Electronic Colloquium on Computational Complexity, Report No. 44 (2013)

Shared Randomness and Quantum Communication in the Multi-Party Model

Dmitry Gavinsky[*] Tsuyoshi Ito[*] Guoming Wang[*†]

Abstract

We study shared randomness in the context of multi-party number-in-hand communication protocols in the simultaneous message passing model. We show that with three or more players, shared randomness exhibits new interesting properties that have no direct analogues in the two-party case.

First, we demonstrate a hierarchy of modes of shared randomness, with the usual shared randomness where all parties access the same random string as the strongest form in the hierarchy. We show exponential separations between its levels, and some of our bounds may be of independent interest. For example, we show that the equality function can be solved by a protocol of constant length using the weakest form of shared randomness, which we call *XOR-shared randomness.*

Second, we show that quantum communication cannot replace shared randomness in the k-party case, where $k \geq 3$ is any constant. We demonstrate a promise function $\mathcal{GP}_k$ that can be computed by a classical protocol of constant length when (the strongest form of) shared randomness is available, but any quantum protocol without shared randomness must send $n^{\Omega(1)}$ qubits to compute it. Moreover, the quantum complexity of $\mathcal{GP}_k$ remains $n^{\Omega(1)}$ even if the "second strongest" mode of shared randomness is available. While a somewhat similar separation was already known in the two-party case, in the multi-party case our statement is qualitatively stronger:

- In the two-party case, only a relational communication problem with similar properties is known.
- In the two-party case, the gap between the two complexities of a problem can be at most exponential, as it is known that $2^{O(c)} \log n$ qubits can always replace shared randomness in any c-bit protocol. Our bounds imply that with quantum communication alone, in general, it is not possible to simulate efficiently even a three-bit three-party classical protocol that uses shared randomness.

1 Introduction

The area of communication complexity deals with the amount of communication required for solving computational problems with distributed input. In the two-party *simultaneous message passing (SMP)* setting of communication complexity, two *players* Alice and Bob receive inputs x and y, respectively, and each sends a message to a third party, the *referee.* Using those messages, the referee computes the output value. When the goal is to compute certain function f, the

[*] NEC Laboratories America, Inc., Princeton, NJ, USA.

[†] Computer Science Division, University of California, Berkeley, Berkeley, CA, USA.

ISSN 1433-8092

success is measured by the probability that the output value of a *communication protocol* equals $f(x, y)$. The *cost* of a communication protocol is the total number of bits sent by the players to the referee.

Shared randomness is a crucial resource in communication complexity. When Alice and Bob have it, they can use a mixed strategy in order to compute f; in particular, the minimax principle implies that the worst-case and the average-case complexities are equal in this case. It is known that without shared randomness the model becomes considerably weaker, and the gap between the worst-case and the average-case complexities of a communication problem can be arbitrary large (constant vs. $\Omega(\sqrt{n})$ in the case of the equality function, as shown by Newman and Szegedy [NS96]).

The SMP model of communication is the weakest among those that have been studied widely. Nevertheless, it is arguably the right model to look at when the goal is to investigate shared randomness. That is because whenever communication between the players is possible (which is the case for all other commonly studied models, but not for SMP), the first player can append $O(\log n)$ bits of *private* randomness to the first message that is sent to the others, and that would not affect the cost of the protocol significantly, as poly-logarithmic cost is usually viewed as efficient. Those random bits are now known to all the participants, and can be used in place of shared randomness. It is known due to Newman [New91] that $O(\log n)$ bits of shared randomness are always enough; therefore, shared randomness does not make much difference in any model that allows direct communication between the players.

In this paper we study shared randomness in the context of the *multi-party version* of the SMP model, where the number of players k is three or larger (the referee is not counted as a player), the input has k fragments and each fragment is known to exactly one player—this regime of distributing input between the players is usually called "number in hand." This model can be viewed as a natural generalization of the two-party model.

We demonstrate several interesting (and somewhat surprising) properties of shared randomness when the number of players is at least three, that have no direct analogues in the two-party case.

1.1 Previous work

In [Yao03], Yao generalized the technique of *quantum fingerprints* [BCWdW01] to show that every classical two-party SMP protocol that uses shared randomness and sends c bits can be simulated by a quantum protocol without shared randomness that sends $2^{O(c)} \log n$ qubits. This naturally raised the question whether quantum communication can always replace shared randomness—that is, whether any communication problem that can be solved by a classical SMP protocol of poly-logarithmic length using shared randomness can also be solved by a quantum protocol of poly-logarithmic length without shared randomness.

The question was addressed by Gavinsky, Kempe, Regev and de Wolf in [GKRdW06], where they demonstrated a two-party *relational* communication problem that can be solved by a classical protocol of cost $O(\log n)$ that uses shared randomness, but requires $n^{\Omega(1)}$ qubits in order to be solved by a quantum protocol without shared randomness. In the same work a question was posed whether a similar separation is possible via a *functional* problem.

2 Our results

Two main results of this work are the following.

First, we establish a hierarchy of modes of shared randomness (Section 4). In the k-party SMP model, we consider *t-shared randomness* for $2 \leq t \leq k$, where every set of t players shares a random string. The k-shared randomness is the usual, unrestricted shared randomness and the strongest mode in the hierarchy, and a smaller value of t gives a weaker form of shared randomness. The $(k-1)$-shared randomness could be also called "randomness on the forehead." Below 2-shared randomness, we also consider an even more restricted mode of shared randomness which we call *XOR-shared randomness*, where the k players receive uniformly random k-tuples of bits whose parity is 0. The precise definitions of these modes of shared randomness will be given in Section 4. We will show that this is a proper hierarchy; i.e., we show exponential separations between its levels.

One of the problems that we study in this context is the multi-party equality function, and we show (Claim 4.1) that it can be solved by a protocol of constant length that uses XOR-shared randomness. We believe that this result might be of independent interest, due to the importance of the equality function.

