Quantum and Classical Communication Complexity of Permutation-Invariant Functions

Ziyi Guan ✉
EPFL, Lausanne, Switzerland

Yunqi Huang ✉
University of Technology Sydney, Australia

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

This paper gives a nearly tight characterization of the quantum communication complexity of the permutation-invariant Boolean functions. With such a characterization, we show that the quantum and randomized communication complexity of the permutation-invariant Boolean functions are quadratically equivalent (up to a logarithmic factor). Our results extend a recent line of research regarding query complexity [2, 16, 11] to communication complexity, showing symmetry prevents exponential quantum speedups.

Furthermore, we show the Log-rank Conjecture holds for any non-trivial total permutation-invariant Boolean function. Moreover, we establish a relationship between the quantum/classical communication complexity and the approximate rank of permutation-invariant Boolean functions. This implies the correctness of the Log-approximate-rank Conjecture for permutation-invariant Boolean functions in both randomized and quantum settings (up to a logarithmic factor).

2012 ACM Subject Classification Theory of computation → Models of computation

Keywords and phrases Communication complexity, Permutation-invariant functions, Log-rank Conjecture, Quantum advantages

Digital Object Identifier 10.4230/LIPIcs.STACS.2024.39

Related Version *Full Version*: `https://arxiv.org/pdf/2401.00454.pdf` [26]

Funding *Ziyi Guan*: partially supported by the Ethereum Foundation.
Penghui Yao: supported by National Natural Science Foundation of China (Grant No. 62332009, 12347104, 61972191) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302901).
Zekun Ye: supported by National Natural Science Foundation of China (Grant No. 62332009, 12347104, 61972191) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302901).

1 Introduction

Exploring quantum advantages is a key problem in the realm of quantum computing. Numerous work focuses on analyzing and characterizing quantum advantages, such as [6, 14, 24, 20, 29, 44]. It has been known that quantum computing demonstrates a potential exponential speedup to solve certain problems than classical computers, such as Simon's problem [40] and integer factoring problem [39]. However, for some problems, the quantum speedups can be at most polynomial, including the unstructured search problems [25] and collision finding problems [4]. In light of the aforementioned phenomenon, Aaronson [1] proposed such a problem: How much structure is needed for huge quantum speedups?

Regarding the above problem, there exist two major directions to explore the structure needed for quantum speedups in the query model, which is a complexity model commonly used to describe quantum advantages. On the one hand, Aaronson and Ambainis [2] conjectured the acceptance probability of a quantum query algorithm to compute a Boolean function can be approximated by a classical deterministic algorithm with only a polynomial increase in the number of queries, which is still one of most important conjecture in the field of Boolean analysis. On the other hand, Watrous conjectured that the quantum and randomized query complexities are also polynomially equivalent for any permutation-invariant function [2]. Along this direction, Aaronson and Ambainis [2] initiated the study on the quantum speedup of permutation-invariant functions with respect to query complexity. They demonstrated that a function invariant under full symmetry does not exhibit exponential quantum speedups, even if the function is partial, thereby resolving the Watrous conjecture. (Interested readers may refer to [2] for a more detailed introduction.) Furthermore, Chailloux [16] expanded upon their work by providing a tighter bound and removing a technical dependence of output symmetry. Recently, Ben-David, Childs, Gilyén, Kretschmer, Podder and Wang [11] further proved that hypergraph symmetries in the adjacency matrix model allow at most a polynomial separation between randomized and quantum query complexities. All the above results demonstrated that symmetries break exponential quantum speedups in the query model.

While the study of problem structure in the roles of quantum speedups has obtained considerable attention in the query model, it is a natural question to consider whether we can derive similar results in other computation models. The communication complexity model comes to attention as it is also extensively used to demonstrate quantum advantages. Furthermore, while the exponential gap between quantum and classical communication models has been shown in many works [35, 7, 21, 22, 33], there are also some problems in communication models that demonstrate at most polynomial quantum speedups, such as set disjointness problem [36] and (gap) Hamming distance problem [28, 38, 43, 18]. Therefore, it is a meaningful question to consider how much structure is needed for significant quantum speedups in the communication complexity model. More specifically, while symmetry breaks quantum exponential advantages in the query model, does there exist a similar conclusion in the communication complexity model? In this paper, we investigate a variant of the Watrous conjecture concerning the quantum and randomized communication complexities of permutation-invariant functions as follows. Briefly, a permutation-invariant Boolean function is a function that is invariant under permutations of its inputs (see Definition 8 for a formal definition).

▶ **Conjecture 1** (Communication complexity version of the Watrous Conjecture.). *For any permutation-invariant function* $f : [m]^n \times [m]^n \to \{-1, 1, *\}$, $R(f) \le Q^*(f)^{O(1)}$, *where* $R(f)$ *and* $Q^*(f)$ *are the randomized and quantum communication complexities of* f*, respectively.*

Furthermore, we study the Log-rank Conjecture proposed by Lovasz and Saks [31], a long-standing open problem in communication complexity. Despite its slow progress on total functions [12, 32, 30], the conjecture has been shown for several subclasses of total permutation-invariant Boolean functions [15] and XOR-symmetric functions [45]. Lee and Shraibman further proposed the Log-approximate-rank Conjecture, stating that the randomized communication and the logarithm of the approximate rank of the input matrix are polynomially equivalent. Surprisingly, this conjecture was later proven false [19], even for its quantum counterpart [5, 41].

In this paper, we investigate both conjectures for permutation-invariant functions.

▶ **Conjecture 2** (Log-rank Conjecture for permutation-invariant functions.). *For any total permutation-invariant function* $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$, $D(f) \le (\log \operatorname{rank}(f))^{O(1)}$, *where* $\operatorname{rank}(f)$ *is the rank of the input matrix of* f.

▶ **Conjecture 3** (Log-Approximate-Rank Conjecture for permutation-invariant functions.). *For any (total or partial) permutation-invariant function* $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$, $R(f) \le \left(\log \widetilde{\operatorname{rank}}(f)\right)^{O(1)}$, *where* $\widetilde{\operatorname{rank}}(f)$ *is the approximate rank of the input matrix of* f *(see Definition 11 for a formal definition).*

▶ **Conjecture 4** (Quantum Log-Approximate-Rank Conjecture for permutation-invariant functions.). *For any (total or partial) permutation-invariant function* $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$, $Q(f) \le \left(\log \widetilde{\operatorname{rank}}(f)\right)^{O(1)}$.

1.1 Our Contribution

To study the communication complexity version of the Watrous conjecture, we start with permutation-invariant Boolean functions, which are essential to analyze general permutation-invariant functions. We show that for any permutation-invariant Boolean function, its classical communication complexity has at most a quasi-quadratic blowup comparing to its quantum communication complexity (Theorem 5). Thus, we cannot hope for exponential quantum speedups of permutation-invariant Boolean functions. Additionally, Theorem 5 gives a nearly tight bound on the quantum communication complexity. Furthermore, we show that every non-trivial permutation-invariant Boolean function satisfies the Log-rank Conjecture in Theorem 6. To resolve the (quantum) Log-Approximate-Rank Conjecture, we investigate the relationship between the quantum/classical communication complexities and the approximate rank of any permutation-invariant Boolean function in Theorem 7.

Consider a Boolean function f. Let $D(f), R(f), Q(f)$ and $Q^*(f)$ be the deterministic communication complexity, randomized communication complexity, quantum communication complexity without prior entanglement, and quantum communication complexity of f, respectively. Let $\operatorname{rank}(f)$ and $\widetilde{\operatorname{rank}}(f)$ be the rank and approximate rank of f. We summarize our results below[1].

▶ **Theorem 5.** *For any permutation-invariant function* $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$ *in Definition 8, the followings hold:*

$$\Omega(m(f)) \le R(f) \le \widetilde{O}\left(m(f)^2\right) \le \widetilde{O}\left(Q^*(f)^2\right) \text{ and}$$
$$\Omega(m(f)) \le Q^*(f) \le Q(f) \le \widetilde{O}(m(f)),$$

where $m(f)$ *is a measure defined in Definition 12. Hence,* $R(f) \le \widetilde{O}(Q^*(f)^2)$ *for any permutation-invariant function* f.

The complexity measure $m(\cdot)$ is inspired by the work [23], where Gahzi et al. introduced a complexity measure to capture $R(f)$. It is worth noting that their complexity measure is equivalent up to a fourth power of $R(f)$, while our complexity measure $m(\cdot)$ is quadratically related to $R(f)$ and almost tightly characterizes the quantum communication complexity.

