Quantum Information and Computation, Vol. 19, No. 5&6 (2019) 0392–0412

PERIODIC FOURIER REPRESENTATION OF BOOLEAN FUNCTIONS

RYUHEI MORI
School of Computing, Tokyo Institute of Technology, Ookayama, Meguro-ku, Tokyo, 152-8552, Japan
Japan Science and Technology Agency, PRESTO, Honcho, Kawaguchi, Saitama, 332-0012, Japan

Received April 5, 2018
Revised March 25, 2019

In this work, we consider a new type of Fourier-like representation of Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$

$$f(x) = \cos\left(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\right).$$

This representation, which we call the periodic Fourier representation, of Boolean function is closely related to a certain type of multipartite Bell inequalities and non-adaptive measurement-based quantum computation with linear side-processing ($\mathrm{NMQC}_{\oplus}$). The minimum number of non-zero coefficients in the above representation, which we call the periodic Fourier sparsity, is equal to the required number of qubits for the exact computation of f by $\mathrm{NMQC}_{\oplus}$. Periodic Fourier representations are not unique, and can be directly obtained both from the Fourier representation and the $\mathbb{F}_2$-polynomial representation. In this work, we first show that Boolean functions related to $\mathbb{Z}/4\mathbb{Z}$-polynomial have small periodic Fourier sparsities. Second, we show that the periodic Fourier sparsity is at least $2^{\deg_{\mathbb{F}_2}(f)}-1$, which means that $\mathrm{NMQC}_{\oplus}$ efficiently computes a Boolean function f if and only if $\mathbb{F}_2$-degree of f is small. Furthermore, we show that any symmetric Boolean function, e.g., AND_n, Mod_n^3, Maj_n, etc, can be exactly computed by depth-2 $\mathrm{NMQC}_{\oplus}$ using a polynomial number of qubits, that implies exponential gaps between $\mathrm{NMQC}_{\oplus}$ and depth-2 $\mathrm{NMQC}_{\oplus}$.

Keywords: Measurement-based quantum computation, XOR game, Fourier analysis
Communicated by: R Cleve & R de Wolf

1 Introduction

1.1 Periodic Fourier representation

Fourier analysis of Boolean function is a powerful tool used in theoretical computer science [17]. A Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ can be represented by a unique $\mathbb{R}$-multilinear polynomial

$$f(x) = \sum_{S\subseteq[n]} \widehat{f}(S) \prod_{i\in S} x_i \tag{1}$$

using Fourier coefficients $(\widehat{f}(S) \in \mathbb{R})_{S\subseteq[n]}$ where $[n] := \{1,2,\dots,n\}$. Here, the number $\left|\{S\in[n] \mid \widehat{f}(S)\neq 0\}\right|$ of non-zero Fourier coefficients, called the Fourier sparsity, is one of the

important complexity measures of Boolean functions, which means the number of $\mathbb{F}_2$-linear Boolean functions correlated to f. On the other hand, another natural complexity measure of Boolean function is the linear sketch complexity [13], which is the smallest number k such that there exists a Boolean function $g\colon \{+1,-1\}^k \to \{+1,-1\}$ and $S_1,\dots,S_k \subseteq [n]$ satisfying

$$f(x) = g\left(\prod_{i\in S_1} x_i, \dots, \prod_{i\in S_k} x_i\right). \tag{2}$$

In fact, the linear sketch complexity is equal to the Fourier dimension, which is a dimension of a linear space spanned by $\{S \subseteq [n] \mid \widehat{f}(S) \neq 0\}$ where a subset S is regarded as a vector in $\mathbb{F}_2^n$ [15]. Importantly, the linear sketch complexity has the above operational definition, and also has another operational characterization which is the one-way communication complexity of $f^{\oplus}(x,y) := f(x \oplus y)$ [15].

Here, the Fourier representation (1) can be regarded as a restriction of general linear sketch (2) where g must be $\mathbb{R}$-linear. In this work, we consider a different type of restriction where g must be the cosine function of $\mathbb{R}$-linear function, i.e.,

$$f(x) = \cos\left(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\right). \tag{3}$$

Here, the constant factor π is not essential, but introduced for the simplicity of analysis. We call (3) the *periodic Fourier representation*. The number $|\{S \subseteq [n] \mid S \neq \varnothing, \phi_S \neq 0\}|$ of non-zero coefficients except for that corresponding to the empty set is the complexity measure which we will consider in this work, and call the *periodic Fourier sparsity*. The periodic Fourier sparsity is operationally characterized as the required number of qubits for computing f exactly by non-adaptive measurement-based quantum computation with linear side-processing ($\mathrm{NMQC}_{\oplus}$) [25], [11]. This fact is a consequence of Werner and Wolf's theorem [25]. Werner and Wolf showed that for given Boolean function $h\colon \{+1,-1\}^k \to \{+1,-1\}$ and input distribution μ on $\{+1,-1\}^k$, the largest bias of winning probability of k-player XOR game (h,μ) in quantum theory is equal to

$$\max_{\phi_0,\dots,\phi_k} \sum_{z_1,\dots,z_k} \mu(z_1,\dots,z_k) h(z_1,\dots,z_k) \cos\left(\pi\left(\phi_0 + \sum_{i=1}^{k} \phi_i z_i\right)\right). \tag{4}$$

This largest winning probability is achieved by using shared k-qubit GHZ state and local measurements $\cos(\pi(\phi_i z_i + \phi_0/k))X + \sin(\pi(\phi_i z_i + \phi_0/k))Y$ where X and Y are the Pauli matrices [25]. If we assume that $z_1,\dots,z_k$ are parities of hidden inputs $x_1,\dots,x_n$, then the situation of XOR game is equivalent to that of $\mathrm{NMQC}_{\oplus}$ [11]. Hence, $\mathrm{NMQC}_{\oplus}$ exactly computes f by using k qubits if and only if the periodic Fourier sparsity of f is at most k.

1.2 Non-adaptive measurement-based quantum computation with linear side-processor

Measurement-based quantum computation (MBQC) is a model of quantum computation based on qubit-wise measurements of prepared state which is independent of input (actually independent also of problem in the following works). When measurement outcomes are used

for choices of other measurements, we say that the MBQC algorithm is adaptive. Raussendorf et al. showed that MBQC with adaptive measurements and linear side-processing using a cluster state can simulate quantum circuit with small overhead [20]. Hoban et al. considered and analyzed non-adaptive MBQC with linear side-processing ($\mathrm{NMQC}_{\oplus}$) [11]. Their results will be briefly introduced in the next section. In the rest of this section, we explain a definition of $\mathrm{NMQC}_{\oplus}$ for computing a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$. Before an input is given, we prepare a k-qubit quantum state ρ for some positive integer k and two binary measurements A_i^0 and A_i^1 for each qubit indexed by $i \in [k]$. After an input $\mathsf{x} \in \{0,1\}^n$ is given, the linear side-processor computes k parities $\mathsf{z}_1 := \bigoplus_{i\in S_1} \mathsf{x}_i, \ldots, \mathsf{z}_k := \bigoplus_{i\in S_k} \mathsf{x}_k$ for fixed subsets $S_1, \ldots, S_k \subseteq [n]$ which are independent of input x. Then, i-th qubit of ρ is measured by $A_i^{\mathsf{z}_i}$ for each $i \in [k]$ independently. Finally, the linear side-processor computes a parity of all measurement outcomes, which is the final output of the $\mathrm{NMQC}_{\oplus}$ algorithm and should be equal to $f(\mathsf{x})$. Hence, $\mathrm{NMQC}_{\oplus}$ algorithm is specified by a positive integer k, a prepared k-qubit state ρ, prepared measurements A_i^0 and A_i^1 for $i \in [k]$ and subsets $S_1, \ldots, S_k \subseteq [n]$.

If we consider $\mathrm{NMQC}_{\oplus}$ with the minimum error probability on given input distribution, Werner and Wolf's theorem implies that we can safely assume that the prepared quantum state ρ is the generalized GHZ state $(|0\cdots0\rangle + |1\cdots1\rangle)/\sqrt{2}$ and the binary measurements are $\cos(\pi(\phi_i z_i + \phi_0/k))X + \sin(\pi(\phi_i z_i + \phi_0/k))Y$ for some parameters $\phi_0, \ldots, \phi_k$ where $z_i = 1 - 2\mathsf{z}_i$ for $i \in [k]$. Especially, we can exactly compute a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ by $\mathrm{NMQC}_{\oplus}$ using k qubits if and only if the periodic Fourier sparsity of f is at most k.

1.3 Background: Foundation of quantum physics by computational complexities

While quantum physics is described by extremely simple mathematics, quantum physics does not have operationally meaningful axioms (often called "postulates" rather than axioms). Recently, quantum physics is believed to be explained by "information processing". Some postulates based on information processing have been suggested [6], [18], [8]. On the other hand, postulates based on "computational complexity" have not been investigated sufficiently. Recently, Barrett et al. showed that generalized probabilistic theories, which are "theories" including quantum theory and obeying a general framework of theories based on weak assumptions, can solve problems in AWPP [3]. Hence, postulates on computational complexity such as "Nature does not allow us to solve NP-hard problem efficiently" could be a candidate of postulates for quantum physics since some of generalized probabilistic theories violate this postulate unless $\mathsf{AWPP} \subseteq \mathsf{NP}$. For discussing computations in generalized probabilistic theories, states, measurements and operations have to be defined for multipartite system [2]. On the other hand, in measurement-based computations, we only needs concepts of states and measurements in multipartite system. Hence, it would be clearer to argue measurement-based computation rather than a standard computation in generalized probabilistic theories since we do not have to define a set of allowed operations in generalized probabilistic theories.

