Title: New separations in quantum communication complexity

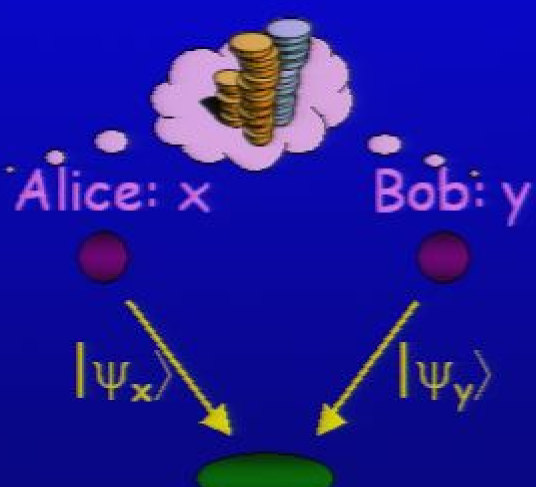
Date: Aug 30, 2006 04:00 PM

URL: http://pirsa.org/06080033

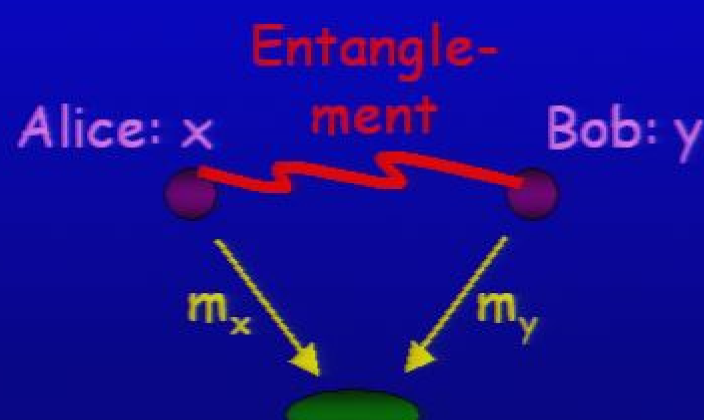
Abstract: In this talk I will present several new results from joint work with Dmitry Gavinsky, Oded Regev and Ronald de Wolf, relating to the model of one-way communication and the simultaneous model of communication. I will describe several separations between various resources (entanglement versus event coin, quantum communication versus classical communication), showing in particular that quantum communication cannot simulate a public coin and that entanglement can be much more powerful than a public coin, even if communication is quantum. I will also present a characterization of the quantum fingerprinting technique.

What is the power of entanglement?

- Determinism vs. Randomness (D vs. R_ε)
- Public Coin vs. Private Coin (R_ε^{pub} vs. R_ε)
- Classical vs. Quantum Communication (R vs. Q)
- **<u>Public Coin vs. Shared Entanglement</u>**
  (R_ε^{pub} vs. R_ε^{ent}, Q_ε^{pub} vs. R_ε^{ent},...)



Referee (quantum): R(x,y)

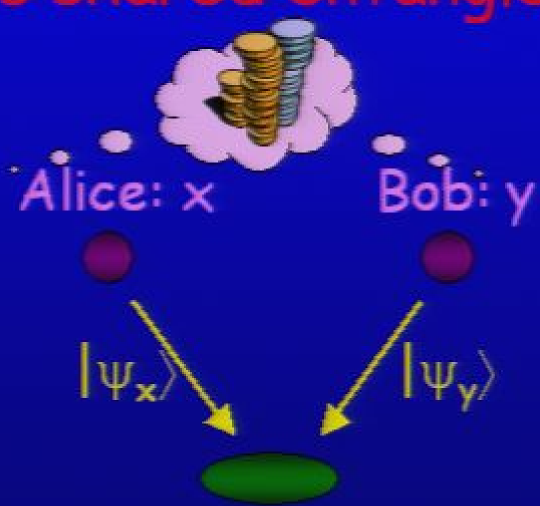


Referee (classical): R(x,y)

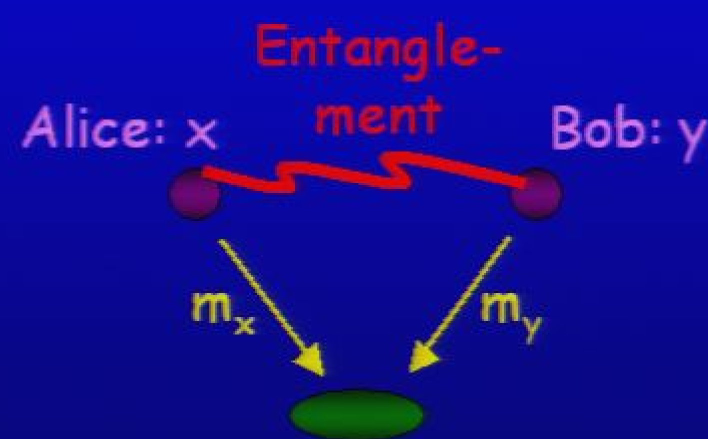
What is the power of entanglement?

- Determinism vs. Randomness (D vs. R_ε)
- Public Coin vs. Private Coin (R_ε^{pub} vs. R_ε)
- Classical vs. Quantum Communication (R vs. Q)
- **<u>Public Coin vs. Shared Entanglement</u>**
  (R_ε^{pub} vs. R_ε^{ent}, Q_ε^{pub} vs. R_ε^{ent},...)

Is shared entanglement stronger than a public coin?



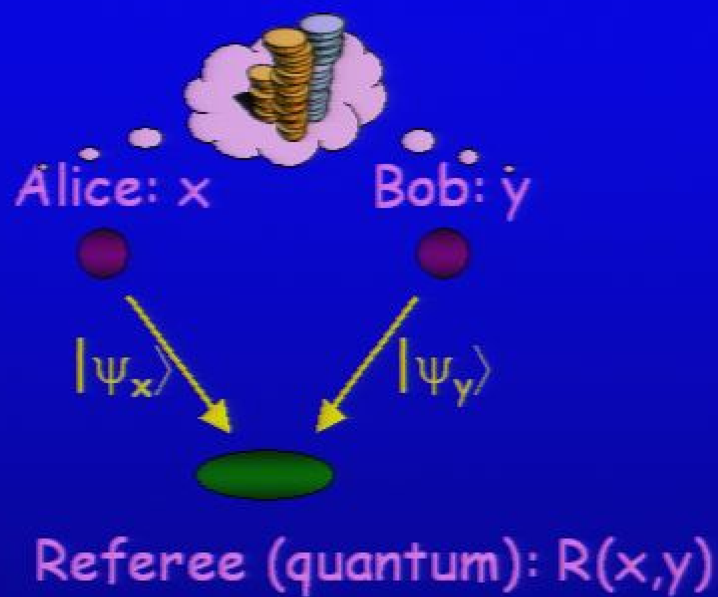
Referee (quantum): R(x,y)

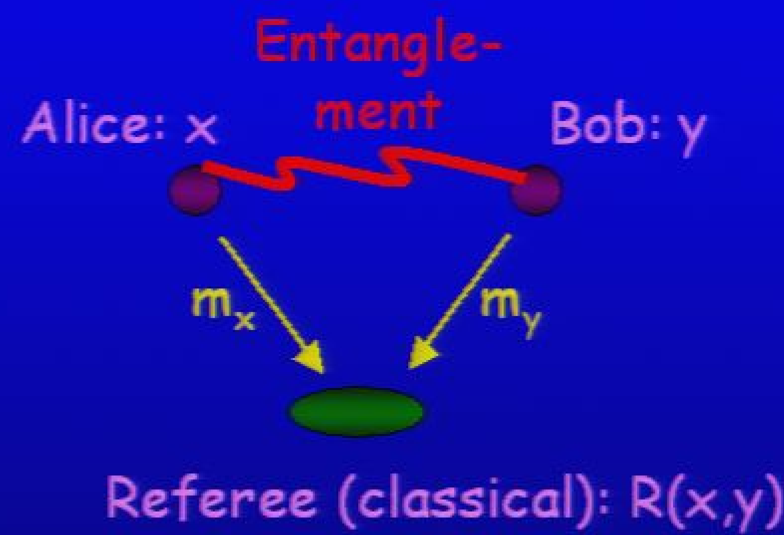


Referee (classical): R(x,y)

Q_ε^{pub} vs. R_ε^{ent} ???

Q_ε^{pub} vs. R_ε^{ent} ???

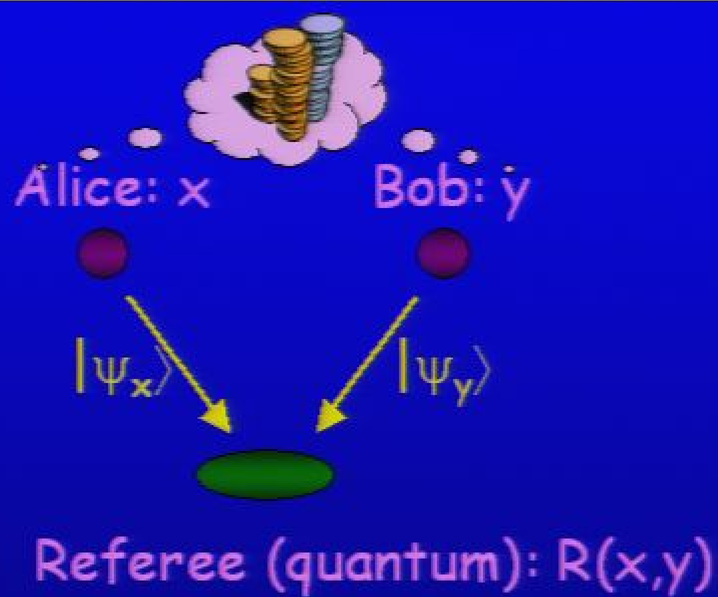


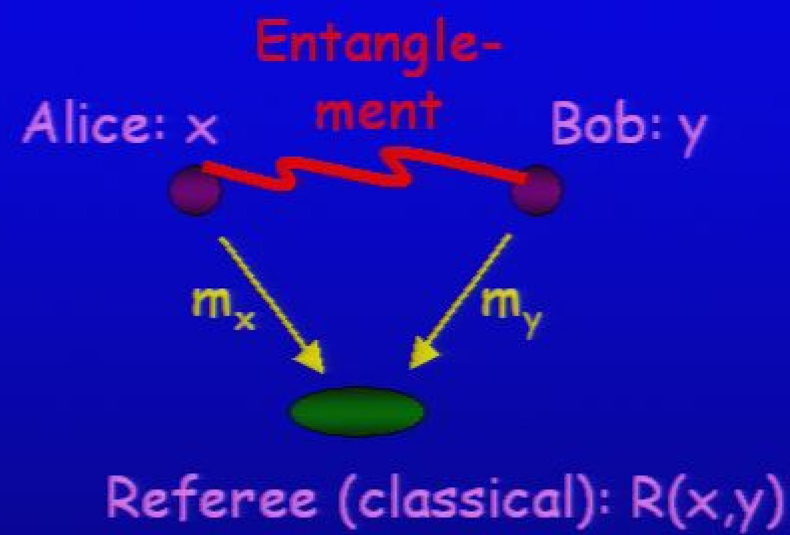


Q_ε^{pub} vs. R_ε^{ent} ???

