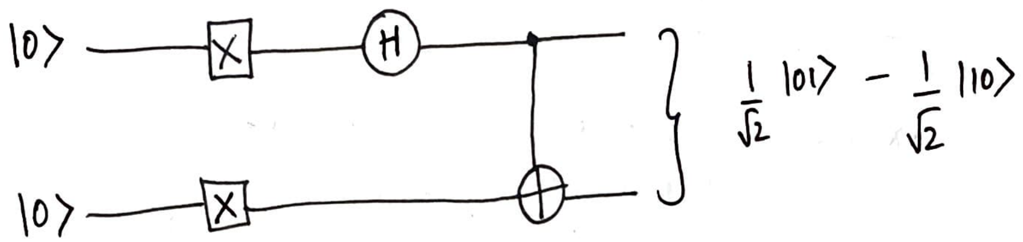
# Quantum Cryptography

## Mid-sem exam

Matta Uma Maheswara Reddy
CRS 2017

(Q2) (a) Circuit diagram for creating $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$ from $|00\rangle$.




firstly we flip both the qubits $\Rightarrow |00\rangle \rightarrow |11\rangle$

Then we pass the first qubit through a Hadamard gate

$\Rightarrow |1\rangle \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$\Rightarrow$ Now we pass this $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$ through a CNOT gate

$\Rightarrow$ We get $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

(b) firstly we are sending both the qubits through X gates (flipping them) and then we pass the first qubit through a Hadamard gate. $(H \cdot X) \otimes (X)$. Then we pass them both through CNOT.

$\therefore$ final matrix $= C_{NOT} \cdot [(H \cdot X) \otimes (X)]$

$C_{NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$\Rightarrow H \cdot X = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$

$$(H\cdot X)\otimes X \Rightarrow \begin{bmatrix} \frac{1}{\sqrt{2}}\cdot 1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \frac{1}{\sqrt{2}}\cdot 1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \frac{1}{\sqrt{2}}\cdot(-1) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \frac{1}{\sqrt{2}}\cdot 1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{bmatrix}$$

$$\Rightarrow C_{NOT}\cdot(H\cdot X\otimes X) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{bmatrix}$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$$

Verification $\Rightarrow$ $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}_{|00\rangle} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

---

(3) (a) Classically speaking, we are dealing with $x\cdot y$ here. $x\cdot y = 0$ for 3 values of $(x,y)$ and $x\cdot y = 1$ for 1 values of $(x,y)$. $\therefore P(x\cdot y = 0) = 75\%$, $P(x\cdot y = 1) = 25\%$.

$\therefore$ Best strategy for A, B would be to output 0 always. i.e. $a=0$, $b=0$. This way they have 75% chance of winning the game. Any other strategy would have $P(\text{win}) < 75\%$.

(b) A, B have an entangled pair. (Say $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$)

A has the first qubit of the pair and B has the second one.

They receive random $(x,y)$ inputs.

Strategy: **A**: If $x=0$ $\Rightarrow$ Do nothing

If $x=1$ $\Rightarrow$ Rotate their qubit by $\pi/8$

Measure their qubit and output the value $a$

**B**: If $y=0$ $\Rightarrow$ Do nothing

If $y=1$ $\Rightarrow$ Rotate their qubit by $-\pi/8$

Measure their qubit and output value $b$.

$\Rightarrow$ If $x=y=0$ $\Rightarrow$ they both do nothing.

Measuring they get $ab=00$ or $ab=11$ $\Rightarrow$ i.e $a=b$

So $a \oplus b = 0$ $\Rightarrow$ They always win. $P=1$

$\Rightarrow$ If $x=0,\ y=1$ (and other way round gives similar output due to symmetry).