Second, we demonstrate a promise function whose classical communication complexity is constant if the strongest form of shared randomness is available, but whose quantum communication complexity is $n^{\Omega(1)}$ if no shared randomness is available (Section 5). Moreover, the quantum complexity remains $n^{\Omega(1)}$ even if the protocol can use $(k-1)$-shared randomness (randomness on the forehead).

Our second result is closely related to [GKRdW06]: We demonstrate a *promise function* that can be solved efficiently in the classical model with shared randomness, but not in the quantum model without it. This answers the main open problem posed in [GKRdW06] for the case of three or more players. We note that the question remains wide open in the two-player case.

Our second result is also related to the aforementioned work by Yao [Yao03], where it was shown, informally speaking, that shared randomness can be replaced by quantum communication with (at most) exponential overhead. In this work we demonstrate a (functional) communication problem that can be solved by a three-bit three-party classical protocol with shared randomness but requires $n^{\Omega(1)}$ qubits without shared randomness (or even with randomness on the forehead). Accordingly, the possibility to simulate shared randomness by quantum communication is a unique feature of the two-party model; with more than two players, the possible advantage of shared randomness over quantum communication is not bounded by any function.

2.1 Technical statements

In the first part, we prove the following.

Theorem 2.1. *Let $k \geq 3$. Then,*

- *For each $t \in \{3, \ldots, k\}$, there exists a k-party promise function that can be solved by a protocol of cost t in the SMP model with classical communication and t-shared randomness but requires $\Omega(tn^{1/t})$ qubits in the SMP model with quantum communication and $(t-1)$-shared randomness.*

- *There exists a k-party total function that can be solved by a protocol of constant cost in the classical SMP model with 2-shared randomness but requires $\Omega(\sqrt{n})$ bits of communication in the classical SMP model with XOR-shared randomness.*
- *There exists a k-party total function that can be solved by a protocol of constant cost in the classical SMP model with XOR-shared randomness but requires $\Omega(\sqrt{n})$ bits of communication in the classical SMP model without shared randomness.*

In the second part of this work, we study the following natural communication problem. For a bit string x, we denote by $|x|$ its Hamming weight, i.e. the number of 1s in x.

Definition 1 (Gap-Parity)**.** Let $x_1, \ldots, x_k$ be n-bit strings such that $|x_1 \oplus \cdots \oplus x_k| \notin [n/3, 2n/3]$. Then we define $\mathcal{GP}_k(x_1, \ldots, x_k) = 0$ if $|x_1 \oplus \cdots \oplus x_k| < n/2$ and $\mathcal{GP}_k(x_1, \ldots, x_k) = 1$ otherwise.

Note that in the SMP model with classical communication and shared randomness, $\mathcal{GP}_k$ has a trivial solution, where each player sends only one bit to the referee.

We will demonstrate that for $k \geq 3$, $\mathcal{GP}_k$ cannot be solved efficiently by a quantum protocol without shared randomness. Moreover, we show that the Gap-Parity problem has no efficient solution with quantum communication even with randomness on the forehead (cf. Section 4).

Theorem 2.2. *Let $k \geq 3$. Using shared randomness, the k-party promise function $\mathcal{GP}_k$ can be solved by a classical SMP protocol of cost k where each player sends a bit. For $2 \leq t \leq k-1$, in the SMP model with quantum communication with t-shared randomness, the complexity of $\mathcal{GP}_k$ is $\Omega(kn^{1-t/k})$. In particular, in the SMP model with quantum communication without shared randomness, the complexity of $\mathcal{GP}_k$ is $\Omega(kn^{1-2/k})$.*

3 Preliminaries

For any n-dimensional vector v, we will write $v(j)$ to denote its jth coordinate, and for any $S \subseteq [n]$ we will use v_S to denote the restriction of v to the coordinates that are elements of S. We use $\bar{0}$ or $\bar{1}$ to denote the vectors of all 0s or all 1s, respectively, when its length is clear from the context.

For any finite set W, let $\mathcal{U}(W)$ denote the uniform distribution over the elements of W.

3.1 Quantum measurements

Unless stated otherwise, we will represent quantum states by their density matrices. We will write $\mathbf{E}_i[\sigma_i]$ or even $\mathbf{E}[\sigma_i]$ to denote the mixed state $(1/k)\sum_i \sigma_i$.

Given a matrix M, we denote by $\|M\|_1$ the *trace norm* of M, defined as the sum of the singular values of M. It is known that given two quantum states σ_0 and σ_1, the optimal probability with which a quantum measurement can correctly distinguish between σ_0 and σ_1 equals $1/2 + \|\sigma_0 - \sigma_1\|_1/4$.

We will use the following special case of the "random access code argument" [GKRdW06, Lemma 2.2], which is a slight generalization of [Nay99, Theorem 2.3] (see also [ANTSV02]).

Claim 3.1. *Let $X \sim \mathcal{U}(\{0,1\}^n)$. Suppose for each instantiation $X = x$ we have a quantum state ρ_x of q qubits. Let σ_a^j be the expectation of ρ_X conditional upon $X(j) = a$, for $j \in [n]$ and $a \in \{0,1\}$. Then $\sum_{j=1}^n \|\sigma_0^j - \sigma_1^j\|_1^2 \in O(q)$.*

Proof. Let $h(p)$ be the binary entropy function: $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$. Lemma 2.2 of [GKRdW06] implies that under the assumption of the claim, it holds that $\sum_{j=1}^{n}\big(1 - h(1/2 - \|\sigma_0^j - \sigma_1^j\|_1/4)\big) \leq q$. The claim follows because $1 - h(1/2 - x/4) \geq x^2/(8\ln 2)$ for $0 \leq x \leq 2$. □

Now let us consider the situation where a quantum measurement is performed in order to predict the parity of several independent binary variables.