Raussendorf et al. showed that adaptive MBQC with linear side-processing using a polynomial-size cluster state can simulate polynomial-size quantum circuit [20]. Anders and Browne observed that adaptive MBQC with linear side-processing using polynomially many tripartite GHZ states can simulate polynomial-size classical circuit [1]. Raussendorf showed that adaptive measurement-based classical computation can compute only affine Boolean functions [19]. Hoban et al. showed that $\mathrm{NMQC}_{\oplus}$ can compute arbitrary Boolean function by using expo-

Table 1. Classes of Boolean functions computable by measurement-based computation with linear side-processing. A, N, E and P stand for "adaptive", "non-adaptive", "exact" and "probabilistic (bounded-error)", respectively.

Theory	Computable	Efficiently computable
Local realistic theory	Affine (AP) [19]	
Quantum theory	Any (NE) [11]	$\mathsf{BQP/qpoly}$ (AP) [20] Restricted (NE) [11]
No-signaling theory	Any (NE)	

nentially large generalized GHZ state [11] on the basis of Werner and Wolf's theorem [25]. Furthermore, they showed that the exact computation of AND_n by $\mathrm{NMQC}_{\oplus}$ requires $2^n - 1$ qubits, which means that computational power of efficient $\mathrm{NMQC}_{\oplus}$ is limited. On the other hand, measurement-based computation with linear side-processing in general no-signaling theory has unlimited computational power since a probability distribution

$$\Pr(\mathsf{a}_1, \ldots, \mathsf{a}_n \mid \mathsf{x}_1, \ldots, \mathsf{x}_n) = \begin{cases} \frac{1}{2^{n-1}}, & \text{if } \bigoplus_{i\in[n]} \mathsf{a}_i = f(\mathsf{x}) \\ 0, & \text{otherwise} \end{cases}$$

for arbitrary Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ satisfies the no-signaling condition. Hence, in general no-signaling theory, the required number of "generalized bits" in non-adaptive measurement-based computation with linear side-processing for arbitrary Boolean function f is at most n, and is equal to the linear sketch complexity of f. Note that here, we do not consider the computational complexity for generating the above state since that is a computation independent of input and can be computed before an input is given. We are able to argue computational complexity after an input is given. We may regard this setting as the "non-uniform setting", and regard the above prepared state as "non-classical advice". These results are summarized in Table 1. Understanding $\mathrm{NMQC}_{\oplus}$ would be important for characterizing quantum physics since general no-signaling theory with linear side-processing allows us to compute arbitrary Boolean function efficiently. The periodic Fourier sparsity of Boolean function is equal to the required number of qubits for exact computation by $\mathrm{NMQC}_{\oplus}$. Hence, in this work, we mainly investigate efficiencies of exact computations by $\mathrm{NMQC}_{\oplus}$, which is the part corresponding to "Restricted (NE)" in Table 1.

1.4 Our results

In this work, we first show some techniques for obtaining periodic Fourier representations (3) with small periodic Fourier sparsity on the basis of $\mathbb{R}$-multilinear, $\mathbb{F}_2$-multilinear and $\mathbb{Z}/4\mathbb{Z}$-multilinear polynomials. More precisely, Boolean functions with small Fourier sparsity or low $\mathbb{F}_2$-degree have a small periodic Fourier sparsity. Furthermore, Boolean functions related with $\mathbb{Z}/4\mathbb{Z}$-polynomial have a small periodic Fourier sparsity as well. For instance, the complete quadratic function, $\mathsf{CQ}_n(\mathsf{x}) := \bigoplus_{1\le i<j\le n} \mathsf{x}_i \wedge \mathsf{x}_j = \lfloor \big(\sum_{i\in[n]} \mathsf{x}_i \mod 4\big)/2 \rfloor$ has the periodic Fourier sparsity $n+1$ on the basis of the $\mathbb{Z}/4\mathbb{Z}$-multilinear polynomial representation while Fourier representation and $\mathbb{F}_2$-polynomial representation give periodic Fourier sparsities $2^n - 1$ and $n(n+1)/2$, respectively. Currently, we do not know any other method for obtaining a periodic Fourier representation.

Next, we show some lower bounds for the periodic Fourier sparsity of Boolean functions.

Hoban et al. showed that the periodic Fourier sparsity of AND_n is 2^n-1 [11]. However, AND_n can be approximated by low $\mathbb{F}_2$-degree polynomial including random input variables [23], and hence, can be computed efficiently with bounded error by $\mathrm{NMQC}_\oplus$ using the above technique. In this work, we show that the periodic Fourier sparsity of a Boolean function f is at least $2^{\deg_{\mathbb{F}_2}(f)}-1$. Hence, periodic Fourier sparsities of Mod_n^3 and Maj_n are at least $2^{n-1}-1$ and $2^{2^{\lfloor \log n \rfloor}}-1$, respectively. Since these Boolean functions cannot be approximated by low $\mathbb{F}_2$-degree polynomial [23], we can expect that these Boolean functions cannot be computed efficiently by $\mathrm{NMQC}_\oplus$ even with bounded error. Let $\mathsf{ENMQC}_\oplus$ be a class of Boolean functions which can be exactly computed by $\mathrm{NMQC}_\oplus$ with a polynomial number of qubits, i.e., $\mathsf{ENMQC}_\oplus$ is a class of Boolean functions with polynomial periodic Fourier sparsity.

Theorem 1. *The periodic Fourier sparsity of Boolean function f is at least $2^{\deg_{\mathbb{F}_2}(f)}-1$. Hence, Mod_n^3 and Maj_n are not in $\mathsf{ENMQC}_\oplus$.*

Let $\mathsf{QNC}_\mathsf{f}^0$ be a class of Boolean functions which can be exactly computed by polynomial-size constant-depth quantum circuit with fan-out gates [10], [12], [24]. Obviously, $\mathsf{ENMQC}_\oplus \subseteq \mathsf{QNC}_\mathsf{f}^0$ as shown in Appendix A. Since $\mathsf{AND}_n, \mathsf{Mod}_n^3, \mathsf{Maj}_n \in \mathsf{QNC}_\mathsf{f}^0$ [24], we obtain $\mathsf{ENMQC}_\oplus \subsetneq \mathsf{QNC}_\mathsf{f}^0$. It is also easy to see $\mathsf{ENMQC}_\oplus \subsetneq \mathsf{TC}^0$ where TC^0 is a class of Boolean functions which can be computed by polynomial-size constant-depth circuit with $\wedge, \neg, \mathsf{Maj}_n$ gates as shown in Appendix A. On the other hand, $\mathsf{QNC}_\mathsf{f}^0$ circuits which exactly compute AND_n, Mod_n^3 and Maj_n can be directly transformed into "depth-2" $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits in which outputs of $\mathrm{NMQC}_\oplus$ in the first layer are used as inputs of $\mathrm{NMQC}_\oplus$ in the second layer where quantum states used in the first layer and the second layer are not entangled [12], [24].

Theorem 2. *Any symmetric Boolean function, e.g., AND_n, Mod_n^3, Maj_n, etc., can be computed exactly by depth-2 $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits.*

Theorem 2 shows a significant gap between $\mathrm{NMQC}_\oplus$, which requires exponentially many qubits for AND_n, Mod_n^3 and Maj_n, and depth-2 $\mathrm{NMQC}_\oplus$, which only needs polynomially many qubits for these Boolean functions. Note that polynomial-depth $\mathrm{NMQC}_\oplus$ is not equivalent to general adaptive MBQC since in polynomial-depth $\mathrm{NMQC}_\oplus$, if a measurement outcome of a qubit q_0 is used for a measurement choice for a qubit q_1, then q_0 and q_1 must be originally separable. Theorem 2 also implies that constant-depth $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits can compute any Boolean functions in TC^0.

Furthermore, since $\mathsf{AC}_\oplus^0$, a class of Boolean functions computed by polynomial-size constant-depth circuit using $\wedge, \oplus, \neg$ gates, cannot compute the majority function [23], [21], we obtain the following theorem on a weak sampling of $\mathrm{NMQC}_\oplus$.

Theorem 3. *For any $\mathrm{NMQC}_\oplus$ with a polynomial number of qubits which does not necessarily compute some Boolean function exactly, there is generally no $\mathsf{AC}_\oplus^0$ circuit whose output is in a support of output distribution of the given $\mathrm{NMQC}_\oplus$ for any input.*

It has been conjectured that an ACC^0 circuit, which is an $\mathsf{AC}_\oplus^0$ circuit with Mod_n^k gates for arbitrary fixed integer k, cannot compute Maj_n. If this conjecture is true, Theorem 3 holds also for ACC^0 in place of $\mathsf{AC}_\oplus^0$.

1.5 Organization

Notion and notations used in this paper are introduced in Section 2. Methods for deriving periodic Fourier representations are shown in Section 3. In Section 4, we show methods for deriving lower bounds of periodic Fourier sparsity, and show exponential lower bounds for Mod_n^3 and Maj_n. In Section 5, we show depth-2 $\mathrm{NMQC}_\oplus$ algorithms using a polynomial number of qubits computing AND_n, Mod_n^3 and Maj_n. In Section 6, well-known multipartite Bell inequalities are understood as $\mathrm{NMQC}_\oplus$ for partial functions. Some algebraic techniques useful for multipartite XOR game are shown as well. In Section 7, we generalize the periodic Fourier sparsity for $\mathrm{NMQC}_\oplus$ with bounded error, and show a relationship between the number of binary digits of coefficients $(\phi_S)_{S\subseteq[n]}$ and $\mathbb{F}_2$-degree.

