

Auxiliary Shared Resources in Quantum and Classical Communication

Dmitry Gavinsky

University of Calgary

This talk is based on:

[GKW04] D. Gavinsky, J. Kempe and R. de Wolf. *Quantum communication cannot simulate a public coin.*

[G05] D. Gavinsky. *A Note on Shared Randomness and Shared Entanglement in Communication.*

Communication Setups

▶ 1-Way Communication:

- ▶ **Alice** receives x and sends a message to **Bob**;
- ▶ **Bob** receives y , reads the message from **Alice** and produces the final output.

▶ Simultaneous Message Passing:

- ▶ **Alice** receives x and sends a message to the **referee**;
- ▶ (at the same time) **Bob** receives y and sends a message to the **referee**;
- ▶ the **referee** reads the messages and produces the final output.

Models' Variations

- ▶ **Communication with shared randomness:** Alice and Bob share a sequence of random bits (fair coin flips).
- ▶ **Quantum communication:** The parties are allowed to send quantum messages; the recipient performs a POVM measurement in order to produce the final output.
- ▶ **Communication with shared entanglement:** Alice and Bob share a number of pairs of entangled qubits (w.l.g., EPR pairs).

Remark

Shared entanglement can be used when communication is classical, as well as shared randomness can be used with quantum communication channels.

Communication Cost

A **communication protocol** describes the behavior of all the participants (says what output each of them produces in response to every possible input).

The total number of (qu)bits sent by all the parties is called the **cost** of the protocol.

For a relation $P \subset X \times Y \times R$, its **communication cost** in a given model is the minimum cost of a protocol in the model which produces a final output $r \in R$ s.t. $(x, y, r) \in P$ with **probability at least $2/3$** , for every possible $x \in X$ and $y \in Y$ given to Alice and Bob, correspondingly.

Models of Interest:

- ▶ R_{pub}^{\parallel} – Classical simultaneous messages with shared randomness.
- ▶ Q^{\parallel} – Quantum simultaneous messages.

Abusing the notation, we will use expressions like “ $Q^{\parallel}(P)$ ” and “ $P \in Q^{\parallel}$ ” (the former addresses the communication cost of P in Q^{\parallel} and the latter means that $Q^{\parallel}(P) \in \text{poly}(\log n)$).

Was known before: Bar-Yossef, Jayram and Kerenidis have demonstrated a relation K s.t. $K \in Q^{\parallel}$ but $R_{pub}^{\parallel}(K) \in \Omega(\sqrt{n})$.

We show: There exists a relation solvable in 0-error setting in R_{pub}^{\parallel} , but not solvable in 0-error in Q^{\parallel} .

Our Relation P

Input: (Alice) $x \in \{0, 1\}^n$, (Bob) $y, s \in \{0, 1\}^n$ with $|s| = n/2$;

Output: Any (i, x_i, y_i) s.t. $s_i = 1$.

0-error Protocol for P in R_{pub}^{\parallel}

For a randomly chosen $i \in \{1, \dots, n\}$:

- ▶ Alice sends (i, x_i) to the referee;
- ▶ Bob sends (y_i, s_i) to the referee;
- ▶ if $s_i = 1$ then the referee is able to produce a correct output (this happens with probability $1/2$).

By repeating 2 times in parallel, the error is reduced to $1/4$.

P Is Hard for Q^{\parallel} for 0-error

Suppose that we have a protocol of cost s .

- ▶ Considering the message which Alice sends to the referee, let a_i be the probability that the referee can 0-error predict x_i from the message. We show that for some $s_0 \in \{0, 1\}^n$ with $|s_0| = n/2$ it must hold that $\forall i$ with $s_{0i} = 1$, $a_i \leq 2s/n$. We fix $s = s_0$ for the rest of the proof.
- ▶ Considering the message which Bob sends to the referee, let b_i be the probability that the referee can 0-error predict y_i from the message. It must hold that $\sum_{i|s_{0i}=1} b_i \leq s$.

P Is Hard for Q^{\parallel} for 0-error (continued)

We show that the following holds:

Lemma

The probability that the referee can 0-error predict both x_i and y_i simultaneously from the messages received from Alice and Bob is at most $4a_i b_i$.

(A modification of this **tensor lemma** will be used again later.)

So,

$$2/3 \leq \Pr[\text{the protocol is correct}] \leq \sum_{i|s_0=1} 4a_i b_i \leq \frac{8s}{n} \cdot \sum b_i \leq \frac{8s^2}{n},$$

which leads to $s \in \Omega(\sqrt{n})$.

Models of Interest:

- ▶ Q_{pub}^{\parallel} – Quantum simultaneous messages with shared randomness.
- ▶ Q_{ent}^{\parallel} – Quantum simultaneous messages with shared entanglement.

We show: There exists a relation solvable **exactly** in Q_{ent}^{\parallel} but not solvable **either exactly or in 0-error** in Q_{pub}^{\parallel} .

Our Relation MHM_n^M

Let M_n be any family of $n/2$ edge-disjoint matchings on elements $\{1, \dots, n\}$, for all even $n \in \mathbb{N}$.