Claim 3.2. *For every $i \in [m]$, let σ_0^i and σ_1^i be quantum states of equal dimension. For $a \in \{0,1\}$, let $\rho_a \overset{def}{=} \mathbf{E}_{\alpha_1\oplus\cdots\oplus\alpha_m=a}[\sigma_{\alpha_1}^1 \otimes \cdots \otimes \sigma_{\alpha_m}^m]$. Then $\|\rho_0 - \rho_1\|_1 = (1/2^{m-1})\prod_{i=1}^{m}\|\sigma_0^i - \sigma_1^i\|_1$.*

Proof. Write:

$$\rho_0 - \rho_1 = \frac{1}{2^{m-1}}(\sigma_0^1 - \sigma_1^1) \otimes \cdots \otimes (\sigma_0^m - \sigma_1^m),$$

and the claim follows from the fact that the trace norm is multiplicative with respect to the tensor product. □

3.2 Communication complexity

In this work we are interested in the following model of communication complexity.

Definition 2 (Multi-party SMP)**.** The k-party simultaneous message passing (SMP) model involves $k+1$ parties: k players $\mathcal{A}_1, \ldots, \mathcal{A}_k$ and a referee. For every $i \in [k]$, player $\mathcal{A}_i$ gets input x_i. They each send one message to the referee, who uses the content of all k messages to compute the output value.

A communication protocol describes the action of each participant. The *cost* or *complexity* of a protocol is the total length of the messages sent by players $A_1, \ldots, A_k$ to the referee. We say that a protocol solves a computational problem defined over k input values if the referee gives a correct answer with probability at least $2/3$ for each possible input.

In this paper we will consider several further modifications of the SMP model:

- In the *quantum* SMP model, the players $\mathcal{A}_1, \ldots, \mathcal{A}_k$ are allowed to send quantum messages, and the referee can perform any quantum measurement in order to determine the output value.

- In the SMP model *with shared randomness*, the players $\mathcal{A}_1, \ldots, \mathcal{A}_k$ have free access to the same string of random bits that were chosen independently from the input values.

- In Section 4, we will define a *hierarchy of modes of shared randomness* in multi-party protocols (where the strongest mode is the standard one, as described above). We demonstrate exponential separations between the levels of the hierarchy (i.e., the hierarchy is proper).

We call a communication protocol *efficient* if its cost is poly-logarithmic in the length of input.

3.3 Read-k families of functions

Let us consider the following model of dependence among random variables.

Definition 3 (Read-k families)**.** Let $X_1, \ldots, X_m$ be independent random variables. For $j \in [r]$, let $P_j \subseteq [m]$ and let f_j be a Boolean function of $(X_i)_{i \in P_j}$. If every $i \in [m]$ belongs to at most k among the r sets $P_1, \ldots, P_r$, then the random variables $Y_j = f_j((X_i)_{i \in P_j})$ are called a *read-k family.*

The following lemma is due to Finner [Fin92].

Lemma 3.3 (Finner [Fin92])**.** *Let $Y_1, \ldots, Y_n$ be a read-k family of random variables taking non-negative values. Then*

$$\mathbf{E}\left[\prod_{i=1}^{n} Y_i\right] \leq \prod_{i=1}^{n} \sqrt[k]{\mathbf{E}[Y_i^k]}.$$

Note that the generalized Hölder inequality implies that $\mathbf{E}[\prod Y_i] \leq \prod \sqrt[n]{\mathbf{E}[Y_i^n]}$ in general, without making any independence assumption. This corresponds to choosing $k = n$ in the lemma. On the other hand, when $k = 1$ (i.e., $Y_1, \ldots, Y_n$ are mutually independent), the expectation of their product equals the product of their expectations. Accordingly, Lemma 3.3 gives a natural interpolation between these two extreme cases.

4 Hierarchy of shared randomness in multi-party protocols

When there are more than two players, it is possible to give the players access to shared randomness in several different ways.

Most naturally, the parties may have free access to the same string of random bits—we call this mode *unrestricted shared randomness.* Note that this mode of shared randomness is often implicitly assumed to be available to the players; for example, unrestricted shared randomness is required in order to be able to use *mixed strategies*, and therefore applicability of the minimax principle in multi-party communication depends on it.

Let $k \geq 2$ be the number of players. For every $t \in \{2, \ldots, k\}$, we can define the mode of *t-shared randomness*, where every t players share their own string of random bits. The k-shared randomness is the same thing as the unrestricted shared randomness. Sometimes we will refer to the $(k-1)$-shared mode as *randomness on the forehead.*

We will also consider *XOR-shared randomness*, where every player $\mathcal{A}_i$ is given access to an arbitrarily long random string r_i, such that every $(k-1)$ strings r_i are uniform and mutually independent but the bitwise XOR of $r_1, \ldots, r_k$ is 0 everywhere.

If we consider the case of $k = 2$, we can see that XOR-shared and 2-shared modes are the same. For $k = 3$, we already have three modes of shared randomness: XOR-shared, 2-shared and 3-shared. We will see below that these three modes offer different computational power.

In general, t-shared randomness is always at least as strong as $(t-1)$-shared randomness, as the latter can always be emulated using the former. Also, XOR-shared randomness can be emulated in the 2-shared mode; to do that, let r_i equal the bit-wise XOR of the random string shared between $\mathcal{A}_{i-1}$ and $\mathcal{A}_i$ and the random string shared between $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$, where the subscripts are interpreted modulo k. Now the strings $r_1, \ldots, r_k$ are distributed as required by the definition of XOR-shared mode.

One interesting example that demonstrates usefulness of XOR-shared randomness when $k \geq 3$ is the *multi-party equality function*; that is, the total Boolean function of k arguments $x_1, \ldots, x_k$ that takes value 1 if and only if $x_1 = x_2 = \cdots = x_k$.

Claim 4.1. *For any $c \in \mathbb{N}$, there exists a classical protocol for the k-party equality function, where XOR-shared randomness is used, each player sends c bits to the referee, and the following holds:*

- *If $x_1 = x_2 = \cdots = x_k$, then the referee's answer is always 1;*
- *otherwise, the referee's answer is 0 with probability $1 - 1/2^c$.*

Proof. For $r, x \in \{0,1\}^n$, let $r \cdot x$ be the inner product of r and x in finite field GF(2): $r \cdot x \overset{\text{def}}{=} \bigoplus_{i:r(i)=1} x(i)$. Consider the following protocol $\mathcal{P}$, where the players use XOR-shared randomness and each of them sends a single bit to the referee:

1. For all $i \in [k]$, the ith player uses his random string $r_i \in \{0,1\}^n$ and computes $m_i \overset{\text{def}}{=} r_i \cdot x_i$, then sends m_i to the referee.
2. The referee outputs $\neg(m_1 \oplus \cdots \oplus m_k)$.

