Quantum Information and Computation, Vol. 24, No. 11&12 (2024) 917–931

MATCHING UPPER BOUNDS ON SYMMETRIC PREDICATES IN QUANTUM COMMUNICATION COMPLEXITY

DAIKI SURUGA
Graduate School of Mathematics, Nagoya University
Furocho, Chikusaku, Nagoya, 464-8602, Japan

Received March 28, 2024
Revised September 28, 2024

In this paper, we focus on the quantum communication complexity of functions of the form $f \circ G = f(G(X_1, Y_1), \ldots, G(X_n, Y_n))$ where $f : \{0,1\}^n \to \{0,1\}$ is a symmetric function, $G : \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$ is any function and Alice (resp. Bob) is given $(X_i)_{i\in[n]}$ (resp. $(Y_i)_{i\in[n]}$). Recently, Chakraborty et al. [STACS 2022] showed that the quantum communication complexity of $f \circ G$ is $O(Q(f)\mathrm{QCC_E}(G))$ when the parties are allowed to use shared entanglement, where $Q(f)$ is the query complexity of f and $\mathrm{QCC_E}(G)$ is the exact communication complexity of G.

In this paper, we first show that the same statement holds *without both shared entanglement and shared randomness*, which generalizes their result. Based on the improved result, we next show tight upper bounds on $f \circ \mathrm{AND}_2$ for any symmetric function f (where $\mathrm{AND}_2 : \{0,1\} \times \{0,1\} \to \{0,1\}$ denotes the 2-bit AND function) in both models: with shared entanglement and without shared entanglement. This matches the well-known lower bound by Razborov [Izv. Math. 67(1) 145, 2003] when shared entanglement is allowed and improves Razborov's bound when shared entanglement is not allowed.

Keywords: two-party communication, quantum communication complexity, symmetric predicates

1 Introduction

1.1 Motivation

Communication complexity The model of (classical) communication complexity was originally introduced by Yao [1]. In this model, there are two players, Alice who receives $x \in \mathcal{X}$ and Bob who receives $y \in \mathcal{Y}$, and both players individually have computationally unbounded power. Their goal is to compute a known function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ with as little communication as possible. Due to this simple structure, lower and upper bounds on communication complexity problems have applications on many other fields such as VLSI design, circuit complexity, data structure, etc. (See [2, 3] for good references.) Communication complexity has been investigated in many prior works since its introduction.

In communication complexity, Set-Disjointness ($\mathsf{DISJ}_n(x,y) = \neg \bigvee_{i\in[n]}(x_i \wedge y_i)$), Equality ($\mathsf{EQ}_n(x,y) = \neg \bigwedge_{i\in[n]}(x_i \oplus y_i)$), and Inner-Product function ($\mathsf{IP}_n(x,y) = \bigoplus_{i\in[n]}(x_i \wedge y_i)$) are three of the most well-studied functions. Denoting the private-coin randomized communication complexity of a function f (with error $\leq 1/3$) as $\mathrm{CC}(f)$, it has been shown that $\mathrm{CC}(\mathsf{DISJ}_n) = \Theta(n)$, $\mathrm{CC}(\mathsf{IP}_n) = \Theta(n)$ and $\mathrm{CC}(\mathsf{EQ}_n) = \Theta(\log n)$ hold. Note that if shared randomness between the two parties is allowed, $\mathrm{CC}^{\mathsf{pub}}(\mathsf{DISJ}_n) = \Theta(n)$, $\mathrm{CC}^{\mathsf{pub}}(\mathsf{IP}_n) = \Theta(n)$

and $\mathrm{CC}^{\mathsf{pub}}(\mathsf{EQ}_n) = \Theta(1)$ hold[a] where $\mathrm{CC}^{\mathsf{pub}}(f)$ denotes the randomized communication complexity of a function f with error $\leq 1/3$ and with shared randomness. Observing from $\mathrm{CC}(\mathsf{EQ}_n) \neq \mathrm{CC}^{\mathsf{pub}}(\mathsf{EQ}_n)$, we see that shared randomness sometimes enables to reduce the communication complexity. Therefore, we need to carefully treat the effect of shared randomness when analyzing the communication complexity of functions. (Note that if $\mathrm{CC}^{\mathsf{pub}}(f)$ is strictly larger than $O(\log n)$, Newman's theorem [8] tells us that $\mathrm{CC}^{\mathsf{pub}}(f) = O(\mathrm{CC}(f))$ holds.)

In 1993, Yao [9] introduced the model of *quantum* communication complexity based on the model of classical communication complexity. The main difference between the classical and quantum model is that Alice and Bob use quantum bits to transmit their information in the quantum model. As quantum information science has been growing up rapidly, quantum communication complexity has been widely studied [10, 11, 12, 13]. In the case of quantum communication complexity, the three functions mentioned above satisfy $\mathrm{QCC}(\mathsf{DISJ}_n) = \Theta(\sqrt{n})$ [14, 15], $\mathrm{QCC}(\mathsf{IP}_n) = \Theta(n)$ [16] and $\mathrm{QCC}(\mathsf{EQ}_n) = \Theta(\log n)$ [17] , where $\mathrm{QCC}(f)$ denotes the private-coin quantum communication complexity of a function f. Note that in private-coin quantum communication complexity, Alice and Bob use neither shared entanglement nor shared randomness. If Alice and Bob have shared entanglement, $\mathrm{QCC}^*(\mathsf{DISJ}_n) = \Theta(\sqrt{n})$ [14, 15], $\mathrm{QCC}^*(\mathsf{IP}_n) = \Theta(n)$ [16] and $\mathrm{QCC}^*(\mathsf{EQ}_n) = \Theta(1)$ [7] hold where $\mathrm{QCC}^*(f)$ denotes the quantum communication complexity of the function f when shared entanglement is allowed. Even though the power of entanglement is not significant in these examples, careful treatment of shared entanglement is important since many non-trivial properties of entanglement have been witnessed (e.g., [18, 19, 20, 21, 13]), including Ref. [21] that shows Newman's theorem [8] does not hold in case of shared entanglement.

