

Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity

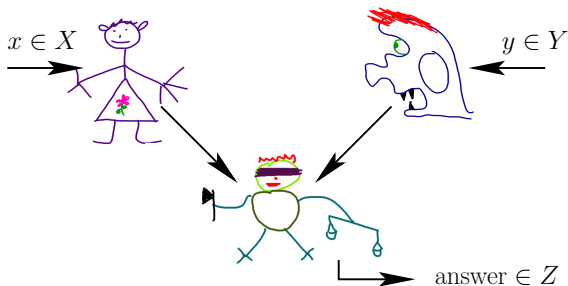
Dmitry Gavinsky

University of Calgary

Joint work with:

Julia Kempe, Oded Regev, Ronald de Wolf

Communication Complexity: the SMP Model



$$P \subseteq X \times Y \times Z$$

$$\text{Is } (x, y, z) \in P ?$$

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 an answer.

Model's Variations

Models: R^{\parallel} , $R^{\parallel, pub}$, Q^{\parallel} , $Q^{\parallel, ent}$,
as well as: $R^{\parallel, ent}$ and $Q^{\parallel, pub}$.

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

Model's Variations

Models: R^{\parallel} , $R^{\parallel, pub}$, Q^{\parallel} , $Q^{\parallel, ent}$,
as well as: $R^{\parallel, ent}$ and $Q^{\parallel, pub}$.

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

Model's Variations

Models: R^{\parallel} , $R^{\parallel, pub}$, Q^{\parallel} , $Q^{\parallel, ent}$,
as well as: $R^{\parallel, ent}$ and $Q^{\parallel, pub}$.

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

Model's Variations

Models: R^{\parallel} , $R^{\parallel, pub}$, Q^{\parallel} , $Q^{\parallel, ent}$,
as well as: $R^{\parallel, ent}$ and $Q^{\parallel, pub}$.

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

Model's Variations

Models: R^{\parallel} , $R^{\parallel, pub}$, Q^{\parallel} , $Q^{\parallel, ent}$,
as well as: $R^{\parallel, ent}$ and $Q^{\parallel, pub}$.

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

Communication Cost

- ▶ A **communication protocol** is a description of the behavior of Alice, Bob and the referee.
- ▶ For a relation $P \subset X \times Y \times Z$, its **communication cost** (in a given model) is the minimum cost of a protocol which produces a good answer **with probability at least $2/3$** , for every possible $x \in X$ and $y \in Y$.
- ▶ Denote by n the total bit-length of the inputs (x and y). We say that a protocol is **efficient** if its communication cost is polylogarithmic in n .

Communication Cost

- ▶ A **communication protocol** is a description of the behavior of Alice, Bob and the referee.
- ▶ For a relation $P \subset X \times Y \times Z$, its **communication cost** (in a given model) is the minimum cost of a protocol which produces a good answer **with probability at least $2/3$** , for every possible $x \in X$ and $y \in Y$.
- ▶ Denote by n the total bit-length of the inputs (x and y). We say that a protocol is **efficient** if its communication cost is polylogarithmic in n .

Communication Cost

- ▶ A **communication protocol** is a description of the behavior of Alice, Bob and the referee.
- ▶ For a relation $P \subset X \times Y \times Z$, its **communication cost** (in a given model) is the minimum cost of a protocol which produces a good answer **with probability at least $2/3$** , for every possible $x \in X$ and $y \in Y$.
- ▶ Denote by n the total bit-length of the inputs (x and y). We say that a protocol is **efficient** if its communication cost is polylogarithmic in n .

Our Results

- ▶ We exhibit a relation P_1 and prove that $R^{\parallel, pub}(P_1) \in O(\log n)$ but $Q^{\parallel}(P_1) \in \Omega(n^{1/3})$.
- ▶ We exhibit a relation P_2 and prove that $R^{\parallel, ent}(P_2) \in O(\log n)$ but $Q^{\parallel, pub}(P_2) \in \Omega((n/\log n)^{1/3})$.
- ▶ Main tool for the lower bounds: new **Quantum State Indistinguishability Lemma**.

Our Results

- ▶ We exhibit a relation P_1 and prove that $R^{\parallel, pub}(P_1) \in O(\log n)$ but $Q^{\parallel}(P_1) \in \Omega(n^{1/3})$.
- ▶ We exhibit a relation P_2 and prove that $R^{\parallel, ent}(P_2) \in O(\log n)$ but $Q^{\parallel, pub}(P_2) \in \Omega((n/\log n)^{1/3})$.
- ▶ Main tool for the lower bounds: new **Quantum State Indistinguishability Lemma**.

Our Results

- ▶ We exhibit a relation P_1 and prove that $R^{\parallel, pub}(P_1) \in O(\log n)$ but $Q^{\parallel}(P_1) \in \Omega(n^{1/3})$.
- ▶ We exhibit a relation P_2 and prove that $R^{\parallel, ent}(P_2) \in O(\log n)$ but $Q^{\parallel, pub}(P_2) \in \Omega((n/\log n)^{1/3})$.
- ▶ Main tool for the lower bounds: new **Quantum State Indistinguishability Lemma**.

