Classical Simulation of Quantum Circuits by Half Gauss Sums

Classical Simulation of Quantum Circuits by Half Gauss Sums

CLASSICAL SIMULATION OF QUANTUM CIRCUITS BY HALF GAUSS SUMS

KAIFENG BU[*†] AND DAX ENSHAN KOH[‡¶§]

ABSTRACT. We give an efficient algorithm to evaluate a certain class of exponential sums, namely the periodic, quadratic, multivariate half Gauss sums. We show that these exponential sums become #P-hard to compute when we omit either the periodicity or quadraticity condition. We apply our results about these exponential sums to the classical simulation of quantum circuits, and give an alternative proof of the Gottesman-Knill theorem. We also explore a connection between these exponential sums and the Holant framework. In particular, we generalize the existing definition of affine signatures to arbitrary dimensions, and use our results about half Gauss sums to show that the Holant problem for the set of affine signatures is tractable.

CONTENTS

(†) SCHOOL OF MATHEMATICAL SCIENCES, ZHEJIANG UNIVERSITY, HANGZHOU, ZHEJIANG 310027, CHINA

(*) DEPARTMENT OF PHYSICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138, USA

(‡) DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139, USA

(¶) ZAPATA COMPUTING, INC., 100 FEDERAL STREET, 20TH FLOOR, BOSTON, MASSACHUSETTS 02110, USA

(§) INSTITUTE OF HIGH PERFORMANCE COMPUTING, AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH (A*STAR), 1 FUSIONOPOLIS WAY, #16-16 CONNEXIS, SINGAPORE 138632, SINGAPORE

E-mail addresses: kfbu@fas.harvard.edu (K.Bu), dax_koh@ihpc.a-star.edu.sg (D.E.Koh).

1. Introduction

Exponential sums have been extensively studied in number theory [1] and have a rich history that dates back to the time of Gauss [2]. They have found numerous applications in communication theory [3], graph theory [4], coding theory [5, 6], cryptography [5, 7], algorithms [5] and many other areas of applied mathematics.

More recently, they have also found useful applications in quantum computation. In 2005, Dawson et al. showed, using Feynman's sum-over-paths technique [8], that the amplitudes of quantum circuits with Toffoli and Hadamard gates can be expressed in terms of exponential sums [9]. Such an approach has complexity-theoretic applications. For example, by noting that the exponential sum can be expressed as a GapP-function, it can be used to show that the complexity class BQP is contained in PP, a result first proved by [10] using different methods.

The idea of using exponential sums to express quantum amplitudes has been developed further in a number of subsequent works [11–17]. For example, in [11], Bacon, van Dam and Russell find an exponential-sum representation of the amplitudes of algebraic quantum circuits. They then exploit the theory of exponential sums to prove several properties of such circuits. For instance, they prove that in the limit of large qudit degree, the acceptance probabilities of such circuits converge to either zero or one.

The use of exponential sums to express quantum amplitudes elucidates a correspondence between quantum circuits and low-degree polynomials, called the *circuit-polynomial correspondence* [13]. This correspondence allows results about polynomials to be used to prove results about quantum circuits, and vice versa. For example, this correspondence was exploited in the forward direction by [14], which provided an alternative proof of the Gottesman-Knill Theorem [18] for quopit Clifford circuits, i.e. Clifford circuits in odd prime dimensions [14], by showing that the amplitudes of such circuits can be expressed in terms of tractable exponential sums.

More generally, the circuit-polynomial correspondence also establishes a connection between exponential sums and the strong classical simulation of quantum circuits—deciding whether a class of quantum circuits is classically simulable, in many cases, can be reduced to the problem of deciding whether an exponential sum is tractable. This has important applications, for example, to the goal of quantum computational supremacy [19–21]—the intractability of an exponential sum can be used to show that the class of circuits it corresponds to cannot be efficiently simulated.

In this paper, we consider a generalization of the exponential sums used in the above examples. In particular, we introduce the periodic, quadratic, multivariate half Gauss sum, and show that these incomplete Gauss sums can be computed efficiently using number-theoretic techniques. Moreover, we show that these exponential sums can be used to express the amplitudes of qudit Clifford circuits, thereby providing an alternative proof of the Gottesman-Knill theorem for qudit

Clifford circuits. We also show that without the periodicity or quadraticity condition, these exponential sums become intractable, under plausible complexity assumptions.

Our work improves on existing results in a number of ways. First, while the results of [13] and [14] are restricted to qubit and quopit systems, respectively, our results hold for all d-level systems. In doing so, we address a limitation of the approach used in [14], where the proof of the Gottesman-Knill theorem works only for d-level systems, where d is restricted to be an odd prime. Second, while previous works on tractable exponential sums are based on Gauss sums [14, 22, 23], ours are based on half Gauss sums, which are a generalization of Gauss sums. Consequently, we find a larger class of tractable exponential sums compared to previous works. Third, we generalize the existing definition of affine signatures [22] to arbitrary dimensions, and use our results about half Gauss sums to show that the Holant problem for the set of affine signatures is tractable. Fourth, we demonstrate the importance of a periodicity condition, which has not been previously explored, to the classical simulation of quantum circuits.

The rest of the paper is structured as follows. In Section 1.1, we summarize the main results of our work. In Section 2, we define half Gauss sums and give an efficient classical algorithm to compute a subclass of these sums, namely the periodic, quadratic, multivariate half Gauss sums. In Section 3, we apply our results about half Gauss sums to Clifford circuits, and provide an alternative proof of the Gottesman-Knill Theorem. In Section 4, we study the hardness of evaluating half Gauss sums that do not satisfy either the periodicity condition or the quadraticity condition. In Section 5, we explore a connection between half Gauss sums and the Holant framework. We generalize the existing definition of affine signatures to arbitrary dimensions, and use our results about half Gauss sums to show that the Holant problem for the set of affine signatures is tractable.

1.1. **Our results.** The complexity of evaluating the exponential sum

$$Z(d,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d} \omega_d^{f(x_1,\ldots,x_n)}, \tag{1}$$

where $d,n\in\mathbb{Z}^+$ are positive integers, $\omega_d = \exp(2\pi i/d)$ is a dth root of unit, and $f(x_1,\ldots,x_n)$ is a polynomial with integer coefficients, has been studied in previous works. In particular, it was proved that $Z(d,f)$ can be evaluated in poly(n) time when f is a quadratic polynomial. This was first proved for the case when d is a prime number [23], before being generalized to the case when d is an arbitrary positive integer [22]. On the other hand, when f is a polynomial of degree ≥ 3, the problem of evaluating such exponential sums was proved to be #P-hard [22, 24].

In this paper, we consider the following generalization of the above exponential sum:

$$Z_{1/2}(d,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d} \xi_d^{f(x_1,\ldots,x_n)}. \tag{2}$$

Here, ξ_d is a chosen square root of ω_d (i.e. $\xi_d^2=\omega_d$) satisfying $\xi_d^{d^2}=1$.

$Z_{1/2^k}(2,f)$		$\deg(f)=1$	$\deg(f)=2$	$\deg(f)\geq 3$
periodic	$k\geq 0$	FP	FP	#P-hard
aperiodic	$k\geq 1$	FP	#P-hard	#P-hard

TABLE 1. Hardness of computing $Z_{1/2^k}(2,f)$, where $k\geq 0$ or $k\geq 1$, and f is a polynomial function with coefficients in $\mathbb{Z}$ and domain $\mathbb{Z}_2^n$. Here, 'periodic' means that f satisfies the periodicity condition (3), and 'aperiodic' means that f does not necessarily satisfy it. The label FP means that $Z_{1/2^k}(d,f)$ can be computed in classical polynomial time, and #P-hard means that there is no efficient classical algorithm to compute $Z_{1/2^k}(d,f)$, unless the widely-believed conjecture FP $\neq$ #P is false.

Unlike $Z(d,f)$, the sum $Z_{1/2}(d,f)$ may not be evaluable in poly(n) time even when f is a quadratic polynomial—the properties of the coefficients of the quadratic polynomial f are crucial to determining the efficiency of evaluating $Z_{1/2}(d,f)$. Assuming plausible complexity assumptions, we prove that a necessary and sufficient condition to guarantee the efficiency of evaluating $Z_{1/2}(d,f)$ for quadratic polynomials f is a periodicity condition, which states that

$$\xi_d^{f(x_1,\ldots,x_n)} = \xi_d^{f(x_1(\text{mod } d),\ldots,x_n(\text{mod } d))}, \tag{3}$$

for all variables $x_1,\ldots,x_n\in\mathbb{Z}$. More precisely, we prove that for quadratic polynomials f satisfying the periodicity condition, $Z_{1/2}(d,f)$ can be evaluated in poly(n) time, and that without the periodicity condition, there is no efficient algorithm to evaluate $Z_{1/2}$ unless the widely-believed assumption that FP $\neq$ #P is false. This is summarized by our main theorem:

Theorem 1. *(Restatement of Theorems 7, 15 and 17) Let $f\in\mathbb{Z}[x_1,\ldots,x_n]$ be a quadratic polynomial over n variables $x_1,\ldots,x_n$ satisfying the periodicity condition. Then $Z_{1/2}(d,f)$ can be computed in polynomial time. If either the quadraticity or periodicity condition is omitted, then $Z_{1/2}(d,f)$ is #P-hard to compute.*

We consider the case $d=2$, and study the complexities of evaluating more general exponential sums, namely those of the form:

$$Z_{1/2^k}(2,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_2} \omega_{2^{k+1}}^{f(x_1,\ldots,x_n)}, \tag{4}$$

where $k\geq 0$ is an integer and f is a polynomial with n variables. Our classification results are summarized in Table 1.

Next, we apply Theorem 1 to the classical simulation of Clifford circuits. In particular, we show that the output probabilities of Clifford circuits can be expressed in terms of half Gauss sums:

Theorem 2. *(Simplified version of Theorem 13) Let C be an m-qudit Clifford circuit. Let $a\in\mathbb{Z}_d^m$ and $b\in\mathbb{Z}_d^k$. Then the probability of obtaining the outcome b when the first k qudits of $C|a\rangle$ are measured is given by*

$$P(b|a) := ||\langle b|_{1..k} C|a\rangle_{a..m}||^2 = \frac{1}{d^l} Z_{1/2}(d,\phi), \tag{5}$$

where $l \in \mathbb{Z}$ and ϕ is a quadratic polynomial that satisfies the periodicity condition (3)*. Moreover, l and ϕ can be computed efficiently.*

Since half Gauss sums can be computed efficiently, Theorem 2 implies that there is an efficient strong simulation of Clifford circuits. This gives an alternative proof (which does not make use of stabilizer techniques) of the Gottesman-Knill Theorem [18].

2. Half Gauss sums

2.1. **Univariate case.** Given two nonzero integers a, d with $d > 0$ and $\gcd(a,d) = 1$, the Gauss sum[1] [25] is defined as:

$$G(a,d) = \sum_{x\in\mathbb{Z}_d} \omega_d^{ax^2}, \tag{6}$$

where $\omega_d = \exp(2\pi \mathrm{i}/d)$ is a root of unity. It has been proved that the Gauss sum $G(a,d)$ can be computed in polynomial time in $\log a$ and $\log d$ [25]. Several useful properties of the Gauss sum $G(a,d)$ have been provided in Appendix B.

In this section, we define a generalization of the Gauss sum, called the half Gauss sum[2]: given two nonzero integers a, d with $d > 0$ and $\gcd(a,d) = 1$, let

$$G_{1/2}(a,d) = \sum_{x\in\mathbb{Z}_d} \xi_d^{ax^2}. \tag{7}$$

Here, ξ_d is a chosen square root of ω_d such that $\xi_d^{d^2} = 1$. This condition is chosen so that the summation over the ring $\mathbb{Z}_d$ is well-defined, i.e. if $x \equiv y \pmod d$, then $\xi_d^{ax^2} = \xi_d^{ay^2}$. Note that such a condition on ξ_d has also been used in the investigation of reflection positivity in parafermion algebra to ensure that the twisted product is well-defined [27, 28].

For $d = 1$, we get $G_{1/2}(a,1) = 1$, which is trivial; hence, we will subsequently restrict our attention to the nontrivial case of $d \geq 2$. Note that we have two choices for ξ_d when d is even, namely (i) $\xi_d = \omega_{2d}$ for all even d, and (ii) $\xi_d = -\omega_{2d}$ for all even d. Since the analyses in both cases are similar, we will present only the first case in this section, and refer the reader to Appendix C for the second case. In other words, ξ_d may be expressed as follows:

$$\xi_d = \begin{cases} -\omega_{2d} = \omega_d^{(d+1)/2}, & d \text{ odd} \\ \omega_{2d}, & d \text{ even.} \end{cases} \tag{8}$$

We will now present properties of the half Gauss sum, its relationship with the Gauss sum, and the computational complexity of evaluating the half Gauss sum.

