1) i) $\langle \psi | \psi \rangle \geq 0$

$\psi = \alpha|0\rangle + \beta|1\rangle$

$\langle \psi | \psi \rangle = \langle \alpha|0\rangle + \beta|1\rangle \,|\, \alpha|0\rangle + \beta|1\rangle \rangle$

$= \alpha^{+}\alpha + \beta^{+}\beta$

$= |\alpha|^2 + |\beta|^2 \geq 0$

ii) $\langle \psi | \psi \rangle = 0$ if and only if $|\psi\rangle = 0$

$\psi = \alpha|0\rangle + \beta|1\rangle$

$\langle \psi | \psi \rangle = \langle \alpha|0\rangle + \beta|1\rangle \,|\, \alpha|0\rangle + \beta|1\rangle \rangle$

$= \alpha^{+}\alpha + \beta^{+}\beta$

$= |\alpha|^2 + |\beta|^2 = 0$

$|\alpha|^2 = 0 \qquad |\beta|^2 = 0$

$|\alpha| = 0 \qquad |\beta| = 0$

$\alpha = a + ib \qquad \beta = c + id$

$|\alpha| = 0 \qquad |\beta| = 0$

$a^2 + b^2 = 0 \qquad c^2 + d^2 = 0$

$a = 0 \qquad c = d = 0$

$b = 0 \qquad \beta = 0$

$\alpha = 0$

$|\psi\rangle = 0$ //

if $|\psi\rangle = 0 \implies \alpha = 0 \quad \beta = 0$

$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 0$ //

iii) $\langle\gamma|\psi\rangle = \langle\psi|\gamma\rangle^{+}$

$\gamma = \alpha_1|0\rangle + \beta_1|1\rangle$

$\psi = \alpha_2|0\rangle + \beta_2|1\rangle$

$\langle\gamma|\psi\rangle = \langle\alpha_1|0\rangle + \beta_1|1\rangle \,|\, \alpha_2|0\rangle + \beta_2|1\rangle\rangle$

$= \alpha_1^{+}\alpha_2 + \beta_1^{+}\beta_2$ — ①

$\langle\psi|\gamma\rangle = \langle\alpha_2|0\rangle + \beta_2|1\rangle \,|\, \alpha_1|0\rangle + \beta_1|1\rangle\rangle$

$= \alpha_2^{+}\alpha_1 + \beta_2^{+}\beta_1$

$\langle\psi|\gamma\rangle^{+} = (\alpha_2^{+}\alpha_1 + \beta_2^{+}\beta_1)^{+}$

$= (\alpha_2^{+}\alpha_1)^{+} + (\beta_2^{+}\beta_1)^{+}$

$= \alpha_1^{+}\alpha_2 + \beta_1^{+}\beta_2$ — ② $(x^{++} = x)$

① AND ② RHS ARE EQUAL

$\implies \langle\gamma|\psi\rangle = \langle\psi|\gamma\rangle^{+}$ //

iv) $\langle \gamma | \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \gamma | \psi_1 \rangle + \lambda_2 \langle \gamma | \psi_2 \rangle$

$$\gamma = \alpha |0\rangle + \beta |1\rangle$$

$$\psi_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

$$\psi_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

LHS

$$\langle \alpha |0\rangle + \beta |1\rangle \,|\, \lambda_1 \alpha_1 |0\rangle + \lambda_1 \beta_1 |1\rangle + \lambda_2 \alpha_2 |0\rangle + \lambda_2 \beta_2 |1\rangle \rangle$$

$$= \langle \alpha |0\rangle + \beta |1\rangle \,|\, (\lambda_1 \alpha_1 + \lambda_2 \alpha_2) |0\rangle + (\lambda_1 \beta + \lambda_2 \beta_2) |1\rangle \rangle$$

$$= \alpha^+ (\lambda_1 \alpha_1 + \lambda_2 \alpha_2) + \beta^+ (\lambda_1 \beta_1 + \lambda_2 \beta_2) \quad - 1$$

