Math. Struct. in Comp. Science (2009), *vol.* 19, *pp.* 119–132. © 2009 Cambridge University Press
doi:10.1017/S0960129508007263 Printed in the United Kingdom

Quantum multiparty communication complexity and circuit lower bounds

IORDANIS KERENIDIS[†]

[†]*CNRS, LRI-Université de Paris-Sud, Paris, France*
Email: jkeren@lri.fr

Received 15 October 2007

We define a quantum model for multiparty communication complexity and prove a simulation theorem between the classical and quantum models. As a result, we show that if the quantum k-party communication complexity of a function f is $\Omega(n/2^k)$, its classical k-party communication is $\Omega(n/2^{k/2})$. Finding such an f would allow us to prove strong classical lower bounds for $k \geqslant \log n$ players and make progress towards solving a major open question about symmetric circuits.

1. Introduction

Communication complexity is a central model of computation with numerous applications. It has been used for proving lower bounds in many areas including Boolean circuits, time–space tradeoffs, data structures, automata and formula size. Examples of these applications can be found in the textbook Kushilevitz and Nisan (1997).

The 'Number on the Forehead' (NoF) model of multiparty communication complexity was introduced by Chandra, Furst and Lipton (Chandra *et al.* 1983). In this model, there are k parties that wish to compute a function $f : X_1 \times \cdots \times X_k \to \{0,1\}$ on the input $(x_1, \ldots, x_k) \in (X_1 \times \cdots \times X_k)$. We can assume without loss of generality that $X_1 = \ldots = X_k = \{0,1\}^n$. Each player sees only $(k-1)$ of the inputs (the other is on his forehead). The players communicate by writing messages on a common blackboard. In the general model, in every round, the players take turns writing one bit on the blackboard that might depend on the previous messages. In the Simultaneous Messages variant (SMNoF), all players simultaneously write a single message on the blackboard. At the end of the protocol, the blackboard must contain enough information to compute the value of $f(x_1, \ldots, x_k)$. The communication cost of the protocol is the number of bits written on the blackboard. The deterministic k-party communication complexity of f, $C(f)$, is the communication cost of the optimal deterministic protocol for f. In the randomised setting, we allow the players to be probabilistic and to share public coins, and for the output of the protocol to be correct with probability at least $1/2 + \delta$. We define

[†] This work was supported in part by ACI Sécurité Informatique SI/03 511 and ANR AlgoQP grants of the French Research Ministry, and also partially supported by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate under Contract Number 015848.

$C_\delta(f)$ to be the probabilistic k-party communication complexity of f with correctness $1/2+\delta$.

The number of players in the above definition is equal to the number of arguments of f. However, we can easily generalise the model for the case of $\ell \leqslant k$ players. The model of communication remains the same and each of the ℓ players still receives $(k-1)$ arguments of f. We use $C_\delta^\ell(f)$ to denote the ℓ-party communication complexity of $f(X_1,\ldots,X_k)$. Note also that we are dealing with functions that are total and boolean.

Multiparty communication complexity has been studied extensively and has proved relevant to important questions in circuit lower bounds. For example, one of the major open problems in circuit complexity is to prove that an explicit function f is not in the circuit complexity class ACC^0, which is defined in the next subsection (see Kushilevitz and Nisan (1997, Open problem 6.21)). By the results of Hastad and Goldmann (1991) and Yao (1990), this question reduces to proving a superlogarithmic communication lower bound for the k-party communication complexity of some explicit function f, where the number of players is superlogarithmic. However, all known techniques for proving multiparty communication lower bounds fail when the number of players becomes $k=\log n$.

In this paper we propose a new technique for proving multiparty communication complexity lower bounds and hence, circuit lower bounds. We define a quantum model for multiparty communication complexity in which both the players' inputs and messages are quantum, and prove a simulation theorem between the classical and quantum models. In outline, our quantum model can be described as follows. The players receive as input a mixed quantum state, which is a classical distribution over the legal inputs to all the classical players. In other words, the quantum forehead is equivalent to a probability distribution over classical foreheads. Moreover, the purification of this input, that is, a register that contains the identity of each classical input, is considered to be part of the quantum blackboard and is used when the final measurement is made. We will provide a formal definition of our model in Section 2.

Using this model, we show how to simulate k classical players with only $k/2$ quantum ones (Section 3). Note that if the success probability of the classical protocol was $1/2+\delta$, the success probability of the quantum protocol is $1/2+\delta/2^C$, where C is the communication of the original protocol. Since the common lower bounds depend only logarithmically on the bias δ (see, for example, Babai *et al.* (1992) and Raz (2000)), this simulation is sufficient for our purposes. This enables us to reduce questions about classical communication to potentially easier questions about quantum communication complexity and shows that quantum information theory could be a powerful tool for proving classical circuit lower bounds (Section 4).

Similar connections between classical and quantum computation have been proved to be very fruitful in recent years. Important results in classical complexity theory have been proved using quantum techniques or inspired by them, including, for example, lower bounds for Locally Decodable Codes (Kerenidis and de Wolf 2003) or local search (Aaronson 2004), inclusions of lattice problems in complexity classes (Aharonov and Regev 2003; Aharonov and Regev 2004) and simple proofs of properties of the class PP (Aaronson 2005) and of lower bounds for matrix rigidity (de Wolf 2005).

