Exponential Separation of Quantum and Classical Non-Interactive Multi-Party Communication Complexity

Dmitry Gavinsky [*] Pavel Pudlák[†]

December 4, 2007

Abstract

We give the first exponential separation between quantum and classical multi-party communication complexity in the (non-interactive) one-way and simultaneous message passing settings.

For every k, we demonstrate a relational communication problem between k parties that can be solved exactly by a quantum simultaneous message passing protocol of cost $O(\log n)$ and requires protocols of cost n^{c/k^2}, where $c > 0$ is a constant, in the classical non-interactive one-way message passing model with shared randomness and bounded error. Thus our separation of corresponding communication classes is superpolynomial as long as $k = o\left(\sqrt{\frac{\log n}{\log\log n}}\right)$ and exponential for $k = O(1)$.

1 Introduction

In this paper we study quantum computation from the perspective of communication complexity. In the two-party model, defined by Yao [Y79], two players are to compute a function of two variables x and y, each knowing only one of the variables. The complexity measure is the number of bits they need to exchange in the worst case. In general players may use shared randomness.

An important generalization is the multi-party communication complexity. In this paper we shall study the most important version of multi-party communication, the *number on a forehead* model, defined by Chandra, Furst and Lipton [CFL83]. In this case a function of k variables $x_1, \ldots, x_k$ is computed by k players each knowing $k-1$ of the variables, namely player i knows $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$. The definition naturally generalizes to the case of *relational problems* (or *relations*), where for a given input there may be several correct outputs, or none.

Obviously, the case of $k = 2$ players coincides with the standard two-party model. On the other hand, proving lower bounds for $k > 2$ players is usually much harder, since they share some common information.

[*]David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo

[†]Institute of Mathematics, Academy of Sciences, Žitna 25, Praha 1, Czech Republic. Supported by grants A1019401 and 1M0021620808

It has been established that quantum communication is exponentially more efficient in a number of versions of the *two-party model*, see [BCW98, R99, BCWW01, BJK04, GKKRW07, G07]. The model of *multi-party quantum communication* has been defined by Kerenidis [K07]. In this paper we shall give the first exponential separation between quantum and classical multi-party communication complexity.

We shall consider two versions of the *non-interactive* model. In the *one-way message passing* model, the first $k-1$ players send one message each to the k'th player. The latter is supposed to give an answer based on the received messages and his portion of input.[1] In the *simultaneous message passing* (*SMP*) model, each of the k players sends a single message to a *referee*, who is supposed to answer based solely on the received messages. Of course, the model of SMP is, in general, weaker than the one-way model, because the answering side (the referee) does not have free access to any piece of input.

We shall show an exponential separation between quantum and classical probabilistic communication complexity in these models. Specifically, for every k we construct a relation and a quantum protocol that uses $O(\log n)$ quantum bits to solve the problem *exactly* in the SMP model, and prove that its classical probabilistic communication complexity is $n^{\Omega(1)}$, even if we allow bounded error.

The exponent in the lower bound decreases with the number of players as $1/k^2$, as long as $k < c_1 \cdot \sqrt{\log n}$, $c_1 > 0$. Thus we get superpolynomial separation as long as the number of players is in $o\left(\frac{\log n}{\log\log n}\right)$, and exponential separation for constant number of players. The lower bound still holds for the stronger model of classical non-interactive one-way communication, even if we allow public randomness (our protocol, like any exact protocol, does not need randomness).

2 Definitions and notation

We write log to denote the logarithmic function with base 2.

Let $P \subseteq X_1 \times \cdots \times X_k \times Z$, where $X_1, \ldots, X_k \subseteq \{0,1\}^n$ are the domains of *arguments* and $Z \subseteq \{0,1\}^*$ is the *range* of the relation P. We say that a k-party protocol S solves P with error bounded by ε if the following holds

- S describes behavior (i.e., which message is sent in every possible case, who produces the answer, and when) by the k players and (optionally) the referee.
- If $x_1 \in X_1, \ldots, x_k \in X_k$ are arguments to P such that the set $\left\{z \in Z \middle| (x_1, \ldots, x_k, z) \in P\right\}$ is not empty, and for $1 \leq i \leq k$, the i'th player is given the values of $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$, then the answer $z_0 \in Z$ produced by S is correct (i.e., $(x_1, \ldots, x_k, z_0) \in P$) with probability at least $1-\varepsilon$.