Composed functions In both classical and quantum communication complexity, many important functions have the form

$$f \circ G : (X, Y) \mapsto f((G(X_1, Y_1)), \ldots, G(X_n, Y_n)) \in \{0, 1\}$$

where $X = (X_i)_{i\in[n]} \in \{0,1\}^{nj}$, $Y = (Y_i)_{i\in[n]} \in \{0,1\}^{nk}$, $f : \{0,1\}^n \to \{0,1\}$ and $G : \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$. This fact is already observed in the three of the most well-studied functions: Set-Disjointness ($\neg\mathsf{OR}_n \circ \mathsf{AND}_2$), Equality ($\mathsf{AND}_n \circ \mathsf{XOR}_2$), and Inner-Product function ($\mathsf{XOR}_n \circ \mathsf{AND}_2$). As a natural consequence of its importance, functions of this form have been investigated deeply [22, 23, 24] in both classical and quantum communication complexity. Even though the functions $f \circ G$ are in general difficult to analyze in detail because of their generality, the analysis may become simpler when G has a simpler form. Let us explain in detail about upper and lower bounds on the quantum communication complexity when G is a simple function such as AND_2, XOR_2. In the case of upper bounds, Buhrman et al. [25] showed $\mathrm{QCC}(f \circ G) = O(\mathrm{Q}(f)\log n)$ holds when $G \in \{\mathsf{AND}_2, \mathsf{XOR}_2\}$, where $\mathrm{Q}(f)$ denotes the bounded error query complexity of a function f. Applying this result, we immediately get $\mathrm{QCC}(\mathsf{DISJ}_n) = O(\sqrt{n}\log n)$ because $Q(\mathsf{OR}_n) = O(\sqrt{n})$ holds by Grover's algorithm. This is an important result since it shows that the fundamental function DISJ_n can be computed more efficiently than in classical scenario (recall $\mathrm{CC}^{\mathsf{pub}}(\mathsf{DISJ}_n) = \Theta(n)$). This upper bound $\mathrm{QCC}(\mathsf{DISJ}_n) = O(\sqrt{n}\log n)$ was later improved by [26] and finally improved

[a] These classical results are shown in [4, 5] for Set-Disjointness, [6] for Inner-product, and [1, 7] for Equality.

to $O(\sqrt{n})$ by [15]. Ref. [25] gives many important upper bounds for functions $f \circ G$. On the other hand, Razborov [14] treated lower bounds of $\mathrm{QCC}^*(f \circ G)$ and showed several tight bounds when f is a symmetric function and G is AND_2. For example, Ref. [14] shows $\mathrm{QCC}^*(\mathsf{DISJ}_n) = \Omega(\sqrt{n})$ and $\mathrm{QCC}^*(\mathsf{IP}_n) = \Omega(n)$. Combining the $O(\sqrt{n})$ bound [15] and $\Omega(\sqrt{n})$ bound [14] imply $\mathrm{QCC}(\mathsf{DISJ}_n) = \Theta(\sqrt{n})$. Our contributions can be understood as a generalization of these works [25, 14, 15].

As described above, the relation $\mathrm{QCC}(f \circ G) = O(\mathrm{Q}(f)\log n)$ holds when the function G is either AND_2 or XOR_2 [25], and this upper bound was then improved to $O(\sqrt{n})$ by Aaronson and Ambainis [15] when $f = \mathsf{OR}_n$. This implies that the $\log n$ factor in [25] is not required in the case of Set-Disjointness function. Considering this fact, one may wonder whether the $\log n$ overhead is not required for arbitrary function when $G \in \{\mathsf{AND}_2, \mathsf{XOR}_2\}$. Chakraborty et al. [27] treated this problem and gave a negative answer. They exhibited a function f that requires $\Omega(Q(f)\log n)$ communication to compute $f \circ \mathsf{XOR}_2$. This means that the upper bound $O(Q(f)\log n)$ in [25] is tight for generic functions. Interestingly, their subsequent work [28] generalized the result and proved the $\log n$ overhead is not required when f is a symmetric function, even though their protocol crucially uses shared entanglement. In this paper, we focus on functions of the form $\mathsf{SYM} \circ G$ where SYM is a symmetric function. As described below in Section 1.2 and Section 1.3, our first result generalizes the paper [28] and our second result shows a tight lower and upper bound on the quantum communication complexity of such functions $\mathsf{SYM} \circ G$ when $G = \mathsf{AND}_2$.

1.2 First result (Theorem 1): On improving the result [28]

As mentioned above, the paper [28] showed that the $\log n$ factor in $O(Q(f)\log n)$ upper bound is not required when we focus on a symmetric function $f = \mathsf{SYM}$. More precisely, it is shown in Ref. [28] that there exists a protocol for a function $\mathsf{SYM} \circ G$ with $O(Q(\mathsf{SYM})\mathrm{QCC}_{\mathrm{E}}(G))$ qubits of communication ($\mathrm{QCC}_{\mathrm{E}}(G)$ denotes the exact communication complexity of G) which uses *shared entanglement*. Even though the amount of shared entanglement in their protocol is not so large, there are cases when the amount of the entanglement is significantly larger than the communication cost $O(Q(\mathsf{SYM})\mathrm{QCC}_{\mathrm{E}}(G))$ as stated in [28, Remark 4]. Thus, in general shared entanglement can not be included as a part of the communication in their protocol. We improve their result and show that the same statement holds even without any shared entanglement. That is, we show the following theorem.

Theorem 1. *For any symmetric function $f : \{0,1\}^n \to \{0,1\}$ and any two-party function $G : \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$,*

$$\mathrm{QCC}(f \circ G) \in O(Q(f)\mathrm{QCC}_{\mathrm{E}}(G)).$$

Proof technique In the paper [28], the desired protocol is constructed by employing a new technique called *noisy amplitude amplification*, which needs a certain amount of entanglement shared between Alice and Bob. Based on the noisy amplitude amplification technique, Ref. [28] shows the following theorem.

Theorem ([28, Theorem 21])**.** *Suppose Alice (resp. Bob) is given $(X_i)_{i\in[n]} \in \{0,1\}^{jn}$ (resp. $(Y_i)_{i\in[n]} \in \{0,1\}^{kn}$). There is a protocol which satisfies the following conditions:*

- *The protocol uses $O(\sqrt{n}\mathrm{QCC}_{\mathrm{E}}(G))$ qubits of communication and $\lceil \log n \rceil$ EPR pairs.*

- *The protocol finds the coordinate i satisfying $G(X_i, Y_i) = 1$ with probability $99/100$ when such i exists, and outputs "No" with probability 1 when no such i exists.*

Using this protocol as a subroutine, the authors of Ref. [28] constructed the main protocol for $f \circ G$, which inherently requires a certain amount of the entanglement.

On the other hand, in the case of Set-Disjointness, Aaronson and Ambainis [15, Theorem 7.1] showed a protocol with $O(\sqrt{n})$ qubits of communication which *does not use any shared entanglement* but does find a coordinate i satisfying $x_i \wedge y_i = 1$ with probability $99/100$. In their protocol, Alice is given input $x \in \{0,1\}^n$ and Bob is given input $y \in \{0,1\}^n$ beforehand, and they treat the inputs as if its coordinates belong to $[n^{1/3}] \times [n^{1/3}] \times [n^{1/3}]$. After this step, they communicate with $O(\sqrt{n})$ qubits and output $i = (\tilde{i}, \tilde{j}, \tilde{k}) \in [n^{1/3}] \times [n^{1/3}] \times [n^{1/3}]$ satisfying $x_i \wedge y_i = 1$ with probability $99/100$. This implies that in their protocol Alice and Bob do not share any quantum state or randomness before the execution of the protocol, and therefore their protocol does not use any shared entanglement.

