Vol.2022-QS-6 No.19
2022/7/8

多人数の量子通信複雑性にける新しい手法

ルガル フランソワ[1,a)]　駿河 大樹[1,b)]

概要：The main conceptual contribution of this technical report is investigating quantum multiparty communication complexity in the setting where communication is *oblivious*. This requirement, which to our knowledge is satisfied by all quantum multiparty protocols in the literature, means that the communication pattern, and in particular the amount of communication exchanged between each pair of players at each round is fixed *independently of the input* before the execution of the protocol. We show, for a wide class of functions, how to prove strong lower bounds on their oblivious quantum k-party communication complexity using lower bounds on their *two-party* communication complexity. We apply this technique to prove tight lower bounds for all symmetric functions, and in particular obtain an optimal $\Omega(k\sqrt{n})$ lower bound on the oblivious quantum k-party communication complexity of the n-bit Set-Disjointness function. We also obtain (nearly) matching upper bounds by examining the optimal protocols for each function. In this technical report, we overview these results and do not give most of the technical proofs.

Bounds on oblivious multiparty quantum communication complexity

1. Introduction

1.1 Background

1.1.1 Communication complexity.

Communication complexity, first introduced by Yao in a seminal paper [30] to investigate circuit complexity, has become a central concept in theoretical computer science with a wide range of applications (see [16], [22] for examples). In its most basic version, called two-party (classical) communication complexity, two players, usually called Alice and Bob, exchange (classical) messages in order to compute a function of their inputs. More precisely, Alice and Bob are given inputs $x_1 \in \{0,1\}^n$ and $x_2 \in \{0,1\}^n$, respectively, and their goal is to compute a function $f : (x_1, x_2) \mapsto \{0,1\}$ by communicating with each other, with as few communication as possible.

There are two important ways of generalizing the classical two-party communication complexity: one is to consider classical *multiparty* communication complexity and the other one is to consider *quantum* two-party communication complexity. In (classical) multiparty communication complexity, there are k players P_1, P_2, ..., P_k, each player P_i is given an input $x_i \in \{0,1\}^n$. The players seek to compute a given function $f : (x_1, \ldots, x_k) \mapsto \{0,1\}$ using as few (classical) communication as possible.[*1] The other way of generalizing the classical two-party communication complexity is *quantum* two-party communication complexity, where Alice and Bob are allowed to use *quantum* communication, i.e., they can exchange messages consisting of quantum bits. Since its introduction by Yao [29], the notion of quantum two-party communication complexity has been the subject of intensive research in the past thirty years, which lead to several significant achievements, e.g., [4], [5], [10], [11], [28], [29].

In this paper, we consider both generalizations simultaneously: we consider quantum multiparty communi-

[1] Nagoya University
[a)] legall@math.nagoya-u.ac.jp
[b)] suruga.daiki.i1@s.mail.nagoya-u.ac.jp

[*1] This way of distributing inputs is called the number-in-hand model. There exists another model, called the number-on-the-forehead model, which we do not consider in this paper.

cation complexity for $k > 2$ parties. This generalization has been the subject of several works [6], [17], [18], [27] but, compared to the two-party case, is still poorly understood.

1.1.2 Set-Disjointness.

One of the most studied functions in communication complexity is Set-Disjointness. For any $k \geq 2$ and any $n \geq 1$, the k-party n-bit Set-Disjointness function, written $\mathrm{DISJ}_{n,k}$, has for input a k-tuple $(x_1, \ldots, x_k)$, where $x_i \in \{0,1\}^n$ for each $i \in \{1, \ldots, k\}$. The output is 1 if there exists an index $j \in \{1, \ldots, n\}$ such that $x_1[j] = x_2[j] = \cdots = x_k[j] = 1$, where $x_i[j]$ denotes the j-th bit of the string x_i, and 0 otherwise. The output can thus be written as

$$\mathrm{DISJ}_{n,k}(x_1, \ldots, x_k) = \bigvee_{j=1}^{n} (x_1[j] \wedge \cdots \wedge x_k[j]).$$

Set-Disjointness plays a central role in communication complexity since a multitude of problems can be analyzed via a reduction from or to this function (see [9] for a good survey). In the two party classical setting, the communication complexity of Set-Disjointness is $\Theta(n)$: while the upper bound $O(n)$ is trivial, the proof of the lower bound $\Omega(n)$, which holds even in the randomized setting, is highly non-trivial [15], [23]. The k-party Set-Disjointness function with $k > 2$ has received much attention as well, especially since it has deep applications to distributed computing [12]. Proving strong lower bounds on multiparty communication complexity, however, is significantly more challenging than in the two-party model. After much effort, a tight lower bound for k-party Set-Disjointness was nevertheless obtained in the classical setting: recent works [2], [25] were able to show a lower bound $\Omega(kn)$ for $\mathrm{DISJ}_{n,k}$, which is (trivially) tight.