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

In addition, we examine the power of our model for quantum multiparty communication by looking at the generalised inner product (GIP) function (Section 5). We provide a quantum protocol with $\log n$-party communication complexity of $O(\log n)$, while the best-known classical protocol requires communication $O(\sqrt{n})$. Proving a tight classical lower bound for this function will provide an example of an exponential separation between classical and quantum communication that holds for a total boolean function. All other known exponential separations in the two-party setting (that is, in the model of two-way communication (Raz 1999), one-way communication (Bar-Yossef *et al.* 2004; Gavinsky *et al.* 2007) and simultaneous messages (Bar-Yossef *et al.* 2004)) are for promise problems or relations.

1.1. *Multiparty communication complexity and circuit lower bounds*

Multiparty communication complexity was introduced as a tool for the study of boolean circuits, however, the known techniques for proving lower bounds are very limited. Babai *et al.* (1992) proved a lower bound of $\Omega(n/2^{2k} + \log \delta)$ for the k-party communication complexity of the generalised inner product function and an $\Omega(n/2^k + \log \delta)$ bound for the quadratic character (Legendre symbol) of the ($mod\ p$) sum of k variables. Raz (Raz 2000) simplified their proof technique and showed a similar lower bound for another function, namely matrix multiplication, which seems to be hard even for $\log n$ players. Unfortunately, the above techniques are limited and cannot prove lower bounds better than $\Omega(n/2^k + \log \delta)$ for any function. Despite the importance of the question and its serious consequences on circuit lower bounds, it has not been possible to find any new lower bound techniques. For the generalised inner product function, Grolmusz (1994) showed an upper bound of $O(k(n/2^k))$.

The Number on the Forehead model is related to the circuit complexity class ACC^0. ACC^0 consists of languages recognised by a family of constant-depth polynomial size, unbounded fan-in circuits with NOT, AND, OR and MOD_m gates, where m is fixed for the family. Finding an explicit function outside the class ACC^0 is a major open question. Yao (Yao 1990) and Beigel and Tarui (Beigel and Tarui 1994) have shown that ACC^0 circuits can be simulated by symmetric circuits. The circuit class $SYM(d,s)$ is the class of circuits of depth 2 whose top gate is a symmetric gate of fan-in s and each of the bottom level gates is an AND gate of fan-in at most d. Specifically, they showed that $ACC^0 \subseteq SYM(\text{polylog } n, 2^{\text{polylog } n})$.

The connection with multiparty communication was made by Hastad and Goldmann (Hastad and Goldmann 1991), who noticed that when a function f belongs to $SYM(d,s)$, there exists a $(d+1)$-party simultaneous protocol with complexity $O(d \log s)$. The protocol is as follows. Since each AND gate has fan-in at most d, at least one of the $d+1$ players must have all the information to compute it. Hence, all the AND gates can be assigned to players. Then, since the top gate of the circuit is a symmetric gate, each player only needs to output the total number of his AND gates that evaluate to 1 (which takes at most $\log s$ bits for each player). Therefore, if we want to show that a function f is outside $SYM(d,s)$, we need to prove a $(d+1)$-party communication lower bound of $\omega(d \log s)$ in the simultaneous model. However, as we said earlier, no techniques are known to give

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

communication lower bounds for $k = \log n$ players or more. In the following sections we describe a technique that can potentially give strong lower bounds for $k \geqslant \log n$ players and hopefully help towards proving that a function is outside ACC^0.

1.2. *Quantum background*

Let H denote a 2-dimensional Hilbert space and $\{|0\rangle, |1\rangle\}$ be an orthonormal basis for this space. A *qubit* is a unit length vector in this space, and thus can be expressed as a linear combination of the basis states: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$. Here α_0, α_1 are complex *amplitudes* and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. An *m-qubit system* is a unit vector in the m-fold tensor space $H \otimes \cdots \otimes H$ and can be expressed as $|\phi\rangle = \sum_{i \in \{0,1\}^m} \alpha_i |i\rangle$. A *mixed state* $\{p_i, |\phi_i\rangle\}$ is a classical distribution over pure quantum states, where the system is in state $|\phi_i\rangle$ with probability p_i.

A quantum state can evolve by a unitary operation or by a measurement. A *unitary* transformation is a linear mapping that preserves the ℓ_2 norm. If we apply a unitary U to a state $|\phi\rangle$, it evolves to $U|\phi\rangle$. A mixed state ρ evolves to $U\rho U^*$. The most general measurement (POVM) allowed by quantum mechanics is specified by a family of positive semidefinite operators $E_i = M_i^* M_i$, $1 \leqslant i \leqslant k$, subject to the condition that $\sum_i E_i = I$. Given a mixed state ρ, the probability of observing the ith outcome under this measurement is given by the trace $p_i = \mathrm{Tr}(E_i \rho) = \mathrm{Tr}(M_i \rho M_i^*)$. If the measurement yields outcome i, the resulting quantum state is $M_i \rho M_i^* / \mathrm{Tr}(M_i \rho M_i^*)$. A general POVM can be thought of as a series of unitary operations and projective measurements.

