On the Fine-Grained Query Complexity of Symmetric Functions

Supartha Podder
Department of Computer Science, Stony Brook University, New York, NY, USA

Penghui Yao
State Key Laboratory for Novel Software Technology, Nanjing University, China
Hefei National Laboratory, China

Zekun Ye
State Key Laboratory for Novel Software Technology, Nanjing University, China

Abstract

Watrous conjectured that the randomized and quantum query complexities of symmetric functions are polynomially equivalent, which was resolved by Ambainis and Aaronson [1], and was later improved in [15, 12]. This paper explores a fine-grained version of the Watrous conjecture, including the randomized and quantum algorithms with success probabilities arbitrarily close to 1/2. Our contributions include the following:

1. An analysis of the optimal success probability of quantum and randomized query algorithms of two fundamental partial symmetric Boolean functions given a fixed number of queries. We prove that for any quantum algorithm computing these two functions using T queries, there exist randomized algorithms using $\mathsf{poly}(T)$ queries that achieve the same success probability as the quantum algorithm, even if the success probability is arbitrarily close to 1/2. These two classes of functions are instrumental in analyzing general symmetric functions.
2. We establish that for any total symmetric Boolean function f, if a quantum algorithm uses T queries to compute f with success probability $1/2+\beta$, then there exists a randomized algorithm using $O(T^2)$ queries to compute f with success probability $1/2+\Omega\left(\delta\beta^2\right)$ on a $1-\delta$ fraction of inputs, where β, δ can be arbitrarily small positive values. As a corollary, we prove a randomized version of Aaronson-Ambainis Conjecture [1] for total symmetric Boolean functions in the regime where the success probability of algorithms can be arbitrarily close to 1/2.
3. We present polynomial equivalences for several fundamental complexity measures of partial symmetric Boolean functions. Specifically, we first prove that for certain partial symmetric Boolean functions, quantum query complexity is at most quadratic in approximate degree for any error arbitrarily close to 1/2. Next, we show exact quantum query complexity is at most quadratic in degree. Additionally, we give the tight bounds of several complexity measures, indicating their polynomial equivalence. Conversely, we exhibit an exponential separation between randomized and exact quantum query complexity for certain partial symmetric Boolean functions.

2012 ACM Subject Classification Theory of computation → Models of computation

Keywords and phrases Query complexity, Symmetric functions, Quantum advantages

Digital Object Identifier 10.4230/LIPIcs.ISAAC.2023.55

Related Version *Full Version*: `https://arxiv.org/pdf/2309.11279.pdf` [36]

Funding *Supartha Podder*: supported by US National Science Foundation (award no 1954311).
Penghui Yao: supported by National Natural Science Foundation of China (Grant No. 62332009, 61972191) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302900).
Zekun Ye: supported by National Natural Science Foundation of China (Grant No. 62332009, 61972191) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302900).

1 Introduction

Exploring quantum advantages is a key problem in quantum computing. A lot of research work has revolved around analyzing and characterizing quantum advantages, such as [14, 22, 16, 29, 45]. Query complexity is a complexity model commonly used to describe quantum advantages. A comprehensive survey on the query complexity can be found in [24]. A series of works [2, 44, 8, 41] has shown that for partial functions, quantum query complexity could be exponentially smaller (or even less) than the randomized query complexity, while for total functions, they are always polynomially related [4]. Although the query complexity model has demonstrated the powerful ability of a quantum computer to solve certain "structured" problems more efficiently than a classical computer, such as Simon's problem [43] and integer factorization problem [42], there only exist at most quadratic quantum speedups for some "unstructured" problems, such as black-box search problems [23]. Thus, one natural question is to explore how much structure is needed for significant quantum speedups [1].

Watrous conjectured that the randomized query complexity and quantum query complexity of partial symmetric functions are polynomial equivalent [1]. Later, Aaronson and Ambainis [1] initiated the study of quantum speedup on the quantum query complexity of symmetric functions, showing that partial functions invariant under full symmetry do not exhibit super-polynomial quantum speedups, which resolves the Watrous conjecture. Their result was later improved by Chailloux [15], who achieved a tighter bound and removed a technical dependence of output symmetry. Recently [12] performed a systematic analysis of functions symmetric under other group actions and characterized when super-polynomial quantum speedups are achievable. However, all these results work in the bounded error regime and do not explicitly consider arbitrary small biases.

In this paper, we propose and investigate a fine-grained version of the Watrous conjecture concerning the quantum and randomized query complexities of symmetric functions with an arbitrary error. Before stating the conjecture, we need to introduce two notions which are essential to this paper. For any Boolean function f and $T > 0$, let the classical T-bias $\delta_C(f, T)$ be the optimal success probability of T-query randomized algorithms minus $1/2$ over all possible inputs. The quantum T-bias $\delta_Q(f, T)$ is defined for quantum algorithms analogously.

▶ **Conjecture 1** (Fine-grained Watrous conjecture). *There exists a constant $c \geq 2$ satisfying that for any partial symmetric function f and any $T > 0$, $\delta_C(f, c \cdot T) \geq \mathsf{poly}\left(\frac{\delta_Q(f,T)}{T}\right)$.*

The reason for $c \geq 2$ is that the n-bit parity function can be exactly computed with $n/2$ quantum queries, while any randomized algorithm with less n queries succeeds with probability $1/2$. It is also not hard to see the fine-grained Watrous conjecture implies that quantum and randomized query complexities of symmetric functions are polynomially related. Indeed, if $\delta_Q(f, T)$ is lower bounded by some constant, then $\delta_C(f, c \cdot T) \geq \Omega(\frac{1}{\mathsf{poly}(T)})$, which implies the randomized query complexity of f is $\mathsf{poly}(T)$ by error reduction.

1.1 Our Motivation and Contribution

To study the fine-grained Watrous conjecture, we start with the following two fundamental symmetric Boolean functions, which are also essential to analyze general symmetric functions:

$$f_n^k(x) = \begin{cases} 0, & \text{if } |x| \in \{0, n\}, \\ 1, & \text{if } |x| \in \{k, n-k\}, \end{cases}$$

where $1 \leq k \leq n/2$ and

$$f_n^{k,l}(x) = \begin{cases} 0, & \text{if } |x| = k, \\ 1, & \text{if } |x| = l, \end{cases}$$

where $k < l$. The famous Deutsch-Jozsa problem [18] and the decision version of the unstructured search problem [23] can be interpreted as special cases of these two functions. Fefferman and Kimmel considered the subset-sized checking problem [19, 21], where the n-bit input string is promised to have either $\sqrt{n}$ or $0.99\sqrt{n}$ many marked items, and the goal is to decide which case. Their result together with [21] proved that it can be served as an oracle separation between AM and QCMA. On a similar flavour, [5] introduced the approximate counting problem, where the n-bit input has either $\leq w$ or $\geq 2w$ many marked items. Our function $f_n^{k,l}(\cdot)$ can be seen as a symmetric variant of these two problems[1]. We study the tradeoff between the number of queries and the optimal success probabilities in quantum and randomized settings for both functions with errors close to $1/2$.

We further consider the relation between various complexity measures of partial symmetric Boolean functions. For total Boolean functions, it has been proved that several fundamental complexity measures are polynomial equivalent (See Table 1 in [4]). Moreover, the tight bounds on several fundamental complexity measures of total symmetric Boolean functions have also been obtained [24]. However, the result for partial symmetric Boolean functions has not been fully characterized.

Our contribution is as follows. For convenience, if f is a symmetric Boolean function, we denote $f(k) = f(x)$ for any $|x| = k$. Additionally, we say an n-bit Boolean function $f : D \to \{0,1\}$ is even if $f(x) = f(n-x)$ for any $x \in D$, where $D \subseteq \{0,1\}^n$.

