Quantum Midsem

Soham Sanjay Zemse
CRS 2012

Q1

a) Quantum Entanglement:

When a group of particles are generated in a special way, such that the quantum state (spin) of each particle in the group is dependent on state of the other particles, even if the particles are seperated by a huge spacial distance.

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

$$= \frac{1}{\sqrt{2}}\left[|+\rangle^{\otimes n} + |-\rangle^{\otimes n}\right]$$

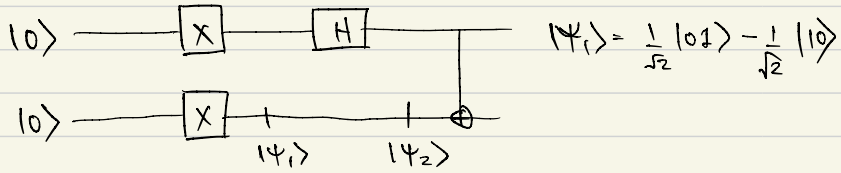
$$= \frac{1}{\sqrt{2}}\left[|+++\ldots n\text{times}\rangle + |---\ldots n\text{times}\rangle\right]$$

Yes, the n-qubits are entangled. If any one is measured as $|+\rangle$ then other $n-1$ qubits would be $|+\rangle$ as well (similarly for $|-\rangle$).

Q2

a) Our state $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

Starts from $|00\rangle$.



Maximally entangled bell states:

$|\psi_1\rangle = 0|11\rangle$

$|\psi_2\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \otimes |1\rangle = \frac{|01\rangle - |11\rangle}{\sqrt{2}}$

b) The matrix that represents circuit is

$$C = CNOT \cdot (H \otimes I) \cdot (X \otimes X) \quad (1)$$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (2)$$

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \quad (3)$$

$$X \otimes X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{—(4)}$$

Now from (1), (2), (3), (4)

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

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

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

Q3

a) For random bits x & y, the value x·y is 0 for 75% time and 1 for 25% time. Means x·y is biased on 0 side.

Best classical strategy: Since A & B cannot know what random bit the other is given, it would be best if both A & B output same bit, e.g. 0. So that a⊕b will be 0. Their winning probability would be 75%

b) Yes. If two entangled qubits x & y are given to A & B. When A measures x, they also get to know what B will get.

For A.

IF x = 0
  output a = 0
else
  output a = 1

For B

output b = 1
(regardless of y value)

With this strategy A & B will win 100% of the time.

Q4

a) Deutsch-Jozsa Algorithm finds whether an n-bit boolean function f(x) is constant or balanced. It should be given that f(x) is either constant or balanced (not somethingelse).

b) In a classical computer, when we have an n-bit boolean function f(x), has 2^n output values (bits). A constant function would give bit 0 for all 2^n inputs (or bit 1). A balanced function would give 2^{n-1} bit 0s and 2^{n-1} bit 1s. Now to check if a given function is balanced or not, in the worst case we have to do $2^{n-1}+1$ queries.

The Deutsch-Jozsa Algorithm does this in one query using parallelism.

c) $f(x_1x_2x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1$

$$Pr\left[|000\rangle\right] = \frac{1}{2^{2\times3}}\left[\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right]^2$$

So if $Pr[|000\rangle]$ is measured as 1, it means function is constant.

Q5 Let $|\psi\rangle = \alpha_\psi |0\rangle + \beta_\psi |1\rangle$
and $|\psi^\perp\rangle = \alpha_{\psi^\perp} |0\rangle + \beta_{\psi^\perp} |1\rangle$

Given: $H|\psi\rangle$ outputs $1/\sqrt{2}\left[|\psi\rangle + |\psi^\perp\rangle\right]$

$$\Rightarrow \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha_\psi \\ \beta_\psi \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha_\psi + \beta_\psi \\ \alpha_\psi - \beta_\psi \end{bmatrix} = \text{L.H.S}$$

$$\text{R.H.S} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha_\psi + \alpha_{\psi^\perp} \\ \beta_\psi + \beta_{\psi^\perp} \end{bmatrix}$$

