Example: $D^{\|}(EQ)=2n$, $R^{\|\,pub}(EQ)=\Theta(1)$ (same protocols).

$R^{\|\,priv}(EQ)=\Theta(\sqrt{n})$ (same protocol doesn't work - Alice sends $(i, E(x)_i)$, but Bob doesn't know i. So each sends $\Theta(\sqrt{n})$ pairs in order for the Referee to find collisions - Birthday Paradox).

We will see a quantum protocol (with no sharing!!) that shows:

$Q^{\|}(EQ)=O(\log n)$ [De Wolf, Burman, '01]

(**) Recall that for any $\varepsilon>0$ we can choose an Error Correcting Code $E:\{0,1\}^n\to\{0,1\}^m$, $m>n$, such that, $\forall x\neq y$ $\frac{1+\varepsilon}{2}m \geq \underbrace{d(E(x),E(y))}_{\text{Hamming distance}} \geq \frac{1-\varepsilon}{2}m$

<u>Quantum fingerprints</u>

Is a transformation from $\{0,1\}^n$ into a space of $\log m$ qubits:

$$x \longrightarrow |m_x\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}(-1)^{\overbrace{E(x)_i}^{\text{the } i^{th} \text{ bit of } E(x)}}|i\rangle \qquad (E \text{ from } (**))$$

- $\log m = \log n\cdot c = \log n + \log c = O(\log n)$

- The states $|m_x\rangle$ are all different but not all are orthogonal.

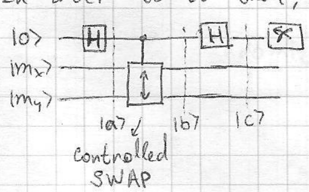
$$\langle m_x|m_x\rangle = 1. \quad \langle m_x|m_y\rangle = \frac{1}{m}\cdot\sum_{i,j}(-1)^{E(x)_i+E(x)_j}\langle i,j\rangle = \frac{1}{m}\cdot\sum_{i=1}^{m}(-1)^{E(x)_i+E(x)_i} \in[-\varepsilon,\varepsilon]$$

because of the way we chose E.

So to <u>solve EQ</u> in the SMP model Alice and Bob send the referee $|m_x\rangle, |m_y\rangle$.

He needs to decide ~~whether~~ if $\langle m_x|m_y\rangle=1$ (then $EQ(x,y)=1$) or $\langle m_x|m_y\rangle\approx 0$ (then $EQ(x,y)=0$).

In order to do that, the referee will use the <u>SWAP test</u>:



- If $|m_x\rangle=|m_y\rangle$: $\Pr(``1")=0$ (SWAP has no effect since $|m_x\rangle=|m_y\rangle$).

~~- If $|\langle m_x|m_y\rangle|\leq\varepsilon$~~ :

If $|\langle m_x | m_y \rangle| \leq \varepsilon$: - ~~the~~

$|a\rangle = \frac{1}{\sqrt{2}} |0\rangle |m_x\rangle |m_y\rangle + \frac{1}{\sqrt{2}} |1\rangle |m_x\rangle |m_y\rangle$

$|b\rangle = \frac{1}{\sqrt{2}} |0\rangle |m_x\rangle |m_y\rangle + \frac{1}{\sqrt{2}} |1\rangle |m_y\rangle |m_x\rangle$

$$|c\rangle = \frac{1}{2}\Big(\big(|0\rangle + |1\rangle\big) |m_x\rangle|m_y\rangle + \big(|0\rangle - |1\rangle\big) |m_y\rangle|m_x\rangle\Big) = |0\rangle \cdot \frac{|m_x\rangle|m_y\rangle + |m_y\rangle|m_x\rangle}{2} + |1\rangle \frac{|m_x\rangle|m_y\rangle - |m_y\rangle|m_x\rangle}{2}$$

Hence: $P(\text{"1"}) = \frac{1}{4} \| |m_x\rangle|m_y\rangle - |m_y\rangle|m_x\rangle \|^2 = \frac{1}{4} \cdot \big(\langle m_x|\langle m_y| - \langle m_y|\langle m_x|\big)\big(|m_x\rangle|m_y\rangle - |m_y\rangle|m_x\rangle\big)$

$= \frac{1}{4}\Big(1+1 - \big(\langle m_y|\langle m_x|\big)\big(|m_x\rangle|m_y\rangle\big) - \big(\langle m_x|\langle m_y|\big)\big(|m_y\rangle|m_x\rangle\big)\Big) =$

~~$2\cdot\langle m_x, m_x\rangle\langle m_y, m_y\rangle$~~ $= \frac{1}{4}\left(2 - 2\cdot |\langle m_x|m_y\rangle|^2\right) \geq \frac{1}{2}(1-\varepsilon^2)$

- So the referee will either know that $|m_x\rangle \neq |m_y\rangle$, if he measures "1", or, if he measures "0", he knows that with constant probability $|m_x\rangle = |m_y\rangle$.