[1] In Theorems 5 and 7, $\widetilde{O}(M(f)) = O\left(M(f)\log^2 n \log\log n\right)$ for any complexity measure M.

▶ **Theorem 6.** *For any non-trivial total permutation-invariant function $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ in Definition 8, we have*

$$D(f) = O\left(\log^2 \operatorname{rank}(f)\right).$$

▶ **Theorem 7.** *For any permutation-invariant function $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$ in Definition 8, we have*

$$R(f) = \widetilde{O}\left(\log^2 \widetilde{\operatorname{rank}}(f)\right) \quad \text{and } Q(f) = \widetilde{O}\left(\log \widetilde{\operatorname{rank}}(f)\right).$$

1.2 Proof Techniques

In this section, we give a high-level technical overview of our main results.

1.2.1 Lower Bound

We outline our approaches to obtain the lower bound on the quantum communication complexity, rank and approximate rank of permutation-invariant functions below:

1. **Quantum communication complexity** and **approximate rank**: In Theorem 5, to prove $Q^*(f) = \Omega(m(f))$ for any permutation-invariant function f, we use the following two-step reduction (see Lemma 15 and Theorem 13): First, we reduce the lower bound of the quantum communication complexity of the Exact Set-Inclusion Problem (ESetInc, Definition 10) to Paturis's approximate degree of symmetric functions [34] by the pattern matrix method [37], a well-known method for lower bound analysis in quantum communication complexity. Second, we reduce the lower bound of any permutation-invariant function to the lower bound of ESetInc. In Theorem 7, we use a similar method to prove the lower bound of approximate rank: $\log \widetilde{\operatorname{rank}}(f) = \Omega(m(f))$.
2. **Rank**: In Theorem 6, we reduce the lower bound of the rank of total permutation-invariant functions to the lower bound of the rank of some representative function instances, such as the set disjointness problem and the equality problem (see Lemma 24).

1.2.2 Upper Bound

We use the following methods to show the upper bounds on the communication complexity of permutation-invariant functions in the randomized, quantum, and deterministic models.

1. **Randomized and quantum models**: In Theorem 5, to prove $R(f) \leq \widetilde{O}\left(m(f)^2\right)$ for any permutation-invariant function f, we first propose a randomized protocol to solve the Set-Inclusion problem (SetInc, Definition 10) using a well-suited sampling method according to the parameters of SetInc (see Lemma 20). Afterward, we use this protocol as a subroutine to solve any permutation-invariant function based on binary search (see Theorem 14). Furthermore, to prove $Q(f) \leq \widetilde{O}(m(f))$, we use the quantum amplitude amplification technique [13, 27] to speed up the above randomized protocol to solve SetInc (see Lemma 21).
2. **Deterministic model**: In Theorem 6, to give an upper bound of deterministic communication complexity of total permutation-invariant functions, we propose a deterministic protocol as follows (see Lemma 25): Alice and Bob first share their Hamming weight of inputs, and decide who sends the input to the other party according to the definition of function and the Hamming weight of inputs. The party that has all the information of inputs will output the answer. Combining Lemmas 24 (described in Section 1.2.1) and 25, Theorem 6 can be proved.

1.3 Related Work

The need for structure in quantum speedups has been studied in the query model extensively. Beals, Buhrman, Cleve, Mosca and de Wolf [8] demonstrated that there exists at most a polynomial quantum speedup for total Boolean functions in the query model. Moreover, Aaronson and Ambainis [2] established that even partial symmetric functions do not allow super-polynomial quantum speedups. Chailloux [16] further improved this result to a broader class of symmetric functions. Ben-David, Childs, Gilyén, Kretschmer, Podder and Wang [11] later analyzed the quantum advantage for functions that are symmetric under different group actions systematically. Ben-David [10] established a quantum and classical polynomial equivalence for a certain set of functions satisfying a specific symmetric promise. Aaronson and Ben-David [3] proved that if domain D satisfies $D = \mathrm{poly}(n)$, there are at most polynomial quantum speedups for computing an n-bit partial Boolean function.

In terms of communication complexity, there are a few results that imply the polynomial equivalence between quantum and classical communication complexity for several instances of permutation-invariant functions. Examples include AND-symmetric functions [36], Hamming distance problem [28, 17], XOR-symmetric functions [45]. While the above results characterized quantum advantage for a certain class of permutation-invariant Boolean functions, our work provides a systemic analysis of all permutation-invariant Boolean functions.

The study of the Log-rank Conjecture and the Log-Approximate-Rank Conjecture has a rich history. Here, we only survey the results about the Log-rank Conjecture and the Log-Approximate-Rank Conjecture about permutation-invariant Boolean functions. Buhuman and de Wolf [15] verified the correctness of the Log-rank Conjecture for AND-symmetric functions. Combining the results of Razborov [36], Sherstov [37] and Suruga [42], it is implied that the Log-Approximate-Rank Conjecture holds for AND-symmetric functions both in the randomized and quantum settings. Moreover, the result of Zhang and Shi [45] implies the Log-rank Conjecture and the (quantum) Log-Approximate-Rank Conjecture hold for XOR-symmetric functions.

In previous work, Ghazi, Kamath and Sudan [23] introduced a complexity measure, which is polynomially equivalent to the randomized communication complexity of permutation-invariant functions defined in Definition 8. This paper is inspired by their work.

1.4 Organization

The remaining part of the paper is organized as follows. In Section 2, we state some notations and definitions used in this paper. In Section 3, we study the quantum and classical communication complexities of permutation-invariant functions. In Section 4, we show the Log-rank Conjecture holds for non-trivial total permutation-invariant functions. In Section 5, we study the Log-approximate Conjecture of permutation-invariant functions both in quantum and classical setting. Finally, a conclusion is made in Section 6. The appendices contain a section on extended preliminaries and omitted proofs.

2 Preliminaries

We introduce the notations and definitions used in this paper.

A **multiset** is a set with possibly repeating elements. We use $\{[\cdot]\}$ to denote multiset and $\{\cdot\}$ to denote standard set. Let S be a multiset, $S \setminus \{a\}$ removes one occurrence of a from S if there is any.

2.1 Boolean Functions

A **partial function** is a function defined only on a subset of its domain $\mathcal{X}$. Formally, given a partial Boolean function $f\colon \mathcal{X} \to \{-1,1,*\}$, $f(x)$ is **undefined** for $x \in \mathcal{X}$ if $f(x) = *$. A **total function** is a function that is defined on the entire domain. We say $f\colon \mathcal{X} \to \{-1,1,*\}$ is a **subfunction** of $g\colon \mathcal{X} \to \{-1,1,*\}$ if $f(x) = g(x)$ or $f(x) = *$ for any $x \in \mathcal{X}$.

A **Boolean predicate** is a partial function that has domain $\mathcal{X} = \{0,1,...,n\}$ for any $n \in \mathbb{N}$.

An **incomplete Boolean matrix** is a matrix with entries in $\{-1,1,*\}$, where undefined entries are filled with $*$.

A **submatrix** is a matrix that is obtained by extracting certain rows and/or columns from a given matrix.

A **half-integer** is a number of the form $n + 1/2$, where $n \in \mathbb{Z}$.

We introduce some Boolean operators as follows. For every $n \in \mathbb{N}$ and $x, y \in \{0,1\}^n$:

- $\overline{x} \coloneqq \{\overline{x_0}, ..., \overline{x_{n-1}}\} = \{1 - x_0, ..., 1 - x_{n-1}\}$;
- $x \wedge y \coloneqq \{x_0 \wedge y_0, ..., x_{n-1} \wedge y_{n-1}\}$; and
- $x \oplus y \coloneqq \{x_0 \oplus y_0, ..., x_{n-1} \oplus y_{n-1}\}$.

