...am Nguyen - U70840587

Question 1.

We notice that one qbit can repretent either bit 0 or 1. Particularly, a quantum state $|\varphi\rangle$ of a qubit is given by.

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1$$

Thus; n qbits represent 2^n classical bits.

For company A; the computer has 53 qbits, so equivalent to 2^{53} classical bits., whereas company - C 's quantum computer has 76 qbits $\simeq 2^{76}$ bits. Thus; for every quantum algorithm run on C-'s computer, it is $\frac{2^{76}}{2^{53}} = 2^{23} = 8{,}388{,}608$, (closed to 10 millions) times in number of represented bits. In conclusion, it is quite appropriate to claim that C's quantum computer is $\simeq 10$ million time faster than A's (Of course we ignore hardware aspect and compeire only computational capility) $\boxtimes$

Question 2,

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle|+\rangle + |-\rangle|-\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right]$$

$$= \frac{1}{\sqrt{2}}\cdot\frac{1}{2}\Big(|00\rangle + \cancel{|01\rangle} + \cancel{|10\rangle} + |11\rangle + |00\rangle - \cancel{|01\rangle} - \cancel{|10\rangle} + |11\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\cancel{2}}\Big(\cancel{2}|00\rangle + 2|11\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

equal

$$= |\Phi^+\rangle \ \text{(Bell state)}$$

- It is entangled, since suppose we can seperabe $|\Phi^+\rangle$ to

$$(\alpha_1|0\rangle + b_1|1\rangle)\otimes(\alpha_2|0\rangle + b_2|1\rangle)$$

$$= a_1a_2|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + b_1b_2|11\rangle$$

$$\Rightarrow \begin{cases} a_1a_2 = \frac{1}{\sqrt{2}} = b_1b_2 \\ a_1b_2 = a_2b_1 = 0 \rightarrow \text{either } a_1 = 0 \text{ or } a_2 = 0 \text{ or} \\ \qquad b_1 = 0 \text{ or } b_2 = 0 \end{cases}$$

thus noway $a_1a_2 = b_1b_2 = \frac{1}{\sqrt{2}}$ $\rightarrow$ this state is entangled.

- Meaning of entangement; when we measure the first qbit, if we obtain 0, then the second qbit is also 0. In probability,

$$p(q_1=0) = \frac{1}{2}, \quad p(q_2=0 \mid q_1=0) = 1$$

$$p(q_1=1) = \frac{1}{2}, \quad p(q_2=1 \mid q_1=1) = 1$$

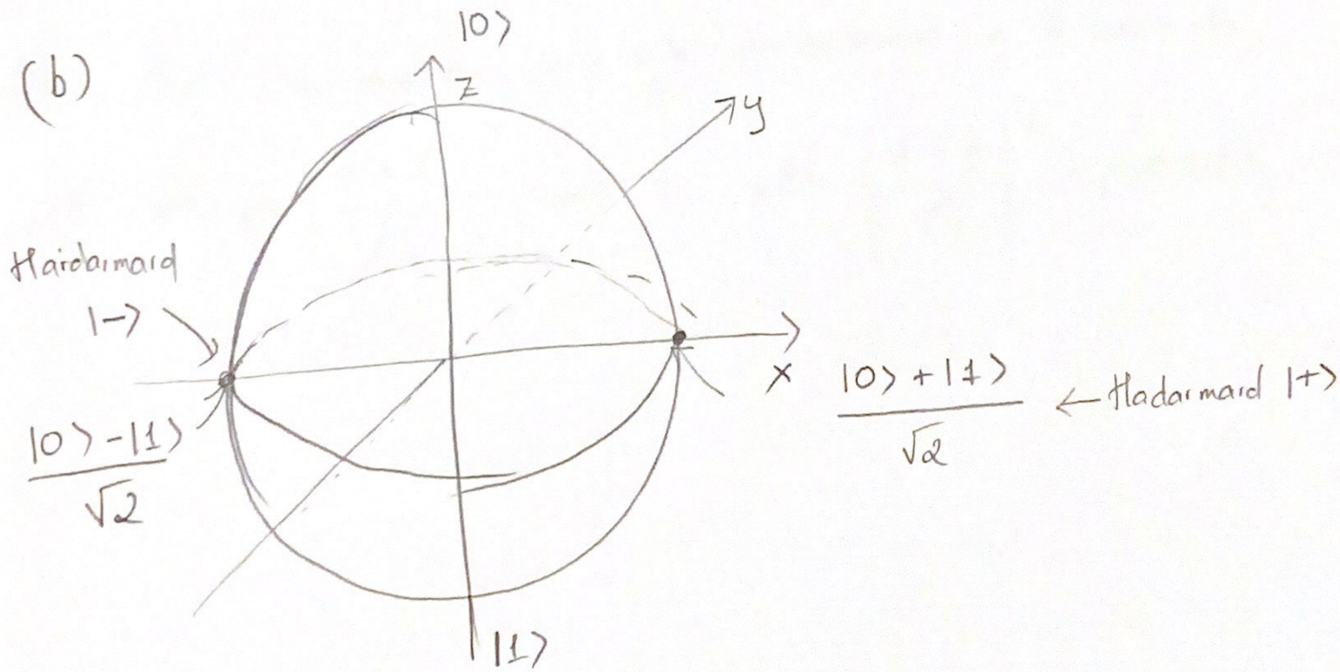
→ We only need to measure one qbit to get the full ~~info~~ infomation.