Proposition 3. *The half Gauss sum satisfies the following properties:*

(1) *If d is odd, then*

$$G_{1/2}(a,d) = G(a(d+1)/2, d). \tag{9}$$

[1] also referred to as the "univariate quadratic homogeneous Gauss sum". See Appendix A.

[2] also referred to as the "univariate quadratic homogeneous half Gauss sum". See Appendix A. Also, note that our definition of "half Gauss sum" differs from that used in [26].

(2) *If d is even, then*

$$G_{1/2}(a,d) = G_{1/2}(a(N_1+bN_2),b)G_{1/2}(aN_2,c), \tag{10}$$

where $d=bc$, $\gcd(b,c)=1$, $2|b$, and N_1 and N_2 are integers satisfying $N_1c+N_2b=1$.

Proof.

(1) If d is odd, $\gcd((d+1)/2,d)=1$ and $\gcd(a,d)=1$. Thus, we have $\gcd(a(d+1)/2,d)=1$. Therefore, we have

$$G_{1/2}(a,d) = \sum_{x\in\mathbb{Z}_d} \xi_d^{ax^2} = \sum_{x\in\mathbb{Z}_d} \omega_d^{a\frac{d+1}{2}x^2} = G(a(d+1)/2,d).$$

(2) If d is even, then a must be odd since $\gcd(a,d)=1$. Hence,

$$G_{1/2}(a,d) = \sum_{x\in\mathbb{Z}_d} \xi_d^{ax^2} = \sum_{x\in\mathbb{Z}_d} \omega_{2d}^{ax^2}.$$

Moreover, d can be decomposed as $d=bc$ with $\gcd(b,c)=1$. Since d is even, it follows that one of b and c is divisible by 2. Without loss of generality, we assume that $2|b$, which implies that $c\equiv 1 \pmod 2$. Since $\gcd(b,c)=1$, there exist two integers N_1 and N_2 such that $N_1c+N_2b=1$. By the Chinese remainder theorem, there exists an isomorphism $\mathbb{Z}_d \to \mathbb{Z}_b\times\mathbb{Z}_c : x\mapsto (y,z)$ with $x\equiv y \pmod b$ and $x\equiv z \pmod c$. In fact, we can choose the map $x=N_2bz+N_1cy$, which can also be written as

$$x = y+N_2b(z-y) = z+N_1c(y-z).$$

Thus,

$$\omega_{2d}^{ax^2} = \omega_{2b}^{aN_1x^2}\omega_{2c}^{aN_2x^2}.$$

Moreover,

$$\omega_{2b}^{aN_1x^2} = \omega_{2b}^{aN_1[y^2+2bN_2(z-y)+N_2^2b^2(y-z)^2]} = \omega_{2b}^{aN_1y^2},$$

where the last equality comes from the fact that $2|b$, and

$$\begin{aligned}
\omega_{2c}^{aN_2x^2} &= \omega_{2c}^{aN_2[z^2+2N_1c(y-z)+N_1^2c^2(y-z)^2]}\\
&= \omega_{2c}^{aN_2z^2}\omega_{2c}^{aN_2N_1^2c^2(y-z)^2}\\
&= \omega_{2c}^{aN_2z^2}\omega_{2c}^{aN_2N_1^2c^2(y^2+z^2)}.
\end{aligned}$$

Since $\omega_{2c}^{c^2}=(-1)^c=-1$ and N_1 is odd as $N_2b+N_1c=1$, we have

$$\begin{aligned}
\omega_{2c}^{aN_2x^2} = \omega_{2c}^{aN_2z^2}(-1)^{aN_2(y^2+z^2)} &= (-\omega_{2c})^{aN_2z^2}(-1)^{aN_2y^2}\\
&= \xi_c^{aN_2z^2}(-1)^{aN_2y^2}.
\end{aligned}$$

Thus,

$$\begin{aligned}
\omega_{2d}^{ax^2} = \omega_{2b}^{aN_1y^2}\xi_c^{aN_2z^2}(-1)^{aN_2y^2} &= \omega_{2b}^{a(N_1+bN_2)y^2}\xi_c^{aN_2z^2}\\
&= \xi_b^{a(N_1+bN_2)y^2}\xi_c^{aN_2z^2}.
\end{aligned}$$

Since $c(N_1+bN_2)+b(1-c)N_2=1$, it follows that $\gcd(N_1+bN_2,b)=1$. Thus $\gcd(a(N_1+bN_2),b)=1$. But $\gcd(aN_2,c)=1$. Therefore, we have

$$\begin{aligned} G_{1/2}(a,d) &= \sum_{y\in\mathbb{Z}_b, z\in\mathbb{Z}_c} \xi_b^{a(N_1+bN_2)y^2}\xi_c^{aN_2z^2} \\ &= G_{1/2}(a(N_1+bN_2),b)G_{1/2}(aN_2,c). \end{aligned}$$

□

Now, any even number d can always be decomposed into $d=2^m c$ with $m\geq 1$ and c being odd. It is straightforward to see that

$$G_{1/2}(a,d)=G_{1/2}(a(N_1+2^mN_2),2^m)G_{1/2}(aN_2,c),$$

where $N_2 2^m+N_1c=1$. As c is odd, it can be rewritten as a Gauss sum by Proposition 3. And so it remains for us to evaluate the half Gauss sum for $d=2^m$, i.e., $G_{1/2}(a,2^m)$.

Proposition 4. *If $m\geq 3$, then*

$$G_{1/2}(a,2^m)=2G_{1/2}(a,2^{m-2}). \tag{11}$$

Moreover,

$$G_{1/2}(a,2)=1+\mathrm{i}^a, \tag{12}$$

$$G_{1/2}(a,2^2)=2\omega_8^a. \tag{13}$$

Proof. First, $G_{1/2}(a,2)$ and $G_{1/2}(a,2^2)$ can be obtained by direct calculation.

Second, for $m\geq 3$,

$$\begin{aligned} G_{1/2}(a,2^m) &= \sum_{x\in[2^m]} \omega_{2^{m+1}}^{ax^2} \\ &= \sum_{x\in[2^{m-1}]} \left[\omega_{2^{m+1}}^{ax^2}+\omega_{2^{m+1}}^{a(x+2^{m-1})^2}\right] \\ &= \sum_{x\in[2^{m-1}]} \omega_{2^{m+1}}^{ax^2}\left[1+\omega_{2^{m+1}}^{a2^mx+a2^{2m-2}}\right] \\ &= \sum_{x\in[2^{m-1}]} \omega_{2^{m+1}}^{ax^2}\,[1+(-1)^x] \\ &= \sum_{y\in[2^{m-2}]} \omega_{2^{m+1}}^{a(2y)^2}\,[1+(-1)^{2y}] \\ &= 2\sum_{y\in[2^{m-2}]} \omega_{2^{m+1}}^{4ay^2} = 2\sum_{y\in[2^{m-2}]} \omega_{2^{m-1}}^{ay^2} \\ &= 2G_{1/2}(a,2^{m-2}). \end{aligned}$$

□

Based on the above properties of the half Gauss sum $G_{1/2}(\cdot,\cdot)$ and the fact that the Gauss sum $G(\cdot,\cdot)$ can be calculated in poly$(\log a,\log d)$-time, we obtain the following corollary:

Corollary 5. *Given two nonzero integers a, d with $d > 0$ and $\gcd(a,d) = 1$, the half Gauss sum can be calculated in $\mathrm{poly}(\log a, \log d)$ time.*

2.2. **Multivariate case.** In this section, we consider a generalization of the Gauss sum (6) to the multivariate case:

$$Z(d,f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_d} \omega_d^{f(x_1,\ldots,x_n)}, \tag{14}$$

where each x_i is summed over a finite ring $\mathbb{Z}_d$, and $f(x_1,\ldots,x_n)$ is a quadratic polynomial with integer coefficients. The *multivariate quadratic Gauss sum* (14) has been proved to be evaluable in polynomial time [22].

We also consider an analogous multivariate generalization of the half Gauss sum:

$$Z_{1/2}(d,f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_d} \xi_d^{f(x_1,\ldots,x_n)}, \tag{15}$$

where $f(x_1,...,x_n) = \sum_{i \le j \in [n]} \alpha_{ij} x_i x_j + \sum_{i \in [n]} \beta_i x_i + \gamma_0$ is a quadratic polynomial with integer coefficients. However, $Z_{1/2}(d,f)$ may not be efficiently evaluable even for quadratic polynomials. It turns out that the existence of an efficient algorithm depends on some periodicity condition.

We say that a polynomial f satisfies the *periodicity condition*[3] if

$$\xi_d^{f(x_1,...,x_n)} = \xi_d^{f(x_1(\mathrm{mod}\ d),...,x_n(\mathrm{mod}\ d))}, \tag{17}$$

for all variables $x_1,...,x_n \in \mathbb{Z}$. This periodicity condition can also be regarded as the well-definedness condition of $Z_{1/2}$ on $\mathbb{Z}_d$. If d is an odd number, then $\xi_d = -\omega_{2d}$, i.e, $\xi_d^d = 1$, which implies that the periodicity condition can always be satisfied for odd d. However, the periodicity condition may not be satisfied in the case of even d.

Proposition 6. *Let d be even, and let $f(x_1,\ldots,x_n) = \sum_{i \le j \in [n]} \alpha_{ij} x_i x_j + \sum_{i \in [n]} \beta_i x_i + \gamma_0$, be a quadratic polynomial. Then, f satisfies the periodicity condition if and only if the cross terms α_{ij} $(i < j)$ and linear terms β_i are all even.*

Proof. It is easy to verify that the quadratic polynomial f satisfies the periodicity condition if all the cross terms α_{ij} $(i < j)$ and linear terms β_i are even.

In the other direction, if f satisfies the periodicity condition, then $\xi_d^{f(x_1,...,x_n)} = \xi_d^{f(x_1(\mathrm{mod}\ d),...,x_n(\mathrm{mod}\ d))}$ for any $x_1,...,x_n \in \mathbb{Z}$. Thus, for any i,

$$\xi_d^{\alpha_{ii}x_i^2 + \beta_i x_i} = \xi_d^{\alpha_{ii}(x_i+d)^2 + \beta_i(x_i+d)},$$

for any $x_i \in \mathbb{Z}$ by choosing $x_j = 0$ for any $j \neq i$. Besides, ξ_d satisfies the conditions $\xi_d^{2d} = 1$ and $\xi_d^{d^2} = 1$. Thus, $\xi_d^{\beta_i d} = (-1)^{\beta_i} = 1$, which implies that β_i is an even

[3] More generally, we say that a function $g : \mathbb{Z}^n \to \mathbb{C}$ is *periodic* with period d if

$$g(x_1,\ldots,x_n) = g(x_1(\mathrm{mod}\ d),\ldots,x_n(\mathrm{mod}\ d)) \tag{16}$$

for all variables $x_1,\ldots,x_n \in \mathbb{Z}$.

number. Since i was chosen arbitrarily, all linear terms β_i are even. Besides, for any fixed i and j with $i < j$, we can choose $x_k = 0$ for any $k \neq i, j$:

$$\xi_d^{\alpha_{ii}x_i^2+\alpha_{jj}x_j^2+\alpha_{ij}x_ix_j+\beta_ix_i+\beta_jx_j} = \xi_d^{\alpha_{ii}(x_i+d)^2+\alpha_{jj}x_j^2+\alpha_{ij}(x_i+d)x_j+\beta_i(x_i+d)+\beta_jx_j},$$

for any $x_i, x_j \in \mathbb{Z}$. This implies that α_{ij} is even. Since i and j were arbitrarily chosen, all the cross terms α_{ij} are even.

□

The periodicity condition of the polynomial f plays an important in the efficient evaluation of the exponential sum $Z_{1/2}$. We denote the set of quadratic polynomials satisfying the periodicity condition by $\mathscr{F}_2^{\text{p.c.}}$. For any quadratic polynomial f satisfying this periodicity condition, the exponential sum $Z_{1/2}(d, f)$ can be evaluated in polynomial time given the description of f.