2.2 Communication Complexity Model

In the two-party communication model, Alice is given input x, and Bob is given input y. Then they aim to compute $f(x,y)$ for some function $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$ by communication protocols. The **deterministic communication complexity** $D(f)$ is defined as the cost of the deterministic protocol with the smallest communication cost, which computes f correctly on any input. The **randomized communication complexity** $R_\epsilon(f)$ is defined as the cost of the randomized protocol with the smallest communication cost, which has access to public randomness and computes f correctly on any input with probability at least $1 - \epsilon$. Similarly, the **quantum communication complexity** $Q(f)$ is defined as the cost of the quantum protocol with the smallest cost, which is not allowed to share prior entanglement, has access to public randomness and computes f correctly on any input with probability at least $1 - \epsilon$. If the quantum protocol is allowed with prior entanglement initially, then the corresponding quantum communication complexity is denoted $Q^*(f)$. If a protocol succeeds with probability at least $1 - \epsilon$ on any input for some constant $\epsilon < 1/2$, we say the protocol is with **bounded error**. If $\epsilon = 1/3$, we abbreviate $R_\epsilon(f), Q_\epsilon(f), Q^*_\epsilon(f)$ as $R(f), Q(f), Q^*(f)$.

2.3 Permutation-Invariant Functions

In the two-party communication model, the function value of a permutation-invariant function is invariant if we perform the same permutation to the inputs of Alice and Bob. Specifically, the formal definition is as follows.

▶ **Definition 8** (Permutation-invariant functions [23]). *A (total or partial) function $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1,*\}$ is permutation-invariant if for all $x, y \in \{0,1\}^n$, and every bijection $\pi : \{0,...,n-1\} \to \{0,...,n-1\}$, $f(x^\pi, y^\pi) = f(x,y)$, where x^π satisfies that $x^\pi_{(i)} = x_{\pi(i)}$ for any $i \in \{0,...,n-1\}$.*

Note that any permutation-invariant function f in Definition 8 depends only on $|x|, |y|$ and $|x \wedge y|$. Here $|\cdot|$ is the Hamming weight for the binary string, i.e., the number of 1's in the string. Thus, for any $a, b \in [n]$, there exists a function $f_{a,b}\colon \{\max\{0, a+b-n\}, ..., \min\{a,b\}\} \to \{-1,1\}$ such that

$$f_{a,b}(|x \wedge y|) = f(x,y), \tag{1}$$

for any $x, y \in \{0,1\}^n$ satisfying $|x| = a, |y| = b$. If there exist $a, b \in [n]$ such that $f_{a,b}$ is not a constant function, we say f is **non-trivial**.

The following definition of jumps partitions the domain of $f_{a,b}$ into different intervals according to the transition of function values.

▶ **Definition 9** (Jump in $f_{a,b}$ [23]). *(c, g) is a jump in $f_{a,b}$ if*

1. $f_{a,b}(c-g) \neq f_{a,b}(c+g)$;
2. $f_{a,b}(c-g), f_{a,b}(c+g) \in \{-1, 1\}$;
3. $f_{a,b}(r)$ *is undefined for* $c - g < r < c + g$.

Moreover, we define $\mathscr{J}(f_{a,b})$ to be the set of all jumps in $f_{a,b}$:

$$\mathscr{J}(f_{a,b}) \coloneqq \left\{ (c,g) : \begin{array}{c} f_{a,b}(c-g), f_{a,b}(c+g) \in \{0,1\} \\ f_{a,b}(c-g) \neq f_{a,b}(c+g) \\ \forall i \in (c-g, c+g), f_{a,b}(i) = * \end{array} \right\}.$$

The following definition gives an important instance of permutation-invariant functions.

▶ **Definition 10** (Set-Inclusion Problem). *We define the Set-Inclusion Problem $\mathsf{SetInc}^n_{a,b,c,g}$ as the following partial function:*

$$\mathsf{SetInc}^n_{a,b,c,g}(x,y) \coloneqq \begin{cases} -1 & \text{if } |x| = a, |y| = b \text{ and } |x \wedge y| \leq c - g, \\ 1 & \text{if } |x| = a, |y| = b \text{ and } |x \wedge y| \geq c + g, \\ * & \text{otherwise.} \end{cases}$$

Additionally, we define the Exact Set-Inclusion Problem $\mathsf{ESetInc}^n_{a,b,c,g}$ as follows.

$$\mathsf{ESetInc}^n_{a,b,c,g}(x,y) \coloneqq \begin{cases} -1 & \text{if } |x| = a, |y| = b \text{ and } |x \wedge y| = c - g, \\ 1 & \text{if } |x| = a, |y| = b \text{ and } |x \wedge y| = c + g, \\ * & \text{otherwise.} \end{cases}$$

2.4 Rank and Approximate Rank

If F is a real matrix, let $\text{rank}(F)$ be the **rank** of F. Then we define the approximate rank for any incomplete matrix as follows.

▶ **Definition 11** (Approximate rank). *For an incomplete matrix $F \in \{-1, 1, *\}^{m \times n}$ and $0 \leq \epsilon < 1$, we say a real matrix A approximates F with error ϵ if:*

(1) $|A_{i,j} - F_{i,j}| \leq \epsilon$ *for any* $i \in [m], j \in [n]$ *such that* $F_{i,j} \neq *$;

(2) $|A_{i,j}| \leq 1$ *for all* $i \in [m], j \in [n]$.

Let $\mathcal{F}_\epsilon$ be the set of all the real matrices that approximate F with error ϵ. The approximate rank of F with error ϵ, denoted by $\widetilde{\text{rank}}_\epsilon(F)$, is the least rank among all real matrices in $\mathcal{F}_\epsilon$. If $\epsilon = 2/3$, we abbreviate $\widetilde{\text{rank}}_\epsilon(F)$ as $\widetilde{\text{rank}}(F)$.

Let f be a Boolean function, $\text{rank}(f) \coloneqq \text{rank}(M_f)$ and $\widetilde{\text{rank}}(f) \coloneqq \widetilde{\text{rank}}(M_f)$, where M_f is the input matrix of f.

3 Polynomial Equivalence on Communication Complexity of Permutation-Invariant Functions

To show the polynomial equivalence between quantum and classical communication complexity of permutation-invariant functions as stated in Theorem 5, we prove the following two theorems (proved in Sections 3.1 and 3.2, respectively) for the quantum and randomized communication complexities of permutation-invariant functions using the measure in Definition 12.

▶ **Definition 12** (Measure $m(f)$). *Fix $n \in \mathbb{Z}$. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,*\}$ be a permutation-invariant function. We define the measure $m(f)$ of f as follows:*

$$m(f) \coloneqq \max_{\substack{a,b\in[n]\\ (c,g)\in\mathscr{J}(f_{a,b})\\ n_1:=\min\{[a-c,c,b-c,n-a-b+c]\}\\ n_2:=\min(\{[a-c,c,b-c,n-a-b+c]\}\setminus\{n_1\})}} \frac{\sqrt{n_1 n_2}}{g} \ .$$

Note that this definition is motivated by Lemma 15.

The measure $m(\cdot)$ is inspired by the complexity measure introduced in [23], which was used to capture the randomized communication complexity of permutation-invariant functions.

▶ **Theorem 13** (Lower Bound). *Fix $n \in \mathbb{Z}$. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,*\}$ be a permutation-invariant function. We have*

$$Q^*(f) = \Omega(m(f)) \ .$$

▶ **Theorem 14** (Upper Bound). *Fix $n \in \mathbb{N}$. Given a permutation-invariant function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,*\}$ and the corresponding measure $m(f)$ defined in Definition 12, we have*

- $R(f) = O\left(m(f)^2 \log^2 n \log\log n\right)$, *and*
- $Q(f) = O\left(m(f) \log^2 n \log\log n\right)$.

3.1 Quantum Communication Complexity Lower Bound

In this section, our goal is to obtain a lower bound on the quantum communication complexity for permutation-invariant functions (Theorem 13). Towards this end, we show that every permutation-invariant function f can be reduced to $\mathsf{ESetInc}$ (defined in Definition 10) and exhibit a lower bound for $\mathsf{ESetInc}$ (Lemma 15). Additionally, Lemma 15 implies if $|x| = a, |y| = b$, then the cost to distinguish $|x \wedge y| = c - g$ from $|x \wedge y| = c + g$ is related to the smallest and the second smallest number in $[a-c, c, b-c, n-a-b+c]$.

