# On Tractable Exponential Sums

Jin-Yi Cai[1,⋆], Xi Chen[2,⋆⋆], Richard Lipton[3], and Pinyan Lu[4]

[1] University of Wisconsin-Madison
jyc@cs.wisc.edu
[2] University of Southern California
csxichen@gmail.com
[3] Georgia Institute of Technology
richard.lipton@cc.gatech.edu
[4] Microsoft Research Asia
pinyanl@microsoft.com

**Abstract.** We consider the problem of evaluating certain exponential sums. These sums take the form

$$\sum_{x_1,x_2,\ldots,x_n \in \mathbb{Z}_N} e^{\frac{2\pi i}{N} f(x_1,x_2,\ldots,x_n)},$$

where each $x_i$ is summed over a ring $\mathbb{Z}_N$, and $f(x_1, x_2, \ldots, x_n)$ is a multivariate polynomial with integer coefficients. We show that the sum can be evaluated in polynomial time in $n$ and $\log N$ when $f$ is a quadratic polynomial. This is true even when the factorization of $N$ is unknown. Previously, this was known for a prime modulus $N$. On the other hand, for very specific families of polynomials of degree $\geq 3$ we show the problem is #P-hard, even for any fixed prime or prime power modulus. This leads to a complexity dichotomy theorem — a complete classification of each problem to be either computable in polynomial time or #P-hard — for a class of exponential sums. These sums arise in the classifications of graph homomorphisms and some other counting CSP type problems, and these results lead to complexity dichotomy theorems. For the polynomial-time algorithm, Gauss sums form the basic building blocks; for the hardness result we prove group-theoretic necessary conditions for tractability.

## 1 Introduction

Exponential sums are among the most studied objects in Number Theory [1,2,3]. They have fascinating properties and innumerable applications. Recently they have also played a pivotal role in the study of computational complexity of graph homomorphisms [4,5].

⋆ Supported by NSF CCF-0830488 and CCF-0914969.

⋆⋆ Most of the work done while the author was a postdoc at the Institute for Advanced Study and Princeton University. Supported by Grants CCF-0832797, DMS-0635607, and the USC Viterbi School of Engineering Startup Fund (from Shang-Hua Teng).

D.T. Lee, D.Z. Chen, and S. Ying (Eds.): FAW 2010, LNCS 6213, pp. 148–159, 2010.

The most fundamental and well-known among exponential sums are those named after Gauss. Let $p$ be an odd prime, and $\omega_p = e^{2\pi i/p}$ be the $p$-th primitive root of unity. Then the Gauss sum over $\mathbb{Z}_p$ is

$$G = \sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right) \omega_p^t, \quad \text{where } \left(\frac{t}{p}\right) \text{ is the Legendre symbol.} \tag{1}$$

In this paper, we will need to use a more general form of the Gauss sum which will be defined later in Section 1. Another well-known expression for $G$ in (1) is

$$G = \sum_{x \in \mathbb{Z}_p} \left(\omega_p\right)^{x^2}.$$

Gauss also knew the remarkable equality $G^2 = (-1)^{(p-1)/2} p$; i.e.,

$$G = \pm\sqrt{p} \quad \text{if } p \equiv 1 \pmod 4, \quad \text{and} \quad G = \pm i\sqrt{p} \quad \text{if } p \equiv 3 \pmod 4. \tag{2}$$

In particular, we have $|G| = \sqrt{p}$, which is an expression that the $p$ terms in the sum $G$ are somewhat "randomly" distributed on the unit circle (but note that the equality is exact). However, the truly amazing fact is that, in all cases, the plus sign (+) always holds in (2). Gauss recorded this conjecture in his diary in May 1801, and on August 30, 1805 Gauss recorded that a proof of the "very elegant theorem mentioned in 1801" had finally been achieved.

In this paper we consider the computational complexity of evaluating exponential sums of the form

$$Z(N, f) = \sum_{x_1, x_2, \ldots, x_n \in \mathbb{Z}_N} e^{\frac{2\pi i}{N} f(x_1, x_2, \ldots, x_n)},$$

where each $x_i$ is summed over a ring $\mathbb{Z}_N$ and $f(x_1, x_2, \ldots, x_n)$ is a multivariate polynomial with integer coefficients. The output of the computation is an algebraic number, in the cyclotomic field $\mathbb{Q}(e^{2\pi i/N})$. Any canonical representation of the output algebraic number will be acceptable [6,7]. These sums are natural generalizations of the sums considered by Gauss and with arbitrary polynomials $f$, they have also played important roles in the development of number theory.

Our main results are as follows: We show that the sum $Z(N, f)$ can be evaluated in polynomial time when $f$ is a quadratic polynomial. The computational complexity is measured in terms of $n$, $\log N$, and the number of bits needed to describe $f$. While it is known that $Z(N, f)$ can be computed efficiently when $N$ is a prime [8], our algorithm works for any composite modulus $N$, even without knowing its prime factorization. On the other hand, for very specific families of polynomials of degree $\geq 3$, we show the problem is #P-hard even for any fixed prime or prime power modulus. This leads to a complexity dichotomy theorem — a complete classification of each problem to be either computable in polynomial time or #P-hard — for a class of exponential sums.

For the polynomial-time algorithm, we employ an iterative process to eliminate one variable at a time. Gauss sums form the basic building blocks. The fact that we know the exact answer to the Gauss sum, *including the sign*, is crucial.