By the definition of XOR-shared randomness, we have that $r_1 \oplus \cdots \oplus r_k = \bar{0}$. Therefore $(r_1 \oplus \cdots \oplus r_k) \cdot x_k = 0$, and we can write

$$\begin{aligned} & m_1 \oplus \cdots \oplus m_k \\ & = r_1 \cdot x_1 \oplus \cdots \oplus r_k \cdot x_k \\ & = r_1 \cdot x_1 \oplus \cdots \oplus r_k \cdot x_k \oplus (r_1 \oplus \cdots \oplus r_k) \cdot x_k \\ & = r_1 \cdot (x_1 \oplus x_k) \oplus \cdots \oplus r_{k-1} \cdot (x_{k-1} \oplus x_k). \end{aligned} \tag{1}$$

Note that $r_1, \ldots, r_{k-1}$ is a uniformly random $(k-1)$-tuple of n-bit strings, and therefore the rightmost part of (1) equals 1 with probability exactly 1/2 if at least one of the $k-1$ values $x_1 \oplus x_k, \ldots, x_{k-1} \oplus x_k$ is different from $\bar{0}$. If, on the other hand, $x_1 = x_2 = \cdots = x_k$ then(1) equals 0 with certainty.

Accordingly, $\mathcal{P}$ outputs "1" whenever $x_1 = x_2 = \cdots = x_k$, and otherwise it outputs "0" with probability 1/2. To get a protocol as promised by our claim, we can run c independent instances of $\mathcal{P}$ in parallel and output "1" if and only if all c instances answered "1". □

We are now prepared to prove that the modes of shared randomness form a proper hierarchy when $k \geq 3$.

Theorem 2.1. Let $k \geq 3$. Then,

- *For each $t \in \{3, \ldots, k\}$, there exists a k-party promise function that can be solved by a protocol of cost t in the SMP model with classical communication and t-shared randomness but requires $\Omega(tn^{1/t})$ qubits in the SMP model with quantum communication and $(t-1)$-shared randomness.*

- *There exists a k-party total function that can be solved by a protocol of constant cost in the classical SMP model with 2-shared randomness but requires $\Omega(\sqrt{n})$ bits of communication in the classical SMP model with XOR-shared randomness.*

- *There exists a k-party total function that can be solved by a protocol of constant cost in the classical SMP model with XOR-shared randomness but requires $\Omega(\sqrt{n})$ bits of communication in the classical SMP model without shared randomness.*

Proof. To prove the first part of the theorem, consider the t-party problem $\mathcal{GP}_t$, letting the players $\mathcal{A}_1, \dots, \mathcal{A}_t$ receive the corresponding fragments of input. (The other $(k-t)$ players do not receive any input.) Theorem 2.2, which will be proved in the next section, implies the result in this case.

The second part follows from considering the two-party equality problem, when the input is distributed between $\mathcal{A}_1$ and $\mathcal{A}_2$ and the other players do not receive any input. It is clear that this problem can be solved with constant cost in the classical SMP model with 2-shared randomness. Now suppose that there exists a protocol of cost c in the classical SMP model with XOR-shared randomness, and we will prove that $c = \Omega(\sqrt{n})$. Note that in this model, the random strings given to $\mathcal{A}_1$ and $\mathcal{A}_2$ are uniform and independent, although they are correlated with the random strings given to the other players. Such a protocol can be transformed without changing the cost to a protocol in the two-party classical SMP model where the two players do not share randomness but each player shares randomness with the referee, because in the latter model, the referee can generate all the messages which would have been generated by players $\mathcal{A}_3, \dots, \mathcal{A}_k$. By the same technique used by Newman [New91], this protocol can be further transformed to a protocol of cost $O(c + \log n)$ in the two-party classical SMP model without shared randomness at all. It was shown by Newman and Szegedy [NS96] that the communication complexity of the equality problem in this model is $\Omega(\sqrt{n})$, and therefore c must be $\Omega(\sqrt{n})$.

The third part follows from considering the k-party equality function. The upper bound is shown in Claim 4.1. The lower bound follows from Newman and Szegedy [NS96], because any k-party SMP protocol without shared randomness among $\mathcal{A}_1, \dots, \mathcal{A}_k$ for the k-party equality function can be used to construct a two-party SMP protocol without shared randomness between two players $\mathcal{A}'_1$ and $\mathcal{A}'_2$ for the two-party equality function without affecting its cost: $\mathcal{A}'_1$ simulates $\mathcal{A}_1$, and $\mathcal{A}'_2$ simulates $\mathcal{A}_2, \dots, \mathcal{A}_k$. □

Remark 1. Besides its own elegance, the hierarchy of shared randomness is a useful technical tool. For our lower bound proof for the quantum complexity of $\mathcal{GP}_k$ (which is the main technical result of Section 5), we need different modes of shared randomness. Informally speaking, we use a hybrid argument that puts certain restrictions on the input values, and those restrictions inevitably create shared randomness of certain type that becomes available to the players. We show that the sort of randomness that is introduced corresponds to one of the restricted modes of shared randomness, whose availability does not make the communication problem easy for quantum communication.

5 Shared randomness vs. quantum communication

In this section, we will analyze the complexity of $\mathcal{GP}_k$ to compare the resource of shared randomness to that of quantum communication in multi-party protocols.

Fix $k \geq 3$. Recall that in the classical SMP model with shared randomness $\mathcal{GP}_k$ has a trivial solution, where each player sends one bit to the referee.

