Introduction to Quantum Information and Communication

Take Home Mid-Sem

Moida Praneeth Jain, 2022101093

Question 5

(a)

To Prove:

$$\sum_{z \in \{0,1\}^n} (-1)^{(x \oplus y) \cdot z} = 2^n \delta(x, y)$$

Proof:

Case 1: $x = y$

$$\sum_{z \in \{0,1\}^n} (-1)^{(x \oplus y) \cdot z}$$

$$\sum_{z \in \{0,1\}^n} (-1)^{0 \cdot z}$$

$$\sum_{z \in \{0,1\}^n} (-1)^{0}$$

$$\sum_{z \in \{0,1\}^n} 1$$

$$2^n$$

$$2^n \times 1$$

$$2^n \delta(x, y)$$

Case 2: $x \neq y$

Let k be the number of digits different between x and y, and let the corresponding indices be $\alpha = \{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k\}$

$$\forall i \in \{1, 2, ..., k\} \; x_{\alpha_i} \neq y_{\alpha_i}$$

$$\forall i \notin \alpha \; x_i = y_i$$

.

$$\sum_{z \in \{0,1\}^n} (-1)^{(x \oplus y) \cdot z}$$

$$\sum_{z \in \{0,1\}^n} (-1)^{\oplus_{i=1}^{n} (x_i \oplus y_i) z_i}$$

$$\sum_{z\in\{0,1\}^n} (-1)^{\oplus_{i=1}^{k} z_{\alpha_i}}$$

$$\sum_{z\in\{0,1\}^n} (-1)^{z_{\alpha_1}\oplus z_{\alpha_2}\oplus\ldots\oplus z_{\alpha_k}}$$

Now, since z is looping through all possible bitstrings of length n, the parity of any subset of its bits will be odd half the times and even half the times.

$$-1+1-1+1\ldots-1+1$$

$$0$$

$$2^n \times 0$$

$$2^n \delta(x,y)$$

Now, from both the cases we get

$$\sum_{z\in\{0,1\}^n} (-1)^{(x\oplus y)\cdot z} = 2^n \delta(x,y)$$

Hence, proven

(b)

Given:

$$f : \{0,1\}^n \mapsto \{0,1\}^n$$

$$U_f\left(|x\rangle_Q \otimes |y\rangle_R\right) := |x\rangle_Q \otimes |y \oplus f(x)\rangle_R$$

$$V_f\left(|x\rangle_Q \otimes |y\rangle_R\right) := (-1)^{y\cdot f(x)}|x\rangle_Q \otimes |y\rangle_R$$

To Prove:

$$V_f\left(|x\rangle_Q \otimes |y\rangle_R\right) = \left(\mathbb{I}_Q \otimes H^{\otimes n}\right)U_f\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)\left(|x\rangle_Q \otimes |y\rangle_R\right)$$

Proof: We will be using the identity $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle$

$$\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)U_f\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)\left(|x\rangle_Q \otimes |y\rangle_R\right)$$

$$\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)U_f\left(\mathbb{I}_Q|x\rangle_Q \otimes H^{\otimes n}|y\rangle_R\right)$$

$$\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)U_f\left(|x\rangle_Q \otimes \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n} (-1)^{y\cdot z}|z\rangle_R\right)$$

$$\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n} (-1)^{y\cdot z}\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)U_f\left(|x\rangle_Q \otimes |z\rangle_R\right)$$

$$\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n} (-1)^{y\cdot z}\left(\mathbb{I}_Q \otimes H^{\otimes n}\right)\left(|x\rangle_Q \otimes |z \oplus f(x)\rangle_R\right)$$

$$\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{y\cdot z}\left(\mathbb{I}_Q|x\rangle_Q \otimes H^{\otimes n}|z\oplus f(x)\rangle_R\right)$$

$$\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{y\cdot z}|x\rangle_Q \otimes \left(\frac{1}{\sqrt{2^n}} \sum_{w\in\{0,1\}^n} (-1)^{(z\oplus f(x))\cdot w}|w\rangle_R\right)$$

$$\frac{1}{2^n} \sum_{z,w\in\{0,1\}^n} (-1)^{(y\cdot z)}(-1)^{(z\oplus f(x))\cdot w}|x\rangle_Q \otimes |w\rangle_R$$

$$\frac{1}{2^n} \sum_{w\in\{0,1\}^n} (-1)^{w\cdot f(x)}|x\rangle_Q \otimes |w\rangle_R \sum_{z\in\{0,1\}^n} (-1)^{(y\oplus w)\cdot z}$$

$$\frac{1}{2^n} \sum_{w\in\{0,1\}^n} (-1)^{w\cdot f(x)}|x\rangle_Q \otimes |w\rangle_R 2^n\delta(w,y)$$

$$\sum_{w\in\{0,1\}^n} (-1)^{w\cdot f(x)}|x\rangle_Q \otimes |w\rangle_R \delta(w,y)$$

$$(-1)^{y\cdot f(x)}|x\rangle_Q \otimes |y\rangle_R$$

$$V_f\left(|x\rangle_Q \otimes |y\rangle_R\right)$$

Hence, proven

Question 6

(a)