The *cost* of S is the maximum possible total number of bits (classical or quantum) communicated before an answer is produced.

We call a protocol *(non-interactive) one-way* if the first $k-1$ players send at most one message each to the k'th player, and no other communication occurs; after that the player k produces an answer.

[1] Note that we consider the *non-interactive* one-way model, as opposed to the following possible scenario: Alice, Bob and Charlie use a protocol, where Alice sends a message to Bob, *after that* Bob sends a message to Charlie, who in turn produces an answer. Cf. Section 5.

We call a protocol *simultaneous message passing* (*SMP*) if each player sends at most one message to the referee, and no other communication occurs; after that the referee produces an answer.

We shall consider the following problem. The input consists of $k-1$ indices $\alpha_1, \dots, \alpha_{k-1}$ and a string c of n bits. The indices jointly determine a matching on $\{1, \dots, n\}$. The parts of the input are distributed among the k players as usual, thus each of the first $k-1$ players knows $k-2$ indices and c, whereas player k knows all the indices, but does not know c. The goal is to compute $i_1, i_2, c_{i_1} \oplus c_{i_2}$, where (i_1, i_2) is an edge of the matching determined by the indices.

Now we shall describe the problem formally. Let $M_n = (m_i^{(n)})_{i=1}^{t(n)}$ be a family of $t(n)$ edge-disjoint perfect matchings over n nodes and $M = \{M_n\}_{n \in N}$. Since the matchings $m_i^{(n)}$ are disjoint, we have $t(n) \le n$.

Definition 1. Let $2 < k < \log(t(n))$, such that $\log(t(n))$ is a multiple of $k-1$, and let $r(n) \overset{\text{def}}{=} \frac{\log(t(n))}{k-1}$. Let $c \in \{0,1\}^n$ and $\alpha_1, \dots, \alpha_{k-1} \in \{0,1\}^{r(n)}$. Denote by $\circ$ concatenation of binary strings; interpret $\alpha_1 \circ \cdots \circ \alpha_{k-1}$ as an integer between 1 and $2^{(k-1)r(n)}$. Then $\big(\alpha_1, \dots, \alpha_{k-1}, c, (i_1, i_2, c_{i_1} \oplus c_{i_2})\big) \in HMP_M^{(n,k)}$ if $\alpha_1 \circ \cdots \circ \alpha_{k-1} \le t(n)$ and $(i_1, i_2) \in m^{(n)}_{\alpha_1 \circ \cdots \circ \alpha_{k-1}}$.

3 A quantum protocol for $HMP_M^{(n,k)}$

Proposition 1. *There exists a quantum k-party SMP communication protocol that exactly solves $HMP_M^{(n,k)}$ using $O(\log n)$ quantum bits for any M.*

Proof. Recall that $|M_n| \le n$. Consider the following protocol.

- Player 1 sends the quantum state
$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{c_i} |i\rangle$$
to the referee, which is $\lceil \log n \rceil$ quantum bits.

- Player k determines (based on his input) the matching $m^{(n)}_{\alpha_1 \circ \cdots \circ \alpha_{k-1}}$ and sends its index to the referee. That costs $\lceil \log(|M_n|) \rceil \le \lceil \log n \rceil$ (classical) bits.

- The referee performs a projective measurement in the orthogonal basis
$$\left\{ |i_1\rangle \pm |i_2\rangle \big| (i_1, i_2) \in m^{(n)}_{\alpha_1 \circ \cdots \circ \alpha_{k-1}} \right\}.$$
When he obtains $|i_1\rangle + |i_2\rangle$ ($|i_1\rangle - |i_2\rangle$), then $c_{i_1} \oplus c_{i_2} = 0$ ($c_{i_1} \oplus c_{i_2} = 1$, respectively), and the answer is produced accordingly.

∎

4 Lower bound for solving $HMP_M^{(n,k)}$ in the classical model

In this section we show that for some choice of M solving $HMP_M^{(n,k)}$ in the classical non-interactive one-way model allowing bounded error and shared randomness is expensive.