Our First Separation: $R^{\parallel, pub}$ vs. Q^{\parallel}

- ▶ **It was known before that** there exists a relation K efficiently solvable in Q^{\parallel} but not in $R^{\parallel, pub}$ (due to Bar-Yossef, Jayram and Kerenidis, STOC'04).
- ▶ **We show that** there exists a relation P_1 efficiently solvable in $R^{\parallel, pub}$ but not in Q^{\parallel} .
- ▶ Therefore, $R^{\parallel, pub}$ and Q^{\parallel} are incomparable.
- ▶ Yao (STOC'03) has shown that any protocol from $R^{\parallel, pub}$ can be simulated in Q^{\parallel} by some exponentially longer protocol.
- ▶ Our result shows that Yao's simulation is essentially optimal.

Our First Separation: $R^{\parallel, pub}$ vs. Q^{\parallel}

- ▶ **It was known before that** there exists a relation K efficiently solvable in Q^{\parallel} but not in $R^{\parallel, pub}$ (due to Bar-Yossef, Jayram and Kerenidis, STOC'04).
- ▶ **We show that** there exists a relation P_1 efficiently solvable in $R^{\parallel, pub}$ but not in Q^{\parallel} .
- ▶ Therefore, $R^{\parallel, pub}$ and Q^{\parallel} are incomparable.
- ▶ Yao (STOC'03) has shown that any protocol from $R^{\parallel, pub}$ can be simulated in Q^{\parallel} by some exponentially longer protocol.
- ▶ Our result shows that Yao's simulation is essentially optimal.

Our First Separation: $R^{\parallel, pub}$ vs. Q^{\parallel}

- ▶ **It was known before that** there exists a relation K efficiently solvable in Q^{\parallel} but not in $R^{\parallel, pub}$ (due to Bar-Yossef, Jayram and Kerenidis, STOC'04).
- ▶ **We show that** there exists a relation P_1 efficiently solvable in $R^{\parallel, pub}$ but not in Q^{\parallel} .
- ▶ Therefore, $R^{\parallel, pub}$ and Q^{\parallel} are **incomparable**.
- ▶ Yao (STOC'03) has shown that any protocol from $R^{\parallel, pub}$ can be simulated in Q^{\parallel} by some exponentially longer protocol.
- ▶ Our result shows that Yao's simulation is **essentially optimal**.

Our First Separation: $R^{\parallel, pub}$ vs. Q^{\parallel}

- ▶ **It was known before that** there exists a relation K efficiently solvable in Q^{\parallel} but not in $R^{\parallel, pub}$ (due to Bar-Yossef, Jayram and Kerenidis, STOC'04).
- ▶ **We show that** there exists a relation P_1 efficiently solvable in $R^{\parallel, pub}$ but not in Q^{\parallel} .
- ▶ Therefore, $R^{\parallel, pub}$ and Q^{\parallel} are incomparable.
- ▶ Yao (STOC'03) has shown that any protocol from $R^{\parallel, pub}$ can be simulated in Q^{\parallel} by some exponentially longer protocol.
- ▶ Our result shows that Yao's simulation is essentially optimal.

Our First Separation: $R^{\parallel, pub}$ vs. Q^{\parallel}

- ▶ **It was known before that** there exists a relation K efficiently solvable in Q^{\parallel} but not in $R^{\parallel, pub}$ (due to Bar-Yossef, Jayram and Kerenidis, STOC'04).
- ▶ **We show that** there exists a relation P_1 efficiently solvable in $R^{\parallel, pub}$ but not in Q^{\parallel} .
- ▶ Therefore, $R^{\parallel, pub}$ and Q^{\parallel} are **incomparable**.
- ▶ Yao (STOC'03) has shown that any protocol from $R^{\parallel, pub}$ can be simulated in Q^{\parallel} by some exponentially longer protocol.
- ▶ Our result shows that Yao's simulation is **essentially optimal**.

Our Relation P_1

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. $s_i = 1$.

Protocol for P_1 in $R^{\parallel, pub}$

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 the protocol 2 times in parallel, the error can be reduced to $1/4$.

Our Relation P_1

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. $s_i = 1$.

Protocol for P_1 in $R^{\parallel, pub}$

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 the protocol 2 times in parallel, the error can be reduced to $1/4$.

Our Relation P_1

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. $s_i = 1$.

Protocol for P_1 in $R^{\parallel, pub}$

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 the protocol 2 times in parallel, the error can be reduced to $1/4$.

P_1 Is Hard for Q^{\parallel}

Using our Indistinguishability Lemma we show that

$$Q^{\parallel}(P_1) \in \Omega\left(n^{1/3}\right).$$

Our Second Separation: $R^{\parallel, ent}$ vs. $Q^{\parallel, pub}$

- ▶ How powerful is entanglement in communication complexity?
The question is very important and not well understood, in general.
- ▶ **We show that** there exists a relation P_2 efficiently solvable in $R^{\parallel, ent}$ but not in $Q^{\parallel, pub}$.
- ▶ The lower bound proof is based on our Indistinguishability Lemma.