Result 2 [GKRW'06]: R_ε^{ent} (R2) << Q_ε^{pub} (R2)

There is a relation R2(x,y) s. t. $R_\varepsilon^{ent}(R2) = O(\log n)$ and $Q_\varepsilon^{pub}(R2) = \Omega(\sqrt[3]{n}/\log n)$.

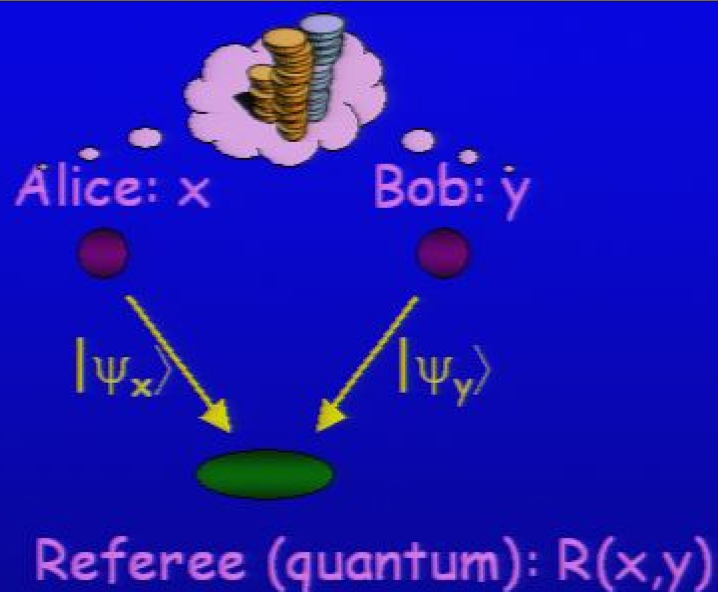


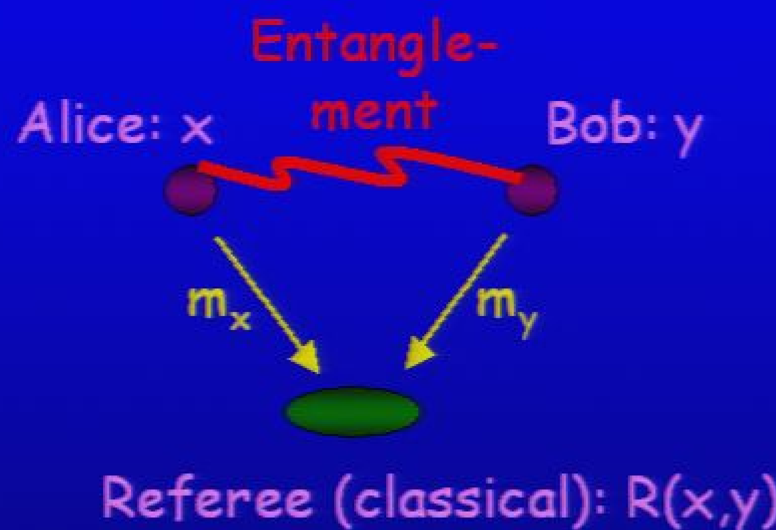


Q_ε^{pub} vs. R_ε^{ent} ???

Result 2 [GKRW'06]: $R_\varepsilon^{ent}(R2) << Q_\varepsilon^{pub}(R2)$

There is a relation $R2(x,y)$ s. t. $R_\varepsilon^{ent}(R2) = O(\log n)$ and $Q_\varepsilon^{pub}(R2) = \Omega(\sqrt[3]{n}/\log n)$.





$\Omega(\sqrt[3]{n}/\log n)$ quantum communication

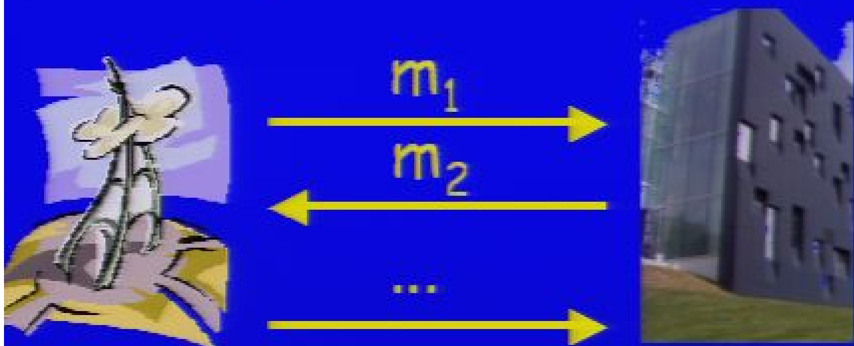
$O(\log n)$ classical communication* (uses log n shared EPR pairs)

Entanglement is much stronger than shared randomness!

* classical protocol due to Harry Buhrman

SMP and other models

Two-way communication model



Bob: y

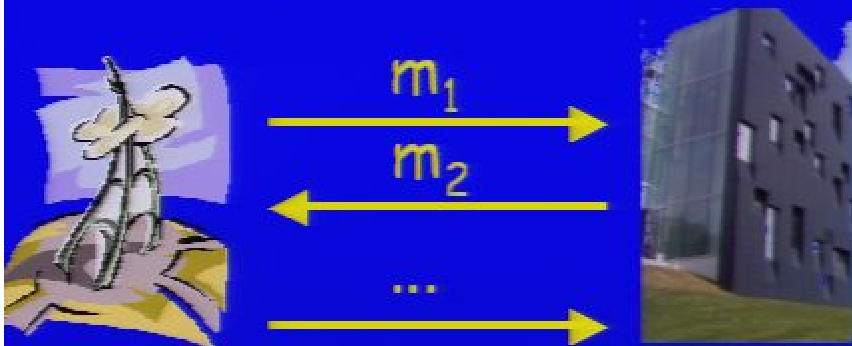
Alice: x

Cost: total communication
needed to compute R(x,y)
in the worst case

Complexities: D^2, R^2_ε, Q^2_ε, $Q^{2,\,ent}_\varepsilon$ ...

SMP and other models

Two-way communication model



Bob: y

Alice: x

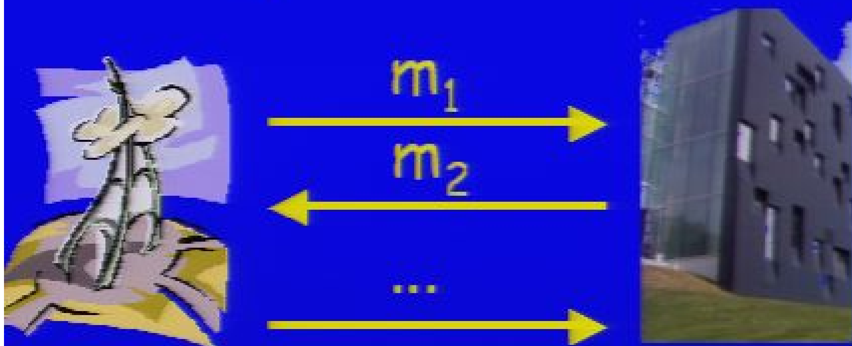
Cost: total communication needed to compute R(x,y) in the worst case

Complexities: D^2, R^2_ε, Q^2_ε, $Q^{2\,ent}_\varepsilon$ ...

SMP model weaker than direct communication models.

SMP and other models

Two-way communication model



Alice: x

Bob: y

Cost: total communication needed to compute $R(x,y)$ in the worst case

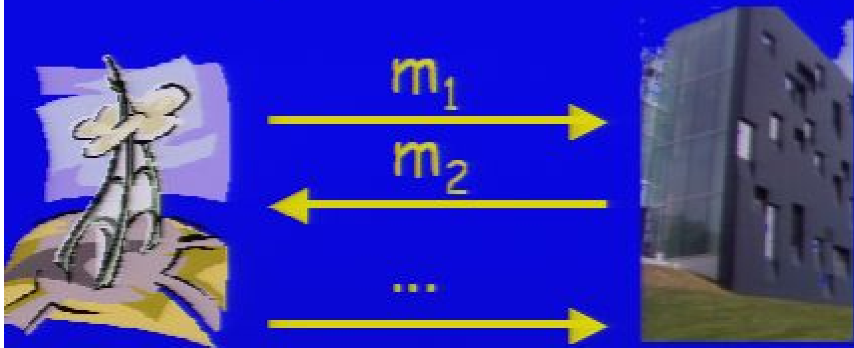
Complexities: D^2, R^2_ε, Q^2_ε, $Q^{2,ent}_\varepsilon$ ...

SMP model weaker than direct communication models.

How well can SMP protocols simulate two-way communication?

SMP and other models

Two-way communication model



Alice: x

Bob: y

Cost: total communication needed to compute R(x,y) in the worst case

Complexities: D^2, R^2_ε, Q^2_ε, $Q^{2,\,ent}_\varepsilon$ ...

SMP model weaker than direct communication models.

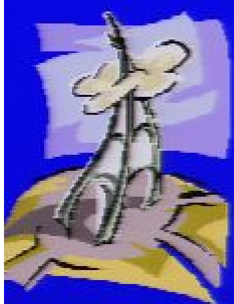
How well can SMP protocols simulate two-way communication?

Result 3 [GKW-1'06]: $Q_\varepsilon = O(2^{4Q^{2,\,ent}_\varepsilon} \log n)$

Every multi-round protocol (even with unlimited entanglement) can be simulated by a generalized <u>repeated fingerprint</u> SMP protocol (with exponential overhead).

SMP and other models

Two-way communication model



m_1 →

m_2 ←

... →

Alice: x

Bob: y

Cost: total communication needed to compute $R(x,y)$ in the worst case

Complexities: D^2, R^2_{ε}, Q^2_{ε}, $Q^{2\,ent}_{\varepsilon}$ ...

SMP model weaker than direct communication models.

How well can SMP protocols simulate two-way communication?

Result 3 [GKW-1'06]: $Q_{\varepsilon} = O(2^{4Q^{2\,ent}_{\varepsilon}} \log n)$

Every multi-round protocol (even with unlimited entanglement) can be simulated by a generalized repeated fingerprint SMP protocol (with exponential overhead).

Also Corollary: $R^{pub} = O(2^{4Q^{2\,ent}_{\varepsilon}} \log n)$

The power of fingerprints

All known nontrivial efficient quantum SMP protocols based on (repeated) quantum fingerprints.

Alice: $x \to |a_x\rangle$ Bob: $y \to |b_y\rangle$

SWAP test: $|\langle a_x|b_y\rangle|^2 \leq \delta_0$ if $f(x,y)=0$ $(\delta_0 < \delta_1)$

$|\langle a_x|b_y\rangle|^2 \geq \delta_1$ if $f(x,y)=1$

Repeat $r = \Theta(1/(\delta_1 - \delta_0)^2)$ times to succeed with constant prob.

The power of fingerprints

All known nontrivial efficient quantum SMP protocols based on (repeated) quantum fingerprints.

Alice: $x \rightarrow |a_x\rangle$ Bob: $y \rightarrow |b_y\rangle$

SWAP test: $|\langle a_x|b_y\rangle|^2 \leq \delta_0$ if $f(x,y)=0$ $(\delta_0 < \delta_1)$

$|\langle a_x|b_y\rangle|^2 \geq \delta_1$ if $f(x,y)=1$

Repeat $r = \Theta(1/(\delta_1 - \delta_0)^2)$ times to succeed with constant prob.