Lemma 4.1. *For every $\varepsilon_1, \varepsilon_2 > 0$ there exists a constant C such that for every k and n the following holds. If a one-way k-party protocol S of cost l uses shared randomness and solves $HMP_M^{(n,k)}$ with error bounded by ε_1, then for any constant ε_2 there exists a protocol S', satisfying*

- *S' solves $HMP_M^{(n,k)}$ with error at most $\varepsilon_1 + \varepsilon_2$, for every possible input;*
- *S' has communication cost at most $(\log n)^C \cdot l$;*
- *the senders (first $k-1$ players) are deterministic, the recipient (k'th player) may use private randomness.*

Intuitively, the lemma says that we can "partially derandomize" the protocol S, preserving its correctness in distribution-free setting (which would not be the case if we simply applied the Min-Max Theorem).

Proof of Lemma 4.1. We shall apply a result of Newman [N91], Proposition 1.1, that shows that the number of shared random bits can be reduced to constant time the logarithm of the input size. More precisely, there exists absolute constants c_1, c_2 such that for every $\varepsilon, \delta > 0$, every protocol that uses l communication bits and solves the problem with error ε can be replaced by a protocol that uses at most $c_1 l$ communication bits, $c_2 \log n$ random bits (where n is the input size) and has error $\leq \varepsilon + \delta$. This theorem was proved only for the two party communication complexity, however the proof is completely general and works for any number of parties and essentially any special way of communication. In particular, the constants c_1, c_2 do not depend on the number of players.

Let S be as suggested by the lemma. Applying Newman's result we conclude that some protocol S_1 uses only $O(\log n)$ shared random bits (and no private randomness), has cost l and solves $HMP_M^{(n,k)}$ with error at most $\varepsilon_1 + \varepsilon_2/2$.

Then there exists a protocol S_2 of cost $l + O(\log n)$, solving the problem with the same error, but with public randomness shared only between the first $k-1$ players (in S_2, one of the senders appends to his message the content of the random string).

Now let us consider the following communication task between the first $k-1$ players: They receive same input as the first $k-1$ players of S_2, and their goal is to produce messages which would, according to S_2, cause the k'th player to produce a correct answer (the k'th player is deterministic in S_2, thus the problem is well-defined). Observe that all $k-1$ players share the knowledge of c, so only the part of input which determines $m \in M_n$ is not available to each player separately. Note also that the protocol S_2 ("restricted" to the first $k-1$ players) solves this problem with error at most $\varepsilon_1 + \varepsilon_2/2$. Recall that $|M_n| \leq n$. We apply Newman's theorem for the second time, concluding that there exists a protocol allowing the first $k-1$ players to accomplish their task with success probability at least $1 - \varepsilon_1 - \varepsilon_2$ using $O(\log(\log(|M_n|))) = O(\log \log n)$ shared random bits.

Therefore, there exists a protocol S_3 of cost $l + O(\log n)$ that solves $HMP_M^{(n,k)}$ with error at most $\varepsilon_1 + \varepsilon_2$, uses $O(\log \log n)$ random bits shared between the first $k-1$ players and no other randomness.

Finally, let us derandomize the first $k-1$ players of S_3. They share $O(\log \log n)$ random bits, they can take one of $(\log n)^{O(1)}$ possible values. Define S' as follows. Let each of the first $k-1$ players send the sequence of messages which he would send, according to S_3, with respect to all possible values of random bits. The recipient (k'th player) randomly chooses one possible value of the random bits, considers only those parts of the messages which correspond to that value and acts according to S_3. This protocol satisfies the requirement of the lemma. $\blacksquare_{\textit{Lemma 4.1}}$