It turns out that the situation is different for an odd or an even modulus $N$. A natural idea is to deal with each prime power in the modulus $N$ separately, and combine the answers by Chinese remaindering. It turns out that the algorithm is more difficult for a modulus which is a power of 2, than for an odd prime power. A more fundamental difficulty arises when $N$ is large and its prime factorization is unknown. We overcome this difficulty as follows: (1) Factor out all powers of 2 in $N$ and deal with it separately. (2) Operate in the remaining odd modulus *as if it were* an odd prime power; whenever this operational commingling encounters an obstacle, we manage to discover a non-trivial factorization of the modulus $N$ into relatively prime parts. In that case we recurse.

**Theorem 1.** *Let $N$ be any positive integer and $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a quadratic polynomial in $n$ variables $x_1, \ldots, x_n$. Then the sum $Z(N, f)$ can be evaluated in polynomial time in $n$, $\log N$, and the number of bits needed to describe $f$.*

Previously, it was known that for quadratic polynomials $f$, the sum can be computed in polynomial time, if $N$ is a prime [8]. An algorithm with running time $O(n^3)$ can also be found in the paper by Ehrenfeucht and Karpinski [9]. Compared to these algorithms, ours works for any $N$ even if it is given as a part of the input and its factorization is unknown. It was also suggested that there is a reduction from root counting. One can express the sum as

$$\sum_{k=0}^{N-1} \#[f = k] \cdot e^{2\pi i k/N}.$$

If $N$ is polynomially bounded and if one can compute $\#[f = k]$ for all $k$, then one can compute the sum. But this works only when $N$ is small. Our results are for general $N$ (polynomial time in the length $\log N$). In our algorithm, Gauss sums play a crucial role. Any claim to the contrary amounts to an independent proof of Gauss's sign formula (that "very elegant theorem mentioned in 1801"), since it is not only a crucial building block of our algorithm, but also a special case of the algorithm. We also note that our treatment for the case when $N$ is a power of 2 is significantly different than previous work. No simple adaptation of ideas from Sylvester's law of inertia seems to work.

For the hardness part, we give several successively more stringent necessary conditions for a class of polynomials to be tractable. The first necessary condition involves the rank of an associated matrix, and the proof uses the widely applicable dichotomy theorem of Bulatov and Grohe [10] on counting graph homomorphisms over non-negative weighted graphs. The second condition involves linear independence and orthogonality. The third and much more stringent necessary condition is group-theoretic in nature; it asserts that the set of row vectors of a certain complex matrix must form a group. In the paper [4], Goldberg et al. had proved a similar condition for $\{-1, +1\}$-matrices, in the study of graph homomorphisms over real weighted graphs. Finally, in subsection 4.1, we give a Generalized Group Condition which leads to a complexity dichotomy.

Previously, it was shown by Ehrenfeucht and Karpinski [9] that for any fixed prime $N$, the problem of computing $Z(N, f)$ for general cubic polynomials $f$ is #P-hard [9]. However, our tests in Section 4 are more powerful. They allow us

to prove the #P-hardness of $Z(N, f)$ even if $f$ belongs to some very restricted families of polynomials, since they fail one of the tests in Section 4.

These sums arise recently in the classifications of graph homomorphisms as well as some other counting CSP type problems (include both CSP and Holant Problems). For example, the special case when $N = 2$ is a key component of the dichotomy of Goldberg et al. [4] for graph homomorphisms over real weighted graphs. It implies that the partition function $Z_{\mathbf{H}}(\cdot)$ (see the definition in section 4) with $H_{1,1} = H_{1,2} = H_{2,1} = 1$ and $H_{2,2} = -1$, which has been an obstacle to the dichotomy theorem of Bulatov and Grohe [10] and was left open for some time, can actually be computed in polynomial time.

**Preliminaries**

Let $\omega_N = e^{2\pi i/N}$ denote the $N$-th primitive root of unity. Let $N = N_1 \cdot N_2$ be a non-trivial factorization, namely $N_1, N_2 > 1$. Suppose $N_1$ and $N_2$ are relatively prime, then there exist integers $a$ and $b$ such that $bN_1 + aN_2 = 1$. It follows that

$$Z(N, f) = Z(N_1, af) \cdot Z(N_2, bf). \tag{3}$$

Therefore, if we know a non-trivial factorization of $N$ into relatively prime factors $N_1$ and $N_2$, then the problem $Z(N, f)$ decomposes. In particular, we can factor $N = 2^k N'$, where $N'$ is odd. Thus we can treat the problems $Z(2^k, \cdot)$ and $Z(N', \cdot)$ separately. In Section 2, we give an algorithm for the case when $N$ is odd and in Section 3 we deal with the case when $N = 2^k$.

Our algorithm crucially relies on the fact that the following general form of Gauss sum $G(a,b)$ can be computed in polynomial time in $\log a$ and $\log b$, even without knowing their prime factorizations. Let $a, b$ be non-zero integers with $b > 0$ and $\gcd(a, b) = 1$. Then $G(a, b)$ denotes the following sum:

$$G(a, b) = \sum_{x \in \mathbb{Z}_b} \omega_b^{ax^2}.$$

The algorithm for computing $G(a, b)$ can be found in the full version [11].