Communication Matrix:

$$\begin{array}{c} \leftarrow x \rightarrow \\ M(EQ) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ \cdots & & & \cdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix} \updownarrow y \end{array}$$

$$\begin{array}{cc} & |a_{x_1}\rangle, |a_{x_2}\rangle, \ldots, |a_{x_{2^n}}\rangle \\ \begin{array}{c} |b_{y_1}\rangle \\ |b_{y_2}\rangle \\ \cdots \\ |b_{y_{2^n}}\rangle \end{array} & \begin{pmatrix} & \cdots & \\ \cdots & |\langle a_x|b_y\rangle|^2 & \cdots \\ & \cdots & \end{pmatrix} \end{array}$$

$M_{xy}(f)=f(x,y)$

The power of fingerprints

Communication Matrix:

$$M(EQ) = \begin{array}{cc} \longleftarrow \ x \ \longrightarrow & \\ \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ \cdots & & & \cdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix} & \updownarrow y \end{array}$$

Learning Theory:

$$L(EQ) = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 1 & & \\ 1 & 1 & -1 & & \\ \cdots & & & \cdots & 1 \\ 1 & & & 1 & -1 \end{pmatrix}$$

$M\ (f)=f(x,y)$

$L\ (f)=(-1)^{f(x,y)}$

The power of fingerprints

Communication Matrix:

$$
\begin{array}{cc}
 & \longleftarrow x \longrightarrow \\
M(EQ) = & \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ \cdots & & & \cdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix} \updownarrow y
\end{array}
$$

$M_{xy}(f)=f(x,y)$

Learning Theory:

$$
L(EQ) = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 1 & & \\ 1 & 1 & -1 & & \\ \cdots & & & \cdots & 1 \\ 1 & & & 1 & -1 \end{pmatrix}
$$

margin

$L_{xy}(f)=(-1)^{f(x,y)}$

$\langle a_x|b_y\rangle \geq \gamma$ if $f(x,y)=0$

$\langle a_x|b_y\rangle \leq -\gamma$ if $f(x,y)=1$

The power of fingerprints

Can relate fingerprints to margins [GKW-1'06]

Cost of repeated fingerprints: $\Omega(\log n / \gamma^2)$

Theorem (Foster) : Let the $2^n \times 2^n$ matrix $L_{xy} = (-1)^{f(x,y)}$.

Every realization of f has margin $\gamma \le \|L\|_{op} / 2^n$.

Cost of repeated fingerprints for IP: $\Omega(2^n)$.

Communication Matrix:

$$M(EQ) = \begin{array}{c} \longleftarrow x \longrightarrow \\ \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ \cdots & & & \cdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix} \end{array} \; \updownarrow y$$

$M_{xy}(f)=f(x,y)$

Learning Theory:

$$L(EQ) = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 1 & & \\ 1 & 1 & -1 & & \\ \cdots & & & \cdots & 1 \\ 1 & & & 1 & -1 \end{pmatrix}$$

margin

$\langle a_x | b_y \rangle \ge \gamma$ if $f(x,y)=0$

$L_{xy}(f)=(-1)^{f(x,y)}$ $\langle a_x | b_y \rangle \le -\gamma$ if $f(x,y)=1$

The power of fingerprints

Connection:

Quantum Communication ⇄ Learning Theory

New lower bounds on $Q^{2,ent}$ from margin bounds: $Q^{2,ent}(f) = \Omega(\log(1/\gamma(f)))$ (independently obtained by Linial and Shraibman'06, they also show $1/\gamma(f) \approx \mathrm{Disc}(f)$)

The power of fingerprints

Connection:

Quantum Communication ⇄ Learning Theory

- New lower bounds on $Q^{2,ent}$ from margin bounds: $Q^{2,ent}(f) = \Omega(\log(1/\gamma(f)))$ (independently obtained by Linial and Shraibman'06, they also show $1/\gamma(f) \approx \mathrm{Disc}(f)$)

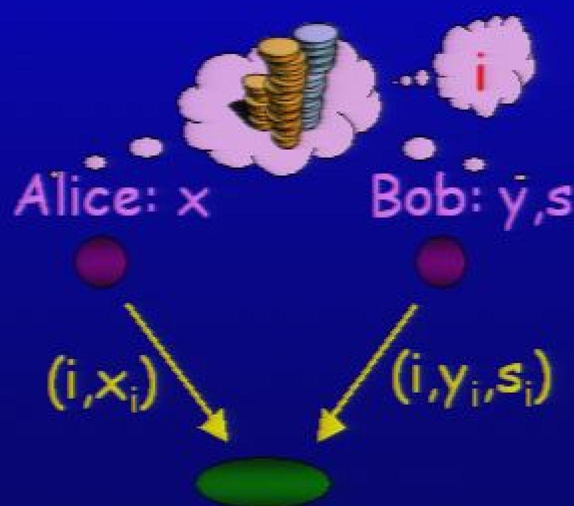
- New upper bounds for SMP and general protocols from margin bounds (embeddings)

- New bounds for margins (embeddings) from SMP upper bounds, possibly coming from simulation of quantum two-way protocols with entanglement (quantum-classical results)

R1: definition and upper bound

Result 1: $R_\varepsilon^{pub}(R1) << Q_\varepsilon(R1)$
There is a relation $R1(x,y)$ s. t. $R_\varepsilon^{pub}(R1) = O(\log n)$ and $Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})$.

Alice: $x \in \{0,1\}^n$
Bob: $y, s \in \{0,1\}^n$ s.t. $|s| = \frac{1}{2}n$ "mask"
Referee: (i, x_i, y_i) s.t. $s_i = 1$



R1: definition and upper bound

Result 1: $R_\varepsilon^{pub}(R1) << Q_\varepsilon(R1)$

There is a relation $R1(x,y)$ s. t. $R_\varepsilon^{pub}(R1) = O(\log n)$ and $Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})$.

Alice: $x \in \{0,1\}^n$

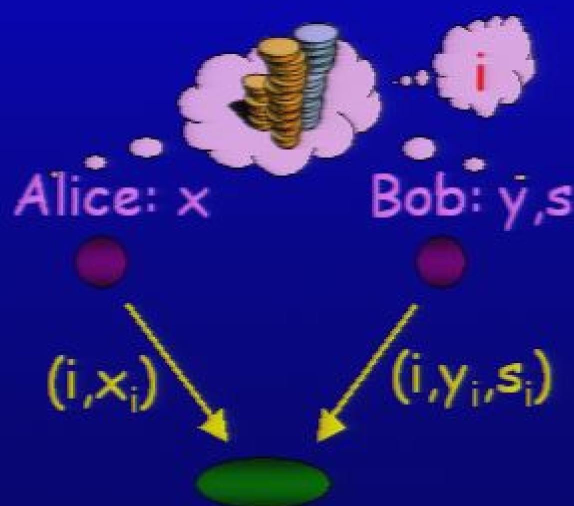
Bob: $y, s \in \{0,1\}^n$ s.t. $|s| = \frac{1}{2}n$ "mask"

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

$s = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1$

$x = 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1$

$y = 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0$



R1: definition and upper bound

Result 1: $R_\varepsilon^{pub}(R1) << Q_\varepsilon(R1)$

There is a relation $R1(x,y)$ s. t. $R_\varepsilon^{pub}(R1) = O(\log n)$ and $Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})$.

Alice: $x \in \{0,1\}^n$

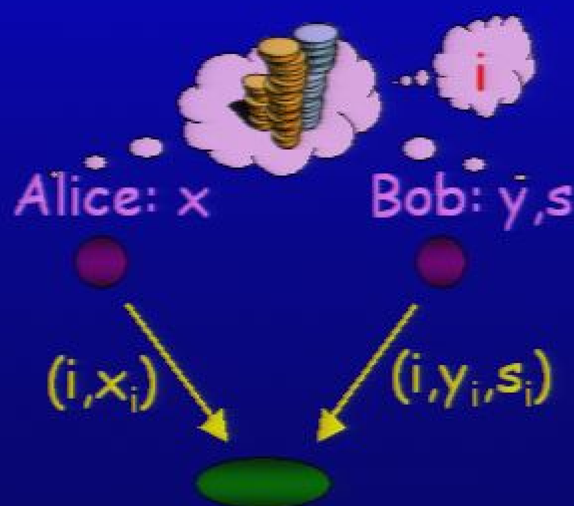
Bob: $y, s \in \{0,1\}^n$ s.t. $|s| = \frac{1}{2}n$ "mask"

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

s = 0 1 1 0 0 1 0 1

x = 1 1 0 0 1 0 0 1

y = 0 1 0 1 1 0 1 0



if $s_i=1 \rightarrow$ output (i,x_i,y_i)
(happens with prob. $\frac{1}{2}$)
repeat a few times to boost success prob.

R2: definition and upper bound

Result 2: R_ε^{ent} (R2) << Q_ε^{pub} (R2)

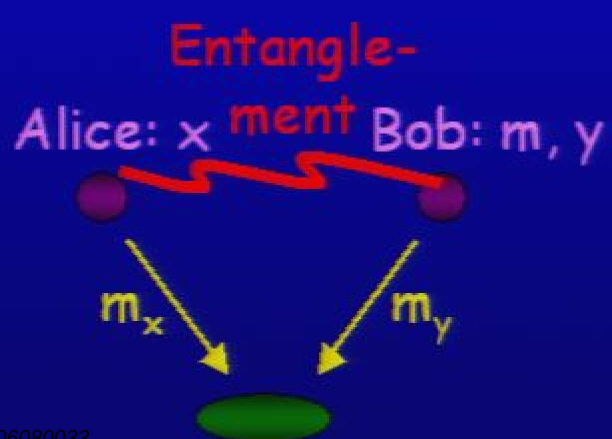
There is a relation R2(x,y) s. t. $R_\varepsilon^{ent}(R2) = O(\log n)$ and $Q_\varepsilon^{pub}(R2) = \Omega(\sqrt[3]{n}/\log n)$.

Alice: $x \in \{0,1\}^n$

Bob: m - matching of n bits

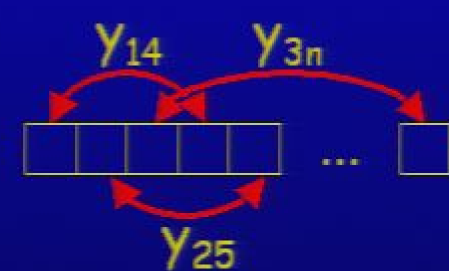
$y \in \{0,1\}^{n/2}$ (a bit y_{ij} for all $(i,j) \in m$)

Referee: $(i, j, x_i \oplus x_j, y_{ij})$ s.t. $(i,j) \in m$



Alice: $x = x_1 x_2 \ldots x_n$

Bob:



R1: definition and upper bound

Result 1: $R_\varepsilon^{pub}(R1) << Q_\varepsilon(R1)$

There is a relation $R1(x,y)$ s. t. $R_\varepsilon^{pub}(R1) = O(\log n)$ and $Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})$.