Repeat the protocol several times to get better probabilities.

$Q''(EQ) = O(\log n)$

Example: $IP(x,y) = \sum_{i=1}^{n} x_i \cdot y_i \mod 2$ (Inner Product).

$D(IP) = n$

Example $DISJ(x,y) = NOR(\underbrace{x \wedge y}_{\text{bit-wise AND}})$ (Disjoint)

$DISJ(x,y) = 1 \iff \nexists i$ such that $x_i = y_i = 1$

$D(DISJ) = n$. Proved in '92: $R(DISJ) = \Theta(n)$ by Kalyanasundaram Schnitger

$Q(DISJ) = O(\sqrt{n})$ (Using a variation of Grover)

A, B have to decide if $\exists i$ s.t. $x_i = y_i = 1$. So, for $z = x \wedge y$, they have to decide if $\exists i$ s.t. $z_i = 1$. This is a search on n bits $z_1, \dots, z_n$, $z_i = f(i)$

We can't use Grover directly, because we don't have a black box for f.

In order to simulate the U_f-s in Grover's algorithm, they will use the protocol

$$\underbrace{\sum_i \alpha_i \cdot |i,b\rangle|0\rangle}_{\text{Alice}} \xrightarrow[\text{(unitary)}]{\text{operation}} \sum_i \alpha_i \cdot |i,b\rangle|x_i\rangle \xrightarrow[O(\log n)]{\text{to Bob}} \underbrace{\sum_i \alpha_i \, |i, b\oplus(x_i \wedge y_i), x_i\rangle}_{\text{Bob}} \xrightarrow[O(\log n)]{\text{to Alice}} \sum_i \alpha_i \, |i, b \oplus (x_i \dots$$

XOR the x_i, and ignore the qubit

A total of $O(\log n)$ bits per round, $O(\sqrt{n})$ rounds.

So this protocol achieves $O(\sqrt{n}\log n)$, due to Burman, Cleve, Widgerson '98

It is possible to improve to $O(\sqrt{n})$.

Theorem: Let $g: \{0,1\}^n \to \{0,1\}$ and $f(x,y) = g(x * y)$, where $*$ is a bitwise operation, $* : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. If there exists a T-query quantum algorithm for g, then $Q(f) \le T \cdot (2\log n + 4)$.

Example: Distributed Deutsch-Josza: $EQ'(x,y) = DeJo(x \oplus y)$, where

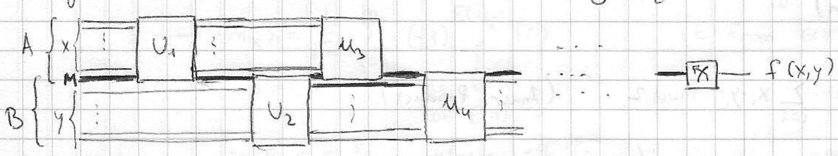
$$DeJo(z) = \begin{cases} 1 & z = 11\ldots1 \text{ or } z = 00\ldots0 \\ 0 & \underbrace{Ham(z)}_{\text{Hamming weight}} = n/2 \end{cases}$$

There is a 1-query algorithm for DeJo, so $Q(EQ') = O(\log n)$ (by the theorem)

However $D(EQ') = \Theta(n)$

We now want to show a lower bound for $Q(IP)$.

We will describe ~~the~~ the communication as a circuit, with a shared quantum register M, which describes the message-qubit.



Lower bound B in this model gives a lower bound of $\frac{B}{2}$ in the general model (since we always send only 1 qubit here, we can simulate sending a set of k qubits ~~&~~ by sending them 1 by 1, where the 2nd party sends garbage).

Singular value decomposition: $\forall A$-matrix $\exists U, V$-unitaries s.t. $A = UDV$, where $D = \text{diagonal}(s_1, \ldots, s_n)$, $s_i \geq 0$. s_i are called "singular value of A".

$$A = \sum_{i=1}^{\text{rank}A} s_i \cdot \underbrace{|\varphi_i\rangle}_{\text{columns of } U} \cdot \underbrace{\langle \psi_i|}_{\text{rows of } V}$$

Remark: In the eigenvalue decomposition $|\varphi_i\rangle = \langle \psi_i|^{\dagger}$ $(U = V^{\dagger})$

Define some matrix norms: Trace norm: $\|A\|_{tr} = \sum_{i=1}^{\text{rank}A} s_i$

Frobenius norm: $\|A\|_F = \|A\|_2 = \sqrt{\sum s_i^2} = \sqrt{tr(A^*A)} = \sqrt{\sum_{i,j} |a_{ij}|^2}$

Infinity norm: (operator norm) $\|A\|_{op} = \|A\|_{\infty} = \max_i s_i = \max_{x, \|x\|=1} \|Ax\|$