2. Quantum multiparty communication complexity

We assume basic familiarity with the formalism of quantum computing – see Nielsen and Chuang (2000) for further details. One natural way of defining the quantum analog of simultaneous multiparty communication would be as follows. There are k parties that wish to compute a function $f : X_1 \times \cdots \times X_k \to \{0,1\}$ on the input $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$. We can assume without loss of generality that $X_1 = \ldots = X_k = \{0,1\}^n$. Each player sees only $(k-1)$ of the inputs (the other one is on his forehead). The players communicate by simultaneously writing a *quantum* message each on a common blackboard that they can all see. After that, the value of f can be computed with high probability by performing some measurement on these quantum messages. The quantum communication cost is the sum of the number of qubits of each message. In this model, we have kept the inputs to the players classical but made the communication quantum. Unfortunately, not very much is known about the power of this model of quantum multiparty communication. It is an open question to see if this model can be exponentially more powerful than the classical one, and also how it is related to our model.

Here we define a different variant of quantum multiparty communication where, in addition, we allow the inputs to the quantum players to be quantum. Our primary goal is to define a natural model that has consequences for the study of circuit lower bounds. In order to make the definition of the quantum model more intuitive, we will

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

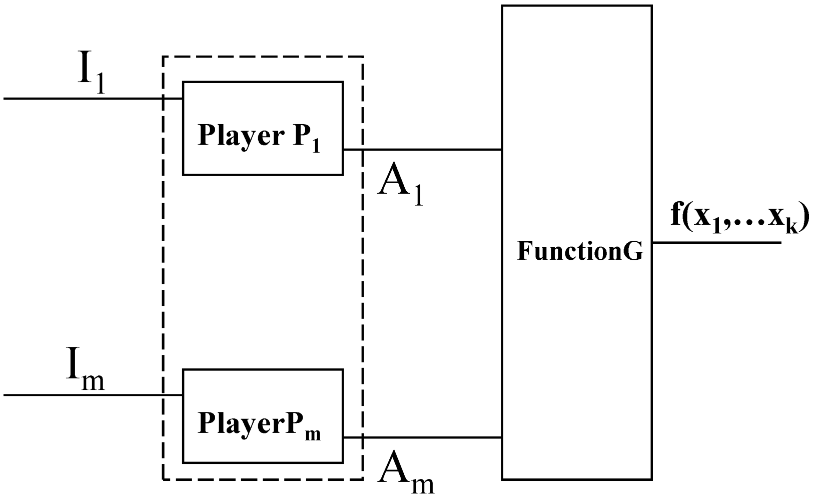

Figure 1. Classical Number on the Forehead

first describe the classical model of the Number on the Forehead in an appropriate way.

In outline, a simultaneous multiparty protocol consists of three rounds (see Figure 1):

1 The players receive their inputs.
2 They each output some answer that depends on their input.
3 The value of f is computed as a function of the players' answers.

For convenience, and without loss of generality, we assume that the players' outputs have the same length. More formally, we have the following definition.

Classical Simultaneous Number on the Forehead (SNoF)

— For $j = 1,\ldots,\ell$ the input to Player P_j is of the form $I_j = (x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_k)$.
— Each Player P_j performs a probabilistic procedure that on input I_j (and some randomness r) outputs an answer A_j.
— The value of the function f is computed by evaluating a function g with $(A_1,\ldots,A_\ell)$ as input, that is, the guess for $f(x_1,\ldots,x_k)$ is equal to $g(A_1,\ldots,A_\ell)$. The function g is fixed in advance and is independent of the input $(x_1,\ldots,x_k)$.

The correctness of the protocol guarantees that for every input $(x_1,\ldots,x_k) \in \{0,1\}^{kn}$, we have

$$Pr[g(A_1,\ldots,A_\ell) = f(x_1,\ldots,x_k)] \geqslant 1/2 + \delta\,,$$

where the probability is over the random coins of the players P_j. The 'communication cost' of the protocol is the sum of the lengths of the outputs of the players or, equivalently, the sum of the lengths of the inputs to the final subcircuit G, that is, $\sum_{i=1}^{\ell} |A_i|$. The communication complexity of f is the cost of the optimal protocol. It is easy to see that the formulation described above is equivalent to the usual simultaneous Number on the Forehead model.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