## 2 Odd Modulus

First, we present a polynomial-time algorithm for the case when $N$ is odd. Let

$$f(x_1, \ldots, x_n) = \sum_{i \le j \in [n]} c_{i,j} x_i x_j + \sum_{i \in [n]} c_i x_i + c_0. \tag{4}$$

We may assume $c_0 = 0$ because it only contributes a constant factor to $Z(N, f)$. For each non-zero coefficient $c = c_{i,j}$ or $c_i$ of $f$, we compute the greatest common divisor $g = \gcd(N, c^{\lfloor \log_2 N \rfloor})$. Note that if $\mathrm{ord}_p N$ is the exact order of a prime $p$ in $N$, then $N \ge p^{\mathrm{ord}_p N}$ and thus $\mathrm{ord}_p N \le \lfloor \log_2 N \rfloor$. Hence if $c$ shares any prime $p$ with $N$, but not all the prime factors of $N$, then $g$ has the factor $p^{\mathrm{ord}_p N}$, and $N = g \cdot (N/g)$ is a non-trivial factorization of $N$ into two relatively prime factors. We can test for each non-zero $c = c_{i,j}$ or $c_i$ whether $N = g \cdot (N/g)$ gives us a non-trivial factorization of $N$ into two relatively prime factors.

By (3), if for some $c$, we did find such a factorization $N = N_1 \cdot N_2$, then the problem decomposes into two subproblems $Z(N_1, \cdot)$ and $Z(N_2, \cdot)$. There can be at most a linear number $\log_2 N$ many such subproblems, and a polynomial-time algorithm for each subproblem will give a polynomial-time algorithm for $Z(N, \cdot)$. Therefore, in the following we assume for each non-zero coefficient $c = c_{i,j}$ or $c_i$, either $\gcd(N, c) = 1$ or $c$ has all prime factors of $N$, and we know, by computing the gcd, which case it is for each coefficient $c$. We consider the following cases.

**Case 1.** There exists some diagonal coefficient $c_{i,i}$ relatively prime to $N$.

Without loss of generality we assume $c_{1,1}$ is relatively prime to $N$. Then $c_{1,1}$ is invertible in $\mathbb{Z}_N$. Since $N$ is odd, 2 is also invertible. Denote by $c'_{1,i}$ an integer such that $c'_{1,i} \equiv (2c_{1,1})^{-1} c_{1,i} \pmod N$, for $2 \le i \le n$. We have, modulo $N$,

$$f(x_1, \ldots, x_n) = c_{1,1}\left[x_1^2 + 2x_1(c'_{1,2}x_2 + \ldots + c'_{1,n}x_n)\right] + \textstyle\sum_{2 \le i \le j \le n} c_{i,j}x_ix_j + \sum_{i \in [n]} c_i x_i.$$

Let $g(x_2, \ldots, x_n) = c'_{1,2}x_2 + \ldots + c'_{1,n}x_n$. Then we can write $f$ as

$$f = c_{1,1}(x_1 + g)^2 + c_1(x_1 + g) + h,$$

where $h$ is some quadratic polynomial in $x_2, \ldots, x_n$. If we substitute $y = x_1 + g$ for $x_1$, then for any fixed $x_2, \ldots, x_n \in \mathbb{Z}_N$, when $x_1$ takes all the values in $\mathbb{Z}_N$, $y$ also takes all the values in $\mathbb{Z}_N$. Hence, we have

$$Z(N, f) = \sum_{x_2, \ldots, x_n \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} \omega_N^{c_{1,1}y^2 + c_1 y + h(x_2, \ldots, x_n)}.$$

Completing the square again, $c_{1,1}y^2 + c_1 y = c_{1,1}(y + (2c_{1,1})^{-1}c_1)^2 + c'$, where

$$c' = -c_1^2/(4c_{1,1}) \in \mathbb{Z}_N \quad \text{and} \quad Z(N, f) = \sum_{x_2, \ldots, x_n \in \mathbb{Z}_N} \sum_{z \in \mathbb{Z}_N} \omega_N^{c_{1,1}z^2 + h'(x_2, \ldots, x_n)},$$

where $h'(x_2, \ldots, x_n) = h(x_2, \ldots, x_n) + c'$ is an explicitly computed quadratic polynomial in $x_2, \ldots, x_n$. It then follows that $Z(N, f) = Z(N, h') \cdot G(c_{1,1}, N)$, where $h'$ has (at least) one fewer variable than $f$ and the Gauss sum $G(c_{1,1}, N)$ can be computed in polynomial time. This completes the proof of Case 1.

**Case 2.** No $c_{i,i}$ is relatively prime to $N$ but there exist some $i, j : 1 \le i < j \le n$ such that $\gcd(c_{i,j}, N) = 1$. By our earlier assumption, for every prime factor $p$ of $N$, $p$ divides every $c_{i,i}$ for all $1 \le i \le n$.

The existence of $c_{i,j}$ for some $i, j : 1 \le i < j \le n$ implies that in particular $n \ge 2$. Without loss of generality, we assume $\gcd(c_{1,2}, N) = 1$. Now we perform the following substitution: $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, and $x_i$ are unchanged for any $2 < i \le n$ if $n > 2$. This transformation is a 1-1 correspondence from $\mathbb{Z}_N^n$ to itself with inverse $y_1 = (x_1 + x_2)/2$ and $y_2 = (x_1 - x_2)/2$ because 2 is invertible in $\mathbb{Z}_N$. Since the transformation is linear it does not change the degree of $f$. It is easily checked that the coefficient of $y_1^2$ in the new polynomial is $c_{1,1} + c_{2,2} + c_{1,2}$. Since $c_{1,1}$ and $c_{2,2}$ have all the prime factors of $N$, $c_{1,1} + c_{2,2} + c_{1,2}$ is relatively prime to $N$. This transformation reduces the computation of $Z(N, f)$ to Case 1.