1. For both randomized setting and quantum setting, we characterize the optimal success probability of algorithms given the number of queries for the function f_n^k (Theorem 3) and $f_n^{k,l}$ (Theorems 4 and 5). As a corollary, we show for any T-query quantum algorithm to compute f_n^k and $f_n^{k,l}$, there exist classical randomized algorithms using $\mathsf{poly}(T)$ queries to simulate the success probability of the quantum algorithm (Corollaries 6 and 7). Additionally, we characterize the exact quantum query complexity of f_n^k (Theorem 8).
2. We establish a relation between the number of queries and the bias of quantum and randomized algorithms to compute total symmetric Boolean functions, where the bias of the algorithms can be arbitrarily small (Theorem 9). As a corollary, we prove a weak version of Conjecture 2: the acceptance probability of a quantum query algorithm to compute a total symmetric Boolean function can be approximated by a randomized algorithm with only a polynomial increase in the number of queries, where the bias of quantum algorithms can be arbitrarily small (Corollary 10).
3. We investigate the relation between different complexity measures of partial symmetric Boolean functions. Specifically, Theorem 12 shows the relation between the quantum query complexity and the approximate degree of even partial symmetric Boolean functions for arbitrarily small bias[2]. Theorem 13 shows exact quantum query complexity and degree are quadratically related. Theorem 14 presents tight bounds of block sensitivity, fractional block sensitivity, quantum query complexity, and approximate degree, where quantum query complexity and approximate degree are in a bounded-error setting. Corollary 15 shows block sensitivity is an upper bound of quantum query complexity. Since it has

[1] Our problem can also be seen as a Gap-Threshold function. Threshold function is defined as $f_n^k(x) = 1$ iff $|x| \geq k$.

[2] Theorem 12 is also a new result for total symmetric Boolean functions.

been known that $Q(f) \geq \Omega(\sqrt{\mathsf{bs}(f)})$ for any (possibly partial) Boolean function f [11], quantum query complexity and block sensitivity of partial symmetric Boolean functions are polynomially related. On the converse, Theorem 16 shows an exponential gap between the exact quantum query complexity and randomized query complexity for some partial symmetric Boolean functions, which is different from total symmetric functions.

▶ **Conjecture 2** (Aaronson-Ambainis Conjecture [1]). *The acceptance probability of a T-query quantum algorithm to compute a Boolean function can be approximated by a deterministic algorithm using* $\mathrm{poly}(T, 1/\epsilon, 1/\delta)$ *queries within an additive error ϵ on a $1-\delta$ fraction of inputs.*

▶ **Theorem 3.** *For $T > 0$, the quantum T-bias and classical T-bias of f_n^k are*

$$\delta_Q\left(f_n^k, T\right) = \begin{cases} \Theta(\frac{k}{n} \cdot T^2), & \text{if } T \leq \sqrt{n/k}, \\ \Theta\left(1\right), & \text{if } T > \sqrt{n/k}, \end{cases}$$

$$\delta_C\left(f_n^k, T\right) = \begin{cases} 0, & \text{if } T = 1, \\ \Theta(\frac{k}{n} \cdot T), & \text{if } 2 \leq T \leq n/k, \\ \Theta(1), & \text{if } T > n/k. \end{cases}$$

▶ **Theorem 4.** *For $f_n^{k,l}$ and $T > 0$, the quantum T-bias is*

$$\delta_Q\left(f_n^{k,l}, T\right) = \begin{cases} \Theta\left(\min\left\{\frac{l-k}{\sqrt{(n-k)l}} \cdot T, \frac{l-k}{n} \cdot T^2\right\}\right), & \text{if } T = O\left(\frac{\sqrt{(n-k)l}}{l-k}\right), \\ \Theta(1), & \text{if } T = \Omega\left(\frac{\sqrt{(n-k)l}}{l-k}\right). \end{cases}$$

▶ **Theorem 5.** *If $T = O\left(\frac{(n-k)l}{(l-k)^2}\right)$, the classical T-bias of $f_n^{k,l}$ satisfies that*

$$\delta_C\left(f_n^{k,l}, T\right) = O\left(\min\left\{\frac{l-k}{\sqrt{(n-k)l}} \cdot \sqrt{T} + \frac{T}{n}, \frac{l-k}{n} \cdot T\right\}\right),$$

$$\delta_C\left(f_n^{k,l}, T\right) = \Omega\left(\max\left\{\frac{(l-k)^2}{(n-k)l} \cdot T, \frac{l-k}{n} \cdot \sqrt{T}\right\}\right).$$

If $T = \Omega\left(\frac{(n-k)l}{(l-k)^2}\right)$, then $\delta_C\left(f_n^{k,l}, T\right) = \Theta(1)$.

▶ **Corollary 6.** *For arbitrarily small bias $\beta > 0$, if there exists a quantum algorithm using T queries to compute f_n^k with success probability $1/2 + \beta$, then there also exists a classical randomized algorithm using $O(T^2)$ queries to compute f_n^k with the same success probability.*

▶ **Corollary 7.** *For arbitrarily small bias $\beta > 0$, if there exists a quantum algorithm using T queries to compute $f_n^{k,l}$ with success probability $1/2 + \beta$, then there also exist classical randomized algorithms using T^2 queries to compute $f_n^{k,l}$ with success probability $1/2 + \Omega\left(\beta^2\right)$ and using T^4 queries to compute $f_n^{k,l}$ with success probability $1/2 + \Omega\left(\beta\right)$. Thus*

$$\delta_C\left(f_n^{k,l}, T^2\right) \geq \Omega\left(\delta_Q(f_n^{k,l}, T)^2\right) \text{ and } \delta_C\left(f_n^{k,l}, T^4\right) \geq \Omega\left(\delta_Q(f_n^{k,l}, T)\right).$$

▶ **Theorem 8.** *The exact quantum query complexity of f_n^k satisfies $\lceil \frac{\pi}{2\theta} \rceil \leq Q_E(f_n^k) \leq \lceil \frac{\pi}{2\theta} \rceil + 2$, where $\theta = 2 \arcsin \sqrt{k/n}$, whereas the zero-error randomized query complexity of f_n^k is $n-k+1$.*

▶ **Theorem 9.** *For any total symmetric Boolean function f and arbitrarily small bias $\beta > 0$, if there exists a quantum algorithm using T queries to compute f with success probability $1/2 + \beta$, then for any $\delta \in (0,1)$, there exists a randomized algorithm using $O(T^2)$ queries to compute f with success probability $1/2 + \Omega\left(\delta\beta^2\right)$ on a $1-\delta$ fraction of inputs.*

▶ **Corollary 10.** *For any total symmetric Boolean function f and arbitrarily small bias $\beta > 0$, if there exists a T-query quantum algorithm to compute f with success probability $1/2 + \beta$, then for any $\epsilon \in (0, \beta), \delta \in (0,1)$, there exists a randomized algorithm using $O(T^2/(\epsilon^2\delta^2))$ queries to compute f with success probability $1/2 + (\beta - \epsilon)$ on a $1-\delta$ fraction of inputs.*

▶ Remark 11. Corollary 10 is a randomized version of Conjecture 2. Moreover, Corollary 10 considers total symmetric Boolean functions, while Conjecture 2 refers to any Boolean function.

▶ **Theorem 12.** *For any (possibly partial) symmetric Boolean function f satisfying $f(x) = f(n-x)$ and arbitrarily small $\beta > 0$, if $T = \widetilde{\mathsf{deg}}_{\frac{1}{2}-\beta}(f)$, there exists a quantum query algorithm using $\lceil T/2 \rceil$ queries to compute f with success probability $1/2 + \Omega\left(\beta/\sqrt{T}\right)$. Namely,*

$$\delta_Q\left(f, \widetilde{\mathsf{deg}}_{\frac{1}{2}-\beta}(f)\right) = \Omega\left(\frac{\beta}{\sqrt{\widetilde{\mathsf{deg}}_{\frac{1}{2}-\beta}(f)}}\right).$$

As a corollary, we have $Q_\epsilon(f) = O(\widetilde{\mathsf{deg}}_\epsilon(f)^2)$ for any error ϵ arbitrarily close to $1/2$.