2 Preliminaries

2.1 Fourier representation

Any function $f\colon \{+1,-1\}^n \to \mathbb{R}$ can be uniquely represented by a $\mathbb{R}$-multilinear polynomial

$$f(x) = \sum_{S\subseteq[n]} \widehat{f}(S) \prod_{i\in S} x_i$$

where $[n] := \{1,2,\dots,n\}$. Here, $\widehat{f}(S)$, which is called the Fourier coefficient, satisfies

$$\widehat{f}(S) = \mathbb{E}\left[f(x)\prod_{i\in S} x_i\right] := \frac{1}{2^n}\sum_{x\in\{+1,-1\}^n} f(x)\prod_{i\in S} x_i.$$

The Fourier sparsity is defined to be the number of non-zero Fourier coefficients. An $\mathbb{R}$-degree of f is defined by $\deg_{\mathbb{R}}(f) := \max\{|S| \mid S\subseteq[n], \widehat{f}(S)\neq 0\}$. Let $\mathbb{R}_\ell := \{x\in\mathbb{R} \mid 2^\ell x\in\mathbb{Z}\}$. Then, for Boolean function $f\colon\{+1,-1\}^n\to\{+1,-1\}$, $\widehat{f}(S)\in\mathbb{R}_{\deg_{\mathbb{R}}(f)-1}$ [17]. The Fourier dimension $\dim(\widehat{f})$ of f is defined by the dimension of linear space on $\mathbb{F}_2$ spanned by $\{1_S \mid S\subseteq[n], \widehat{f}(S)\neq 0\}$ where $1_S\in\mathbb{F}_2^n$ is the vector whose i-th element is 1 if and only if $i\in S$. In this paper, for a binary variable $x\in\{+1,-1\}$, x denotes the corresponding variable in $\{0,1\}$, i.e., $\mathsf{x} = (1-x)/2$. Similarly, we sometimes regard a Boolean function as $\{0,1\}^n\to\{0,1\}$ rather than $\{+1,-1\}^n\to\{+1,-1\}$. This is not necessarily explicitly stated. In this paper, when we consider a Fourier coefficient $\widehat{f}(S)$ of a Boolean function f, f is always regarded as $\{+1,-1\}^n\to\{+1,-1\}$.

2.2 $\mathbb{F}_2$-polynomial representation

Any Boolean function $f\colon\{0,1\}^n\to\{0,1\}$ can be uniquely represented by an $\mathbb{F}_2$-multilinear polynomial

$$f(\mathsf{x}) = \bigoplus_{S\subseteq[n]} c_S \prod_{i\in S} \mathsf{x}_i.$$

Here, a coefficient c_S satisfies

$$c_S = \bigoplus_{\mathsf{x},\,\mathrm{supp}(\mathsf{x})\subseteq S} f(\mathsf{x}) \tag{5}$$

where $\mathrm{supp}(\mathsf{x}) := \{i\in[n] \mid \mathsf{x}_i = 1\}$. An $\mathbb{F}_2$-degree of f is defined by $\deg_{\mathbb{F}_2}(f) := \max\{|S| \mid S\subseteq[n], c_S\neq 0\}$.

2.3 Periodic Fourier representation

Any Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ can be (not uniquely) represented by

$$f(x) = \cos\left(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\right).$$

Here, the number of non-zero coefficients corresponding to non-empty subset $|\{S \subseteq [n] \mid S \neq \varnothing, \phi_S \neq 0\}|$ is called the periodic Fourier sparsity of the representation. The periodic Fourier sparsity $\mathsf{pfs}(f)$ of f is defined by the minimum of periodic Fourier sparsities of all periodic Fourier representations of f. For a coefficient ϕ_S, the unique k such that $\phi_S \in \mathbb{R}_k \setminus \mathbb{R}_{k-1}$ is called the number of binary digits of ϕ_S. A maximum of the numbers of binary digits of ϕ_S for all $S \subseteq [n]$ is called the number of binary digits of a periodic Fourier representation. Without loss of generality, we can assume that $\phi_S \notin \mathbb{R}_0$ for $S \neq \varnothing$. Since $\sin(\pi x) = \cos(\pi(x - \frac{1}{2}))$, the periodic Fourier sparsity and the number of binary digits of non-constant Boolean function are invariant even if a periodic Fourier representation (3) uses the sine function in place of the cosine function. Hence, we will sometimes use (3) with the sine function.

2.4 Specific Boolean functions

In this section, we will introduce specific Boolean functions which appear in this paper. The subscript $_n$ stands for the number of input variables. In the following explanations, we assume that Boolean functions are $\{0,1\}^n \to \{0,1\}$.

- XOR_n: The XOR function.
- AND_n: The AND function.
- OR_n: The OR function.
- Maj_n: The majority function. The number n of input variables is assumed to be odd.
- CQ_n: The complete quadratic function, i.e., $\mathsf{CQ}_n(\mathsf{x}) := \bigoplus_{1\le i<j\le n} \mathsf{x}_i \wedge \mathsf{x}_j$.
- C^3_n: The complete cubic function, i.e., $\mathsf{C}^3_n(\mathsf{x}) := \bigoplus_{1\le i<j<k\le n} \mathsf{x}_i \wedge \mathsf{x}_j \wedge \mathsf{x}_k$.
- Mod^k_n: The k-modular counting function, i.e., $\mathsf{Mod}^k_n(\mathsf{x}) = 1$ if and only if $\sum_{i\in[n]} \mathsf{x}_i$ is divisible by k.
- Exact^k_n: The k-exactness function, i.e., $\mathsf{Exact}^k_n(\mathsf{x}) = 1$ if and only if $\sum_{i\in[n]} \mathsf{x}_i = k$.

Furthermore, we define $\mathsf{LSB}^\ell\colon \mathbb{Z}_{\ge 0} \to \{0,1\}$ which is the k-th lowest significant bit (LSB) function, i.e., $\mathsf{LSB}^\ell(m) = 1$ if and only if k-th LSB of binary representation of m is 1. Note that $\mathsf{XOR}_n(\mathsf{x}) = \mathsf{LSB}^1\big(\sum_{i\in[n]} \mathsf{x}_\mathsf{i}\big)$ and $\mathsf{CQ}_n(\mathsf{x}) = \mathsf{LSB}^2\big(\sum_{i\in[n]} \mathsf{x}_\mathsf{i}\big)$.

3 Periodic Fourier sparsity: Upper bounds

3.1 $\mathbb{R}$-polynomial and $\mathbb{F}_2$-polynomial

In this section, we consider how to obtain periodic Fourier representations (3) from the Fourier representation and the $\mathbb{F}_2$-polynomial representations. In contrast to the Fourier representation and the $\mathbb{F}_2$-polynomial representation of Boolean functions, a periodic Fourier representation is not unique. For instance, XOR_2 and Maj_3 can be represented in the following two

ways

$$\begin{aligned}\mathsf{XOR}_2(x_1,x_2) &= \sin\left(\frac{\pi}{2}x_1x_2\right)\\ &= \sin\left(\frac{\pi}{2}\left(-1+x_1+x_2\right)\right).\\ \mathsf{Maj}_3(x_1,x_2,x_3) &= \sin\left(\frac{\pi}{4}\left(x_1+x_2+x_3-x_1x_2x_3\right)\right)\\ &= \sin\left(\frac{\pi}{4}\left(-1+2x_1+2x_2+2x_3-x_1x_2-x_2x_3-x_3x_1\right)\right).\end{aligned}$$

While the first representations merely use the Fourier representations, the second representations use the periodicity of the sine function. In the following, we show how to generalize these representations to general Boolean functions. From $f(x) = \sin\left(\frac{\pi}{2}f(x)\right) = \sin\left(\frac{\pi}{2}\sum_{S\subseteq[n]}\widehat{f}(S)\prod_{i\in S}x_i\right)$, we immediately obtain the following construction.

Construction 1. A Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ has a periodic Fourier representation

$$f(x) = \sin\left(\frac{\pi}{2}\sum_{S\subseteq[n]}\widehat{f}(S)\prod_{i\in S}x_i\right)$$

with the periodic Fourier sparsity $|\{S\subseteq[n] \mid S\neq\varnothing, \widehat{f}(S)\neq 0\}|$ and the number of binary digits at most $\deg_{\mathbb{R}}(f)$.

There are Boolean functions whose Fourier sparsity is full but whose $\mathbb{F}_2$-degree is small, e.g., the inner product function, the complete quadratic function of even size, etc [22], [17]. The following construction shows that a Boolean function with low $\mathbb{F}_2$-degree has small periodic Fourier sparsity.

Construction 2. Assume that Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ has the $\mathbb{F}_2$-polynomial representation $f(\mathsf{x}) = \bigoplus_{S\subseteq[n]} c_S \prod_{i\in S}\mathsf{x}_i$ for $(c_S\in\{0,1\})_{S\subseteq[n]}$. Then, f has a periodic Fourier representation (3) where

$$\phi_S = (-1)^{|S|}\sum_{T\supseteq S}\frac{1}{2^{|T|}}c_T \tag{6}$$

with the periodic Fourier sparsity $|\{S\subseteq[n] \mid S\neq\varnothing, \exists T\supseteq S, c_T\neq 0\}| \leq n^{\deg_{\mathbb{F}_2}(f)}$ and the number of binary digits $\deg_{\mathbb{F}_2}(f)$.