As a warm-up, consider the case of quantum protocols *without shared randomness.*[1] Let $\mathcal{P}$ be a quantum protocol that communicates c qubits and solves $\mathcal{GP}_k$, and let $\mathcal{U}_k$ be the uniform distribution over k-tuples $(x_1, \ldots, x_k) \in \{0,1\}^{n \times k}$. Now consider the behavior of $\mathcal{P}$ when the input is distributed according to $\mathcal{U}_k$ (note that such input is almost never valid for $\mathcal{GP}_k$).

For $i \in [k]$, let σ_i be a density matrix representing the (mixed) state that the referee receives from $\mathcal{A}_i$ when the input distribution is $\mathcal{U}_k$. Since the senders share no randomness and $\mathcal{U}_k$ is a product distribution, the state of the referee before his measurement is performed can be written as $\sigma_1 \otimes \cdots \otimes \sigma_k$.

For $i \in [k]$, let X_i be an n-bit random string taking the value of input x_i. By Claim 3.1, there exists $j_0 \in [n]$ such that $\sum_{i=1}^{k} \|\sigma_0^i - \sigma_1^i\|_1^2 \in O(c/n)$, where σ_a^i is the message from $\mathcal{A}_i$, conditional upon $X_i(j_0) = a$.

Since the random variables $X_1(j_0), \ldots, X_k(j_0)$ are mutually independent and each $X_i(j_0)$ can be correlated only with σ_i, Claim 3.2 implies that the referee can predict $X_1(j_0) \oplus \cdots \oplus X_k(j_0)$ with probability at most $1/2 + (1/2^{k+1}) \prod_{i=1}^{k} \|\sigma_0^i - \sigma_1^i\|_1$, which is at most $1/2 + O(c/(kn))^{k/2}$ by the inequality of arithmetic and geometric means.

Note that this guarantees that the "advantage over random guess" that the referee can have in predicting $X_1(j_0) \oplus \cdots \oplus X_k(j_0)$ using the messages received from the players is $o(1/n)$, as long as $k \geq 3$ and $c \in o(kn^{1-2/k})$. Moreover, similar reasoning can be applied to conclude that for most of the values of $j_0 \in [n]$, the possible advantage in predicting $X_1(j_0) \oplus \cdots \oplus X_k(j_0)$ must be very small.

With this observation in hand, we would like to apply a "hybrid-like" reasoning, arguing that in order to distinguish between those inputs where most of bitwise XORs equal 0 and those where most equal 1, a protocol should be able, informally, to "accumulate advantage" from different input positions. We would like to claim that this is impossible as long as the advantage is negligible for almost every $j_0 \in [n]$.

Here comes the main subtlety of our proof. Note that using hybrid-like argument puts a condition on a part of the input: specifically, in order for the "hybrid scenario" to get through, it has to be argued that it is hard for the protocol to predict most of the values of $X_1(j) \oplus \cdots \oplus X_k(j)$, even if the players "know" the values of $X_1(j') \oplus \cdots \oplus X_k(j')$ for those positions j' that were considered in the earlier stages of the induction. But such conditioning creates certain type of shared randomness between the players, and we can no longer assume mutual independence of the messages received by the referee, as we have done in the reasoning above.

Recall that we are dealing with a communication problem that is easy in the presence of shared randomness even classically. How can we hope for quantum hardness, as required for the hybrid argument to be applicable? It turns out that *the mode of shared randomness that results*

[1] We shall see soon why in the actual proof we have to consider different modes of shared randomness, even if our only purpose was to get a lower bound on the complexity of $\mathcal{GP}_k$ in the quantum model without shared randomness.

from using the hybrid method is not powerful enough to make the problem easy, even for quantum communication. Our proof of Lemma 5.1 below follows rather closely the outline given above, but it also contains some new ingredients required to make the argument robust against weaker modes of shared randomness.

5.1 Exponential Separation for multi-party protocols

We are ready to prove our main technical statement.

Theorem 2.2. Let $k \geq 3$. Using shared randomness, the k-party promise function $\mathcal{GP}_k$ can be solved by a classical SMP protocol of cost k where each player sends a bit. For $2 \leq t \leq k-1$, in the SMP model with quantum communication with t-shared randomness, the complexity of $\mathcal{GP}_k$ is $\Omega(kn^{1-t/k})$. In particular, in the SMP model with quantum communication without shared randomness, the complexity of $\mathcal{GP}_k$ is $\Omega(kn^{1-2/k})$.

First, we set up notation to describe protocol $\mathcal{P}$ which uses t-shared randomness. Let $\mathcal{V}_{k,t} = \{S \subseteq [k] \colon |S| = t\}$. For any $S \in \mathcal{V}_{k,t}$, let R_S be the random string (of arbitrary length) shared by the players $\mathcal{A}_i$ for $i \in S$. Then $\mathcal{A}_i$ holds the R_S's for all $S \in \mathcal{V}_{k,t}$ containing i. For convenience, let $\tilde{R}_i = (R_S)_{i \in S \in \mathcal{V}_{k,t}}$ be the $\binom{k-1}{t-1}$-tuple of these random strings. For each instantiation $R_S = r_S$, let $\tilde{r}_i = (r_S)_{i \in S \in \mathcal{V}_{k,t}}$ be the corresponding instantiation of $\tilde{R}_i$. In addition, let $\vec{R} = (R_S)_{S \in \mathcal{V}_{k,t}}$ be the $\binom{k}{t}$-tuple of all shared random strings, and let $\vec{r} = (r_S)_{S \in \mathcal{V}_{k,t}}$ be any instantiation of $\vec{R}$. For each $i \in [k]$, player $\mathcal{A}_i$ sends a quantum state $\rho^i_{x_i,\tilde{r}_i}$ conditional upon receiving input x_i and random strings $\tilde{R}_i = \tilde{r}_i$. Let c_i be the length of the quantum message sent by $\mathcal{A}_i$; i.e., the length of state $\rho^i_{x_i,\tilde{r}_i}$ is c_i qubits. By assumption, $c \overset{\text{def}}{=} \sum_{i=1}^k c_i = o(kn^{1-t/k})$.

