Reminder:

Cor: Let $P$ be a matrix of acceptance probabilities of a $q$-qubit communication protocol. $\Rightarrow$ $q \geq \frac{1}{2}\log\frac{\|P\|_{tr}}{2^n}$

If $P$ is the matrix of a communication protocol for $IP$, if $IP(x,y)=0$ then $P_{x,y} \geq \frac{2}{3}$ and if $IP(x,y)=1$ then $P_{x,y} \leq \frac{1}{3}$

Reminder:

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

Let $M_{IP}$ be the matrix: $(M_{IP})_{x,y} = (-1)^{IP(x,y)}$

$$M_{IP}^{(1)} = \begin{array}{c} \\ 0 \\ 1 \end{array}\begin{array}{c} \begin{array}{cc} 0 & 1 \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array} = \sqrt{2}\cdot M$$

It is easy to prove: $M_{IP}^{(k)} = (\sqrt{2})^k \cdot H^{\otimes k}$

$$M_{IP}^{(2)} = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array} = 2\cdot H\otimes H$$

Put $A=P$, $B=M_{IP}$ into the lemma:

$$\|P\|_{tr} \geq \frac{|\langle P, M_{IP}\rangle|}{\|M_{IP}\|_{op}} = \frac{|\langle P, M_{IP}\rangle|}{2^{n/2}}$$

$\|M_{IP}\|_{op}$ = maximum eigenvalue of $M_{IP}$ = maximum eigenvalue of $(\sqrt{2})^n \cdot H^{\otimes n}$

$(M_{IP})_{x,y}=1 \longrightarrow P_{x,y} \geq \frac{2}{3}$, $(M_{IP})_{x,y}=-1 \longrightarrow P_{x,y} \leq \frac{1}{3}$

Each row of $M_{IP}$, except for the 1st, has $\frac{n}{2}$ ones and $\frac{n}{2}$ zeros.

$$\langle P, M_{IP}\rangle = \sum_{x,y} (M_{IP})_{x,y}\cdot (P_{x,y})^* \geq \underbrace{2^n \cdot \frac{2}{3}}_{1^{st}\text{ row}} + \underbrace{2^{n-1}}_{\text{other rows}}\left(\frac{2}{3}\cdot 2^{n-1} - \frac{1}{3}\cdot 2^{n-1}\right) \geq 2^{2n-1}\cdot\frac{1}{3}$$

So, from Cor., any $q$-qubit communication protocol has:

$$q \geq \frac{1}{2}\log\frac{2^{2n-1}}{2^n\cdot 3\cdot 2^{n/2}} = \frac{1}{2}\log\frac{2^{n/2}}{6} = \frac{n}{4} - \frac{1}{2}\log 6 \geq \frac{n}{4} - 2$$

(This is a lower bound for computing $IP$ with quantum communication)

Remark: This lower bound can be impoved to $n-c$, $c$ is constant.

# Quantum Information

## Bell inequalities

Assume Alice & Bob share an EPR state. We send Alice $x \in \{0,1\}$, and Bob $y \in \{0,1\}$, which tells them in what basis to measure the state (from 2 predetermined basises). They answer $a,b \in \{0,1\}$. We want Alice & Bob to send us $a,b$ such that $a \oplus b = x \wedge y$. (Each of them only knows either $x$ or $y$).


- A deterministic strategy (without quantum and ~~prob~~ randomization) can't solve this with probability higher than $\frac{3}{4}$.
- Any randomized strategy (with either ~~random~~ public or private coins) is a distribution on deterministic strategies. So any non-quantum strategy wins w.p $\leq 75\%$

Quantumly: if A&B share 1 EPR pair they can win w.p $\geq 85\%$.

Alice

$x=1$ Std. basis. "1" "0" Return measurement

$x=0$ $|+\rangle, |-\rangle$ basis, $|-\rangle$ return 0, $|+\rangle$ return 1

Bob

$y=0$ Basis: $1_0$ "1", $0_0$ "0"

$y=1$ Basis: $1_1$ "1", $0_1$ "0", $\alpha = 22.5^\circ$

Assume Alice measures 1st.