▶ **Theorem 13.** *For any partial symmetric Boolean function f, we have $Q_E(f) = O(\mathsf{deg}(f)^2)$.*

▶ **Theorem 14.** *For any partial symmetric Boolean function f, we have*

$$\begin{aligned} \mathsf{bs}(f) = \Theta\left(\mathsf{fbs}(f)\right) &= \left(\max_{k<l:f(k)\neq f(l)} \frac{n}{l-k}\right), \\ Q(f) = \Theta\left(\widetilde{\mathsf{deg}}(f)\right) &= \left(\max_{k<l:f(k)\neq f(l)} \frac{\sqrt{(n-k)l}}{l-k}\right). \end{aligned}$$

▶ **Corollary 15.** *For any partial symmetric Boolean function f, we have $Q(f) = O\left(\mathsf{bs}(f)\right)$.*

▶ **Theorem 16.** *There exists a partial symmetric Boolean function f such that $Q_E(f) = \Omega(n)$ and $R(f) = O(1)$.*

1.2 Proof Techniques

In this section, we give a high-level technical overview of our main results (See full version [36] for the detailed proof).

1.2.1 Upper and Lower Bounds on Quantum T-bias

We use several methods to show the upper bound on the quantum T-bias of different symmetric Boolean functions:

1. For f_n^k, we show if the number of a quantum algorithm is no more than T queries, then the bias β of the algorithm is at most $O(T^2/\,\mathsf{bs}(f_n^k))$, where $\mathsf{bs}(f_n^k)$ is the block sensitivity of f_n^k. By solving a lower bound of $\mathsf{bs}(f_n^k)$, we obtain an upper bound on the quantum T-bias of f_n^k (Theorem 3).
2. For $f_n^{k,l}$, using Paturi's lower bound technique [35] for the approximate degree of symmetric Boolean functions, we give the following lower bound:

$$Q_\epsilon(f_n^{k,l}) \geq \frac{1}{2}\widetilde{\mathsf{deg}}_\epsilon\left(f_n^{k,l}\right) = \Omega\left(\max\left\{\frac{\beta\sqrt{(n-k)\,l}}{l-k}, \sqrt{\frac{\beta n}{l-k}}\right\}\right),$$

where $\beta = 1/2-\epsilon$. The quantum T-bias of $f_n^{k,l}$ is derived by this lower bound (Theorem 4).

To obtain the lower bound on the quantum T-bias, we also use diverse ideas to design T-query quantum algorithms:

1. For f_n^k and $f_n^{k,l}$, we use various variants of amplitude amplification algorithm and analyze the success probability of algorithms meticulously (Theorems 3 and 4).
2. For even symmetric Boolean functions, we design a novel quantum algorithm by taking advantage of the Chebyshev expansion and constructing controlled Grover's diffusion operations (Theorem 12).

1.2.2 Upper and Lower Bounds on Classical T-bias

For f_n^k and $f_n^{k,l}$, we show the upper bound on the classical T-bias by analyzing the total variation distance of distributions; for the lower bound, we give sampling algorithms to estimate Hamming weights of the input and analyze the success probability of the algorithms also by analyzing the distance between distributions (Theorems 3 and 5).

For the lower bound on the classical T-bias of total symmetric Boolean functions, we design an innovative randomized algorithm by utilizing the Kravchuk polynomial when the number of queries is T. The analysis of the algorithm also uses the orthogonality property of the Kravchuk polynomial (Theorem 9).

1.2.3 The Relation Between Complexity Measures

The key ideas to build the relation between complexity measures of partial symmetric Boolean functions are as follows:

1. In Theorem 13, we show the relation between the exact quantum query complexity and the degree by giving the lower bound of the degree and designing a matching exact quantum algorithm up to a polynomial level. Similar to the proof of Theorem 8, the exact quantum algorithm makes use of a subroutine to distinguish $|x| = k$ from $|x| = l$ exactly [25].
2. In Theorem 14, the analysis of block sensitivity and fractional block sensitivity relies on the symmetry property of the function. Furthermore, we show the quantum query complexity and the approximate degree of any partial symmetric Boolean function f are equivalent to a constant factor. While the lower bound is well known (Fact 1), we show $Q(f) \leq \widetilde{\mathsf{deg}}(f)$ by giving a quantum approximate counting algorithm using $O(\widetilde{\mathsf{deg}}(f))$ quantum queries.
3. The exponential gap in Theorem 16 is shown by giving a function easy to compute in a bounded-error case but has a large degree.

1.3 Related Work

The need for structure in quantum speedups has been studied extensively. Beals, Buhrman, Cleve, Mosca and de Wolf [9] showed that there exists at most polynomial quantum speedups for total Boolean functions in the query model. Thus, the exponential speedups may only occur at partial functions. Furthermore, Aaronson and Ambainis [1] showed that symmetric functions do not allow super-polynomial quantum speedups, even if the functions are partial. Chailloux [15] improved this result for a broader class of symmetric functions. Ben-David, Childs, Gilyén, Kretschmer, Podder and Wang [12] further showed that hypergraph symmetries in the adjacency matrix model allow at most polynomial separations between quantum and randomized query complexities. Ben-David [10] proved a classical and quantum polynomial equivalence for a class of functions satisfying a certain symmetric promise. Aaronson and Ben-David [3] showed that there exists at most polynomial quantum speedups to compute an n-bit partial Boolean function if the domain $D = \text{poly}(n)$. Nonetheless, all these results concern the algorithms with a constant probability of success. They do not cover the query complexity with a subconstant probability of success.

We also survey some results about the optimal success probability of quantum algorithms when the number of queries is fixed. For the unstructured search problem, Zalka [46] showed an optimal success probability of a quantum algorithm given the number of queries. For the collision finding problem, Zhandry [47] gave the upper bound on the success probability of quantum algorithms when the number of queries is fixed, which matched the algorithm proposed by Brassard, Høyer and Tapp [13]. Ambainis and Iraids [6] analyzed the optimal success probability of one-query quantum algorithms to compute EQUALITY_n and AND_n functions. Montanaro, Jozsa, and Mitchison [33] indicated the optimal success probability of small symmetric Boolean functions when given any number of queries by numerical results. There is not much study about the optimal success probability with a given number of queries for symmetric Boolean functions. Our work will fill the gap in this field.

For the complexity measures of a nonconstant n-bit total symmetric Boolean function f, it has been known that $R(f)$, $D(f)$, $\mathsf{deg}(f)$, $s(f)$, $bs(f)$ are $\Theta(n)$, and $Q(f) = \Theta\left(\widetilde{\mathsf{deg}}(f)\right) = \Theta\left(\sqrt{n(n-\Gamma(f))}\right)$, where $\Gamma(f) = \min\{|2k-n+1| : f(k) \neq f(k+1)\}$ [24]. Sherstov [40] gave an almost tight characterization of $\mathsf{deg}_\epsilon(f)$ for specific $\epsilon \in [1/2^n, 1/3]$. Afterward, de Wolf [17] obtained the optimal bound. Regarding the complexity measures of partial symmetric Boolean functions, Aaronson and Ambainis [1] showed for any partial symmetric Boolean function f, $R(f) = O\left(Q(f)^2\right)$ as mentioned before. Researchers also studied the exact quantum query complexity for many instances of partial symmetric Boolean functions. For example, Deutsch and Jozsa [18] studied the first partially symmetric Boolean function. Afterward, generalized Deutsch-Jozsa problems were studied in [33, 37, 38]. He, Sun, Yang and Yuan [25] established the asymptotically optimal bound for the exact quantum query complexity of distinguishing whether $|x| = k$ or l. Qiu and Zheng [37, 39] studied the exact quantum query complexity of symmetric Boolean functions with degree 1 or 2. Additionally, several works [7, 20, 31] explored the connections between block sensitivity, fractional block sensitivity and degree for bounded functions.

In a similar work, Montanaro, Nishimura and Raymond [34] studied the unbounded error query complexity of Boolean functions in a scenario where it is only required that the query algorithm succeeds with a probability strictly greater than 1/2. They proved quantum and classical query complexities are related by a constant factor for any (possibly partial) Boolean function. Similar results are also known in the communication complexity model [27, 26]. Compared to the result in [34], we aim to analyze the relation between

quantum/classical query complexity and bias more precisely. For instance, we show for any quantum algorithm computing f_n^k and $f_n^{k,l}$ using T queries, there exist randomized algorithms using $\mathrm{poly}(T)$ queries that have the same bias as the quantum algorithm. Such a conclusion is not implied by [34] since the unbounded error model only requires a strictly positive bias without quantitative analysis.