Theorem 7. *If $f \in \mathscr{F}_2^{\text{p.c.}}$ is a quadratic polynomial satisfying the periodicity condition, then $Z_{1/2}(d, f)$ can be evaluated in polynomial time.*

Proof. Consider the expression

$$f(x_1, ..., x_n) = \sum_{i \leq j \in [n]} \alpha_{ij} x_i x_j + \sum_{i \in [n]} \beta_i x_i + \gamma_0,$$

with the cross term α_{ij} $(i < j)$ and linear term β_i being even. We may assume that $\gamma_0 = 0$, as it only contributes an additive constant term to $Z_{1/2}(d, f)$.
Case (i): All diagonal terms α_{ii} are even. In this case, $Z_{1/2}(d, f) = Z(d, f/2)$, which can be evaluated in polynomial time [22].
Case (ii): There exists at least one diagonal term α_{ii} that is odd.
Case (iia): d is odd. Then, $\xi_d = \omega_d^{(d+1)/2}$. Thus, $Z_{1/2}(d, f) = Z(d, \frac{d+1}{2} f)$, which can be evaluated in polynomial time [22].
Case (iib): $d = 2^m$. Then, $\xi_d = \omega_{2d}$. Since there exists at least one diagonal term α_{ii} that is odd, we assume that α_{11} is odd without loss of generality. Since α_{11} is odd, it is invertible in $\mathbb{Z}_{2d}$ with $2d = 2^{m+1}$. We can rewrite the quadratic polynomial f to separate the term involving x_1:

$$f(x_1, \ldots, x_n) = \alpha_{11}[x_1^2 + x_1 f_1(\hat{x}_1, x_2, \ldots, x_n)] + f_2(\hat{x}_1, x_2, ..., x_n),$$

where f_1 is a linear function over $n - 1$ variables $\{x_2, \ldots, x_n\}$ with

$$f_1(\hat{x}_1, x_2, \ldots, x_n) = \sum_{j \geq 2} \alpha_{11}^{-1} \alpha_{1j} x_j + \alpha_{11}^{-1} \beta_1,$$

and f_2 is a quadratic polynomial with even cross terms and linear terms over $n - 1$ variables $\{x_2, ..., x_n\}$. Here, the notation $\hat{x}_1$ means that the variable x_1 is absent from the polynomial.

Since the cross terms and linear terms are even,

$$f_1 = 2f_1' = 2\left(\sum_{j \geq 2} \frac{\alpha_{11}^{-1}\alpha_{1j}}{2} x_j + \frac{\alpha_{11}^{-1}\beta_1}{2}\right).$$

Thus,

$$f = \alpha_{11}(x_1 + f_1')^2 + f',$$

where f' is a quadratic polynomial with even cross terms and linear terms over $n-1$ variables $\{x_2,\ldots,x_n\}$. Therefore,

$$\begin{aligned} Z_{1/2}(d,f)=\sum_{x_1,\ldots,x_n\in\mathbb{Z}_d}\xi_d^{\alpha_{11}(x_1+f_1')^2+f'} &= \sum_{x_2,..,x_n\in\mathbb{Z}_d}\xi_d^{f'}\sum_{x_1\in\mathbb{Z}_d}\xi_d^{\alpha_{11}(x_1+f_1')^2} \\ &= Z_{1/2}(d,f')G_{1/2}(\alpha_{11},d), \end{aligned}$$

where the last equality comes from the fact that the summation over $x_1\in\mathbb{Z}_d$ is independent of the value of f_1'. This reduces the evaluation of $Z_{1/2}(d,f)$ to $Z_{1/2}(d,f')$ where f' is a quadratic polynomial over $n-1$ variables with even cross terms and linear terms. We can repeat this step until all the diagonal terms are even, which then reduces to Case (i).

Case (iic): $d=2^mc$, with c being odd and $c\geq 3$. Then, $\xi_d=\omega_{2d}$. Since there exists at least one diagonal term α_{ii} that is odd, we shall take, without loss of generality, the first t diagonal terms α_{ii} ($1\leq i\leq t$) to be odd and the other diagonal terms α_{ii} ($i\geq t+1$) to be even.

Now, we can rewrite f as follows

$$f(x_1,\ldots,x_n)=\sum_{i=1}^{t}x_i^2+f_1(x_1,..,x_n),$$

where the coefficients of the quadratic form f_1 are all even. Hence, $f=\sum_{i=1}^{t}x_i^2+2f_1'$, with $f_1'=f_1/2$.

Since $\gcd(2^m,c)=1$, there exist two integers N_1 and N_2 such that $N_2 2^m+N_1c=1$. Adopting a process similar to that used in the proof of Proposition 3, we find, using the Chinese remainder theorem, that there exists an isomorphism $\mathbb{Z}_d\to\mathbb{Z}_{2^m}\times\mathbb{Z}_c :: x_i\mapsto(y_i,z_i)$ with $x_i\equiv y_i \pmod{2^m}$ and $x_i\equiv z_i \pmod{c}$. Thus, we have

$$\begin{aligned} & Z_{1/2}(d,f) \\ = & \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d}\xi_d^{\sum_{i=1}^t x_i^2}\omega_d^{f_1'(x_1,..,x_n)} \\ = & \sum_{y_1,\ldots,y_n\in\mathbb{Z}_{2^m}}\sum_{z_1,\ldots,z_n\in\mathbb{Z}_c}\xi_{2^m}^{\sum_{i=1}^t(N_1+2^mN_2)y_i^2}\xi_c^{\sum_{i=1}^t N_2z_i^2}\omega_{2^m}^{N_1f_1'(y_1,\ldots,y_n)}\omega_c^{N_2f_1'(z_1,\ldots,z_n)} \\ = & \sum_{y_1,\ldots,y_n\in\mathbb{Z}_{2^m}}\xi_{2^m}^{\sum_{i=1}^t(N_1+2^mN_2)y_i^2}\omega_{2^m}^{N_1f_1'(y_1,\ldots,y_n)}\sum_{z_1,\ldots,z_n\in\mathbb{Z}_c}\xi_c^{\sum_{i=1}^t N_2z_i^2}\omega_c^{N_2f_1'(z_1,\ldots,z_n)} \\ = & \sum_{y_1,\ldots,y_n\in\mathbb{Z}_{2^m}}\xi_{2^m}^{\sum_{i=1}^t(N_1+2^mN_2)y_i^2}\omega_{2^m}^{(N_1+2^mN_2)f_1'(y_1,\ldots,y_n)} \\ & \times\sum_{z_1,\ldots,z_n\in\mathbb{Z}_c}\xi_c^{\sum_{i=1}^t N_2z_i^2}\omega_c^{N_2f_1'(z_1,\ldots,z_n)} \\ = & Z_{1/2}(2^m,(N_1+2^mN_2)f)Z_{1/2}(c,N_2f), \end{aligned}$$

where the second-to-last equality comes from the fact that $\omega_{2^m}^{2^m}=1$. This reduces the computation of $Z_{1/2}(d,f)$ to Case (iia) and Case (iib).

□

Here, we have shown the existence of efficient algorithms to evaluate half Gauss sums with quadratic polynomials that satisfy the periodicity condition. We note, however, that if we omit either the periodicity or quadraticity condition, these sums become hard to compute (under a plausible complexity-theoretic conjecture). We will return to a discussion of this in Section 4.

Finally, we note here that there is a nice relationship between half Gauss sums $Z_{1/2}(d,f)$ and the number of zeros of functions of the form $f(x)-k \pmod{d}$ or $\pmod{2d}$. We explore this further in Appendix D.

3. m-QUDIT CLIFFORD CIRCUITS

In this section, we apply our results on the half Gauss sum to Clifford circuits. Let $d \geq 2$ and $m \geq 1$ be integers. The m-qudit Clifford group is the set of operations (called *Clifford operations*) on m qudits that are generated by the following gates: X, Y, Z, F, G, CZ [28–31].

Here, X, Y and Z are the d-level Pauli matrices defined by

$$X\left|k\right\rangle = \left|k+1\right\rangle, \; Y\left|k\right\rangle = \xi_d^{1-2k}\left|k-1\right\rangle, \; Z\left|k\right\rangle = \omega_d^k\left|k\right\rangle, \tag{18}$$

F is the Fourier gate defined by

$$F\left|k\right\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega_d^{kl}\left|l\right\rangle, \tag{19}$$

G is the Gaussian gate defined by

$$G\left|k\right\rangle = \xi_d^{k^2}\left|k\right\rangle, \tag{20}$$

and CZ is the controlled-Z gate defined by

$$CZ\left|k_1,k_2\right\rangle = \omega_d^{k_1k_2}\left|k_1,k_2\right\rangle. \tag{21}$$

Note that the gates X, Y, Z are the qudit generalizations of the qubit Pauli gates

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \; \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{22}$$

and the F, G and CZ gates are the qudit generalizations of the Hadamard gate $\frac{1}{\sqrt{2}}(X+Z)$, the phase gate $\mathrm{diag}(1,\mathrm{i})$, and the controlled-$Z$ gate $\mathrm{diag}(1,1,1,-1)$, respectively, on qubits.

It is straightforward to check that the gates (18)–(21) satisfy the following algebraic relations [28, 30]:

$$\begin{aligned} X^d = Y^d = Z^d = F^4 = G^{2d} = (FG)^3 q_d^{-1} = I, \\ XYX^{-1}Y^{-1} = YZY^{-1}Z^{-1} = ZXZ^{-1}X^{-1} = \omega_d, \\ XYZ = \xi_d, \; FXF^{-1} = Z, \; GXG^{-1} = Y^{-1}, \end{aligned}$$

where

$$q_d = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\xi_d^{j^2}.$$

From the above identities, it is easy to see that the X and Y gates can be expressed in terms of the other gates, and so the following gate set suffices to generate the Clifford group: $\mathscr{C} = \{Z, G, F, CZ\}$. An *$m$-qudit Clifford circuit* is a circuit with m registers and whose gates are all Clifford operations. We shall assume that the Clifford circuit is unitary, i.e. there are no intermediate measurements in the circuit[4].

Without loss of generality, we will assume that (i) each register of the Clifford circuit C begins with an F gate and ends with an $F^\dagger$ gate, and that (ii) the internal circuit (i.e. the full circuit minus the first and last layers) consists of only gates in $\mathscr{C}$. In other words, C is of the form

$$C = (F^\dagger)^{\otimes m} C' F^{\otimes m}, \tag{23}$$

where the internal circuit C' comprises only gates in $\mathscr{C}$. This loses no generality because any Clifford circuit can be transformed into a circuit of the above form, first, by inserting 4 F gates at the start of each register and the pair $F^\dagger F$ at the end of each register, and second, by compiling the internal circuit using only gates in $\mathscr{C}$.

For each m-qudit Clifford circuit, we adopt the following labeling scheme: divide each horizontal wire of the internal part of C into segments, with each segment corresponding to a portion of the wire which is either between 2 F gates, or between an F gate and an $F^\dagger$ gate. It is easy to verify that the total number of segments is given by $n = h - m$, where h is the total number of F or $F^\dagger$ gates (including those in the first and last layers) in C. Label the segments $x_1, \ldots, x_n$.

We will also use the following terminology. The leftmost labels on each register are called *inceptive indices*. The rightmost labels on each register are called *terminal indices*. All other indices are called *internal indices*. For a set of indices $I = \{i_1, \ldots, i_s\}$, we use x_I to denote the tuple $(x_{i_1}, \ldots, x_{i_s})$.

Definition 8. Let C be a Clifford circuit with labels $\{x_1, \ldots, x_n\}$. The *phase polynomial*[5] of C is the polynomial

$$S_C(x_1, \ldots, x_n) = 2 \sum_{\gamma \in \Gamma} \prod_{i \in I_\gamma} x_i + \sum_{g \in \mathscr{G}} \prod_{j \in I_g} x_j^2, \tag{25}$$

where Γ is the set of internal F, Z, CZ gates, and $\mathscr{G}$ is the set of G gates in C.

We now show that if C is a Clifford circuit, then its phase polynomial S_C is a quadratic polynomial that satisfies the periodicity condition.

[4] Note that the results in this section do not hold if the Clifford circuit contains intermediate measurements whose outcomes affect which gates or measurements are performed next. These circuits are called adaptive Clifford circuits, and their amplitudes are #P-hard to compute in general [32, 33].

[5] This definition is chosen specifically so that both Proposition 9 and Eq. (28), which will be stated later, hold. Note that there are examples of Clifford circuits C and phase polynomials S_C for which Eq. (28) holds but Proposition 9 does not. For example, consider the single-qubit Clifford circuit HSH, where $S = \sum_{x \in \{0,1\}} i^x |x\rangle\langle x|$ is the phase gate. Since $x = x^2$ for all $x \in \mathbb{Z}_2$, the all-zero amplitude of C can be written as a half-Gauss sum in two different ways:

$$\langle 0 | C | 0 \rangle = Z_{1/2}(2, S) = Z_{1/2}(2, S') \tag{24}$$

where $S(x) = x$ and $S'(x) = x^2$. While S' satisfies the periodicity condition (for $d = 2$), S does not.