As before, let $\mathcal{U}_k$ be the uniform distribution over k-tuples $(x_1, \ldots, x_k) \in \{0,1\}^{n \times k}$. To prove the theorem, we will use the following lemma.

Lemma 5.1. *Let $2 \leq t \leq k-1$, and let $\mathcal{P}$ be a quantum SMP protocol of cost $c = o(kn^{1-t/k})$ that uses t-shared randomness as defined above. Suppose the player $\mathcal{A}_i$ receives the random input X_i for $(X_1, \ldots, X_k) \in \mathcal{U}(\{0,1\}^{n \times k})$. Then there exists $J \subseteq [n]$ of size at least $2n/3$ such that for every $j \in J$ a referee who is allowed to apply an arbitrary quantum measurement to the messages received according to $\mathcal{P}$ can predict the value of $X_1(j) \oplus \cdots \oplus X_k(j)$ with probability at most $1/2 + o(1/n)$.*

Proof. Let $\sigma^i_{a,\vec{r}}(j)$ be the expectation of $\rho^i_{X_i,\tilde{R}_i}$ conditional upon $X_i(j) = a$ and $\vec{R} = \vec{r}$, for any $i \in [k]$, $j \in [n]$, $a \in \{0,1\}$ and possible $\vec{r}$. Define $\alpha_{i,\vec{r}} \in \mathbb{R}^n$ as

$$\alpha_{i,\vec{r}}(j) = \frac{1}{2}\|\sigma^i_{0,\vec{r}}(j) - \sigma^i_{1,\vec{r}}(j)\|_1. \tag{2}$$

Then by Claim 3.1,

$$\sum_{j=1}^n (\alpha_{i,\vec{r}}(j))^2 \leq O(c_i).$$

Taking the sum of both sides over $i \in [k]$ and using $\sum_{i=1}^{k} c_i = c$ yields

$$\sum_{i=1}^{k}\sum_{j=1}^{n}(\alpha_{i,\vec{r}}(j))^2 \leq O(c).$$

This holds for any possible $\vec{r}$. So

$$\mathbf{E}\left[\sum_{i=1}^{k}\sum_{j=1}^{n}(\alpha_{i,\vec{R}}(j))^2\right] \leq O(c).$$

(Here the expectation is taken with respect to the R_S's). Thus, there exists some $J \subseteq [n]$ of size at least $2n/3$ such that, for any $j_0 \in J$,

$$\mathbf{E}\left[\sum_{i=1}^{k}(\alpha_{i,\vec{R}}(j_0))^2\right] \leq O\left(\frac{c}{n}\right). \tag{3}$$

Let $\sigma_{a,\vec{r}}(j_0)$ be the expectation of $\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}$ conditional upon $X_1(j_0) \oplus \cdots \oplus X_k(j_0) = a$ and $\vec{R} = \vec{r}$, for any $a \in \{0,1\}$ and possible $\vec{r}$. Since the $X_i(j_0)$'s are i.i.d. with $X_i(j_0) \sim \mathcal{U}(\{0,1\})$, and they are also independent from the R_S's, we have

$$\sigma_{a,\vec{r}}(j_0) = \mathbf{E}_{a_1 \oplus \cdots \oplus a_k = a}[\sigma^1_{a_1,\tilde{r}_1}(j_0) \otimes \cdots \otimes \sigma^k_{a_k,\tilde{r}_k}(j_0)].$$

(Here the expectation is taken with respect to the a_i's). So by Claim 3.2 and (2) we get

$$\|\sigma_{0,\vec{r}}(j_0) - \sigma_{1,\vec{r}}(j_0)\|_1 = 2\prod_{i=1}^{k}\alpha_{i,\vec{r}}(j_0).$$

Now let $\sigma_a(j_0)$ be the expectation of $\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}$ conditional upon $X_1(j_0) \oplus \cdots \oplus X_k(j_0) = a$, for $a \in \{0,1\}$. Then $\sigma_a(j_0) = \mathbf{E}[\sigma_{a,\vec{R}}(j_0)]$. Thus,

$$\begin{aligned}
\|\sigma_0(j_0) - \sigma_1(j_0)\|_1 &= \|\mathbf{E}[\sigma_{0,\vec{R}}(j_0)] - \mathbf{E}[\sigma_{1,\vec{R}}(j_0)]\|_1 \\
&\leq \mathbf{E}[\|\sigma_{0,\vec{R}}(j_0) - \sigma_{1,\vec{R}}(j_0)\|_1] \\
&= 2\,\mathbf{E}\left[\prod_{i=1}^{k}\alpha_{i,\vec{R}}(j_0)\right].
\end{aligned}$$

Note that $Z_i \overset{\text{def}}{=} \alpha_{i,\tilde{R}_i}(j_0)$ is a non-negative function of the R_S's for $i \in S \in \mathcal{V}_{k,t}$. (Recall that $\tilde{R}_i = (R_S)_{i \in S \in \mathcal{V}_{k,t}}$.) Since the R_S's are independent random variables, and each R_S is read t times (by the Z_i's for $i \in S$), we know that $Z_1, \ldots, Z_k$ form a read-t family. Thus, by invoking Lemma 3.3, we get

$$\mathbf{E}\left[\prod_{i=1}^{k}\alpha_{i,\vec{R}}(j_0)\right] \leq \left(\prod_{i=1}^{k}\mathbf{E}[(\alpha_{i,\vec{R}}(j_0))^t]\right)^{1/t}.$$

Since $0 \le \alpha_{i,\vec{R}}(j_0) \le 1$ and $t \ge 2$, we have

$$\left(\prod_{i=1}^{k} \mathbf{E}[(\alpha_{i,\vec{R}}(j_0))^t] \right)^{1/t} \le \left(\prod_{i=1}^{k} \mathbf{E}[(\alpha_{i,\vec{R}}(j_0))^2] \right)^{1/t}.$$