In the quantum setting, Buhrman et al. [5] showed that the two-party quantum communication complexity of the Set-Disjointness function is $O(\sqrt{n} \log n)$, which gives a nearly quadratic improvement over the classical case. The logarithmic factor was then removed by Aaronson and Ambainis [1], who thus obtained an $O(\sqrt{n})$ upper bound. A matching lower bound $\Omega(\sqrt{n})$ was then proved by Razborov [24]. For k-party quantum communication complexity, an $O(k\sqrt{n} \log n)$ upper bound is easy to obtain from the two-party upper bound from [5].[*2] An important open problem, which is fundamental to understand the power of quantum distributed computing, is showing the tightness of this upper bound. In view of the difficulty in proving the $\Omega(kn)$ lower bound in the classical setting, proving a $\Omega(k\sqrt{n})$ lower bound in the quantum setting is expected to be challenging.

[*2] We showed (in Theorem 3 in Section 5) how to obtain an improved $O(k\sqrt{n})$ upper bound based on the protocol from [1].

1.2 Our contributions

1.2.1 Our model.

The main conceptual contribution of this paper is investigating quantum multiparty communication complexity in the setting where communication is *oblivious*. This requirement means that the communication pattern, and in particular the amount of communication exchanged between each pair of players at each round is fixed *independently of the input* before the execution of the protocol. This requirement is widely used in classical networking systems (e.g., [13], [19], [21]) and classical distributed algorithms (e.g., [7]), and to our knowledge is satisfied by all known quantum communication protocols that have been designed so far. It has also been considered in the quantum setting by Jain et al. [14], Result 3, who gave an $\Omega(n/r^2)$ bound on the quantum communication complexity of r-round k-party oblivious protocols for a promise version of Set-Disjointness.

1.2.2 Our results.

The main result of this paper holds for a class of functions which has a property that we call *two-party-reduction*. We say that a k-player function f_k has a two-party-reduction to a two-party function f_2 if the function f_2 can be "embedded" in f_k by embedding the inputs of f_2 in *any* position among the inputs of f_k. Many important functions such as any k-party symmetric function (including as important special cases the Set Disjointness function $\mathrm{DISJ}_{n,k}$ and the k-party inner product function) or the k-party equality function have this property. For a formal definition of the reduction property, we refer to Definition 2 in Section 3. Our main result is as follows.

Theorem 1 (informal) *Let f_k be a k-party function that has a two-party-reduction to a two-party function f_2. Then the oblivious k-party quantum communication complexity of f_k is at least k times the two-party quantum communication complexity of f_2.*

Theorem 1 enables us to prove strong lower bounds on

oblivious quantum k-party communication complexity using the quantum two-party communication complexity.[*3] This is useful since two-party quantum communication complexity is a much more investigated topic than k-party quantum communication complexity, and several tight bounds are known is this setting. For example, we show how to use Theorem 1 to analyze the oblivious quantum k-party communication complexity of $\mathrm{DISJ}_{n,k}$ and obtain a tight $\Omega(k\sqrt{n})$ bound:

Corollary 1. *The oblivious k-party quantum communication complexity of* $\mathrm{DISJ}_{n,k}$ *is* $\Omega(k\sqrt{n})$.

More generally, Theorem 1 enables us to derive tight bounds for the oblivious quantum k-party communication complexity of arbitrary symmetric functions. Since symmetric functions play an important role in communication complexity [8], [20], [24], [26], [31], our results might thus have broad applications. Additionally, we also give lower bounds for non-symmetric functions that have the two-party reduction property, such as the equality function. Our results are summarized in Table 1.