Based on the construction of the protocol in [15] rather than the noisy amplitude amplification technique used in [28], we successfully construct a generalized version of the above theorem in Proposition 2 which does not require any shared entanglement. Once we show the generalized version, the rest is shown in a similar manner as in [28], which is described in Section 4. Thus, we obtain the protocol for $\mathsf{SYM} \circ G$ using $O(Q(\mathsf{SYM})\mathrm{QCC_E}(G))$ qubits which does not use any shared entanglement.

1.3 Second result (Theorem 2, 3): On tight upper bounds for $\mathsf{SYM} \circ \mathsf{AND}_2$

In our second result, we focus on tight upper bounds on the quantum communication complexity of $\mathsf{SYM} \circ \mathsf{AND}_2$. We first note here that the paper [28] and our first result already exhibit protocols with $O(Q(\mathsf{SYM}))$ qubits which are more efficient than the protocol in [25] with $O(Q(\mathsf{SYM}) \log n)$ qubits. However, even a protocol with $O(Q(\mathsf{SYM}))$ qubits of communication does not generally give a tight upper bound. For example, the quantum communication complexity of $\mathsf{AND}_n \circ \mathsf{AND}_2$ is $O(1)$ but $Q(\mathsf{AND}_n) = \Theta(\sqrt{n})$. Therefore, we need to develop another technique to show a tight upper bound.

In this framework, Razborov [14] and Sherstov [29] showed the following strong result, based on a simple fact that for any symmetric function SYM, there is a corresponding function D satisfying $\mathsf{SYM}(x) = D(|x|)$ where $|x|$ denotes the Hamming weight of a bit string x.

Theorem ([14, Theorem 2.1] and [29, Theorem 1.1]). *Let $\mathsf{SYM}_n : \{0,1\}^n \to \{0,1\}$ be a symmetric function and $D : \{0, \ldots, n\} \to \{0,1\}$ be a function satisfying $\mathsf{SYM}_n(x) = D(|x|)$. Define*

$$\begin{aligned} \ell_0(D) &= \max\left\{\ell \mid 1 \le \ell \le n/2 \text{ and } D(\ell) \neq D(\ell-1)\right\}, \\ \ell_1(D) &= \max\left\{n-\ell \mid n/2 \le \ell < n \text{ and } D(\ell) \neq D(\ell+1)\right\}. \end{aligned}$$

Then we have $\mathrm{QCC}^*(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in \Omega(\sqrt{n\ell_0(D)} + \ell_1(D))$ and $\mathrm{QCC}(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in O(\{\sqrt{n\ell_0(D)} + \ell_1(D)\} \log n)$.

This theorem already shows the nearly tight bound $\mathrm{QCC}^*(\mathsf{SYM}_n \circ \mathsf{AND}_2) = \tilde{\Theta}(\sqrt{n\ell_0(D)} + \ell_1(D))$ up to a multiplicative $\log n$ factor.[b] To show an exact tight upper bound, it is thus sufficient to create a protocol with $O(\sqrt{n\ell_0(D)} + \ell_1(D))$ qubits of communication by removing

[b] The tilde notation $\tilde{\Theta}$ hides the multiplicative $\log n$ factor.

the $\log n$ factor. In this paper, we successfully show that the multiplicative $\log n$ factor is not required in the model with shared entanglement. That is, we get the following theorem.

Theorem 2. *For any symmetric function $\mathsf{SYM}_n : \{0,1\}^n \to \{0,1\}$, $\mathrm{QCC}^*(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D)} + \ell_1(D))$ holds.*

In the model without shared entanglement, we also show a similar statement, albeit with an additive $\log\log n$ factor. Thus we show

Theorem 3. *For any symmetric function $\mathsf{SYM}_n : \{0,1\}^n \to \{0,1\}$, $\mathrm{QCC}(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D)} + \ell_1(D) + \log\log n)$ holds.*

This shows, for the first time, the tight relation $\mathrm{QCC}^*(\mathsf{SYM}_n \circ \mathsf{AND}_2) = \Theta(\sqrt{n\ell_0(D)} + \ell_1(D))$ in the model with shared entanglement, matching the lower bound by [14, 29]. In the model without shared entanglement, however, there is still a $\log\log n$ gap between the communication cost of our protocol and the lower bound [14, 29]. To fill this gap, we also show that our protocol without shared entanglement is in fact optimal:

Proposition 1. *For any non-trivial symmetric function $f_n : \{0,1\}^n \to \{0,1\}$,*

- *if the function f_n satisfies $\ell_0(D_{f_n}) > 0$ or $\ell_1(D_{f_n}) > 1$,*
$$\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}) + \log\log n)$$
holds.
- *Otherwise (If f_n satisfies $\ell_0(D_{f_n}) = 0$ and $\ell_1(D_{f_n}) \leq 1$), $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Theta(1)$ holds.*

In the proof of Proposition 1, the fooling set argument, a standard technique in communication complexity, plays a fundamental role.

Proof technique Let us now explain the main idea for the desired protocol used in Theorem 2 and Theorem 3. To create the desired protocol for $\mathsf{SYM} \circ \mathsf{AND}_2$, we first decompose the symmetric function $\mathsf{SYM}(x) = D(|x|)$ into the two symmetric functions $\mathsf{SYM}_0(x) := D_0(|x|)$ and $\mathsf{SYM}_1(x) := D_1(|x|)$ as follows:

$$D_0(m) := \begin{cases} D(m) & \text{if } m \leq \ell_0(D) \\ 0 & \text{otherwise} \end{cases}, \quad D_1(m) = \begin{cases} D(m) & \text{if } m > n - \ell_1(D) \\ 0 & \text{otherwise} \end{cases}.$$

Note that the function D takes a constant value on the interval $[\ell_0(D), n-\ell_1(D)]$. As discussed in Section 5, it turns out that computing $\mathsf{SYM}_0 \circ \mathsf{AND}_2$ and $\mathsf{SYM}_1 \circ \mathsf{AND}_2$ separately is enough to compute the entire function $\mathsf{SYM} \circ \mathsf{AND}_2$. Therefore, we only need to design two distinct protocols: one protocol for $\mathsf{SYM}_0 \circ \mathsf{AND}_2$ and the other protocol for $\mathsf{SYM}_1 \circ \mathsf{AND}_2$. We now explain how to design the two protocols.

- To compute $\mathsf{SYM}_0 \circ \mathsf{AND}_2$, we simply use our first result. This uses $O(\sqrt{n\ell_0(D)})$ qubits of communication since $Q(\mathsf{SYM}_0) = O(\sqrt{n\ell_0(D)})$ holds by [30, Theorem 4.10].
- To compute $\mathsf{SYM}_1 \circ \mathsf{AND}_2$, Alice and Bob directly compute the number of elements in the set $\{i \in [n] \mid \mathsf{AND}_2(x_i, y_i) = 1\}$ under the condition[c] $\min\{|x|, |y|\} \geq n - \ell_0(D)$.

[c] If the condition does not hold, $\mathsf{SYM}_1 \circ \mathsf{AND}_2(x, y)$ must be zero. Alice and Bob check this condition with only two bits of communication.