Then by the inequality of arithmetic and geometric means and (3),

$$\begin{aligned} \left(\prod_{i=1}^{k} \mathbf{E}[(\alpha_{i,\vec{R}}(j_0))^2] \right)^{1/t} &\le \left(\frac{1}{k} \sum_{i=1}^{k} \mathbf{E}[(\alpha_{i,\vec{R}}(j_0))^2] \right)^{k/t} \\ &\le \left(O\left(\frac{c}{kn} \right) \right)^{k/t} = o\left(\frac{1}{n} \right), \end{aligned}$$

provided $c = o(kn^{1-t/k})$. So, we have $\|\sigma_0(j_0) - \sigma_1(j_0)\|_1 = o(1/n)$. Namely, the referee can predict the value of $X_1(j_0) \oplus \cdots \oplus X_k(j_0)$ with probability at most $1/2 + o(1/n)$. This holds for any $j_0 \in J$. □

Proof of Theorem 2.2. Let $\mathcal{P}$ be a quantum SMP protocol of cost $c = o(kn^{1-t/k})$ that uses t-shared randomness. We will show that there exist $L = \lfloor 3n/4 \rfloor$ coordinates[2] $j_1, \ldots, j_L \in [n]$ satisfying the following conditions. For $l \in [L]$ and $a \in \{0,1\}$, let $W_{l,a}$ be the set of k-tuples $(x_1, \ldots, x_k) \in \{0,1\}^{n \times k}$ satisfying $x_1(j) \oplus \cdots \oplus x_k(j) = a$ for $j = j_1, j_2, \ldots, j_l$, and let $\tau_{l,a} = \mathbf{E}[\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}]$ for $(X_1, \ldots, X_k) \sim \mathcal{U}(W_{l,a})$ (here the expectation is taken with respect to the X_i's and R_S's). Then: (i) $\|\tau_{1,0} - \tau_{1,1}\|_1 = o(1/n)$; (ii) for any $l \in [L-1]$, $\|\tau_{l,0} - \tau_{l+1,0}\|_1 = o(1/n)$ and $\|\tau_{l,1} - \tau_{l+1,1}\|_1 = o(1/n)$. If this is true, then by the triangle inequality,

$$\begin{aligned} &\|\tau_{L,0} - \tau_{L,1}\|_1 \\ &\le \sum_{l=1}^{L-1} \|\tau_{l,0} - \tau_{l+1,0}\|_1 + \sum_{l=1}^{L-1} \|\tau_{l,1} - \tau_{l+1,1}\|_1 \\ &\quad + \|\tau_{1,0} - \tau_{1,1}\|_1 \\ &= o(L/n) \\ &= o(1). \end{aligned} \tag{4}$$

On the other hand, for any $(x_1, \ldots, x_k) \in W_{L,0}$, it holds that $|x_1 \oplus x_2 \oplus \cdots \oplus x_k| \le n - L < n/3$ and hence $\mathcal{GP}_k(x_1, \ldots, x_k) = 0$. Similarly, for any $(x_1, \ldots, x_k) \in W_{L,1}$, it holds that $|x_1 \oplus x_2 \oplus \cdots \oplus x_k| \ge L > 2n/3$ and hence $\mathcal{GP}_k(x_1, \ldots, x_k) = 1$. Therefore, if the referee can correctly predict the value of $\mathcal{GP}_k(x_1, \ldots, x_k)$ on any $(x_1, \ldots, x_k) \in W_{L,0} \sqcup W_{L,1}$, then he should be able to distinguish between $\tau_{L,0}$ and $\tau_{L,1}$ with probability at least $2/3$, which implies that $\|\tau_{L,0} - \tau_{L,1}\|_1 = \Omega(1)$. But this is contradictory to (4). So the referee must fail to solve $\mathcal{GP}_k$ on some valid input from $W_{L,0}$ or $W_{L,1}$.

To find the desired $j_1, \ldots, j_L$, we use one initial step and $L-1$ inductive steps as follows.

[2] In fact, our statement holds for any $L \le (1-\varepsilon)n$, where ε can be any small constant.

Initial Step: Consider the behavior of $\mathcal{P}$ on the random input $(X_1, \ldots, X_k) \in \mathcal{U}(\{0,1\}^{n\times k})$. By a straightforward application of Lemma 5.1, there exists $J \subseteq [n]$ of size at least $2n/3$ such that, for any $j \in J$, the referee can predict the value of $X_1(j) \oplus \cdots \oplus X_k(j)$ with probability at most $1/2 + o(1/n)$. In other words, for any $j \in J$, we have $\|\sigma_0(j) - \sigma_1(j)\|_1 = o(1/n)$ where $\sigma_a(j)$ is the expectation of $\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}$ conditional upon $X_1(j) \oplus \cdots \oplus X_k(j) = a$, for $a \in \{0,1\}$. Set j_1 to be any $j \in J$. Then $\|\tau_{1,0} - \tau_{1,1}\|_1 = \|\sigma_0(j) - \sigma_1(j)\|_1 = o(1/n)$ as desired.

Inductive Step: Suppose now we have fixed $j_1, \ldots, j_l \in [n]$ for some $l \leq 3n/4$. Let $T = \{j_1, \ldots, j_l\}$ and $T^c = [n] \setminus T$.

Let us consider the behavior of $\mathcal{P}$ on the random input $(X_1, \ldots, X_k) \sim \mathcal{U}(W_{l,0})$ (recall that $W_{l,0}$ is the set of $(x_1, \ldots, x_k) \in \{0,1\}^{n\times k}$ satisfying $(x_1 \oplus \cdots \oplus x_k)_T = \bar{0}$). Note that the X_i's are not completely independent but only $(k-1)$-wise independent. So there exists some correlation among the inputs to different players, which might be exploited to gain some advantage. However, we will show that, even in this case, the referee can still predict the value of $X_1(j) \oplus \cdots \oplus X_k(j)$ with probability at most $1/2 + o(1/n)$ for at least $2/3$ fraction of $j \in T^c$.

