INDIAN STATISTICAL INSTITUTE
M. Tech (CrS) II year : 2021–2022
Quantum Cryptology and Security
Mid-Semester Examination

Date: 03. 12. 2021 | Maximum Marks: 50 | Time: 3 Hours

Answer any part of any question. Maximum marks you can obtain is 50. The paper is of 55 marks.

Please answer all parts of a question at the same place.

1. (a) Briefly explain the idea of quantum entanglement.

   (b) Is the following n-qubit quantum state

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

   entangled? Give explanation.

   [2+3=5]

2. (a) Draw the circuit diagram for creating the maximally entangled Bell State, $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$, starting from state $|00\rangle$.

   (b) Provide the complete 4×4 matrix representation for the above circuit.

   [5+5=10]

3. Suppose A and B are two parties staying far apart, without any communication channel. Suppose A is given a random bit x and B is given another random bit y. Without communicating among themselves A outputs the bit a and B outputs another bit b. They win the game if $a \oplus b = x \cdot y$.

   (a) Classically what could be the best strategy for A and B to win this game?

   (b) Can they achieve a better strategy in quantum domain with an entanglement? If yes, explain.

   [2+3=5]

4. (a) Clearly state the problem statement that the Deutsch-Jozsa algorithm solves.

   (b) Compare the query complexity of Deutsch-Jozsa algorithm with respect to the corresponding classical query complexity.

   (c) For the given 3-input 1-output Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$, write down the output state just before the measurement step in the Deutsch-Jozsa algorithm.

   [2+3+5=10]

5. Characterize the quantum states $|\psi\rangle, |\psi^{\perp}\rangle$, such that Hadamard gate when applied on $|\psi\rangle$, outputs $\frac{1}{\sqrt{2}}\left(|\psi\rangle + |\psi^{\perp}\rangle\right)$ and when applied on $|\psi^{\perp}\rangle$ results $\frac{1}{\sqrt{2}}\left(|\psi\rangle - |\psi^{\perp}\rangle\right)$. Note that, $|\psi\rangle = |0\rangle$ and $|\psi^{\perp}\rangle = |1\rangle$ satisfy the conditions while $|\psi\rangle = |0\rangle$ and $|\psi^{\perp}\rangle = i\,|1\rangle$ does not satisfy the condition. [5]

6. (a) State the purpose of Grover's search algorithm in terms of the effective key length in the domain of symmetric key cryptography.

   (b) Given a 3-input 1-output Boolean function $f(x_1, x_2, x_3) = 1 \oplus x_2x_3 \oplus x_1x_2x_3$, how to determine the input point(s) where $f(x_1, x_2, x_3) = 0$, using the Grover's algorithm.

[3+7=10]

7. (a) Clearly write down the problem statement of Simon's algorithm.

   (b) Consider the truth table of a 3-input 3-output Boolean function $f : \{0,1\}^3 \to \{0,1\}^3$ as given below. Find the hidden shift (if any) using the Simon's algorithm. Explain all the steps with relevant circuit diagram.

x	$f(x)$
000	110
001	101
010	000
011	011
100	101
101	110
110	011
111	000

Table 1: The truth table of the Boolean function $f : \{0,1\}^3 \to \{0,1\}^3$.

[2+(6+2)=10]

1.

(a) <u>Quantum Entanglement</u>

A set of quibx whose combined state is $|\psi\rangle$ is said to be in a state of entanglement if $|\psi\rangle$ can't be decomposed as $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ where $|\phi_1\rangle$ & $|\phi_2\rangle$ are two independent quantum states.

<u>Example</u>:

Consider $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

The above $|\psi\rangle$ can't be written as a tensor product of two single qubit state.

We can also extend the definition to arbitrary number of qubits, if the state of a system of n qubits can't be written as a tensor product of two independent sets.

~~We know that the entangled state is remain~~

(b) Given n-qubit quantum state

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

Yes the given n qubit state is entangled.

We know, an entangled state remains entangled irrespective of the choice of the basis.

We know $H\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = |0\rangle$ &

$H\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = |1\rangle$.

Also. $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ & $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$,

where H is the hadamard gate., $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

Now, if we consider $H^{\otimes n}$ i.e. n times tensor of H gates.