▶ **Lemma 15.** *Fix $n, a, b \in \mathbb{Z}$. Consider c and g such that $c+g, c-g \in \mathbb{Z}$. Let $n_1 \coloneqq \min\{[a-c, c, b-c, n-a-b+c]\}$ and $n_2 \coloneqq \min\left(\{[a-c, c, b-c, n-a-b+c]\} \setminus \{n_1\}\right)$. We have*

$$Q^*\left(\mathsf{ESetInc}^n_{a,b,c,g}\right) = \Omega\left(\frac{\sqrt{n_1 n_2}}{g}\right).$$

Proof of Theorem 13. By the definitions of $f_{a,b}$ and jump of $f_{a,b}$, any quantum protocol computing f can also compute $\mathsf{ESetInc}^n_{a,b,c,g}$ for any a, b and any jump $(c,g) \in \mathscr{J}(f_{a,b})$. Therefore, given a jump (c,g) for $f_{a,b}$, the cost of computing $\mathsf{ESetInc}^n_{a,b,c,g}$ lower bounds the cost of computing f. By Lemma 15, we have $Q^*(f) \geq \frac{\sqrt{n_1 n_2}}{g}$ for any jump (c,g) in $f_{a,b}$, where n_1, n_2 are the smallest and the second smallest number in $\{[a-c, c, b-c, n-a-b+c]\}$. We conclude that $Q^*(f) = \Omega\left(m(f)\right)$ as desired. ◀

Now we remain to show Lemma 15. We note that the following two lemmas imply Lemma 15 directly, where Lemma 16 reduces the instance such that the parameter only relies on n_1, n_2, g and Lemma 17 gives the final lower bound.

▶ **Lemma 16.** *Fix $n, a, b \in \mathbb{Z}$. Consider c and g such that $c+g, c-g \in \mathbb{Z}$. Let $n_1 := \min\{[a-c, c, b-c, n-a-b+c]\}$ and $n_2 := \min\left(\{[a-c, c, b-c, n-a-b+c]\} \setminus \{n_1\}\right)$. We have*

$$Q^*\left(\mathsf{ESetInc}^{n}_{a,b,c,g}\right) \geq Q^*\left(\mathsf{ESetInc}^{n_1+3n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right).$$

▶ **Lemma 17.** *For $n_1, n_2 \in \mathbb{N}$ such that $n_1 \leq n_2$, we have*

$$Q^*\left(\mathsf{ESetInc}^{n_1+3n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right) = \Omega\left(\frac{\sqrt{n_1 n_2}}{g}\right).$$

We use the following two results on $\mathsf{ESetInc}$ to show Lemmas 16 and 17 (See full version [26] for the detailed proofs). Specifically, Lemma 18 is a variant of Lemma 4.1 in [18] and shows some reduction methods to the instances of the Exact Set-Inclusion Problem. Lemma 19 is a generalization of Theorem 5 in [9] proved by pattern matrix method and shows the lower bound of a special instance of the Exact Set-Inclusion Problem.

▶ **Lemma 18.** *Fix $n, a, b \in \mathbb{Z}$. Consider c and g such that $c+g, c-g \in \mathbb{Z}$. The following relations hold.*

1. $Q^*\left(\mathsf{ESetInc}^{n}_{a,b,c,g}\right) \leq Q^*\left(\mathsf{ESetInc}^{n+\ell}_{a+\ell_1+\ell_3,b+\ell_2+\ell_3,c+\ell_3,g}\right)$ *for integers $\ell_1, \ell_2, \ell_3 \geq 0$ such that $\ell_1+\ell_2+\ell_3 \leq \ell$;*
2. $Q^*\left(\mathsf{ESetInc}^{n}_{a,b,c,g}\right) = Q^*\left(\mathsf{ESetInc}^{n}_{a,n-b,a-c,g}\right) = Q^*\left(\mathsf{ESetInc}^{n}_{n-a,b,b-c,g}\right)$*;*
3. $Q^*\left(\mathsf{ESetInc}^{n}_{a,b,c,g}\right) \leq Q^*\left(\mathsf{ESetInc}^{kn}_{ka,kb,kc,kg}\right)$*, where $k \geq 1$ is an integer.*

▶ **Lemma 19.** *For every $k \in \mathbb{Z}$, if l is a half-integer and $l \leq k/2$, then $Q^*\left(\mathsf{ESetInc}^{4k}_{2k,k,l,1/2}\right) = \Omega\left(\sqrt{kl}\right)$.*

Proof of Lemma 16. Using the second item of Lemma 18, we assume $n_1 = c$ without loss of generality. Furthermore, we assume $n_2 = a-c$. Let $n_3 := b-c, n_4 := n-a-b+c$. Then $n_3, n_4 \geq n_2 \geq n_1$ and $n = n_1+n_2+n_3+n_4$. By Lemma 18, we have

$$\begin{aligned}
Q^*\left(\mathsf{ESetInc}^{n_1+3n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right) &= Q^*\left(\mathsf{ESetInc}^{n_1+n_2+n_2+n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right)\\
&\leq Q^*\left(\mathsf{ESetInc}^{n_1+n_2+n_3+n_4}_{n_1+n_2,n_1+n_3,n_1,g}\right)\\
&= Q^*\left(\mathsf{ESetInc}^{n}_{a,b,c,g}\right).
\end{aligned}$$

If $n_2 = b-c$ or $n-a-b+c$, the argument is similar. ◀

Proof of Lemma 17. Let $m_1 = \left\lfloor \frac{n_1}{2g} + \frac{1}{2} \right\rfloor - \frac{1}{2}$, i.e., m_1 is the largest half-integer no more than $\frac{n_1}{2g}$. Similarly, let $m_2 = \left\lfloor \frac{n_2}{2g} + \frac{1}{2} \right\rfloor - \frac{1}{2}$. By Lemma 18, we have

$$Q^*\left(\mathsf{ESetInc}^{n_1+3n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right) \geq Q^*\left(\mathsf{ESetInc}^{m_1+3m_2}_{m_1+m_2,m_1+m_2,m_1,1/2}\right).$$

Then we discuss the following three cases:

- *Case 1:* $m_1 = m_2 = 1/2$. We have

$$Q^*\left(\mathsf{ESetInc}^{m_1+3m_2}_{m_1+m_2,m_1+m_2,m_1,1/2}\right) = \Omega(1) = \Omega\left(\sqrt{m_1 m_2}\right).$$

- *Case 2:* $m_2 \geq 3/2$ *and* $m_1 = 1/2$. Let $m_2' \coloneqq \left\lfloor \frac{m_1+m_2}{2} \right\rfloor, l_1 \coloneqq m_1 + m_2 - 2m_2', l_2 \coloneqq m_1 + m_2 - m_2', l \coloneqq m_1 + 3m_2 - 4m_2'$. Then,

$$l - (l_1 + l_2) = m_2 - m_1 - m_2' \geq \frac{m_2 + m_1}{2} - m_2' \geq 0.$$

By Lemmas 18 and 19, we have

$$\begin{aligned} Q^*\left(\mathsf{ESetInc}^{m_1+3m_2}_{m_1+m_2,m_1+m_2,m_1,1/2}\right) &= Q^*\left(\mathsf{ESetInc}^{4m_2'+l}_{2m_2'+l_1,m_2'+l_2,m_1,1/2}\right) \\ &\geq Q^*\left(\mathsf{ESetInc}^{4m_2'}_{2m_2',m_2',m_1,1/2}\right) \\ &= \Omega\left(\sqrt{m_1 m_2'}\right) \\ &= \Omega\left(\sqrt{m_1 m_2}\right). \end{aligned}$$

- *Case 3:* $m_1 \geq 3/2$. Let $m \coloneqq \left\lfloor \frac{m_1}{6} + \frac{m_2}{2} \right\rfloor, k \coloneqq \left\lfloor \frac{m_1}{3} + \frac{1}{2} \right\rfloor - \frac{1}{2}, l_3 \coloneqq m_1 - k, l_1 \coloneqq (m_1 + m_2 - 2m) - l_3, l_2 \coloneqq (m_1 + m_2 - m) - l_3, l \coloneqq m_1 + 3m_2 - 4m$. Since k is the largest half-integer smaller than $\frac{m_1}{3}$, we have $k \leq \frac{1}{2} \cdot \left\lfloor \frac{2m_1}{3} \right\rfloor$. Since $m_1 \leq m_2$, we have

$$k \leq \frac{1}{2} \cdot \left\lfloor \frac{2m_1}{3} \right\rfloor \leq \frac{1}{2} \cdot \left\lfloor \frac{m_1}{6} + \frac{m_2}{2} \right\rfloor \leq \frac{m}{2} \ , \tag{2}$$

and

$$l - (l_1 + l_2 + l_3) = m_2 - k - m \geq m_2 - \frac{m_1}{3} - \left(\frac{m_1}{6} + \frac{m_2}{2}\right) \geq 0 \ . \tag{3}$$