By taking the negation on the inputs, this problem is reduced to the computation of the number of elements in the set $\{i \in [n] \mid x_i = 0 \text{ or } y_i = 0\}$ under the condition $\min\{|x|, |y|\} \leq \ell_0(D)$. In fact, this problem and related problems have been analyzed in several works [31, 32, 33, 34] and it is shown in [32, Theorem 3.1] that $O(\ell_0(D))$ classical communication is sufficient when shared randomness is allowed (and the additional $O(\log \log n)$ bits of communication[d] are required to convert the shared randomness into private randomness).

Combining the above protocols, we create the desired protocol that computes $\mathsf{SYM} \circ \mathsf{AND}_2$ with $O(\sqrt{n\ell_0(D_f)}+\ell_1(D_f))$ communication. One thing which should be noted is that as seen in the above protocol, what Alice and Bob needed to share beforehand is shared randomness, not shared entanglement. This means that we in fact show the upper bound $O(\sqrt{n\ell_0(D_f)} + \ell_1(D_f))$ in a weaker communication model where shared randomness is allowed but shared entanglement is not allowed.

1.4 Organization of the paper

In Section 2, we list several notations and facts used in this paper. In Section 3, we generalize the protocol for Set-Disjointness [15] and create a useful protocol which is used for our main results. In Section 4, we treat the first result and show Theorem 1. In Section 5, we treat the second result and show Theorem 2 and Theorem 3.

2 Preliminaries

Model of communication A natural model of quantum communication (without shared entanglement) between Alice and Bob for computing $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ is as follows:

1. Alice is given $x \in \mathcal{X}$ and Bob is given $y \in \mathcal{Y}$. The entire registers are initially set to $|0\rangle_A^{n_A}|0\rangle_C|0\rangle_B^{n_B}$ for some positive integers n_A, n_B.
2. Alice performs a unitary operator on AC which depend on her input x,.
3. Bob performs a unitary operator on BC which depend on his input y,.

   ⋮ Step 2 and 3 are repeated for a specified number of rounds.

4. Finally, both players perform an individual measurement on the register A for Alice and B for Bob and output answers based on the outcomes.

In the model with shared entanglement, the initial registers are instead set to $|\psi\rangle_{AB}|0\rangle_C$ for a pure state $|\psi\rangle$. Any other natural models considered in literature [9, 10, 35] have essentially the same power as of this model.

For any function f, we denote the quantum communication complexity of zero-error protocols, the bounded-error quantum communication complexity (with error $\leq 1/3$) *without shared entanglement*, the bounded-error quantum communication complexity (with error $\leq 1/3$) with

[d] In this case, $\min\{|x|, |y|\} \geq n - \ell_0(D)$ holds and therefore Newman's theorem tells us that $O(\log \log \#\{x \mid |x| \geq n - \ell_0(D)\})$ bits simulates the shared randomness. As shown in Section 5, the additional bits required are in fact bounded by $O(\log \log n)$.

shared entanglement of a function f by $\mathrm{QCC_E}(f), \mathrm{QCC}(f)$ and $\mathrm{QCC}^*(f)$ respectively. Trivially, it holds that $\mathrm{QCC}^*(f) \le \mathrm{QCC}(f) \le \mathrm{QCC_E}(f)$. We also denote the bounded-error query complexity of a function f by $\mathrm{Q}(f)$. For a n-bit string x, we denote the bitwise negation of x by $\neg x = (\neg x_1, \dots, \neg x_n)$.

Symmetric function Here we list several important facts about symmetric functions. For any symmetric function f, f can be represented as $f(x) = D_f(|x|)$ using some function $D_f : \{0, 1, \dots, n\} \to \{0, 1\}$. Denoting

$$\begin{aligned} \ell_0(D_f) &= \max\left\{\ell \mid 1 \le \ell \le n/2 \text{ and } D_f(\ell) \ne D_f(\ell - 1)\right\}, \\ \ell_1(D_f) &= \max\left\{n - \ell \mid n/2 \le \ell < n \text{ and } D_f(\ell) \ne D_f(\ell + 1)\right\}, \end{aligned}$$

prior works [36, 30] show that the query complexity $Q(f)$ of a symmetric function f is characterized as $Q(f) = \Theta(\sqrt{n(\ell_0(D_f) + \ell_1(D_f))})$.

3 Communication cost for finding elements

This section is devoted to show Proposition 2, which is the quantum communication version of [15, Theorem 5.16].

Proposition 2. *There is a protocol $\mathsf{FIND\text{-}MORE}_k$ using $O(\sqrt{\frac{n}{k}}\mathrm{QCC_E}(G))$ qubits and using shared randomness which satisfies the following:*

- *The protocol outputs a coordinate $i \in [n]$ such that $G(X_i, Y_i) = 1$ w.p. $\ge 99/100$ when there exist at least k such coordinates.*
- *The protocol answers "there is no such coordinate" w.p. 1 when there is no such coordinate.*
- *The protocol does not use any shared entanglement.*

The proof is given in Section 3.2.

3.1 A key lemma

To show Proposition 2, we first show the following lemma:

Lemma 1. *For $\gamma \in \mathbb{N}$, there is a protocol $\mathsf{FIND\text{-}EXACT}_\gamma$ using $O(\sqrt{\frac{n}{\gamma}}\mathrm{QCC_E}(G))$ qubits and shared randomness which satisfies the following:*

- *The protocol outputs a coordinate $i \in [n]$ such that $G(X_i, Y_i) = 1$ w.p. $\ge 99/100$ when there exist exactly k such coordinates for some $k \in (\gamma/3, 2\gamma/3)$.*
- *The protocol answers "there is no such coordinate" w.p. 1 when there is no such coordinate.*
- *The protocol does not use any shared entanglement.*

In the proof of Lemma 1, we use Lemma 2 which is a modified protocol of the one given in [15, Section 7]. See Appendix 1 for the modification.

Lemma 2. *There is a protocol $\mathsf{FIND\text{-}ONE}$ with $O(\sqrt{n}\mathrm{QCC_E}(G))$ cost which satisfies the following:*

- *The protocol outputs the coordinate $i \in [n]$ such that $G(X_i, Y_i) = 1$ w.p. $\geq 99/100$ when such i exists.*
- *The protocol answers "there is no such coordinate" w.p. 1 when there is no such coordinate.*
- *The protocol does not use any shared entanglement.*

Proof of Lemma 1. We first divide the set $\{1, \dots, n\}$ into n/γ subsets $A_j = \{(j-1)\gamma + 1, \dots, j\gamma\}$ $(1 \leq j \leq n/\gamma)$, each containing γ sub-inputs. Using shared randomness, Alice and Bob pick a set of coordinates $\{i_1, \dots, i_{n/\gamma}\} \subset [n]$ where each i_j is chosen uniformly at random from the set A_j. Alice and Bob then perform the protocol FIND-ONE pretending the inputs are $(X_{i_1}, \dots, X_{i_{n/\gamma}})$ for Alice and $(Y_{i_1}, \dots, Y_{i_{n/\gamma}})$ for Bob. Since FIND-ONE requires $O(\sqrt{n}\mathrm{QCC_E}(G))$ qubits of communication for the input length n, this protocol with the input length n/γ requires $O(\sqrt{\frac{n}{\gamma}}\mathrm{QCC_E}(G))$ qubits of communication.