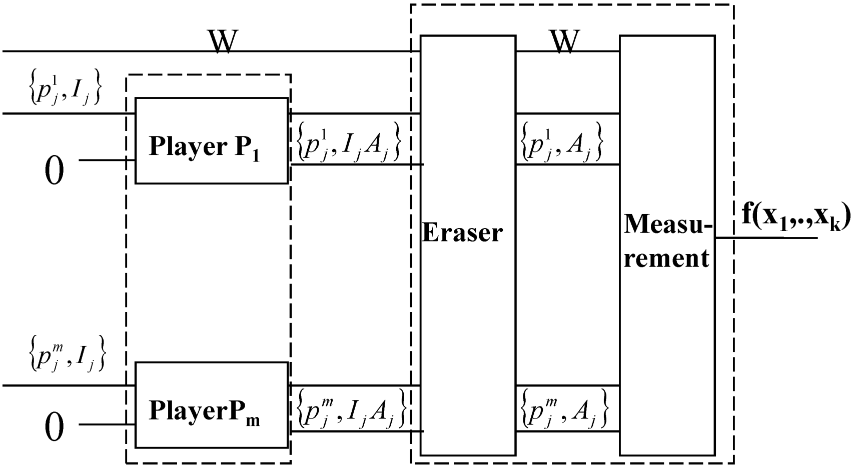

Figure 2. Quantum Simultaneous Number on the Forehead

Intuitively, we define the quantum analog as follows (see Figure 2):

1 The players receive quantum inputs.
2 They perform a quantum procedure in order to compute their outputs.
3 The value of f is computed by performing a measurement on the quantum outputs.

However, we have to be careful with the constraints we need to impose on these operations and with the definition of the 'cost' of the protocol. More formally, the quantum model is defined as follows.

Quantum Simultaneous Number on the Forehead

— For $i = 1, \ldots, \ell$, each quantum player P_i receives as input the quantum mixed state $(\rho_i = \{p_j^i, (j, I_j)\})$ with $j = 1, \ldots, k$, that is, a probability distribution over all the legal classical inputs. We also assume that a purification of this state is available in some other register W that is unavailable to the players but will be part of the final measurement in the third round. In other words, we assume that for every $i = 1, \ldots, \ell$, the input state is

$$|\phi_i\rangle = \sum_{j=1}^{k} \sqrt{p_j^i}\, |j\rangle\, |j, I_j\rangle \ .$$

The second register of this state is the input for player P_i and the first register contains the purification of this mixed state. The distribution is fixed by the protocol and is independent of the input $(x_1, \ldots, x_k)$.

— In the second round each of the ℓ players performs the quantum mapping

$$|j, I_j\rangle\, |0\rangle \mapsto |j, I_j\rangle\, \left|A_j^i\right\rangle \ ,$$

where A_j^i is the quantum answer of player P_i to input j, I_j.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

— The third round takes as input the quantum states

$$|\psi_i\rangle = \sum_{j=1}^{k} \sqrt{p^i_j}\, |j\rangle\, |j, I_j\rangle\, |A^i_j\rangle\ .$$

In order to ensure that the measurement does not take advantage of the fact that the second registers contain the input of the function, we first erase it by performing the mapping

$$E\ :\ |j\rangle\, |j, I_j\rangle \mapsto |j\rangle\, |0\rangle\ ,$$

resulting in the states

$$|\psi_i\rangle = \sum_{j=1}^{k} \sqrt{p^i_j}\, |j\rangle\, |A^i_j\rangle\ .$$

Then a general measurement M is performed on these states whose outcome is the guess for $f(x_1, \ldots, x_k)$. The measurement M is fixed by the protocol and is independent of the input x.

The correctness of the protocol implies that for all $(x_1, \ldots, x_k) \in \{0, 1\}^{kn}$,

$$Pr[\text{outcome of } M = f(x_1, \ldots, x_k)] \geqslant 1/2 + \delta\ .$$

The communication cost of the protocol is the sum of the lengths of the inputs to the final measurement M, that is, $\sum_{i=1}^{\ell} |A_i|$, where $|A_i|$ is the size of the answer register of player i[†]. The communication complexity of f is the cost of the optimal protocol.

Let us make a few remarks about our definition. First, the inputs $\{p^i_j, (j, I_j)\}$ ensure that each player gains information for $(k - 1)$ of the inputs x_i, exactly like the classical players. In the special case where the distributions $\{p^i\}$ are delta functions, the inputs become equal to the classical inputs.

Second, the quantum ‘erasure’ of the inputs in the third round of the protocol is necessary in order to ensure that the final measurement only depends on the players’ answers, exactly like in the classical case. Moreover, we do not use the simpler way of erasing the quantum inputs by just tracing out the input registers (instead of performing the unitary map E), since that would be equivalent to a model with classical inputs.

3. Simulating classical players

In this section we prove that we can simulate a k-party classical protocol by a $k/2$-party quantum protocol with the same communication, albeit with larger error probability.

The main idea of our simulation is as follows. In any protocol, the value of the function f is computed as a boolean function $g : \{-1, 1\}^C \to \{-1, 1\}$ of the output of the players. However, any such boolean function g has correlation at least $2^{-C/2}$ with a parity function,

[†] More precisely, the communication should be defined as $\sum_{i=1}^{\ell}(|W_i| + |A_i|)$, where W_i is the Hilbert space that contains the purification of the input of player i. However, the communication according to this definition is in the worst case an additive factor of $\ell \log k$ greater than our definition, which will not be of any significance.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

that is, a parity of a subset of the input bits. Hence, we can substitute the initial protocol with another one in which the value of f is computed as a parity function of the output of the players (note that the success bias of the protocol reduces by a factor of $2^{-C/2}$). Now, instead of looking at the output of the k players as one long string, consider it as a concatenation of $k/2$ pairs of individual outputs; the parity function on the entire output can be thought of as a parity of $k/2$ parities, each one on a pair of individual outputs. The second part of our simulation describes a quantum procedure in which each of the $k/2$ quantum players provides enough information to compute one of these $k/2$ parities and hence compute the value of f.