1.4 Organization

The remainder of the paper is organized as follows. In Section 2, we review some definitions and facts. In Section 3, we prove Theorem 9 pertaining to connections between quantum and randomized algorithms of symmetric Boolean functions in the small-bias regime. In Section 4, we prove Theorem 12 to show the relation between the quantum query complexity and the approximate degree for arbitrarily small bias. Finally, a conclusion is made in Section 5.

2 Preliminaries

For an n-bit Boolean function $f : D \to \{0,1\}$, if $D = \{0,1\}^n$, f is a total function; if $D \subset \{0,1\}^n$, f is a partial function. We say f is symmetric if $f(x)$ only depends on $|x|$, where $|x|$ is the number of 1's in x. Correspondingly, we say $g : \{-1,1\}^n \to \mathbb{R}$ is symmetric if $g(x)$ only depends on $|x|$, where $|x|$ is the number of -1's in x. Every $g : \{-1,1\}^n \to \mathbb{R}$ can be uniquely expressed as $g(x) = \sum_{S\subseteq[n]} \widehat{g}(S)x_S$, where $x_S = \prod_{j\in S} x_j$ and $\widehat{g}(S)$ is the Fourier coefficient of g for any $S \subseteq [n]$. Let $H(n,i,T)$ be the hypergeometric distribution sampling T times from $x \in \{0,1\}^n$ satisfying that $|x| = i$ without replacement. A binomial distribution with parameters n, p is written as $B(n,p)$.

2.1 Query Models and Complexity Measures

In the classical query model, for an input $x \in \{0,1\}^n$, we can obtain x_i for some i by making one query. The deterministic query complexity of f, denoted by $D(f)$, is the minimum number of queries required by a deterministic algorithm to compute f on the worst input. The randomized query complexity of f, denoted by $R_\epsilon(f)$, is the minimum number of queries required by a randomized algorithm to compute f with error ϵ on the worst input. If $\epsilon = 1/3$, we abbreviate $R_\epsilon(f)$ to $R(f)$. Moreover, $R_0(f)$ is called the zero-error randomized query complexity of f.

In the quantum query model, a query algorithm can be described as follows: it starts with a fixed state $|\psi_0\rangle$ and then performs the sequence of operations $U_0, O_x, U_1, \ldots, O_x, U_t$, where U_i's are unitary operators not depend on x and the query oracle O_x is defined as $O_x|i\rangle|b\rangle = |i\rangle|x_i \oplus b\rangle$ for any $i \in [n]$ and $b \in \{0,1\}$. This leads to the final state $|\psi_x\rangle = U_t O_x U_{t-1} \cdots U_1 O_x U_0 |\psi_0\rangle$. The output result is obtained by measuring $|\psi_x\rangle$. The exact query complexity of f, denoted by $Q_E(f)$, is the minimum number of queries required by a quantum algorithm to compute f exactly on the worst input. Such a quantum algorithm is called an exact quantum algorithm. The quantum query complexity of f, denoted by $Q_\epsilon(f)$, is the minimum number of queries required by a quantum algorithm to compute f with ϵ on the worst input. If $\epsilon = 1/3$, we abbreviate $Q_\epsilon(f)$ to $Q(f)$.

Then we overview some notations about complexity measures of Boolean functions. The degree of f, denoted as $\mathsf{deg}(f)$, is the minimum degree of all real multilinear polynomial representations of f. The approximate degree of f, denoted by $\widetilde{\mathsf{deg}}_\epsilon(f)$, is the minimum degree among all real multilinear polynomials that approximate f with error ϵ. If $\epsilon = 1/3$, we abbreviate $\widetilde{\mathsf{deg}}_\epsilon(f)$ as $\widetilde{\mathsf{deg}}(f)$. The block sensitivity of f on x, denoted as $\mathsf{bs}(f,x)$, is the

maximum number of disjoint sensitive blocks in x. The block sensitivity of f is defined as $\mathsf{bs}(f) = \max_x \mathsf{bs}(f,x)$. The value of $\mathsf{bs}(f,x)$ can be expressed as an integer linear program. The fractional relaxation of the integer program yields the fractional block sensitivity of f on x, denoted as $\mathsf{fbs}(f,x)$. The fractional block sensitivity of f is defined as $\mathsf{fbs}(f) = \max_x \mathsf{fbs}(f,x)$.

▶ **Fact 1** ([9]). *If f is a Boolean function, then $Q_E(f) \geq \mathsf{deg}(f)/2$ and $Q_\epsilon(f) \geq \widetilde{\mathsf{deg}}_\epsilon(f)/2$.*

2.2 Orthonormal Polynomials and Fourier Growth

▶ **Fact 2** (Corollary 2.3 in [30]). *For any $0 \leq j \leq T$, the Kravchuk polynomial is defined as*

$$K_j(t,T) = \sum_{i=0}^{j} \binom{t}{i}\binom{T-t}{j-i}(-1)^i.$$

Then for any $0 \leq l, m \leq T$, there exists the following orthogonality property:

$$\sum_{t=0}^{T} \binom{T}{t} K_l(t,T)K_m(t,T) = 2^T \binom{T}{l}\delta_{l,m},$$

where $\delta_{l,m} = 1$ if $l = m$, and $\delta_{l,m} = 0$ if $l \neq m$.

▶ **Fact 3** (Parseval's identity, Page 84 in [32]). *For a function $g : [-1,1] \to [-1,1]$, if $g(x) = \sum_{i=0}^{T} a_i T_i(x)$ for any $x \in [-1,1]$, where T_i is the Chebyshev polynomial such that $T_i(\cos\theta) = \cos(i\theta)$, then*

$$\int_{-1}^{1} \frac{1}{\sqrt{1-x^2}} \left(g(x)\right)^2 dx = \pi a_0^2 + \frac{\pi}{2}\sum_{i=1}^{T} a_i^2.$$

▶ **Fact 4** (Theorem 1 in [28]). *If symmetric function $f : \{-1,1\}^n \to [-1,1]$ has degree d, then*

$$\sum_{S\subseteq[n]:|S|=l} |\widehat{f}(S)| \leq \frac{d^l}{l!},$$

where $\widehat{f}(S)$ is the Fourier coefficients of f for any $S \subseteq [n]$.

3 The Relation Between Quantum and Randomized Algorithms of Symmetric Boolean Functions for Arbitrarily Small Bias

In this section, we give the proof of Theorem 9. First, we state Lemma 17, which is needed to prove the theorem. In Lemma 17, since g is a symmetric function, we let $\widehat{g}(l) = \widehat{g}(S)$ for any $|S| = l$ with a slight abuse of notation, where $\widehat{g}(S)$ is the Fourier coefficients of g for $S \subseteq [n]$. Moreover, $K_l(t,T)$ is the Kravchuk polynomial as Fact 2.