$\Rightarrow \alpha_\psi + \beta_\psi = \alpha_\psi + \alpha_{\psi^\perp} \quad \Rightarrow \alpha_{\psi^\perp} = \beta_\psi$ — (1)

and $\alpha_\psi - \beta_\psi = \beta_\psi + \beta_{\psi^\perp} \quad \Rightarrow \beta_{\psi^\perp} = \alpha_\psi - 2\beta_\psi$ — (2)

$$\Rightarrow \boxed{|\psi^\perp\rangle = \beta_\psi |0\rangle + \left[\alpha_\psi - 2\beta_\psi\right] |1\rangle \quad \text{when } |\psi\rangle = \alpha_\psi |0\rangle + \beta_\psi |1\rangle} \quad \text{— (3)}$$

We can now see that $|\psi\rangle = |0\rangle$ and $|\psi^\perp\rangle = |1\rangle$ satisfies because the pair satisfies (3)

Also $|0\rangle$ and $|1\rangle$ do not satisfy because from (3) for $|\psi\rangle = |0\rangle$, we have a unique $|\psi^\perp\rangle = |1\rangle$. Hence $|1\rangle$ do not satisfy.

Q6

a) Grover's search algorithm runs in $O(\sqrt{n})$ complexity while the classical counter part runs in $O(n)$.

In terms of a 2^n-bit symmetric cipher, classical worst case to find the key is 2^n bruteforce iterations. However using Grover's algorithm, a quantum computer can brute-force a 2^n-bit symmetric cipher in $2^{n/2}$ iterations.

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

search $f(x_1 x_2 x_3) = 0$

Since we have $N = 2^3$ number of inputs from which we want to find a particular input. The input that yeilds $f(x_1 x_2 x_3) = 0$, we call it good and other inputs as bad.

$$|\psi\rangle = \frac{1}{\sqrt{8}} |good\rangle + \sqrt{\frac{7}{8}} |bad\rangle$$

let $\theta \in [0, \pi/2]$ such that $\sin\theta = 1/\sqrt{8}$

$$\Rightarrow |\psi\rangle = \sin\theta\, |good\rangle + \cos\theta\, |bad\rangle$$

Now Grover's Iterate $G = HHH\ U_0\ HHH\ U_f$

$$U_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } x \neq 0^n \\ |x\rangle & \text{if } x = 0^n \end{cases} = 2|000\rangle\langle 000| - I$$

Let $|s\rangle$ be superposition of all N states corresponding to the N inputs of $f(x_1 x_2 x_3)$.

$$G = HHH(2|0\rangle\langle 0| - I) HHH\, U_f = (2|s\rangle\langle s| - I)\, U_f$$

We have $|\psi\rangle = \sin\theta\,|good\rangle + \cos\theta\,|bad\rangle$

$$\rightarrow \quad G|\psi\rangle = \sin 3\theta\,|good\rangle + \cos 3\theta\,|bad\rangle$$

A single application of G on $|\psi\rangle$ changes probability of measuring good state from $\sin\theta$ to $\sin 3\theta$.

If we keep on doing this K times,

$$G^K|\psi\rangle = \sin(2K+1)\,|good\rangle + \cos(2K+1)\,|bad\rangle$$

probability of measuring bad state decreases and hence after $\sqrt{8}$ applications of G, probability of observing good state is great.

$$K = \sqrt{8} \approx 3.$$

$$G^3|\psi\rangle = \sin 7\theta\,|good\rangle + \cos 7\theta\,|bad\rangle$$

$$\sin\theta = \frac{1}{\sqrt{8}} = 0.35$$

$$\sin 7\theta = 0.5745 \geq 0.5$$

So we will most likely measure good state on quantum comp.

Q7

a) Simon's Algorithm:

We have a n-bit boolean function $f(x) : \{0,1\}^n \rightarrow \{0,1\}^K$ it's given that for any two $x, y \in \{0,1\}^n$, $F(x) = f(y)$ if and only if $x = y \oplus s$ for some fixed $s \in \{0,1\}^n$, $K \geq n/2$. Problem is to find the value s.