Title: Two exponential separations in communication complexity through bounded-error quantum state indistinguishability

Date: Jan 11, 2006 04:00 PM

URL: http://pirsa.org/06010001

Abstract: We consider the problem of bounded-error quantum state identification: given one of two known states, what is the optimal probability with which we can identify the given state, subject to our guess being correct with high probability (but we are permitted to output "don't know" instead of a guess). We prove a direct product theorem for this problem. Our proof is based on semidefinite programming duality and the technique may be of wider interest. Using this result, we present two new exponential separations in the simultaneous message passing model of communication complexity. Both are shown in the strongest possible sense: -- we describe a relation that can be computed with O(log n) classical bits of communication in the presence of shared randomness, but needs n^(1/3) communication if the parties don't share randomness, even if communication is quantum; -- we describe a relation that can be computed with O(log n) classical bits of communication in the presence of shared entanglement, but needs (almost) n^(1/3) communication if the parties share randomness but no entanglement, even if communication is quantum.

Two Exponential Separations in Communication Complexity Through Quantum States Indistinguishability

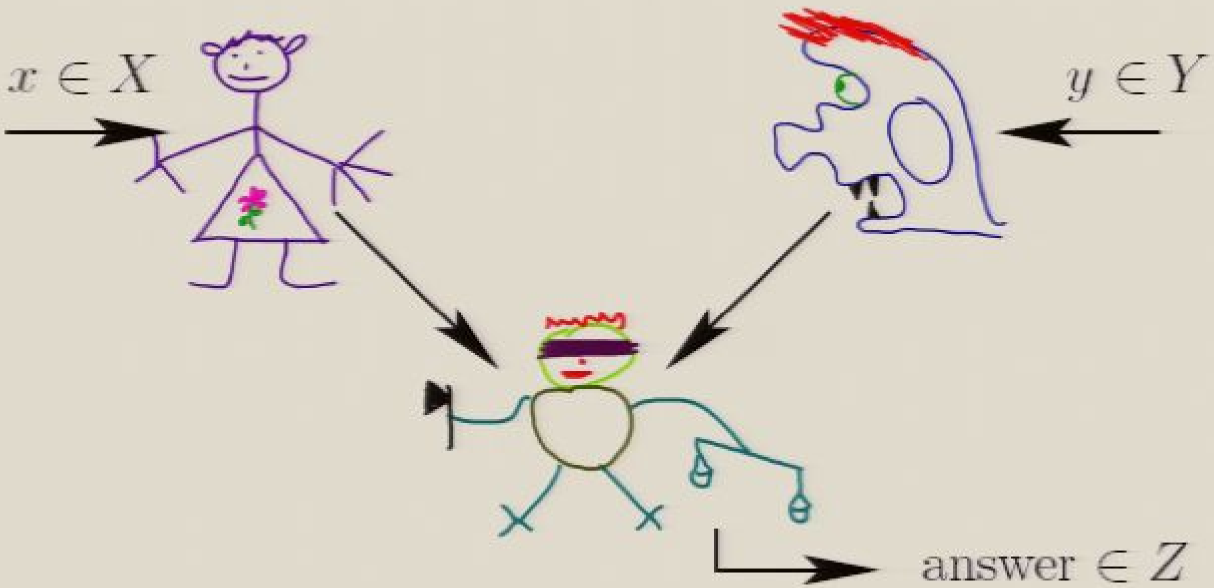
Dmitry Gavinsky

University of Calgary

Joint work with:

