

Quantum Communication Cannot Simulate a Public Coin

Dmitry Gavinsky
University of Calgary

Joint work with
Julia Kempe and **Ronald de Wolf**

Simultaneous model of communication

- *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.

A *communication protocol* describes the behavior of Alice, Bob and the referee (says what output each of them produces in response to every possible input).

The total number of bits sent to the referee is called the *cost* of the protocol.

Simultaneous model: Variations

- *Simultaneous communication with public coin:* Alice and Bob share a common sequence of random bits (coin flips).
- *Simultaneous quantum communication:* Alice and Bob are allowed to send quantum messages; the referee performs a POVM measurement in order to produce his output (the cost is measured in qubits in this case).

For a relation $P \subset X \times Y \times R$, let $\underline{R}^{\parallel, pub}(P)$ be the minimum cost of a public coin simultaneous protocol allowing the referee to produce $r \in R$ s.t. $(x, y, r) \in P$ with probability at least $2/3$, for every possible $x \in X$ and $y \in Y$ being given to Alice and Bob, correspondingly.

Similarly, let $\underline{Q}^{\parallel}(P)$ be the minimum cost of a quantum protocol for P .

What other people say:

- Bar-Yossef, Jayram and Kerenidis: there exists a relation K , s.t. $Q^{\parallel}(K) \in O(\log n)$, $R^{\parallel, pub}(K) \in \Omega(\sqrt{n})$.
- Yao: for any relation K ,

$$Q^{\parallel}(K) \in 2^{O\left(R^{\parallel, pub}(K)\right)} \log n.$$

What we have to add:

We show a relation P , s.t. $R^{\parallel, pub}(P) \in O(\log n)$, $Q^{\parallel}(P) \in \Omega(\sqrt{n})$, and therefore

- the models of simultaneous communication with public coin and simultaneous quantum communication are *incomparable*;
- the bound by Yao cannot be significantly improved.

Definition of P

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

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

We consider this problem in 0-error (*Las Vegas*) version: the referee may not err, but is permitted to *declare failure* with probability at most $1/3$.

We claim that

$$R^{\parallel, pub}(P) \in O(\log n)$$

but

$$Q^{\parallel}(P) \in \Omega(\sqrt{n}).$$

$$\mathbf{R}^{\parallel, \text{pub}}(\mathbf{P}) \in \mathbf{O}(\log n)$$

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

- 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 probability is reduced to $1/4$.

The protocol is 0-error.

$$Q^{\parallel}(\mathbf{P}) \in \Omega(\sqrt{n})$$

Suppose that we have a protocol of cost m .

- Considering the message which Alice sends to the referee, let a_i be the probability that the referee can 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 $s_{0i} = 1$, $a_i \leq 2m/n$. 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 predict y_i from the message. It must hold that $\sum_{i|s_{0i}=1} b_i \leq m$.
- As we show, the probability that the referee can predict both x_i and y_i simultaneously from the messages received from Alice and Bob is at most $a_i b_i$.

$$Q^{\parallel}(\mathbf{P}) \in \Omega(\sqrt{n})$$

Now we can conclude that

$$\begin{aligned} 2/3 &\leq \Pr[\text{the protocol is correct}] \\ &\leq \sum_{i|s_{0i}=1} a_i b_i \\ &\leq \frac{2m}{n} \cdot \sum b_i \\ &\leq \frac{2m^2}{n}, \end{aligned}$$

which leads to

$$m \in \Omega(\sqrt{n}),$$

as required.

Open Problems

Our result, as well as the backwards separation by Bar-Yossef, Jayram and Kerenidis have only been shown for relational problems.

Can similar separations be established for functions?

There is a *popular conjecture* that the models are incomparable also for *partial* functions, but equal for *total* functions.