We formally prove the following theorem.

Theorem 1. Let P be a SNoF protocol for the function $f : X_1, \dots, X_k \to \{0,1\}$ with k players, communication C and correctness $1/2+\delta$. Then, there exists a quantum SNoF protocol Q for the same function f with $k/2$ quantum players, communication $C/2$ and correctness $1/2+\delta/2^C$ on an average input.

Proof. First we prove a lemma similar to Lemma 2 in Kerenidis and de Wolf (2003), which shows that we can assume the players compute the parity of a subset of the answer bits as their guess for f. We switch from the $\{0,1\}$-notation to the $\{-1,1\}$-notation for f, we view the answers of the players A_i as (C/k)-bit strings and $A_i[j]$ the j-th bit of the string A_i. Let $S_i \subseteq [C/k]$ be some subset of bits of A_i and $A_{S_i} = \prod_{j \in S_i} A_i[j]$ be the parity of the subset S_i of the bits of A_i.

Lemma 1. Let P be a classical protocol with communication C and correctness probability $1/2+\delta$ and assume that the players compute a function $g(A_1, \dots, A_k)$ as their guess for $f(x)$, where A_i is the answer of player i. Then there exists a classical protocol P' with communication C that works on average input with correctness $1/2+\delta/2^{C/2}$ and where the players compute a parity of a subset of bits of the answers A_i, that is, $g(A_1, \dots, A_k) = \oplus_{i=1}^k A_{S_i}$.

Proof. Let $f(x) = b$. From the correctness of the protocol P we know that

$$E_x[g(A_1, \dots, A_k) \cdot b] \geqslant 2\delta\,.$$

We can represent g by its Fourier representation as

$$g(A_1, \dots, A_k) = \sum_{S_1, \dots, S_k} \hat{g}_{S_1, \dots, S_k} A_{S_1} \cdots A_{S_k}$$

and have

$$2\delta \leqslant E_x[g(A_1, \dots, A_k) \cdot b] = \sum_{S_1, \dots, S_k} \hat{g}_{S_1, \dots, S_k} E_x[A_{S_1} \cdots A_{S_k} \cdot b]\,.$$

By the fact that $\sum_{S_1, \dots, S_k} (\hat{g}_{S_1, \dots, S_k})^2 = 1$, we have $\sum_{S_1, \dots, S_k} \hat{g}_{S_1, \dots, S_k} \leqslant 2^{C/2}$, and hence there exist some subsets $S_1, \dots, S_k$ for which

$$E_x[A_{S_1} \cdots A_{S_k} \cdot b] \geqslant 2\delta/2^{C/2}\,.$$

This means that the protocol P' that would output the XOR of these subsets is correct on an average input with probability $\geqslant 1/2+\delta/2^{C/2}$. □

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

Thus, in the classical protocol P', in the first round each player j receives input I_j, in the second round they output the answers A_j, and in the third round the guess for f is computed by considering all the players' outputs together as one string and taking the XOR of a subset of these bits. We will now describe the quantum protocol with only $k/2$ players that simulates the classical k-party one. We denote the $k/2$ quantum players with $i = 1, 3, \ldots, k-1$.

— For every $i = 1, 3, \ldots, k-1$, we consider the following states:

$$|\phi_i\rangle = |i\rangle\,|i, I_i\rangle + |i+1\rangle\,|i+1, I_{i+1}\rangle\,,$$

where the second register is the input of quantum player i and the first is the purification of the state in the workspace W. Note that the reduced density matrix of quantum player i is the same as if he was classical player i with probability $1/2$ and classical player $i+1$ with probability $1/2$, so this is a legal input.

— In the second round, each quantum player P_i performs the mapping

$$T\,:|j, I_j\rangle\,|0\rangle \mapsto |j, I_j\rangle\,|A_j\rangle\,,$$

that is, on input $|j, I_j\rangle$ computes the same function A_j as the classical player j in P'. Note that the answer of the classical player j can depend on his private randomness, and we assume that the quantum player uses for each input (j, I_j) the same randomness used by the classical player j. The total communication is

$$\frac{k}{2}\frac{C}{k} = \frac{C}{2}$$

qubits.

— In the third round, the states are

$$|\phi_i\rangle = |i\rangle\,|i, I_i\rangle\,|A_i\rangle + |i+1\rangle\,|i+1, I_{i+1}\rangle\,|A_{i+1}\rangle\,.$$

First, the 'erasure' circuit erases the input registers resulting in the states

$$|\psi_i\rangle = |i\rangle\,|A_i\rangle + |i+1\rangle\,|A_{i+1}\rangle\,.$$

Finally, a measurement on the states is performed (described by Lemma 2) that computes f with high probability.