4.1 On the families of perfect matchings

We will construct a family M' of perfect matchings that makes $HMP_{M'}^{(n,k)}$ hard for the classical model. Our construction is based on some results in extremal graph theory concerning the number of edges in graphs with forbidden subgraphs. Let

$$ex(n, \{G_1, \ldots, G_j\}),$$

denote the maximal number of edges that a graph on n vertices can have without containing any of the graphs $G_1, \ldots, G_j$ as (not necessarily induced) graphs. These numbers have been studies especially for cycles C_d. By a result of Bondy and Simonovits [BS74]

$$ex(n, \{C_{2d}\}) \leq 90dn^{1+1/d}.$$

Lower bounds of the form

$$ex(n, \{C_3, C_4, \ldots, C_{2d}\}) = \Omega(n^{1+2/(3d+\nu)}),$$

have been shown by Lubotzki, Phillips and Sarnak (with $\nu = 3$) [LPS88] and Lazebnik, Ustimenko and Woldar [LUW95] (with $\nu = -2$ and $\nu = -3$, depending on the parity of ν). These bounds were obtained using explicit constructions. These constructions are, moreover, bipartite regular graphs (i.e., the degrees of all vertices are equal).

Our main combinatorial lemma is an immediate corollary of these results.

Lemma 4.2. *For every d and every prime power t there exist a number n and a bipartite t-regular graph $G_{n,d}$ on n vertices such that*

1. *$n \leq t^{\frac{3}{2}d}$,*
2. *$G_{n,d}$ can be decomposed into t disjoint perfect matchings,*
3. *every set of edges E spans at least $|E|^{1-1/(d+1)}/90d$ vertices.*

Proof. In [LUW95] Lazebnik *et al.* constructed t-regular bipartite graphs satisfying the first condition and such that they do not contain C_{2d}. It is well-known that regular bipartite graphs can be decomposed into edge-disjoint perfect matchings. (Namely, one can easily check that the assumption of Hall's theorem is satisfied, hence the graph contains a perfect matching. If we delete the edges of this matching the remaining graph is still bipartite and regular.) The condition about forbidden cycles implies 3., according to the result of Bondy and Simonovits [BS74]. $\blacksquare$

For our lower bound on k-party communication complexity we need the number of matchings be of the form $t = 2^{r(k-1)}$, therefore we shall consider only powers of 2. For a t of this form, let n and $G_{n,2k}$ be the number and the graph from the lemma. We shall define a family of perfect disjoint matchings $M_{n,k} = (m_i^{(n,k)})_{i=1}^t$ to be the perfect matchings of $G_{n,2k}$. It would be more natural to parametrize this family by r and k, since for each pair r and k we have one such family of matchings (with $t = 2^{r(k-1)}$ and $n \leq 2^{3k(k-1)r}$). We use n instead of r, since it indicates the size of inputs. For future reference we note that

$$t \geq n^{1/3k}.$$

4.2 Lower bound for $HMP_{M_{n,k}}^{(n,k)}$

First we recall some properties of the *mutual information* of random variables that we shall need in the proof. Let $\mathbf{X}$ and $\mathbf{Y}$ be random variables, then we define their mutual information by

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{X},\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}),$$

where H is entropy. We shall need the following facts:

1. $H(\mathbf{X}|\mathbf{Y}) = \sum_y H(\mathbf{X}|\mathbf{Y}=y) \cdot Pr(\mathbf{Y}=y)$.
2. $I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = \sum_z I(\mathbf{X};\mathbf{Y}|\mathbf{Z}=z) \cdot Pr(\mathbf{Z}=z)$.
3. If $\mathbf{Y}_1, \dots, \mathbf{Y}_n$ are independent, then
$$I(\mathbf{X};\mathbf{Y}_1,\dots,\mathbf{Y}_n) \geq \sum_j I(\mathbf{X};\mathbf{Y}_j).$$

The first fact follows from the definition by direct computation. The second one is a consequence of the first one. To prove the third fact, write

$$I(\mathbf{X};\mathbf{Y}_1,\dots,\mathbf{Y}_n) = H(\mathbf{Y}_1,\dots,\mathbf{Y}_n) - H(\mathbf{Y}_1,\dots,\mathbf{Y}_n|\mathbf{X}).$$

Then express the first term as the sum of entropies and apply the subadditivity of entropy to the second term.

We shall also use Markov's inequality in the following form. If $0 \leq \mathbf{X} \leq \beta$ and $0 \leq \alpha < \beta$, then

$$Pr(\mathbf{X} \geq \alpha) \geq \frac{E(\mathbf{X}) - \alpha}{\beta - \alpha},$$

where E denotes expectation.