To complement our lower bounds, we show tight (up to possible polylogarithmic factors) upper bounds for these functions. The upper bounds are summarized in Table 1 as well. Note that if we apply our generic $O(k \log n \cdot G_n(f))$ bound to $\mathrm{DISJ}_{n,k}$, we only get the upper bound $O(k \log n \cdot \sqrt{n})$. We thus prove directly an optimal $O(k\sqrt{n})$ upper bound (Theorem 3) by showing how to adapt the optimal two-party protocol from [1] to the k-party setting.

2. Models of Quantum Communication

Notations: All logarithms are base 2 in this paper. We denote $[k] = \{1, \ldots, k\}$. For any set $\mathcal{X}$ and $k \geq 1$, $\mathcal{X}^k := \underbrace{\mathcal{X} \times \cdots \times \mathcal{X}}_{k}$.

Here we formally define the quantum multiparty communication model. As mentioned in Section 1.2, this communication model satisfies the oblivious routing condition, meaning that the number of (classical or quantum) bits used in communication at each round is predetermined (independent of inputs, private randomness, public randomness and outcome of quantum measurements). Since details of the model are important especially when proving lower bounds, we explain the model in detail below.

[*3] Note that in the two-party setting, the notions of oblivious communication complexity and non-oblivious communication complexity essentially coincide, since any non-oblivious communication protocol can be converted into an oblivious communication protocol by increasing the complexity by a factor at most two.

2.1 Quantum multiparty communication model

In k-party quantum communication model, at each round, players are allowed to send classical or quantum messages to all of the players but the number of (classical or quantum) bits used in communication is predetermined. Therefore for any k-player M-round protocol Π, we define the functions $C_{P_i \to P_j} : [M] \to \mathbb{N} \cup \{0\}$ $(i, j \in [k])$ which represent the number of bits $C_{P_i \to P_j}(m)$ transmitted at m-th round from i-th player to j-th player.

Procedure: Before the execution of the protocol, all players $P_1, \ldots, P_k$ share an entangled state or public randomness if needed. Each player P_i is then given an input. At each round $m \leq M$, every player P_i performs some operations onto P_i's register and send $C_{P_i \to P_1}(m)$ bits to the player P_1, $C_{P_i \to P_2}(m)$ bits to the player P_2, $\cdots$, and $C_{P_i \to P_k}(m)$ bits to the player P_k. All messages from all players are sent simultaneously. This continues until M-th round is finished. Finally, each player P_i output the answer based on the contents of P_i's register.

We define the communication cost of this protocol as

$$\mathrm{QCC}(\Pi) := \sum_{m \in [M]} \sum_{\substack{i,j \in [k] \\ i \neq j}} C_{P_i \to P_j}(m).$$

2.2 Protocol for computing a function

We define a protocol computing a function as follows.

Definition 1. *We say a protocol* Π *computes* $f : \mathcal{X}_1 \times \cdots \times \mathcal{X}_k \to \mathcal{Y}$ *with error* $\varepsilon \in [0, 1/2)$ *if for any* $i \in [k]$ *and any* $x = (x_1, \ldots, x_k) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_k$, $\Pr(\Pi^i_{\mathrm{out}}(x) \neq f(x)) \leq \varepsilon$ *holds where* $\Pi^i_{\mathrm{out}}(x)$ *denotes* P_i*'s output of the protocol on input* x.

We denote by $\mathcal{P}_k(f, \varepsilon)$ the set of k-party protocols computing a function f with error ε in the quantum multiparty communication model. The quantum communication complexity of function f with error ε in the model is defined as $\mathrm{QCC}(f, \varepsilon) := \min_{\Pi \in \mathcal{P}_k(f,\varepsilon)} \mathrm{QCC}(\Pi)$.

We also define the bounded round communication complexity of function f as $\mathrm{QCC}^M(f, \varepsilon) := \min_{\Pi \in \mathcal{P}^M_k(f,\varepsilon)} \mathrm{QCC}(\Pi)$ where we use the superscript M to denote the set of M-round protocols $\mathcal{P}^M_k(f, \varepsilon)$. Regarding the coordinator model, we define $\mathcal{P}_k(f, \varepsilon)_{\mathrm{Co}}, \mathrm{QCC}_{\mathrm{Co}}(f, \varepsilon), \mathcal{P}^M_k(f, \varepsilon)_{\mathrm{Co}}$, and $\mathrm{QCC}^M_{\mathrm{Co}}(f, \varepsilon)$ in similar manners as above.