Proposition 9. *If C is a Clifford circuit, then $S_C \in \mathscr{F}_2^{\text{p.c.}}$.*

Proof. Since each gate in C is incident to at most 2 segments, the degree of the polynomial is at most 2. The only terms which can have odd coefficients are terms of the form x_i^2. The remaining terms, which are all either linear and cross terms, have even coefficients, which implies that $S_C \in \mathscr{F}_2^{\text{p.c.}}$. □

The reverse direction is also true: for every polynomial $S \in \mathscr{F}_2^{\text{p.c.}}$, there exists a Clifford circuit C such that $S = S_C$, as the following proposition shows:

Proposition 10. *Let $\mathscr{A}$ be the class of Clifford circuits. The function*

$$\begin{aligned} \Theta : \mathscr{A} &\to \mathscr{F}_2^{\text{p.c.}} && (26) \\ C &\mapsto S_C && (27) \end{aligned}$$

is surjective.

Proof. Let

$$S = \sum_{i \le j \in [n]} \alpha_{ij} x_i x_j + \sum_{i \in [n]} \beta_i x_i \in \mathscr{F}_2^{\text{p.c.}},$$

i.e. α_{ij} is even for $i < j$ and β_i is even for all i. Construct the circuit $C = (F^\dagger)^{\otimes n} C' F^{\otimes n}$, where C' is defined as follows:

(1) for each $i \in [n]$, apply the gate G α_{ii} times.
(2) for each $i < j \in [n]$, apply the gate CZ $\alpha_{ij}/2$ times.
(3) for each $i \in [n]$, apply the gate Z $\beta_i/2$ times.

Then,

$$S_C = \sum_{i \in [n]} \alpha_{ii} x_i^2 + 2 \left(\sum_{i < j \in [n]} \frac{\alpha_{ij}}{2} x_{ij} + \sum_{i \in [n]} \frac{\beta_i}{2} x_i \right) = S,$$

which implies that Θ is surjective. □

We now show that the amplitudes of Clifford circuits can be expressed in terms of half Gauss sums.

Theorem 11. *Let $C = (F^\dagger)^{\otimes m} C' F^{\otimes m}$ be an m-qubit Clifford circuit with h F or $F^\dagger$ gates and $n = h - m$ labels $x_1, \ldots, x_n$. Then,*

$$\langle 0|^{\otimes m} C |0\rangle^{\otimes m} = \frac{1}{\sqrt{d^h}} \sum_{x_1,\ldots,x_n \in \mathbb{Z}_d} \xi_d^{S_C(x_1,\ldots,x_n)} = \frac{1}{\sqrt{d^h}} Z_{1/2}(d, S_C). \tag{28}$$

Proof. Apply the sum-over-paths technique [9, 14] to the Clifford circuit C. □

Theorem 11 can be easily generalized to also allow us to compute amplitudes of Clifford circuits with arbitrary computational-basis states as inputs or outputs:

Proposition 12. *Let $C = (F^\dagger)^{\otimes m} C' F^{\otimes m}$ be an m-qudit Clifford circuit with h F or $F^\dagger$ gates and $n = h - m$ labels $x_1, \ldots, x_n$. Let $a, b \in \mathbb{Z}_d^m$. Then,*

$$\langle b| C |a\rangle = \frac{1}{\sqrt{d^h}} Z_{1/2}(d, S_C + 2a \cdot x_I + 2b \cdot x_F), \tag{29}$$

where I and J are the inceptive and terminal indices (written in order) of C respectively.

Proof. We start by writing

$$\begin{aligned}\langle b|\,(F^\dagger)^{\otimes m}C'F^{\otimes m}\,|a\rangle &= \langle 0^m|\,(X^\dagger)^b(F^\dagger)^{\otimes m}C'F^{\otimes m}X^a\,|0^m\rangle\\ &= \langle 0^m|\,(F^\dagger)^{\otimes m}(Z^\dagger)^bC'Z^aF^{\otimes m}\,|0^m\rangle\,.\end{aligned}$$

Note that $C^* = (F^\dagger)^{\otimes m}(Z^\dagger)^bC'Z^aF^{\otimes m}$ is itself a Clifford circuit, and we could apply Theorem 11 to it:

$$\langle b|\,C\,|a\rangle = \frac{1}{\sqrt{d^h}}Z_{1/2}(d,S_{C^*}),$$

where

$$S_{C^*}(x_1,\ldots,x_n) = S_c(x_1,\ldots,x_n) + 2a\cdot x_I + 2b\cdot x_F.$$

□

A corollary of the above result is that we can express the probabilities of outcomes of qudit Clifford circuits in terms of half Gauss sums even when only a subset of registers is measured. This was previously shown to hold for quopit Clifford circuits [34], i.e., qudit Clifford circuits, where d is an odd prime.

Theorem 13. *Let $C = (F^\dagger)^{\otimes m}C'F^{\otimes m}$ be an m-qudit Clifford circuit with h F or $F^\dagger$ gates and $n = h - m$ labels $x_1,\ldots,x_n$. Assume that C' contains at least one F gate on each register. Let I be the inceptive indices, J be the internal indices, F be the first k terminal indices, and E be the last $m-k$ terminal indices. Let $a \in \mathbb{Z}_d^m$ and $b \in \mathbb{Z}_d^k$. Then the probability*

$$P(b|a) = ||\,\langle b|_{1..k}\,C\,|a\rangle_{a..m}\,||^2 \tag{30}$$

of obtaining the outcome b when the first k qudits of $C\,|a\rangle$ are measured is given by

$$P(b|a) = \frac{1}{d^{n+k}}Z_{1/2}(d,\phi), \tag{31}$$

where

$$\begin{aligned}\phi(x_I,y_I,x_F,y_F,x_J,y_J,w_E) \quad &= \quad S_c(x_I,x_J,x_F,w_E) - S_c(y_I,y_J,y_F,w_E)\\ &\qquad +2a\cdot(x_I-y_I)+2b\cdot(x_F-y_F).\end{aligned} \tag{32}$$

Proof.

$$\begin{aligned}
P(b|a) &= ||\langle b|_{1..k} U |a\rangle_{a..m}||^2 \\
&= \sum_{\beta\in\mathbb{Z}_d^{m-k}} |\langle b\beta|C|a\rangle|^2 \\
&= \sum_{\beta\in\mathbb{Z}_d^{m-k}} \left|\frac{1}{\sqrt{h}} Z_{1/2}(d, S_C + 2a\cdot x_I + 2(b,\beta)\cdot(x_F, x_E)\right|^2 \\
&= \frac{1}{d^h} \sum_{x,y\in\mathbb{Z}_d^n} \xi_d^{S_C(x)-S_C(y)+2a\cdot(x_I-y_I)+2b\cdot(x_F-y_F)} \sum_{\beta\in\mathbb{Z}_d^{m-k}} \omega_d^{\beta\cdot(x_E-y_E)} \\
&= \frac{1}{d^{h-m+k}} \sum_{x_I,y_I\in\mathbb{Z}_d^n} \sum_{x_F,y_F\in\mathbb{Z}_d^k} \sum_{x_J,y_J\in\mathbb{Z}_d^{n-2m}} \sum_{w_E\in\mathbb{Z}_d^{m-k}} \xi_d^{\phi(x_I,y_I,x_F,y_F,x_J,y_J,w_E)} \\
&= \frac{1}{d^{n+k}} Z_{1/2}(d,\phi). \qquad (33)
\end{aligned}$$

where in the fifth line, we used the property that

$$\sum_{\beta\in\mathbb{Z}_d^{m-k}} \omega_d^{\beta\cdot(x_E-y_E)} = d^{m-k}\delta_{x_E,y_E}. \qquad (34)$$

□

Since half Gauss sums can be computed efficiently, the above proof gives an alternative proof of the Gottesman-Knill Theorem [18] for all qudit Clifford circuits:

Corollary 14. (Gottesman-Knill Theorem—strong version) *Qudit Clifford circuits acting on computational basis input states can be efficiently simulated (in the strong sense [35]) by a classical computer.*

Since strong simulation implies weak simulation [36], Corollary 14 implies that there is an efficient classical algorithm that samples from the output distributions of qudit Clifford circuits. Note that such an efficient classical simulation algorithm exists even in the case when there is a logarithmic number of T gates [37].

4. HARDNESS RESULTS AND COMPLEXITY DICHOTOMY THEOREMS

In this section, we show that extending the class of periodic quadratic half Gauss sums in various ways leads to intractable exponential sums. See Table 1 for a summary of our results.

4.1. **Degree-3 polynomials with periodicity condition.**

We shall show, under plausible complexity assumptions, that if we omit the quadraticity condition (while possibly keeping the periodicity condition) from Theorem 1, then there is no efficient algorithm that can compute the exponential sum $Z_{1/2}(d, f)$ on all inputs (d, f). More formally, consider the following problem.

($\mathscr{A}$) `Input:` f, where $f : \mathbb{Z}^n \to \mathbb{Z}$ is a polynomial function of degree ≤ 3 that satisfies the periodicity condition

`Output:` $Z_{1/2}(2, f) = \sum_{x \in \mathbb{Z}_2^n} \mathrm{i}^{f(x)}$.

Our goal is to show that ($\mathscr{A}$) is #P-hard to compute. To this end, we consider the following problem.

($\mathscr{B}$) `Input:` g, where $g : \mathbb{Z}^n \to \mathbb{Z}$ is a polynomial of degree ≤ 3

`Output:` $\mathrm{gap}(g) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x)}$.

It is well-known that ($\mathscr{B}$) is a #P-hard problem (see Theorem 1 of [24]). Hence, to show that ($\mathscr{A}$) is also #P-hard, it suffices to show that there is an efficient reduction from ($\mathscr{B}$) to ($\mathscr{A}$). Indeed, such a reduction is provided by the following chain of equalities:

$$\mathrm{gap}(g) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x)} = \sum_{x \in \mathbb{Z}_2^n} \mathrm{i}^{2g(x)} = Z_{1/2}(2, 2g). \tag{35}$$

Since $2g$ satisfies the periodicity condition[6] for $d = 2$, it follows that $\mathrm{gap}(g)$ can be efficiently computed given an efficient algorithm for $\mathscr{A}$.

Combining these results with Theorem 7 gives the following theorem.

Theorem 15. *The following computational problem is* #P*-hard:*

($\mathscr{C}$) `Input:` *(d, f), where $d \in \mathbb{Z}_{\geq 2}$ and $f : \mathbb{Z}^n \to \mathbb{Z}$ is a degree-3 polynomial function that satisfies the periodicity condition*

`Output:` $Z_{1/2}(d, f) = \sum_{x \in \mathbb{Z}_2^n} \mathrm{i}^{f(x)}$.

4.2. **Degree-2 polynomials without periodicity condition.** We shall show, under plausible complexity assumptions, that if we omit the periodicity condition (while keeping the quadraticity condition) from Theorem 1, then there is no efficient algorithm that can compute the exponential sum $Z_{1/2}(d, f)$ on all inputs (d, f).

To see this, we first consider the following problem:

($\mathscr{D}$) `Input:` f, where $f : \mathbb{Z}^n \to \mathbb{Z}$ is a polynomial function of degree ≤ 2

`Output:` $Z_{1/2}(2, f) = \sum_{x \in \mathbb{Z}_2^n} \mathrm{i}^{f(x)}$.

Note that the inputs of ($\mathscr{D}$) are allowed to be any arbitrary polynomial of degree ≤ 2, including those that do not satisfy the periodicity condition. We will now show that ($\mathscr{B}$) reduces to ($\mathscr{D}$).

Theorem 16. *There exists a polynomial-time reduction from ($\mathscr{B}$) to ($\mathscr{D}$).*

Proof. Assume that there exists an oracle $O_{\mathscr{D}}$ for the problem ($\mathscr{D}$). We will use it to construct a polynomial-time algorithm $T_{\mathscr{B}}$ for ($\mathscr{B}$) as follows. Let g denote the input to the algorithm $T_{\mathscr{B}}$, i.e. $g : \mathbb{Z}^n \to \mathbb{Z}$ is a polynomial of degree ≤ 3.

[6] This can be verified directly by using the definition of periodicity. Alternatively, this also follows immediately from Theorem 25 in Appendix E, where we fully characterize the set of periodic polynomials with degree ≤ 3 when $d = 2$.