$x=0, y=0$ : $Pr(a \oplus b = 0) = Pr(a=0 \wedge b=0) + Pr(a=1 \wedge b=1) = Pr(a=0) \cdot Pr(b=0 \mid a=0) +$

$+ Pr(a=1) \cdot Pr(b=1 \mid a=1) = \frac{1}{2} Pr(b=0 \mid \text{Bob's state: } |-\rangle) + \frac{1}{2} Pr(b=1 \mid \text{Bob's state: } |+\rangle) =$

$= \frac{1}{2} \left( |\langle 0_0 | - \rangle|^2 + |\langle 1_0 | + \rangle|^2 \right) = (\cos\alpha)^2$

$x=0, y=1$ : $Pr(a \oplus b = 0) = \frac{1}{2} \left( |\langle 0_1 | - \rangle|^2 + |\langle 1_1 | + \rangle|^2 \right) = (\cos\alpha)^2$

$x=1, y=0$ : $Pr(a \oplus b = 0) = \frac{1}{2} \left( |\langle 0_0 | 0 \rangle|^2 + |\langle 1_0 | 1 \rangle|^2 \right) = (\cos\alpha)^2$

$x=1, y=1$ : $Pr(a \oplus b = 1) = \frac{1}{2} \left( |\langle 1_1 | 0 \rangle|^2 + |\langle 0_1 | 1 \rangle|^2 \right) = (\cos\alpha)^2$

So winning probability is $\cos^2\alpha = \frac{1}{2}(1+\cos 2\alpha) = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \geq 0.85$

Remark: Taking $\alpha = 22.5^\circ$ is optimal$_\times$ for this protocol.

This probability for success is optimal for any quantum protocol!

Proof: Assume Alice & Bob share some $|\psi\rangle$ state (of any dimension!).

A measurement can be modeled by $\leq 2$ projectors: $\Pi_0, \Pi_1$, $\Pi_j^2 = \Pi_j = \Pi_j^\dagger$, and $\Pi_0 + \Pi_1 = \mathbb{1}$ (if we didn't measure "0", then we had to measure "1")

The probability to measure "0" is $\|\Pi_0|\psi\rangle\|^2 = \langle\psi|\Pi_0|\psi\rangle$ (since $\Pi_0^2 = \Pi_0$)

So for Alice has projectors $\Pi_0^x, \Pi_1^x$ and Bob has: $\Pi_0^y, \Pi_1^y$.

Define: $A^x = \Pi_0^x - \Pi_1^x$, $B^y = \Pi_0^y - \Pi_1^y$. $\Rightarrow (A^x)^\dagger = A^x$, $(B^y)^\dagger = B^y$

For any $x,y \in \{0,1\}$: $Pr(a\oplus b=0) = \langle\psi|\Pi_0^x \otimes \Pi_0^y|\psi\rangle + \langle\psi|\Pi_1^x \otimes \Pi_1^y|\psi\rangle$

$Pr(a\oplus b=1) = \langle\psi|\Pi_0^x \otimes \Pi_1^y|\psi\rangle + \langle\psi|\Pi_1^x \otimes \Pi_0^y|\psi\rangle$

$Pr(a\oplus b=0) - Pr(a\oplus b=1) = \langle\psi|\Pi_0^x \otimes (\Pi_0^y - \Pi_1^y)|\psi\rangle + \langle\psi|\Pi_1^x (\Pi_0^y - \Pi_1^y)|\psi\rangle =$

$= \langle\psi|(\Pi_0^x - \Pi_1^x) \otimes (\Pi_0^y - \Pi_1^y)|\psi\rangle = \langle\psi|A^x \otimes B^y|\psi\rangle$

$Pr(a\oplus b=0) - Pr(a\oplus b=1) = 2\cdot Pr(a\oplus b=0) - 1 = 1 - 2\cdot Pr(a\oplus b\neq 1) = \langle\psi|A^x \otimes B^y|\psi\rangle$

$Pr(a\oplus b = x\wedge y) = \frac{1}{4}\Big( Pr(a\oplus b=0 \mid x=0,y=0) + Pr(a\oplus b=0 \mid x=0,y=1) + Pr(a\oplus b=0 \mid x=1,y=0) + Pr(a\oplus b=1 \mid x=1,y=1)\Big) =$

$= \frac{1}{8}\big( \langle\psi|A^0\otimes B^0 + A^0\otimes B^1 + A^1\otimes B^0 - A^1\otimes B^1|\psi\rangle + 4\big)$