Functions	2-party protocols		k-party oblivious protocols	
	Lower	Upper	Lower	Upper
Symmetric functions	$\Omega(G_n(f))$ in [24]	$O(\log n \cdot G_n(f))$ in [24]	$\Omega(k \cdot G_n(f))$ Proposition 3	$O(k \log n \cdot G_n(f))$ Theorem 4
Set-Disjointness	$\Omega(\sqrt{n})$ in [24]	$O(\sqrt{n})$ in [1]	$\Omega(k\sqrt{n})$ Corollary 1	$O(k\sqrt{n})$ Theorem 3
Set-Disjointness in M-round ($M \leq \sqrt{n}/2$)	$\tilde{\Omega}(n/M)$ in [3]	$O(n/M)$ (folklore)	$\tilde{\Omega}(k \cdot n/M)$ Proposition 5	$O(k \cdot n/M)$ Corollary 2
Equality function	$\Omega(1)$ (trivial)	$O(1)$ e.g., [16]	$\Omega(k)$ Proposition 4	$O(k)$ Proposition 6

表 1 Our results for oblivious quantum k-party communication complexity, along with known bounds for the two-party setting. For a symmetric function f, the notation $G_n(f)$ refers to the quantity defined in Equation (1).

2.3 Symmetric functions

A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is symmetric if there exists a function $D_f : [n] \cup \{0\} \to \{0,1\}$ such that $f(x,y) = D_f(|x \cap y|)$, where $x \cap y$ is the intersection of the two sets $x, y \subseteq [n]$ corresponding to the strings x, y. This means that the function f depends only on the Hamming weight of (the intersection of) the inputs. For any symmetric function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, let us write

$$G_n(f) = \sqrt{n l_0(D_f)} + l_1(D_f), \tag{1}$$

where

$$l_0(D_f) = \max_{1 \leq l \leq n/2} \{ l \,|D_f(l) \neq D_f(l-1)\},$$
$$l_1(D_f) = \max_{n/2 \leq l < n} \{ n - l \,|D_f(l) \neq D_f(l+1)\}.$$

Razborov [24] showed the lower bound $\Omega(G_n(f))$ on the quantum two-party communication complexity of any symmetric function f, and also obtained a nearly matching upper bound $O(G_n(f) \log n)$. We also note that for any function D_f, this function is constant on the interval $[l_0(D_f), n - l_1(D_f)]$ by the definitions of $l_0(D_f)$ and $l_1(D_f)$. We use this fact to prove a nearly matching upper bound on the oblivious quantum multiparty communication model.

Analogously, a k-party function $f : \{0,1\}^{n \cdot k} \to \{0,1\}$ is symmetric when represented as $f(x_1, \ldots, x_k) = D_f(|x_1 \cap \cdots \cap x_k|)$ using some function $D_f : [n] \cup \{0\} \to \{0,1\}$. The k-party n-bit Set-Disjointness function $\mathrm{DISJ}_{n,k}$ defined in Section 1 is a symmetric function. The k-party n-bit equality function $\mathrm{IP}_{n,k}$, defined for any $x_1, \ldots, x_k \in \{0,1\}^n$ as

$$\mathrm{IP}_{n,k}(x_1, \ldots, x_k) = (x_1[1] \wedge \cdots \wedge x_k[1]) \oplus \cdots \cdots \oplus (x_1[n] \wedge \cdots \wedge x_k[n])$$

is also symmetric. On the other hand, the k-party n-bit equality function $\mathrm{Equality}_{n,k}$, defined for any $x_1, \ldots, x_k \in \{0,1\}^n$ as

$$\mathrm{Equality}_{n,k}(x_1, \ldots, x_k) = \begin{cases} 1 & \text{if } x_1 = x_2 = \cdots = x_k, \\ 0 & \text{otherwise,} \end{cases}$$

is not symmetric.

3. Lower bounds

Here we show Proposition 1, which relates the communication complexity of a k-party function $f_k : \mathcal{X}^k \to \mathcal{Y}$ to the communication complexity of a two-party function $\tilde{f}_2 : \mathcal{X} \times \mathcal{X} \to \mathcal{Y}$ when f_2 is a *two-party-reduction* from $\tilde{f}_k$ in the following sense.