**Case 3.** No coefficients $c_{i,j}$ of $f$, where $1 \le i \le j \le n$, are relatively prime to $N$. However, there exists a $c_i$ relatively prime to $N$, for some $i : 1 \le i \le n$. Without loss of generality, assume $\gcd(c_1, N) = 1$. Let $p$ be a prime divisor of $N$, then

$$p \mid c_{1,1}, \ldots, c_{1,n} \quad \text{and yet} \quad p \nmid c_1. \tag{5}$$

Let $k = \mathrm{ord}_p N$ be the exact order of $p$ in $N$ with $k \ge 1$. Write $N = p^k N_1$, then $\gcd(p, N_1) = 1$, and for some integers $a$ and $b$, we have $bp^k + aN_1 = 1$. By (3), $Z(N, f) = Z(p^k, af) \cdot Z(N_1, bf)$. Note that $\gcd(a, p) = 1$. Hence the condition (5) for the coefficients of $f$ also holds for $af$. We will show $Z(p^k, af) = 0$. For notational simplicity, we will write below $f$ for $af$.

$$Z(p^k, f) = \sum_{x_2, \ldots, x_n \in \mathbb{Z}_{p^k}} \omega_{p^k}^{\sum_{2 \le i \le j \le n} c_{i,j} x_i x_j + \sum_{2 \le i \le n} c_i x_i} \sum_{x_1 \in \mathbb{Z}_{p^k}} \omega_{p^k}^{\sum_{1 \le i \le n} c_{1,i} x_1 x_i + c_1 x_1}.$$

We fix any $x_2, \ldots, x_n \in \mathbb{Z}_{p^k}$, and consider the inner sum over $x_1$. If $k = 1$, then all terms $c_{1,i} x_1 x_i$ disappear, and because $p \nmid c_1$, the inner sum is equal to 0.

Now suppose $k > 1$. We repeat the sum for $p$ times with $x^{(j)} = x_1 + j \cdot p^{k-1}$ where $0 \le j \le p - 1$. Then by (5), we have $c_{1,i} x_1 x_i \equiv c_{1,i} x^{(j)} x_i \pmod{p^k}$ and

$$\sum_{x_1 \in \mathbb{Z}_{p^k}} \omega_{p^k}^{\sum_{1 \le i \le n} c_{1,i} x_1 x_i + c_1 x_1} = \frac{1}{p} \sum_{x_1 \in \mathbb{Z}_{p^k}} \omega_{p^k}^{\sum_{1 \le i \le n} c_{1,i} x_1 x_i + c_1 x_1} \left( \sum_{j=0}^{p-1} \omega_p^{j c_1} \right).$$

By $p \nmid c_1$, the geometric sum $\sum_{j=0}^{p-1} \omega_p^{j c_1} = 0$. This finishes Case 3.

**Case 4.** No coefficients $c_{i,j}$ and $c_\ell$ of $f$, where $1 \le i \le j \le n$ and $1 \le \ell \le n$, are relatively prime to $N$.
By our earlier assumption, this means that every prime factor of $N$ divides every coefficient $c_{i,j}$ and $c_\ell$. Then we can find the joint gcd $d$ of $N$ with all these coefficients, which must at least contain every prime factor of $N$, and divide out $d$ in the exponent. By $\omega_N^d = \omega_{N/d}$, we get $Z(N, f) = d \cdot Z(N/d, f')$ where $f' = f/d$ is the quadratic polynomial obtained from $f$ by dividing every coefficient with $d$.This reduces the modulus from $N$ to $N/d$.

By combining all the four cases, we get a polynomial-time algorithm for the case when $N$ is odd.

## 3 Modulus Is a Power of 2

Next, we deal with the more difficult case when the modulus, denoted by $q$ here, is a power of 2: $q = 2^k$ for some $k \ge 1$. We note that the property of an element $c \in \mathbb{Z}_q$ being even or odd is well-defined.

For the case when $k = 1$, $Z(q, f)$ is computable in polynomial time by [8]. So we always assume $k > 1$ below. The algorithm goes as follows. For each round, we show how to, in polynomial time, either

1. output the correct value of $Z(q, f)$; or

2. construct a new quadratic polynomial $g \in \mathbb{Z}_{q/2}[x_1, \ldots, x_n]$ and reduce the computation of $Z(q, f)$ to the computation of $Z(q/2, g)$; or
3. construct a new quadratic polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_{n-1}]$, and reduce the computation of $Z(q, f)$ to the computation of $Z(q, g)$.

This gives us a polynomial-time algorithm for evaluating $Z(q, f)$ since we know how to solve the two base cases when either $k = 1$ or $n = 0$ efficiently.

Suppose we have a polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ as in (4). Our first step is to transform $f$ so that all the coefficients of its cross terms ($c_{i,j}$, where $1 \le i < j \le n$) and linear terms ($c_i$) are even. Assume $f$ does not yet have this property. We let $t$ be the smallest index in $[n]$ such that one of $\{c_t, c_{t,j} : j > t\}$ is odd. By separating out the terms involving $x_t$, we rewrite $f$ as follows

$$f \;=\; c_{t,t} \cdot x_t^2 + x_t \cdot f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) + f_2(x_1, \ldots, \widehat{x_t}, \ldots, x_n), \tag{6}$$

where $f_1$ is an affine linear function and $f_2$ is a quadratic polynomial. Both $f_1$ and $f_2$ here are over variables $\{x_1, \ldots, x_n\} - \{x_t\}$. Here the notation $\widehat{x_t}$ means that $x_t$ does not appear in the polynomial. Moreover

$$f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) \;=\; \textstyle\sum_{i<t} c_{i,t} x_i + \sum_{j>t} c_{t,j} x_j + c_t. \tag{7}$$