Alice: $x \in \{0,1\}^n$

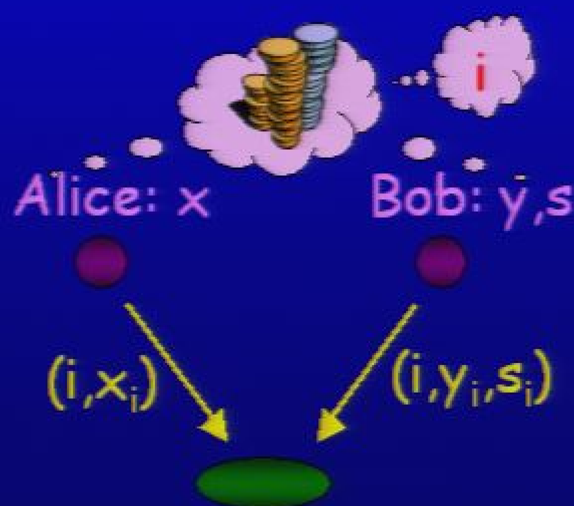
Bob: $y, s \in \{0,1\}^n$ s.t. $|s| = \frac{1}{2}n$ "mask"

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

s = 0 1 1 0 0 1 0 1

x = 1 1 0 0 1 0 0 1

y = 0 1 0 1 1 0 1 0



if $s_i = 1 \rightarrow$ output (i, x_i, y_i)

(happens with prob. $\frac{1}{2}$)

repeat a few times to boost success prob.

R2: definition and upper bound

Result 2: R_ε^{ent} (R2) << Q_ε^{pub} (R2)

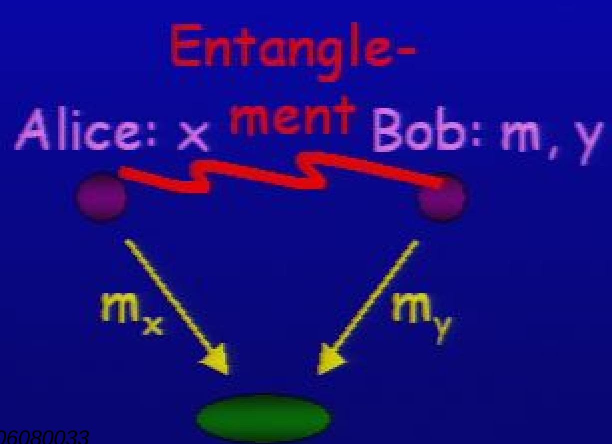
There is a relation R2(x,y) s. t. $R_\varepsilon^{ent}(R2) = O(\log n)$ and $Q_\varepsilon^{pub}(R2) = \Omega(\sqrt[3]{n}/\log n)$.

Alice: $x \in \{0,1\}^n$

Bob: m - matching of n bits

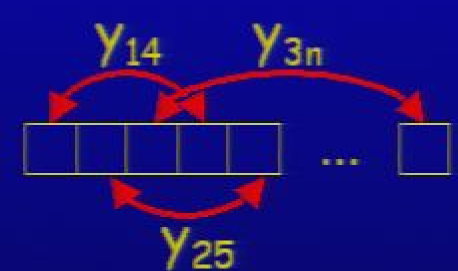
$y \in \{0,1\}^{n/2}$ (a bit y_{ij} for all $(i,j) \in m$)

Referee: $(i,j,x_i \oplus x_j, y_{ij})$ s.t. $(i,j) \in m$



Alice: $x = x_1 x_2 \ldots x_n$

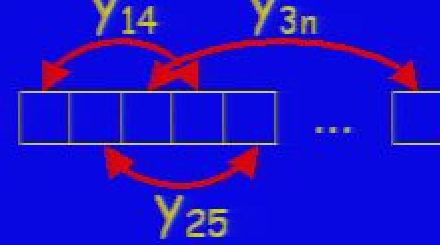
Bob:



R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$

Alice: $x = x_1 x_2 \dots x_n$ **Bob:**

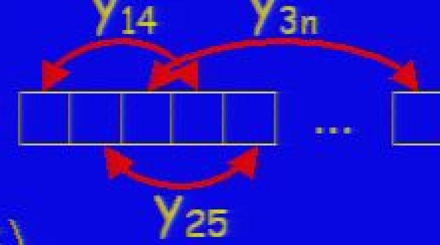


·**Referee:** output $(i, j, x_i \oplus x_j, y_{ij})$

R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs

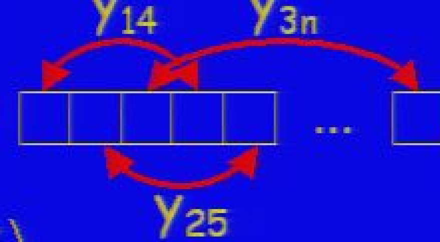
$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$$

·Referee: output $(i, j, x_i \oplus x_j, y_{ij})$

R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$$

- Alice: $|i\rangle_A \rightarrow (-1)^{x_i} |i\rangle_A$

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$$

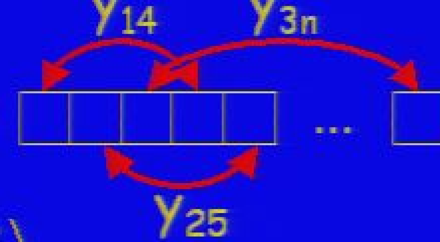
- **Referee:**

output $(i, j, x_i \oplus x_j, y_{ij})$

R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$$

- Alice: $|i\rangle_A \rightarrow (-1)^{x_i} |i\rangle_A$

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$$

- Bob: measure with

  $\Pi_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ for $(i,j) \in m$

  send i, j, y_{ij} (2 log n +1 bits)

$$|\Psi\rangle_{AB} = |i\rangle_A |i\rangle_B + (-1)^{x_i \oplus x_j} |j\rangle_A |j\rangle_B$$

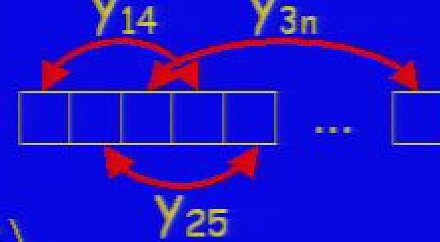
- **Referee:**

output $(i, j, x_i \oplus x_j, y_{ij})$

R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$$

- Alice: $|i\rangle_A \rightarrow (-1)^{x_i} |i\rangle_A$

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$$

- Bob: measure with
  $\Pi_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ for $(i,j) \in m$
  send i, j, y_{ij} (2 log n +1 bits)

$$|\Psi\rangle_{AB} = |i\rangle_A |i\rangle_B + (-1)^{x_i \oplus x_j} |j\rangle_A |j\rangle_B$$

- Alice and Bob: apply $H^{\otimes \log n}$

$$|\Psi\rangle_{AB} = \sum_{s,t} \left\{ (-1)^{(s+t)\bullet i} + (-1)^{x_i \oplus x_j} (-1)^{(s+t)\bullet j} \right\} |s\rangle_A |t\rangle_B$$

- **Referee:** output $(i, j, x_i \oplus x_j, y_{ij})$ ✓ ✓

R2: definition and upper bound

$\boxed{O(\log n) \text{ classical bits}}$ **Alice:** $x = x_1 x_2 \ldots x_n$ **Bob:** y_{14} y_{3n} y_{25}

- Share log n EPR pairs $\qquad |\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$
- Alice: $|i\rangle_A \rightarrow (-1)^{x_i} |i\rangle_A \qquad |\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$
- Bob: measure with
  $\Pi_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ for $(i,j) \in m$ $\qquad |\Psi\rangle_{AB} = |i\rangle_A |i\rangle_B + (-1)^{x_i \oplus x_j} |j\rangle_A |j\rangle_B$
  send i, j, y_{ij} (2 log n +1 bits)
- Alice and Bob: apply $H^{\otimes \log n}$

$$|\Psi\rangle_{AB} = \sum_{s,t} \left\{ (-1)^{(s+t)\bullet i} + (-1)^{x_i \oplus x_j} (-1)^{(s+t)\bullet j} \right\} |s\rangle_A |t\rangle_B$$

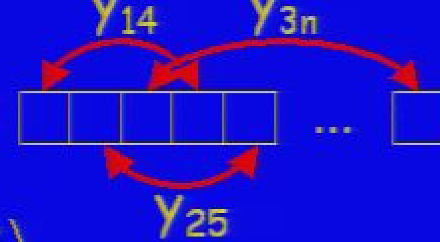
- Alice and Bob : measure $|s\rangle_A$, $|t\rangle_B$, send s,t (2 log n bits)

- **Referee:** output $(i, j, x_i \oplus x_j, y_{ij})$ ✓ ✓

R2: definition and upper bound

$O(\log n)$ classical bits

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs $\qquad |\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$
- Alice: $|i\rangle_A \to (-1)^{x_i} |i\rangle_A \qquad |\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$
- Bob: measure with
  $\Pi_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ for $(i,j) \in m$
  send i, j, y_{ij} (2 log n +1 bits) $\qquad |\Psi\rangle_{AB} = |i\rangle_A |i\rangle_B + (-1)^{x_i \oplus x_j} |j\rangle_A |j\rangle_B$
- Alice and Bob: apply $H^{\otimes \log n}$

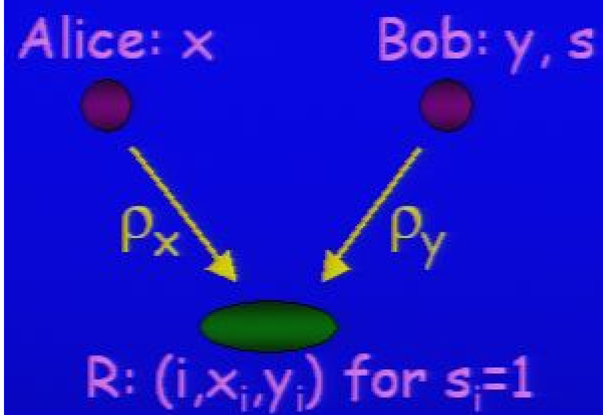
$$|\Psi\rangle_{AB} = \sum_{s,t} \left\{ (-1)^{(s+t)\cdot i} + (-1)^{x_i \oplus x_j} (-1)^{(s+t)\cdot j} \right\} |s\rangle_A |t\rangle_B$$

- Alice and Bob : measure $|s\rangle_A$, $|t\rangle_B$, send s,t (2 log n bits)

- **Referee:** $(s+t)\bullet(i+j) = x_i \oplus x_j \to$ output $(i, j, x_i \oplus x_j, y_{ij})$ ✓ ✓ ✓

R1: lower bound

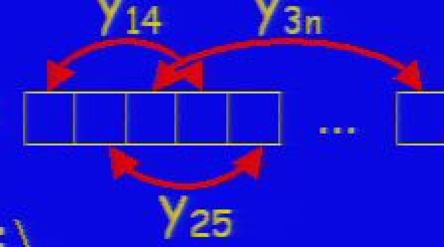
$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



R2: definition and upper bound

$O(\log n)$ classical bits

Alice: $x = x_1 x_2 \ldots x_n$ **Bob:**



- Share log n EPR pairs

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} |i\rangle_A |i\rangle_B$$

- Alice: $|i\rangle_A \to (-1)^{x_i} |i\rangle_A$

$$|\Psi\rangle_{AB} = \sum_{i=1}^{n} (-1)^{x_i} |i\rangle_A |i\rangle_B$$

- Bob: measure with

  $\Pi_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ for $(i,j) \in m$

  send i, j, y_{ij} (2 log n +1 bits)

$$|\Psi\rangle_{AB} = |i\rangle_A |i\rangle_B + (-1)^{x_i \oplus x_j} |j\rangle_A |j\rangle_B$$