▶ **Lemma 17.** *Given a symmetric function $g : \{-1,1\}^n \to [-1,1]$ such that $\mathsf{deg}(g) = d$, for any $d \leq T \leq n$ and $x \in \{-1,1\}^n$, we have*

$$g(x) = \mathbb{E}_{t\sim H(n,|x|,T)} \sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l}\frac{K_l(t,T)}{\binom{T}{l}},$$

$$\mathbb{E}_{t\sim B(T,\frac{1}{2})} \left(\sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l}\frac{K_l(t,T)}{\binom{T}{l}}\right)^2 \leq 2.$$

Proof. Since $g : \{-1,1\}^n \to [-1,1]$ is a symmetric function and $\mathsf{deg}(g) = d$, for any $d \le T \le n$ and $x \in \{-1,1\}^n$, we have

$$\begin{aligned}
g(x) &= \sum_{S\subseteq[n]:|S|\le d} \widehat{g}(S)x_S \\
&= \sum_{l=0}^{d} \widehat{g}(l) \sum_{S\subseteq[n]:|S|=l} x_S \\
&= \sum_{l=0}^{d} \widehat{g}(l) \frac{1}{\binom{n-l}{T-l}} \sum_{U\subseteq[n]:|U|=T} \sum_{S\subseteq U:|S|=l} x_S \\
&= \sum_{l=0}^{d} \widehat{g}(l) \frac{\binom{n}{l}}{\binom{n}{T}\binom{T}{l}} \sum_{U\subseteq[n]:|U|=T} \sum_{S\subseteq U:|S|=l} x_S \\
&= \frac{1}{\binom{n}{T}} \sum_{U\subseteq[n]:|U|=T} \sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l} \frac{\sum_{S\subseteq U:|S|=l} x_S}{\binom{T}{l}} \\
&= \frac{1}{\binom{n}{T}} \sum_{t=0}^{T} \binom{|x|}{t}\binom{n-|x|}{T-t} \sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l} \frac{\sum_{i=0}^{l}\binom{t}{i}\binom{T-t}{l-i}(-1)^i}{\binom{T}{l}} \\
&= \mathbb{E}_{t\sim H(n,|x|,T)} \sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l} \frac{K_l(t,T)}{\binom{T}{l}}.
\end{aligned}$$

Let $c_l = \widehat{g}(l)\binom{n}{l}$. By Fact 4, we have $|c_l| \le \frac{d^l}{l!}$. Then we have

$$\begin{aligned}
\mathbb{E}_{t\sim B(T,\frac{1}{2})} \left(\sum_{l=0}^{d} \widehat{g}(l)\binom{n}{l}\frac{K_l(t,T)}{\binom{T}{l}}\right)^2 &= \frac{1}{2^T}\sum_{t=0}^{T}\binom{T}{t}\left(\sum_{l=0}^{d} c_l \frac{K_l(t,T)}{\binom{T}{l}}\right)^2 \\
&= \sum_{l=0}^{d} \frac{c_l^2}{\binom{T}{l}} \\
&\le \sum_{l=0}^{d} \frac{d^l}{l!}\cdot\frac{d^l}{l!}\cdot\frac{l!}{\prod_{i=0}^{l-1} T-i} \\
&\le \sum_{l=0}^{d} \frac{1}{l!}\cdot\frac{d^{2l}}{\prod_{i=0}^{l-1} T-i} \\
&\le \sum_{l=0}^{d}\prod_{i=0}^{l-1}\frac{d^2}{T-i} \\
&\le \sum_{l=0}^{d}\left(\frac{1}{2}\right)^l \\
&\le 2,
\end{aligned}$$

where the second equality comes from the orthogonality property of the Kravchuk polynomial (Fact 2). ◀

Proof of Theorem 9. For any total symmetric Boolean function f and $0 < \beta < 1/2, 0 < \delta < 1$, let $\epsilon = 1/2 - \beta$. Suppose there exists a quantum algorithm using T queries to compute f with success probability $1/2+\beta$. By Fact 1, we have $\widetilde{\mathsf{deg}}_\epsilon(f) \le 2T$. Let $d = \widetilde{\mathsf{deg}}_\epsilon(f)$. Next, it suffices to prove there exists a randomized algorithm using $O(d^2)$ queries to compute f with success probability $1/2 + \Omega\left(\delta\beta^2\right)$ on a $1-\delta$ fraction of inputs.

Since $d = \widetilde{\mathsf{deg}}_\epsilon(f)$, there exists a degree-$d$ symmetric function $f' : \{0,1\}^n \to [0,1]$ satisfying if $f(x) = 0$, then $f'(x) \leq 1/2 - \beta$; if $f(x) = 1$, then $f'(x) \geq 1/2 + \beta$. It means that $(1 - 2f(x))(1 - 2f'(x)) \geq 2\beta$. Let $h : \{0,1\}^n \to [-1,1]$ be defined as $h(x) = 1 - 2f'(x)$ and $g : \{-1,1\}^n \to [-1,1]$ defined as $g(1-2x) = h(x)$ for any $x \in \{0,1\}^n$. Then g is also a degree-d symmetric function. By Lemma 17, for any $d \leq T \leq n$ and $x \in \{-1,1\}^n$, we have

$$g(x) = \mathbb{E}_{t\sim H(n,|x|,T)} \sum_{l=0}^{d} \widehat{g}(l) \binom{n}{l} \frac{K_l(t,T)}{\binom{T}{l}}.$$

Let

$$A_t = \sum_{l=0}^{d} \widehat{g}(l) \binom{n}{l} \frac{K_l(t,T)}{\binom{T}{l}}. \tag{1}$$

Then for $x \in \{0,1\}^n$, we have $h(x) = \mathbb{E}_{t\sim H(n,|x|,T)} A_t$, where $|x|$ is the number of 1's in x. For any $0 \leq t \leq T$, let

$$A'_t = \begin{cases} \min\left\{A_t, \frac{16}{\delta\beta}\right\}, & \text{if } A_t \geq 0, \\ \max\left\{A_t, -\frac{16}{\delta\beta}\right\}, & \text{if } A_t < 0. \end{cases} \tag{2}$$

Suppose x follows the uniform distribution of $\{0,1\}^n$. We give Algorithm 1 to compute $f(x)$ using $T = 2d^2 + d$ queries. The error analysis of Algorithm 1 is as follows. Given

Algorithm 1 A T-query quantum algorithm to compute $f(x)$.

1. Query T distinct bits in x uniformly and denote the number of 1's by t.
2. Compute the value of A_t as Equation (1).
3. Output 0 with the probability $\frac{1}{2}(1 + \frac{\delta\beta}{16}A'_t)$ and output 1 with the probability $\frac{1}{2}(1 - \frac{\delta\beta}{16}A'_t)$, where A'_t is defined as Equation (2).

$x \in \{0,1\}^n$, let $h'(x) = \mathbb{E}_{t\sim H(n,|x|,T)} A'_t$. Then the probability that the algorithm outputs 0 is $\frac{1}{2}\left(1 + \frac{\delta\beta}{16}h'(x)\right)$ and the probability that the algorithm outputs 1 is $\frac{1}{2}\left(1 - \frac{\delta\beta}{16}h'(x)\right)$. By Lemma 17, we have $\mathbb{E}_{t\sim B(T,\frac{1}{2})} A_t^2 \leq 2$. Since

$$\left|\mathbb{E}_{t\sim B(T,\frac{1}{2})} A_t\right| = \left|\frac{1}{2^n} \sum_{x\in\{0,1\}^n} \mathbb{E}_{t\sim H(n,|x|,T)} A_t\right| = \left|\frac{1}{2^n} \sum_{x\in\{0,1\}^n} h(x)\right| \leq 1, \tag{3}$$

we have $\sigma^2(A_t) = \mathbb{E}A_t^2 - (\mathbb{E}A_t)^2 \leq 2$ when t follows the binomial distribution $B(T, \frac{1}{2})$. By Chebyshev's inequality, we have

$$P(|A_t - \mathbb{E}A_t| \geq 2\delta) \leq \frac{1}{\delta^2}. \tag{4}$$

By Equation (2), we have

$$A'_t = \begin{cases} A_t, & \text{if } |A_t| \leq \frac{16}{\delta\beta}. \\ -\frac{16}{\delta\beta}, & \text{if } A_t < -\frac{16}{\delta\beta}. \\ \frac{16}{\delta\beta}, & \text{if } A_t > \frac{16}{\delta\beta}. \end{cases}$$

Thus if $|A_t| \leq \frac{16}{\delta\beta}$, then $|A_t - A'_t| = 0$; if $|A_t| > \frac{16}{\delta\beta}$, then $|A_t - A'_t| = |A_t| - \frac{16}{\delta\beta}$. Then we have

$$\mathbb{E}_t|A_t - A'_t| = \mathbb{E}_{t:|A_t|\geq\frac{16}{\delta\beta}}\left(|A_t| - \frac{16}{\delta\beta}\right). \tag{5}$$