Then we have

$$\begin{aligned} & Q^*\left(\mathsf{ESetInc}^{m_1+3m_2}_{m_1+m_2,m_1+m_2,m_1,1/2}\right) & \\ = \ & Q^*\left(\mathsf{ESetInc}^{4m+l}_{2m+l_1+l_3,m+l_2+l_3,k+l_3,1/2}\right) & \\ \geq \ & Q^*\left(\mathsf{ESetInc}^{4m}_{2m,m,k,1/2}\right) & \text{(by Lemma 18 and Equation (3))} \\ = \ & \Omega\left(\sqrt{mk}\right) & \text{(by Lemma 19 and Equation (2))} \\ = \ & \Omega\left(\sqrt{m_1 m_2}\right) \ . & \end{aligned}$$

We conclude that

$$Q^*\left(\mathsf{ESetInc}^{n_1+3n_2}_{n_1+n_2,n_1+n_2,n_1,g}\right) \geq Q^*\left(\mathsf{ESetInc}^{m_1+3m_2}_{m_1+m_2,m_1+m_2,m_1,1/2}\right) = \Omega\left(\frac{\sqrt{n_1 n_2}}{g}\right) \ . \quad \blacktriangleleft$$

3.2 Randomized and Quantum Communication Complexity Upper Bound

We show upper bounds on the randomized and quantum communication complexities for permutation invariant functions (Theorem 14). Similar to Section 3.1, we do so by giving upper bounds for a specific problem, SetInc (see Definition 10), and reducing permutation-invariant functions to SetInc.

The following two lemmas capture the randomized and quantum communication complexity for SetInc, respectively.

▶ **Lemma 20** (Classical Upper Bound). *Fix $n, a, b \in \mathbb{Z}$. Consider c, g such that $c + g, c - g \in \mathbb{Z}$. Let $n_1 := \min\{[a - c, c, b - c, n - a - b + c]\}$ and $n_2 := \min(\{[a - c, c, b - c, n - a - b + c]\} \setminus \{n_1\})$. For any input $x, y \in \{0,1\}^n$ of $\mathsf{SetInc}^n_{a,b,c,g}$, there exists a randomized communication protocol that computes $\mathsf{SetInc}^n_{a,b,c,g}(x, y)$ using $O\left(\frac{n_1 n_2}{g^2}\log n \log\log n\right)$ bits of communication with success probability at least $1 - 1/(6\log n)$.*

▶ **Lemma 21** (Quantum Upper Bound). *Fix $n, a, b \in \mathbb{Z}$. Consider c, g such that $c + g, c - g \in \mathbb{Z}$. Let $n_1 := \min\{[a - c, c, b - c, n - a - b + c]\}$ and $n_2 := \min(\{[a - c, c, b - c, n - a - b + c]\} \setminus \{n_1\})$. For any input $x, y \in \{0,1\}^n$ of $\mathsf{SetInc}^n_{a,b,c,g}$, there exists a quantum communication protocol without prior entanglement that computes $\mathsf{SetInc}^n_{a,b,c,g}(x, y)$ using $O\left(\frac{\sqrt{n_1 n_2}}{g}\log n \log\log n\right)$ qubits of communication with success probability at least $1 - 1/(6\log n)$.*

We note that Lemma 21 is a quantum speedup version of Lemma 20 by quantum amplitude amplification. The proof of Lemma 20 is given at the end of this section, and the proof of Lemma 21 can be seen in the full version [26].

Now we explain how to derive Theorem 14 from the lemmas above.

Proof of Theorem 14. We first present a randomized protocol to compute f based on binary search:

1. Alice and Bob exchange $a := |x|, b := |y|$.
2. Alice and Bob both derive $f_{a,b}$ such that $f_{a,b}(|x \wedge y|) = f(x, y)$.
3. Let $\mathscr{J}(f_{a,b}) = \{(c_i, g_i)\}_{i\in[k]}$ for some $k \le n$ be the set of jumps of $f_{a,b}$ as in Definition 9.
4. Alice and Bob use binary search to determine $i \in \{0, 1, ..., k\}$ such that $|x \wedge y| \in I_i$, where I_i is defined in Equation (4).

We first discuss the communication complexity of the above protocol. The first step takes $O(\log n)$ bits of communication. The fourth step costs $O\left(m(f)^2 \log^2 n \log\log n\right)$ bits of communication: For each $i \in [k]$, Alice and Bob can determine whether $|x \wedge y| \le c_i - g_i$ or $|x \wedge y| \ge c_i + g_i$ by $O(m(f)^2 \log n \log\log n)$ with a success probability of at least $1 - 1/(6\log n)$ by Lemma 20. Since binary search takes at most $\lceil\log(k+1)\rceil = O(\log n)$ rounds, the total communication cost is $O\left(m(f)^2 \log^2 n \log\log n\right)$.

Now we argue for the correctness of the protocol. Notice that the set of jumps $\mathscr{J}(f_{a,b})$ invokes $k + 1$ intervals:

$$\{I_0 := [0, c_1 - g_1], I_1 := [c_1 + g_1, c_2 - g_2], \ldots, I_{k-1} := [c_{k-1} + g_{k-1}, c_k - g_k], I_k := [c_k + g_k, n]\} \quad . \tag{4}$$

In particular, the followings hold:

- For every $j \in [0, k]$ and $z_1, z_2 \in I_j$ such that $f_{a,b}(z_1) \ne *$ and $f_{a,b}(z_2) \ne *$, we have $f_{a,b}(z_1) = f_{a,b}(z_2)$.
- If $z \notin I_j$ for any $j \in [0, k]$, then $f_{a,b}(z) = *$.

Therefore, Alice and Bob start from $i = \lfloor(k+1)/2\rfloor$ to determine whether $|x \wedge y| \le c_i - g_i$ or $|x \wedge y| \ge c_i + g_i$ with success probability of at least $1 - 1/(6\log n)$. Depending on the result, they repeat the same process similar to binary search to find the interval that $|x \wedge y|$ falls in. After at most $\lceil\log(k+1)\rceil = O(\log n)$ repetitions, there is only one remaining interval and they can easily determine $f_{a,b}(|x \wedge y|)$. For $n \ge 2$, the failure probability of the above protocol is at most

$$1 - \left(1 - \frac{1}{6\log n}\right)^{\lceil\log(k+1)\rceil} \le \frac{\lceil\log(k+1)\rceil}{6\log n} \le \frac{\lceil\log(n+1)\rceil}{3\log n^2} \le \frac{1}{3}.$$

For the quantum case, Alice and Bob use the same protocol above, but we invoke Lemma 21 to analyze the communication complexity. ◀

Proof of Lemma 20. We rely on the following two claims to prove the lemma.

▶ **Fact 22** ([2, Lemma 30])**.** *Fix $0 < \epsilon < \beta < 1$ such that $\beta + \epsilon \leq 1$. For a set S, suppose there is a subset S' of S such that $\frac{|S'|}{|S|} \leq \beta - \epsilon$ or $\frac{|S'|}{|S|} \geq \beta + \epsilon$. Suppose we can sample from S uniformly and ask whether the sample is in S'. Then we can decide whether $\frac{|S'|}{|S|} \leq \beta - \epsilon$ or $\frac{|S'|}{|S|} \geq \beta + \epsilon$ by $O(\beta/\epsilon^2)$ samples, with success probability at least $2/3$.*

▶ **Fact 23.** *Suppose $x, y \in \{0,1\}^n$ are the inputs of Alice and Bob such that $|x| \neq |y|$. Alice and Bob can sample an element from $S \coloneqq \{i : x_i \neq y_i\}$ uniformly using $O(\log n)$ bits of communication.*

We refer interesting readers to the full version [26] for the proof of Fact 23. Now we prove the lemma by casing on the values of n_1 and n_2.