By the minimality of $t$, $c_{i,t}$ is even for all $i < t$ and at least one of $\{c_t, c_{t,j} : j > t\}$ is odd. We claim that

$$Z(q, f) \;=\; \sum_{x_1, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, \ldots, x_n)} \;=\; \sum_{\substack{x_1, \ldots, x_n \in \mathbb{Z}_q \\ f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) \equiv 0 \bmod 2}} \omega_q^{f(x_1, \ldots, x_n)}. \tag{8}$$

This is because

$$\sum_{\substack{x_1, \ldots, x_n \in \mathbb{Z}_q \\ f_1 \equiv 1 \bmod 2}} \omega_q^{f(x_1, \ldots, x_n)} \;=\; \sum_{\substack{x_1, \ldots, \widehat{x_t}, \ldots, x_n \in \mathbb{Z}_q \\ f_1 \equiv 1 \bmod 2}} \; \sum_{x_t \in \mathbb{Z}_q} \omega_q^{c_{t,t} x_t^2 + x_t f_1 + f_2}.$$

However, for any fixed $x_1, \ldots, \widehat{x_t}, \ldots, x_n$, the inner sum is equal to $\omega_q^{f_2}$ times

$$\sum_{x_t \in [0 : 2^{k-1} - 1]} \omega_q^{c_{t,t} x_t^2 + x_t f_1} + \omega_q^{c_{t,t}(x_t + 2^{k-1})^2 + (x_t + 2^{k-1}) f_1} = \left(1 + (-1)^{f_1}\right) \sum_{x_t} \omega_q^{c_{t,t} x_t^2 + x_t f_1} = 0,$$

since $f_1 \equiv 1 \bmod 2$. Note that we used $(x + 2^{k-1})^2 \equiv x^2 \pmod{2^k}$ when $k > 1$ in the first equation.

Recall that $f_1$ (see (7)) is an affine linear form of $\{x_1, \ldots, \widehat{x_t}, \ldots, x_n\}$. Also note that $c_{i,t}$ is even for all $i < t$ and one of $\{c_t, c_{t,j} : j > t\}$ is odd. We consider the following two cases.

In the first case, $c_{t,j}$ is even for all $j > t$ and $c_t$ is odd, then $f_1$ is odd for any assignment $(x_1, \ldots, \widehat{x_t}, \ldots, x_n)$ in $\mathbb{Z}_q^{n-1}$. As a result, $Z(q, f) = 0$ by (8).

In the second case, there exists at least one $j > t$ such that $c_{t,j}$ is odd. Let $\ell > t$ be the smallest of such $j$'s. Then we substitute the variable $x_\ell$ in $f$ with a new variable $x'_\ell$, where (as $c_{t,\ell}$ is odd, $c_{t,\ell}$ is invertible in $\mathbb{Z}_q$)

$$x_\ell \;=\; c_{t,\ell}^{-1} \left(2x'_\ell - \left(\textstyle\sum_{i<t} c_{i,t} x_i + \sum_{j>t, j \neq \ell} c_{t,j} x_j + c_t\right)\right). \tag{9}$$

and let $f'$ denote the new quadratic polynomial in $\mathbb{Z}_q[x_1, \ldots, x_{\ell-1}, x'_\ell, x_{\ell+1}, \ldots, x_n]$. We claim that

$$Z(q, f') = 2 \cdot Z(q, f) = 2 \cdot \sum_{\substack{x_1, \ldots, x_n \in \mathbb{Z}_q \\ f_1 \equiv 0 \bmod 2}} \omega_q^{f(x_1, \ldots, x_n)}.$$

To this end, we define the following map from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^n$: $(x_1, \ldots, x'_\ell, \ldots, x_n) \mapsto (x_1, \ldots, x_\ell, \ldots, x_n)$, where $x_\ell$ satisfies (9). It is easy to check that the range of this map is exactly the set of $(x_1, \ldots, x_\ell, \ldots, x_n)$ in $\mathbb{Z}_q^n$ such that $f_1$ is even. Moreover, for every such tuple $(x_1, \ldots, x_\ell, \ldots, x_n)$ the number of its preimages in $\mathbb{Z}_q^n$ is exactly 2. The claim then follows.

As a result, to compute $Z(q, f)$, we only need to compute $Z(q, f')$, and the advantage of the new polynomial $f'$ over $f$ is the following property. The proof of Property 1 can be found in the full version [11].

*Property 1.* For every cross and linear term that involves $x_1, \ldots, x_t$, its coefficient in $f'$ is even.

To summarize, after substituting $x_\ell$ with $x'_\ell$ using (9), we obtain a quadratic polynomial $f'$ such that $Z(q, f') = 2 \cdot Z(q, f)$ and for all cross and linear terms that involve $x_1, \ldots, x_t$, its coefficient in $f'$ is even. We can repeat this substitution procedure on $f'$: either we show that $Z(q, f')$ is trivially 0 or we get a quadratic polynomial $f''$ such that $Z(q, f'') = 2 \cdot Z(q, f')$ and the parameter $t$ increases by at least one. As a result, given any quadratic polynomial $f$, we can, in polynomial time, either show that $Z(q, f)$ is 0 or construct a new quadratic polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_n]$ such that $Z(q, f) = 2^d \cdot Z(q, g)$ for some known integer $d \leq n$, and every cross term and linear term of $g$ has an even coefficient.