By Equation (3), we have $|\mathbb{E}A_t| \leq 1$. Since $0 < \delta < 1, 0 < \beta < 1/2$, if $|A_t| > \frac{16}{\delta\beta}$, then $|A_t - \mathbb{E}A_t| \geq |A_t| - 1 \geq \frac{15}{\delta\beta}$. Thus, we have

$$\begin{aligned}
\mathbb{E}_{t:|A_t|\geq\frac{16}{\delta\beta}}\left(|A_t| - \frac{16}{\delta\beta}\right) &\leq \mathbb{E}_{t:|A_t-\mathbb{E}A_t|\geq\frac{15}{\delta\beta}}\left(|A_t| - \frac{16}{\delta\beta}\right) \\
&= \sum_{a=0}^{\infty}\mathbb{E}_{t:\frac{15\cdot 2^a}{\delta\beta}\leq|A_t-\mathbb{E}A_t|\leq\frac{15\cdot 2^{a+1}}{\delta\beta}}\left(|A_t| - \frac{16}{\delta\beta}\right) \\
&\leq \sum_{a=0}^{\infty}\mathbb{E}_{t:|A_t-\mathbb{E}A_t|\geq\frac{15\cdot 2^a}{\delta\beta}}\left(\frac{15\cdot 2^{a+1}}{\delta\beta} + 1 - \frac{16}{\delta\beta}\right) \\
&\leq \sum_{a=0}^{\infty}\mathbb{E}_{t:|A_t-\mathbb{E}A_t|\geq\frac{15\cdot 2^a}{\delta\beta}}\frac{16\left(2^{a+1}-1\right)}{\delta\beta} \\
&\leq \sum_{a=0}^{\infty}\left(\frac{\delta\beta}{15\cdot 2^{a-1}}\right)^2\cdot\frac{16\left(2^{a+1}-1\right)}{\delta\beta} \\
&= \frac{64}{225}\delta\beta\cdot\sum_{a=0}^{\infty}\frac{2^{a+1}-1}{4^a} \\
&\leq \delta\beta,
\end{aligned} \tag{6}$$

where the fourth inequality comes from Equation (4). Combining Equations (5) and (6), we have

$$\mathbb{E}_{t\sim B(T,\frac{1}{2})}|A_t - A'_t| \leq \delta\beta. \tag{7}$$

For $x \in \{0,1\}^n$, we have $h(x) = \mathbb{E}_{t\sim H(n,|x|,T)}A_t$ and $h'(x) = \mathbb{E}_{t\sim H(n,|x|,T)}A'_t$. Then we have

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}|h(x) - h'(x)| = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}\mathbb{E}_{t\sim H(n,|x|,T)}|A_t - A'_t| = \mathbb{E}_{t\sim B(T,\frac{1}{2})}|A_t - A'_t| \leq \delta\beta.$$

by Equation 7. Thus, there are at least $1-\delta$ fractions of inputs x such that $|h(x)-h'(x)| \leq \beta$. For such x, since $h(x)(1-2f(x)) \geq 2\beta$, we have $h'(x)(1-2f(x)) \geq \beta$. Therefore, if $f(x) = 0$, then $h'(x) \geq \beta$; if $f(x) = 1$, then $h'(x) \leq -\beta$. Thus, for at least $1-\beta$ fractions of inputs, the bias of the algorithm is at least $\beta\cdot\delta\beta/16 = \delta\beta^2/16$. ◀

4 The Relation Between Quantum Query Complexity and Approximate Degree for Arbitrarily Small Bias

In this section, we give the proof of Theorem 12.

Proof of Theorem 12. Given a (possibly partial) n-bit symmetric Boolean function $f : D \to \{0,1\}$, where $D \subseteq \{0,1\}^n$ and $f(x) = f(n-x)$ for any $x \in D$. For $0 < \epsilon < 1/2$, let $T = \mathsf{deg}_\epsilon(f)$ and $\beta = 1/2 - \epsilon$. Same as the proof of Theorem 9, for any function f' that approximates f with error ϵ, we have $(1-2f(x))(1-2f'(x)) \geq 2\beta$.

Let $g : [-1,1] \to [-1,1]$ be defined as $g\left(1-2|x|/n\right) = 1-2f(x)$ for any $x \in D$. Since $f(x) = f(n-x)$, g is an even function. Assume function $h : [-1,1] \to [-1,1]$ is the optimal approximation polynomial of g with degree T. Then $g(x)h(x) \geq 2\beta$ and h is also an

even function. Thus, $h(x)$ can be expressed as $\sum_{i=0}^{\lceil T/2\rceil} a_i T_{2i}(x)$ for any $x \in [-1,1]$, where $T_{2i}(x)$ is the Chebyshev polynomial of degree $2i$ and $T_{2i}(\cos\eta) = \cos 2i\eta$ for any $\eta \in [0,\pi]$. Furthermore, we have $h(\cos\eta) = \sum_{i=0}^{\lceil T/2\rceil} a_i \cos 2i\eta$ for any $\eta \in [0,\pi]$. Let $\cos\eta_x = 1 - 2|x|/n$. Then $(1-2f(x))\, h(\cos\eta_x) \geq 2\beta$ and

$$\begin{aligned} h(\cos\eta_x) &= \sum_{i=0}^{\lceil T/2\rceil} a_i \cos 2i\eta_x \\ &= \sum_{i:a_i\geq 0} a_i \left(2\cos^2 i\eta_x - 1\right) + \sum_{i:a_i<0} a_i \left(1 - 2\sin^2 i\eta_x\right) \\ &= \left(\sum_{i:a_i\geq 0} 2a_i \cos^2 i\eta_x - \sum_{i:a_i<0} 2a_i \sin^2 i\eta_x\right) + \left(\sum_{i:a_i<0} a_i - \sum_{i:a_i\geq 0} a_i\right) \\ &= \Delta_x - M, \end{aligned} \tag{8}$$

where $\Delta_x = 2\left(\sum_{a_i\geq 0} a_i \cos^2 i\eta_x - \sum_{a_i<0} a_i \sin^2 i\eta_x\right)$ and $M = \sum_{i=0}^{\lceil T/2\rceil} |a_i|$. By Fact 3, $\sum_{i=0}^{\lceil T/2\rceil} a_i^2 \leq \frac{2}{\pi}\int_{-1}^{1} \frac{1}{\sqrt{1-x^2}} dx = 2$. Thus,

$$M \leq \sqrt{2\lceil T/2\rceil + 1} \leq \sqrt{2(T+1)}. \tag{9}$$

Let $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i\in[n]} |i\rangle |-\rangle$. Then $\langle\psi|O_x|\psi\rangle = 1 - 2|x|/n = \cos\eta_x$. As a result, there exists a state $|\psi^\perp\rangle$ such that $\langle\psi|\psi^\perp\rangle = 0$ and $O_x|\psi\rangle = \cos\eta_x |\psi\rangle + \sin\eta_x |\psi^\perp\rangle$. For the following reflection operation

$$S_0 = 2|\psi\rangle\langle\psi| - I, S_1 = 2O_x|\psi\rangle\langle\psi| O_x - I = O_x S_0 O_x, \tag{10}$$

we have

$$\begin{aligned} S_1 S_0 |\psi\rangle &= \cos 2\eta_x |\psi\rangle + \sin 2\eta_x |\psi^\perp\rangle, \\ S_1 S_0 |\psi^\perp\rangle &= -\sin 2\eta_x |\psi\rangle + \cos 2\eta_x |\psi^\perp\rangle. \end{aligned} \tag{11}$$

Let R_0 be the corresponding controlled operation of S_0, i.e., for any $|\phi\rangle$,

$$R_0|\phi\rangle|+\rangle = |\phi\rangle|+\rangle, R_0|\phi\rangle|-\rangle = (S_0|\phi\rangle)|-\rangle. \tag{12}$$