Julia Kempe, Oded Regev, Ronald de Wolf

Communication Complexity: the SMP Model



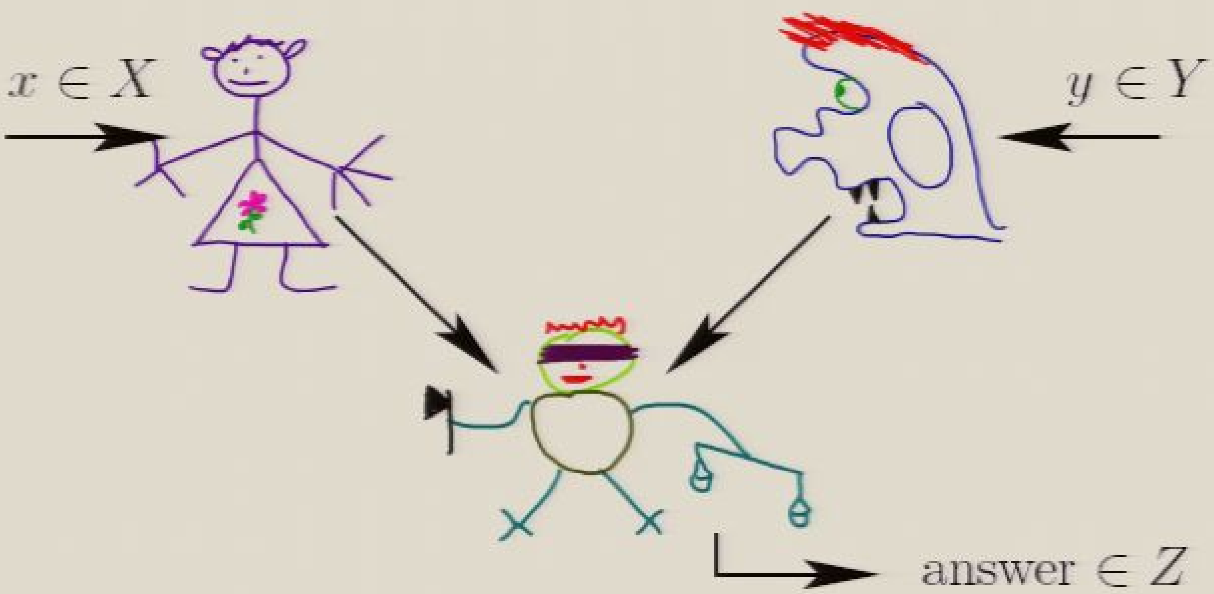
$P \subseteq X \times Y \times Z$

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.

Communication Complexity: the SMP Model



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

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: $R^{||}$, $R^{||,pub}$, $Q^{||}$, $Q^{||,ent}$

- **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.o.g., EPR pairs).

Model's Variations

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

- **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: $R^{\|}$, $R^{\|,pub}$, $Q^{\|}$, $Q^{\|,ent}$,
as well as: $R^{\|,ent}$ and $Q^{\|,pub}$.

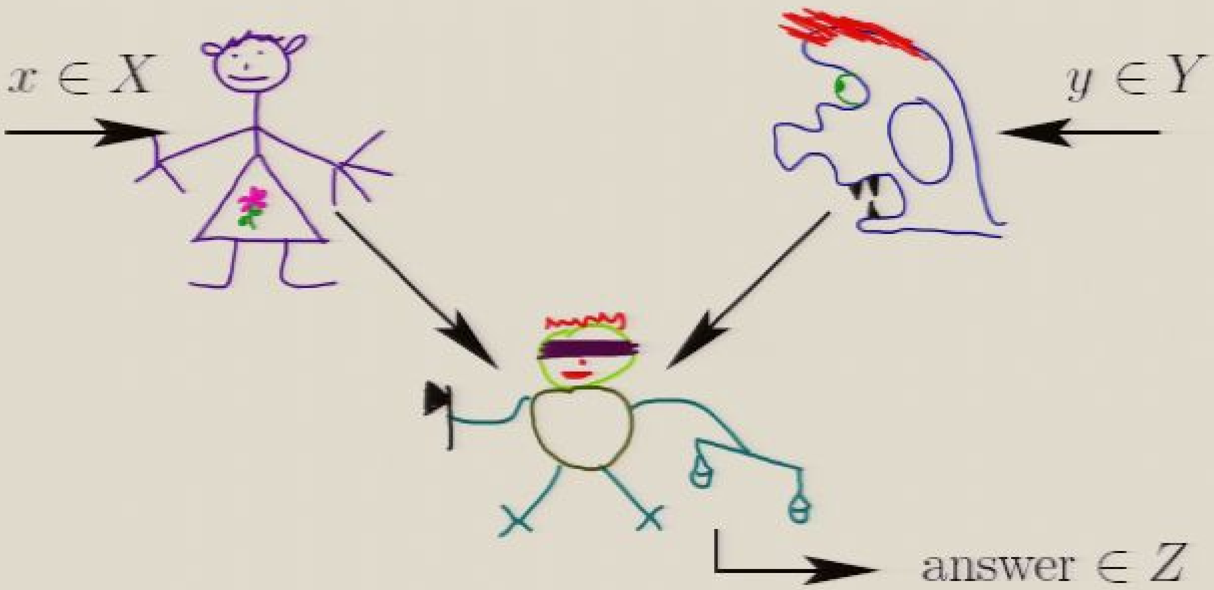
- **Communication with shared randomness:** Alice and Bob share a sequence of random bits (fair coin flips).
- **Quantum communication:** Alice and Bob send quantum messages, the referee performs a POVM measurement in order to produce the final output.
- **Communication with shared entanglement:** Alice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