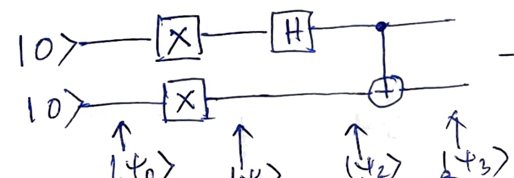
So, $H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2}}\left[H^{\otimes n}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} + H^{\otimes n}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right]$

$= \frac{1}{\sqrt{2}}\left[|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right].$

Now, $\frac{1}{\sqrt{2}}\left[|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right]$ is entangled in standard computational basis. And $H^{\otimes n}$ is just a unitary transformation which change hadamard basis in n qubit to standard computational basis. So, $|\psi\rangle$ also have to be entangled as a state is entangled irrespective of choice of basis.

2.

(a)



$\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle = |\psi\rangle.$

This is the circuit ~~diagram~~ diagram which transform $|00\rangle$ to $|\psi\rangle$

Here $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

 is the CNOT gate whose matrix is $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Now we look step by step how we get the maximally entangled state $|\psi\rangle$.

$|\psi_0\rangle = |00\rangle$

$|\psi_1\rangle = (X \otimes X)|00\rangle = X|0\rangle \otimes X|0\rangle = |1\rangle \otimes |1\rangle = |11\rangle$

$|\psi_2\rangle = (H \otimes I)|11\rangle$

$= (H|1\rangle) \otimes (I|1\rangle) = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |1\rangle$

$= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle.$

$|\psi_3\rangle = \text{CNOT}\left(\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle = |\psi\rangle$

(b) To compute the matrix representation of above circuit If we multiply all the ~~circu~~ matrix of the corresponding circuit then that will be enough.

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

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

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

So, the required matrix for the circuit

$$M = CNOT \cdot (H \otimes I) \cdot (X \otimes X).$$

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

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

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

Verification: $$M|00\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}$$

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

So, $M = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$ is the matrix of the circuit

3.

(a) A & B are given a random bit x & y respectively. Without communicating among themselves A outputs the bit a & B outputs the bit b.

They win the game if they can ensure that:

$$x \cdot y = a \oplus b.$$

In classical setting, the best Alice & Bob can do is to output $a=0$ & $b=0$ (or $a=1$ & $b=1$) no matter what the input bits x & y are.

Since $x \cdot y$ is 0 for 3 out of 4 possible combination of x & y, Alice & Bob will win the game with probability $= \frac{3}{4} = 0.75$.

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

(b) Yes they can achieve a better strategy in quantum domain with an entanglement.

Suppose Alice & Bob will share a maximally entangled state $= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Now we discuss what Alice & Bob will do after receiving x & y respectively.

<u>Alice</u> (after receiving 'x')

If $x = 0$ she will just measure her qubit

If $x = 1$ she will apply $R_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ rotation to her qubit & measure it.

Bob (after receiving y)

If $y=0$ he applies $R_2 = \begin{bmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix}$ rotation

to his qubit & measure it.

If $y=1$ he applies $R_3 = \begin{bmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix}$ rotation

matrix to his qubit & measure it.

Now analyze the winning probability of this strategy.

Alice & Bob will win the game iff they output $ab \in \{00, 11\}$ when the input is $xy \in \{00, 01, 10\}$ & if they output $ab \in \{01, 10\}$ when the input is $xy = 11$.

(i) $xy = 00$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{I \otimes R_2} \frac{1}{\sqrt{2}}\Big[|0\rangle\left(\cos\tfrac{\pi}{8}|0\rangle - \sin\tfrac{\pi}{8}|1\rangle\right) + |1\rangle\left(\sin\tfrac{\pi}{8}|0\rangle + \cos\tfrac{\pi}{4}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\cos\tfrac{\pi}{8}|00\rangle - \sin\tfrac{\pi}{8}|01\rangle + \sin\tfrac{\pi}{8}|10\rangle + \cos\tfrac{\pi}{8}|11\rangle\right]$$

So, the winning probability

$$P(\text{win}) = P(|00\rangle) + P(|11\rangle) = \frac{1}{2}\left[\cos^2\tfrac{\pi}{8} + \cos^2\tfrac{\pi}{8}\right] = \cos^2\tfrac{\pi}{8}$$
$$\approx 0.854.$$

Sly,

(ii) $xy = 01$ we apply $I \otimes R_3$ to the bell state & then calculate $P(|00\rangle) + P(|11\rangle)$ which is again almost 0.854

(iii) $xy = 10$ we apply $R_1 \otimes R_2$ to the bell state & calculate $P(|00\rangle) + P(|11\rangle)$ which is the winning probability & almost 0.854.