For $1 \leq i < j < k \leq n$, let $a_{ijk}, a_{ij}, a_i, a \in \mathbb{Z}_2$ be the coefficients of the polynomial $g \pmod 2$, viz.

$$g(x_1,\dots,x_n) = \sum_{1\leq i_1<i_2<i_3\leq n} a_{i_1,i_2,i_3} x_{i_1}x_{i_2}x_{i_3} + \sum_{1\leq i_1<i_2\leq n} a_{i_1,i_2} x_{i_1}x_{i_2} + \sum_{i=1}^{n} a_i x_i + a \pmod 2. \tag{36}$$

Note that the ability to represent $g \pmod 2$ as a multilinear polynomial arises from the identity $x^2 = x$ for $x \in \mathbb{Z}_2$. The motivation for expressing g in the above form comes from the fact that the desired output $\text{gap}(g)$ of $T_{\mathscr{B}}$ depends on only values $g(x) (\text{mod } 2)$.

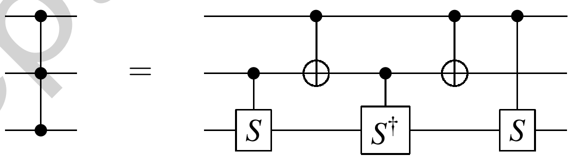
Next, we exploit the circuit-polynomial correspondence [13] to construct an IQP circuit C over the gate set $\{Z, CZ, CCZ\}$ whose circuit amplitudes can be expressed in terms of the gap of g. Let $C = H^{\otimes n} C' H^{\otimes n}$ be an IQP circuit whose internal circuit C' is constructed as follows:

(i) Place a Z gate on the ith wire if $a_i = 1$.
(ii) Place a CZ gate between the ith and jth wires if $a_{ij} = 1$.
(iii) Place a CCZ gate between the ith, jth and kth wires if $a_{ijk} = 1$.

Then, the amplitude of measuring the all-zero string when the circuit C is applied to the all-zero state is given by

$$\langle 0| C |0\rangle = \frac{1}{2^n}\text{gap}(g-a) = \frac{1}{2^n}\sum_{x\in\mathbb{Z}_2^n}(-1)^{g(x)-a} = \frac{1}{2^n}(-1)^a \text{gap}(g). \tag{37}$$

Now, construct the circuit $C_{\mathscr{G}}$ that performs the same unitary operation as C, but which consists of only gates in $\mathscr{G}$, where $\mathscr{G}$ is the strictly universal[7] gate set $\mathscr{G} = \{H, Z, CS\}$, where $CS = \text{diag}(1,1,1,\mathrm{i})$ is the controlled-phase gate satisfying $CS|x_i, x_j\rangle = \mathrm{i}^{x_i x_j}|x_i, x_j\rangle$. To achieve this, we replace all the CZ and CCZ gates in C by circuit gadgets comprising only H and CS gates. This may be achieved by making use of the following circuit identity (which follows from Lemma 6.1 of [40]):



(38)

as well as the following identities:

$$CZ = (CS)^2, \tag{39}$$

$$C(S^\dagger) = (CS)^3, \tag{40}$$

$$CX_{12} = H_2 CZ_{12} H_2, \tag{41}$$

which allow the gates CCZ and CZ to be expressed completely in terms of H and CS. Note that by construction, each register in $C_{\mathscr{G}}$ begins and ends with a H gate, i.e. $C_{\mathscr{G}} = H^{\otimes n} C'_{\mathscr{G}} H^{\otimes n}$ for some circuit $C'_{\mathscr{G}}$ over the gate set $\mathscr{G}$.

[7] Note that Z is not needed for universality, since $\{H, CS\}$ is already universal (see [38] or Theorem 1 of [39]).

Next, mirroring the labeling scheme for Clifford circuits described in Section 3, we construct the phase polynomial f corresponding to $C_{\mathscr{G}}$ as follows:

> Divide each wire of the internal circuit $C'_{\mathscr{G}}$ into segments, with each segment corresponding to a portion of the wire between two H gates. Label the segments $x_1,\ldots,x_N$, where the total number of segments is $N := h-n$, where h is the total number of H gates in $C_{\mathscr{G}}$.

Define the phase polynomial of $C_{\mathscr{G}}$ to be

$$f(x_1,\ldots,x_N) = 2\sum_{\gamma\in\Gamma}\prod_{I\in I_\gamma} x_i + \sum_{g\in\mathscr{G}}\prod_{i\in I_g} x_i, \tag{42}$$

where Γ is the set of internal H gates and $\mathscr{G}$ is the set of CS gates.

Then, the following all-zero amplitude of $C_{\mathscr{G}}$ may be written as

$$\langle 0|C_{\mathscr{G}}|0\rangle = \frac{1}{\sqrt{h}} Z_{1/2}(2,f) = \frac{1}{\sqrt{h}}\sum_{x\in\mathbb{Z}_2^N} \mathrm{i}^{f(x)}. \tag{43}$$

Since $\langle 0|C_{\mathscr{G}}|0\rangle = \langle 0|C|0\rangle$, it follows from Eqs. (37) and (43) that

$$\mathrm{gap}(g) = \frac{2^n}{\sqrt{h}}(-1)^a Z_{1/2}(2,f). \tag{44}$$

Next, feed f into the oracle $O_{\mathscr{D}}$ to get $Z_{1/2}(2,f)$. Finally, use Eq. (44) to calculate and output $\mathrm{gap}(g)$.

Since each step of the above reduction $T_{\mathscr{B}}$ takes polynomial time, the entire reduction runs in polynomial time.

□

Since $(\mathscr{B})$ is #P-hard, it follows from the above reduction that $(\mathscr{D})$ is also #P-hard. Combining this results with Theorem 7 gives the following theorem.

Theorem 17. *The following computational problem is #P-hard:*

$(\mathscr{C})$ `Input`*:* (d,f)*, where* $d\in\mathbb{Z}_{\geq 2}$ *and* $f:\mathbb{Z}^n\to\mathbb{Z}$ *is an aperiodic degree-2 polynomial function*

`Output`*:* $Z_{1/2}(d,f) = \sum_{x\in\mathbb{Z}_2^n}\mathrm{i}^{f(x)}$.

4.3. **Other incomplete Gauss sums:** In this section, we restrict our attention to $d=2$, and consider incomplete Gauss sums of the form:

$$Z_{1/2^k}(2,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_2} \omega_{2^{k+1}}^{f(x_1,\ldots,x_n)} \tag{45}$$

with $k\geq 2$. For $k=2$, the exponential sum

$$Z_{1/4} = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_2} \omega_8^{f(x_1,\ldots,x_n)},$$

with no requirement on the periodicity of the polynomial f, corresponds to the gate set $\{H,T,CZ\}$, which is universal, and it can be shown that computing such sums is #P-hard. However, for quadratic polynomial f satisfying the periodicity condition, we can reduce the evaluation of $Z_{1/4}(2,f)$ to the evaluation of $Z_{1/2}(2,f')$, for some quadratic polynomial f' satisfying the periodicity condition, which in turn can be evaluated in poly(n) time. More generally, for any $k \geq 2$, if f is a quadratic polynomial satisfying the periodicity condition, the incomplete Gauss sum $Z_{1/2^k}(2, f)$ can be reduced to $Z_{1/2}(2, f')$.

Lemma 18. *Let $d = 2$, and let $f = \sum_{i \leq j} \alpha_{ij} x_i x_j + \sum_i \beta_i x_i$ be a quadratic polynomial. Then f satisfies the periodicity condition*

$$\omega_{2^{k+1}}^{f(x_1,\ldots,x_n)} = \omega_{2^{k+1}}^{f((x_1 \bmod 2),\ldots,(x_n \bmod 2))}, \tag{46}$$

if and only if $2^{k-1}|\alpha_{ii}$, $2^k|\alpha_{ij}$ $(i< j)$ and $2^k|\beta_i$. Thus, $Z_{1/2}^{k+1}(2, f) = Z_{1/2}(2, f/2^{k-1})$, where $f/2^{k-1}$ satisfies the periodicity condition for $\omega_2 = \sqrt{-1}$.

Proof. It is easy to verify that the quadratic polynomial f satisfies the periodicity condition if $2|\alpha_{ii}$, $4|\alpha_{ij}$ $(i < j)$ and $4|\beta_i$.

For any i,

$$\omega_{2^{k+1}}^{\alpha_{ii}x_i^2 + \beta_i x_i} = \omega_{2^{k+1}}^{\alpha_{ii}(x_i+2)^2 + \beta_i(x_i+2)}$$

for any $x_i \in \mathbb{Z}$, which implies that $2^{k-1}|\alpha_{ii}$ and $2^k|\beta_i$.

Moreover, for any fixed i and j with $i < j$, we can choose $x_k = 0$ for any $k \neq i, j$ to get

$$\omega_{2^{k+1}}^{\alpha_{ii}x_i^2 + \alpha_{ii}x_j^2 + \alpha_{ij}x_i x_j + \beta_i x_i + \beta_j x_j} = \omega_{2^{k+1}}^{\alpha_{ii}(x_i+2)^2 + \alpha_{ii}x_j^2 + \alpha_{ij}(x_i+2)x_j + \beta_i(x_i+2) + \beta_j x_j}$$

for any $x_i, x_j \in \mathbb{Z}$. This implies that $2^k|\alpha_{ij}$. Since i, j were arbitrarily chosen, it follows that all cross terms α_{ij} satisfy $2^k|\alpha_{ij}$.

□

4.4. **Complexity dichotomy theorems.** In 1979, Valiant introduced the complexity class #P to characterize the computational complexity of counting problems [41], and ever since then, this has been a subject of much research.

Among the many important results arising from this research are the complexity dichotomy theorems, which have attracted considerable attention [42–48]. These theorems state, roughly, that for certain classes of counting problems, each problem in the class is either efficiently computable or #P-hard. (See [49] for an overview.)

These dichotomy theorems have applications to the study of exponential sums. An example of such a theorem was provided by [22], which proved that computing Gauss sums $Z(d, f)$ can be performed efficiently when $\deg(f) \leq 2$ and is #P-hard when $\deg(f) \geq 3$. Note that the polynomials considered by [22] all satisfy the periodicity condition. Hence, if we combine these #P-hardness results with Theorem 7, we arrive at a new dichotomy theorem: if $\deg(f) \leq 2$, then the exponential sum $Z_{1/2}(d, f)$ is computable in polynomial time. Otherwise, if $\deg(f) \geq 3$, then computing $Z_{1/2}(d, f)$ is #P-hard.

Furthermore, for the class of aperiodic exponential sums, our results imply another new complexity dichotomy theorem: if $\deg(f) \leq 1$, then the exponential sum $Z_{1/2}(d, f)$ is computable in polynomial time, otherwise if $\deg(f) \geq 2$, then computing $Z_{1/2}(d, f)$ is #P-hard. For a summary of these results, see Table 1.

5. Tractable signature in Holant problem

In this section, we will apply our results about half Gauss sums to an important framework called the Holant framework, which we will now describe. Let $\mathscr{F}$ be a set of functions, where each element $f \in \mathscr{F} : \mathbb{Z}_d^n \to \mathbb{C}$. A signature grid $\Omega = (G, \mathscr{F})$ is a tuple, where $G = (V, E)$ is a hypergraph and each $v \in \mathscr{F}$ is assigned a function $f_v \in F$ with arity equal to the number of hyperedges incident to it. A $\mathbb{Z}_d$ assignment σ for every $e \in E$ gives an evaluation $\prod_v f_v(\sigma|_{E(v)})$, where $E(v)$ denotes the edges incident to v. Given an input instance Ω, we are interested in computing

$$\text{Holant}_\Omega = \sum_{\sigma : E \to \mathbb{Z}_d} \prod_v f_v(\sigma|_{E(v)}). \tag{47}$$

Affine signatures over $\mathbb{Z}_2$ and $\mathbb{Z}_3$ were defined in [48, 50]. In this section, we give a definition of affine signtures over $\mathbb{Z}_d$, for $d \geq 2$.

(1) **Affine signature over $\mathbb{Z}_d$**: Let f be a signature of arity n with inputs $x_1, \ldots, x_n$ over the domain $\mathbb{Z}_d$, then f is affine if it has the following form

$$\lambda \chi_{A\vec{x}=0} \xi_d^{g(x_1,\ldots,x_n)} \tag{48}$$

where $\lambda \in \mathbb{C}$, ξ_d is a chosen square root of $\omega_d = \exp(2\pi i/d)$ such that $\xi_d^{d^2} = 1$, A is a matrix over $\mathbb{Z}_d$, χ is a 0–1 indicator function such that $\chi_{A\vec{x}=0} = 1$ if and only if $A\vec{x} = 0$, and $g(x_1,,,.x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ is a quadratic polynomial with even cross and linear terms. Let $\mathscr{A}$ to be the set of all affine signatures. It is straightforward to check that $\mathscr{A}$ is closed under multiplication.