Definition 2. *A function $\tilde{f}_2 : \mathcal{X} \times \mathcal{X} \to \mathcal{Y}$ is a two-party-reduction from $f_k : \mathcal{X}^k \to \mathcal{Y}$ if for any $i \in [k]$, there is a map $x_{-i} : \mathcal{X} \to \mathcal{X}^{k-1}$ such that*

$$\forall x_1, x_2 \in \mathcal{X} \quad \tilde{f}_2(x_1, x_2) = f_k([x_{-i}(x_2), i, x_1])$$

holds, where $[y, i, x] := (y_1 \ldots, y_{i-1}, x, y_i, \ldots, y_{k-1})$ for $y = (y_i)_{i \leq k-1} \in \mathcal{X}^{k-1}$ and $x \in \mathcal{X}$.

For example, $\mathrm{DISJ}_{n,2}$ is a two-party-reduction from $\mathrm{DISJ}_{n,k}$ $(k \geq 2)$ because we can take $\mathcal{X} = \{0,1\}^n$, $\mathcal{Y} = \{0,1\}^n$ and $x_{-i}(x) = (x, 1^n, \ldots, 1^n)$.

Using this definition, we show the following proposition.

Proposition 1. *Let $f_k : \mathcal{X}^k \to \mathcal{Y}$ be a function and suppose $\tilde{f}_2 : \mathcal{X} \times \mathcal{X} \to \mathcal{Y}$ is a two-party-reduction of f_k. For any protocol $\Pi_k \in \mathcal{P}_k(f_k, \varepsilon)$, there is a two-party protocol $\tilde{\Pi} \in \mathcal{P}_2(\tilde{f}_2, \varepsilon)$ such that $\mathrm{QCC}(\tilde{\Pi}) \leq \frac{2\mathrm{QCC}(\Pi_k)}{k}$ holds.*

We also show a proposition which considers the bounded round setting.

Proposition 2. *Let f_k and $\tilde{f}_2$ be the same as in Proposition 1. For any protocol $\Pi_k \in \mathcal{P}_k^M(f_k, \varepsilon)$, there is a protocol $\tilde{\Pi} \in \mathcal{P}_2^M(\tilde{f}_2, \varepsilon)$ such that $\mathrm{QCC}(\tilde{\Pi}) \leq \frac{\mathrm{QCC}(\Pi_k)}{k}$ holds.*

Using Proposition 1, we next show the following theorem.

Theorem 1 (formal version)**.** *Let $f_{n,k} : \{0,1\}^{n \cdot k} \to \{0,1\}$ be a function and $\tilde{f}_n$ be a two-party-reduction of $f_{n,k}$. Then*

$$\forall n, k, \quad \mathrm{QCC}(f_{n,k}, \varepsilon) \geq \frac{k}{2} \cdot \mathrm{QCC}(\tilde{f}_n, \varepsilon).$$

We can also prove a similar proposition in the bounded round scenario using Proposition 2:

Theorem 2. *Let $f_{n,k}$ and $\tilde{f}_n$ be the same as Theorem 1. Then for any n, k, $\mathrm{QCC}^M(f_{n,k}, \varepsilon) \geq \frac{k}{2} \cdot \mathrm{QCC}^M(\tilde{f}_n, \varepsilon)$ holds.*

4. Applications

Here we investigate the lower bounds of some important functions such as Symmetric functions, Set-disjointness and Equality.

We first apply Theorem 1 to symmetric functions. Recall that any k-party symmetric function f can be represented as $f(x_1, \ldots, x_k) = D_f(|x_1 \cap \cdots \cap x_k|)$ (each player is given $x_i (1 \leq i \leq k)$ as input) using some function $D_f : [n] \cup \{0\} \to \{0,1\}$.