(iv) $m_y = 11$ then we apply $R_1 \otimes R_3$ to the bell state & calculate the probabity $P(|01\rangle) + P(|10\rangle)$ which is almost 0.854.

So, in every case we get winning probability 0.854 which is greater than 0.75 in classical case.

4.

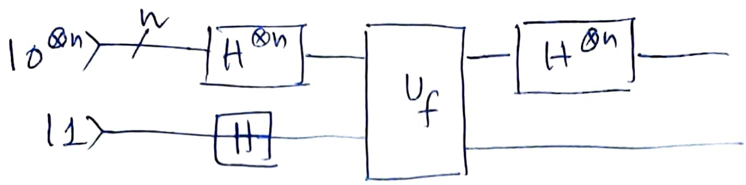
(a) Problem statement that the Deutsch-Jozsa algoritm solve:

Given a n-bit Boolean function $f(x)$ as an oracle, find if the function $f(x)$ is balanced or constant given the promise that $f(x)$ is either constant or balanced.

(b) First we will analyze the classical complexity of solving the problem.

In case of n bit balanced fn. f the output of the truth table has $\frac{2^n}{2}$ no of zeros & $\frac{2^n}{2}$ no of 1's. We are given a promise that $f(x)$ is either constant or balanced. So, in worst case, we will need $\frac{2^n}{2}+1$ many quaries to the fn. $f(x)$ so that if all the $\frac{2^n}{2}+1$ $f(x)$ values are the same then we say that the fn. is constant, else we say that it is balanced.

So, in classical setting we have $\frac{2^n}{2}+1$ many quaries



After applying the above circuit on $|0^{\otimes n}\rangle|1\rangle$.
we can observe the final output, ignoring the last qubit.

Then we can see that

$$P(|0^{\otimes n}\rangle) = \frac{1}{2^{2n}}\Big[\sum_{x\in\{0,1\}^n} (-1)^{f(x)}\Big]^2$$

If $f(x)$ is constant we get $P(|0^{\otimes n}\rangle) = 1$ & if $f(x)$ is balanced we get $P(|0^{\otimes n}\rangle) = 0$.

So, after apply DJ algo if we can measure $|0^{\otimes n}\rangle$ with prob 1 then $f(x)$ is constant & we cant get $|0^{\otimes n}\rangle$ if $f(x)$ is balanced.

So, by a single query we can decide $f(x)$ is constant or balanced in ~~clas~~ quantum case.

(c) Given Boolean fn. $f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$.

$$|0^{\otimes 3}\rangle|1\rangle \xrightarrow{H^{\otimes 3}\otimes H} \frac{1}{\sqrt{2^3}}\big(|000\rangle+|001\rangle+|010\rangle+|011\rangle + |100\rangle+|101\rangle+|110\rangle+|111\rangle\big)|-\rangle$$

$$\xrightarrow{U_f} \frac{1}{\sqrt{8}}\big(|000\rangle+|001\rangle+|010\rangle-|011\rangle + |100\rangle-|101\rangle-|110\rangle-|111\rangle\big)|-\rangle$$

$$\xrightarrow{H^{\otimes 3}\otimes I} \frac{1}{8}\big(W_f(|000\rangle)|000\rangle + W_f(|001\rangle)|001\rangle + \cdots + W_f(|111\rangle)|111\rangle\big)|-\rangle$$

Here $W_f(|000\rangle) = 0.$

$W_f(|001\rangle) = 4$

$W_f(|010\rangle) = 4.$

$W_f(|011\rangle) = -2$

$W_f(|100\rangle) = 4.$

$W_f(|101\rangle) = -2$

$W_f(|110\rangle) = -2$

$W_f(|111\rangle) = -4$

~~So, the required output~~ $\cancel{= \frac{1}{8}(8|000\rangle)}$

~~So, the fn. is~~

So, the required output (before measurement.

$$= \frac{1}{8}\Big(4|001\rangle + 4|010\rangle - 2|011\rangle + 4|100\rangle - 2|101\rangle - 2|110\rangle - 4|111\rangle \Big).|-\rangle.$$

6

(a) Let $E: K \times M \to C$ be a symmetric key encryption scheme., $K \in \{0,1\}^n$.