We need to show that there exists a quantum procedure M on the states $|\psi_i\rangle$ that is able to compute the function $\oplus_{i=1}^{k} S_i$. A key observation is that we can rewrite the function as

$$\oplus_{i=1}^{k} S_i = \oplus_{i=1,3,\ldots,k-1}(S_i \oplus S_{i+1})\,.$$

It is a simple calculation to show that if we can independently predict each $S_i \oplus S_{i+1}$ with probability $1/2 + \epsilon$, we can predict the entire $\oplus_i S_i$ with probability $1/2 + 2^{k/2-1}\epsilon^{k/2}$. The following lemma from Wehner and de Wolf (2005) describes a quantum procedure M to compute $S_i \oplus S_{i+1}$ with the optimal ϵ.

Lemma 2 (Wehner and de Wolf 2005, Theorem 2). Suppose $f : \{0,1\}^{2t} \to \{0,1\}$ is a boolean function. There exists a quantum procedure M to compute $f(a_0, a_1)$ with success probability $1/2 + 1/2^{t+1}$ using only one copy of $|0\rangle\,|a_0\rangle + |1\rangle\,|a_1\rangle$, with $a_0, a_1 \in \{0,1\}^t$.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

We use this lemma with $t = C/k$ and get $\epsilon = 1/2^{C/k+1}$. We also note that the success probability is independent of the a_0, a_1. Hence, there exists a quantum procedure that will output the correct $\oplus_i S_i$ with probability

$$Pr[M \text{ outputs } \oplus_i S_i] = \frac{1}{2} + 2^{k/2-1} \cdot \frac{1}{2^{(C+k)/2}} = \frac{1}{2} + \frac{1}{2^{C/2+1}}.$$

Finally, the quantum protocol is correct with probability

$$\begin{aligned} p &= Pr[M \text{ outputs } \oplus S_i] \cdot Pr[\oplus S_i = b] + \\ &\quad Pr[M \text{ does not output } \oplus S_i] \cdot Pr[\oplus S_i \neq b] \\ &= \left(\frac{1}{2} + \frac{1}{2^{C/2+1}}\right)\left(\frac{1}{2} + \frac{\delta}{2^{C/2}}\right) + \left(\frac{1}{2} - \frac{1}{2^{C/2+1}}\right)\left(\frac{1}{2} - \frac{\delta}{2^{C/2}}\right) = \frac{1}{2} + \frac{\delta}{2^{C}}. \end{aligned}$$ □

Note that the success probability of the quantum protocol is not guaranteed for every input but only on average input. In fact, it is easy to see that it works for any distribution on inputs since Lemma 1 does not depend on the distribution of the input. Though proving lower bounds for such protocols can be potentially harder than proving lower bounds for worst-case protocols, most known lower bounds work equally well for both cases.

4. A quantum reduction for circuit lower bounds

The theorem in the previous section shows how to simulate a classical protocol with k players using a quantum protocol with $k/2$ players, albeit with a smaller bias. We are going to use this theorem to get a reduction from a classical circuit lower bound question to one about quantum communication complexity.

Theorem 2. Suppose $f : X_1 \times \cdots \times X_k \to \{0,1\}$ is a function for which the $(k/2)$-party quantum average communication complexity is

$$QC^{k/2}_{\delta'} = \gamma\left(k\frac{n}{2^{k/2}} + \log \delta'\right)$$

for a positive constant γ. Then, this function does not belong to the class $SYM(k-1, 2^{o(n/2^{k/2})})$.

Proof. In order to show a contradiction, let us assume that the function does indeed belong to $SYM(k-1, 2^{o(n/2^{k/2})})$. Then, by Hastad and Goldmann (1991), the function f will have classical k-party communication complexity at most

$$C_\delta \leqslant \frac{\gamma}{1+\gamma}\left(k\frac{n}{2^{k/2}} + \log \delta\right)$$

for any constant γ and success probability $1/2+\delta$. By Theorem 1, there exists a $(k/2)$-party quantum protocol with correctness $1/2 + \delta/2^{C_\delta}$ and quantum communication

$$QC^{k/2}_{\delta/2^{C_\delta}} = C_\delta/2.$$

Hence,

$$\begin{aligned} QC^{k/2}_{\delta/2^{C_\delta}} &= \frac{C_\delta}{2} \\ &= \frac{1+\gamma}{2}C_\delta - \frac{\gamma}{2}C_\delta \leqslant \frac{\gamma}{2}\left(k\frac{n}{2^{k/2}} + \log \delta\right) - \frac{\gamma}{2}C_\delta \end{aligned}$$

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

$$= \frac{\gamma}{2}\left(k\frac{n}{2^{k/2}} + \log\frac{\delta}{2^{C_\delta}}\right),$$

which contradicts the assumption of the theorem for $\delta' = \delta/2^{C_\delta}$. □

Taking $k = \log n + 1$, the function f is not in $SYM(\log n, 2^{o(\sqrt{n})})$. In other words, we have reduced the question of finding a function outside the class $SYM(\log n, 2^{\omega(polylogn)})$ to that of finding an explicit function $f : X_1 \times \cdots \times X_k \to \{0, 1\}$ with $(k/2)$-party quantum complexity equal to $\Omega(n/2^{k/2} + \log\delta)$. Note that we do know explicit functions for which the classical communication is exactly of this form, for example, the matrix multiplication function (Raz 2000) and the quadratic character function (Babai *et al.* 1992). In fact, the proofs given in these papers only consider k-party communication, but as we will see in Section 5, they can easily be modified for the case of $\ell \leqslant k$ parties.