Model's Variations

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

- **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 Complexity: the SMP Model



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

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

- **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 $y \in Y$.

Our Results

- We state and prove a Quantum State Indistinguishability Lemma.
- We exhibit a relation P_1, using the Lemma we prove that $R^{\|,pub}(P_1) \in O(\log n)$ but $Q^{\|}(P_1) \in \Omega\left(n^{1/3}\right)$.
- We exhibit a relation P_2, using the Lemma we prove that $R^{\|,pub}(P_2) \in O(\log n)$ but $Q^{\|}(P_2) \in \Omega\left((n/\log n)^{1/3}\right)$.

Our Results

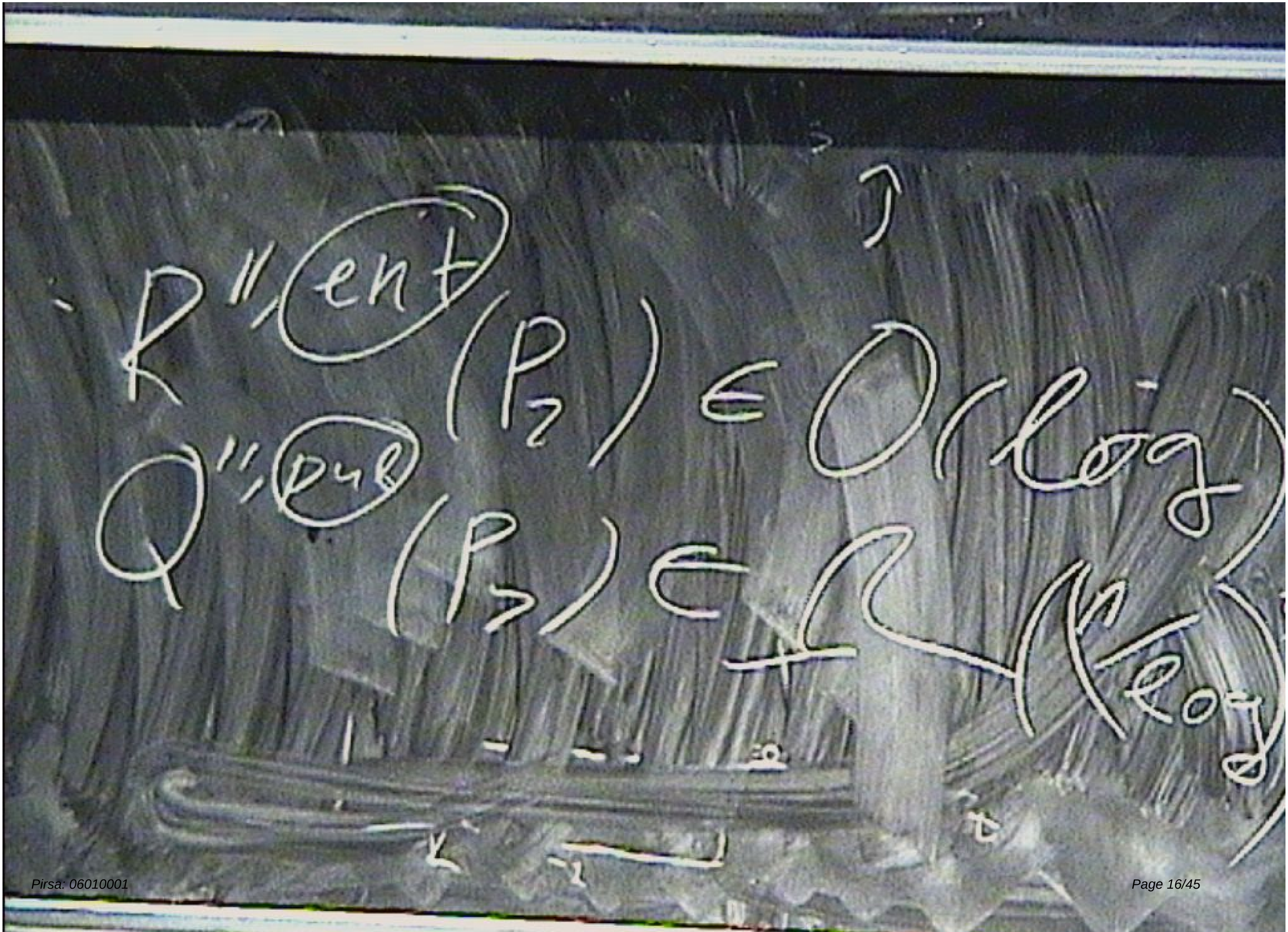
- We state and prove a Quantum State Indistinguishability Lemma.
- We exhibit a relation P_1, using the Lemma we prove that $R^{\|,pub}(P_1) \in O(\log n)$ but $Q^{\|}(P_1) \in \Omega\left(n^{1/3}\right)$.
- We exhibit a relation P_2, using the Lemma we prove that $R^{\|,pub}(P_2) \in O(\log n)$ but $Q^{\|}(P_2) \in \Omega\left((n/\log n)^{1/3}\right)$.