(2) **Degenerate function on n variables** Let

$$\mathscr{D} = \{ \otimes_i [f_i(0), f_i(1), \ldots, f_i(d-1)] \mid f_i(j) \in \mathbb{C} \} \tag{49}$$

be the set of functions that can be expressed as the tensor product of unary function.

(3) **The set $\mathscr{P}$**: Let $\mathscr{P}$ be the set of functions that can be written as the composition of unary functions and the binary equality relation $=_2$, where $=_2(i, j)$ is equal to 1 if $i = j$ and 0 otherwise.

Theorem 19. *Given a class of functions $\mathscr{F}$, if $\mathscr{F} \subseteq \mathscr{A}$ or $\mathscr{F} \subseteq \mathscr{P}$, then* Holant$(\mathscr{F})$ *is computable in polynomial time.*

Proof. (1) If $\mathscr{F} \subseteq \mathscr{P}$, then following [48], we can group the variables into connected components if these variables are connected by the binary equality relation $=_2$. In any connected component, let us start with a variable that takes a value in $\mathbb{Z}_d$, and follow any edges labeled by the binary equality relation. There is at most one extension of this assignment, i.e., each variable in this connected component must take the same value as the value that was taken at the beginning. Then we can easily compute the value of the Holant by simply multiplying all the values. There are at most d values, as we have d choices at the starting edge.

(2) If $\mathscr{F} \subseteq \mathscr{A}$, then the method in [48] may not work, as Gaussian elimination may not be applicable for general $\mathbb{Z}_d$. To get around this, we consider the inner

product representation of the Holant problem Holant($\mathscr{F}$), which can be written as

$$\text{Holant}(\mathscr{F}) = (\otimes_e \langle \text{GHZ}_e|)(\otimes_v |f_v\rangle), \tag{50}$$

where $|\text{GHZ}_e\rangle$ denotes the GHZ state on $(\mathbb{C}_d)^{\otimes|e|}$, where $|e|$ denotes the number of vertices incident to the edge e. For example, if $|e| \ = \{1,2,3\}$, then $|\text{GHZ}_e\rangle$ is $|+\rangle = \sum_{i=0}^{d-1} |i\rangle$, $|\text{Bell}\rangle = \sum_{i=0}^{d-1} |ii\rangle$ and $|\text{GHZ}\rangle = \sum_{i=0}^{d-1} |iii\rangle$, respectively.

Since $f_v \in \mathscr{A}$,

$$|f_v\rangle = \sum_{x_1,\dots,x_k \in \mathbb{Z}_d} \chi_{A_v\vec{x}=0} \xi_d^{g_v(x_1,\dots,x_k)} |x_1,\dots,x_k\rangle, \tag{51}$$

where g_v is a quadratic polynomial with even cross and linear terms, and k denotes the arity of f_v. If we omit the term $\chi_{A_v\vec{x}=0}$ in the above expression, then the remaining expression represents a stabilizer state, which we denote as $|\text{STAB}\rangle_v$. Now consider $\sum_{i=1}^{k} A_{1,i}x_i + A_{1,k+1} = 0 \pmod d$ that is given by the first line of $A\vec{x} = 0$. We can add an ancilla qudit with $\langle 0| \prod_j (CX)^{A_{1j}} X^{A_{1,k+1}} |0\rangle$ with control qudit being $j = 1,\dots,k$. Then, $|f_v\rangle$ can be written as

$$|f_v\rangle = \langle 0|^{\otimes m_v} \prod_{i,j} (CX)^{A_{ij}} X^{A_{i,k+1}} |\text{STAB}\rangle_v |0\rangle^{\otimes m_v}, \tag{52}$$

where m_v is the number of rows in A_v. Therefore,

$$\text{Holant}(\mathscr{F}) = (\otimes_e \langle \text{GHZ}_e|)(\otimes_v \langle 0|^{\otimes m_v})(\otimes_v \prod_{i,j} (CX)^{A_{ij}} X^{A_{i,k+1}} |\text{STAB}\rangle_v |0\rangle^{\otimes m_v}),$$

which is just a product of two stabilizer states. It can be computed in polynomial time by the Gottesman-Knill theorem [18].

□

While Theorem 19 addresses the question about which functions lead to tractable Holant problems, we leave open the question about which functions lead to intractable Holant problems: for which classes of functions $\mathscr{F}$ does it hold that (i) $\mathscr{F}$ is neither in $\mathscr{P}$ nor $\mathscr{A}$ and (ii) Holant($\mathscr{F}$) is #P-hard?

6. Concluding remarks

In this paper, we found a larger (compared to previous results) class of quadratic exponential sums whose evaluation we proved to be tractable. In particular, we studied the periodic, quadratic, multivariate half Gauss sums, and gave an efficient algorithm to evaluate these incomplete Gauss sums. We showed that without either the periodicity or quadraticity condition, these exponential sums become intractable under plausible complexity assumptions. These results demonstrate the importance of a periodicity condition, which has not been explored in previous works. Moreover, we show that these tractable exponential sums can be used to express the amplitudes of qudit Clifford circuits, thereby providing an alternative proof of the Gottesman-Knill theorem for qudit Clifford circuits. Last but not least, we provided a tractable affine signature in arbitrary dimensions in the Holant framework.

ACKNOWLEDGMENTS

We thank Arthur Jaffe for useful discussions. K.B. thanks the Templeton Religion Trust for partial support of this research under grant TRT0159, the ARO Grant W911NF-19-1-0302 and the ARO MURI Grant W911NF-20-1-0082, and also thanks Zhejiang University for the support of an Academic Award for Outstanding Doctoral Candidates. D.E.K. was funded by EPiQC, an NSF Expedition in Computing, under Grant CCF-1729369.

APPENDIX A. EXPONENTIAL SUM TERMINOLOGY

In this appendix, we summarize some of the terminology used in the main text. An *exponential sum* is a sum of the form

$$\sum_{x\in A} e^{f(x)}, \tag{53}$$

where $A \subseteq V$ is a finite set, V is an arbitrary set, and $f : V \to \mathbb{C}$ is a complex-valued function.

The exponential sums used in this paper are all *incomplete Gauss sums*[8], which are sums of the form

$$Z_I(d,b,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d} \omega_b^{f(x_1,\ldots,x_n)} \tag{54}$$

where $d,n,b \in \mathbb{Z}^+$ satisfy $d \leq b$ and f is a polynomial with integer coefficients.

Two special cases of incomplete Gauss sums are the *Gauss sum*, defined as

$$Z(d,f) = Z_I(d,d,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d} \omega_d^{f(x_1,\ldots,x_n)}. \tag{55}$$

and the *half Gauss sum*, defined as

$$Z_{1/2}(d,f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_d} \xi_d^{f(x_1,\ldots,x_n)}. \tag{56}$$

With this terminology, note that Gauss sums are a special case of half Gauss sums, which are in turn a special case of incomplete Gauss sums.

When f is quadratic, $Z(d,f)$ and $Z_{1/2}(d,f)$ reduce to the (multivariate) quadratic Gauss sum (14) and (multivariate) quadratic half Gauss sum (15) respectively. When $n = 1$ and f is a homogeneous quadratic polynomial (i.e. $f(x) = ax^2$), the sums $Z(d,f)$ and $Z_{1/2}(d,f)$ reduce to the univariate quadratic homogeneous Gauss sum (6) (which is usually just referred to as a Gauss sum [25]) and univariate quadratic homogeneous half Gauss sum (7) respectively. Note that univariate quadratic Gauss sums are also called Weil sums [23].

[8] Here, we generalized the definition of "incomplete Gauss sums" used in [51, 52] to the multivariate case.

Appendix B. Properties of Gauss sum

In this section, we give some basic facts about the Gauss sum $G(\cdot,\cdot)$ [25]. Given two nonzero integers a,d with $d>0$ and $\gcd(a,d)=1$,

$$G(a,d)=\sum_{x\in\mathbb{Z}_d}\omega_d^{ax^2}.$$

The Gauss sum satisfies the following properties:

(1) If d is odd, then

$$G(a,d)=\left(\frac{a}{d}\right)G(1,d), \tag{57}$$

where $\left(\frac{a}{d}\right)$ is the Jacobi symbol. Moreover,

$$G(1,d)=\begin{cases}\sqrt{d}, & d\equiv 1 \pmod 4\\ \mathrm{i}\sqrt{d}, & d\equiv 3 \pmod 4).\end{cases} \tag{58}$$

(2) If $d=2^k$, then for $k\geq 4$,

$$G(a,2^k)=2G(a,2^{k-1}). \tag{59}$$

(3) If $d=bc$ with $\gcd(b,c)=1$, then

$$G(a,bc)=G(ab,c)G(ac,b). \tag{60}$$

Appendix C. Half Gauss sum for $\xi_d=-\omega_{2d}$ with even d

In the main text, we chose $\xi_d=\omega_{2d}$ for all even numbers d. Note that in the case when d is even, ξ_d can be chosen to be $\pm\omega_{2d}$. Here, we consider the case $\xi_d=-\omega_{2d}$ for all even numbers d. To distinguish these two cases, we define $G_{1/2}(a,d)_+$ for the case when $\xi_d=\omega_{2d}$ and $G_{1/2}(a,d)_-$ for the case when $\xi_d=-\omega_{2d}$ for even d. Thus, we have the following two properties for $G_{1/2}(a,d)_-$.

Lemma 20. *If d is even, then*

$$G_{1/2}(a,d)_-=G_{1/2}(a(N_1+bN_2),b)_-G_{1/2}(aN_2,c), \tag{61}$$

where $d=bc$, $\gcd(b,c)=1$, $2|b$ and integers N_1 and N_2 satisfy $N_1c+N_2b=1$.

Proof. Following the approach in the proof of Proposition 3, we obtain

$$\begin{aligned}\xi_d^{ax^2}=(-1)^{ax^2}\omega_{2b}^{aN_1x^2}\omega_{2c}^{aN_2x^2} &= (-1)^{ay^2}\omega_{2b}^{aN_1y^2}\xi_c^{aN_2z^2}(-1)^{aN_2y^2}\\ &= (-\omega_{2b})^{a(N_1+bN_2)y^2}\xi_c^{aN_2z^2}\\ &= \xi_b^{a(N_1+bN_2)y^2}\xi_c^{aN_2z^2},\end{aligned}$$

which completes the proof of the lemma. □

Lemma 21. *If $m\geq 3$, then*

$$G_{1/2}(a,2^m)_-=2G_{1/2}(a,2^{m-2})_+. \tag{62}$$

Proof. For $m \geq 3$,

$$\begin{aligned}
G_{1/2}(a,2^m)_- &= \sum_{x\in[2^m]} (-\omega_{2^{m+1}})^{ax^2} \\
&= \sum_{x\in[2^{m-1}]} \left[(-\omega_{2^{m+1}})^{ax^2} + (-\omega_{2^{m+1}})^{a(x+2^{m-1})^2}\right] \\
&= \sum_{x\in[2^{m-1}]} (-\omega_{2^{m+1}})^{ax^2} \left[1+(-\omega_{2^{m+1}})^{a2^m x + a2^{2m-2}}\right] \\
&= \sum_{x\in[2^{m-1}]} (-1)^{ax^2} \omega_{2^{m+1}}^{ax^2} [1+(-1)^x] \\
&= \sum_{y\in[2^{m-2}]} \omega_{2^{m+1}}^{a(2y)^2} [1+(-1)^{2y}] \\
&= 2\sum_{y\in[2^{m-2}]} \omega_{2^{m+1}}^{4ay^2} = 2\sum_{y\in[2^{m-2}]} \omega_{2^{m-1}}^{ay^2} \\
&= 2G_{1/2}(a,2^{m-2})_+.
\end{aligned}$$

□

Appendix D. Relationship between half Gauss sums and zeros of a polynomial

In this appendix, we explore the relationship between half Gauss sums $Z_{1/2}(d,f)$ and the number of zeros of functions of the form $f(x)-k \pmod d$ or $\pmod{2d}$. We start with the following theorem.