RHS

$$\lambda_1 \langle \alpha |0\rangle + \beta |1\rangle \,|\, \alpha_1 |0\rangle + \beta_1 |1\rangle \rangle + \lambda_2 \langle \alpha |0\rangle + \beta |1\rangle \,|\, \alpha_2 |0\rangle + \beta_2 |1\rangle \rangle$$

$$= \lambda_1 (\alpha^+ \alpha_1 + \beta^+ \beta_1) + \lambda_2 (\alpha^+ \alpha_2 + \beta^+ \beta_2)$$

$$= \lambda_1 \alpha^+ \alpha_1 + \lambda_1 \beta^+ \beta_1 + \lambda_2 \alpha^+ \alpha_2 + \lambda_2 \beta^+ \beta_2$$

$$= \alpha^+ (\lambda_1 \alpha_1 + \lambda_2 \alpha_2) + \beta^+ (\lambda_1 \beta_1 + \lambda_2 \beta_2) \quad - 2$$

$$1 = 2$$

HENCE, $\langle \gamma | \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \gamma | \psi_1 \rangle + \lambda_2 \langle \gamma | \psi_2 \rangle$

2) $h(x) = f(x) \oplus g(x)$ [ASSUME OUTPUT IS A M LENTH BINARY]

LETS PROVE if f and g are the same function, h is always 0.

As $g(x) = f(x)$,

for all values of x, $f(x) = g(x) = y$

$h(x) = f(x) \oplus g(x) = y \oplus y$

if y is some m length boolean like 1011..... 011,

then $y \oplus y$ is

$$
\begin{array}{r}
y_1 y_2 \cdots y_m \\
\oplus\ y_1 y_2 \cdots y_m
\end{array}
$$

where $y_i \in \{0,1\}$

$0 \oplus 0 = 1 \oplus 1 = 0$

k^{TH} bit of $h = y \oplus y$ is given by

$h_k = y_k \oplus y_k$

So for any y_i, $y_i \oplus y_i = 0$

And hence $y \oplus y$ is of length m with all 0's.

Therefore $h(x) = 0$ //

NOW LET US PROVE THAT IF $h=0$, THEN f AND g ARE THE SAME FUNCTION.

Take a random x,

$$h(x) = f(x) \oplus g(x)$$

FOR ALL x, $h(x) = 0$

So $f(x) \oplus g(x) = 0$

Assuming the output is of length m (could be single bit as well),

$$f(x) = a \quad [a_1 a_2 \dots a_m]$$

$$g(x) = b \quad [b_1 b_2 \dots b_m]$$

where $a_i, b_i \in \{0,1\}$

they are bits

$$h(x) = f(x) \oplus g(x) = a \oplus b$$

$$\begin{array}{rcccc} & a_1 & a_2 & \dots & a_m \\ \oplus & b_1 & b_2 & \dots & b_m \end{array}$$

k^{TH} bit of h is given by

$$h_k = a_k \oplus b_k$$

We know $h(x) = 0$, so $h_k = 0$

$a_k \oplus b_k = 0$

we know $0 \oplus 0 = 0$ $\quad 0 \oplus 1 = 1$

$1 \oplus 1 = 0$ $\quad 1 \oplus 0 = 1$

so $a_k = b_k = 0$ OR

$a_k = b_k = 1$

either case $a_k = b_k$ $\forall$ k from 1 to m.

So $a = b$

$\Rightarrow f(x) = b(x)$

IF WE ASSUME $f(x)$ AND $g(x)$ RETURNS SINGLE BIT

0 OR 1, PROOF IS A LOT EASIER.

LETS PROVE if f and g are the same

function, h is always 0.