Theorem 4.3. *For every $\varepsilon > 0$ there exists a constant $\gamma > 0$ such that for every $k \geq 2$, $k = o\left(\sqrt{\frac{\log n}{\log\log n}}\right)$, any non-interactive one-way protocol solving $HMP_{M_{n,k}}^{(n,k)}$ with error $\frac{1}{2} - \varepsilon$ has to communicate at least n^{γ/k^2} bits of information.*

Proof of Theorem 4.3. Let n be fixed. Recall that $t \geq n^{1/3k}$ and $r = \log t/(k-1)$.

Let S be a k-party protocol of cost l, satisfying the theorem requirement. Let $1/2 - \varepsilon$ be the guaranteed upper bound on the error probability of S. Let S' be another protocol with error at most $1/2 - \varepsilon/2$, as guaranteed by Lemma 4.1.

Let $c \in \{0,1\}^n$ and consider the $2^{(k-2)r}$ inputs of the form

$$(\alpha_1, \ldots, \alpha_{k-2}, \sum_{i=1}^{k-2} \alpha_i, c).$$

We interpret strings α_i in the sum as vectors in GF_2^r. Notice that for *any* subset of $k-2$ of the first $k-1$ coordinates we get all $2^{(k-2)r}$ values of the $k-2$-tuples of strings. Let w be concatenation of the strings of messages that the first $k-1$ players send to player k for these inputs, assuming they are using the protocol S'. Since each of these players can see only $k-2$ coordinates from the first $k-1$ coordinates, the string w encodes all messages that they ever send for the given string c.

Recall that by Lemma 4.1 the first $k-1$ players in S' are deterministic, and therefore for every tuple $(\alpha_1, \ldots, \alpha_{k-1})$ we can, using w, prepare the $k-1$ messages which are received by the k'th player when the input is $(\alpha_1, \ldots, \alpha_{k-1}, c)$ (and the input of the k'th player himself is $\alpha_1, \ldots, \alpha_{k-1}$, i.e., the encoding of the matching). Consequently, for each matching $m \in M_{n,k}$ it is possible to obtain, using the information contained in w, a triple (i_1, i_2, e), such that $(i_1, i_2) \in m$ and $e = c_{i_1} \oplus c_{i_2}$ with probability at least $\frac{1}{2} + \frac{\varepsilon}{2}$. Consider the following algorithm that constructs a string of pairs of indices A and a string of bits B using w as the input.

1. Let A and B be empty strings initially.
2. Let $m \in M_{n,k}$, such that every edge in m has at most one endpoint in the support of the pairs of A. If no such matching exists, **halt**.
3. Using w, get a triple (i_1, i_2, e), such that $(i_1, i_2) \in m$ and $e = c_{i_1} \oplus c_{i_2}$ with probability at least $\frac{1}{2} + \frac{\varepsilon}{2}$ (this is the answer that player k produces given the messages of the players $1, \ldots, k-1$ and the matching m).
4. Let $A := A \circ \{i_1, i_2\}$ and $B := B \circ e$.
5. Return to Step 2.

It follows from the properties of $M_{n,k}$ that if we take one edge from each $m' \in M_{n,k}$ then at least $t^{1-\frac{1}{2k+1}}/180k$ vertices are touched by those edges. Therefore, as long as $|A| < t^{1-\frac{1}{2k+1}}/180k$, it is possible to find $m \in M_{n,k}$ which satisfies the requirement of Step 2. On the other hand, each iteration of the algorithm adds at most 2 new elements to A, therefore the algorithm always performs at least $\frac{1}{2}t^{1-\frac{1}{2k+1}}/180k$ iterations. Let s be the least number of the steps of the algorithm (the lengths of the strings A and B), thus

$$s \geq t^{1-\frac{1}{2k+1}}/360k. \tag{1}$$

We shall show that the mutual information between (A, B) and c is $\Omega(s)$. Intuitively it seems clear, because the pairs A chosen by the algorithm form a tree, thus the bits $c_{i_1} \oplus c_{i_2}$ are independent, and $e = c_{i_1} \oplus c_{i_2}$ with probability at least $\frac{1}{2} + \frac{\varepsilon}{2}$. Notice, however, that the pairs in A and the bits in B are not independent, as we are choosing next matching according to the outcome of the previous stage. Therefore a formal proof of this fact is needed.