Definition

For any

$$x = (a^{(A)}, m) \text{ and } y = a^{(B)},$$

where $a^{(A)}, a^{(B)} \in \{0, 1\}^n$ and $m \in M_n$, denote: $a = a^{(A)} \oplus a^{(B)}$ (\oplus stands for bitwise XOR). Then

$$MHM_n^M(x, y) = \{(i, j, b) \mid a_i \oplus a_j = b, (i, j) \in m\}.$$

We will assume an encoding of length $O(\log n)$ for all $m \in M_n$.

Exact Protocol for MHM_n^M in Q_{ent}^{\parallel}

The following protocol is a generalization of that used by Bar-Yossef, Jayram and Kerenidis.

- ▶ Before the communication starts, Alice and Bob share $\lceil \log n \rceil$ pairs of entangled qubits: $\sum_{i \in [n]} |i\rangle |i\rangle$.
- ▶ When Alice receives $x = (a^{(A)}, m)$ she applies the following transformation to her part of the entangled pairs:

$$|i\rangle \rightarrow (-1)^{a_i^{(A)}} |i\rangle.$$

Then she sends her part of the entangled pairs and m to the referee. Similarly, Bob flips the sign of those parts of the superposition $\sum |i\rangle |i\rangle$ which correspond to $a_i^{(B)} = 1$ and sends his part of the entangled state to the referee.

Exact Protocol for MHM_n^M in Q_{ent}^{\parallel} (continued)

- ▶ Referee obtains m and

$$|\varphi\rangle = \frac{1}{\sqrt{n}} \sum_{i \in [n]} (-1)^{a_i} |i\rangle$$

(by “uncomputing” the repetitions $|i\rangle |i\rangle$). He measures the state $|\varphi\rangle$ in the orthogonal basis $\left\{ \frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle) \mid (k, l) \in m \right\}$ and answers $(k, l, 0)$ if $|k\rangle + |l\rangle$ has been observed in the measurement and $(k, l, 1)$ if $|k\rangle - |l\rangle$ has been observed.

Communication cost of the protocol is $O(\log n)$. Simple analysis (similar to that used in [BJK]) shows that the protocol **exactly** solves MHM_n^M in Q_{ent}^{\parallel} .

MHM_n^M Is Hard for Q_{pub}^{\parallel} for 0-error

Suppose that we have a protocol of cost s . The following lower bound technique is similar to the previous one.

- ▶ Fix the input distribution to be uniform, thus getting rid of the shared randomness.
- ▶ For “sufficiently many” $m \in M_n$ the resulting deterministic protocol must be correct with high probability. We show that for one such $m_0 = (e_i)_{i=1}^{n/2}$ the referee returns none of e_i -s with probability higher than $p_0 \in O(s/\sqrt{n})$. Set $m \equiv m_0$.
- ▶ From the Holevo bound and a modification of our tensor lemma, we obtain that $s \in \Omega(n^{1/6})$.

Models of Interest:

- ▶ R_{pub}^{\parallel} (R_{pub}^1) – Classical simultaneous messages (1-way communication) with shared randomness.
- ▶ Q^{\parallel} – Quantum simultaneous messages.

Was known before: Yao has shown that for any boolean f ,

$$Q^{\parallel}(f) \in 2^{O(R_{pub}^{\parallel}(f))} \log n.$$

We show: For any boolean f ,

$$Q^{\parallel}(f) \in 2^{O(R_{pub}^1(f))} \log n.$$

Remark

Public coin **is relevant** in this context; Newman's result establishes equivalence between R_{pub}^1 and R^1 "up to additive log", which becomes critical when exponentiated.

Consider a communication protocol for $f(x, y)$ in R_{pub}^1 of cost s which uses $O(\log n)$ public bits.

Let $a(x, q)$ be the message sent by Alice when her part of the input is x and the public coin content is q . Similarly, let $b(y, a, q)$ be the answer returned by Bob when his part of the input is y , the public coin content is q and the message received from Alice is a .

Simulation idea:

For high enough $k \in 2^{O(s)}$, Alice sends k copies of

$$|\alpha\rangle \stackrel{\text{def}}{=} 2^{-\frac{r}{2}} \cdot \sum_q |q\rangle |a(x, q)\rangle |1\rangle.$$

Bob sends k copies of

$$|\beta\rangle \stackrel{\text{def}}{=} 2^{-\frac{r+s}{2}} \cdot \sum_{q,a} |q\rangle |a\rangle |b(y, a, q)\rangle.$$

The referee estimates the value of $\langle \alpha | \beta \rangle$ and accepts if it is high.

Strength of the Improvement

Our simulation is “more powerful” than that originally suggested by Yao.

We demonstrate a function f , such that

$$R_{pub}^1(f) \in O(\log(\log n))$$

but

$$R_{pub}^{\parallel}(f) \in \Omega(\log n).$$

In other words, membership of f in Q^{\parallel} follows from our simulation technique, while Yao's result would not be sufficient.

- ▶ We know that $Q^1 = Q_{pub}^1 \subseteq R_{ent}^1 = Q_{ent}^1$. Are these classes equal?
- ▶ We were only able to demonstrate that $MHM_n^M \notin Q_{pub}^{\parallel}$ for “don’t know” setting, while we conjecture that the problem is hard for Q_{pub}^{\parallel} in the standard (bounded-error) setting as well.
- ▶ Same for $P \notin Q^{\parallel}$.
- ▶ We have shown our separation using a relation. Can similar results be obtained for a (partial) boolean function? What about a total function?