- *Case 1: $n_1 = c$ and $n_2 = a - c$.* According to Definition 10, we have either $\frac{|x\wedge y|}{|x|} \leq \frac{c-g}{a}$ or $\frac{|x\wedge y|}{|x|} \geq \frac{c+g}{a}$. Alice and Bob estimate $\frac{|x\wedge y|}{|x|}$ as follows: Alice chooses an index i such that $x_i = 1$ uniformly at random. Then Alice sends i to Bob, and Bob checks whether $y_i = 1$. By Fact 22, setting $\beta \coloneqq \frac{c}{a}$, $\epsilon \coloneqq \frac{g}{a}$, Alice and Bob can decide whether $\frac{|x\wedge y|}{|x|} \leq \frac{c-g}{a}$ or $\frac{|x\wedge y|}{|x|} \geq \frac{c+g}{a}$ with bounded error using $O\left(\frac{ac}{g^2}\right) = O\left(\frac{n_1 n_2}{g^2}\right)$ samples. Since $|x| = a$, using $O\left(\frac{n_1 n_2}{g^2} \log\log n\right)$ samples, they can decide whether $|x \wedge y| \leq c - g$ or $|x \wedge y| \geq c + g$ with success probability at least $1 - 1/(6\log n)$ by error reduction. Thus, the communication complexity is $O\left(\frac{n_1 n_2}{g^2} \log n \log\log n\right)$.
- *Case 2: $n_1 = a - c$ and $n_2 = c$, or $n_1 = a - c$ and $n_2 = c$, or $n_1 = c$ and $n_2 = b - c$.* A similar argument as in Case 1 applies.
- *Case 3: $n_1 = c$ and $n_2 = n - a - b + c$.* Since $n_1 \leq n_2$, we have $a + b \leq n$. Then we consider the following two cases:
  1. *Case 3.1: $a + b < n$.* Let $m \coloneqq n_1 + n_2$, $p \coloneqq \frac{|x\wedge y|}{|\overline{x}\oplus y|}$. Since

$$\begin{aligned}|\overline{x} \oplus y| &= |x \wedge y| + |\overline{x} \wedge \overline{y}| \\ &= |x \wedge y| + (n - (a + b - |x \wedge y|)) \ , \\ &= n - (a + b) + 2|x \wedge y|\end{aligned}$$

we have

$$p = \frac{|x \wedge y|}{n - (a+b) + 2|x \wedge y|} = \frac{1}{\frac{n-(a+b)}{|x\wedge y|} + 2} \ .$$

Notice that p is an increasing function with respect to $|x\wedge y|$. As a result, if $|x\wedge y| \leq c-g$, then $p \leq \frac{c-g}{m-2g}$; if $|x \wedge y| \geq c + g$, then $p \geq \frac{c+g}{m+2g}$. Let

$$\beta \coloneqq \frac{1}{2}\left(\frac{c+g}{m+2g} + \frac{c-g}{m-2g}\right) = \frac{cm - 2g^2}{m^2 - 4g^2} \text{ and } \epsilon \coloneqq \frac{1}{2}\left(\frac{c+g}{m+2g} - \frac{c-g}{m-2g}\right) = \frac{gm}{m^2 - 4g^2} \ .$$

Since $c - g \geq 0$, we have $\beta \leq \frac{c+g}{m+2g} \leq \frac{2c}{m}$ and

$$\begin{aligned}\epsilon &= \frac{1}{2}\left(\frac{c+g}{m+2g} - \frac{c}{m}\right) + \frac{1}{2}\left(\frac{c}{m} - \frac{c-g}{m-2g}\right) \\ &= \frac{1}{2}\left(\frac{g(m-2c)}{m(m+2g)} + \frac{g(m-2c)}{m(m-2g)}\right) \\ &= O\left(\frac{g}{m}\right) \ .\end{aligned}$$

For any $x \in \{0,1\}^n$, we let $S_x \coloneqq \{i : x_i = 1\}$. By Fact 23, Alice and Bob can sample i from $S_{\overline{x} \oplus y}$ uniformly using $O(\log n)$ bits communication. Since $i \in S_{\overline{x} \oplus y}$, if $x_i = y_i = 1$, then $i \in S_{x \wedge y}$; if $x_i = y_i = 0$, then $i \notin S_{x \wedge y}$. By Fact 22, using $O\left(\frac{\beta}{\epsilon^2}\right) = O\left(\frac{mc}{g^2}\right) = O\left(\frac{n_1 n_2}{g^2}\right)$ samples, Alice and Bob can decide whether $p \le \beta - \epsilon$ or $p \ge \beta + \epsilon$ with bounded error. Equivalently, Alice and Bob can distinguish $|x \wedge y| \le c - g$ from $|x \wedge y| \ge c + g$ with bounded error. By error reduction, using $O\left(\frac{n_1 n_2}{g^2} \log \log n\right)$ samples, they can decide whether $|x \wedge y| \ge c - g$ or $|x \wedge y| \le c + g$ with success probability at least $1 - 1/(6 \log n)$. Thus, the communication complexity is $O\left(\frac{n_1 n_2}{g^2} \log n \log \log n\right)$.

2. *Case 3.2:* $a + b = n$. Alice and Bob generate new inputs $x' = x0$ and $y' = y0$ (pad a zero after the original input). We know

$$\mathsf{SetInc}^n_{a,b,c,g}(x, y) = \mathsf{SetInc}^{n+1}_{a,b,c,g}(x', y') \ .$$

Since $a + b < n + 1$, Alice and Bob perform the protocol in Case 3.1 in the new inputs, and the complexity analysis is similar to Case 3.1.

- *Case 4: $n_1 = n - a - b + c$ and $n_2 = c$, or $n_1 = a - c$ and $n_2 = b - c$, or $n_1 = b - c$ and $n_2 = a - c$.* A similar argument as in Case 3 works. ◀

4 Log-Rank Conjecture for Permutation-Invariant Functions

Theorem 6 states the Log-rank Conjecture for permutation-invariants functions. We argue for the lower bound (Lemma 24) and the upper bound (Lemma 25) separately.

▶ **Lemma 24.** *Fix $n \in \mathbb{N}$. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ be a non-trivial total permutation-invariant function. For every $a, b \in [n]$ such that $f_{a,b}$ is not a constant function, we have*

$$\log \operatorname{rank}(f) = \Omega\left(\max\left\{\log n, \min\left\{a, b, n-a, n-b\right\}\right\}\right),$$

where $f_{a,b}$ is defined as Equation (1).

▶ **Lemma 25.** *Fix $n \in \mathbb{N}$. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ be a non-trivial total permutation-invariant function.*

$$D(f) = O\left(\max_{a,b\in[n]:f_{a,b} \text{ is not constant}} \min\left\{a, b, n-a, n-b\right\} \cdot \log n\right) \ ,$$

where $f_{a,b}$ is defined as Equation (1).

We prove Lemma 24 below, and the proof of Lemma 25 can be found in the full version [26].

Proof of Lemma 24. We rely on the following two claims to prove the lemma. Two claims show the lower bound on the rank of some special functions respectively.

▶ **Fact 26** ([15], merging Corollary 6 with Lemma 4)**.** *Fix $n \in \mathbb{N}$. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ be defined as $f(x, y) \coloneqq D(|x \wedge y|)$ for some predicate $D : \{0, 1, ..., n\} \to \{-1, 1\}$. If t is the smallest integer such that $D(t) \ne D(t-1)$, then $\log \operatorname{rank}(f) = \Omega\left(\log\left(\sum_{i=t}^{n} \binom{n}{i}\right)\right)$.*

▶ **Fact 27.** *Fix $n \in \mathbb{N}$. Let $\mathcal{X}, \mathcal{Y} := \{x \in \{0,1\}^n : |x| = k\}$, where $k \le n/2$. Let $\mathsf{DISJ}_n^k : \mathcal{X} \times \mathcal{Y} \to \{-1, 1\}$ and $\mathsf{EQ}_n^k : \mathcal{X} \times \mathcal{Y} \to \{-1, 1\}$ be defined as*

$$\mathsf{DISJ}_n^k(x, y) := \begin{cases} -1 & \text{if } |x \wedge y| = 0 \\ 1 & \text{if } |x \wedge y| \neq 0 \end{cases} \text{ and } \mathsf{EQ}_n^k(x, y) := \begin{cases} -1 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases} .$$

Then $\operatorname{rank}\left(\mathsf{DISJ}_n^k\right) \ge \binom{n}{k} - 1$ *and* $\operatorname{rank}\left(\mathsf{EQ}_n^k\right) \ge \binom{n}{k} - 1$.

We refer interesting readers to the full version [26] for the proof of Fact 27. Now we prove the lemma by casing on the values of a and b.