Consider the following random variables.

- $\mathbf{C}$ – the uniform distribution on the strings $c \in \{0,1\}^n$.
- $\mathbf{W}$ – the distribution on the strings w when the uniform distribution on the strings c is uniform; thus $\mathbf{W}$ is a function of $\mathbf{C}$.
- $\mathbf{A}$ and $\mathbf{B}$ – the distribution on the strings produced by the above algorithm when the distribution on strings c is uniform; these random variables can be viewed as functions of $\mathbf{W}$ and some random variable independent of $\mathbf{C}$ (the random bits of player k).

The assumption about $\mathbf{A}$ and $\mathbf{B}$ can be stated as follows. For every $j = 1, \ldots, s$,

$$Pr(\mathbf{B}_j = \mathbf{C}_{(\mathbf{A}_j)_1} \oplus \mathbf{C}_{(\mathbf{A}_j)_2}) \geq \frac{1}{2} + \frac{\varepsilon}{2}.$$

Our proof of the theorem is based on estimating $I(\mathbf{A}, \mathbf{B}; \mathbf{C})$ in two ways. The upper bound is easy:

$$I(\mathbf{A}, \mathbf{B}; \mathbf{C}) \leq I(\mathbf{W}; \mathbf{C}) \leq H(\mathbf{W}) \leq |\mathbf{W}|, \tag{2}$$

since $\mathbf{A}, \mathbf{B}$ are functions of the random variable $\mathbf{W}$ and a random variable independent of $\mathbf{C}$.

To prove a lower bound on $I(\mathbf{A}, \mathbf{B}; \mathbf{C})$, we consider two cases.

(1) $H(\mathbf{C}|\mathbf{A}) < n - \xi s$. Here $\xi > 0$ is a sufficiently small fraction of ε that will be specified later. In this case

$$I(\mathbf{A}, \mathbf{B}; \mathbf{C}) \geq I(\mathbf{A}; \mathbf{C}) = H(\mathbf{C}) - H(\mathbf{C}|\mathbf{A}) > n - (n - \xi s) = \xi s.$$

(2) $H(\mathbf{C}|\mathbf{A}) \geq n - \xi s$. Observe that according to the chaining rule

$$I(\mathbf{A}, \mathbf{B}; \mathbf{C}) = I(\mathbf{A}; \mathbf{C}) + I(\mathbf{B}; \mathbf{C}|\mathbf{A}) \geq I(\mathbf{B}; \mathbf{C}|\mathbf{A}).$$

Hence it suffices to estimate $I(\mathbf{B}; \mathbf{C}|\mathbf{A})$.

Let $\mathbf{D}$ be the random variable whose value is the number of indices j such that $\mathbf{B}_j = \mathbf{C}_{(\mathbf{A}_j)_1} \oplus \mathbf{C}_{(\mathbf{A}_j)_2}$. The assumption about the correctness of the protocol implies that

$$E(\mathbf{D}) \geq (1/2 + \varepsilon/2)s,$$

Consider the mapping

$$A \mapsto E(\mathbf{D}|\mathbf{A} = A)$$

as a random variable. Let

$$\Delta_1(A) \equiv_{df} E(\mathbf{D}|\mathbf{A} = A) \geq (1/2 + \varepsilon/4)s. \tag{3}$$

By Markov's inequality,

$$Pr(\Delta_1(\mathbf{A})) = \sum_{A;\Delta_1(A)} Pr(\mathbf{A} = A) \geq \frac{\varepsilon/2}{1 - \varepsilon/2} \geq \varepsilon/2. \tag{4}$$

Let

$$\Delta_2(A) \equiv_{df} H(\mathbf{C}|\mathbf{A} = A) \geq n - \frac{4}{\varepsilon}\xi s.$$

In a similar fashion, we get

$$Pr(\Delta_2(\mathbf{A})) \geq 1 - \frac{\varepsilon}{4}.$$

Whence

$$Pr(\Delta_2(A) \wedge \Delta_2(A) \geq \varepsilon/2 - \varepsilon/4 = \varepsilon/4.$$

By (4),

$$I(\mathbf{B};\mathbf{C}|\mathbf{A}) = \sum_a I(\mathbf{B};\mathbf{C}|\mathbf{A}=A)\cdot Pr(\mathbf{A}=A) \geq \frac{\varepsilon}{4}\cdot \min_{A;\Delta_1(A)\wedge\Delta_2(A)} I(\mathbf{B};\mathbf{C}|\mathbf{A}=A). \tag{5}$$

So it remains to estimate $I(\mathbf{B};\mathbf{C}|\mathbf{A}=A)$ for A satisfying $\Delta_1 \wedge \Delta_2$.