We now analyze the correctness probability of this protocol, following the technique used in [15, Lemma 5.15]. Assume there exist exactly k coordinates satisfying $G(X_i, Y_i) = 1$ and $3k/2 < \gamma < 3k$ holds, and let $\{x_1, \dots, x_k\} \subset [n]$ be the set of such coordinates and $I_1, \dots, I_{n/\gamma}$ be the random variables for picking up $i_1, \dots, i_{n/\gamma}$. Then for any $i \in [k]$, there is a unique $j(i) \in \{1, \dots, n/\gamma\}$ such that $x_i \in A_{j(i)}$, since $A_1, \dots, A_{n/\gamma}$ give a partition of the set $[n]$. Therefore the event

$$E_{i_0} := \text{"The coordinate } x_{i_0} \text{ alone is chosen by } I_1 \cdots I_{n/\gamma} \text{ among all } x_1, \dots, x_k\text{."}$$

is equivalent to "$I_{j(i_0)} = x_{i_0}$ and $\forall j \neq j(i_0),\ \forall i \in [k] \setminus \{i_0\},\ I_j \neq x_i$". We thus obtain

$$\Pr(E_{i_0}) = \Pr(I_{j(i_0)} = x_{i_0}) \cdot \Pr(\forall j \neq j(i_0),\ \forall i \in [k] \setminus \{i_0\}\ I_j \neq x_i).$$

Now observe that the probability: $\Pr(I_{j(i_0)} = x_{i_0})$ is equal to $1/\gamma$ by definition of I_j, and the probability: $\Pr(\forall j \neq j(i_0),\ \forall i \in [k] \setminus \{i_0\}\ I_j \neq x_i)$ satisfies

$$\begin{aligned}
\Pr(\forall j \neq j(i_0),\ \forall i \in [k] \setminus \{i_0\}\ I_j \neq x_i) &= 1 - \Pr(\exists i \in [k] \setminus \{i_0\}\ s.t.\ \exists j \neq j_{i_0},\ I_j = x_i) \\
&\geq 1 - \sum_{i \in [k] \setminus \{i_0\}} \Pr(\exists j \neq j_{i_0}\ s.t.\ I_j = x_i) \\
&\geq 1 - \frac{(k-1)}{\gamma}
\end{aligned}$$

due to $\Pr(A) = 1 - \Pr(A^c)$ (the superscript c denotes the complement) and $\Pr(\bigcup_i A_i) \leq \sum_i \Pr(A_i)$ for any events A and A_i's. Therefore it follows that

$$\Pr(E_{i_0}) \geq \frac{1}{\gamma}\left(1 - \frac{k-1}{\gamma}\right) \geq \frac{1}{\gamma}\left(1 - \frac{k}{\gamma}\right).$$

Considering the events "the coordinate i_0 is chosen" are mutually disjoint, we see that the probability of "exactly one such coordinate is chosen" is at least $k/\gamma - (k/\gamma)^2$. Since $3k/2 < \gamma < 3k$ holds, we observe that the probability is at least $2/9$. This shows the event "at least one element is chosen" occurs w.p. $\geq 2/9$.

Therefore, by the property of FIND-ONE, our new protocol satisfies the following:

- The protocol outputs the coordinate $i \in [n]$ such that $G(X_i, Y_i) = 1$ w.p. $\Omega(1)$ when there exist exactly k such coordinates for some k satisfying $3k/2 < \gamma < 3k$.
- The protocol answers "there is no such coordinate" w.p. 1 when there is no such coordinate.
- The protocol does not use any shared entanglement.

To amplify the success probability $\Omega(1)$ to 99/100, Alice and Bob perform this above protocol recursively while at each repetition checking if the output i_{out} satisfies $G(X_{i_{\text{out}}}, Y_{i_{\text{out}}}) = 1$. This repetition uses only some constant overhead on the communication cost and hence we obtain the desired statement. □

3.2 Proof of Proposition 2

Using the protocol $\mathsf{FIND\text{-}EXACT}_\gamma$, we show Proposition 2 as follows.

Proof of Proposition 2. The protocol $\mathsf{FIND\text{-}MORE}_k$ is executed as follows:

(1) For $j = 0$ to $\log_2(n/k)$, Alice and Bob perform $\mathsf{FIND\text{-}EXACT}_{\gamma_j}$ where $\gamma_j = 2^j k$.

(2) As shared randomness, Alice and Bob pick one coordinate i uniformly at random from the set $[n]$ and check if $G(X_i, Y_i) = 1$. This is repeated for $O(1)$ times.

We first analyze the communication cost of this protocol. The first step requires

$$\sum_{j=0}^{\log_2(n/k)} O\left(\sqrt{\frac{n}{2^j k}}\mathrm{QCC}_{\mathrm{E}}(G)\right) = O\left(\sqrt{\frac{n}{k}}\mathrm{QCC}_{\mathrm{E}}(G)\right) \sum_{j=0}^{\log_2(n/k)} \frac{1}{2^{j/2}} = O\left(\sqrt{\frac{n}{k}}\mathrm{QCC}_{\mathrm{E}}(G)\right)$$

qubits of communication. The second step requires $O(\mathrm{QCC}_{\mathrm{E}}(G))$ qubits of communication. Therefore, in total, $O\left(\sqrt{\frac{n}{k}}\mathrm{QCC}_{\mathrm{E}}(G)\right)$ qubits are used in this protocol.

Next we analyze the correctness probability of this protocol. Let $k^* \geq k$ be the number of coordinates satisfying $G(X_i, Y_i) = 1$. If $k^* \leq n/3$, then there exists j satisfying $3k^*/2 < \gamma_j < 3k^*$. Therefore, $\mathsf{FIND\text{-}EXACT}_{\gamma_j}$ finds the desired coordinate w.p. $\geq 99/100$. On the other hand, if $k^* > n/3$, the second step finds the desired coordinate w.p. 1/3. Then O(1) repetitions increase the success probability to 99/100. □

4 Communication protocol for symmetric functions

In [28, Theorem 22 and Theorem 25], the following theorem has been shown (with a slightly different expression):

Theorem ([28, Theorem 22 and Theorem 25])**.** *Suppose $\mathsf{FIND\text{-}MORE}_k$ uses m EPR-pairs as shared entanglement and* arbitrarily amount of *shared randomness. Then for any symmetric function $f : \{0,1\}^n \to \{0,1\}$ and any two-party function $G : \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$, there is a protocol with $O(Q(f)\mathrm{QCC}_{\mathrm{E}}(G))$ qubits which satisfies the following:*

- *The protocol successfully computes $f \circ G$ with probability $\geq 99/100$.*
- *The protocol uses $m \cdot O(\ell_0(D_f) + \ell_1(D_f))$ EPR-pairs as shared entanglement.*
- *The protocol uses $O(\log n)$ bits of shared randomness.*

As is shown in Proposition 2, our modified protocol $\mathsf{FIND\text{-}MORE}_k$ does not use any shared entanglement. Therefore, we set $m = 0$ in the statement above and obtain the following theorem. (Note that $O(\log n)$ bits of shared randomness are included in a part of communication since the $O(\log n)$ bits are negligible compared to $Q(f) \geq \Omega(\sqrt{n})$ when f is not trivial.)