A doesn't rotate $\Rightarrow$ gets classical bit $a$

B rotates by $-\pi/8$

$\Rightarrow$ If $a=0$ $\Rightarrow$ B's qubit becomes $\cos\pi/8\,|0\rangle - \sin\pi/8\,|1\rangle$

$\Rightarrow$ Measuring $\Rightarrow$ $P(b=0) = \cos^2\pi/8$, $P(b=1) = \sin^2\pi/8$

$\therefore P(\text{winning}) = \cos^2\pi/8$ $(a=0, b=0)$

If $a=1$ $\Rightarrow$ B's qubit becomes $\sin\pi/8\,|0\rangle + \cos\pi/8\,|1\rangle$

$P(b=1) = \cos^2\pi/8$, $P(b=0) = \sin^2\pi/8$

$\therefore P(\text{winning}) = \cos^2\pi/8$ $(a=1, b=1)$

$\therefore$ Overall winning $= \frac{1}{2}\cos^2(\pi/8) + \frac{1}{2}\cos^2(\pi/8) = \cos^2\pi/8$

$\Rightarrow$ $x=1,\ y=1$ $\Rightarrow$ Both rotate.

$\Rightarrow$ Chances of ~~getting~~ both measuring different classical bits

$\Rightarrow$ i.e. $|01\rangle, |10\rangle$ $\Rightarrow$ $\frac{1}{2}$

$\Rightarrow \therefore P(\text{winning}) = \frac{1}{4}\cdot 1 + \frac{1}{4}\cdot\cos^2\pi/8 + \frac{1}{4}\cdot\cos^2\pi/8 + \frac{1}{4}\cdot\frac{1}{2}$

$\Rightarrow 0.25 + 0.25\times 2\times 0.853 + 0.25\times 0.5 = 0.8015$

$\therefore P(\text{winning}) \simeq \underline{\underline{80\%}}$ $\rightarrow$ Better than best case scenario in a classical setting.

Q5 Let $|\psi\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ , $|\psi^{\perp}\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$

$|\psi\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}$ , $|\psi^{\perp}\rangle = \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}$

$\Rightarrow H|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\psi\rangle + |\psi^{\perp}\rangle\right)$

$$\Rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha_1+\alpha_2\\ \beta_1+\beta_2\end{pmatrix}$$

$\Rightarrow \alpha_1+\beta_1 = \alpha_1+\alpha_2$ $\quad\Rightarrow \therefore\ \beta_1 = \alpha_2$

$\alpha_1-\beta_1 = \beta_1+\beta_2$ $\quad \beta_2 = \alpha_1 - 2\beta_1$

$H|\psi^{\perp}\rangle = \frac{1}{\sqrt{2}}\left(|\psi\rangle - |\psi^{\perp}\rangle\right)$

$$\Rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha_2\\ \beta_2\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha_1-\alpha_2\\ \beta_1-\beta_2\end{pmatrix}$$

$\Rightarrow \alpha_2+\beta_2 = \alpha_1-\alpha_2$ $\quad\Rightarrow\ \alpha_2 = \beta_1$

$\alpha_2-\beta_2 = \beta_1-\beta_2$

$\therefore\ \cancel{\beta_1 \neq \beta_2}$ $\quad \cancel{\alpha_2+\beta_2 = \alpha_1+\alpha_2}$

$\cancel{\beta_1+\beta_2 \neq \alpha_1-\beta_1}$

$\Rightarrow \alpha_1 = 2\beta_1+\beta_2 = 2\alpha_2+\beta_2$

$\therefore |\psi^{\perp}\rangle = \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}$ , $|\psi\rangle = \begin{pmatrix}2\alpha_2+\beta_2\\ \alpha_2\end{pmatrix}$

$|\alpha_2|^2+|\beta_2|^2 = 1$ , $|2\alpha_2+\beta_2|^2 + |\alpha_2|^2 = 1$

$\Rightarrow 4|\alpha_2|^2 + |\beta_2|^2 + 2\alpha_2\beta_2^* + 2\beta_2\alpha_2^* + |\alpha_2|^2 = 1$

