, revealing an odd-even effect when r is odd.

On the basis of computational evidence and partial proofs, we conjecture that our results will extend in the following ways. The first conjecture desires to remove the multilinear restriction on the quadratic polynomials. The ones for higher degree d hold promise of relevance to general quantum circuits. In the following, T_k and $T_{k,q}$ denote integers that depend on the subscripted quantities, and on P and r.

Conjecture 1 *For any multivariate polynomial P of $n \geq 2$ variables over $\mathbb{Z}_{2^r}$ of degree up to 2, and any integer k, it holds that $N_P[k] = T_k 2^{\lceil \frac{rn}{2} \rceil - 1}$. Furthermore,*

$$\sum_{i=0}^{2^q-1} N_P[(k + 2^{r-q}i)] = T_{k,q} 2^{\lceil \frac{rn}{2} \rceil + q - 1}.$$

Conjecture 2 *For any multivariate polynomial P of $n \geq 2$ variables over $\mathbb{Z}_{2^r}$, of degree up to d, and any integer k, it holds that $N_P[k] = T_k p^{\lceil \frac{rn}{d} \rceil - 1}$.*

Conjecture 3 *For any multivariate polynomial P of $n \geq 2$ variables over $\mathbb{Z}_{p^r}$, where p is prime, of degree up to 2, and any integer k, it holds that $N_P[k] = T_k p^{\lceil \frac{rn}{2} \rceil - 1}$.*

Conjecture 4 *For any multivariate polynomial P of $n \geq 2$ variables, of degree up to 2, over $\mathbb{Z}_{p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}}$, where $p_1, p_2, \ldots, p_m$ are prime, and any integer k, it holds that*

$$N_P[k] = T_k \prod_i p_i^{(\lceil \frac{r_i n}{2} \rceil - 1}.$$

Conjecture 5 *For any multivariate polynomial P of $n \geq 2$ variables, of degree up to d, over $\mathbb{Z}_{p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}}$, where $p_1, p_2, \ldots, p_m$ are prime, and any integer k, it holds that*

$$N_P[k] = T_k \prod_i p_i^{(\lceil \frac{r_i n}{d} \rceil - 1}.$$

The closest basis for comparison that we know are the *Chevalley-Warning theorems* (see [9]) over $\mathbb{Z}_p$ for p prime, or over any finite field of characteristic p. They say that provided the number n of variables is greater than the degree of the polynomial q, the number of solutions to $q(\mathbf{x}) = 0$ is a multiple of p. (The same goes for simultaneous equations $q_j(\mathbf{x}) = 0$ provided n exceeds the degree of the product of the q_j.) In our case the modulus is 2^r in place of p. However, there is also the stronger element that our results and conjectures have n as well as r in the exponent of the multiplicand.

Despite the pathology of zero-divisors, we believe that the solution sets of polynomials modulo composites should have a natural, attractive, and unifying theory. Such a theory seems relevant to the prospects for progress in complexity lower bounds. We hope that the work in this paper promotes interest and strategies in building this theory.

References

1. Dawson, C., Haselgrove, H., Hines, A., Mortimer, D., Nielsen, M., Osborne, T.: Quantum computing and polynomial equations over the finite field Z_2. Quantum Information and Computation **5** (2004) 102–112
2. Cai, J.Y., Chen, X., Lipton, R., Lu, P.: On tractable exponential sums. In: Proceedings of FAW 2010. (2010) 48–59
3. Cai, J.Y., Chen, X., Lu, P.: Graph homomorphisms with complex values: A dichotomy theorem. http://arxiv.org/abs/0903.4728 (2011) v2, 2011.
4. Gottesman, D.: The Heisenberg representation of quantum computers. http://arxiv.org/abs/quant-ph/9807006 (1998)
5. Aaronson, S., Gottesman, D.: Improved simulation of stabilizer circuits. Phys. Rev. A **70** (2004)
6. Clark, S., Jozsa, R., Linden, N.: Generalized Clifford groups and simulation of associated quantum circuits. Quantum Information and Computation **8** (2008) 106–126
7. Jozsa, R.: Embedding classical into quantum computation. In: Proceedings of MMICS'08. (2008) 43–49 arXiv:quant-ph 0812.4511.
8. Bacon, D., van Dam, W., Russell, A.: Analyzing algebraic quantum circuits using exponential sums. http://www.cs.ucsb.edu/ vandam/LeastAction.pdf (2008)
9. Clark, P.: The Chevalley-Warning theorem (featuring...the Erdős-Ginsburg-Ziv theorem). http://math.uga.edu/ pete/4400ChevalleyWarning.pdf (2010)
10. Williams, R.: Non-uniform ACC lower bounds. In: Proc. 26th Annual IEEE Conference on Computational Complexity. (2011) 231–240
11. Shor, P.W.: Fault-tolerant quantum computation. In: Proceedings of the 37th Annual IEEE Symposium on Foundations of Computer Science. (1996) 56–65