Let $|\pm_i\rangle = \underbrace{|-\rangle\cdots|-\rangle}_{i}\underbrace{|+\rangle\cdots|+\rangle}_{\lceil T/2\rceil - i}$. If $a_i \geq 0$, let

$$P_i^+ = (|\psi\rangle\langle\psi|)\otimes(|\pm_i\rangle\langle\pm_i|), P_i^- = (I - |\psi\rangle\langle\psi|)\otimes(|\pm_i\rangle\langle\pm_i|).$$

If $a_i < 0$, let

$$P_i^- = (|\psi\rangle\langle\psi|)\otimes(|\pm_i\rangle\langle\pm_i|), P_i^+ = (I - |\psi\rangle\langle\psi|)\otimes(|\pm_i\rangle\langle\pm_i|).$$

Let $P_0 = \sum_i P_i^+, P_1 = \sum_i P_i^-$. Then $P_0 + P_1 = I$. Let $\alpha_i = \sqrt{\frac{|a_i|}{M}}$. Then $\sum_i \alpha_i^2 = 1$. We give Algorithm 2 to compute $f(x)$ and analyze the success probability of the algorithm as follows. Since R_0 is the corresponding controlled reflection operation of S_0, the final state after performing Step 2 of Algorithm 2 is

$$\sum_{i=0}^{\lceil T/2\rceil} \alpha_i \left(\underbrace{(O_x S_0)\cdots(O_x S_0)}_{i \text{ times}}|\psi\rangle\right)|\pm_i\rangle.$$

Algorithm 2 A T-query quantum algorithm to compute $f(x)$.

1. Prepare the initial state $\sum_{i=0}^{\lceil T/2\rceil} \alpha_i |\psi\rangle |\pm_i\rangle$, which consists of the first qudit and $\lceil T/2\rceil$ ancillary qubits, where $\alpha_i, |\psi\rangle, |\pm_i\rangle$ are defined on Page 11.
2. For $i = 1$ to $\lceil T/2\rceil$, we perform unitary operation $(O_x \otimes I)R_0$ in the first qudit and the i-th ancillary qubit, where R_0 is given in Equation (12).
3. Perform the project measurement $\{P_0, P_1\}$ defined on Page 11 to the final state and output the measurement result.

If i is even, then

$$\begin{aligned}\left(\underbrace{(O_xS_0)\cdots(O_xS_0)}_{i \text{ times}}|\psi\rangle\right)|\pm_i\rangle &= \left(\underbrace{(O_xS_0O_xS_0)\cdots(O_xS_0O_xS_0)}_{i/2 \text{ times}}|\psi\rangle\right)|\pm_i\rangle \\ &= \left(\underbrace{(S_1S_0)\cdots(S_1S_0)}_{i/2 \text{ times}}|\psi\rangle\right)|\pm_i\rangle \\ &= \left(\cos i\eta_x |\psi\rangle + \sin i\eta_x |\psi^\perp\rangle\right)|\pm_i\rangle,\end{aligned}$$

where the second equality comes from $S_1 = O_xS_0O_x$ and the third equality comes from Equation (11). Similarly, if i is odd, by Equation (11) and $S_1 = O_xS_0O_x$, we have

$$\begin{aligned}\left(\underbrace{(O_xS_0)\cdots(O_xS_0)}_{i \text{ times}}|\psi\rangle\right)|\pm_i\rangle &= \left(\underbrace{(O_xS_0)\cdots(O_xS_0)}_{i-1 \text{ times}}\left(\cos\eta_x |\psi\rangle + \sin\eta_x |\psi^\perp\rangle\right)\right)|\pm_i\rangle \\ &= \left(\underbrace{(S_1S_0)\cdots(S_1S_0)}_{(i-1)/2}\left(\cos\eta_x |\psi\rangle + \sin\eta_x |\psi^\perp\rangle\right)\right)|\pm_i\rangle \\ &= \left(\cos i\eta_x |\psi\rangle + \sin i\eta_x |\psi^\perp\rangle\right)|\pm_i\rangle.\end{aligned}$$

Thus, after performing Step 2 of Algorithm 2, the final state is

$$\sum_{i=0}^{\lceil T/2\rceil} \alpha_i \left(\cos i\eta_x |\psi\rangle + \sin i\eta_x |\psi^\perp\rangle\right)|\pm_i\rangle.$$

By Equation (8), the probability that the measurement result is 0 is

$$\begin{aligned}p_x &= \sum_{i:a_i\geq 0} \alpha_i^2 \cos^2 i\eta_x + \sum_{i:a_i<0} \alpha_i^2 \sin^2 i\eta_x \\ &= \frac{1}{M}\left(\sum_{i:a_i\geq 0} a_i \cos^2 i\eta_x - \sum_{i:a_i<0} a_i \sin^2 i\eta_x\right) \\ &= \frac{\Delta_x}{2M} \\ &= \frac{1}{2} + \frac{h(\cos\eta_x)}{2M},\end{aligned}$$

and the probability that the algorithm outputs 1 is $1/2 - h(\cos\eta_x)/(2M)$. Since $(1 - 2f(x))h(\cos\eta_x) \geq 2\beta$, the probability that the algorithm outputs $f(x)$ is at least $1/2 + \beta/M$.

By Equation (9), the bias of the algorithm is at least $\beta/M \geq \beta/\sqrt{2T+2}$. Then we can amplify the success probability to $1/2+\beta$ by running $O(T)$ times Algorithm 2 repetitively (see full version [36] for the detailed proof). Thus, there exists a quantum algorithm using $O(T^2)$ queries to with success probability $1-\epsilon$, which implies $Q_\epsilon(f) = O\left(\widetilde{\mathsf{deg}}_\epsilon(f)^2\right)$. ◀

▶ Remark 18. We conjecture that $f(x) = f(n-x)$ is not a necessary condition. If an n-bit (possibly partial) symmetric Boolean function f satisfies that $f(x) \neq f(n-x)$ for some $x \in D$, we can define a new $2n$-bit Boolean function f^* such that

$$f^*(x) = \begin{cases} f(x), & \text{if } |x| \leq n, \\ f(2n-x), & \text{if } |x| > n. \end{cases}$$

Then f^* satisfies that $f^*(x) = f^*(2n-x)$. Although we can run Algorithm 2 to f^*, we do not know how to relate $\widetilde{\mathsf{deg}}_\epsilon(f^*)$ and $\widetilde{\mathsf{deg}}_\epsilon(f)$ for any ϵ arbitrarily close to $1/2$. Thus, the query complexity of the algorithm is not promised. We leave this case as an open problem.

5 Conclusion

This paper analyzes the quantum advantage of computing two fundamental partial symmetric Boolean functions by studying the optimal success probability of T-query quantum and randomized algorithms. Moreover, we analyze the relation between the number of queries and the bias of quantum and randomized algorithms to compute total symmetric Boolean functions when the bias of the algorithms can be arbitrarily small. Furthermore, we show the relation of several fundamental complexity measures of partial symmetric Boolean functions. We leave the fine-grained Watrous conjecture as an open problem for further study.

References

1. Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10:133–166, 2014. doi:10.4086/toc.2014.v010a006.
2. Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. *SIAM Journal on Computing*, 47(3):982–1038, 2018. doi:10.1137/15M1050902.
3. Scott Aaronson and Shalev Ben-David. Sculpting quantum speedups. In *Proceedings of the 31st Conference on Computational Complexity*, volume 50, pages 26:1–26:28, 2016. doi:10.4230/LIPIcs.CCC.2016.26.
4. Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. Degree vs. approximate degree and quantum implications of Huang's sensitivity theorem. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1330–1342. ACM, 2021. doi:10.1145/3406325.3451047.
5. Scott Aaronson, Robin Kothari, William Kretschmer, and Justin Thaler. Quantum lower bounds for approximate counting via Laurent polynomials. In *Proceedings of the 35th Computational Complexity Conference*, pages 7:1–7:47, 2020. doi:10.4230/LIPIcs.CCC.2020.7.
6. Andris Ambainis and Janis Iraids. Optimal one-shot quantum algorithm for EQUALITY and AND. *Baltic Journal of Modern Computing*, 4(4), 2016. doi:10.22364/bjmc.2016.4.4.09.
7. Arturs Backurs and Mohammad Bavarian. On the sum of L1 influences. In *Proceedings of the IEEE 29th Conference on Computational Complexity*, pages 132–143, 2014. doi:10.1109/CCC.2014.21.
8. Nikhil Bansal and Makrand Sinha. k-Forrelation optimally separates quantum and classical query complexity. In *Proccedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1303–1316, 2021. doi:10.1145/3406325.3451040.