5. The quantum communication complexity of GIP

In this section we study the power of our quantum communication model further by looking at the function of generalised inner product (GIP). We will look at general multiparty protocols, where the players' answers can depend on each other. It should be clear how one can define the quantum model for general multiparty computation, where now each player P_j takes as input I_j together with all previous answers $A_1, \dots, A_{j-1}$, and performs a controlled unitary operation. We refrain from giving a formal definition for the general model, since for the circuit lower bounds we need only look at the simultaneous version and, moreover, for our separation we only use a very simple non-simultaneous protocol.

The Generalised Inner Product Function $GIP(X_1, \dots, X_k)$

Let $X_i \in \{0, 1\}^n$. We can think of the k inputs as the rows of a $k \times n$ matrix. Then $GIP(X_1, \dots, X_k)$ is equal to the number (mod 2) of the columns of the matrix that have all elements equal to 1. More formally, using X_i^j to denote the (i, j) element of this matrix (which is equal to the j-th bit of X_i), we have

$$GIP(X_1, \dots, X_k) = \sum_{j=1}^{n}\prod_{i=1}^{k} X_i^j (\text{mod } 2).$$

The function GIP has been studied extensively in the multiparty communication model. Babai *et al.* (Babai *et al.* 1992) showed an $\Omega(n/2^{2k})$ lower bound in the general multiparty model, where the answers of the players may depend on previous answers. Chung (Chung 1990) claimed to improve this to $\Omega(n/2^k)$, but the proof is flawed.

It is easy to see that the ℓ-party randomised communication complexity of the function $GIP(X_1, \dots, X_k)$ is at least the ℓ-party randomised communication complexity of $GIP(X_1, \dots, X_\ell)$. If there exists an ℓ-party communication protocol P for the function $GIP(X_1, \dots, X_k)$, we can construct an ℓ-party protocol for $GIP(X_1, \dots, X_\ell)$ by fixing $X_{\ell+1}, \dots, X_k$ to be the $\mathbf{1}$ vectors.

On the other hand, Grolmusz (Grolmusz 1994) described a k-party communication protocol for $GIP(X_1, \dots, X_k)$ with communication $(2k-1)\left\lceil n/(2^{k-1} - 1)\right\rceil$. This is a slightly

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

non-simultaneous protocol, since player 1 first outputs a message and then, depending on that message, the other players output their answers simultaneously.

Using our simulation from Theorem 1, we can show that there exists a quantum $\lceil (k-1)/2 \rceil + 1$-party communication protocol for GIP with the same communication and the same correctness probability (we can assume without loss of generality that k is odd). For $k = \log(n+1)+1$, the quantum communication is only $O(\log n)$. The best-known classical protocol for $k = \log(n+1)+1$ has communication $O(\sqrt{n})$. Showing that this bound is optimal, or in other words improving the lower bound for GIP to $\Omega(n/2^k)$ would establish an exponential separation between randomised and quantum multiparty communication complexity.

Theorem 3. Let $k = \log(n+1)+1$ and $\ell = \lceil (k-1)2 \rceil + 1$, and let δ be a constant. Then the ℓ-party quantum communication complexity of $GIP(X_1, \dots, X_k)$ is $QC_\delta^\ell(GIP) = O(\log n)$.

Proof. Grolmusz (Grolmusz 1994) showed a k-party protocol for $GIP(X_1, \dots, X_k)$ with communication

$$(2k-1)\left\lceil \frac{n}{2^{k-1}-1} \right\rceil .$$

Taking $k = \log(n+1)+1$, the communication cost is $(2k-1)$ bits. In fact, the first player communicates a $(k-1)$-bit string and a single bit and the other $(k-1)$ players simultaneously communicate a single bit each. The final answer is the parity of the single bits. The single bits of the $(k-1)$ players depend on the message of the first player, so this is not a simultaneous messages protocol. We are going to simulate exactly the protocol of Grolmusz by using only $\lceil (k-1)2 \rceil + 1$ quantum players.

Quantum protocol

Let $I_1, \dots, I_k$ be the inputs to the k players in Grolmusz's protocol and $A_1, \dots, A_k$ the messages they output. As we said earlier, $A_1 \in \{0,1\}^{k-1} \times \{0,1\}$, and for $i = 2, \dots, k$, we have A_i is a bit that depends on (I_i, A_1). The idea is to use the first quantum player to simulate exactly the first classical player, and for the other players we use our simulation technique from Section 3. Our protocol is non-simultaneous since the answers of the quantum players $2, \dots, k$ depend on the classical answer of player 1. More specifically:

— In the first round, we create the states

$$|\phi_1\rangle = |1, I_1\rangle , \quad |\phi_i\rangle = |i\rangle\, |i, I_i\rangle + |i+1\rangle\, |i+1, I_{i+1}\rangle , \quad i = 2, 4, \dots, k-1 .$$