- Alice and Bob: apply $H^{\otimes \log n}$

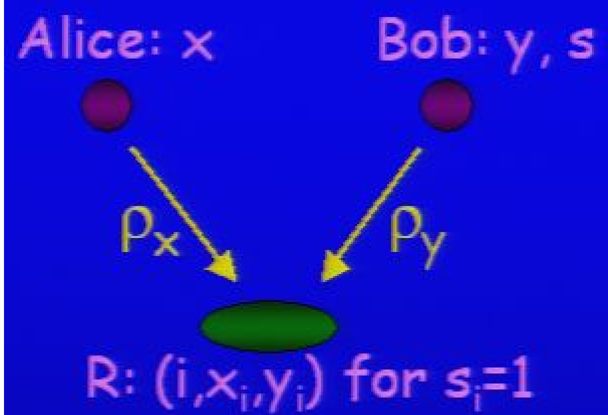
$$|\Psi\rangle_{AB} = \sum_{s,t} \left\{ (-1)^{(s+t)\bullet i} + (-1)^{x_i \oplus x_j} (-1)^{(s+t)\bullet j} \right\} |s\rangle_A |t\rangle_B$$

- Alice and Bob : measure $|s\rangle_A$, $|t\rangle_B$, send s,t (2 log n bits)

- **Referee:** $(s+t)\bullet(i+j) = x_i \oplus x_j \to$ output $(i, j, x_i \oplus x_j, y_{ij})$ ✓ ✓ ✓

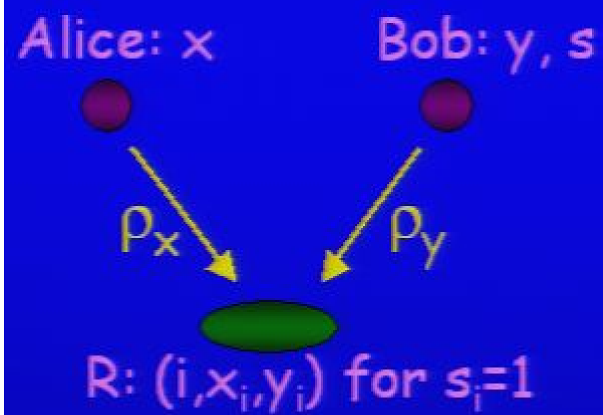
R1: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



R1: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



Information Theory:

extract subproblem for fixed index j

$$\rho_0^j = \frac{1}{2^{n-1}} \sum_{x:x_j=0} \rho_x \qquad \rho_1^j = \frac{1}{2^{n-1}} \sum_{x:x_j=1} \rho_x$$

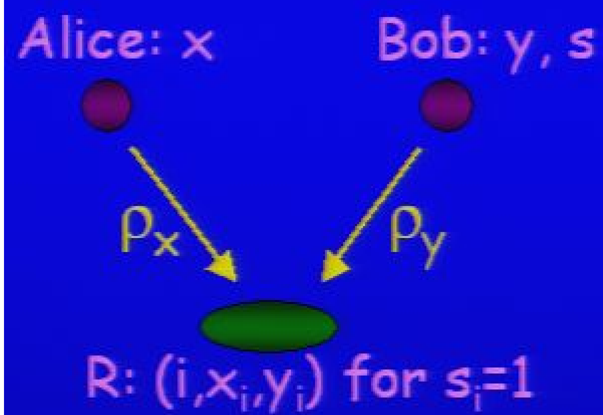
Given $\rho_{x_j}^j \otimes \rho_{y_j}^j$ output

(x_i, y_i) if $i=j$ (correctly with prob. $1-\varepsilon$)

"don't know" if $i \neq j$

R1: lower bound

$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$



Information Theory:

extract subproblem for fixed index j

$$\rho_0^j = \frac{1}{2^{n-1}} \sum_{x:x_j=0} \rho_x \qquad \rho_1^j = \frac{1}{2^{n-1}} \sum_{x:x_j=1} \rho_x$$

Given $\rho_{x_j}^j \otimes \rho_{y_j}^j$ output

(x_i, y_i) if $i=j$ (correctly with prob. $1-\varepsilon$)

"don't know" if $i \neq j$

Relate to known bounds on Random Access Codes [Nayak'99]

given ρ_x output x_j and given ρ_y output y_j

Bounded Error State Identification

State Identification

Given ρ_0 or ρ_1, identify which one.

Optimal success probability given by $\frac{1}{2} + \frac{1}{2}\,|\rho_0 - \rho_1|_{tr}$

Trace distance is too small $\rightarrow$ error prob. too close to $\frac{1}{2}$.

State Identification

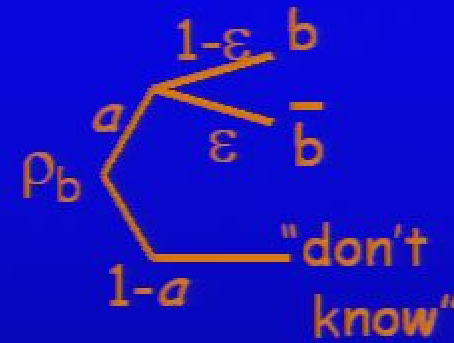
Given ρ_0 or ρ_1, identify which one.

Optimal success probability given by $\frac{1}{2} + \frac{1}{2} |\rho_0 - \rho_1|_{tr}$

Trace distance is too small $\rightarrow$ error prob. too close to $\frac{1}{2}$.

Bounded error state identification:

Referee can be wrong with prob. at most ε if he makes a guess, but he may say "don't know".



Goal: maximize the probability to output a guess ("0" or "1") (call it a_ε).

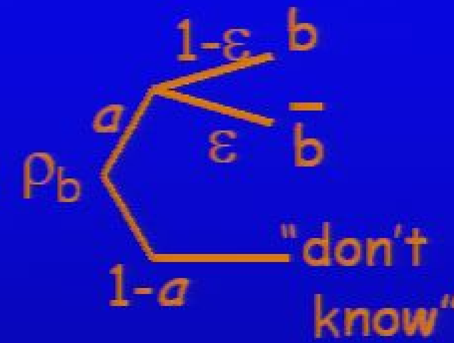
State Identification

Given ρ_0 or ρ_1, identify which one.

Optimal success probability given by $\frac{1}{2} + \frac{1}{2}\,|\rho_0 - \rho_1|_{tr}$

Trace distance is too small $\rightarrow$ error prob. too close to $\frac{1}{2}$.

Bounded error state identification:



Referee can be wrong with prob. at most ε if he makes a guess, but he may say "don't know".

Goal: maximize the probability to output a guess ("0" or "1") (call it a_ε).

a_ε is not determined by $\rho_0 - \rho_1$ but can be written as a semidefinite program (SDP).

State Identification

Example:

$|\phi_0\rangle = \sqrt{a}|0\rangle + \sqrt{1-a}\,|2\rangle$
$|\phi_1\rangle = \sqrt{a}\,|1\rangle + \sqrt{1-a}\,|2\rangle$

$|\phi_0 - \phi_1|_{tr} \approx \sqrt{a}$ (small) error probability $\frac{1}{2}(1-\sqrt{a})$

Measure in computational basis:

observe $|0\rangle \rightarrow$ output "0"
observe $|1\rangle \rightarrow$ output "1"
observe $|2\rangle \rightarrow$ output "don't know"

Gain: error probability reduced to 0

Cost: we get an answer only with probability a

Tensor Lemma

Suppose we are given two independent problems:

ρ_0, ρ_1 with a_ε = max. prob. of guess

σ_0, σ_1 with b_ε = max. prob. of guess

Tensored problem: given $\rho_0 \otimes \sigma_0$, $\rho_0 \otimes \sigma_1$, $\rho_1 \otimes \sigma_0$ or $\rho_1 \otimes \sigma_1$ identify which one in the bounded error setting. Let $p_{\varepsilon'}$ be the maximum probability of making a guess.

Expect: $p_{\varepsilon'} = O(a_\varepsilon \cdot b_\varepsilon)$ ("Direct Product Theorem")

Tensor Lemma

Suppose we are given two independent problems:

ρ_0, ρ_1 with a_ε = max. prob. of guess
σ_0, σ_1 with b_ε = max. prob. of guess

Tensored problem: given $\rho_0 \otimes \sigma_0$, $\rho_0 \otimes \sigma_1$, $\rho_1 \otimes \sigma_0$ or $\rho_1 \otimes \sigma_1$ identify which one in the bounded error setting. Let $p_{\varepsilon'}$ be the maximum probability of making a guess.

Expect: $p_{\varepsilon'} = O(a_\varepsilon \cdot b_\varepsilon)$ ("Direct Product Theorem")

Subtle:

- True classically, but optimal 2-register measurement is NOT a tensor measurement
- Not true if $\varepsilon' > \frac{1}{2}\varepsilon$
- Not true if we want to identify only $\rho_0 \otimes \sigma_0$, $\rho_1 \otimes \sigma_1$ vs. $\rho_0 \otimes \sigma_1$, $\rho_1 \otimes \sigma_0$ (can be $p_{\varepsilon'} = O(\sqrt{a_\varepsilon \cdot b_\varepsilon})$)

Tensor Lemma

Suppose we are given two independent problems:

ρ_0, ρ_1 with a_ε = max. prob. of guess

σ_0, σ_1 with b_ε = max. prob. of guess

Tensored problem: given $\rho_0 \otimes \sigma_0$, $\rho_0 \otimes \sigma_1$, $\rho_1 \otimes \sigma_0$ or $\rho_1 \otimes \sigma_1$ identify which one in the bounded error setting. Let $p_{\varepsilon'}$ be the maximum probability of making a guess.

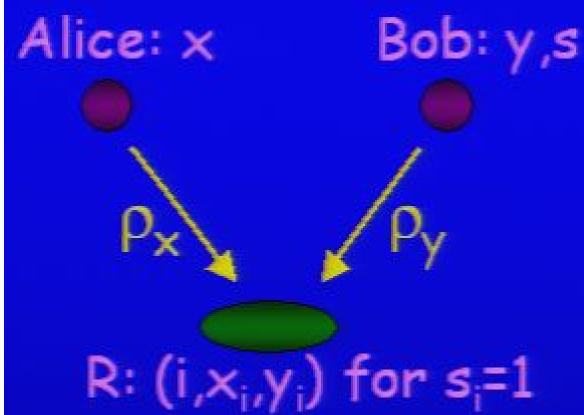
Expect: $p_{\varepsilon'} = O(a_\varepsilon \cdot b_\varepsilon)$ ("Direct Product Theorem")

We show (using semidefinite programming duality):

1. If ρ_0, ρ_1 pure and σ_0, σ_1 mixed, then $p_{\varepsilon/2} = O(a_\varepsilon \cdot b_\varepsilon)$.
2. In general $p_{\varepsilon/2} = O(|\rho_0 - \rho_1|_{tr} \cdot b_\varepsilon)$ (purify and use 1.)

R1, R2: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$

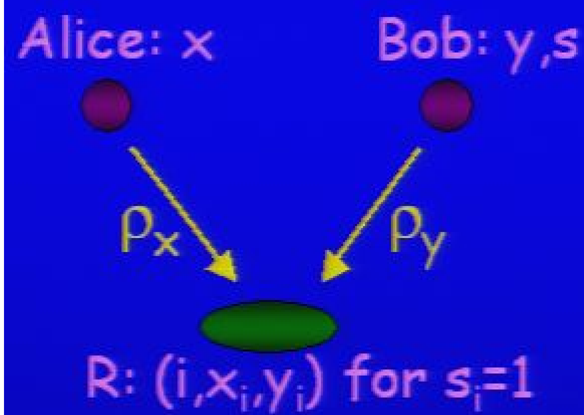


$\frac{1}{2}$ n "state identification problems"
Referee must solve at least one

Information theory and tensor lemma give lower bound.