Proposition 3. *For any k-party n-bit symmetric function $f_{n,k}$, $\mathrm{QCC}(f_{n,k}, 1/3) \in \Omega\left(k\{\sqrt{nl_0(D_{f_{n,k}})} + l_1(D_{f_{n,k}})\}\right)$.*

Proof. For $i \in [k]$, define $x_{-i} : \{0,1\}^n \to \{0,1\}^{n \cdot (k-1)}$ as $x_{-i}(x) = (x, 1^n, \ldots, 1^n)$. Then we have that for any $i \in [k]$ and any $x_1, x_2 \in \{0,1\}^n$, $f_{n,2}(x_1, x_2) = f_{n,k}([x_{-i}(x_2), i, x_1])$. This implies $f_{n,2}$ is a two-party-reduction of $f_{n,k}$. Therefore, Theorem 1 yields $\mathrm{QCC}(f_{n,k}, 1/3) \in \Omega(k \cdot \mathrm{QCC}(f_{n,2}, 1/3))$. Applying the well known lower bound $\Omega(\sqrt{nl_0(D_{f_{n,2}})} + l_1(D_{f_{n,2}}))$ of the two-party function $f_{n,2}$ [24], we obtain $\mathrm{QCC}(f_{n,k}, 1/3) \in \Omega\left(k\{\sqrt{nl_0(D_{f_{n,k}})} + l_1(D_{f_{n,k}})\}\right)$. □

This lower bound is so strong that we get the optimal $\Omega(n \cdot k)$ bound for Inner-product function (as $l_0(D_{f_{n,k}}) = l_1(D_{f_{n,k}}) = \Theta(n)$ holds) and $\Omega(k\sqrt{n})$ lower bound for Set-disjointness function (as $l_0(D_{f_{n,k}}) = 1$ and $l_1(D_{f_{n,k}}) = 0$ holds), which turns out to be optimal in our setting as listed in Section 5.

Next, we examine the lower bound of Equality function.

Proposition 4. *For any k-party protocol for $\mathrm{Equality}_{n,k}$, $\mathrm{QCC}(\mathrm{Equality}_{n,k}, 1/3) \in \Omega(k)$.*

Proof. For $i \in [k]$, define $x_{-i} : \{0,1\}^n \to \{0,1\}^{n \cdot (k-1)}$ as $x_{-i}(x) = (x, x, \ldots, x)$ (i.e., making $k-1$ copies of x). Then we have that for any $i \in [k]$, any $x_1, x_2 \in \{0,1\}^n$, $\mathrm{Equality}_{n,2}(x_1, x_2) = \mathrm{Equality}_{n,k}([x_{-i}(x_2), i, x_1])$. Therefore by Theorem 1, the trivial lower bound $\Omega(1)$ of two-party n-bit Equality function yields $\mathrm{QCC}(\mathrm{Equality}_{n,k}, 1/3) \in \Omega(k)$. □

We also prove a lower bound in bounded round scenario using Theorem 2.

Proposition 5. $\mathrm{QCC}^M(\mathrm{DISJ}_{n,k}, 1/3) \in \Omega\left(\frac{n \cdot k}{M \log^8 M}\right)$.

Proof. Using $\Omega\left(n/(M \log^8 M)\right)$ lower bound of two-party M-round Set-disjointness function [3], we obtain $\mathrm{QCC}^M(\mathrm{DISJ}_{n,k}, 1/3) \in \Omega\left(n \cdot k/(M \log^8 M)\right)$ which is nearly tight as listed in Section 5. □

5. Matching upper bounds

In this section, we list the upper bound $O(k\sqrt{n})$ for $\mathrm{DISJ}_{n,k}$, the upper bound $O(k \log n(\sqrt{nl_0(D_f)} + l_1(D_f)))$ for symmetric functions and the upper bound $O(k \log n)$ for $\mathrm{Equality}_{n,k}$. Without being noted explicitly, all of the optimal protocols satisfy the oblivious routing condition. These are (sometimes nearly) matching upper bounds since we have the same lower bounds in Section 4.

5.1 Optimal protocol for $\mathrm{DISJ}_{n,k}$

Adopting the arguments from [1], Section 7, which gives a two-party protocol for DISJ with $O(\sqrt{n})$-communication cost, we obtain the protocol with $O(k \cdot \sqrt{n})$ cost. This gives the following theorem.

Theorem 3. $\mathrm{QCC}(\mathrm{DISJ}_{n,k}, 1/3) \in O(k\sqrt{n})$.