Proof. By replacing x_i with $(1-x_i)/2$, we obtain the real-polynomial representation using modulo 2

$$f(x) \equiv \sum_{S\subseteq[n]} c_S \prod_{i\in S}\frac{1-x_i}{2} \mod 2$$

where f at the left-hand side is a function from $\{+1,-1\}^n$ to $\{0,1\}$. Hence,

$$\begin{aligned}f(x) &= \cos\left(\pi\sum_{S\subseteq[n]} c_S\prod_{i\in S}\frac{1-x_i}{2}\right)\\ &= \cos\left(\pi\sum_{S\subseteq[n]} c_S\frac{1}{2^{|S|}}\sum_{T\subseteq S}\prod_{i\in T}(-x_i)\right)\end{aligned}$$

$$= \cos\left(\pi \sum_{T\subseteq[n]} (-1)^{|T|} \left(\sum_{S\supseteq T} \frac{1}{2^{|S|}} c_S\right) \prod_{i\in T} x_i\right)$$

where f at the left-hand side is a function from $\{+1,-1\}^n$ to $\{+1,-1\}$. □

Here, the number of binary digits obtained by Construction 2 is optimal.

Lemma 1. *If f has a periodic Fourier representation* (3) *with $\phi_S \in \mathbb{R}_k$ for all $S \subseteq [n]$, then* $\deg_{\mathbb{F}_2}(f) \le k$.

Proof. For $f\colon \{0,1\}^n \to \{0,1\}$, there is an integer-valued function $t\colon \{+1,-1\}^n \to \mathbb{Z}$, such that

$$\sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i = 2t(x) + f(\mathsf{x}).$$

Hence, from (5),

$$\begin{aligned} c_S &\equiv \sum_{\mathsf{x},\,\mathrm{supp}(\mathsf{x})\subseteq S} \sum_{T\subseteq[n]} \phi_T \prod_{i\in T} (1-2\mathsf{x}_i) \mod 2 \\ &\equiv 2^{|S|} \sum_{T\subseteq \bar{S}} \phi_T \mod 2. \end{aligned}$$

Hence, for $|S| > k$, $c_S = 0$. □

From Constructions 1 and 2, the periodic Fourier representation (3) has both the features of $\mathbb{R}$-polynomial and $\mathbb{F}_2$-polynomial. For the complete quadratic function of even size, Constructions 1 and 2 give the periodic Fourier sparsities $2^n - 1$ and $n(n+1)/2$, respectively. Hence, Construction 2 gives a sparser representation. Conversely, for some Boolean function, Construction 1 gives a sparser representation.

Example 2. For $f(\mathsf{x}) := (\mathsf{x}_1 \oplus \cdots \oplus \mathsf{x}_{n/k}) \wedge \cdots \wedge (\mathsf{x}_{n-n/k+1} \oplus \cdots \oplus \mathsf{x}_n)$ where n is a multiple of an integer k, Constructions 1 and 2 give the periodic Fourier sparsities $2^k - 1$ and $(n/k+1)^k - 1$, respectively. In Section 4, we will show $\mathsf{pfs}(f) \ge 2^{\deg_{\mathbb{F}_2}(f)} - 1$, which shows the optimality of Construction 1 in this case.

The following lemma is useful for obtaining a periodic Fourier representation for $f = g \wedge h$ from periodic Fourier representations for g and h.

Lemma 3. *Let $f_1, f_2, \ldots, f_k$ be Boolean functions on the common input variables $x_1, \ldots, x_n$. Assume f_j has a periodic Fourier representation with a periodic Fourier sparsity s_j and the number of binary digits ℓ_j. Then, $\bigwedge_{j=1}^k f_j$ has a periodic Fourier representation with the periodic Fourier sparsity at most $\prod_{j=1}^k (s_j+1) - 1$ and the number of binary digits at most $\sum_{j=1}^k \ell_j$.*

Proof. From the assumption, there exists a periodic Fourier representation

$$f_j(x) = \cos\left(\pi \sum_{S\subseteq[n]} \phi_S^{(j)} \prod_{i\in S} x_i\right)$$

using $(\phi_S^{(j)} \in \mathbb{R}_{\ell_j})_{S\subseteq[n]}$ for each $j = 1, \ldots, k$. Here, $f_j(x) = -1$ if and only if $\sum_{S\subseteq[n]} \phi_S^{(j)} \prod_{i\in S} x_i$ is an odd integer. Hence,

$$\left(\bigwedge_{j=1}^{k} f_j\right)(x) = \cos\left(\pi \prod_{j=1}^{k}\left(\sum_{S\subseteq[n]} \phi_S^{(j)} \prod_{i\in S} x_i\right)\right).$$

□

Similarly, for $f = g \oplus h$, we obtain $f(x) = \cos(\pi(\widetilde{g}(x) + \widetilde{h}(x)))$ where $\widetilde{g}$ and $\widetilde{h}$ satisfy $g(x) = \cos(\pi\widetilde{g}(x))$ and $h(x) = \cos(\pi\widetilde{h}(x))$. This technique would be useful for $f = g \wedge h$ or $f = g \oplus h$ where Construction 1 is suitable for g and Construction 2 is suitable for h.

3.2 $\mathbb{Z}/4\mathbb{Z}$*-polynomial*

There exist Boolean functions whose periodic Fourier sparsity is smaller than those obtained by Constructions 1 and 2.

Example 4. When n is even, the complete quadratic function CQ_n is a bent function, i.e., $|\widehat{\mathsf{CQ}_n}(S)| = 2^{-n/2}$ for all $S \subseteq [n]$ [17]. Hence, Construction 1 gives the periodic Fourier sparsity $2^n - 1$. Construction 2 gives the periodic Fourier sparsity $n(n+1)/2$. However, the periodic Fourier sparsity of CQ_n is smaller. It is easy to see that $\mathsf{CQ}_n(\mathsf{x})$ is the second LSB in the number of 1s in x as shown in Appendix C. Hence, we obtain the following periodic Fourier representation

$$\mathsf{CQ}_n(x) = \cos\left(\frac{\pi}{2}\left(\sum_{i=1}^{n}\frac{1-x_i}{2} - \frac{1-\prod_{i=1}^{n} x_i}{2}\right)\right)$$

with the periodic Fourier sparsity $n+1$ and the number of binary digits 2. This explains the result in [11] using the periodic Fourier representation.

We can generalize Example 4 as follows.

Construction 3. Assume that a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ has a representation

$$f(\mathsf{x}) = \mathsf{LSB}^2\left(\sum_{S\subseteq[n],|S|\le k} c_S \prod_{i\in S} \mathsf{x}_i\right)$$

using integers $(c_S \in \{0,1,2,3\})_S$. Let

$$g(\mathsf{x}) := \sum_{S\subseteq[n],|S|\le k} c_S \prod_{i\in S} \mathsf{x}_i \mod 2.$$

Then, f has a periodic Fourier representation

$$f(x) = \cos\left(\frac{\pi}{2}\left(\sum_{S\subseteq[n],|S|\le k} c_S \prod_{i\in S}\frac{1-x_i}{2} - \frac{1-\sum_{S\subseteq[n]}\widehat{g}(S)\prod_{i\in S} x_i}{2}\right)\right)$$

with the periodic Fourier sparsity at most $|\{S \subseteq [n] \mid S \neq \varnothing, \exists T \supseteq S, c_T \neq 0\}| + |\{S \subseteq [n] \mid S \neq \varnothing, \widehat{g}(S) \neq 0\}|$ and the number of binary digits at most $\max\{k, \deg_{\mathbb{R}}(g)\} + 1$.

Example 5. The complete cubic function $\mathsf{C}_n^3(\mathsf{x})$ is 1 if $\sum_{i=1}^n \mathsf{x}_i \equiv 3 \mod 4$, and 0 otherwise. From $\mathsf{C}_n^3 = \mathsf{CQ}_n \wedge \mathsf{XOR}_n$, Example 4 and the construction in Lemma 3, we obtain a periodic Fourier representation

$$\begin{aligned}\mathsf{C}_n^3(x) &= \cos\left(\frac{\pi}{2}\left(\sum_{i=1}^n \frac{1-x_i}{2} - \frac{1-\prod_{i=1}^n x_i}{2}\right)\frac{1-\prod_{i=1}^n x_i}{2}\right)\\ &= \cos\left(\frac{\pi}{8}\left(n-2-\sum_{i=1}^n x_i\right)\left(1-\prod_{i=1}^n x_i\right)\right)\end{aligned}$$

with a periodic Fourier sparsity $2n+1$ (or $2n$ when $n \equiv 2 \mod 8$) and the number of binary digits 3 for $n \geq 3$.

Currently, we do not know any Boolean function whose periodic Fourier sparsity is not given by Constructions 1, 2, and 3 or their combination by Lemma 3. Note that Construction 3 cannot be generalized to the third LSB since the Fourier representation for the second LSB has high Fourier sparsity and cannot be used for the cancellation (we cannot use periodic Fourier representations of LSB_n^2 using the periodicity of the cosine function for the cancellation).

4 Periodic Fourier sparsity: Lower bounds

In this section, we show lower bounds of the periodic Fourier sparsity of given Boolean function. Gopalan et al. showed a relationship between the Fourier sparsity and the number of binary digits of the Fourier coefficients [9]. This result can be straightforwardly generalized to the periodic Fourier representation.