Theorem 22. *Let $f:\mathbb{Z}_d^n \to \mathbb{Z}$.*

(1) *If d is even, then*

$$|\{x\in\mathbb{Z}_d^n : f(x) = j \bmod 2d\}| = \frac{1}{2d}\sum_{k=0}^{2d-1} \xi_d^{-kj} Z_{1/2}(d,kf). \tag{63}$$

(2) *If d is odd, then*

$$|\{x\in\mathbb{Z}_d^n : f(x) = j \bmod d\}| = \frac{1}{d}\sum_{k=0}^{d-1} \xi_d^{-kj} Z_{1/2}(d,kf). \tag{64}$$

Proof.

(1) If d is even, then $\xi_d = \omega_{2d}$ and $\xi_d^{2d} = 1$. Hence,

$$\begin{aligned}
Z_{1/2}(d,kf) &= \sum_{x\in\mathbb{Z}_d^n} \xi_d^{kf(x)} \\
&= \sum_{j=0}^{2d-1} \xi_d^{kj} \, |\{x\in\mathbb{Z}_d^n : f(x) = j \bmod 2d\}|.
\end{aligned} \tag{65}$$

By taking the inverse Fourier transform, we obtain Eq. (63).

(2) If d is odd, then $\xi_d^d = 1$. Hence,

$$Z_{1/2}(d,kf) = \sum_{x\in\mathbb{Z}_d^n} \xi_d^{kf(x)}$$
$$= \sum_{j=0}^{d-1} \xi_d^{kj} \ |\{x\in\mathbb{Z}_d^n : f(x) = j \bmod d\}|. \tag{66}$$

By taking the inverse Fourier transform, we obtain Eq. (64).

□

This allows us to write the number of zeros of a function $f : \mathbb{Z}_d^n \to \mathbb{Z} \mod d$ in terms of half Gauss sums:

Theorem 23.

$$|\{x\in\mathbb{Z}_d^n : f(x) = 0 \bmod d\}| = \frac{1}{d}\sum_{l=0}^{d-1} Z_{1/2}(d, s_d l f), \tag{67}$$

where $s_d = 2$ if d is even and 1 if d is odd.

Proof. When d is odd, setting $j=0$ in Eq. (64) gives Eq. (67).

Next, let d be even. Then,

$$\begin{aligned}|\{x\in\mathbb{Z}_d^n : f(x) = 0 \bmod d\}| &= |\{x\in\mathbb{Z}_d^n : f(x) = 0 \bmod 2d\}| \\ &\quad + |\{x\in\mathbb{Z}_d^n : f(x) = d \bmod 2d\}| \\ &= \frac{1}{2d}\sum_{k=0}^{2d-1} Z_{1/2}(d,kf) + \frac{1}{2d}\sum_{k=0}^{2d-1}\xi_d^{-kd} Z_{1/2}(d,kf) \\ &= \frac{1}{2d}\sum_{k=0}^{2d-1}\left(1+(-1)^k\right) Z_{1/2}(d,kf) \\ &= \frac{1}{d}\sum_{l=0}^{d-1} Z_{1/2}(d,2lf), \end{aligned} \tag{68}$$

where we used $\xi_d^d = -1$ in the third line.

□

Appendix E. Characterization of periodic polynomials of degree ≤ 3 for $d = 2$

In this appendix, we give a characterization of polynomials with degree $\leq$ 3 that satisfy the periodicity condition for $d=2$. We will use the following notation: let $\mathrm{mod}_2(x)$ be the unique integer $y\in\mathbb{Z}_2$ for which $x \equiv y \bmod 2$.

We start by proving the following identity.

Lemma 24. *Let $a,b,c,x,y\in\mathbb{Z}$. If a, b and c have the same parity (i.e. if a, b and c are either all even or all odd), then*

$$ax^2y + bxy^2 + cxy \equiv a\,\mathrm{mod}_2(x^2y) + b\,\mathrm{mod}_2(xy^2) + c\,\mathrm{mod}_2(xy) \pmod 4 \tag{69}$$
$$= (a+b+c)\mathrm{mod}_2(xy) \pmod 4. \tag{70}$$

Proof. Write $x = 2q+u$ and $y = 2r+v$, where $q, r \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_2$.

Then the RHS of Eq. (69) is

$$\begin{aligned}
\text{RHS} &= a\,\text{mod}_2(x^2y) + b\,\text{mod}_2\left(xy^2\right) + c\,\text{mod}_2(xy)\\
&= a\,\text{mod}_2\left[(2q+u)^2(2r+v)\right] + b\,\text{mod}_2\left[(2q+u)(2r+v)^2\right]\\
&\qquad + c\,\text{mod}_2[(2q+u)(2r+v)]\\
&= a\,\text{mod}_2\left(u^2v\right) + b\,\text{mod}_2\left(uv^2\right) + c\,\text{mod}_2(uv)\\
&= auv + buv + cuv\\
&= (a+b+c)uv\\
&= (a+b+c)\text{mod}_2(x)\text{mod}_2(y)\\
&= (a+b+c)\text{mod}_2(xy).
\end{aligned}$$

On the other hand, the LHS of Eq. (69) is

$$\begin{aligned}
\text{LHS} &= ax^2y + bxy^2 + cxy\\
&= a(2q+u)^2(2r+v) + b(2q+u)(2r+v)^2 + c(2q+u)(2r+v)\\
&= a\left(4q^2+4qu+u^2\right)(2r+v) + b(2q+u)\left(4r^2+4rv+v^2\right)\\
&\quad + c(4qr+2qv+2ur+uv)\\
&\equiv au^2(2r+v) + b(2q+u)v^2 + c(2qv+2ur+uv) \quad \text{mod } 4\\
&= 2au^2r + au^2v + 2bqv^2 + ubv^2 + 2cqv + 2cur + cuv\\
&= 2aur + auv + 2bqv + ubv + 2cqv + 2cur + cuv \quad \because u, v \in \{0,1\}\\
&= 2(a+c)ur + 2(b+c)qv + (a+b+c)uv\\
&\equiv (a+b+c)uv \text{ mod } 4,
\end{aligned}$$

where the last equivalence holds because a, b, c have the same parity, i.e. $a+c$ and $b+c$ are even.

□

Theorem 25. *Let $n \in \mathbb{Z}^+$ and let*

$$g(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant i_3 \leqslant n} a_{i_1 i_2 i_3} x_{i_1} x_{i_2} x_{i_3} + \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant n} a_{i_1 i_2} x_{i_1} x_{i_2} + \sum_{i=1}^{n} a_i x_i + a$$

be a polynomial of degree ≤ 3 with coefficients that satisfy a_{ijk}, a_{ij}, a_i and $a \in \mathbb{Z}$ for all $i \leqslant j \leqslant k \in \{1, \dots, n\}$. Then, g satisfies the periodicity condition for $d = 2$ if and only if for all distinct $i, j, k \in \{1, \dots, n\}$,

(i) *a_i, a_{iii} and a_{ijk} are even,*
(ii) *a_{ij}, a_{ijj} and a_{iij} have the same parity.*

Proof.

($\Rightarrow$) Assume that g satisfies the periodicity condition for $d = 2$. Then for all $x_1, \dots, x_n \in \mathbb{Z}$,

$$\mathrm{i}^{g(x_1,\dots,x_n)} = \mathrm{i}^{g(x_1 \text{ mod } 2, \dots, x_n \text{ mod } 2)} \tag{71}$$

$$\iff \quad g(x_1, \dots, x_n) \equiv g(x_1 \text{ mod } 2, \dots, x_n \text{ mod } 2) \ \text{ mod } 4. \tag{72}$$

Denote

$$\tilde{g}(x,y,z) = g(x,y,z,0,\ldots,0) \tag{73}$$

$$\begin{aligned}&= a_{111}x^3 + a_{222}y^3 + a_{333}z^3\\ &\quad + a_{112}x^2y + a_{113}x^2z + a_{122}xy^2\\ &\quad + a_{223}y^2z + a_{133}xz^2 + a_{233}yz^2 + a_{123}xyz\\ &\quad + a_{11}x^2 + a_{22}y^2 + a_{33}z^2\\ &\quad + a_{12}xy + a_{13}xz + a_{23}yz\\ &\quad + a_1x + a_2y + a_3z + a.\end{aligned} \tag{74}$$

Then, Eq. (72) implies that for all $x,y,z \in \mathbb{Z}$,

$$\tilde{g}(x,y,z) = \tilde{g}(x \bmod 2, y \bmod 2, z \bmod 2) \bmod 4. \tag{75}$$

We will now use Eq. (75) repeatedly to find necessary conditions that the coefficients of the polynomial g must satisfy.

First, Eq. (75) implies that

$$\tilde{g}(0,0,0) = \tilde{g}(2,0,0) \bmod 4 \tag{76}$$

$$\begin{aligned}\implies \quad 0 &= a_{111}2^3 + a_{11}2^2 + a_12 \bmod 4\\ &= 2a_1 \bmod 4,\end{aligned} \tag{77}$$

which implies that a_1 is even. By symmetry between 1 and i for $i \in \{1,\ldots,n\}$,

$$\boxed{a_i \text{ is even} \quad \forall i \in \{1,\ldots,n\}.} \tag{78}$$

Second, Eq. (75) implies that

$$\tilde{g}(1,0,0) = \tilde{g}(-1,0,0) \bmod 4 \tag{79}$$

$$\implies \quad a_{111} + a_{11} + a_1 = -a_{111} + a_{11} - a_1 \bmod 4 \tag{80}$$

$$\implies \quad 2a_{111} + 2a_1 = 0 \bmod 4. \tag{81}$$

By Eq. (78), a_1 is even, and so $2a_1 = 0 \bmod 4$. Hence,

$$2a_{111} = 0 \bmod 4, \tag{82}$$

which implies that a_{111} is even. By symmetry between 1 and i for $i \in \{1,\ldots,n\}$,

$$\boxed{a_{iii} \text{ is even} \quad \forall i \in \{1,\ldots,n\}.} \tag{83}$$

Third, Eq. (75) implies that

$$\begin{aligned}&\tilde{g}(0,1,0) = \tilde{g}(2,1,0) \bmod 4\\ \implies\ & a_{222} + a_{22} + a_2 = a_{111}8 + a_{222} + a_{112}4 + a_{122}2\\ &\qquad\qquad + a_{11}4 + a_{22} + a_{12}2 + a_12 + a_2 \bmod 4\\ \implies\ & 2a_1 + 2a_{12} + 2a_{122} = 0 \bmod 4.\end{aligned}$$

By Eq. (78), a_1 is even, and so, $2a_1 = 0 \bmod 4$. Hence,

$$2(a_{12} + a_{122}) = 0 \bmod 4, \tag{84}$$

which implies that $a_{12}+a_{122}$ is even, i.e. a_{12} and a_{122} have the same parity.

By symmetry,

$$\boxed{a_{ij}, a_{ijj}, a_{iij} \text{ have the same parity} \quad \forall i<j \in \{1,\dots,n\}.} \tag{85}$$

Fourth, Eq. (75) implies that

$$\begin{aligned}
&\tilde{g}(0,1,1) = \tilde{g}(2,1,1) \bmod 4\\
\implies\ & a_{222}+a_{333}+a_{223}+a_{233}+a_{22}+a_{33}+a_{23}+a_{2}+a_{3}\\
&\qquad = a_{111}8+a_{222}+a_{333}+a_{112}4+a_{113}4+a_{122}2+a_{223}\\
&\qquad\quad +a_{133}2+a_{233}+a_{123}2+a_{11}4+a_{22}+a_{33}+a_{12}2\\
&\qquad\quad +a_{13}2+a_{23}+a_{1}2+a_{2}+a_{3} \bmod 4\\
\implies\ & 2(a_{122}+a_{133}+a_{123}+a_{12}+a_{13}+a_{1}) = 0 \bmod 4.
\end{aligned}$$

By Eq. (83), $a_{122}+a_{12}$ and $a_{133}+a_{13}$ are both even, and hence $2(a_{122}+a_{12}) = 0 \bmod 4$ and $2(a_{133}+a_{13}) = 0 \bmod 4$. Also, Eq. (78) implies that a_1 is even, and so, $2a_1 = 0 \bmod 4$. Therefore,

$$2a_{123} = 0 \bmod 4, \tag{86}$$

which implies that a_{123} is even. By symmetry,

$$\boxed{a_{ijk} \text{ is even} \quad \forall i<j<k \in \{1,\dots,n\}.} \tag{87}$$

Together, Eqs. (78), (83), (85) and (87) imply the consequent of the logical biconditional in Theorem 25.