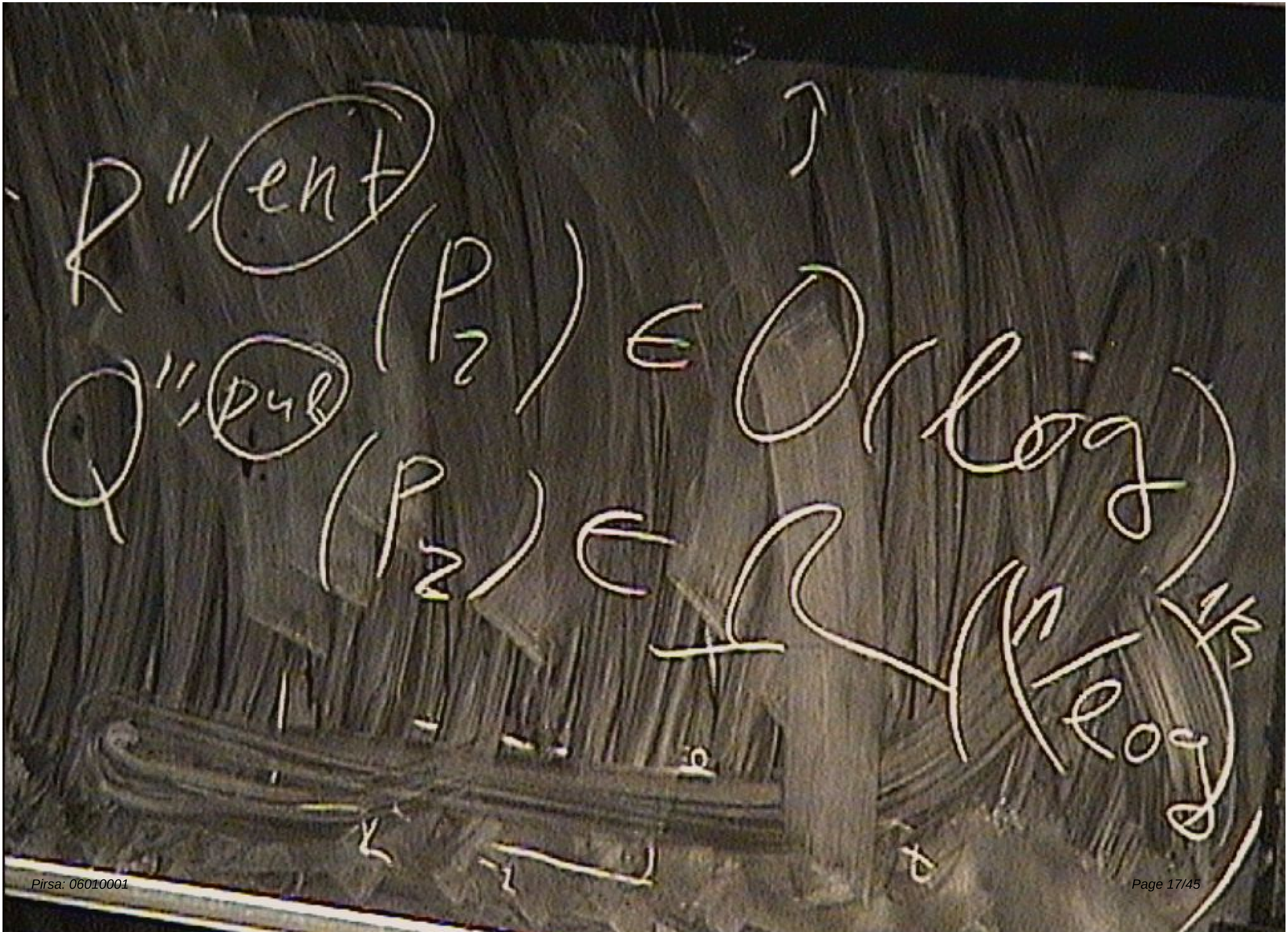
Our Results

- We state and prove a Quantum State Indistinguishability Lemma.
- We exhibit a relation P_1, using the Lemma we prove that $R^{\|,pub}(P_1) \in O(\log n)$ but $Q^{\|}(P_1) \in \Omega\left(n^{1/3}\right)$.
- We exhibit a relation P_2, using the Lemma we prove that $R^{\|,pub}(P_2) \in O(\log n)$ but $Q^{\|}(P_2) \in \Omega\left((n/\log n)^{1/3}\right)$.

$$R^{\parallel, ent}(P_2) \in O(\log$$

$$Q^{\parallel, pub}(P_2) \in \Omega\left(\frac{n}{\log}\right.$$


R''ent(P2) ∈ O(log)
Q''pure(P2) ∈ Ω(log)


$R^{\text{"ent"}}(P_2) \in O(\log)$
$Q^{\text{"pur"}}(P_2) \in \Omega\left(\left(\frac{n}{\log}\right)^{1/3}\right)$

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ by some exponentially longer protocol.

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ by some exponentially longer protocol.
- Our result shows that Yao's simulation is essentially optimal.

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ by some exponentially longer protocol.
- Our result shows that Yao's simulation is essentially optimal.

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ by some exponentially longer protocol.
- Our result shows that Yao's simulation is essentially optimal.

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ 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. $s_i = 1$.

0-error Protocol for P_1 in $R^{\|,pub}$