Let $Y_i = (X_i)_T$. Then $(Y_1, \ldots, Y_k)$ is uniformly distributed among all $(y_1, \ldots, y_k) \in \{0,1\}^{l\times k}$ satisfying $y_1 \oplus \cdots \oplus y_k = \bar{0}$. Namely, $(Y_1, \ldots, Y_k)$ can be viewed as some XOR randomness (which is a special kind of 2-shared randomness) shared by the players. Also, note that the $(X_i)_{T^c}$'s are i.i.d. with $(X_i)_{T^c} \sim \mathcal{U}(\{0,1\}^{n-l})$, and they are also independent from the Y_i's. Finally, the Y_i's and $(X_i)_{T^c}$'s are all independent from the R_S's.

Now consider the following protocol $\mathcal{P}'$ which attempts to solve $\mathcal{GP}_k$ for $(n-l)$-bit strings. The players share XOR randomness $(Y'_1, \ldots, Y'_k)$ which has the same distribution as $(Y_1, \ldots, Y_k)$. In addition, they also share t-shared randomness $(R'_S)_{S\in\mathcal{V}_{k,t}}$ which has the same distribution as $(R_S)_{S\in\mathcal{V}_{k,t}}$. Furthermore, the Y'_i's and R'_S's are independent. Now suppose player $\mathcal{A}_i$ receives input $x'_i \in \{0,1\}^{n-l}$ and random strings $Y'_i = y_i$ and $\tilde{R}'_i = \tilde{r}_i$. Then $\mathcal{A}_i$ first finds the unique $x_i \in \{0,1\}^n$ such that $(x_i)_T = y_i$ and $(x_i)_{T^c} = x'_i$, and then sends the quantum message $\rho^i_{x_i,\tilde{r}_i}$ of $\mathcal{P}$ to the referee.

Since the $(Y'_1, \ldots, Y'_k)$ is a special kind of 2-shared randomness, $\mathcal{P}'$ uses only t-shared randomness. So by Lemma 5.1 (replacing the original n by $n-l$ and noting that $n-l = \Theta(n)$, since $l \leq 3n/4$), we know that, on the random input $(X'_1, \ldots, X'_k) \sim \mathcal{U}(\{0,1\}^{(n-l)\times k})$, there exists $J' \subseteq [n-l]$ of size at least $2(n-l)/3$ such that for any $j \in J'$ the referee can predict the value of $X'_1(j) \oplus \cdots \oplus X'_k(j)$ with probability at most $1/2 + o(1/n)$ using the messages received according to $\mathcal{P}'$. Meanwhile, by the construction of X'_i's, Y'_i's, R'_S's and $\mathcal{P}'$, it is obvious that the joint message sent according to $\mathcal{P}'$ has the same distribution as $\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}$. In addition, the bits of X'_i are in one-to-one correspondence with the bits of $(X_i)_{T^c}$. Thus, getting back to the original protocol $\mathcal{P}$, we know that, on the random input $(X_1, \ldots, X_k) \sim \mathcal{U}(W_{l,0})$, there exists $J_0 \subseteq T^c$ of size at least $2(n-l)/3$ (corresponding to J') such that for any $j \in J_0$ the referee can predict the value of $X_1(j) \oplus \cdots \oplus X_k(j)$ with probability at most $1/2 + o(1/n)$ using the messages received according to $\mathcal{P}$. So for any $j \in J_0$, we have $\|\sigma_0(j) - \sigma_1(j)\|_1 = o(1/n)$, where $\sigma_a(j)$ is the expectation of $\rho^1_{X_1,\tilde{R}_1} \otimes \cdots \otimes \rho^k_{X_k,\tilde{R}_k}$ conditional upon $X_1(j) \oplus \cdots \oplus X_k(j) = a$ for $a \in \{0,1\}$. Now if we set $j_{l+1} = j$, then depending on the value of $x_1(j) \oplus \cdots \oplus x_k(j)$, $W_{l,0}$ is split into to two equal-sized subsets: $W_{l+1,0}$ and $W_{l,0} \setminus W_{l+1,0}$. It follows that $\tau_{l,0} = (\sigma_0(j) + \sigma_1(j))/2$ and $\tau_{l+1,0} = \sigma_0(j)$, and hence $\|\tau_{l,0} - \tau_{l+1,0}\|_1 = \|\sigma_0(j) - \sigma_1(j)\|_1/2 = o(1/n)$.

By a similar argument, we can also prove that, on the random input $(X_1, \ldots, X_k) \sim \mathcal{U}(W_{l,1})$, there also exists $J_1 \subseteq T^c$ of size at least $2(n-l)/3$ such that for any $j \in J_1$ the referee can predict $X_1(j) \oplus \cdots \oplus X_k(j)$ with probability at most $1/2 + o(1/n)$. Then, if we set j_{l+1} to be any $j \in J_1$, then we get $\|\tau_{l,1} - \tau_{l+1,1}\|_1 = o(1/n)$.

Now since $|J_0|, |J_1| \geq 2(n-l)/3$, $J_0 \cap J_1$ must be non-empty. We set j_{l+1} to be any $j \in T_0 \cap T_1$. Then we achieve both $\|\tau_{l,0} - \tau_{l+1,0}\|_1 = o(1/n)$ and $\|\tau_{l,1} - \tau_{l+1,1}\|_1 = o(1/n)$.

Iterate this inductive step $L-1$ times, and in the end we obtain the desired $j_1, \ldots, j_L$. This completes a proof of the theorem. □

Acknowledgments

The authors thank anonymous reviewers for helpful comments on previous versions of this paper. The authors acknowledge support by ARO/NSA under grant W911NF-09-1-0569.

References

[ANTSV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16, Article 167902), 2001.

[Fin92] H. Finner. A generalization of hölder inequality and some probability inequalities. *The Annals of Probability*, 20(4):1893–1901, 1992.

[GKRdW06] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. In *Proceedings of the 38th Symposium on Theory of Computing*, pages 594–603, 2006.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 369–377, 1999.

[New91] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[NS96] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of the 28th Symposium on Theory of Computing*, pages 561–570, 1996.

[Yao03] A. C.-C. Yao. On the power of quantum fingerprinting. In *Proceedings of the 35th Symposium on Theory of Computing*, pages 77–81, 2003.