Lemma 6 ([9])**.** *For any Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ with a periodic Fourier representation with the periodic Fourier sparsity s, all coefficients ϕ_S in the representation are in $\mathbb{R}_{\lfloor \log(s+1)\rfloor}$.*

Proof. We will prove this lemma by induction on n. For $n = 0$, the lemma obviously holds. For $n \geq 1$, we consider two cases. First, we assume $s = 2^n - 1$. There exists some integer-valued function $t\colon \{+1,-1\}^n \to \mathbb{Z}$ such that

$$\sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i = 2t(x) + \frac{1-f(x)}{2}.$$

For $S \subseteq [n]$,

$$\phi_S = 2\widehat{t}(S) - \frac{\widehat{f}(S)}{2} + \frac{1}{2}\delta_S$$

where δ_S is 1 if S is the empty set, and is 0 otherwise. Here, $\widehat{t}(S) \in \mathbb{R}_n$ since $t(x)$ is an integer-valued function. Since $\widehat{f}(S) \in \mathbb{R}_{n-1}$, we obtain $\phi_S \in \mathbb{R}_n$ for $n \geq 1$.

Second, we assume $s < 2^n - 1$. In this case, there exists a non-empty $S^* \subseteq [n]$ such that $\phi_{S^*} = 0$. We will show $\phi_U \in \mathbb{R}_{\lfloor \log(s+1)\rfloor}$ for arbitrary $U \subseteq [n]$ not equal to S^*. Let $i^* \in [n]$ be an index included only by one of S^* and U. Let $V := (S^* \oplus U) \setminus \{i^*\}$ where $\oplus$ stands for the symmetric difference of two sets. Let $h\colon \{+1,-1\}^{n-1} \to \{+1,-1\}$ be

$$h(x_1,\ldots,x_{i^*-1},x_{i^*+1},\ldots,x_n) := f\left(x_1,\ldots,x_{i^*-1},\prod_{i\in V} x_i, x_{i^*+1},\ldots,x_n\right).$$

We can straightforwardly obtain a periodic Fourier representation of h from that of f by replacing x_{i^*} with $\prod_{i\in V} x_i$. In this transformation, two terms for $S \subseteq [n] \setminus \{i^*\}$ and $(S \oplus V) \cup \{i^*\}$ are merged into a single term. In the above transform, $\phi_{S^*} = 0$ and ϕ_U are merged, which means that ϕ_U is still one of the coefficient in the periodic Fourier representation of h. The periodic sparsity of the representation of h is obviously at most s. Hence, from the induction hypothesis, we obtain $\phi_U \in \mathbb{R}_{\lfloor \log(s+1) \rfloor}$. □

From Lemmas 1 and 6, we obtain Theorem 1, i.e., $\mathsf{pfs}(f) \geq 2^{\deg_{\mathbb{F}_2}(f)} - 1$. For Mod_n^3, this lower bound matches the upper bound obtained by Construction 1.

Lemma 7. *For n divisible by 3, $\mathsf{pfs}(\mathsf{Mod}_n^3) = 2^{n-1} - 1$. For n not divisible by 3, $\mathsf{pfs}(\mathsf{Mod}_n^3) = 2^n - 1$.*

Proof. From (5), it is easy to see that $\deg_{\mathbb{F}_2}(\mathsf{Mod}_n^3)$ is equal to $n-1$ if n is divisible by 3, and is equal to n if n is not divisible by 3. Hence, from Theorem 1, we obtain the lower bounds. From Construction 1 and the Fourier representation shown in Appendix B, we obtain the upper bounds. □

Finally, we show the following lower bound, which is at most $n+1$ but useful for showing the optimality of Example 4.

Lemma 8. *For a Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ with $\deg_{\mathbb{F}_2}(f) \geq 2$, $\mathsf{pfs}(f) \geq \dim(\widehat{f}) + 1$.*

Proof. $\mathsf{pfs}(f) \geq \dim(\widehat{f})$ since the Fourier dimension is the linear sketch complexity [15]. We assume $\mathsf{pfs}(f) = \dim(\widehat{f})$. Then, all monomials in a periodic Fourier representation (3) are linearly independent. Hence, we can control each term independently, that implies all non-zero coefficients ϕ_S must be in $\mathbb{R}_1$. In that case, f must be an affine function, i.e., $\deg_{\mathbb{F}_2}(f) \leq 1$. □

5 Depth-2 $\mathrm{NMQC}_\oplus$ algorithms for AND_n, Mod_n^3 and Maj_n

In Section 4, we showed that AND_n, Mod_n^3 and Maj_n cannot be exactly computed by $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits. Interestingly, $\mathsf{QNC}_\mathsf{f}^0$ circuits which exactly compute the above Boolean functions can be directly transformed into "depth-2" $\mathrm{NMQC}_\oplus$ [12], [24].

Definition 9 (Depth-d $\mathrm{NMQC}_\oplus$)**.** Depth-d $\mathrm{NMQC}_\oplus$ consists of d layers of $\mathrm{NMQC}_\oplus$. Qubits used in the same layers could be entangled. However, qubits used in different layers have to be separable. At the first layer, qubits are locally measured according to $\mathbb{F}_2$-linear functions of input x. At i-th layer, qubits are locally measured according to $\mathbb{F}_2$-linear functions of input x and outcomes $a_1, \ldots, a_{i-1}$ of the previous layers for $i \in [d]$ where a_i denotes the outcomes of the local measurements at i-th layer. An output of depth-d $\mathrm{NMQC}_\oplus$ is an $\mathbb{F}_2$-linear function of all outcomes $a_1, \ldots, a_d$ of the local measurements.

Proof of Theorem 2. We first sketch the depth-2 $\mathrm{NMQC}_\oplus$ algorithm for OR_n function [12], [24]. For each $k \in \{0, 1, \ldots, \lfloor \log n \rfloor\}$, $\mathrm{NMQC}_\oplus$ can compute $Z_k \in \{+1, -1\}$ with expectation

$$\mathbb{E}[Z_k] = \cos\left(\frac{\pi}{2^k} \sum_{i\in[n]} \frac{1 - x_i}{2}\right) \tag{7}$$

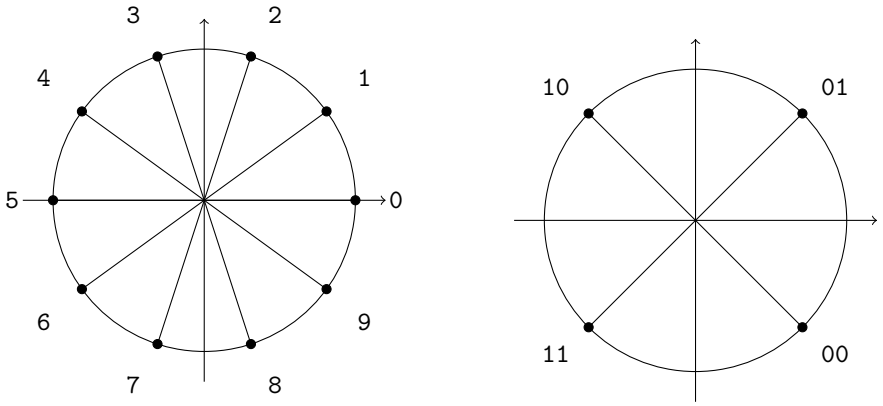


Fig. 1. Left: Generalized the GHZ–Mermin paradox for P_n^5. Right: Maximum violation of Svetlichny's inequality by Belinskiĭ and Klyshko.

by using n qubits. If x is all-zero, $Z_k = +1$ with probability 1 for all k. If x is not all-zero, $\sum_{i\in[n]} \mathsf{x}_i = 2^{k^*}h$ for some positive integer k^* and a positive odd integer h. Hence, $Z_{k^*} = -1$ with probability 1. The above $\mathrm{NMQC}_\oplus$ algorithm reduces OR_n function to $\mathsf{OR}_{\lfloor \log n \rfloor+1}$ function. Then, we can apply the $\mathrm{NMQC}_\oplus$ algorithm using exponentially many qubits to $\mathsf{OR}_{\lfloor \log n \rfloor+1}$. The total number of qubits used in the depth-2 $\mathrm{NMQC}_\oplus$ algorithm is $(\lfloor \log n \rfloor + 1)n + 2^{\lfloor \log n \rfloor+1} - 1$. By introducing an appropriate constant term in (7), we obtain a depth-2 $\mathrm{NMQC}_\oplus$ algorithm for Exact_n^k using the same number of qubits. By taking a parity of Exact_n^k for appropriate ks, we obtain depth-2 $\mathrm{NMQC}_\oplus$ algorithms for arbitrary symmetric Boolean function including Mod_n^3 and Maj_n. □

Hence, there is an exponential gap between $\mathrm{NMQC}_\oplus$ and depth-2 $\mathrm{NMQC}_\oplus$. From the above depth-2 $\mathrm{NMQC}_\oplus$ algorithm for Maj_n, we obtain Theorem 3 since $\mathsf{AC}^0_\oplus$ cannot compute the majority function [23], [21]. Conversely, $\mathrm{NMQC}_\oplus$ with a quasi-polynomially many qubits can simulate $\mathsf{AC}^0_\oplus$ circuit with bounded error by Construction 2 since $\mathsf{AC}^0_\oplus$ circuit can be approximated by an $\mathbb{F}_2$-polynomial including random input variables of $\mathbb{F}_2$-degree $\mathsf{poly}(\log \frac{n}{\epsilon})$ with error probability at most ϵ [23]. Theorem 2 implies that constant-depth $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits can compute Boolean functions in TC^0. However, it is an open question whether constant-depth $\mathrm{NMQC}_\oplus$ using a polynomial number of qubits can compute Boolean functions not in TC^0. If qubits used in different layers are allowed to be entangled, constant-depth measurement-based quantum computation has the same computational power as $\mathsf{QNC}^0_\mathsf{f}$ [7].