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. $s_i = 1$.

0-error Protocol for P_1 in $R^{\|,pub}$

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

- 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. $s_i = 1$.

0-error Protocol for P_1 in $R^{\|,pub}$

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

- 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 $1/4$.

$R^{\|,pub}$ vs. $Q^{\|}$

- **It was known before that** there exists a relation K efficiently solvable in $Q^{\|}$ but not in $R^{\|,pub}$ (due to Bar-Yossef, Jayram and Kerenidis).
- **We show that** there exists a relation P_1 efficiently solvable in $R^{\|,pub}$ but not in $Q^{\|}$ (in fact, our protocol for P_1 in $R^{\|,pub}$ is 0-error).
- Therefore, $R^{\|,pub}$ and $Q^{\|}$ are incomparable.
- Yao has shown that any protocol from $R^{\|,pub}$ can be simulated in $Q^{\|}$ 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. $s_i = 1$.

0-error Protocol for P_1 in $R^{||,pub}$

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

- 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 $Q^{\|}$

Using the Indistinguishability Lemma we show that

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

$R^{\|,ent}$ vs. $Q^{\|,pub}$

- **We show that** there exists a relation P_2 efficiently solvable in $R^{\|,ent}$ but not in $Q^{\|,pub}$.
- In fact, our protocol for P_2 in $R^{\|,ent}$ is exact.