Using the protocol used in Theorem 3, we can create M-round protocol for $\mathrm{DISJ}_{n,k}$ with $O(n \cdot k/M)$ communication cost when $M \leq \sqrt{n}$. The important fact here is that in the protocol with $O(k\sqrt{n})$ cost, the coordinator and players interact only for $O(\sqrt{n})$ rounds. To create the desired protocol, let us now divide the input $x \in \{0,1\}^n$ into n/M^2 sub-inputs, each contains M^2 elements. We next apply the above protocol *in parallel* with the n/M^2 sub-inputs where each of sub-inputs uses $O(M)$ rounds and $O(kM)$ communication. The

new protocol still uses $O(M)$ rounds although the communication cost grows up to $\frac{n}{M^2}O(kM) = O(n \cdot k/M)$. The success probability is still the same since the original protocol is a one-sided error protocol.

Therefore, this protocol has M-round and the communication cost $O(n \cdot k/M)$ which nearly matches the lower bound $\Omega\left(n \cdot k/(M \log^8 M)\right)$ described in Section 4. Therefore we obtain the following corollary:

Corollary 2. $\mathrm{QCC}^M(\mathrm{DISJ}_{n,k}, 1/3) \in O(n \cdot k/M)$ *when* $M \leq \sqrt{n}$.

5.2 Symmetric functions

The following theorem is shown by generalizing Section 4 of [24] which investigates only the two-player setting.

Theorem 4. *For any k-party n-bit symmetric function $f_{n,k}$,*

$$\mathrm{QCC}(f_{n,k}, 1/3) \in O\left(k \log n \{\sqrt{n l_0(D_{f_{n,k}})} + l_1(D_{f_{n,k}})\}\right).$$

5.3 Optimal protocol for $\mathrm{Equality}_{n,k}$

By a standard argument of hash functions (see, e.g., [16]), we obtain the following proposition.

Proposition 6. $\mathrm{QCC}(\mathrm{Equality}_{n,k}, 1/3) \in O(k)$.

6. Acknowledgements

FLG was partially supported by JSPS KAKENHI grants Nos. JP16H01705, JP19H04066, JP20H00579, JP20H04139 and by MEXT Q-LEAP grants Nos. JPMXS0118067394 and JPMXS0120319794. DS would like to take this opportunity to thank the "Nagoya University Interdisciplinary Frontier Fellowship" supported by JST and Nagoya University.

参考文献

[1] Aaronson, S. and Ambainis, A.: Quantum search of spatial regions, *44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 200–209 , (2003).

[2] Braverman, M., Ellen, F., Oshman, R., Pitassi, T. and Vaikuntanathan, V.: A tight bound for set disjointness in the message-passing model, *54th Annual Symposium on Foundations of Computer Science*, pp. 668–677, (2013).

[3] Braverman, M., Garg, A., Ko, Y. K., Mao, J. and Touchette, D.: Near-optimal bounds on the bounded-round quantum communication complexity of disjointness, *SIAM Journal on Computing*, Vol. 47, No. 6, pp. 2277–2314, (2018).

[4] Buhrman, H., Cleve, R., Watrous, J. and de Wolf, R.: Quantum Fingerprinting, *Phys. Rev. Lett.*, Vol. 87, p. 167902, (2001).

[5] Buhrman, H., Cleve, R. and Wigderson, A.: Quantum vs. classical communication and computation, *30th annual ACM symposium on Theory of computing*, pp. 63–68, (1998).

[6] Buhrman, H., van Dam, W., Høyer, P. and Tapp, A.: Multiparty quantum communication complexity, *Phys. Rev. A*, Vol. 60, pp. 2737–2741 , (1999).

[7] Censor-Hillel, K., Kaski, P., Korhonen, J. H., Lenzen, C., Paz, A. and Suomela, J.: Algebraic methods in the congested clique, *Distributed Computing*, Vol. 32, No. 6, pp. 461–478, (2019).

[8] Chakraborty, S., Chattopadhyay, A., Høyer, P., Mande, N. S., Paraashar, M. and de Wolf, R.: Symmetry and Quantum Query-To-Communication Simulation, *39th International Symposium on Theoretical Aspects of Computer Science*, Vol. 219, pp. 20:1–20:23, (2022).

[9] Chattopadhyay, A. and Pitassi, T.: SIGACT News Complexity Theory Column 67, *SIGACT News*, Vol. 41, No. 3, p. 58, (2010).