Let such an A be fixed. Let $\mathbf{C'}_j$ be the random variables defined as follows. For $j = 1,\dots,s$, let $\mathbf{C'}_j = \mathbf{C}_{i_1} \oplus \mathbf{C}_{i_2}$ where (i_1, i_2) is the j-th pair of a. For the rest of indices j, we set each $\mathbf{C'}_j$ to be equal to $\mathbf{C}_i$ for some i, so that the variables $\mathbf{C'}_j$ are independent. Then the information contained in $\mathbf{C}$ and $\mathbf{C'}$ is the same, so we can replace the first by the second. Thus

$$I(\mathbf{B};\mathbf{C}|\mathbf{A}=A) = I(\mathbf{B};\mathbf{C'}|\mathbf{A}=A) \geq \sum_j I(\mathbf{B};\mathbf{C'}_j|\mathbf{A}=A) \geq$$

$$\sum_{j=1}^{s} I(\mathbf{B};\mathbf{C'}_j|\mathbf{A}=A) \geq \sum_{j=1}^{s} I(\mathbf{B}_j;\mathbf{C'}_j|\mathbf{A}=A).$$

By $\Delta_1(A)$ (and Markov's inequality again), there are at least $\frac{\varepsilon}{4}s$ indices j, $1 \leq j \leq s$, satisfying

$$Pr(\mathbf{B}_j = \mathbf{C}'_j|\mathbf{A}=A) \geq \frac{1}{2} + \frac{\varepsilon}{8}. \tag{6}$$

By $\Delta_2(A)$,

$$\sum_j H(\mathbf{C}'_j|\mathbf{A}=A) \geq H(\mathbf{C}'|\mathbf{A}=A) = H(\mathbf{C}|\mathbf{A}=A) \geq n - \frac{4\xi}{\varepsilon}s.$$

Hence there are at least $\geq n - \frac{8\xi}{\varepsilon}s$ indices j, $1 \leq j \leq n$ such that

$$H(\mathbf{C}'_j|\mathbf{A}=A) \geq 1/2. \tag{7}$$

Thus there are at least $\frac{\varepsilon}{4}s - \frac{8\xi}{\varepsilon}s$ indices j, $1 \leq j \leq s$ that satisfy both (6) and (7). Setting $\xi = \frac{\varepsilon^2}{64}$, this number is $\frac{\varepsilon}{8}s$. For such indices $I(\mathbf{B}_j;\mathbf{C'}_j|\mathbf{A}=A) \geq \delta$, where $\delta > 0$ depends only on ε, whence

$$I(\mathbf{B};\mathbf{C'}|\mathbf{A}=A) \geq \frac{\varepsilon\delta}{8}s.$$

By (5) and (1) we have

$$I(\mathbf{A},\mathbf{B};\mathbf{C}) \geq \frac{\varepsilon^2\delta}{32}s \geq \eta t^{1-\frac{1}{2k+1}}/k. \tag{8}$$

where $\eta = \frac{\varepsilon^2\delta}{32\cdot 360}$. To get our lower bound on the communication complexity, we shall compare the bounds (2) and (8). Recall that w consists of $2^{(k-2)r}$ messages, each having length at most $(\log n)^C \cdot l$, for some constant C. Thus

$$I(\mathbf{A},\mathbf{B};\mathbf{C}) \leq |\mathbf{W}| \leq 2^{(k-2)r}(\log n)^C \cdot l = 2^{(k-2)\frac{\log t}{k-1}}(\log n)^C \cdot l =$$

$$t^{\frac{k-2}{k-1}}(\log n)^C \cdot l \leq t^{1-\frac{1}{k-1}}(\log n)^C \cdot l.$$