9 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. doi:10.1145/502090.502097.

10 Shalev Ben-David. The structure of promises in quantum speedups. In *Proceedings of the 11th Conference on the Theory of Quantum Computation, Communication and Cryptography*, volume 61, pages 7:1–7:14, 2016. doi:10.4230/LIPIcs.TQC.2016.7.

11 Shalev Ben-David. Lecture 6: The polynomial method. https://cs.uwaterloo.ca/~s4bendav/CS867QIC890/CS867QIC890W21week4notes.pdf, 2021.

12 Shalev Ben-David, Andrew M. Childs, András Gilyén, William Kretschmer, Supartha Podder, and Daochen Wang. Symmetries, graph properties, and quantum speedups. In *Proceedings of the 61st IEEE Annual Symposium on Foundations of Computer Science*, pages 649–660, 2020. doi:10.1109/FOCS46700.2020.00066.

13 Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In *LATIN 1998: Theoretical Informatics, Third Latin American Symposium*, volume 1380, pages 163–169, 1998. doi:10.1007/BFb0054319.

14 Sergey Bravyi, David Gosset, Robert König, and Marco Tomamichel. Quantum advantage with noisy shallow circuits in 3D. In *Proccedings of the 60th IEEE Annual Symposium on Foundations of Computer Science*, pages 995–999, 2019. doi:10.1109/FOCS.2019.00064.

15 André Chailloux. A note on the quantum query complexity of permutation symmetric functions. In *Proceedings of the 10th Innovations in Theoretical Computer Science Conference*, volume 124, pages 19:1–19:7, 2019. doi:10.4230/LIPIcs.ITCS.2019.19.

16 Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. Exponential separations between learning with and without quantum memory. In *Proccedings of the 62nd IEEE Annual Symposium on Foundations of Computer Science*, pages 574–585, 2021. doi:10.1109/FOCS52979.2021.00063.

17 Ronald de Wolf. A note on quantum algorithms and the minimal degree of ϵ-error polynomials for symmetric functions. *Quantum Information and Computation*, 8(10):943–950, 2008. doi:10.26421/QIC8.10-4.

18 David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, 1992. doi:10.1098/rspa.1992.0167.

19 Bill Fefferman and Shelby Kimmel. Quantum vs. Classical Proofs and Subset Verification. In *Proceedings of the 43rd International Symposium on Mathematical Foundations of Computer Science*, volume 117, pages 22:1–22:23, 2018. doi:10.4230/LIPIcs.MFCS.2018.22.

20 Yuval Filmus, Hamed Hatami, Nathan Keller, and Noam Lifshitz. On the sum of L1 influences of bounded functions. *Israel Journal of Mathematics*, 214(1):167–192, 2016. doi:10.1007/s11856-016-1355-0.

21 Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th annual ACM symposium on Theory of computing*, pages 59–68, 1986. doi:10.1145/12130.12137.

22 Daniel Grier and Luke Schaeffer. Interactive shallow clifford circuits: quantum advantage against NC^1 and beyond. In *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 875–888, 2020. doi:10.1145/3357713.3384332.

23 L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th IEEE Annual Symposium on Theory of Computing*, pages 212–219, 1996.

24 Buhrman Harry and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002. doi:10.1016/S0304-3975(01)00144-X.

25 Xiaoyu He, Xiaoming Sun, Guang Yang, and Pei Yuan. Exact quantum query complexity of weight decision problems. *Science China Information Sciences*, 66:129503, 2023. Also see arXiv:1801.05717. doi:10.1007/s11432-021-3468-x.

26 Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Unbounded-error classical and quantum communication complexity. In *Proceedings of the 18th International Symposium on Algorithms and Computation, ISAAC 2007*, volume 4835, pages 100–111, 2007. doi:10.1007/978-3-540-77120-3_11.

27 Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Unbounded-error one-way classical and quantum communication complexity. In *Proceedings of the 34th International Colloquium on Automata, Languages and Programming, ICALP 2007*, volume 4596, pages 110–121, 2007. doi:10.1007/978-3-540-73420-8_12.

28 Siddharth Iyer, Anup Rao, Victor Reis, Thomas Rothvoss, and Amir Yehudayoff. Tight bounds on the Fourier growth of bounded functions on the hypercube. *arXiv preprint*, 2021. arXiv:2107.06309.

29 John Kallaugher. A quantum advantage for a natural streaming problem. In *Proccedings of the 62nd IEEE Annual Symposium on Foundations of Computer Science*, pages 897–908, 2021. doi:10.1109/FOCS52979.2021.00091.

30 Vladimir I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces. *IEEE Transactions on Information Theory*, 41(5):1303–1321, 1995. doi:10.1109/18.412678.

31 Shachar Lovett and Jiapeng Zhang. Fractional certificates for bounded functions. In *Proceedings of the 14th Innovations in Theoretical Computer Science Conference*, volume 251, pages 84:1–84:13, 2023. doi:10.4230/LIPIcs.ITCS.2023.84.

32 John C. Mason and David C. Handscomb. *Chebyshev polynomials*. CRC Press, 2002.

33 Ashley Montanaro, Richard Jozsa, and Graeme Mitchison. On exact quantum query complexity. *Algorithmica*, 71(4):775–796, 2015. doi:10.1007/s00453-013-9826-8.

34 Ashley Montanaro, Harumichi Nishimura, and Rudy Raymond. Unbounded-error quantum query complexity. In *Proceedings of the 19th International Symposium on Algorithms and Computation, ISAAC 2008*, volume 5369, pages 919–930, 2008. doi:10.1007/978-3-540-92182-0_80.

35 Ramamohan Paturi. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 468–474. ACM, 1992. doi:10.1145/129712.129758.

36 Supartha Podder, Penghui Yao, and Zekun Ye. On the fine-grained query complexity of symmetric functions. *arXiv preprint*, 2023. arXiv:2309.11279.

37 Daowen Qiu and Shenggen Zheng. Characterizations of symmetrically partial Boolean functions with exact quantum query complexity. *arXiv preprint*, 2016. arXiv:1603.06505.

38 Daowen Qiu and Shenggen Zheng. Generalized Deutsch-Jozsa problem and the optimal quantum algorithm. *Physical Review A*, 97(6):062331, 2018. doi:10.1103/PhysRevA.97.062331.

39 Daowen Qiu and Shenggen Zheng. Revisiting Deutsch-Jozsa algorithm. *Information and Computation*, 2020(275):104605, 2020. doi:10.1016/j.ic.2020.104605.

40 Alexander A. Sherstov. Approximate inclusion-exclusion for arbitrary symmetric functions. *Computational Complexity*, 18(2):219–247, 2009. doi:10.1007/s00037-009-0274-4.

41 Alexander A. Sherstov, Andrey A. Storozhenko, and Pei Wu. An optimal separation of randomized and quantum query complexity. In *Proccedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1289–1302, 2021. doi:10.1145/3406325.3451019.

42 Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi:10.1109/SFCS.1994.365700.

43 Daniel R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, 1994. doi:10.1109/SFCS.1994.365701.

44 Avishay Tal. Towards optimal separations between quantum and randomized query complexities. In *Proccedings of the 61st Annual Symposium on Foundations of Computer Science*, pages 228–239, 2020. doi:10.1109/FOCS46700.2020.00030.

45 Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In *Proceedings of the 63rd IEEE Annual Symposium on Foundations of Computer Science*, pages 69–74, 2022. doi:10.1109/FOCS54457.2022.00014.

46 Christof Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60(4):2746, 2000. doi:10.1103/PhysRevA.60.2746.

47 Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information and Computation*, 15(7&8):557–567, 2015. doi:10.26421/QIC15.7-8-2.