We can assume $a \le b \le n/2$ without loss of generality because the cases where $a > n/2$ or $b > n/2$ can be obtained by flipping each bit of Alice or Bob's input. Thus, it suffices to prove $\log \operatorname{rank}(f) = \Omega(\max\{\log n, a\})$.

We prove the following two claims that directly lead to our result:

1. If $a \le b \le n/2$ and $a = o(\log n)$, then $\log \operatorname{rank}(f) = \Omega(\log n)$.
2. If $a \le b \le n/2$ and $a = \Omega(\log n)$, then $\log \operatorname{rank}(f) = \Omega(a)$.

We first prove Item 1. Suppose $a \le b \le n/2$ and $a = o(\log n)$. Since $f_{a,b}$ is not a constant function, there exists $c \in [0, a)$ such that $f_{a,b}(c) \neq f_{a,b}(c+1)$. Without loss of generality, we assume $f_{a,b}(c) = -1$. Let $n' := n - (a + b - c - 2)$. Since $b \le n/2$ and $c \le a = o(\log n)$, $n' = n - (a + b - c - 2) = \Omega(n)$. Let $\mathcal{X}$ and $\mathcal{Y}$ be the set $\left\{x \in \{0,1\}^{n'} : |x| = 1\right\}$. For any $x \in \mathcal{X}, y \in \mathcal{Y}$,

$$\mathsf{DISJ}_{n'}^1(x, y) = f_{a,b}(|x \wedge y| + c) = f(x', y') \ ,$$

where

$$x' := x \underbrace{1 \cdots 1}_{c} \underbrace{1 \cdots 1}_{a-c-1} \underbrace{0 \cdots 0}_{b-c-1} \text{ and } y' := y \underbrace{1 \cdots 1}_{c} \underbrace{0 \cdots 0}_{a-c-1} \underbrace{1 \cdots 1}_{b-c-1} \ .$$

Thus, $\mathsf{DISJ}_{n'}^1$ is a submatrix of f. By Fact 27, we have

$$\log \operatorname{rank}(f) \ge \log \operatorname{rank}(\mathsf{DISJ}_{n'}^1) \ge \log(n' - 1) = \Omega(\log n) .$$

Now we prove Item 2. Suppose $a, b \le n/2$ and $\min\{a, b\} = \Omega(\log n)$, we consider the following three cases:

- *Case 1: There exists $c \in [4a/7, 3a/5)$ such that $f_{a,b}(c) \neq f_{a,b}(c+1)$.* Let $k = \lfloor a/2 \rfloor$ and $k' = \lceil a/2 \rceil$. Let $g : \{0,1\}^k \times \{0,1\}^k \to \{-1, 1\}$ be such that $g(x, y) = f_{a,b}(|x' \wedge y'|)$ for every $x, y \in \{0,1\}^k$, where

  $$x' := x\overline{x} \underbrace{0 \cdots 0}_{k} \underbrace{1 \cdots 1}_{k'} \underbrace{0 \cdots 0}_{b-a} \underbrace{0 \cdots 0}_{n-b-2k} \text{ and } y' := y \underbrace{0 \cdots 0}_{k} \overline{y} \underbrace{1 \cdots 1}_{k'} \underbrace{1 \cdots 1}_{b-a} \underbrace{0 \cdots 0}_{n-b-2k} \ .$$

  Observe that $x', y' \in \{0,1\}^n$ and $|x'| = a, |y'| = b$. Moreover, $g(x, y) = D(|x \wedge y|)$ for predicate $D : \{0, 1, ..., k\} \to \{-1, 1\}$ such that $D(z) = f_{a,b}(z + k')$ for every $z \in [0, k]$. Thus, we have $D(c - k') \neq D(c - k' + 1)$. By Fact 26, we have

  $$\log \operatorname{rank}(g) = \Omega\left(\log\left(\sum_{i=c-k'+1}^{k} \binom{k}{i}\right)\right) \ .$$

  Since $c - k' + 1 < 3a/5 - \lceil a/2 \rceil + 1 \le a/10 \le k/2$, we conclude $\log \operatorname{rank}(g) = \Omega(k) = \Omega(a)$.

- *Case 2: There exists $c \in [0, 4a/7)$ such that $f_{a,b}(c) \neq f_{a,b}(c+1)$ and $f_{a,b}$ is a constant function in the range* $[c, 3a/5)$. Without loss of generality, we assume $f_{a,b}(c) = -1$. Let $l := \lfloor 3a/5 \rfloor$, $l' := \lceil 2a/5 \rceil$, $m := n - (c + b - a + 2l')$. Since $a \leq b \leq n/2$ and $c < 4a/7$, we have

  $$m = n - (c + b - a + 2l') \geq 2a - 2l' - c = 2l - c \geq 2(l - c) \ .$$

  Let $\mathcal{X}$ and $\mathcal{Y}$ be the set $\{x \in \{0,1\}^m : |x| = l - c\}$. For every $x \in \mathcal{X}, y \in \mathcal{Y}$, we have

  $$\mathsf{DISJ}_m^{l-c}(x, y) = f_{a,b}(|x' \wedge y'|) = f(x', y') \ ,$$

  where

  $$x' := x \underbrace{1 \cdots 1}_{c} \underbrace{0 \cdots 0}_{b-a} \underbrace{0 \cdots 0}_{l'} \underbrace{1 \cdots 1}_{l'} \text{ and } y' := y \underbrace{1 \cdots 1}_{c} \underbrace{1 \cdots 1}_{b-a} \underbrace{1 \cdots 1}_{l'} \underbrace{0 \cdots 0}_{l'}.$$

  Thus, DISJ_m^{l-c} is a submatrix of f. By Fact 27, we have

  $$\log \operatorname{rank}(f) \geq \log \operatorname{rank}(\mathsf{DISJ}_m^{l-c}) = \Omega\left(\log \binom{m}{l-c}\right) = \Omega(l - c) = \Omega(a) \ .$$

- *Case 3: There exists $c \in [3a/5, a)$ such that $f_{a,b}(c) \neq f_{a,b}(c+1)$ and $f_{a,b}$ is a constant function in the range* $[0, c)$. Without loss of generality, we assume $f_{a,b}(c) = -1$. Since $a \leq b \leq \frac{n}{2}$, we have $n - b + c \geq a + c \geq 2c$. Let $\mathcal{X}$ and $\mathcal{Y}$ be the set $\left\{x \in \{0,1\}^{n-b+c} : |x| = c\right\}$. For every $x \in \mathcal{X}, y \in \mathcal{Y}$, we have

  $$\mathsf{EQ}_{n-b+c}^{c}(x, y) = f_{a,b}(|x' \wedge y'|) = f(x', y'),$$

  where

  $$x' := x \underbrace{0 \cdots 0}_{b-a} \underbrace{0 \cdots 0}_{a-c} \text{ and } y' := y \underbrace{1 \cdots 1}_{b-a} \underbrace{0 \cdots 0}_{a-c} \ .$$

  Thus, EQ_{n-b+c}^{c} is a submatrix of f. By Fact 27, we have

  $$\log \operatorname{rank}(f) \geq \log \operatorname{rank}(\mathsf{EQ}_{n-b+c}^{c}) = \Omega\left(\log \binom{n-b+c}{c}\right) = \Omega(c) = \Omega(a) \ . \quad ◀$$

5 Log-Approximate-Rank Conjecture for Permutation-Invariant Functions

We discuss Theorem 7. In particular, we use the following two lemmas (proved in the full version [26]) to prove Theorem 7. Additionally, we note that Lemmas 28 and 29 are variants of Lemmas 18 and 19.