$\mathcal{B}$ be a key recovery adversery for E.

let k be the secret key.

$\mathcal{B}$ outputs $\hat{k} \in \{0,1\}^n$.

$P(\mathcal{B} \text{ win}) = P(\hat{k} = k) = \frac{1}{2^n}$.

which can be defined as the good set for ~~A~~ $\mathcal{B}$.

Now, from grovers algo probabsity of good set $\sin\theta$.

$\therefore$ $\sin^2\theta = \frac{1}{2^n}$.

$\Rightarrow \theta = \frac{1}{2^{n/2}}$ [small θ $\sin\theta \approx \theta$].

Now, $(2t+1)\,\theta = \frac{\pi}{2}$.

$2t+1 = \frac{\pi}{2\theta}$.

$2t = \frac{\pi}{2\theta} - 1 \Rightarrow t = \frac{\pi}{4\theta} - \frac{1}{2}$.

$t \approx O(2^{n/2})$.

So, the efficient complexity becomes $O(2^{n/2})$.

6.

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

We have to determine the input points such that

$f(x_1, x_2, x_3) = 0$.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

$H = \{ (x_1, x_2, x_3) : f(x_1, x_2, x_3) = 0 \}$

$= \{ (x_1, x_2, x_3) : h(x_1, x_2, x_3) = 1 \}$.

$P(\text{good state in } H) = \frac{1}{2^3} = \frac{1}{8}$.

Apply Grover's algorithm $\sqrt{8}$ times ≈ 2.828 times

So, apply almost 3 times Grover algorithm ~~one~~ to find the set G.

7.

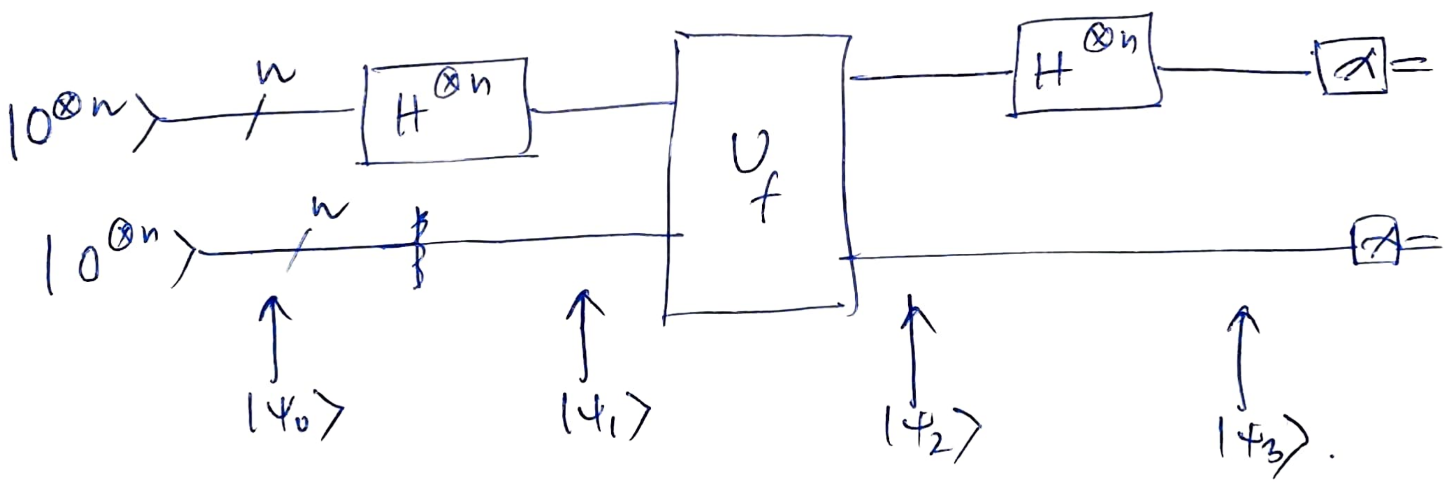
(a) Suppose we are given a Boolean function $f(x): \{0,1\}^n \rightarrow \{0,1\}^n$ with a promise that for any two arbitrary inputs x & y, $f(x) = f(y)$ iff $x = y \oplus s$ for some fixed $s \in \{0,1\}^n$.