- It is a Bell state, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Question 3 Given $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

(a) Base on Bohr' rule; α and β is complex number in $\mathbb{C}$, satisfying $|\alpha|^2 + |\beta|^2 = 1$. This is similar to the probability rules since when we measure the superposition $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, the resulting bit is 0 with probability of $|\alpha|^2$ and $|1|$ with probability of $|\beta|^2$ (amplitude). Since two events are disjointed and forming the sample space $\Omega = \{0, 1\} \rightarrow P(\phi = 0) + P(\phi = 1) = 1$;

(b)



(C) We first need to compute $|0\rangle$ and $|1\rangle$ on Hardarman basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad\qquad |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

$$\Rightarrow$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad\qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

Thus, $|\phi\rangle = \alpha \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \beta \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

Note that, the resulting bit after measurement in H basis is

0 with prob $\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2$ and 1 with $\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2$ in probability.

(d) The BB84 protocal work as follows.

+) Alice wants to send Bob a message containing classical bits $a \in \{0, 1\}$

+) Everytime Alice sends the message to Bob, she flips a coin, says $b = 0$ or 1 ($0 =$ Hedd and $1 =$ Tail)

→ If $b = 0$; she encodes the message using $\{|0\rangle, |1\rangle\}$ basis.

→ If $b = 1$; she encodes the message using $\{|+\rangle, |-\rangle\}$ basis.

+) Alice sends the encoded message to Bob, (private chaneel) Bob measures it using both $\{|0\rangle; |1\rangle\}$ and $\{|+\rangle; |-\rangle\}$ basis; receiving b' α' message.

+) Alice sends Bob a string of $\{b_i\}$, (public channel) Bob compare b_i' and b_i. If $b_i \neq b_i'$ → discard resulting a'

$b_1 = b_i'$ → keeping a'

+) The message now contain $a_i = a_i'$ (Since sent quantum states are measured in the same basis as encoded)

Effectiveness First, the evesdroper (Eve) cannot copy the state due to no-cloning theorem of quantum states. The only thing Eve can do is to measure the sent state before Bob. Suppose, she correctly guesses the basis of sent state, the state is intact an received by Bob. However, if she guesses it wrong, the state will be disrupted. For example Alice sents bit $a = 0$ endoded to $|\phi\rangle = |0\rangle$ $(b = 0, a = 0)$ (We denote $|\varphi_{ab}\rangle = |\varphi_{00}\rangle = |0\rangle$). the state is mesured by Eve in wrng basis, which is Hadamard resulted in

$$|\phi'\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right)$$

Clearly, now the state has been disrupted by Eve's measure and the Bob with have a different measure when compare to Alice.

Bob and Alice can perform a sanity check by sacrifying half of the sent bits. If the error is beyond this threshold, it is cleare that there is a eavdropper, then Bob and Alice will cancel the prototol. Otherwise; it passed the test, then Bob & Alice continue using the protocol.

Question 4 We have $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

(a) $|0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

(b) $|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

This is Pauli-X matrix, equivalence to NOT operation, which simply transforms $|0\rangle \longmapsto |1\rangle$

$|1\rangle \longmapsto |0\rangle$

c) $-|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & -0 \\ i & 0 \end{pmatrix} + \begin{pmatrix} 0 & -i \\ 0 & 0 \end{pmatrix}$

$= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \rightarrow$ this is Pauli-y

(d) $|0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

should be

$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ← Pauli - Z

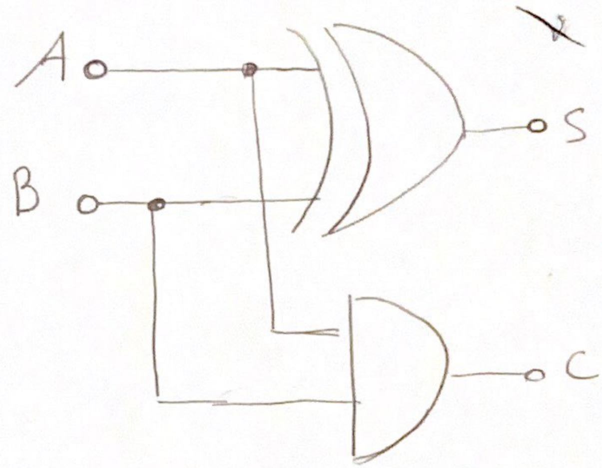
If $|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ → cannot be Pauli Z

$\Rightarrow |0\rangle\langle 1| - |1\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$? not a gate

since not unitary

Question 5

Half-adder in classical computer:



In quantum computer