As $g(x) = f(x)$,

for all values of x, $f(x) = g(x) = y$

$h(x) = f(x) \oplus g(x) = y \oplus y$ $\quad y \in \{0,1\}$

$0 \oplus 0 = 1 \oplus 1 = 0$

So, $y \oplus y = 0$

hence $h(x) = 0$ $\forall x$ //

NOW LET US PROVE THAT IF $h = 0$, THEN f AND g ARE THE SAME FUNCTION.

Take a random x,

$$h(x) = f(x) \oplus g(x)$$

FOR ALL x, $h(x) = 0$

So $f(x) \oplus g(x) = 0$

$f(x) = a$

$g(x) = b$

$a, b \in \{0, 1\}$

$a \oplus b = 0$

we know $0 \oplus 0 = 0$ $\quad 0 \oplus 1 = 1$

$1 \oplus 1 = 0$ $\quad 1 \oplus 0 = 1$

SO $a = b = 0$ OR

$a = b = 1$

either case $a = b$

$f(x) = g(x) \ \forall x$ //

3) $x = x_1 \dots x_n$

$$(-1)^x = (-1)^{(x_1 + x_2 \dots x_n)}$$

$$XOR(x) = x_1 \oplus \dots \oplus x_n$$

To PROVE:

1. $(-1)^x = 1 \quad \Rightarrow \quad XOR(x) = 0$

2. $XOR(x) = 0 \quad \Rightarrow \quad (-1)^x = 1$

1. $(-1)^x = 1 \quad \Rightarrow \quad XOR(x) = 0$

GIVEN:

$$(-1)^x = 1$$

$$(-1)^x = (-1)^{(x_1 + x_2 \dots x_n)} = 1$$

We know $(-1)^y = 1$

only if y is even.

so $x_1 + x_2 + \dots x_n =$ even

$x_i \in \{0, 1\}$

As x_i is either 0 or 1, we know that there are even number of 1's in $x_1, x_2 \dots x_n$.

So XOR(x) is given by

$$XOR(x) = x_1 \oplus \dots \oplus x_n$$

We know that even number of x_i are 1 and the rest are 0s.

Assume 2k bits of x_i are 1 and n-2k are 0s.

$k \in [0, n/2]$

We know $1 \oplus 1 = 0$ and we know XOR is commutative and associative, so the 2k 1's can be written as k sets of XOR

$$\underline{(1 \oplus 1)} \oplus \underline{(1 \oplus 1)} \dots \oplus \underline{(1 \oplus 1)}$$

$$0 \oplus 0 \oplus \dots \oplus 0$$

We know $0 \oplus 0 = 0$

So this boils down to 0.

Similarly $(n-2k)$ 0's also comes down to 0 after applying the XOR.

So $XOR(x) = x_1 \oplus x_2 \dots \oplus x_n = 0$ //

2. $XOR(x) = 0 \Rightarrow (-1)^{x} = 1$

GIVEN $XOR(x) = 0$

$$x_1 \oplus x_2 \oplus \dots \oplus x_n = 0$$

We know $0 \oplus 0 = 0$

$1 \oplus 1 = 0$

but $0 \oplus 1 = 1$

So, we want all the 1's in x_i to cancel out. If there are ODD $(2k+1)$ 1's, then the $2k$ ones cancel to be 0, but the last 1 remains as $1 \oplus 0 = 1$

and hence $XOR(x) = 1$

CONTRADICTION.

So there can only be even 1's in x_i.

$\Rightarrow$ There are $2k$ ones in x_i $k \in [0, n/2]$

$$(-1)^{x} = (-1)^{(x_1 + \dots + x_n)}$$

$x_i \rightarrow 2k$ ones

$(n-2k)$ zeroes.

$$x_1 + \dots + x_n = (n-2k)\times 0 + 2k \times 1$$

$$= 2k$$

$$= \text{EVEN}$$

$(-1)^{\text{EVEN}}$ IS ALWAYS 1

$$\Rightarrow (-1)^{\Sigma} = 1 \quad //.$$