R1, R2: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



$\frac{1}{2}$ n "state identification problems"
Referee must solve at least one

Information theory and tensor lemma give lower bound.

Tensor lemma also gives the lower bound for R2.

A separation for a Boolean <u>function</u>

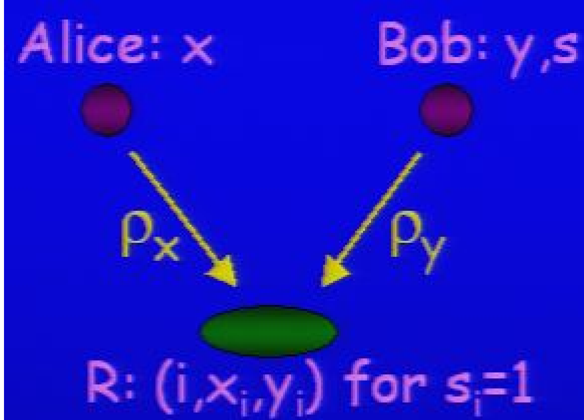
So far (nearly) all exponential separations for communication are for a relation (multi-valued):

- *One*-round: classical vs. quantum comm. [BJK'04]
- SMP: quantum comm. vs. classical w. public coin
- SMP: quantum comm. vs. classical w. entanglement

Exception: Two-round: classical vs. quantum comm. [Raz'99]

R1, R2: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



$\frac{1}{2}$ n "state identification problems"
Referee must solve at least one

Information theory and tensor lemma give lower bound.

Tensor lemma also gives the lower bound for R2.

Tensor Lemma

Suppose we are given two independent problems:

ρ_0, ρ_1 with a_ε = max. prob. of guess

σ_0, σ_1 with b_ε = max. prob. of guess

Tensored problem: given $\rho_0 \otimes \sigma_0$, $\rho_0 \otimes \sigma_1$, $\rho_1 \otimes \sigma_0$ or $\rho_1 \otimes \sigma_1$ identify which one in the bounded error setting. Let $p_{\varepsilon'}$ be the maximum probability of making a guess.

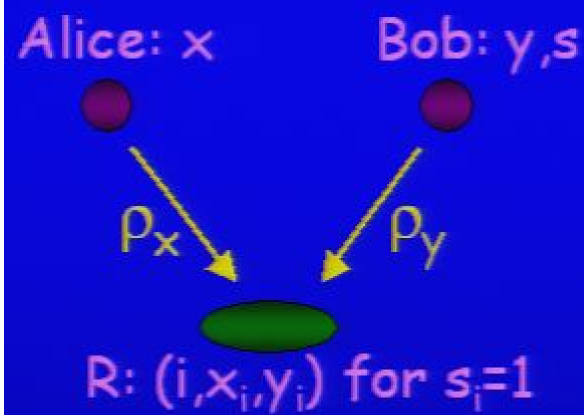
Expect: $p_{\varepsilon'} = O(a_\varepsilon \cdot b_\varepsilon)$ ("Direct Product Theorem")

We show (using semidefinite programming duality):

1. If ρ_0, ρ_1 pure and σ_0, σ_1 mixed, then $p_{\varepsilon/2} = O(a_\varepsilon \cdot b_\varepsilon)$.
2. In general $p_{\varepsilon/2} = O(|\rho_0 - \rho_1|_{tr} \cdot b_\varepsilon)$ (purify and use 1.)

R1, R2: lower bound

$$\boxed{Q_\varepsilon(R1) = \Omega(\sqrt[3]{n})}$$



$\frac{1}{2}$ n "state identification problems"
Referee must solve at least one

Information theory and tensor lemma give lower bound.

Tensor lemma also gives the lower bound for R2.

A separation for a Boolean function

So far (nearly) all exponential separations for communication are for a relation (multi-valued):

- One-round: classical vs. quantum comm. [BJK'04]
- SMP: quantum comm. vs. classical w. public coin
- SMP: quantum comm. vs. classical w. entanglement

Exception: Two-round: classical vs. quantum comm. [Raz'99]

A separation for a Boolean <u>function</u>

So far (nearly) all exponential separations for communication are for a relation (multi-valued):

- One-round: classical vs. quantum comm. [BJK'04]
- SMP: quantum comm. vs. classical w. public coin
- SMP: quantum comm. vs. classical w. entanglement

Exception: Two-round: classical vs. quantum comm. [Raz'99]

Question: Is there a such a separation for a function?

A separation for a Boolean function

So far (nearly) all exponential separations for communication are for a relation (multi-valued):

- One-round: classical vs. quantum comm. [BJK'04]
- SMP: quantum comm. vs. classical w. public coin
- SMP: quantum comm. vs. classical w. entanglement

Exception: Two-round: classical vs. quantum comm. [Raz'99]

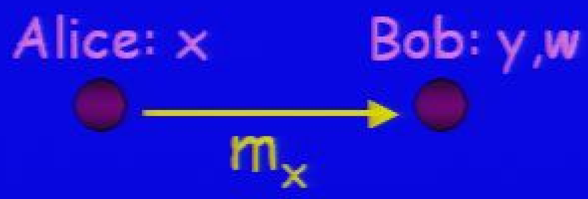
Question: Is there a such a separation for a function?

Result 4 [GKW'06]: One-round: $Q^1_\varepsilon(f) << R^{1,pub}_\varepsilon(f)$
There is a partial function $f(x,y)$ s. t. $Q^1_\varepsilon(f) = O(\log n^{3/2})$ and $R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n}\log n^{\frac{1}{4}})$.

Was independently proved for a slightly modified problem by Kerenidis and Raz in quant-ph/0607173.

The function

Variant of the hidden matching problem:

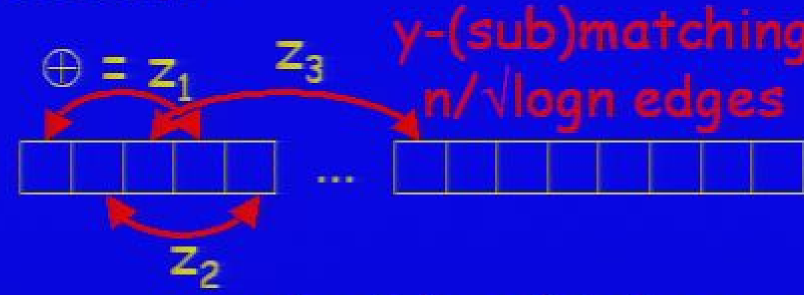


The function

Variant of the hidden matching problem:

Alice: x $\xrightarrow{m_x}$ Bob: y, w

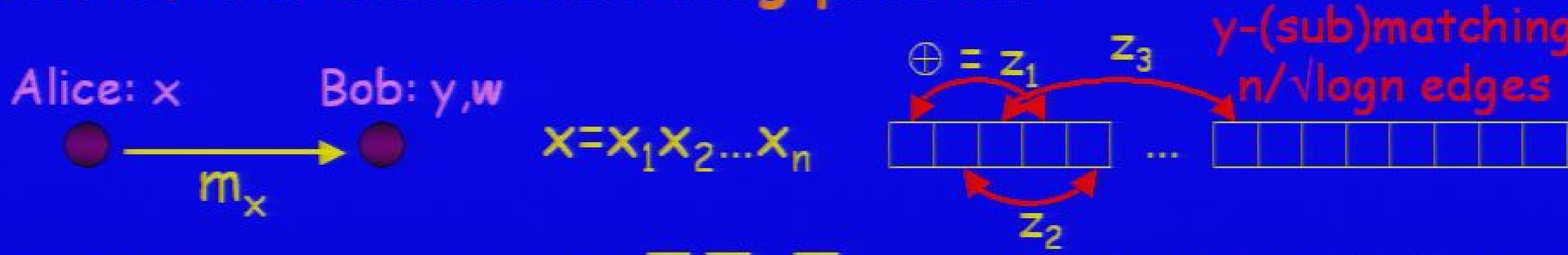
$x = x_1 x_2 \ldots x_n$



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z_{n/\sqrt{\log n}}}$ decide which one

The function

Variant of the hidden matching problem:



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z}_{n/\sqrt{\log n}}$ decide which one

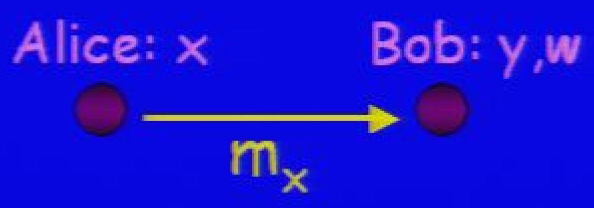
Input:
x - n bit string
y - $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ)
w - $n/\sqrt{\log n}$ bit string

Promise:
Let $z_\ell = x_{i_\ell} \oplus x_{j_\ell}$ string of XORs of the edges and $b \in \{0,1\}$.
Then $w = z \oplus b^{n/\sqrt{\log n}}$.

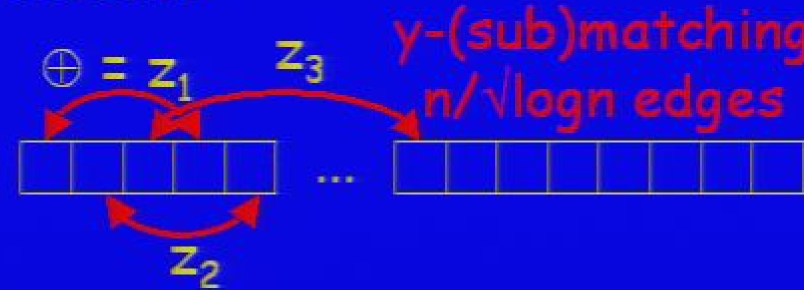
Output:
$f(x,y,w) = b$

The function

Variant of the hidden matching problem:



$x = x_1 x_2 \ldots x_n$



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z}_{n/\sqrt{\log n}}$ decide which one

Input:
x – n bit string
y – $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ)
w – $n/\sqrt{\log n}$ bit string

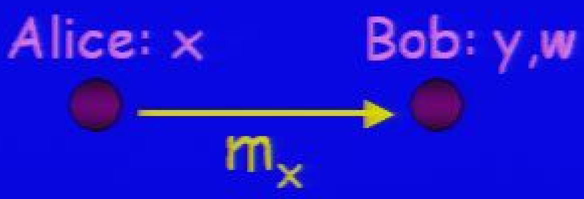
Promise:
Let $z_\ell = x_{i_\ell} \oplus x_{j_\ell}$ string of XORs of the edges and $b \in \{0,1\}$.
Then $w = z \oplus b^{n/\sqrt{\log n}}$.