$\Rightarrow 2|\alpha_2|^2 + \alpha_2\beta_2^* + \beta_2\alpha_2^* = 0$

In terms of $\alpha_1, \beta_1$ $\Rightarrow 2|\beta_1|^2 + \beta_1(\alpha_1-2\beta_1)^* + (\alpha_1-2\beta_1)\beta_1^* = 0$

$\Rightarrow 2|\beta_1|^2 + \beta_1\alpha_1^* - 2\beta_1\beta_1^* + \alpha_1\beta_1^* - 2\beta_1\beta_1^* = 0$

$\Rightarrow 2\beta_1\beta_1^* = \alpha_1\beta_1^* + \alpha_1^*\beta_1$

Using $|\psi\rangle$ and $|\psi^{\perp}\rangle$ are orthogonal.

$|\psi\rangle\cdot|\psi^{\perp}\rangle = 0$ $\quad\Rightarrow (\alpha_1^*\ \ \beta_1^*)\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = 0$

$\Rightarrow \alpha_1^*\alpha_2 + \beta_1^*\beta_2 = 0 \Rightarrow \alpha_1^*\beta_1 + \beta_1^*(\alpha_1-2\beta_1) = 0$

$\Rightarrow 2\beta_1\beta_1^* = \alpha_1\beta_1^* + \alpha_1^*\beta_1$

$\therefore$ for $|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$, we just need $\underline{2\beta_1\beta_1^* = \alpha_1\beta_1^* + \alpha_1^*\beta_1}$

If $|\psi\rangle = |0\rangle \Rightarrow \alpha_1 = 1,\ \beta_1 = 0$, $|\psi^\perp\rangle = |1\rangle$, $\alpha_2 = 0,\ \beta_2 = 1$

then $\Rightarrow \alpha_2 = \beta_1 \Rightarrow 0 = 0$ satisfied

$\beta_2 = \alpha_1 - 2\beta_1 \Rightarrow 1 = 1 - 0 =$ satisfied

If $|\psi\rangle = |0\rangle$, $|\psi^\perp\rangle = i\,|1\rangle$

$\Rightarrow \alpha_2 = \beta_1 \Rightarrow 0 = 0$ ✓

$\beta_2 = \alpha_1 - 2\beta_1 \Rightarrow i = 0 - 2\cdot 0 \neq 0$ ✗ Not satisfied.

---

(Q1) for a given n qubits, the combined state $|\psi\rangle$ is said to be entangled, if $|\psi\rangle$ cannot be broken down into the form

(a) $|\psi\rangle = |\phi\rangle \otimes |\gamma\rangle$ where

$|\phi\rangle$ & $|\gamma\rangle$ are independent quantum states.

Example: $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ $\rightarrow$ Cannot be broken down into $\otimes$ of two independent states.

$\dfrac{|00\rangle + |10\rangle}{\sqrt{2}}$ $\Rightarrow$ Not entangled as $\dfrac{|00\rangle + |10\rangle}{\sqrt{2}} = \left(\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle$

(b) $$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} + \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n}\right)$$

Apply n-bit Hadamard transformation $\Rightarrow$

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2}} H^{\otimes n}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} + \frac{1}{\sqrt{2}} H^{\otimes n}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$$

This state is entangled. $H^{\otimes n}$ is a unitary transformation. So the only way to get an entangled state is if we started with one such state.

$\therefore$ $\underline{|\psi\rangle \text{ is entangled}}$. (Entanglement is irrespective of the basis).

Q4 (a) Given a Boolean function $f$

$f : \{0,1\}^n \rightarrow \{0,1\}$. We have to determine if the given function is balanced or constant.

**Balanced** ⇒ Returns 0's for exactly half the inputs
Returns 1's for exactly half the other inputs

**Constant** ⇒ Returns either all 0's or all 1's for all inputs.

Deutsch - Jozsa helps ~~det~~ find a given function is balanced or constant with just one query.

(b) **Classical**: In the worst case scenario, we'd need to go through one more than half of all inputs to determine if $f$ is balanced or constant.

Imagine for half the inputs you get all 0's, Then for the next one – you get a 1 ⇒ Then $f$ is balanced.
└ you get a 0 ⇒ Then $f$ is constant.