Theorem 1. *For any symmetric function* $f : \{0,1\}^n \to \{0,1\}$ *and any two-party function* $G : \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$,

$$\mathrm{QCC}(f \circ G) \in O(Q(f)\mathrm{QCC_E}(G)).$$

5 Tight upper bound for symmetric functions

In this section, we show the following two theorems:

Theorem 2. *For any symmetric function* $\mathsf{SYM}_n : \{0,1\}^n \to \{0,1\}$, $\mathrm{QCC}^*(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D)} + \ell_1(D)$ *holds.*

Theorem 3. *For any symmetric function* $\mathsf{SYM}_n : \{0,1\}^n \to \{0,1\}$, $\mathrm{QCC}(\mathsf{SYM}_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D)} + \ell_1(D) + \log\log n)$ *holds.*

To show these theorems, we use the following protocol that is a modification of the protocol given in [32, Theorem 3.1]. For completeness, we describe the modification in Appendix B.

Proposition 3. *Suppose the inputs* $x, y \in \{0,1\}^n$ *satisfy* $\max\{|x|, |y|\} \leq k$. *There is a public coin classical protocol*[e] *with* $O(k)$ *bits of communication which computes the set* $\{i | x_i = y_i = 1\} \subset [n]$ *w.p.* $99/100$.

Following the technique used in [14, Section 4], we prove Theorem 2 and Theorem 3 as follows:

Proof of Theorem 2 and Theorem 3. Let us first describe some important facts based on the arguments in [14, 29]. For any symmetric function f_n, the corresponding function D_{f_n} is constant on the interval $[\ell_0(D_{f_n}), n - \ell_1(D_{f_n})]$. Without loss of generality, assume D_{f_n} takes 0 on the interval. (If D_{f_n} takes 1 on the interval, we take the negation of D_{f_n}.) Defining D_0 and $D_1 : \{0, \ldots, n\} \to \{0,1\}$ as

$$D_0(m) = \begin{cases} D_{f_n}(m) & \text{if } m \leq \ell_0(D_{f_n}) \\ 0 & \text{otherwise} \end{cases}, D_1(m) = \begin{cases} D_{f_n}(m) & \text{if } m > n - \ell_1(D_{f_n}) \\ 0 & \text{otherwise} \end{cases},$$

$D_{f_n} = D_0 \vee D_1$ holds. Therefore, by defining $f_n^0(x) := D_0(|x|)$ and $f_n^1(x) := D_1(|x|)$, we get $f_n \circ \mathsf{AND}_2 = (f_n^0 \circ \mathsf{AND}_2) \vee (f_n^1 \circ \mathsf{AND}_2)$. This means, computing $f_n^0 \circ \mathsf{AND}_2$ and $f_n^1 \circ \mathsf{AND}_2$ separately is sufficient to compute the entire function $f_n \circ \mathsf{AND}_2$. As another important fact needed for our explanation, we note that the query complexity of f_n^0 equals to $O(\sqrt{n\ell_0(D_{f_n})})$ which is proven in [36].

From now on, we describe two protocols: one protocol for the computation of f_n^0 and the other one for the computation of f_n^1.

- **Protocol for** f_n^0: We simply apply the protocol of Theorem 1 with $G = \mathsf{AND}_2$ (note that f_n^0 is a symmetric function). This protocol uses $O(\sqrt{n\ell_0(D_{f_n})})$ qubits because $Q(f_n^1) = \Theta(\sqrt{n\ell_0(D_{f_n})})$ holds.

[e] Note that this protocol may use a large amount of shared randomness.

- **Protocol for** f_n^1: First, Bob sends Alice one bit: 1 if $|\neg y| \leq \ell_1(D_{f_n})$ and 0 otherwise. If Alice receives 1 and $|\neg x| \leq \ell_1(D_{f_n})$ holds, they perform the protocol of Proposition 3 with the inputs $\neg x$ and $\neg y$. Otherwise, $\min\{|x|, |y|\} < n - \ell_0(D_{f_n})$ holds and therefore $f_n^0 \circ \mathsf{AND}_2(x, y)$ must be zero by the definition of D_1. After the execution of the protocol of Proposition 3, Alice and Bob know the set $\{i \in [n] \mid x_i = y_i = 0\}$. Next, Alice sends $|\neg x|$ and Bob sends $|\neg y|$ using $\log \ell_0(D_{f_n})$ communication, and they finally compute $\#\{i \leq n \mid x_i = y_i = 1\}$ as $\#\{i \leq n \mid x_i = y_i = 1\} = n + \#\{i \in [n] \mid x_i = y_i = 0\} - |\neg x| - |\neg y|$. This protocol uses $O(\ell_1(D_{f_n}))$ communication bits.

  We then evaluate the cost for public coins. Even though the execution of this protocol may require much shared randomness, Newman's theorem [8] ensures that $O(\log \log |S|)$ bits are sufficient when the inputs x, y belong to a set S. Since $|\neg x|, |\neg y| \leq \ell_1(D_{f_n})$ holds when executed and using the fact $\#\{x \in \{0,1\}^n \mid |\neg x| \leq k\} \leq n^k$, we conclude that $O(\log(\log n^{\ell_1(D_{f_n})})) = O(\log \ell_1(D_{f_n}) + \log \log n)$ bits of shared randomness are sufficient. Moreover, since $O(\log \ell_1(D_{f_n}))$ bits of shared randomness are negligible compared to $O(\ell_1(D_{f_n}))$ bits in communication and therefore included as a part of communication with no additional communication cost, we only need to use $O(\log \log n)$ bits as a shared randomness.

Combining these two protocols, we get the desired protocol with $O(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}))$ cost which uses $O(\log \log n)$ public coins. This shows $\mathrm{QCC}^*(f_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}))$ and $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}) + \log \log n)$ by Alice sending $O(\log \log n)$ random bits instead of the shared randomness. $\square$

By combining the arguments we showed so far, we obtain the tight bound $\mathrm{QCC}^*(f_n \circ \mathsf{AND}_2) \in \Theta(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}))$ on the communication model with shared entanglement. On the model without shared entanglement, our bound $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in O(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}) + \log \log n)$ still have the additive $\log \log n$ difference from the lower bound. We next show this upper bound is indeed optimal by using a standard technique, the *fooling set* argument.