Define: $|a^x\rangle = (A^x \otimes \mathbb{1})|\psi\rangle$, $|b^y\rangle = (\mathbb{1}\otimes B^y)|\psi\rangle$. Notice that: $\langle\psi|A^x\otimes B^y|\psi\rangle = \langle a^x|b^y\rangle$

Then: $Pr(a\oplus b = x\wedge y) = \frac{1}{8}\big(\langle a^0|b^0\rangle + \langle a^0|b^1\rangle + \langle a^1|b^0\rangle - \langle a^1|b^1\rangle + 4\big) =$

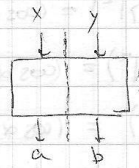
$= \frac{1}{8}\big( \langle a^0|(|b^0\rangle + |b^1\rangle) + \langle a^1|(|b^0\rangle - |b^1\rangle) + 4\big) \leq \frac{1}{8}\big( \||b^0\rangle + |b^1\rangle\| + \||b^0\rangle - |b^1\rangle\| + 4\big) \leq$

Choosing $|a^0\rangle$ parallel to $|b^0\rangle + |b^1\rangle$ and $|a^1\rangle$ parallel to $|b^0\rangle - |b^1\rangle$; $\||a^0\rangle\| = \||a^1\rangle\| = 1$

$\leq \frac{1}{8}(2\sqrt{2} + 4) = \frac{\sqrt{2}+2}{4} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) = 0.85\ldots$

maximum when $|b^0\rangle$ is orthogonal to $|b^1\rangle$ (exercise) □

Non-local box:




$x\wedge y = a\oplus b$ with probability 1.

(The 2 parts can be far apart)

From Bell's inequalities: CHSH inequality: quantumly we can approximate a NLB w.p 85%

Theorem (Van Dam, Cleve) If NLB exists, then communication complexity for any function is 1 bit.

Proof: Let $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be the function we want to compute.

Def: A bit $c$ is distributed if Alice has $a$ and Bob has $b$ such that $c = a \oplus b$.

A function $f(x,y)$ is distributively computed if given $x$ to Alice & $y$ to Bob, they can compute a distributed bit $f(x,y)$.

Lemma: AND of 2 distributed bits can be computed distributively with 2 NLB.

Proof: Alice has $x_1, x_2$, Bob has $y_1, y_2$. We want to find $a$ for Alice, $b$ for Bob s.t.

$a \oplus b = \text{AND}(x_1 \oplus y_1,\ x_2 \oplus y_2)$

$$\text{AND}(x_1 \oplus y_1, x_2 \oplus y_2) = (x_1 \wedge x_2) \oplus (x_1 \wedge y_2) \oplus (x_2 \wedge y_1) \oplus (y_1 \wedge y_2)$$

- $(x_1 \wedge x_2)$: Alice computes this, $a_1$
- $(x_1 \wedge y_2)$: use NLB to get $a_2 \oplus b_2$
- $(x_2 \wedge y_1)$: use NLB to get $a_3 \oplus b_3$
- $(y_1 \wedge y_2)$: Bob computes this, $b_1$

Choose: $a = a_1 \oplus a_2 \oplus a_3$, $b = b_1 \oplus b_2 \oplus b_3$.

□

Remark: A quantum protocol (with entanglement, no communication) can approximate AND w.p.: $\left(\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\right)^2 + \left(1 - \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\right)^2 = \frac{3}{4} = 75\%$

- $\left(\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\right)^2$: both correct $x_1 \wedge y_2, x_2 \wedge y_1$
- $\left(1 - \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\right)^2$: both incorrect

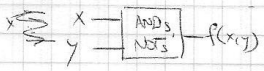
Lemma: NOT of a distributed bit can be computed distributively (without NLB).

Proof: Alice has $a$, Bob has $b$. We want $a', b'$ s.t. $a \oplus b' = \overline{(a \oplus b)}$.

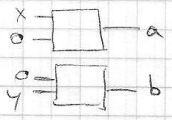
We can choose: $a' = \bar{a}$, $b' = b$.

□

So we first express $f(x,y)$ as a circuit of ANDs and NOTs.




Alice will use this box wit $x$ and $0$, Bob wit $0$ and $x$.




Notice that the 1st wire has a distributed $x_1$ bit, the 2nd wire has a distributed $x_2$ bit, and so on.

Alice and Bob execute all the ANDs and NOTs distributively. They get $a, b$ s.t. $a \oplus b = f(x,y)$. Alice sends $a$ to Bob, and he computes $f(x,y)$.

□