[10] Cleve, R. and Buhrman, H.: Substituting quantum entanglement for communication, *Phys. Rev. A*, Vol. 56, No. 2, p. 1201, (1997).

[11] Cleve, R., Dam, W. v., Nielsen, M. and Tapp, A.: Quantum Entanglement and the Communication Complexity of the Inner Product Function, *Selected Papers from the First NASA International Conference on Quantum Computing and Quantum Communications*, QCQC '98, Berlin, Heidelberg, Springer-Verlag, pp. 61–74 , (1998).

[12] Drucker, A., Kuhn, F. and Oshman, R.: The Communication Complexity of Distributed Task Allocation, *ACM Symposium on Principles of Distributed Computing*, PODC '12, pp. 67–76, (2012).

[13] Fiat, A. and Woeginger, G. J.(eds.): *Online algorithms: The state of the art*, Lecture Notes in Computer Science, Vol. 1442, Springer (1998).

[14] Jain, R., Radhakrishnan, J. and Sen, P.: A lower bound for the bounded round quantum communication complexity of set disjointness, *44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 220–229, (2003).

[15] Kalyanasundaram, B. and Schintger, G.: The probabilistic communication complexity of set intersection, *SIAM Journal on Discrete Mathematics*, Vol. 5, No. 4, pp. 545–557, (1992).

[16] Kushilevitz, E. and Nisan, N.: *Communication Complexity*, Cambridge University Press (1996).

[17] Le Gall, F. and Nakajima, S.: Multiparty quantum communication complexity of triangle finding, *12th Conference on the Theory of Quantum Computation, Communication and Cryptography*,, (2018).

[18] Lee, T., Schechtman, G. and Shraibman, A.: Lower bounds on quantum multiparty communication complexity, *24th Annual IEEE Conference on Computational Complexity*, pp. 254–262, (2009).

[19] Ni, L. M. and McKinley, P. K.: A survey of wormhole routing techniques in direct networks, *Computer*, Vol. 26, No. 2, pp. 62–76, (1993).

[20] Paturi, R.: On the degree of polynomials that approximate symmetric boolean functions (preliminary version), *24th annual ACM symposium on Theory of computing*, pp. 468–474, (1992).

[21] Räcke, H. and Schmid, S.: Compact Oblivious Routing, *27th Annual European Symposium on Algorithms*, Vol. 144, pp. 75:1–75:14, (2019).

[22] Rao, A. and Yehudayoff, A.: *Communication Complexity: and Applications* (2020).
[23] Razborov, A. A.: On the distributional complexity of disjointness, *Theoretical Computer Science*, Vol. 106, No. 2, pp. 385–390, (1992).
[24] Razborov, A. A.: Quantum communication complexity of symmetric predicates, *Izvestiya: Mathematics*, Vol. 67, No. 1, p. 145, (2003).
[25] Rosén, A. and Urrutia, F.: A New Approach to Multi-Party Peer-to-Peer Communication Complexity, *10th Innovations in Theoretical Computer Science*, Vol. 124, pp. 64:1–64:19, (2018).
[26] Sherstov, A. A.: The Pattern Matrix Method, *SIAM Journal on Computing*, Vol. 40, No. 6, pp. 1969–2000, (2011).
[27] Tani, S., Nakanishi, M. and Yamashita, S.: Multiparty quantum communication complexity with routed messages, *IEICE transactions on information and systems*, Vol. 92, No. 2, pp. 191–199, (2009).
[28] Touchette, D.: Quantum Information Complexity, *47th Annual ACM Symposium on Theory of Computing*, STOC '15, New York, NY, USA, Association for Computing Machinery, pp. 317–326, (2015).
[29] Yao, A. C.-C.: Quantum circuit complexity, *34th Annual Foundations of Computer Science*, pp. 352–361, (1993).
[30] Yao, A. C.-C.: Some Complexity Questions Related to Distributive Computing(Preliminary Report), *11th Annual ACM Symposium on Theory of Computing*, pp. 209–213, (1979).
[31] Zhang, Z. and Shi, Y.: Communication complexities of symmetric XOR functions, *Quantum Information & Computation*, Vol. 9, No. 3, pp. 255–263 , (2009).