$R^{\|,ent}$ vs. $Q^{\|,pub}$

- **We show that** there exists a relation P_2 efficiently solvable in $R^{\|,ent}$ but not in $Q^{\|,pub}$.
- In fact, our protocol for P_2 in $R^{\|,ent}$ is exact.

Quantum States Distinguishing

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

Possible correctness requirements:

Quantum States Distinguishing

Goal: given a quantum system in one of several a priori known states, a student has to decide what the state is.
Possible correctness requirements:

- **Unrestricted:** The student can be wrong. The goal is to make the probability of the right answer as high as possible.
- **Bounded Error:** The student 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.
- 0-**Error:** The student cannot be wrong but he may refuse to answer. The goal is to make the probability of answering as high as possible.

Quantum States Distinguishing

Goal: given a quantum system in one of several a priori known states, a student has to decide what the state is.
Possible correctness requirements:

- **Unrestricted:** The student can be wrong. The goal is to make the probability of the right answer as high as possible.
- **Bounded Error:** The student 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.
- 0-**Error:** The student cannot be wrong but he may refuse to answer. The goal is to make the probability of answering as high as possible.

Quantum States Distinguishing

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

Possible correctness requirements:

- **Unrestricted:** The student can be wrong. The goal is to make the probability of the right answer as high as possible.
- **Bounded Error:** The student 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.
- 0-**Error:** The student cannot be wrong but he may refuse to answer. The goal is to make the probability of answering as high as possible.

Indistinguishability Lemma

Our separations of communication models will be based on the following Indistinguishability Lemma:

Lemma

Suppose that the success probability of unrestricted distinguishing of the quantum states σ_1 and σ_2 is at most $1/2 + a$ and the answering probability for constant-error distinguishing of the states ρ_1 and ρ_2 is at most b.
Then there exists a constant ε such that the answering probability for ε-error distinguishing of the family

$$\{\sigma_1 \otimes \rho_1,\ \sigma_1 \otimes \rho_2,\ \sigma_2 \otimes \rho_1,\ \sigma_2 \otimes \rho_2\}$$

is at most $O(ab)$.

Quantum States Distinguishing

Goal: given a quantum system in one of several a priori known states, a student has to decide what the state is.
Possible correctness requirements:

- **Unrestricted:** The student can be wrong. The goal is to make the probability of the right answer as high as possible.
- **Bounded Error:** The student 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.
- 0-**Error:** The student cannot be wrong but he may refuse to answer. The goal is to make the probability of answering as high as possible.

Indistinguishability Lemma

Our separations of communication models will be based on the following Indistinguishability Lemma:

Lemma

Suppose that the success probability of unrestricted distinguishing of the quantum states σ_1 and σ_2 is at most $1/2 + a$ and the answering probability for constant-error distinguishing of the states ρ_1 and ρ_2 is at most b.
Then there exists a constant ε such that the answering probability for ε-error distinguishing of the family

$$\{\sigma_1 \otimes \rho_1,\ \sigma_1 \otimes \rho_2,\ \sigma_2 \otimes \rho_1,\ \sigma_2 \otimes \rho_2\}$$

is at most $O(ab)$.

A Counterintuitive Example

Suppose that instead of **distinguishing** the elements of $\{\sigma_i \otimes \rho_j \mid i, j \in \{1, 2\}\}$ we want **to identify i $\oplus$ j**...

- Let $|\alpha_1\rangle = |\beta_1\rangle = |0\rangle$, $|\alpha_2\rangle = |\beta_2\rangle = \sqrt{1-\delta^2}\,|0\rangle + \delta\,|1\rangle$.
- Then the success probability of unrestricted distinguishing of $|\alpha_1\rangle\langle\alpha_1|$ from $|\alpha_2\rangle\langle\alpha_2|$ is $1/2 + \Theta(\delta^2)$ and the answering probability for constant-error distinguishing of $|\beta_1\rangle\langle\beta_1|$ from $|\beta_2\rangle\langle\beta_2|$ is $\Theta(\delta^2)$.
- But the answering probability for constant-error identification of $i \oplus j$, given one of [illegible] is Θ [illegible]

A Counterintuitive Example

Suppose that instead of **distinguishing** the elements of $\{\sigma_i \otimes \rho_j \mid i,j \in \{1,2\}\}$ we want **to identify $\mathbf{i} \oplus \mathbf{j}$**...