6 Partial function and multipartite Bell inequalities

In this section, we briefly introduce some partial functions which can be exactly computed by $\mathrm{NMQC}_\oplus$ with n qubits. The following examples have been known in the context of multipartite Bell inequalities. However, to the knowledge of the author, intuitive graphical interpretations by angles on a unit circle using Werner and Wolf's characterization (4) have

not been shown. A partial Boolean function $P_n^k\colon \{+1,-1\}^n \to \{+1,-1\}$ is defined by

$$P_n^k(x) := \begin{cases} +1, & \text{if } \sum_{i\in[n]} \mathsf{x}_i \equiv 0 \mod 2k \\ -1, & \text{if } \sum_{i\in[n]} \mathsf{x}_i \equiv k \mod 2k. \end{cases}$$

This partial Boolean function can be represented by

$$P_n^k(x) = \cos\left(\frac{\pi}{k}\sum_{i\in[n]}\frac{1-x_i}{2}\right).$$

This is a simple generalization of the GHZ–Mermin paradox [5]. Note that this idea was used in (7) in which there is k on which the above promise is satisfied. This idea is useful for total functions with bounded error and for multipartite Bell inequalities as well. The complete quadratic function $\mathsf{CQ}_n(x)$, which is the second LSB of $\sum_{i\in[n]}\mathsf{x}_i$, satisfies

$$\frac{1}{\sqrt{2}}\mathsf{CQ}_n(x) = \cos\left(\frac{\pi}{2}\left(-\frac{1}{2}+\sum_{i\in[n]}\frac{1-x_i}{2}\right)\right).$$

This argument quite simply explains Belinskiĭ and Klyshko's maximum quantum violation of Svetlichny's inequality, which is a generalization of maximum quantum violation of CHSH inequality [14]. Fig. 1 shows graphical interpretations of the above quantum algorithms.

The complete quadratic function CQ_n is useful for computing general XOR functions distributively. Multipartite XOR game for XOR function is an important problem in the context of foundations of quantum physics [6], [14], [16]. An n-partite distributive AND function can be computed by

$$\begin{aligned}\mathsf{AND}_2\left(\bigoplus_{i=1}^n \mathsf{x}_1^i, \bigoplus_{i=1}^n \mathsf{x}_2^i\right) &= \mathsf{CQ}_{2n}(\mathsf{x}_1^1,\dots,\mathsf{x}_2^n) \oplus \mathsf{CQ}_n(\mathsf{x}_1^1,\dots,\mathsf{x}_1^n) \\ &\quad \oplus \mathsf{CQ}_n(\mathsf{x}_2^1,\dots,\mathsf{x}_2^n)\end{aligned}$$

where x_1^i and x_2^i are inputs for i-th player for $i \in [n]$. Hence, any $\mathbb{F}_2$-quadratic Boolean function can be distributively computed by using CQ_n, e.g., the majority function on 3 bits $\mathsf{Maj}_3(\mathsf{x},\mathsf{y},\mathsf{z}) = \mathsf{CQ}_3(\mathsf{x},\mathsf{y},\mathsf{z}) = \mathsf{x}\wedge\mathsf{y}\oplus\mathsf{y}\wedge\mathsf{z}\oplus\mathsf{z}\wedge\mathsf{x}$ can be distributively computed by

$$\begin{aligned}\mathsf{Maj}_3\left(\bigoplus_{i=1}^n \mathsf{x}^i, \bigoplus_{i=1}^n \mathsf{y}^i, \bigoplus_{i=1}^n \mathsf{z}^i\right) &= \mathsf{CQ}_{2n}(\mathsf{x},\mathsf{y}) \oplus \mathsf{CQ}_n(\mathsf{x}) \oplus \mathsf{CQ}_n(\mathsf{y}) \\ &\quad \oplus \mathsf{CQ}_{2n}(\mathsf{y},\mathsf{z}) \oplus \mathsf{CQ}_n(\mathsf{y}) \oplus \mathsf{CQ}_n(\mathsf{z}) \\ &\quad \oplus \mathsf{CQ}_{2n}(\mathsf{z},\mathsf{x}) \oplus \mathsf{CQ}_n(\mathsf{z}) \oplus \mathsf{CQ}_n(\mathsf{x}) \\ &= \mathsf{CQ}_{2n}(\mathsf{x},\mathsf{y}) \oplus \mathsf{CQ}_{2n}(\mathsf{y},\mathsf{z}) \oplus \mathsf{CQ}_{2n}(\mathsf{z},\mathsf{x}).\end{aligned}$$

Hence, Maj_3 can be distributively computed with bias $2^{-3/2}$ in quantum theory. This argument explains techniques in [14] in the algebraic way. As another example, an n-partite distributive complete quadratic function can be computed by

$$\mathsf{CQ}_m\left(\bigoplus_{i=1}^n \mathsf{x}_1^i, \bigoplus_{i=1}^n \mathsf{x}_2^i, \cdots, \bigoplus_{i=1}^n \mathsf{x}_m^i\right) = \mathsf{CQ}_{nm}(\mathsf{x}) \oplus \bigoplus_{j=1}^m \mathsf{CQ}_n(\mathsf{x}_j)$$

with bias $2^{-(m+1)/2}$ in quantum theory.

7 Discussions on $\mathrm{NMQC}_{\oplus}$ with bounded error

Obviously, bounded-error computational complexities are much more important than zero-error computational complexities in general. We can consider two models of bounded-error $\mathrm{NMQC}_{\oplus}$. In the first setting, we consider the best $\mathrm{NMQC}_{\oplus}$ algorithm for given input distribution. In this case, from Werner and Wolf's theorem (4), it is sufficient to consider Werner and Wolf's $\mathrm{NMQC}_{\oplus}$ algorithms, which use shared generalized GHZ state and particular type of local measurements. The required number of qubits is represented by the following approximate periodic Fourier sparsity.

Definition 10. For a Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$, an input distribution μ on $\{+1,-1\}^n$ and an error probability $\epsilon \in [0,1/2)$, an approximate periodic Fourier sparsity $\widetilde{\mathsf{pfs}}_{\mu,\epsilon}(f)$ is defined by

$$\widetilde{\mathsf{pfs}}_{\mu,\epsilon}(f) := \min\left\{\mathsf{pfs}(g) \mid g\colon \{+1,-1\}^n \to [-1,+1],\, \mathbb{E}_{x\sim\mu}[|f(x)-g(x)|] \le 2\epsilon\right\}.$$

Let $F\colon \{+1,-1\}^n \to \{+1,-1\}$ be a probabilistic Boolean function such that $F(x) = +1$ with probability $(1+g(x))/2$. Since $|f(x)-g(x)| = 1 - f(x)g(x)$, $\Pr_{F,x\sim\mu}(F(x) \neq f(x)) = \mathbb{E}_{F,x\sim\mu}[(1-F(x)f(x))/2] = \mathbb{E}_{x\sim\mu}[(1-g(x)f(x))/2] = \mathbb{E}_{x\sim\mu}[|f(x)-g(x)|/2] \le \epsilon$. Hence, $\widetilde{\mathsf{pfs}}_{\mu,\epsilon}(f)$ is equal to the required number of qubits for computing f with error probability at most ϵ on input distribution μ. From the minimax theorem, $\max_{\mu} \widetilde{\mathsf{pfs}}_{\mu,\epsilon}(f)$ is equal to the number of required qubits for probabilistic $\mathrm{NMQC}_{\oplus}$ algorithm computing f with error probability at most ϵ for any input. Here, a probabilistic $\mathrm{NMQC}_{\oplus}$ algorithm has to randomly choose a set of parities used in the computation. Hence, this computational model does not necessarily have a deterministic linear side-processor. In the second setting, we consider (not probabilistic) general $\mathrm{NMQC}_{\oplus}$ algorithms with error probability at most ϵ for any input. For a fixed set $\mathcal{T} \subseteq 2^{[n]} \setminus \{\varnothing\}$ of parities used in $\mathrm{NMQC}_{\oplus}$, we can apply the minimax theorem. Hence, there is an $\mathrm{NMQC}_{\oplus}$ algorithm using parities in $\mathcal{T}$ which computes f with error probability at most ϵ for any input if and only if there exist random variables $(\Phi_S \in \mathbb{R})_{S\in\mathcal{T}\cup\{\varnothing\}}$ such that

$$\left| f(x) - \mathbb{E}_{\Phi}\left[\cos\left(\Phi_{\varnothing} + \sum_{S\in\mathcal{T}} \Phi_S \prod_{i\in S} x_i\right)\right]\right| \le 2\epsilon \tag{8}$$

for any $x \in \{+1,-1\}^n$. Note that a corresponding $\mathrm{NMQC}_{\oplus}$ algorithm uses generalized GHZ state and local measurements $\mathbb{E}_{\Phi}[\cos(\pi(\Phi_S \prod_{i\in S} x_i + \Phi_{\varnothing}/|\mathcal{T}|))X + \sin(\pi(\Phi_S \prod_{i\in S} x_i + \Phi_{\varnothing}/|\mathcal{T}|))Y]$ for $S \in \mathcal{T}$. The required number of qubits is represented by the following approximate periodic Fourier sparsity.

Definition 11. For a Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and an error probability $\epsilon \in [0,1/2)$, an approximate periodic Fourier sparsity $\widetilde{\mathsf{pfs}}_{\epsilon}(f)$ is defined by minimum $|\mathcal{T}|$ among all $\mathcal{T} \subseteq 2^{[n]} \setminus \{\varnothing\}$ satisfying (8).