Output:
$f(x,y,w) = b$

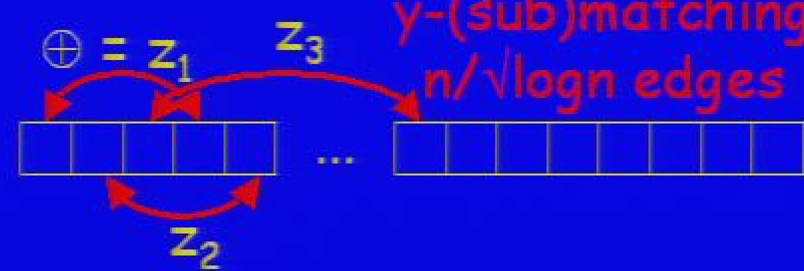
Quantum protocol: Alice sends $|m_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$

The function

Variant of the hidden matching problem:



$x=x_1x_2\ldots x_n$



$w = z_1z_2\ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2}\ldots\overline{z_{n/\sqrt{\log n}}}$ decide which one

Input:
x – n bit string
y – $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ)
w – $n/\sqrt{\log n}$ bit string

Promise:
Let $z_\ell = x_{i_\ell} \oplus x_{j_\ell}$ string of XORs of the edges and $b \in \{0,1\}$.
Then $w = z \oplus b^{n/\sqrt{\log n}}$.

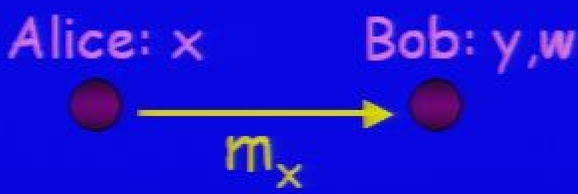
Output:
$f(x,y,w) = b$

Quantum protocol: Alice sends $|m_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$

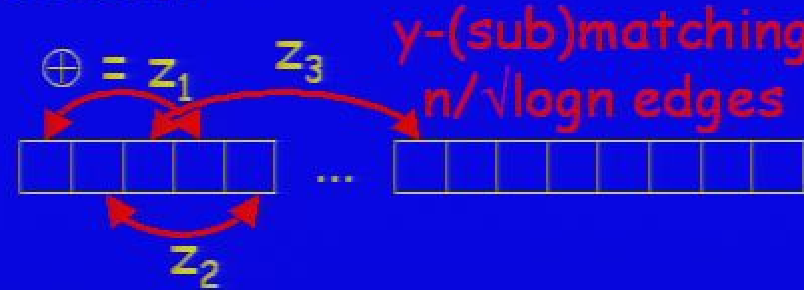
Bob: measures in basis spanned by the edges: $\Pi_\ell = |i_\ell\rangle\langle i_\ell| + |j_\ell\rangle\langle j_\ell|$

The function

Variant of the hidden matching problem:



$x = x_1 x_2 \ldots x_n$



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z}_{n/\sqrt{\log n}}$ decide which one

Input:
x - n bit string
y - $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ)
w - $n/\sqrt{\log n}$ bit string

Promise:
Let $z_\ell = x_{i\ell} \oplus x_{j\ell}$ string of XORs of the edges and $b \in \{0,1\}$.
Then $w = z \oplus b^{n/\sqrt{\log n}}$.

Output:
$f(x,y,w) = b$

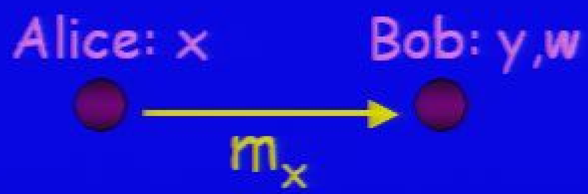
Quantum protocol: Alice sends $|m_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$

Bob: measures in basis spanned by the edges: $\Pi_\ell = |i_\ell\rangle\langle i_\ell| + |j_\ell\rangle\langle j_\ell|$

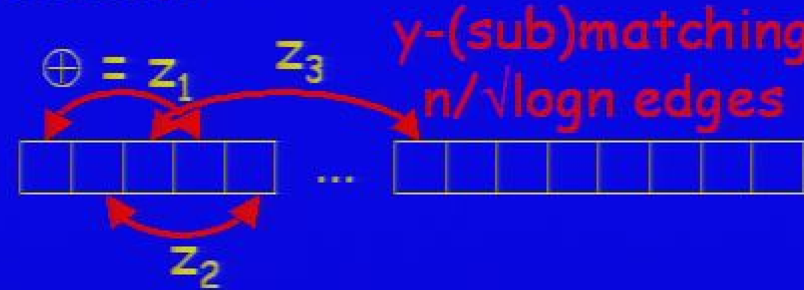
if outcome ℓ: $\frac{1}{\sqrt{2}}\left(|i_\ell\rangle + (-1)^{x_{i_\ell} \oplus x_{j_\ell}} |j_\ell\rangle\right)$

The function

Variant of the hidden matching problem:



$x = x_1 x_2 \ldots x_n$



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z}_{n/\sqrt{\log n}}$ decide which one

Input:
x - n bit string
y - $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ)
w - $n/\sqrt{\log n}$ bit string

Promise:
Let $z_\ell = x_{i\ell} \oplus x_{j\ell}$ string of XORs of the edges and $b \in \{0,1\}$.
Then $w = z \oplus b^{n/\sqrt{\log n}}$.

Output:
$f(x,y,w) = b$

Quantum protocol: Alice sends $|m_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$

Bob: measures in basis spanned by the edges: $\Pi_\ell = |i_\ell\rangle\langle i_\ell| + |j_\ell\rangle\langle j_\ell|$

if outcome ℓ: $\frac{1}{\sqrt{2}}\left(|i_\ell\rangle + (-1)^{x_{i_\ell} \oplus x_{j_\ell}} |j_\ell\rangle\right)$

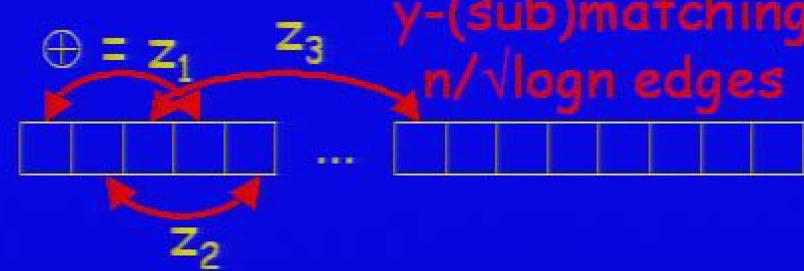
measure in $|\pm\rangle$ basis to determine $z_\ell = x_{i\ell} \oplus x_{j\ell}$, compare with w_ℓ

The function

Variant of the hidden matching problem:

Alice: x $\xrightarrow{m_x}$ Bob: y,w

$x = x_1 x_2 \ldots x_n$



$w = z_1 z_2 \ldots z_{n/\sqrt{\log n}}$ or $w = \overline{z_1}\,\overline{z_2} \ldots \overline{z}_{n/\sqrt{\log n}}$ decide which one

Input:	Promise:	Output:
x – n bit string y – $n/\sqrt{\log n}$ edges (i_ℓ, j_ℓ) w – $n/\sqrt{\log n}$ bit string	Let $z_\ell = x_{i\ell} \oplus x_{j\ell}$ string of XORs of the edges and $b \in \{0,1\}$. Then $w = z \oplus b^{n/\sqrt{\log n}}$.	$f(x,y,w) = b$

zero-error

Quantum protocol: Alice sends $|m_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$ logn qubits

Bob: measures in basis spanned by the edges: $\Pi_\ell = |i_\ell\rangle\langle i_\ell| + |j_\ell\rangle\langle j_\ell|$

if outcome ℓ: $\frac{1}{\sqrt{2}}\left(|i_\ell\rangle + (-1)^{x_{i_\ell} \oplus x_{j_\ell}} |j_\ell\rangle\right)$ $1/\sqrt{\log n}$ probability

measure in $|\pm\rangle$ basis to determine $z_\ell = x_{i\ell} \oplus x_{j\ell}$, compare with w_ℓ

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f)=\Omega(\sqrt{n}\ \log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f)=\Omega(\sqrt{n}\ \log n^{\frac{1}{4}})$ (tight)

Lower bound - ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n} \log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with > 2^{n-c-1} x's in its pre-image and error at most 1/5. Fix this message m.

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n}\,\log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with $> 2^{n-c-1}$ x's in its pre-image and error at most 1/5. Fix this message m.
3. We show: given m and for uniform y and x in its pre-image, the distribution of z is close to uniform (if $c < \sqrt{n}\,\log n^{\frac{1}{4}}$): $d(z, U_{n/\sqrt{\log n}}) < \delta$

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$	$R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n}\,\log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with > 2^{n-c-1} x's in its pre-image and error at most 1/5. Fix this message m.
3. We show: given m and for uniform y and x in its pre-image, the distribution of z is close to uniform (if $c<\sqrt{n}\,\log n^{\frac{1}{4}}$): $d(z,U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}}, U_{n/\sqrt{\log n}}) < \delta$ & $d(z\oplus 1^{n/\sqrt{\log n}}, U_{n/\sqrt{\log n}}) < \delta$

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f)=\Omega(\sqrt{n}\,\log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with $> 2^{n-c-1}$ x's in its pre-image and error at most 1/5. Fix this message m.
3. We show: given m and for uniform y and x in its pre-image, the distribution of z is close to uniform (if $c<\sqrt{n}\,\log n^{\frac{1}{4}}$): $d(z,U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta \;\&\; d(z\oplus 1^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}}, z\oplus 1^{n/\sqrt{\log n}}) < 2\delta$

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $\qquad R^{1,pub}_\varepsilon(f)=\Omega(\sqrt{n}\,\log n^{\frac{1}{4}})$ (tight)

Lower bound – ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with $> 2^{n-c-1}$ x's in its pre-image and error at most 1/5. Fix this message m.
3. We show: given m and for uniform y and x in its pre-image, the distribution of z is close to uniform (if $c<\sqrt{n}\log n^{\frac{1}{4}}$): $d(z,U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta$ & $d(z\oplus 1^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}}, z\oplus 1^{n/\sqrt{\log n}}) < 2\delta$

$\rightarrow$ Bob cannot distinguish the two cases and determine b

Classical lower bound for f

$Q^1_\varepsilon(f) = O(\log n^{3/2})$ $R^{1,pub}_\varepsilon(f)=\Omega(\sqrt{n}\ \log n^{\frac{1}{4}})$ (tight)

Lower bound - ideas:

1. By Yao's principle assume deterministic protocol and uniform distribution on x,y and b (this fixes w)
2. Assume c bits of communication, error 1/10. The 2^c messages partition the x's into 2^c sets (pre-images). At least half the x's appear in sets of size at least 2^{n-c-1}. Hence there is a message m with $> 2^{n-c-1}$ x's in its pre-image and error at most 1/5. Fix this message m.
3. We show: given m and for uniform y and x in its pre-image, the distribution of z is close to uniform (if $c<\sqrt{n}\ \log n^{\frac{1}{4}}$): $d(z,U_{n/\sqrt{\log n}}) < \delta$