— In the second round, quantum player 1 first outputs the classical string A_1. The other players read the classical string A_1 and proceed to perform the mapping

$$T : |j, I_j\rangle\, |0\rangle \mapsto |j, I_j\rangle\, (-1)^{A_j}\, |0\rangle .$$

— In the third round, we have the classical string A_1 and the states

$$|\chi_i\rangle = |i\rangle\, |i, I_i\rangle\, (-1)^{A_i}\, |0\rangle + |i+1\rangle\, |i+1, I_{i+1}\rangle\, (-1)^{A_{i+1}}\, |0\rangle , \; i = 2, \dots, k-1 .$$

The protocol quantumly 'erases' the inputs resulting in the states

$$|\psi_i\rangle = (-1)^{A_i}\, |i\rangle + (-1)^{A_{i+1}}\, |i+1\rangle .$$

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

By measuring in the basis $\{|i\rangle \pm |i+1\rangle\}$, we can compute $A_i \oplus A_{i+1}$ exactly and hence compute the parity of all the bits as in the classical protocol.

The correctness of the protocol is $1/2 + \delta$, which is the same as in the classical case. □

6. Conclusions

We have defined a model for quantum multiparty communication with quantum inputs and proved a simulation theorem between the quantum and classical models. This enabled us to reduce the question of showing that a function is outside the circuit complexity class $SYM(\log n, 2^{\omega(polylogn)})$ to the question of finding an explicit function f for which the ℓ-party average case quantum communication complexity is $\Omega(n/2^{\ell} + \log\delta)$. Note that we know functions for which the classical communication is of that form (for example, the matrix multiplication function (Raz 2000) and the quadratic character function (Babai *et al.* 1992)); in other words, we are looking for a function for which quantum communication does not help.

References

Aaronson, S. (2004) Lower bounds for local search by quantum arguments. In: *Proceedings of 36th ACM STOC*.

Aaronson, S. (2005) Quantum Computing, Postselection, and Probabilistic Polynomial-Time. In: *Proceedings of the Royal Society A* **461** (2063) 3473–3482.

Aharonov, D. and Regev, O. (2003) A Lattice Problem in Quantum NP. In: *Proc. 44th IEEE FOCS*.

Aharonov, D. and Regev, O. (2004) Lattice problems in NP ∩ coNP. In: *Proc. 45th IEEE FOCS*.

Babai, L., Nisan, N. and Szegedy, M. (1992) Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *Journal of Computer and System Sciences* **45** (2) 204–232.

Bar-Yossef, Z., Jayram, T. S. and Kerenidis, I. (2004) Exponential Separation of Quantum and Classical One-Way Communication Complexity. *Proceedings of 36th ACM STOC*.

Beigel, R. and Tarui, J. (1994) On ACC. *Computational Complexity* **4** (4) 350–366.

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

Chandra, A. K., Furst, M. L. and Lipton, R. J. (1983) Multi-party protocols. In: *Proceedings of the 15th annual ACM STOC*.

Chung, F. (1990) Quasi-random classes of hypergraphs. *Random Structures and Algorithms* **1** (4) 363–382.

Gavinsky, D., Kempe, J., Kerenidis, I., Raz, R. and de Wolf, R. (2007) Exponential separations for one-way quantum communication complexity, with applications to cryptography. *Proceedings of ACM STOC*.

Grolmusz, V. (1994) The BNS Lower Bound for Multi-Party Protocols is Nearly Optimal. *Information and Computation* **112** (1) 51–54.

Hastad, J. and Goldmann, M. (1991) On the power of small-depth threshold circuits. *Computational Complexity* **1** 113–129.

Kerenidis, I. and de Wolf, R. (2003) Exponential Lower Bound for 2-Query Locally Decodable Codes via a Quantum Argument. In: *Proceedings of the 15th annual ACM STOC*.

Kushilevitz, E. and Nisan, N. (1997) *Communication complexity*, Cambridge University Press.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press

M. Nielsen and I. Chuang. (2000) *Quantum Computation and Quantum Information*, Cambridge University Press.

Raz, R. (1999) Exponential separation of quantum and classical communication complexity. In: *Proceedings of 31st ACM STOC*.

Raz, R. (2000) The BNS-Chung Criterion for multi-party communication complexity. *Journal of Computational Complexity* **9** (2) 113–122.

Wehner, S. and de Wolf, R. (2005) Improved Lower Bounds for Locally Decodable Codes and Private Information Retrieval. In 32nd ICALP. *Springer-Verlag Lecture Notes in Computer Science* **3580** 1424–1436.

de Wolf, R. (2005) Lower Bounds on Matrix Rigidity via a Quantum Argument. In: 33rd International Colloquium on Automata, Languages and Programming (ICALP'06). *Springer-Verlag Lecture Notes in Computer Science* **4051** 62–71.

Yao, A. C. (1990) On ACC and threshold circuits. In: *Proc. 31st Ann. IEEE FOCS*.

https://doi.org/10.1017/S0960129508007263 Published online by Cambridge University Press