For notational simplicity, we can just assume that the given $f$ in (4) already satisfies this condition. (Or equivalently, we rewrite $f$ for $g$.) We will show that, given such a polynomial $f$ in $n$ variables, we can reduce it either to the computation of $Z(q/2, f')$, in which $f'$ is a quadratic polynomial in $n$ variables; or to the computation of $Z(q, f'')$, in which $f''$ is a quadratic polynomial in $n-1$ variables. We consider the following two cases: $c_{i,i}$ is even for all $i \in [n]$; or at least one of the $c_{i,i}$'s is odd.

In the first case, we know $c_{i,j}$ and $c_i$ are even for all $1 \leq i \leq j \leq n$. We use $c'_{i,j}$ and $c'_i$ to denote integers in $[0 : 2^{k-1} - 1]$ such that $c_{i,j} \equiv 2c'_{i,j} \pmod q$ and $c_i \equiv 2c'_i \pmod q$, respectively. Then,

$$Z(q, f) = \omega_q^{c_0} \cdot \sum_{x_1, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{2\left(\sum_{i \leq j \in [n]} c'_{i,j} x_i x_j + \sum_{i \in [n]} c'_i x_i\right)} = 2^n \cdot \omega_q^{c_0} \cdot Z(2^{k-1}, f'),$$

where

$$f' = \textstyle\sum_{i \leq j \in [n]} c'_{i,j} x_i x_j + \sum_{i \in [n]} c'_i x_i$$

is a quadratic polynomial over $\mathbb{Z}_{q/2} = \mathbb{Z}_{2^{k-1}}$. This reduces the computation of $Z(q, f)$ to $Z(q/2, f')$.

In the second case, without loss of generality, we assume $c_{1,1}$ is odd, then

$$f = c_{1,1}(x_1^2 + 2x_1 f_1) + f_2 = c_{1,1}(x_1 + f_1)^2 + f',$$

where $f_1$ is an affine linear form, and both $f_2$ and $f'$ are quadratic polynomials, all of which are over $x_2, \ldots, x_n$. We are able to do this because $c_{1,j}$ and $c_1$, for all $j \geq 2$, are even. Now we have

$$Z(q,f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{c_{1,1}(x_1+f_1)^2+f'} = \sum_{x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f'} \cdot \sum_{x_1 \in \mathbb{Z}_q} \omega_q^{c_{1,1}(x_1+f_1)^2} = G(c_{1,1},q) \cdot Z(q,f').$$

The last equation is because the sum over $x_1 \in \mathbb{Z}_q$ is independent of the value of $f_1$. This reduces the computation of $Z(q,f)$ to $Z(q,f')$, and $f'$ is a quadratic polynomial in $n-1$ variables.

To sum up, given any quadratic $f$, we can, in polynomial time, either output the correct value of $Z(q,f)$; or reduce one of the two parameters, $k$ or $n$, by at least 1. This gives us a polynomial-time algorithm for $Z(q,f)$ when $q = 2^k$.

## 4 #P-Hardness

We first introduce the definition of a *partition function* $Z_{\mathbf{A}}(\cdot)$ [12,13,14,10,15], where $\mathbf{A}$ is a symmetric complex matrix. We give four necessary conditions on the matrix $\mathbf{A}$ for the problem of computing $Z_{\mathbf{A}}(\cdot)$ being *not* #P-hard. Then we demonstrate the wide applicability of these four conditions by reducing $Z_{\mathbf{A}}(\cdot)$, for some appropriate $\mathbf{A}$, to $Z(N,f)$ and proving that even computing $Z(N,f)$ for some very restricted families of polynomials over a fixed modulus $N$ is #P-hard. Finally, we show that, for a large class of problems defined using $Z(N,f)$, these conditions actually cover all the #P-hard cases. Together with the polynomial-time algorithm presented in Section 2 and 3, they imply an explicit complexity dichotomy theorem for this class.

Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric $m \times m$ matrix, then we define the partition function $Z_{\mathbf{A}}(\cdot)$ as follows: Given any undirected graph $G = (V,E)$ (Here $G$ is allowed to have multi-edges but no self loops)

$$Z_{\mathbf{A}}(G) = \sum_{\xi: V \to [m]} \mathrm{wt}_{\mathbf{A}}(G,\xi), \quad \text{where} \quad \mathrm{wt}_{\mathbf{A}}(G,\xi) = \prod_{(u,v) \in E} A_{\xi(u),\xi(v)}. \tag{10}$$

The complexity of $Z_{\mathbf{A}}(\cdot)$, for various $\mathbf{A}$, has been studied intensely [12,13,14,10,15]. We need the following lemma which can be proved following an important result of Bulatov and Grohe [10]. The proof uses the technique of Valiant [16,17] called interpolation, which is omitted here.

**Lemma 1 (The Rank-1 Condition).** *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric matrix and let $\mathbf{A}'$ be the matrix such that $A'_{i,j} = |A_{i,j}|$ for all $i,j$. If there exists a $2 \times 2$ sub-matrix $\mathbf{B}$ of $\mathbf{A}'$, such that, $\mathbf{B}$ is of full rank and at least three of the four entries of $\mathbf{B}$ are non-zero, then computing $Z_{\mathbf{A}}(\cdot)$ is* #P-hard.

We can use lemma 1 to prove a stronger necessary condition for $Z_{\mathbf{A}}(\cdot)$ being *not* #P-hard. The proof can be found in the full version [11]. In the statement below, we let $\mathbf{A}_{i,*}$ denote the $i$-th row vector of $\mathbf{A}$. We say a matrix $\mathbf{A}$ is *$M$-discrete*, for some integer $M \geq 1$, if every entry of $\mathbf{A}$ is an $M$-th root of unity.