Our goal is to determine the s.

This problem is the Simon's problem.

(b) $f : \{0,1\}^3 \to \{0,1\}^3$ given by

x	$f(x)$
000	110
001	101
010	000
011	011
100	101
101	110
110	011
111	000



$$|\psi_0\rangle = |0^{\otimes n}\rangle |0^{\otimes n}\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0^{\otimes n}\rangle.$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_3\rangle = \sum_y |y\rangle \otimes \left(\frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right)$$

$$\cancel{= \sum |y\rangle \otimes \left(\frac{1}{2^n} \left\{ (-1)^{y_1 \oplus y_2 \oplus y_3} |000\rangle + (-1)^{y_1 \oplus y_2} |011\rangle + (-1)^{y_1} \right. \right.}$$

$$= \sum |y\rangle \otimes \left(\frac{1}{2^n} \left\{ |110\rangle + (-1)^{y_3} |101\rangle + (-1)^{y_2} |000\rangle + (-1)^{y_2 \oplus y_3} |011\rangle + (-1)^{y_1} |101\rangle + (-1)^{y_1 \oplus y_3} |110\rangle + (-1)^{y_1 \oplus y_2} |011\rangle + (-1)^{y_1 \oplus y_2 \oplus y_3} |000\rangle \right\} \right).$$

let $y_1 = (0\,1\,0)$, $y_2 = (1\,1\,1)$.

$s = (s_1\ s_2\ s_3)$

$y_1 \cdot s = 0 = y_2 \cdot s$

$\Rightarrow s_2 = 0 = s_1 \oplus s_2 \oplus s_3$.

$\Rightarrow s_1 \oplus s_3 = 0$.

So, $s' = (0\,0\,0)$, $s'' = (1\,0\,1)$.

$f(000) = f(101) = 110$.

So, $s' = s''$.

5. Let $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $|\psi^{\perp}\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$.

$$H|\psi\rangle = \frac{1}{\sqrt{2}} |\psi\rangle + |\psi^{\perp}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \gamma \\ \beta + \delta \end{pmatrix}.$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha+\gamma \\ \beta+\delta \end{pmatrix}.$$

$$\Rightarrow \begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix} = \begin{pmatrix} \alpha+\gamma \\ \beta+\delta \end{pmatrix}.$$

$$\Rightarrow \gamma = \beta.$$
$$\delta = \alpha - 2\beta.$$

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

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha-\gamma \\ \beta-\delta \end{pmatrix}.$$

$$\Rightarrow \begin{pmatrix} \gamma+\delta \\ \gamma-\delta \end{pmatrix} = \begin{pmatrix} \alpha-\gamma \\ \beta-\delta \end{pmatrix}.$$

$$\Rightarrow \gamma = \beta.$$
$$\delta = \alpha - 2\beta.$$

So, we have $\gamma = \beta$, $\delta = \alpha - 2\beta$.

So, $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ & $|\psi^{\perp}\rangle = \begin{pmatrix} \beta \\ \alpha - 2\beta \end{pmatrix}$.

Now, $\langle\psi^{\perp}| = (\beta^* \quad \alpha^* - 2\beta^*)$.

$$\langle\psi^{\perp}|\psi\rangle = (\beta^* \quad \alpha^* - 2\beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\beta^* + \alpha^*\beta - 2\beta^*\beta.$$

So, we have $\langle\psi^{\perp}|\psi\rangle = 0$.

$$\Rightarrow \alpha\beta^* + \alpha^*\beta = 2\beta^*\beta.$$

$$\Rightarrow \boxed{2|\beta|^2 = \alpha\beta^* + \alpha^*\beta}$$

This is the characterization of $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ s.t it satisfies the above properties.