∴ **Complexity** ⇒ $2^{n-1}+1$ inputs ⇒ $O(2^{n-1}+1) = O(2^n)$

**Quantum** ⇒ Deutsch -Jozsa ⇒ 1 input only.

In one query, we can say $f$ is balanced if output is $|1\rangle$, $f$ is constant if output is $|0\rangle$.

**Complexity** ≡ $O(1)$

Classical ⇒ **exponential**, Quantum ⇒ **constant time** ($O(1)$)

(c) $f(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3$

$f: \{0,1\}^3 \to \{0,1\}$

One step before measurement for Deutsch-Jozsa ⇒

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x.z \oplus f(x)}}{2^3} |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$ (Given 3 input)

$\sum_x (-1)^{x.z \oplus f(x)}$ is Walsh Transform $= W_f(z)$

$$|\psi_3\rangle = \sum_{z \in \{0,1\}^3} \frac{W_f(z)}{2^3} . |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

| Input | f | $W_f$ |
|---|---|---|
| 000 | 0 | 0 |
| 001 | 0 | 4 |
| 010 | 0 | 4 |
| 011 | 1 | 0 |
| 100 | 0 | 4 |
| 101 | 1 | 0 |
| 110 | 1 | 0 |
| 111 | 1 | -4 |

$$\therefore |\psi_3\rangle = \frac{1}{2^3}\left(4|001\rangle + 4|010\rangle + 4|100\rangle - 4|111\rangle\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\Rightarrow \frac{1}{2\sqrt{2}}\left(\left(|001\rangle + |010\rangle + |100\rangle - |111\rangle\right) \otimes \left(|0\rangle - |1\rangle\right)\right)$$

Q6 (a) Grover's search algorithm determines $x$ for $f(x)=1$ ($f:\{0,1\}^n \to \{0,1\}$) in $O(2^{n/2})$ complexity.

That'd mean Grover's algorithm can brute-force a 128-bit symmetric cryptographic key in $O(2^{64})$ and 512 bit in $O(2^{256})$. A classical brute force would need $O(2^{128})$ and $O(2^{512})$ run time.

$\therefore$ It reduces time complexity drastically.

To be quantum fool proof, it is suggested to double the key lengths, as Grover's effectively makes the key lengths half.

n key classical $\to O(2^n)$ Brute force classical.
$\to O(2^{n/2})$ brute force quantum

(b) $f(x_1, x_2, x_3) = 1 \oplus x_2 x_3 \oplus x_1 x_2 x_3$

Take $f_1(x_1, x_2, x_3) = 1 \oplus f(x_1, x_2, x_3)$

$= x_2 x_3 \oplus x_1 x_2 x_3$

$f(x_1, x_2, x_3) = 0 \iff f_1(x_1, x_2, x_3) = 1$

| Input | $f$ | $f_1$ |
|---|---|---|
| 000 | 1 | 0 |
| 001 | 1 | 0 |
| 010 | 1 | 0 |
| 011 | 0 | 1 |
| 100 | 1 | 0 |
| 101 | 1 | 0 |
| 110 | 1 | 0 |
| 111 | 1 | 0 |

Classically we'd need to brute force $2^3$ times $\Rightarrow$ 8 times on $f_1$

Grover's $\Rightarrow O(2^{3/2}) \approx 3$

$\therefore$ We'd need to apply Grover and solve it in 3 steps.

(But there is only one x s.t $f_1(x) = 1$)

$\therefore$ Worst case scenario Grover = 3 steps

Best case = 1 step

(Q7) (a) Given a function

$f: \{0,1\}^n \to \{0,1\}^n$ with given that for some unknown $s$, $s \in \{0,1\}^n$ $\forall$ $x, y \in \{0,1\}^n$

$f(x) = f(y)$ if and only if $x \oplus y \in \{0^n, s\}$

Our goal is to find out $s$ by making as few queries to $f(x)$ as possible.