**Lemma 2 (Orthogonality).** *Let $M$ be a positive integer and let $\mathbf{A}$ be a symmetric and* $M$-discrete *$m \times m$ matrix. If there exist $i \neq j \in [m]$ such that $\mathbf{A}_{i,*}$ and $\mathbf{A}_{j,*}$ are* neither *linearly dependent* nor *orthogonal, then $Z_{\mathbf{A}}(\cdot)$ is* #P-hard.

Next we prove a much stronger *group-theoretic* necessary condition for $Z_{\mathbf{A}}(\cdot)$ being not #P-hard, where $\mathbf{A}$ is any *discrete unitary matrix* as defined below. A similar condition was first used by Goldberg et al. in [4] for $\{+1, -1\}$-matrices, in the study of $Z_{\mathbf{A}}(\cdot)$ over real matrices. In the rest of this section, we will use $[0 : m-1]$ to index the rows and columns of an $m \times m$ matrix for convenience.

**Definition 1 (Discrete Unitary Matrix).** *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be an $m \times m$ symmetric complex matrix. We say $\mathbf{A}$ is an* $M$-discrete unitary matrix*, for some positive integer $M$, if it is* $M$-discrete *and satisfies*

— $\forall\, i \in [0 : m-1]$, $A_{1,i} = A_{i,1} = 1$; $\forall\, i \neq j$, $\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*} \rangle = 0$, *where*

$$\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*} \rangle = \sum_{k \in [m]} \mathbf{A}_{i,k} \overline{\mathbf{A}_{j,k}}.$$

Given two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{C}^m$ we let $\mathbf{x} \circ \mathbf{y}$ denote their Hadamard product $\mathbf{z}$: $\mathbf{z} = \mathbf{x} \circ \mathbf{y} \in \mathbb{C}^m$, where $z_i = x_i \cdot y_i$ for all $i$.

**Lemma 3 (The Group Condition).** *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be an $m \times m$ symmetric $M$-discrete unitary matrix, for some positive integer $M$. Then computing $Z_{\mathbf{A}}(\cdot)$ is #P-hard, unless $\mathbf{A}$ satisfies the following* Group Condition*:*

— $\forall\, i, j \in [0 : m-1]$, $\exists\, k \in [0 : m-1]$ *such that* $\mathbf{A}_{k,*} = \mathbf{A}_{i,*} \circ \mathbf{A}_{j,*}$.

These three necessary conditions are very powerful and can be used to prove the #P-hardness of $Z(N, f)$, for some very restricted families of polynomials $f$ over a fixed modulus $N$. We would like to say, e.g., evaluating $Z(N, f)$, when $f$ contains terms $x_1x_2x_3$, is #P-hard. However, we have to be very careful; such complexity-theoretic statements are only meaningful for a sequence of polynomials, and not an individual polynomial. This motivates the following definition. Let $h \in \mathbb{Z}[x_1, \ldots, x_r]$ be a fixed polynomial (e.g., $h = x_1x_2x_3$, with $r = 3$). We say $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is an *$h$-type* polynomial, if there exists an $r$-uniform hypergraph $G = (V, E)$ with $V = [n]$ such that (We allow $G$ to have multi-edges, i.e., $E$ is a multiset; and edges in $E$ are *ordered* subsets of $[n]$ of cardinality $r$)

$$f(x_1, \ldots, x_n) = \sum_{(i_1, \ldots, i_r) \in E} h(x_{i_1}, \ldots, x_{i_r}). \tag{11}$$

**Definition 2.** *Let $q = p^t$ be a prime power and $h \in \mathbb{Z}[x_1, \ldots, x_r]$ be a polynomial. We use $\mathcal{S}[q, h]$ to denote the following problem: given an $r$-uniform hypergraph $G$, compute $Z(q, f)$, where $f$ is the* $h$-type polynomial *defined by $G$.*

Using these three necessary conditions, it is easy to prove the #P-hardness of the following problems, with

$$h_1(x_1, x_2, x_3) = x_1x_2x_3, \quad h_2(x_1, x_2) = x_1^2x_2 \quad \text{and} \quad h_3(x_1, x_2) = x_1x_2 + x_1^2x_2^2.$$

**Corollary 1.** *For any fixed prime power $q = p^t$, $\mathcal{S}[q, h_1]$ is #P-hard; For any prime power $q \notin \{2, 4\}$, $\mathcal{S}[q, h_2]$ and $\mathcal{S}[q, h_3]$ are #P-hard.*

*Proof.* We will only prove the statement for $\mathcal{S}[q, h_3]$ here. For $\mathcal{S}[q, h_3]$, let $\mathbf{A}$ be the following $m \times m$ symmetric and $q$-discrete matrix:

$$A_{i,j} = \omega_q^{h_3(i,j)}, \qquad \text{for all } i, j \in [0 : q - 1]. \tag{12}$$

It is easy to see that $Z_{\mathbf{A}}(\cdot)$ is computationally equivalent to $\mathcal{S}[q, h_3]$. Moreover, when $q$ is an odd prime power, the two vectors $\mathbf{A}_{0,*}$ and $\mathbf{A}_{1,*}$ are neither linearly dependent nor orthogonal and thus, by Lemma 2, $\mathcal{S}[q, h_3]$ is #P-hard. For the case when $q = 2^t$ and $t > 2$, it can be checked that $\mathbf{A}$ is $q$-discrete unitary but does not satisfy the Group Condition. Then by Lemma 3, $\mathcal{S}[q, h_3]$ is #P-hard.