For those 3 norms: $\forall U, V$-unitaries: $\|A\| = \|UAV\|$

__Definition__: The __inner product__ of matrices A, B is:

$$\underline{\langle A,B\rangle} = \sum_{ij} a_{ij}^* b_{ij} = tr(A^\dagger B)$$

(1) $\langle UAV, UBV\rangle = tr(V^\dagger A^\dagger U^\dagger U B V) = tr(A^\dagger B) = \langle A, B\rangle$
U, V unitaries

(2) $\langle A, A\rangle = \|A\|_F$

__Lemma__: $|\langle A,B\rangle| \leq \|A\|_{tr} \cdot \|B\|_{op}$

__Proof__: Use the singular value decomposition: $A = \sum_i s_i |\varphi_i\rangle\langle\psi_i|$

$$|\langle A,B\rangle| = |tr(\sum_i s_i |\psi_i\rangle\langle\varphi_i| \cdot B)| \underset{\text{triangle-ineq.}}{\leq} \sum_i s_i \cdot tr \cdot ||\psi_i\rangle\langle\varphi_i| B| =$$

$$= \sum_i s_i \cdot |\langle\varphi_i| B |\psi_i\rangle| \underset{\||\varphi_i\rangle\| = 1}{\leq} \sum_i s_i \cdot \|B|\psi_i\rangle\| \leq \sum_i s_i \cdot \|B\|_{op} = \|A\|_{tr} \cdot \|B\|_{op}.$$

$\square$

__Yao-Kremer decomposition__: protocol with q qubits of communication (in our circuit-model) $\rightarrow$ then the final state is of the form:

$$\sum_{m \in \{0,1\}^q} |\alpha_{x,m}\rangle \cdot |m_q\rangle |\beta_{y,m}\rangle, \quad \text{s.t } m_q \text{ - last bit of } m, \ \||\alpha_{x,m}\rangle\| \leq 1, \ \||\beta_{y,m}\rangle\| \leq$$

Proof is by induction on q. For $q=0$ it's trivial. Assume for q. Assume Alice applies U_{q+1} (similar for Bob). The new state becomes:

$$|new\rangle = \sum_{m \in \{0,1\}^q} U_{q+1}(|\alpha_{x,m}\rangle \cdot |m_q\rangle) \cdot |\beta_{y,m}\rangle$$

Let $\Pi_0 = |0\rangle\langle 0|$, $\Pi_1 = |1\rangle\langle 1|$ projection on $|0\rangle$ of message qubit, and let $Tr_A(|\alpha\rangle|m\rangle) = |\alpha\rangle$.

Then: $|\alpha_{x,m_0}\rangle := Tr_A \Pi_0 U_{q+1}(|\alpha_{x,m}\rangle |m_q\rangle)$, $|\alpha_{x,m_1}\rangle := Tr_A \Pi_1 U_{q+1}(|\alpha_{x,m}\rangle |m_q\rangle)$.

By definition: $|\alpha_{x,m_0}\rangle|0\rangle + |\alpha_{x,m_1}\rangle|1\rangle = U_{q+1} |\alpha_{x,m}\rangle|m_q\rangle \quad (m_0 \in \{0,1\}^{q+1}, \ m_1 \in \{0,1\}^{q+1})$

Also, define $|\beta_{y,m_0}\rangle = |\beta_{y,m_1}\rangle = |\beta_{y,m}\rangle$. So:

$$|new\rangle = \sum_{m \in \{0,1\}^{q+1}} |\alpha_{x,m}\rangle|m_q\rangle|\beta_{y,m}\rangle$$

$\square$

Hence, the probability to ~~measure~~ accept x,y after q steps is:

$$Pr(\text{"1"}) = \left\| \sum_{\substack{m \in \{0,1\}^q \\ m_q = 1}} |\alpha_{x,m}\rangle |\beta_{y,m}\rangle \right\|^2 = \sum_{\substack{m, m_q = 1 \\ m', m'_q = 1}} \underbrace{\langle\alpha_{x,m}|\alpha_{x,m'}\rangle}_{\alpha_{x,k}} \cdot \underbrace{\langle\beta_{y,m}|\beta_{y,m'}\rangle}_{\beta_{y,k}}$$

So: $Pr(\text{"1"}) = \sum_{k=1}^{2^{2q-2}} \alpha_{x,k} \cdot \beta_{y,k}$, for $|\alpha_{x,k}|, |\beta_{y,k}| \leq 1$, $\alpha_{x,k}, \beta_{y,k} \in \mathbb{C}$

__Corollary__: Let P be a $2^n \times 2^n$ matrix of acceptance probabilities$_x$ of a protocol wit q qubits of communication. Then $q \geq \frac{1}{2} \log \frac{\|P\|_{tr}}{2^n}$.