Proposition 1. *For any non-trivial symmetric function* $f_n : \{0,1\}^n \to \{0,1\}$,

- *if the function* f_n *satisfies* $\ell_0(D_{f_n}) > 0$ *or* $\ell_1(D_{f_n}) > 1$,

$$\mathrm{QCC}(f_n \circ \mathit{AND}_2) \in \Omega(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}) + \log \log n)$$

  holds.

- *Otherwise (i.e., if* f_n *satisfies* $\ell_0(D_{f_n}) = 0$ *and* $\ell_1(D_{f_n}) \leq 1$*),* $\mathrm{QCC}(f_n \circ \mathit{AND}_2) \in \Theta(1)$ *holds.*

Proof. Let us first prove that $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Theta(1)$ holds when $\ell_0(D_{f_n}) = 0$ and $\ell_1(D_{f_n}) \leq 1$ hold. In this case, there are only two types of the functions: $f_n = \mathsf{AND}_n$ or $f_n = \neg\mathsf{AND}_n$. In either case of the functions, Alice and Bob only need to send one single bit expressing whether $x = (1, \ldots, 1)$ for Alice ($y = (1, \ldots, 1)$ for Bob). Therefore we obtain $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Theta(1)$ since a lower bound $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(1)$ is trivial.

The rest is to show $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}) + \log \log n)$ holds assuming $\ell_0(D_{f_n}) > 0$ or $\ell_1(D_{f_n}) > 1$. First, we note that the $\log \log n$ factor becomes negligible comparing to $\sqrt{n\ell_0(D_{f_n})}+\ell_1(D_{f_n})$ when $\ell_0(D_{f_n}) > 0$ holds. This means that the well-known lower bound $\Omega(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}))$ [14] already gives a tight lower bound. Therefore, we only need to show $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\ell_1(D_{f_n}) + \log\log n)$ holds assuming $\ell_0(D_{f_n}) = 0$. Moreover, the lower bound $\mathrm{QCC}^*(f_n \circ \mathsf{AND}_2) \in \Omega(\sqrt{n\ell_0(D_{f_n})} + \ell_1(D_{f_n}))$ shown in [14] implies $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\ell_1(D_{f_n}))$. Therefore, it is sufficient to show $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\log\log n)$ when $\ell_0(D_{f_n}) = 0$ and $\ell_1(D_{f_n}) > 1$ hold.

Assuming $\ell_0(D_{f_n}) = 0$, $\ell_1(D_{f_n}) > 1$ and $D_{f_n} \equiv 0$ on $[\ell_0(D_{f_n}), n - \ell_1(D_{f_n})]$ without loss of generality, we show $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \in \Omega(\log\log n)$. To show this, we use the fooling set argument:

Theorem 4 (Fooling set argument [2, 3])**.** *For a function $f : X \times Y \to \{0,1\}$, assume that a subset $S \subset X \times Y$ satisfies*

- *for any $(x,y) \in S$, $f(x,y) = 1$,*
- *for any $(x,y),(x',y') \in S$, $(x,y) \neq (x',y') \Rightarrow f(x',y) = 0$ or $f(x,y') = 0$.*

Then the deterministic communication complexity of f is larger or equal to $\log|S|$.

Define

$$\mathrm{FS}_n := \{(x,y) \in \{0,1\}^n \times \{0,1\}^n \mid x = y \text{ and } |\neg x| = \ell_1(D_{f_n}) - 1\}.$$

Then we see that for any $(x,y) \in \mathrm{FS}_n$, $f_n \circ \mathsf{AND}_2(x,y) = 1$ and for any $(x,y),(x',y') \in \mathrm{FS}_n$, $(x,y) \neq (x',y')$ implies $f_n \circ \mathsf{AND}_2(x,y') = f_n \circ \mathsf{AND}_2(x',y) = 0$. Therefore, the deterministic communication complexity $\mathrm{DCC}(f_n \circ \mathsf{AND}_2)$ satisfies

$$\mathrm{DCC}(f_n \circ \mathsf{AND}_2) \geq \log_2|\mathrm{FS}_n|$$

by the fooling set argument. As shown in [37, Theorem 4], it is well-known that $\mathrm{QCC}(f) \geq \log \mathrm{DCC}(f)$ for any function f. Therefore, by observing $|\mathrm{FS}_n| = \binom{n}{\ell_1(D_{f_n})-1} \geq \Omega(n)$ for $\ell_1(D_{f_n}) > 1$, we obtain the desired statement $\mathrm{QCC}(f_n \circ \mathsf{AND}_2) \geq \Omega(\log\log n)$. $\square$

Acknowledgements

The author was partially supported by the MEXT Q-LEAP grant No. JPMXS0120319794. The author would like to take this opportunity to thank the Nagoya University Interdisciplinary Frontier Fellowship supported by Nagoya University and JST, the establishment of university fellowships towards the creation of science technology innovation, Grant Number JPMJFS2120. The author also would like to thank François Le Gall for his kindness and valuable comments and Ronald de Wolf for kind comments on an earlier draft of this paper. The author also would like to thank the anonymous reviewer for a careful review and valuable comments.