From the above argument, $\max_{\mu} \widetilde{\mathsf{pfs}}_{\mu,\epsilon}(f) \le \widetilde{\mathsf{pfs}}_{\epsilon}(f)$. Note that in the context of query complexity, approximate $\mathbb{R}$-degree with respect to the infinity norm plays a similar role of approximate Fourier sparsities although it only gives a lower bound of quantum query complexity [4]. Deriving lower bounds of these approximate periodic Fourier sparsities is an open problem. A connection between the number of binary digits of approximate periodic Fourier representation and $\mathbb{F}_2$-degree of f can be obtained similarly to Lemma 1.

Theorem 4. *Assume that a Boolean function $f\colon \{+1,-1\}^n \to \{+1,-1\}$ satisfying (8) for $\mathcal{T} = 2^{[n]} \setminus \{\varnothing\}$ using random variables $(\Phi_S \in \mathbb{R}_\ell)_{S\subseteq[n]}$. Then, there is a probabilistic polynomial p of $\mathbb{F}_2$-degree at most $2^\ell - 1$ satisfying $\Pr_p(p(x) \neq f(x)) \leq \epsilon$ for any $x \in \{+1,-1\}^n$.*

Proof. We will construct a probabilistic polynomial of $\mathbb{F}_2$-degree at most $2^\ell - 1$ which is equal to 0 with probability exactly equal to $(1 + \cos(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i)/2$ for each realization $(\phi_S)_{S\subseteq[n]}$ of $(\Phi_S)_{S\subseteq[n]}$. For each $S \subseteq [n]$, we define $\bar{\phi}_S := 2^\ell \phi_S$, which is guaranteed to be an integer from the assumption. $\cos\bigl(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\bigr)$ is equal to $\cos\bigl(\pi\bigl(-\sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i + 2k\bigr)\bigr)$ for any integer k. Let $k = \lceil \frac{1}{2} \sum_{S\subseteq[n]} \phi_S \rceil$ so that $2k - \sum_{S\subseteq[n]} \phi_S \geq 0$. Then, $\cos\bigl(\pi\bigl(\sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\bigr)\bigr)$ is determined by $y_i(x) := \mathsf{LSB}^{i+1}\left(-\sum_{S\subseteq[n]} \bar{\phi}_S \prod_{i\in S} x_i + k2^{\ell+1}\right)$ for $i = 0, 1, \ldots, \ell$. Obviously, y_0 is a constant function. For $i \geq 1$,

$$\begin{aligned} y_i(x) &= \mathsf{LSB}^{i+1}\left(-\sum_{S\subseteq[n]} \bar{\phi}_S \prod_{i\in S} x_i + k2^{\ell+1}\right) = \mathsf{LSB}^{i+1}\left(\sum_{S\subseteq[n]} \bar{\phi}_S \left(2\bigoplus_{i\in S} \mathsf{x}_i - 1\right) + k2^{\ell+1}\right) \\ &= \mathsf{LSB}^{i+1}\left(2\sum_{S\subseteq[n]} \bar{\phi}_S \bigoplus_{i\in S} \mathsf{x}_i + \left(k2^{\ell+1} - \sum_{S\subseteq[n]} \bar{\phi}_S\right)\right) \\ &= \mathsf{LSB}^{i}\left(\sum_{S\subseteq[n]} \bar{\phi}_S \bigoplus_{i\in S} \mathsf{x}_i + \left\lfloor \frac{k2^{\ell+1} - \sum_{S\subseteq[n]} \bar{\phi}_S}{2} \right\rfloor\right). \end{aligned}$$

We can obtain an explicit $\mathbb{F}_2$-polynomial representation of $y_i(x)$ by using the following lemma.

Lemma 12. *For $\ell \geq 1$,*

$$\mathsf{LSB}^\ell\left(\sum_{i\in[n]} \mathsf{x}_i\right) = \bigoplus_{1\leq i_1<i_2<\cdots<i_{2^{\ell-1}}\leq n} \bigwedge_{j=1}^{2^{\ell-1}} \mathsf{x}_{i_j}.$$

The proof is shown in Appendix C. From Lemma 12, $y_i(x)$ has $\mathbb{F}_2$-degree at most 2^{i-1} for $i \geq 1$. Then, $\cos(\sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i) = \cos(\sum_{i=0}^{\ell} 2^{-i} y_{\ell-i}(x))$. Let Z be a random variable uniformly distributed in $[0,1]$ which is a randomness used in the probabilistic polynomial. Let

$$S := \begin{cases} 0, & \text{if } \frac{1+\cos\left(\pi \sum_{i=0}^{\ell} 2^{-i} y_{\ell-i}(x)\right)}{2} > Z \\ 1, & \text{otherwise.} \end{cases}$$

Then, S is equal to 0 with probability

$$\frac{1 + \cos\left(\pi \sum_{i=0}^{\ell} 2^{-i} y_{\ell-i}\right)}{2} = \frac{1 + \cos\left(\pi \sum_{S\subseteq[n]} \phi_S \prod_{i\in S} x_i\right)}{2}$$

Since $y_i(x)$ have $\mathbb{F}_2$-degree at most 2^{i-1} for $i \in [\ell]$, a probabilistic polynomial computing S has $\mathbb{F}_2$-degree at most $2^{\ell-1} + 2^{\ell-2} + \cdots + 2^0 = 2^\ell - 1$. By using the randomness of $(\Phi_S)_{S\subseteq[n]}$, we obtain a probabilistic polynomial of $\mathbb{F}_2$-degree at most $2^\ell - 1$ with error probability at most ϵ. □

Hence, a Boolean function which can be computed with bounded error by $\mathrm{NMQC}_\oplus$ with constant number of binary digits can be approximated by probabilistic $\mathbb{F}_2$-polynomial of constant degree.

Acknowledgment

This work was supported by JST PRESTO Grant Number JPMJPR1867 and JSPS KAKENHI Grant Number JP17K17711.

References

1. Janet Anders and Dan E. Browne. Computational power of correlations. *Phys. Rev. Lett.*, 102:050502, Feb 2009.
2. Jonathan Barrett. Information processing in generalized probabilistic theories. *Phys. Rev. A*, 75:032304, Mar 2007.
3. Jonathan Barrett, Niel de Beaudrap, Matty J. Hoban, and Ciarán M. Lee. The computational landscape of general physical theories. `https://arxiv.org/abs/1702.08483v1`, 2017.
4. Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001.
5. Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005.
6. Gilles Brassard, Harry Buhrman, Noah Linden, André A. Méthot, Alain Tapp, and Falk Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96:250401, Jun 2006.
7. Dan Browne, Elham Kashefi, and Simon Perdrix. Computational depth complexity of measurement-based quantum computation. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 35–46. Springer, 2010.
8. Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Informational derivation of quantum theory. *Phys. Rev. A*, 84:012311, Jul 2011.
9. Parikshit Gopalan, Ryan O'Donnell, Rocco A Servedio, Amir Shpilka, and Karl Wimmer. Testing Fourier dimensionality and sparsity. *SIAM Journal on Computing*, 40(4):1075–1100, 2011.
10. Frederic Green, Steven Homer, Cristopher Moore, and Christopher Pollett. Counting, fanout and the complexity of quantum ACC. *Quantum Info. Comput.*, 2(1):35–65, December 2002.
11. Matty J. Hoban, Earl T. Campbell, Klearchos Loukopoulos, and Dan E. Browne. Non-adaptive measurement-based quantum computation and multi-party Bell inequalities. *New Journal of Physics*, 13(2):023014, 2011.
12. Peter Høyer and Robert Špalek. Quantum fan-out is powerful. *Theory of Computing*, 1(5):81–103, 2005.
13. Sampath Kannan, Elchanan Mossel, Swagato Sanyal, and Grigory Yaroslavtsev. Linear sketching over $\mathbb{F}_2$. In *33rd Computational Complexity Conference (CCC 2018)*, volume 102 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:37, 2018.
14. Samuel Marcovitch and Benni Reznik. Implications of communication complexity in multipartite systems. *Phys. Rev. A*, 77:032120, Mar 2008.
15. Ashley Montanaro and Tobias Osborne. On the communication complexity of XOR functions. `https://arxiv.org/abs/0909.3392v2`, 2010.
16. Ryuhei Mori. Three-input majority function as the unique optimal function for the bias amplification using nonlocal boxes. *Phys. Rev. A*, 94:052130, Nov 2016.
17. Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
18. Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. Information causality as a physical principle. *Nature*, 461(7267):1101–1104, 2009.
19. Robert Raussendorf. Contextuality in measurement-based quantum computation. *Phys. Rev. A*, 88:022322, Aug 2013.
20. Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, Aug 2003.
21. Alexander A. Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\&, \oplus\}$. *Math. Notes Acad. Sci. USSR*, 41(4):333–338, 1987.

22. Oscar S. Rothaus. On "Bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.
23. Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82. ACM, 1987.
24. Yasuhiro Takahashi and Seiichiro Tani. Collapse of the hierarchy of constant-depth exact quantum circuits. *computational complexity*, 25(4):849–881, Dec 2016.
25. Reinhard F. Werner and Michael M. Wolf. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, Aug 2001.

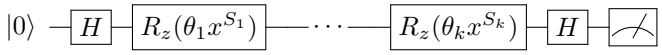
Appendix A Non-adaptive measurement-based quantum computation and circuit model

Here, we give a graphical proof that (4) can be achieved by generalized GHZ state and local measurements. Let H be the 2×2 Hadamard transform and $R_z(\theta) := |0\rangle\langle 0| + \mathrm{e}^{i\theta}|1\rangle\langle 1|$. It is easy to confirm the following lemma.