### 4.1 A Dichotomy Theorem for $\mathcal{S}[q, h]$

Let $q$ be a prime power, and $h \in \mathbb{Z}_q[x_1, x_2]$ be a symmetric polynomial. By the proof of Corollary 1 above, the problem $\mathcal{S}[q, h]$ is computationally equivalent to $Z_{\mathbf{A}}(\cdot)$, where $\mathbf{A}$ is the following $q \times q$ and $q$-discrete matrix:

$$A_{i,j} = \omega_q^{h(i,j)}, \qquad \text{for all } i, j \in [0 : q - 1]. \tag{13}$$

Although the Orthogonality and the Group conditions can be used to prove the #P-hardness of $\mathcal{S}[q, h]$ for many interesting polynomials $h$, as demonstrated in Corollary 1, it does not cover all the #P-hard $\mathcal{S}[q, h]$. For example, even if we assume that $h$ is symmetric; and every monomial in $h(x_1, x_2)$ contains both $x_1$ and $x_2$ (and thus, $h(0, x) = h(x, 0) = 0$ for all $x \in \mathbb{Z}_q$ and the matrix $\mathbf{A}$ defined in (13) is both symmetric and *normalized*: $A_{0,i} = A_{i,0} = 1$ for all $i$), the Group condition can not deal with the case when there exist indices $i \neq j \in [0 : q - 1]$ such that $\mathbf{A}_{i,*} = \mathbf{A}_{j,*}$. We will use $\mathcal{C}$ to denote this class of problems.

We can prove a stronger theorem — the fourth condition. It is a *strengthening* of the current Group condition, leading to a complexity dichotomy theorem for the class $\mathcal{C}$. Due to the space limit, we omit its proof here.

**Lemma 4 (The Generalized Group Condition).** *Let $\mathbf{A}$ be an $m \times m$ symmetric, normalized and $M$-discrete matrix for some positive integer $M$ such that for all $i, j \in [0 : m - 1]$, either $\mathbf{A}_{i,*} = \mathbf{A}_{j,*}$ or $\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*} \rangle = 0$. Let $T_1, \ldots, T_\ell$ be a partition of $[0 : m - 1]$, such that, $\mathbf{A}_{i,*} = \mathbf{A}_{j,*} \iff \exists\, k \in [\ell] : i, j \in T_k$. Then $Z_{\mathbf{A}}(\cdot)$ is #P-hard unless $\mathbf{A}$ satisfies the following* Generalized *Group condition:*

— *For all $k \in [\ell]$, $|T_k| = m/\ell$;* and *for all $i, j \in [0 : m - 1]$, there exists a $k \in [0 : m - 1]$ such that $\mathbf{A}_{k,*} = \mathbf{A}_{i,*} \circ \mathbf{A}_{j,*}$.*

By combining the Generalized Group condition with the Orthogonality condition, we are able to show that for every problem $\mathcal{S}[q,h]$ in the class $\mathcal{C}$, either $\mathcal{S}[q,h]$ is #P-hard; or we have $\mathbf{A} = \mathbf{J} \otimes \mathbf{A}'$, where $\mathbf{J}$ is an all-1 matrix and $\mathbf{A}'$ is a $q$-discrete unitary matrix that satisfies the original Group Condition. The latter can ultimately lead to a polynomial-time algorithm for $Z_{\mathbf{A}}(\cdot)$ and $\mathcal{S}[q,h]$, using the algorithm developed in Section 2 and 3.

**Acknowledgements.** We thank Eric Bach, Richard Brualdi, Michael Kowalczyk, Endre Szemeredi and Mingji Xia for helpful discussions.

## References

1. Lang, S.: Algebraic Number Theory. Addison-Wesley, Reading (1970)
2. Hua, L.: Introduction to Number Theory. Springer, Heidelberg (1982)
3. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Springer, Heidelberg (1998)
4. Goldberg, L., Grohe, M., Jerrum, M., Thurley, M.: A complexity dichotomy for partition functions with mixed signs. In: Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science, pp. 493–504 (2009)
5. Cai, J.Y., Chen, X., Lu, P.: Graph homomorphisms with complex values: A dichotomy theorem. In: Proceedings of the 37th International Colloquium on Automata, Languages and Programming (2010)
6. Grabmeier, J., Kaltofen, E., Weispfenning, V.: Computer Algebra Handbook. Springer, Heidelberg (2003)
7. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (2003)
8. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
9. Ehrenfeucht, A., Karpinski, M.: The computational complexity of (XOR, AND)-counting problems. University of Bonn (1990)
10. Bulatov, A., Grohe, M.: The complexity of partition functions. Theoretical Computer Science 348(2), 148–186 (2005)
11. Cai, J.-Y., Chen, X., Lipton, R., Lu, P.: On tractable exponential sums. arXiv (1005.2632) (2010)
12. Lovász, L.: Operations with structures. Acta Mathematica Hungarica 18, 321–328 (1967)
13. Dyer, M., Greenhill, C.: The complexity of counting graph homomorphisms. In: Proceedings of the 9th International Conference on Random Structures and Algorithms, pp. 260–289 (2000)
14. Freedman, M., Lovász, L., Schrijver, A.: Reflection positivity, rank connectivity, and homomorphism of graphs. Journal of the American Mathematical Society 20, 37–51 (2007)
15. Dyer, M.E., Goldberg, L.A., Paterson, M.: On counting homomorphisms to directed acyclic graphs. Journal of the ACM 54(6) (2007)
16. Valiant, L.G.: The complexity of enumeration and reliability problems. SIAM Journal on Computing 8(3), 410–421 (1979)
17. Valiant, L.: The complexity of computing the permanent. Theoretical Computer Science 8, 189–201 (1979)