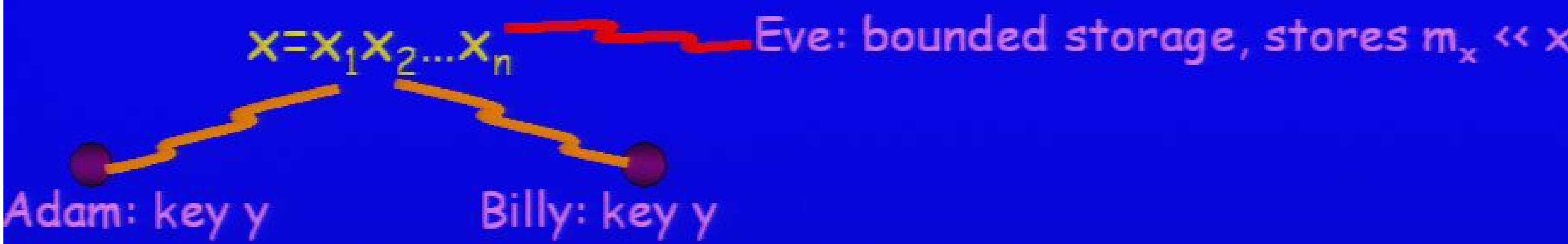
$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta$ & $d(z\oplus 1^{n/\sqrt{\log n}},U_{n/\sqrt{\log n}}) < \delta$

$\rightarrow d(z\oplus 0^{n/\sqrt{\log n}}, z\oplus 1^{n/\sqrt{\log n}}) < 2\delta$

$\rightarrow$ Bob cannot distinguish the two cases and determine b

Bounded storage model

Bounded storage model - secure secret key generation:



Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$ — Eve: bounded storage, stores $m_x \ll x$

Adam: key y $\downarrow$ z

Billy: key y $\downarrow$ z

Adam and Billy use y to extract secret shared key z from x

Bounded storage model

Bounded storage model - secure secret key generation:

Eve: bounded storage, stores m_x << x

Adam and Billy use y to extract secret shared key z from x

Adam: key y

z

Billy: key y

z

"Everlasting security": z is secure

Bounded storage model

Bounded storage model - secure secret key generation:

Eve: bounded storage, stores $m_x \ll x$

Adam: key y → z

Billy: key y → z

Adam and Billy use y to extract secret shared key z from x

"Everlasting security": z is secure <u>even if Eve learns y</u> later

i.e. distribution of z given m_x and y is close to uniform for uniform y and x (in pre-image of m_x)

Bounded storage model

Bounded storage model - secure secret key generation:

Eve: bounded storage, stores $m_x \ll x$

Adam: key y → z

Billy: key y → z

Adam and Billy use y to extract secret shared key z from x

"Everlasting security": z is secure <u>even if Eve learns y</u> later

i.e. distribution of z given m_x and y is close to uniform for uniform y and x (in pre-image of m_x)

Question: Does z remain secure if storage is quantum?

Bounded storage model

Bounded storage model - secure secret key generation:

Eve: bounded storage, stores $m_x \ll x$

Adam: key y → z

Billy: key y → z

Adam and Billy use y to extract secret shared key z from x

"Everlasting security": z is secure even if Eve learns y later

i.e. distribution of z given m_x and y is close to uniform for uniform y and x (in pre-image of m_x)

Question: Does z remain secure if storage is quantum?

Corollary:

NO (at least in certain settings there is a counterexample).

Bounded storage model

Bounded storage model – secure secret key generation:

$x = x_1 x_2 \ldots x_n$

Eve: bounded storage, stores $m_x \ll x$

Adam: key y → z

Billy: key y → z

Adam and Billy use y to extract secret shared key z from x

Bounded storage model

Bounded storage model – secure secret key generation:

$x = x_1 x_2 \ldots x_n$

Eve: bounded storage, stores $m_x \ll x$

Billy: key y

$\downarrow$

z

Adam and Billy use y to extract secret shared key z from x

Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$

Eve: bounded storage, stores $m_x \ll x$

Adam: key y → z

Billy: key y → z

Adam and Billy use y to extract secret shared key z from x

Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$

Eve: bounded storage, stores $m_x \ll x$

Billy: key y

$\downarrow$

z

Adam and Billy use y to extract secret shared key z from x

Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$ — Eve: bounded storage, stores $m_x \ll x$

Billy: key y

$\downarrow$

z

Adam and Billy use y to extract secret shared key z from x

Eve: given m_x and y tries to infer z

Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$

Eve: bounded storage, stores $m_x \ll x$

Billy: key y

$\downarrow$

z

Adam and Billy use y to extract secret shared key z from x

Eve: given m_x and y tries to infer z

One-way communication:

Alice: x $\xrightarrow{m_x}$ Bob: y

Bob: given m_x and y tries to infer z

Bounded storage model

Bounded storage model - secure secret key generation:

$x = x_1 x_2 \ldots x_n$ Eve: bounded storage, stores $m_x \ll x$

Billy: key y

$\downarrow$

z

Adam and Billy use y to extract secret shared key z from x

Eve: given m_x and y tries to infer z

One-way communication:

Alice: x $\xrightarrow{m_x}$ Bob: y

Bob: given m_x and y tries to infer z

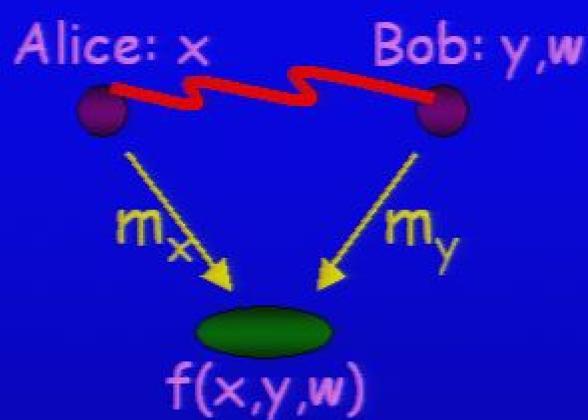
Our function gives counterexample:

if classical storage $= \sqrt{n} \log n^{\frac{1}{4}}$ then z is close to uniform

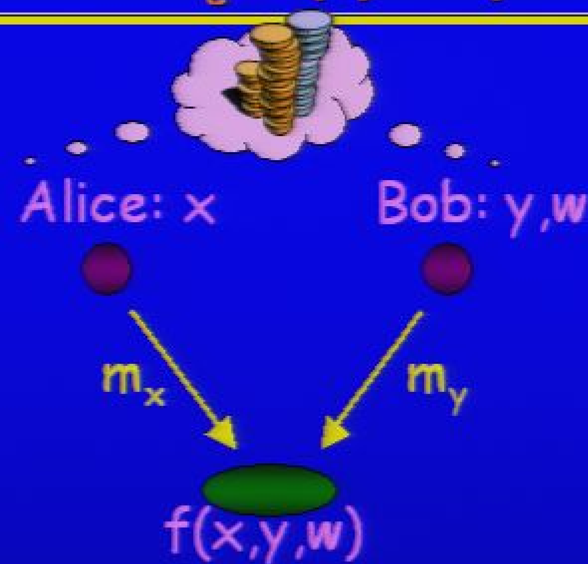
if quantum storage $= \sqrt{n} \log n^{\frac{1}{4}}$ z is far from uniform

SMP separation for f

One way: $Q^1_\varepsilon(f) = O(\log n^{3/2})$ and $R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n} \log n^{\frac{1}{4}})$

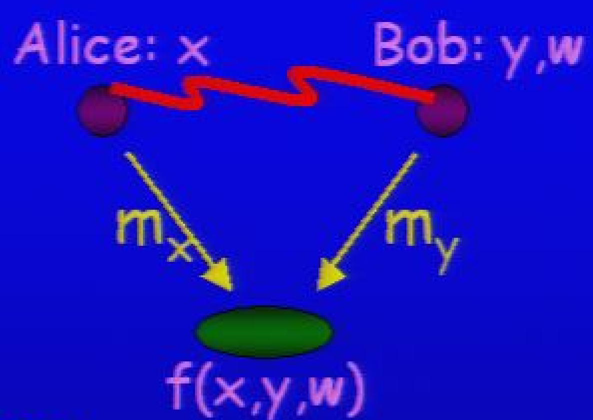


vs.

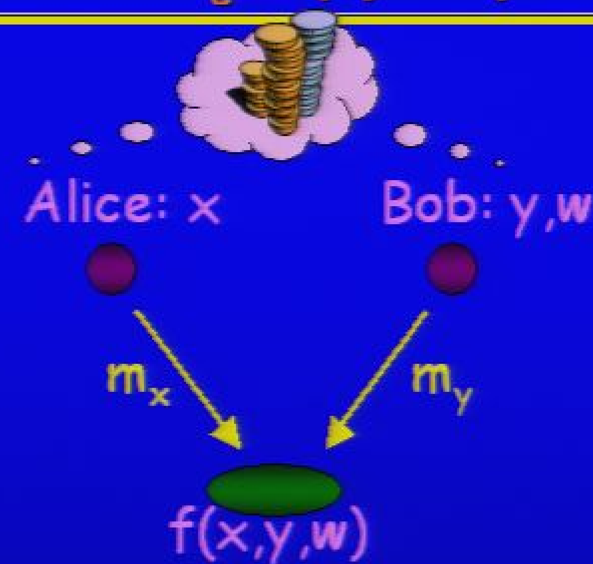


SMP separation for f

One way: $Q^1_\varepsilon(f) = O(\log n^{3/2})$ and $R^{1,pub}_\varepsilon(f) = \Omega(\sqrt{n} \log n^{\frac{1}{4}})$



vs.



Corollary:

Quantum protocol also works in SMP model with shared entanglement (similar to the Buhrman protocol)

Classical lower bound also holds in the SMP model for classical communication with public coin.

$R_\varepsilon^{ent}(f) = O(\log n^{3/2})$ $R_\varepsilon^{pub}(f) = \Omega(\sqrt{n} \log n^{\frac{1}{4}})$

Summary

- One round separation for a Boolean function ($Q^1_\varepsilon(f) \ll R^1_\varepsilon{}^{pub}(f)$ and $R_\varepsilon^{ent}(f) \ll R_\varepsilon^{pub}(f)$); example where quantum bounded storage becomes insecure
- Bounded error quantum state identification pb.
- Tensor lemma (direct product theorem)
- Classical communication + shared randomness beats qubit communication ($R_\varepsilon^{pub}(R1) \ll Q_\varepsilon(R1)$)
- Classical communication + shared entanglement beats qubit communication ($R_\varepsilon^{ent}(R2) \ll Q_\varepsilon^{pub}(R2)$)
- Fingerprints in the SMP model can simulate multi-round protocols with unlimited entanglement (with exponential overhead)

Open Questions

- An exponential separation for a *total* Boolean function (instead of a partial one)?
- Prove or disprove the general tensor lemma (would imply $Q_\varepsilon(R1)=\Omega(\sqrt{n})$, which is tight)
- Is there a relation (or function) R such that $R_\varepsilon^{ent}(R) >> Q_\varepsilon^{pub}(R)$?
- Other applications of the tensor lemma?

Thank you!

joint work with

Dmitry Gavinsky

Oded Regev

Ronald de Wolf

[GKWR'06] **D. Gavinsky, J. Kempe, O. Regev, R. de Wolf**: "*Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity*", **STOC'06**, p. 594-603 (2006), quant-ph/0511013

[GKW-1'06] **D. Gavinsky, J. Kempe, R. de Wolf**: "*Strengths and Weaknesses of Quantum Fingerprinting*", **Complexity'06**, p. 288-195 (2006), quant-ph/0603173

[GKW-2'06] **D. Gavinsky, J. Kempe, R. de Wolf**: "*Exponential Separation of Quantum and Classical One-Way Communication Complexity for a Boolean Function*", quant-ph/0607174

[KR'06] **I. Kerenidis, Ran Raz**: "*The one-way communication complexity of the Boolean Hidden Matching Problem*", quant-ph/0607173