Comparing this with the lower bound (8), we get

$$l \geq \frac{\eta t^{\frac{1}{k-1}-\frac{1}{2k+1}}}{k \cdot (\log n)^C} \geq \frac{\eta n^{\frac{1}{3k}\left(\frac{1}{k-1}-\frac{1}{2k+1}\right)}}{k \cdot (\log n)^C} \geq \frac{\eta n^{\frac{1}{6k^2}}}{k \cdot (\log n)^C} \geq n^{\gamma/k^2},$$

for a sufficiently small constant γ, as $k^2 \in o\left(\frac{\log n}{\log\log n}\right)$. ■ *Theorem 4.3*

The theorem together with the protocol given in Proposition 1 for Proposition 1 leads to the following corollary:

Corollary 4.4. *For $k(n) = o\left(\sqrt{\frac{\log n}{\log\log n}}\right)$, there exists a k-party relational communication problem that can be solved exactly by a quantum simultaneous message passing protocol of cost $O(\log n)$ and requires superpolynomially more expensive protocols in the model of probabilistic non-interactive one-way communication with public randomness. For $k = O(1)$ we get an exponential gap.*

5 Open problems

- Extend the statement of Corollary 4.4 to bigger values of k.
- Give a separation similar to the one shown here through a (partial) function. How much can be saved by using quantum communication for total functions?
- Give a separation for the multi-party interactive setting. Even the case of three players and one-way interactive message passing (i.e., Alice speaks to Bob, after that Bob speaks to Charlie, who, in turn, responds) looks very interesting.

Acknowledgments

We would like to thank Michal Koucký and Jiří Sgall for useful discussions about the problem considered in this paper.

Part of this work was done while D. Gavinsky was visiting the Institute of Mathematics, CAS in Prague.

References

[BCW98] H. Buhrman, R. Cleve and A. Wigderson. Quantum vs. Classical Communication and Computation. *Proceedings of the 30th Symposium on Theory of Computing, pp. 63-68*, 1998.

[BCWW01] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf. Quantum Fingerprinting. *Physical Review Letters 87(16), article 167902*, 2001.

[BJK04] Z. Bar-Yossef, T. S. Jayram and I. Kerenidis. Exponential Separation of Quantum and Classical One-Way Communication Complexity. *Proceedings of 36th Symposium on Theory of Computing, pp. 128-137*, 2004.

[BS74] J. Bondy and M. Simonovits. Cycles of Even Length in Graphs. *Journal of Combinatorial Theory, Series B, 16, pp. 87-105*, 1974.

[CFL83] A. Chandra, M. Furst and R. Lipton. Multi-party protocols. *Proceedings of the 15th Symposium on Theory of Computing, pp. 94-99*, 1983.

[G07] D. Gavinsky. Classical Interaction Cannot Replace a Quantum Message. *Submitted, http://arxiv.org/abs/quant-ph/0703215, http://eccc.hpi-web.de/eccc-reports/2007/TR07-058/*, 2007.

[GKKRW07] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz and R. de Wolf. Exponential Separations for One-Way Quantum Communication Complexity, with Applications to Cryptography. *Proceedings of the 39th Symposium on Theory of Computing*, 2007.

[K07] I. Kerenidis. Quantum Multiparty communication complexity and circuit lower bounds. *4th Annual Conference on Theory and Applications of Models of Computation*, 2007.

[LPS88] A. Lubotzki, R. Phillips and P. Sarnak. Ramanujan Graphs. *Combinatorica 8, pp. 261-277*, 1988.

[LUW95] F. Lazebnik, V. Ustimenko and A. Woldar. A New Series of Dense Graphs of High Girth. *Bulletin of AMS 32, pp. 73-79*, 1995.

[N91] I. Newman. Private vs. Common Random Bits in Communication Complexity. *Information Processing Letters 39(2), pp. 67-71*, 1991.

[R99] R. Raz. Exponential Separation of Quantum and Classical Communication Complexity. *Proceedings of the 31st Symposium on Theory of Computing, pp. 358-367*, 1999.

[Y79] A. C-C. Yao. Some Complexity Questions Related to Distributed Computing. *Proceedings of the 11th Symposium on Theory of Computing, pp. 209-213*, 1979.