▶ **Lemma 28.** *Let $n, a, b, c, g \in \mathbb{Z}^+$. The following relations hold:*

1. $\widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{a,b,c,g}^{n}\right) \leq \widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{a+\ell_1+\ell_3, b+\ell_2+\ell_3, c+\ell_3, g}^{n+\ell}\right)$ *for $\ell_1, \ell_2, \ell_3 \geq 0$ such that $\ell_1 + \ell_2 + \ell_3 \leq \ell$;*
2. $\widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{a,b,c,g}^{n}\right) = \widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{a,n-b,a-c,g}^{n}\right) = \widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{n-a,b,b-c,g}^{n}\right)$*; and*
3. $\widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{a,b,c,g}^{n}\right) \leq \widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{ka,kb,kc,kg}^{kn}\right)$ *for $k \geq 1$.*

▶ **Lemma 29.** *Fix $k \in \mathbb{Z}$. Let l be a half-integer such that $l \leq k/2$. We have*

$$\log\left(\widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}_{2k,k,l,1/2}^{4k}\right)\right) = \Omega\left(\sqrt{kl}\right).$$

Proof sketch of Theorem 7. We use a similar argument as in the proof of Lemma 15. Namely, for every $a, b \in [n]$ and jump $(c, g) \in \mathscr{J}(f_{a,b})$, let $n_1 \coloneqq \min\{[a-c, c, b-c, n-a-b+c]\}$ and $n_2 \coloneqq \min(\{[a-c, c, b-c, n-a-b+c]\} \setminus \{n_1\})$. We have

$$\log \widetilde{\operatorname{rank}}\left(\mathsf{ESetInc}^n_{a,b,c,g}\right) = \Omega\left(\frac{\sqrt{n_1 n_2}}{g}\right) .$$

Since $\mathsf{ESetInc}^n_{a,b,c,g}$ is a subfunction of f, we have

$$\log \widetilde{\operatorname{rank}}(f) = \Omega\left(\max_{\substack{a,b\in[n]\\(c,g)\in\mathscr{J}(f_{a,b})}} \frac{\sqrt{n_1 n_2}}{g}\right) = \Omega(m(f)) .$$

Combining Theorem 14 and the above equation, we have Theorem 7 as desired. ◀

6 Conclusion

This paper proves that the randomized communication complexity of permutation-invariant Boolean functions is at most quadratic of the quantum communication complexity (up to a logarithmic factor). Our results suggest that symmetries prevent exponential quantum speedups in communication complexity, extending the analogous research on query complexity. Furthermore, we prove that the Log-rank Conjecture and Log-approximate-rank Conjecture hold for non-trivial permutation-invariant Boolean functions (up to a logarithmic factor). There are some interesting problems to explore in the future.

- *Permutation invariance over higher alphabets.* In this paper, the permutation-invariant function is a binary function. The interesting question is to generalize our results to larger alphabets, i.e., to permutation-invariant functions of the form $f : X^n \times Y^n \to R$ where X, Y and R are not necessarily binary sets.
- *Generalized permutation invariance.* It is possible to generalize our results for a larger class of symmetric functions. One candidate might be a class of functions that have graph-symmetric properties. Suppose $\mathcal{G}_A, \mathcal{G}_B$ are two sets of n-vertices graphs, and G_n is a group that acts on the edges of an n-vertices graph and permutes them in a way that corresponds to relabeling the vertices of the underlying graph. A function $f : \mathcal{G}_A \times \mathcal{G}_B \to \{0, 1\}$ is graph-symmetric if $f(x, y) = f(x \circ \pi, y \circ \pi)$, where $x \in \mathcal{G}_A, y \in \mathcal{G}_B$, and $\pi \in G_n$.

References

1 Scott Aaronson. How much structure is needed for huge quantum speedups? *arXiv preprint*, 2022. arXiv:2209.06930.

2 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`.

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 and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of ACM*, 51(4):595–605, 2004. `doi:10.1145/1008731.1008735`.

5 Anurag Anshu, Naresh Goud Boddu, and Dave Touchette. Quantum log-approximate-rank conjecture is also false. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 982–994, 2019. doi:10.1109/FOCS.2019.00063.

6 Anurag Anshu, Dave Touchette, Penghui Yao, and Nengkun Yu. Exponential separation of quantum communication and classical information. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 277–288. ACM, 2017. doi:10.1145/3055399.3055401.

7 Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 128–137. ACM, 2004. doi:10.1145/1007352.1007379.

8 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.

9 Aleksandrs Belovs, Arturo Castellanos, François Le Gall, Guillaume Malod, and Alexander A. Sherstov. Quantum communication complexity of distribution testing. *Quantum Information and Computation*, 21(15&16):1261–1273, 2021. doi:10.26421/QIC21.15-16-1.

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, 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.

12 Eli Ben-Sasson, Shachar Lovett, and Noga Ron-Zewi. An additive combinatorics approach relating rank to communication complexity. *J. ACM*, 61(4), 2014. doi:10.1145/2629598.

13 Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

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 Harry Buhrman and Ronald de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, pages 120–130, 2001. doi:10.1109/CCC.2001.933879.

16 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.

17 Amit Chakrabarti and Oded Regev. An optimal lower bound on the communication complexity of gap-hamming-distance. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, pages 51–60, 2011. doi:10.1145/1993636.1993644.

18 Amit Chakrabarti and Oded Regev. An optimal lower bound on the communication complexity of Gap-Hamming-Distance. *SIAM Journal on Computing*, 41(5):1299–1317, 2012. doi:10.1137/120861072.

19 Arkadev Chattopadhyay, Nikhil S. Mande, and Suhail Sherif. The log-approximate-rank conjecture is false. *J. ACM*, 67(4), June 2020. doi:10.1145/3396695.

20 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.

21 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 516–525. ACM, 2007. doi:10.1145/1250790.1250866.

22 Dmitry Gavinsky and Pavel Pudlák. Exponential separation of quantum and classical non-interactive multi-party communication complexity. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 332–339. IEEE Computer Society, 2008. doi:10.1109/CCC.2008.27.

23 Badih Ghazi, Pritish Kamath, and Madhu Sudan. Communication complexity of permutation-invariant functions. In *Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1902–1921, 2016. doi:10.1137/1.9781611974331.ch134.

24 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.

25 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. doi:10.1145/237814.237866.

26 Ziyi Guan, Yunqi Huang, Penghui Yao, and Zekun Ye. Quantum and classical communication complexity of permutation-invariant functions. *arXiv preprint*, 2024. arXiv:2401.00454.

27 Yassine Hamoudi and Frédéric Magniez. Quantum chebyshev's inequality and applications. In *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, volume 132, pages 69:1–69:16, 2019. doi:10.4230/LIPIcs.ICALP.2019.69.

28 Wei Huang, Yaoyun Shi, Shengyu Zhang, and Yufan Zhu. The communication complexity of the Hamming distance problem. *Information Processing Letter*, 99(4):149–153, 2006. doi:10.1016/j.ipl.2006.01.014.

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 Alexander Knop, Shachar Lovett, Sam McGuire, and Weiqiang Yuan. Log-rank and lifting for and-functions. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 197–208, 2021. doi:10.1145/3406325.3450999.

31 L. Lovasz and M. Saks. Lattices, mobius functions and communications complexity. In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, pages 81–90, 1988. doi:10.1109/SFCS.1988.21924.

32 Shachar Lovett. Communication is bounded by root of rank. *J. ACM*, 63(1), 2016. doi:10.1145/2724704.

33 Ashley Montanaro. A new exponential separation between quantum and classical one-way communication complexity. *Quantum Information and Computation*, 11(7&8):574–591, 2011. doi:10.26421/QIC11.7-8-3.

34 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.

35 Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, pages 358–367. ACM, 1999. doi:10.1145/301250.301343.

36 Alexander A Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145, 2003. doi:10.1070/IM2003v067n01ABEH000422.

37 Alexander A. Sherstov. The pattern matrix method. *SIAM Journal of Computing*, 40(6):1969–2000, 2011. doi:10.1137/080733644.

38 Alexander A. Sherstov. The communication complexity of gap Hamming distance. *Theory of Computing*, 8(1):197–208, 2012. doi:10.4086/toc.2012.v008a008.

39 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, November 1994. doi:10.1109/SFCS.1994.365700.

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

41 Makrand Sinha and Ronald de Wolf. Exponential separation between quantum communication and logarithm of approximate rank. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 966–981, 2019. `doi:10.1109/FOCS.2019.00062`.

42 Daiki Suruga. Matching upper bounds on symmetric predicates in quantum communication complexity. *arXiv preprint*, 2006. arXiv:2301.00370.

43 Thomas Vidick. A concentration inequality for the overlap of a vector on a large set, with application to the communication complexity of the Gap-Hamming-Distance problem. *Chicago Journal of Theoretical Computer Science*, 2012, 2012. URL: `http://cjtcs.cs.uchicago.edu/articles/2012/1/contents.html`.

44 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`.

45 Zhiqiang Zhang and Yaoyun Shi. Communication complexities of symmetric XOR functions. *Quantum Information and Computation*, 9(3&4):255–263, 2009. `doi:10.26421/QIC9.3-4-5`.