($\Leftarrow$) Assume that (i) and (ii) in Theorem 25 hold. Then,

$$\begin{aligned}
& g(\mathrm{mod}_2(x_1),\dots,\mathrm{mod}_2(x_n))\\
=& \sum_{1\leqslant i_1\leqslant i_2\leqslant i_3\leqslant n} a_{i_i i_2 i_3}\mathrm{mod}_2(x_{i_1})\mathrm{mod}_2(x_{i_2})\mathrm{mod}_2(x_{i_3})\\
&+ \sum_{1\leqslant i_1\leqslant i_2\leqslant n} a_{i_1 i_2}\mathrm{mod}_2(x_{i_1})\mathrm{mod}_2(x_{i_2}) + \sum_{i=1}^{n} a_i \mathrm{mod}_2(x_i) + a\\
=& \sum_{1\leqslant i_1\leqslant i_2\leqslant i_3\leqslant n} a_{i_i i_2 i_3}\mathrm{mod}_2(x_{i_1}x_{i_2}x_{i_3})\\
&+ \sum_{1\leqslant i_1\leqslant i_2\leqslant n} a_{i_1 i_2}\mathrm{mod}_2(x_{i_1}x_{i_2}) + \sum_{i=1}^{n} a_i \mathrm{mod}_2(x_i) + a\\
=& \sum_i \underbrace{a_{iii}\mathrm{mod}_2(x_i^3)}_{\textcircled{1}} + \sum_{i<j} \underbrace{\left[a_{iij}\mathrm{mod}_2(x_i^2 x_j) + a_{ijj}\mathrm{mod}_2(x_i x_j^2) + a_{ij}\mathrm{mod}_2(x_i x_j)\right]}_{\textcircled{2}}\\
&+ \sum_{i<j<k} \underbrace{a_{ijk}\mathrm{mod}_2(x_i x_j x_k)}_{\textcircled{3}} + \sum_i \underbrace{a_{ii}\mathrm{mod}_2(x_i^2)}_{\textcircled{4}} + \sum_i \underbrace{a_i\mathrm{mod}_2(x_i)}_{\textcircled{5}} + a
\end{aligned} \tag{88}$$

To evaluate ①, ③ and ⑤ mod 4, we use the identity

$$2a \,\mathrm{mod}_2(x) \equiv 2ax \pmod 4 \quad \forall a,x \in \mathbb{Z} \tag{89}$$

Since a_{iii}, a_{ijk} and a_i are even, it follows that

$$\textcircled{1} = a_{iii}x_i^3 \bmod 4 \tag{90}$$

$$\textcircled{3} = a_{ijk}x_ix_jx_k \bmod 4 \tag{91}$$

$$\textcircled{5} = a_ix_i \bmod 4 \tag{92}$$

To evaluate $\textcircled{3}$ mod 4, we use the identity

$$a \operatorname{mod}_2(x^2) \equiv ax^2 \pmod 4 \quad \forall a, x \in \mathbb{Z} \tag{93}$$

which gives

$$\textcircled{4} = a_{ii}x_i^2 \bmod 4 \tag{94}$$

To evaluate $\textcircled{2}$ mod 4, we use Lemma 24, which implies that

$$\textcircled{2} = a_{iij}x_i^2x_j + a_{ijj}x_ix_j^2 + a_{ij}x_ix_j \bmod 4 \tag{95}$$

Substituting Eqs. (90), (95), (91), (94) and (92) into Eq. (88) gives

$$g(\operatorname{mod}_2(x_1), \ldots, \operatorname{mod}_2(x_n)) = g(x_1, \ldots, x_n) \tag{96}$$

which means that g satisfies the periodicity condition.

□

References

[1] L.-K. Hua, *Introduction to number theory*. Springer Science & Business Media, 2012.

[2] C. Gauss, *Disquisitiones Arithmeticae*. Fleischer, Leipzig, 1801.

[3] K. G. Paterson, “Applications of exponential sums in communications theory,” in *Cryptography and Coding* (M. Walker, ed.), (Berlin, Heidelberg), pp. 1–24, Springer Berlin Heidelberg, 1999.

[4] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley, “A complexity dichotomy for partition functions with mixed signs,” *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3336–3402, 2010.

[5] I. E. Shparlinski, “Exponential sums in coding theory, cryptology and algorithms,” in *Coding Theory and Cryptology*, pp. 323–383, World Scientific, 2002.

[6] N. E. Hurt, “Exponential sums and coding theory: a review,” *Acta Applicandae Mathematica*, vol. 46, no. 1, pp. 49–91, 1997.

[7] I. E. Shparlinski, “Exponential sums and lattice reduction: Applications to cryptography,” in *Finite fields with applications to coding theory, cryptography and related areas*, pp. 286–298, Springer, 2002.

[8] R. P. Feynman, A. R. Hibbs, and D. F. Styer, *Quantum mechanics and path integrals*. Courier Corporation, 2010.

[9] C. M. Dawson, A. P. Hines, D. Mortimer, H. L. Haselgrove, M. A. Nielsen, and T. J. Osborne, “Quantum computing and polynomial equations over the finite field $\mathbb{Z}_2$,” *Quantum Information & Computation*, vol. 5, no. 2, pp. 102–112, 2005.

[10] L. M. Adleman, J. DeMarrais, and M.-D. A. Huang, “Quantum computability,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1524–1540, 1997.

[11] D. Bacon, W. Van Dam, and A. Russell, “Analyzing algebraic quantum circuits using exponential sums,” *Available at http://www.cs.ucsb.edu/ vandam/publications.html*, 2008.

[12] M. D. Penney, D. E. Koh, and R. W. Spekkens, “Quantum circuit dynamics via path integrals: Is there a classical action for discrete-time paths?,” *New Journal of Physics*, vol. 19, no. 7, p. 073006, 2017.

[13] A. Montanaro, “Quantum circuits and low-degree polynomials over $\mathbb{F}_2$,” *Journal of Physics A: Mathematical and Theoretical*, vol. 50, no. 8, p. 084002, 2017.

[14] D. E. Koh, M. D. Penney, and R. W. Spekkens, “Computing quopit Clifford circuit amplitudes by the sum-over-paths technique,” *Quantum Information & Computation*, vol. 17, no. 13&14, pp. 1081–1095, 2017.

[15] M. Amy, P. Azimzadeh, and M. Mosca, “On the controlled-not complexity of controlled-not–phase circuits,” *Quantum Science and Technology*, vol. 4, no. 1, p. 015002, 2018.

[16] M. Amy, “Towards large-scale functional verification of universal quantum circuits,” *EPTCS 287, 2019, pp. 1-21. arXiv preprint arXiv:1805.06908*, 2018.

[17] L. Kocia and P. Love, “Stationary Phase Method in Discrete Wigner Functions and Classical Simulation of Quantum Circuits,” *Quantum*, vol. 5, p. 494, July 2021.

[18] D. Gottesman, “The Heisenberg representation of quantum computers,” *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pp. 32–43, 1999.

[19] J. Preskill, “Quantum computing and the entanglement frontier,” *arXiv preprint arXiv:1203.5813*, 2012.

[20] A. W. Harrow and A. Montanaro, “Quantum computational supremacy,” *Nature*, vol. 549, no. 7671, p. 203, 2017.

[21] A. M. Dalzell, A. W. Harrow, D. E. Koh, and R. L. La Placa, “How many qubits are needed for quantum computational supremacy?,” *Quantum*, vol. 4, p. 264, May 2020.

[22] J.-Y. Cai, X. Chen, R. Lipton, and P. Lu, “On tractable exponential sums,” in *Frontiers in Algorithmics* (D.-T. Lee, D. Z. Chen, and S. Ying, eds.), (Berlin, Heidelberg), pp. 148–159, Springer Berlin Heidelberg, 2010.

[23] R. Lidl and H. Niederreiter, *Finite fields*, vol. 20. Cambridge university press, 1997.

[24] A. Ehrenfeucht and M. Karpinski, “The computational complexity of (XOR,AND)-counting problems,” tech. rep., Proc. 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA) (2001), 1990.

[25] S. Lang, *Algebraic Number Theory*. Addison-Wesley, 1970.

[26] B. C. Berndt and R. J. Evans, “Half Gauss Sums,” *Mathematische Annalen*, vol. 249, no. 2, pp. 115–125, 1980.

[27] A. Jaffe and B. Janssens, “Reflection positive doubles,” *Journal of Functional Analysis*, vol. 272, no. 8, pp. 3506–3557, 2017.

[28] A. Jaffe and Z. Liu, “Planar para algebras, reflection positivity,” *Communications in Mathematical Physics*, vol. 352, pp. 95–133, May 2017.

[29] J. M. Farinholt, “An ideal characterization of the Clifford operators,” *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 30, p. 305303, 2014.

[30] A. Jaffe, Z. Liu, and A. Wozniakowski, “Constructive simulation and topological design of protocols,” *New Journal of Physics*, vol. 19, no. 6, p. 063016, 2017.

[31] A. Jaffe, Z. Liu, and A. Wozniakowski, “Holographic software for quantum networks,” *Science China Mathematics*, vol. 61, pp. 593–626, Apr 2018.

[32] R. Jozsa and M. Van Den Nest, “Classical simulation complexity of extended Clifford circuits,” *Quantum Information & Computation*, vol. 14, no. 7&8, pp. 633–648, 2014.

[33] D. E. Koh, “Further extensions of Clifford circuits and their classical simulation complexities,” *Quantum Information & Computation*, vol. 17, no. 3&4, pp. 0262–0282, 2017.

[34] Mark D Penney and Robert W Spekkens. Private Communication, 2017.

[35] M. V. den Nest, “Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond,” *Quantum Information & Computation*, vol. 10, no. 3-4, pp. 0258–0271, 2010.

[36] B. M. Terhal and D. P. DiVincenzo, “Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games,” *Quantum Information & Computation*, vol. 4, no. 2, pp. 134–145, 2004.

[37] S. Bravyi and D. Gosset, “Improved classical simulation of quantum circuits dominated by Clifford gates,” *Physical review letters*, vol. 116, no. 25, p. 250501, 2016.

[38] A. Y. Kitaev, “Quantum computations: algorithms and error correction,” *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997.

[39] D. Aharonov, "A simple proof that Toffoli and Hadamard are quantum universal," *arXiv preprint quant-ph/0301040*, 2003.

[40] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical review A*, vol. 52, no. 5, p. 3457, 1995.

[41] L. Valiant, "The complexity of enumeration and reliability problems," *SIAM Journal on Computing*, vol. 8, no. 3, pp. 410–421, 1979.

[42] N. Creignou and M. Hermann, "Complexity of generalized satisfiability counting problems," *Information and Computation*, vol. 125, no. 1, pp. 1 – 12, 1996.

[43] M. Dyer, L. A. Goldberg, and M. Paterson, "On counting homomorphisms to directed acyclic graphs," *J. ACM*, vol. 54, Dec. 2007.

[44] A. Bulatov and M. Grohe, "The complexity of partition functions," in *Automata, Languages and Programming* (J. Díaz, J. Karhumäki, A. Lepistö, and D. Sannella, eds.), (Berlin, Heidelberg), pp. 294–306, Springer Berlin Heidelberg, 2004.

[45] L. Goldberg, M. Grohe, M. Jerrum, and M. Thurley, "A complexity dichotomy for partition functions with mixed signs," *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3336–3402, 2010.

[46] A. A. Bulatov, "The complexity of the counting constraint satisfaction problem," in *Automata, Languages and Programming* (L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, eds.), (Berlin, Heidelberg), pp. 646–661, Springer Berlin Heidelberg, 2008.

[47] M. Dyer, L. Goldberg, and M. Jerrum, "The complexity of weighted Boolean #CSP," *SIAM Journal on Computing*, vol. 38, no. 5, pp. 1970–1986, 2009.

[48] J.-Y. Cai, P. Lu, and M. Xia, "The complexity of complex weighted Boolean #CSP," *Journal of Computer and System Sciences*, vol. 80, no. 1, pp. 217 – 236, 2014.

[49] J.-Y. Cai and X. Chen, *Complexity Dichotomies for Counting Problems : Volume 1, Boolean Domain*. Cambridge University Press, 2015.

[50] T. Williams, *Advances in the Computational Complexity of Holant Problems*. PhD thesis, University of Wisconsin-Madison, 2015.

[51] D. H. Lehmer, "Incomplete Gauss sums," *Mathematika*, vol. 23, no. 2, pp. 125–135, 1976.

[52] R. Evans, M. Minei, and B. Yee, "Incomplete higher-order Gauss sums," *Journal of mathematical analysis and applications*, vol. 281, no. 2, pp. 454–476, 2003.