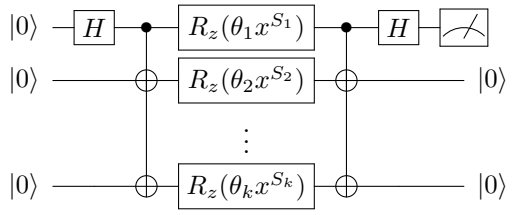
Lemma 13 ([12])**.**

$$\left|\langle 0| H R_z(\theta) H |0\rangle\right|^2 = \frac{1+\cos(\theta)}{2}.$$

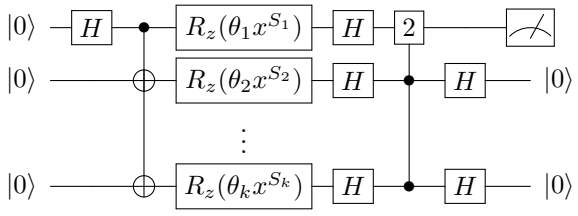
From this lemma, the bias in (4) is obtained by the following one-qubit circuit.



where $x^S := \prod_{i\in S} x_i$. By using fan-out gates [10], [12], we obtain the following equivalent circuit.



This circuit is useful when we consider computations by $\mathsf{QNC}^0_\mathsf{f}$ circuit [12], [24]. Since the fan-out gate is equivalent to the Mod2 gate conjugated by Hadamard gates, we obtain the following equivalent circuit.

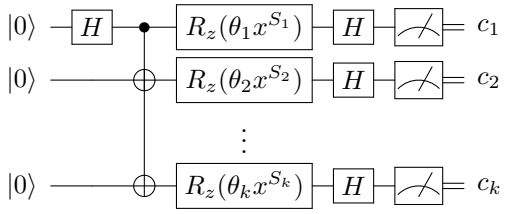


Here, we can measure all qubits before the Mod2 gate is applied and output XOR of mea-

Table 2. Computational power of measurement-based quantum computation with linear side-processing.

Side processor	State	Adaptivity	Complexity
Linear	Cluster state	Adaptive	BQP [20]
Linear	Tripartite GHZ state	Adaptive	P [1]
Linear	Generalized GHZ state	Non-adaptive	$\subseteq \mathsf{TC}^0$

surement outcomes.



The last circuit is equivalent to a setting of $\mathrm{NMQC}_{\oplus}$ using shared generalized GHZ state. The first Hadamard gate and fan-out gate generate the generalized GHZ state and following gates and measurements corresponding to non-adaptive measurements of qubits. Since the computation needs only one qubit on a circuit model, it can be simulated by TC^0 circuit as mentioned in [10]. Note that we can also directly prove this by simulating periodicity of cosine function by threshold circuits. Computational powers of several types of MBQC are summarized in Table 2.

Appendix B Fourier representation of Mod_n^3

Lemma 14. *For n divisible by 3, $\widehat{\mathsf{Mod}_n^3}(S)$ is in $\mathbb{R}_{n-2} \setminus \mathbb{R}_{n-3}$ for all $S \subseteq [n]$ of even size and is equal to zero for all S of odd size. For n not divisible by 3, $\widehat{\mathsf{Mod}_n^3}(S) \in \mathbb{R}_{n-1} \setminus \mathbb{R}_{n-2}$ for all non-empty $S \subseteq [n]$.*

Proof. Assume that n is divisible by 3. Then, $2\mathrm{Re}\left(\prod_{i=1}^n \left(\frac{-1+x_i\sqrt{-3}}{2}\right)\right)$ is 2 if $\sum_{i\in[n]} \mathsf{x}_i$ is divisible by 3, and -1 if not where $\mathrm{Re}(\omega)$ is the real part of a complex number ω. Hence,

$$\begin{aligned}
\mathsf{Mod}_n^3(x) &= \frac{1}{3}\left(-4\mathrm{Re}\left(\prod_{i=1}^n \left(\frac{-1+x_i\sqrt{-3}}{2}\right)\right)+1\right) \\
&= \frac{1}{3}\left(\frac{(-1)^{n+1}}{2^{n-2}}\mathrm{Re}\left(\sum_{S\subseteq[n]}\prod_{i\in S}(-x_i\sqrt{-3})\right)+1\right) \\
&= \frac{1}{3}\left(\frac{(-1)^{n+1}}{2^{n-2}}\sum_{\substack{S\subseteq[n]\\ |S| \text{ is even}}}\prod_{i\in S}(x_i\sqrt{-3})+1\right) \\
&= \frac{1}{3}+\frac{(-1)^{n+1}}{2^{n-2}3}\sum_{\substack{S\subseteq[n]\\ |S| \text{ is even}}}(-3)^{|S|/2}\prod_{i\in S}x_i.
\end{aligned}$$

0001	110101001110
0010	110101001111
0011	110101010000
⋮	⋮
1111	110101011100
10000	110101011101

Fig. 2. Let n be 110101011101 as the binary representation and $\ell = 5$. Left: Numbers from 1 to $2^{\ell-1}$. Right: Numbers from $n - 2^{\ell-1} + 1$ to n.

Hence, Fourier coefficients for S of odd size are zero and those for S of even size are in $\mathbb{R}_{n-2} \setminus \mathbb{R}_{n-3}$.

Assume that $n \equiv 1 \mod 3$. Then, $2\mathrm{Re}\left(\left(\frac{-1-\sqrt{-3}}{2}\right)\prod_{i=1}^{n}\left(\frac{-1+x_i\sqrt{-3}}{2}\right)\right)$ is 2 if $\sum_{i\in[n]} \mathsf{x}_i$ is divisible by 3, and -1 if not. Hence,

$$\begin{aligned}
\mathsf{Mod}_n^3(x) &= \frac{1}{3}\left(-4\mathrm{Re}\left(\left(\frac{-1-\sqrt{-3}}{2}\right)\prod_{i=1}^{n}\left(\frac{-1+x_i\sqrt{-3}}{2}\right)\right)+1\right)\\
&= \frac{1}{3}\left(\frac{(-1)^n}{2^{n-1}}\mathrm{Re}\left((1+\sqrt{-3})\sum_{S\subseteq[n]}\prod_{i\in S}(-x_i\sqrt{-3})\right)+1\right)\\
&= \frac{1}{3}\left(\frac{(-1)^n}{2^{n-1}}\left(\sum_{\substack{S\subseteq[n]\\ |S| \text{ is even}}}\prod_{i\in S}(x_i\sqrt{-3}) - \sqrt{-3}\sum_{\substack{S\subseteq[n]\\ |S| \text{ is odd}}}\prod_{i\in S}(x_i\sqrt{-3})\right)+1\right)\\
&= \frac{1}{3} + \frac{(-1)^n}{2^{n-1}3}\sum_{S\subseteq[n]}(-1)^{\lfloor |S|/2\rfloor}3^{\lfloor (|S|+1)/2\rfloor}\prod_{i\in S}x_i
\end{aligned}$$

Hence, all Fourier coefficients for non-empty S are in $\mathbb{R}_{n-1} \setminus \mathbb{R}_{n-2}$.

Assume that $n \equiv 2 \mod 3$. Then, $2\mathrm{Re}\left(\left(\frac{-1+\sqrt{-3}}{2}\right)\prod_{i=1}^{n}\left(\frac{-1+x_i\sqrt{-3}}{2}\right)\right)$ is 2 if $\sum_{i\in[n]} \mathsf{x}_i$ is divisible by 3, and -1 if not. The rest of the proof is same as that for the case $n \equiv 1 \mod 3$. □

Appendix C LSB function: The proof of Lemma 12

From

$$\begin{aligned}
\bigoplus_{1\le i_1<i_2<\cdots<i_{2^{\ell-1}}\le n} x_{i_1}\wedge x_{i_2}\wedge\cdots\wedge x_{i_{2^{\ell-1}}} &= \binom{n}{2^{\ell-1}} \mod 2\\
&= \frac{n(n-1)\cdots(n-2^{\ell-1}+1)}{2^{\ell-1}!} \mod 2
\end{aligned}$$

we will count the numbers of factor 2s in the denominator and the numerator. The number of factor 2s in arbitrary given integer k is equal to the number of trailing zeros in the binary representation of k. Hence, the number of factor 2s in $2^{\ell-1}!$ is equal to the sum of the number of trailing zeros of integers from 1 to $2^{\ell-1}$. We do not have to count it explicitly. Next, we count the number of factor 2s in the numerator. In integers from $n - 2^{\ell-1} + 1$ to n, all of

bit patterns of length $\ell - 1$ appear in the least significant $\ell - 1$ bits as shown in Fig. 2. An important case is the all-zero case. Let m be the unique integer at least $n - 2^{\ell-1} + 1$ and at most n which can be divided by $2^{\ell-1}$. For counting the number of trailing zeros of m, the ℓ-th bit of m is concerned. Here, the ℓ-th bit of m is equal to the ℓ-th bit of n. If the ℓ-th bit of n is 1, then, the number of trailing zeros of m is equal to $\ell - 1$. In this case the numbers of factor 2s in the numerator and the denominator are equal. If the ℓ-th bit of n is 0, then, the number of trailing zeros of m is greater than $\ell - 1$. In this case, the number of factor 2s in the numerator is greater than that in the denominator. This means that $\binom{n}{2^{\ell-1}} \mod 2$ is equal to $\mathrm{LSB}^{\ell}(\sum_i x_i)$. An example is shown in Fig. 2.