Our Second Separation: $R^{\parallel, ent}$ vs. $Q^{\parallel, pub}$

- ▶ How powerful is entanglement in communication complexity?
The question is very important and not well understood, in general.
- ▶ **We show that** there exists a relation P_2 efficiently solvable in $R^{\parallel, ent}$ but not in $Q^{\parallel, pub}$.
- ▶ The lower bound proof is based on our Indistinguishability Lemma.

Our Second Separation: $R^{\parallel, ent}$ vs. $Q^{\parallel, pub}$

- ▶ How powerful is entanglement in communication complexity?
The question is very important and not well understood, in general.
- ▶ **We show that** there exists a relation P_2 efficiently solvable in $R^{\parallel, ent}$ but not in $Q^{\parallel, pub}$.
- ▶ The lower bound proof is based on our Indistinguishability Lemma.

Quantum State Distinguishing

Goal: given a quantum system in one of several a priori known states, a **referee** has to decide what the state is.

Possible correctness requirements:

- ▶ **Unrestricted:** The referee can be wrong. The goal is to make the probability of the right answer as high as possible.
- ▶ **Bounded Error:** The referee can be wrong with probability at most ϵ if he gives an answer, but he may refuse to answer. The goal is to make the probability of answering as high as possible.

Quantum State Distinguishing

Goal: given a quantum system in one of several a priori known states, a **referee** has to decide what the state is.

Possible correctness requirements:

- ▶ **Unrestricted:** The referee can be wrong. The goal is to make the **probability of the right answer** as high as possible.
- ▶ **Bounded Error:** The referee can be wrong with probability at most ε if he gives an answer, but he may refuse to answer. The goal is to make the **probability of answering** as high as possible.

Quantum State Distinguishing

Goal: given a quantum system in one of several a priori known states, a **referee** has to decide what the state is.

Possible correctness requirements:

- ▶ **Unrestricted:** The referee can be wrong. The goal is to make the **probability of the right answer** as high as possible.
- ▶ **Bounded Error:** The referee can be wrong with probability at most ε if he gives an answer, but he may refuse to answer. The goal is to make the **probability of answering** as high as possible.

Indistinguishability Lemma

- ▶ Let the success probability of unrestricted distinguishing of the quantum states α_1 and α_2 be at most $1/2 + a$.
- ▶ Let the answering probability for bounded error distinguishing of the states β_1 and β_2 be at most b .
- ▶ We show that the answering probability for bounded error distinguishing among the 4 states

$$\alpha_1 \otimes \beta_1, \alpha_1 \otimes \beta_2, \alpha_2 \otimes \beta_1, \alpha_2 \otimes \beta_2$$

is (at most) $O(ab)$.

- ▶ The proof is technical, based on SDP duality.

Indistinguishability Lemma

- ▶ Let the success probability of unrestricted distinguishing of the quantum states α_1 and α_2 be at most $1/2 + a$.
- ▶ Let the answering probability for bounded error distinguishing of the states β_1 and β_2 be at most b .
- ▶ We show that the answering probability for bounded error distinguishing among the 4 states

$$\alpha_1 \otimes \beta_1, \alpha_1 \otimes \beta_2, \alpha_2 \otimes \beta_1, \alpha_2 \otimes \beta_2$$

is (at most) $O(ab)$.

- ▶ The proof is technical, based on SDP duality.

Indistinguishability Lemma

- ▶ Let the success probability of unrestricted distinguishing of the quantum states α_1 and α_2 be at most $1/2 + a$.
- ▶ Let the answering probability for bounded error distinguishing of the states β_1 and β_2 be at most b .
- ▶ We show that the answering probability for bounded error distinguishing among the 4 states

$$\alpha_1 \otimes \beta_1, \alpha_1 \otimes \beta_2, \alpha_2 \otimes \beta_1, \alpha_2 \otimes \beta_2$$

is (at most) $O(ab)$.

- ▶ The proof is technical, based on SDP duality.

Indistinguishability Lemma

- ▶ Let the success probability of unrestricted distinguishing of the quantum states α_1 and α_2 be at most $1/2 + a$.
- ▶ Let the answering probability for bounded error distinguishing of the states β_1 and β_2 be at most b .
- ▶ We show that the answering probability for bounded error distinguishing among the 4 states

$$\alpha_1 \otimes \beta_1, \alpha_1 \otimes \beta_2, \alpha_2 \otimes \beta_1, \alpha_2 \otimes \beta_2$$

is (at most) $O(ab)$.

- ▶ The proof is technical, based on SDP duality.

Open Problems

- ▶ We have shown our separations using relations. Can similar results be obtained for (partial) functions? What about total functions?
- ▶ Stronger forms of the Quantum State Indistinguishability Lemma?

Open Problems

- ▶ We have shown our separations using relations. Can similar results be obtained for (partial) functions? What about total functions?
- ▶ Stronger forms of the Quantum State Indistinguishability Lemma?



Thank



Yo~~x~~!!!