- Let $|\alpha_1\rangle = |\beta_1\rangle = |0\rangle$, $|\alpha_2\rangle = |\beta_2\rangle = \sqrt{1-\delta^2}\,|0\rangle + \delta\,|1\rangle$.
- Then the success probability of unrestricted distinguishing of $|\alpha_1\rangle\langle\alpha_1|$ from $|\alpha_2\rangle\langle\alpha_2|$ is $1/2 + \Theta\left(\delta^2\right)$ and the answering probability for constant-error distinguishing of $|\beta_1\rangle\langle\beta_1|$ from $|\beta_2\rangle\langle\beta_2|$ is $\Theta\left(\delta^2\right)$.
- But the answering probability for constant-error identification of $i \oplus j$, given one of $\{|\alpha_i\rangle\langle\alpha_i| \otimes |\beta_j\rangle\langle\beta_j|\}$ is $\Theta\left(\delta^2\right)$!

A Counterintuitive Example

Suppose that instead of **distinguishing** the elements of $\{\sigma_i \otimes \rho_j \mid i,j \in \{1,2\}\}$ we want **to identify i $\oplus$ j**...

- Let $|\alpha_1\rangle = |\beta_1\rangle = |0\rangle$, $|\alpha_2\rangle = |\beta_2\rangle = \sqrt{1-\delta^2}\,|0\rangle + \delta\,|1\rangle$.
- Then the success probability of unrestricted distinguishing of $|\alpha_1\rangle\langle\alpha_1|$ from $|\alpha_2\rangle\langle\alpha_2|$ is $1/2 + \Theta(\delta^2)$ and the answering probability for constant-error distinguishing of $|\beta_1\rangle\langle\beta_1|$ from $|\beta_2\rangle\langle\beta_2|$ is $\Theta(\delta^2)$.
- But the answering probability for constant-error identification of $i \oplus j$, given one of $\{|\alpha_i\rangle\langle\alpha_i| \otimes |\beta_j\rangle\langle\beta_j|\}$ is $\Theta(\delta^2)$!

A Counterintuitive Example

Suppose that instead of **distinguishing** the elements of $\{\sigma_i \otimes \rho_j \mid i, j \in \{1,2\}\}$ we want **to identify i $\oplus$ j**...

- Let $|\alpha_1\rangle = |\beta_1\rangle = |0\rangle$, $|\alpha_2\rangle = |\beta_2\rangle = \sqrt{1-\delta^2}\,|0\rangle + \delta\,|1\rangle$.
- Then the success probability of unrestricted distinguishing of $|\alpha_1\rangle\langle\alpha_1|$ from $|\alpha_2\rangle\langle\alpha_2|$ is $1/2 + \Theta\left(\delta^2\right)$ and the answering probability for constant-error distinguishing of $|\beta_1\rangle\langle\beta_1|$ from $|\beta_2\rangle\langle\beta_2|$ is $\Theta\left(\delta^2\right)$.
- But the answering probability for constant-error identification of $i \oplus j$, given one of $\{|\alpha_i\rangle\langle\alpha_i| \otimes |\beta_j\rangle\langle\beta_j|\}$ is $\Theta\left(\delta^2\right)$!

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
You!!!

Indistinguishability Lemma

Our separations of communication models will be based on the following Indistinguishability Lemma:

Lemma

Suppose that the success probability of unrestricted distinguishing of the quantum states σ_1 *and* σ_2 *is at most* $1/2 + a$ *and the answering probability for constant-error distinguishing of the states* ρ_1 *and* ρ_2 *is at most* b.
Then there exists a constant ε *such that the answering probability for* ε*-error distinguishing of the family*

$$\{\sigma_1 \otimes \rho_1,\ \sigma_1 \otimes \rho_2,\ \sigma_2 \otimes \rho_1,\ \sigma_2 \otimes \rho_2\}$$

is at most $O(ab)$.