References

1. A. Yao (1979), *Some complexity questions related to distributive computing (preliminary report)*, STOC, pp. 209-213.

2. E. Kushilevitz and N. Nisan (1996), *Communication Complexity*, Cambridge University Press.
3. A. Rao and A. Yehudayoff (2020), *Communication Complexity: and Applications*, Cambridge University Press.
4. A. A Razborov (1992), *On the distributional complexity of disjointness*, Theor. Comput. Sci., 106(2):385-390, 1992.
5. Z. Bar-Yossef, T.S. Jayram, R. Kumar, and D. Sivakumar (2004), *An information statistics approach to data stream and communication complexity*, J. Comput. Syst. Sci., 68(4):702-732.
6. B. Chor and O. Goldreich (1988), *Unbiased bits from sources of weak randomness and probabilistic communication complexity*, SIAM J. Comput., 17(2):230-261.
7. T. Feder, E. Kushilevitz, M. Naor, and N. Nisan (1995), *Amortized communication complexity*, SIAM J. Comput., 24(4):736-750.
8. I. Newman (1991), *Private vs. common random bits in communication complexity*, Inf. Process. Lett., 39(2):67-71.
9. A. Yao (1993), *Quantum circuit complexity*, FOCS, pp. 352-361.
10. R. Cleve and H. Buhrman (1997), *Substituting quantum entanglement for communication*, Phys. Rev. A, 56(2):1201, 1997.
11. H. Buhrman, R. Cleve, and W. van Dam (2001), *Quantum entanglement and communication complexity*, SIAM J. Comput., 30(6):1829-1841.
12. G. Brassard (2003), *Quantum communication complexity*, Found. Phys., 33(11):1593-1616, 2003.
13. H. Buhrman, R. Cleve, S. Massar, and R. de Wolf (2010), *Nonlocality and communication complexity*, Rev. Mod. Phys., 82:665-698, 2010.
14. A. A Razborov (2003), *Quantum communication complexity of symmetric predicates*, Izvestiya: Mathematics, 67(1):145.
15. S. Aaronson and A. Ambainis (2005), *Quantum search of spatial regions*, Theory Comput, 1(4):47-79.
16. R. Cleve, W. van Dam, M. Nielsen, and A. Tapp (1998), *Quantum entanglement and the communication complexity of the inner product function*, QCQC, pp. 61-74.
17. H. Buhrman and R. de Wolf (2001), *Communication complexity lower bounds by polynomials*, CCC, pp. 120-130.
18. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt (1969), *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett., 23:880-884.
19. N. D. Mermin (1990), *Simple unified form for the major no-hidden-variables theorems* Phys. Rev. Lett., 65:3373-3376.
20. D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf (2006), *Bounded-error quantum state identification and exponential separations in communication complexity*, STOC, pp. 594-603.
21. D. Gavinsky (2008), *On the role of shared entanglement*, Quantum Inf. Comput., 8(1):82-95, 2008.
22. Y. Shi and Y. Zhu (2009), *Quantum communication complexity of block-composed functions*, Quantum Inf. Comput., 9(5):444-460, 2009.
23. T. Lee and S. Zhang (2010), *Composition theorems in communication complexity*, ICALP, pp. 475-489.
24. A. Ada, A. Chattopadhyay, O. Fawzi, and P. Nguyen (2012), *The nof multiparty communication complexity of composed functions*, ICALP, pp. 13-24.
25. H. Buhrman, R. Cleve, and A. Wigderson (1998), *Quantum vs. classical communication and computation*, STOC, pp. 63-68.
26. P. Høyer and R. de Wolf (2002), *Improved quantum communication complexity bounds for disjointness and equality*, STACS, pp. 299-310.
27. S. Chakraborty, A. Chattopadhyay, N. S. Mande, and M. Paraashar (2020), *Quantum query-to-communication simulation needs a logarithmic overhead*, CCC, 32:1-32:15.
28. S. Chakraborty, A. Chattopadhyay, P. Høyer, Nikhil S. Mande, Manaswi Paraashar, and Ronald de Wolf (2022), *Symmetry and quantum query-to-communication simulation*, STACS, pp. 20:1-20:23.
29. A. A. Sherstov (2011), *The pattern matrix method*, SIAM J. Comput., 40(6):1969-2000.
30. R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf (2001), *Quantum lower bounds by*

polynomials, Journal of the ACM, 48(4):778-797.
31. W. Huang, Y. Shi, S. Zhang, and Y. Zhu (2006), *The communication complexity of the hamming distance problem*, Inf. Process. Lett., 99(4):149-153.
32. J. Brody, A. Chakrabarti, R. Kondapally, D. P. Woodruff, and G. Yaroslavtsev (2014), *Beyond set disjointness: The communication complexity of finding the intersection*, PODC, pp. 106-113.
33. J. Brody, A. Chakrabarti, R. Kondapally, D. P. Woodruff, and G. Yaroslavtsev (2016), *Certifying equality with limited interaction*, Algorithmica, 76(3):796-845.
34. D. Huang, S. Pettie, Y. Zhang, and Z. Zhang (2020), *The communication complexity of set intersection and multiple equality testing*, SODA, pp. 1715-1732.
35. D. Touchette (2015), *Quantum information complexity*, STOC, pp. 317-326.
36. R. Paturi (1992), *On the degree of polynomials that approximate symmetric boolean functions (preliminary version)*, STOC, pp. 468-474.
37. I. Kremer and N. Nisan (1995), *Quantum communication*, Technical report.

Appendix A Modification for Lemma 2

Here we describe how the protocol given in [15, Section 7] is modified to the protocol in Theorem 2. In [15, Section 7], the authors proposed a protocol that finds $i \in [n]$ such that $x_i \wedge y_i = 1$ where Alice is given $x \in \{0,1\}^n$ and Bob is given $y \in \{0,1\}^n$. In the protocol, Alice and Bob perform the query

$$O_{\mathrm{AND}} : |i, z\rangle_A |i\rangle_B \mapsto |i, z \oplus (x_i \wedge y_i)\rangle_A |i\rangle_B$$

for $O(\sqrt{n})$ times and other operations which require $O(\sqrt{n})$ communication. Since the query operation is implemented using 2-qubits of communication, this protocol requires $2O(\sqrt{n}) + O(\sqrt{n}) = O(\sqrt{n})$ communication.

Our modification for finding i such that $G(X_i, Y_i) = 1$ is simple. We just replace the query O_{AND} to

$$O_G : |i, z\rangle_A |i\rangle_B \mapsto |i, z \oplus G(X_i, Y_i)\rangle_A |i\rangle_B.$$

This protocol indeed finds the desired coordinate i, which is shown in the same manner as in [15, Section 7]. Let us analyze the communication cost of this protocol. Since $\mathrm{QCC_E}(G)$ denotes the exact communication complexity of G, the operation O_G is implemented using $2\mathrm{QCC_E}(G)$ qubits. (First $\mathrm{QCC_E}(G)$ communication is used to compute G and the second $\mathrm{QCC_E}(G)$ is used to compute reversely and clear the unwanted registers.) Other operations are the same as in the original protocol and therefore use $O(\sqrt{n})$ communication. Considering that the operation O_G is performed for $O(\sqrt{n})$ times, we see that our modified protocol uses $O(\sqrt{n}) + \mathrm{QCC_E}(G)O(\sqrt{n}) = O(\mathrm{QCC_E}(G)\sqrt{n})$ qubits of communication.

Appendix B Modification for Proposition 3

In [32, Theorem 3.1], the authors originally showed the following.

Theorem 5. *Suppose the inputs $x, y \in \{0,1\}^n$ satisfy $\max\{|x|, |y|\} \leq k$. There exists an $O(\sqrt{k})$-round constructive randomized classical protocol that outputs the set $\{i \mid x_i = y_i = 1\}$ with success probability $1 - 1/poly(k)$. In the model of shared randomness the total expected communication is $O(k)$.*

To modify this theorem for Proposition 3, we need to take care of the success probability and the *expected* communication. To take care of the success probability, we first take a sufficiently large constant k_0 such that for any $k \geq k_0$, $1/\mathrm{poly}(k) \leq 1/200$. If $k < k_0$ holds, the parties perform the protocol in Theorem 5 with the constant k_0. This requires $O(k_0)$ expected communication. Otherwise (i.e., when $k > k_0$ holds), the parties perform the protocol in Theorem 5 with the constant k, which requires $O(k)$ expected communication. Since k_0 is a constant, the protocol by this modification still requires $O(k)$ expected communication with error $\leq 1/200$.

To convert the expected communication to the worst-case communication, we use Markov inequality. Suppose this protocol requires $C \cdot k$ expected communication. Then the probability of "the communication cost $\geq 200C \cdot k$" is less than or equal to $1/200$ by Markov inequality. We create the desired protocol by Alice and Bob aborting communication when its cost gets $200C \cdot k$. This modified protocol still have the success probability $\geq 99/100$, since the first modification has the error $1/200$ and the second modification affects the error at most $1/200$.