Before the first Hadamard, the state is

$$|0\rangle_A|\psi\rangle_B|\varphi\rangle_C$$

After the first Hadamard, the state is

$$H_A|0\rangle_A|\psi\rangle_B|\varphi\rangle_C$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_A\right)|\psi\rangle_B|\varphi\rangle_C$$

$$\frac{1}{\sqrt{2}}|0\rangle_A|\psi\rangle_B|\varphi\rangle_C + \frac{1}{\sqrt{2}}|1\rangle_A|\psi\rangle_B|\varphi\rangle_C$$

After the Controlled-SWAP, the state is

$$\frac{1}{\sqrt{2}}|0\rangle_A|\psi\rangle_B|\varphi\rangle_C + \frac{1}{\sqrt{2}}|1\rangle_A|\varphi\rangle_B|\psi\rangle_C$$

After the second Hadamard, we get the required state

$$|\psi'\rangle_{ABC} = H_A\left(\frac{1}{\sqrt{2}}|0\rangle_A|\psi\rangle_B|\varphi\rangle_C + \frac{1}{\sqrt{2}}|1\rangle_A|\varphi\rangle_B|\psi\rangle_C\right)$$

$$|\psi'\rangle_{ABC} = \frac{1}{\sqrt{2}} H_A |0\rangle_A |\psi\rangle_B |\varphi\rangle_C + \frac{1}{\sqrt{2}} H_A |1\rangle_A |\varphi\rangle_B |\psi\rangle_C$$

$$|\psi'\rangle_{ABC} = \frac{1}{2}\big(|0\rangle_A + |1\rangle_A\big)|\psi\rangle_B |\varphi\rangle_C + \frac{1}{2}\big(|0\rangle_A - |1\rangle_A\big)|\varphi\rangle_B |\psi\rangle_C$$

$$|\psi'\rangle_{ABC} = \frac{1}{2}|0\rangle_A\big(|\psi\rangle_B|\varphi\rangle_C + |\varphi\rangle_B|\psi\rangle_C\big) + \frac{1}{2}|1\rangle_A\big(|\psi\rangle_B|\varphi\rangle_C - |\varphi\rangle_B|\psi\rangle_C\big)$$

This is the required tripartite state

(b)

$$p_0 = \frac{1}{2}\big(\langle\psi|_B\langle\varphi|_C + \langle\varphi|_B\langle\psi|_C\big)\frac{1}{2}\big(|\psi\rangle_B|\varphi\rangle_C + |\varphi\rangle_B|\psi\rangle_C\big)$$

$$p_0 = \frac{1}{4}\big(\langle\psi|_B\langle\varphi|_C|\psi\rangle_B|\varphi\rangle_C + \langle\psi|_B\langle\varphi|_C|\varphi\rangle_B|\psi\rangle_C + \langle\varphi|_B\langle\psi|_C|\psi\rangle_B|\varphi\rangle_C + \langle\varphi|_B\langle\psi|_C|\varphi\rangle_B|\psi\rangle_C\big)$$

$$p_0 = \frac{1}{4}\big(\langle\psi|\psi\rangle_B \otimes \langle\varphi|\varphi\rangle_C + \langle\psi|\varphi\rangle_B \otimes \langle\varphi|\psi\rangle_C + \langle\varphi|\psi\rangle_B \otimes \langle\psi|\varphi\rangle_C + \langle\varphi|\varphi\rangle_B \otimes \langle\psi|\psi\rangle_C\big)$$

$$p_0 = \frac{1}{4}(1 + |\langle\psi|\varphi\rangle|^2 + |\langle\psi|\varphi\rangle|^2 + 1)$$

$$p_0 = \frac{1}{2} + \frac{1}{2}|\langle\psi|\varphi\rangle|^2$$

Since $p_0 + p_1 = 1$,

$$p_1 = \frac{1}{2} - \frac{1}{2}|\langle\psi|\varphi\rangle|^2$$

(c)

Since $|\psi\rangle_A$ and $|\varphi\rangle_B$ are pure states, their fidelity is $|\langle\psi|\varphi\rangle|^2$

The probability of measuring a 0 is p_0, so we get

$$p_0 = \frac{m}{N}$$

$$\frac{1}{2} + \frac{1}{2}|\langle\psi|\varphi\rangle|^2 = \frac{m}{N}$$

$$1 + |\langle\psi|\varphi\rangle|^2 = 2\frac{m}{N}$$

$$|\langle\psi|\varphi\rangle|^2 = 2\frac{m}{N} - 1$$

This is the required fidelity

Question 7

Given:

$$f : \{0,1\}^n \mapsto \{0,1\}^n$$

$$\forall x, y \in \{0,1\}^n \; f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, d\}$$

$$U_f\left(|x\rangle_Q \otimes |y\rangle_R\right) := |x\rangle_Q \otimes |y \oplus f(x)\rangle_R$$

(a)

To Prove: f is one-to-one when $d = 0^n$ and two-to-one otherwise

Proof:

Case 1: $d = 0^n$

$$\forall x, y \in \{0,1\}^n \ f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, 0^n\}$$

$$\forall x, y \in \{0,1\}^n \ f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n\}$$

$$\forall x, y \in \{0,1\}^n \ f(x) = f(y) \leftrightarrow x \oplus y = 0^n$$

$$\forall x, y \in \{0,1\}^n \ f(x) = f(y) \leftrightarrow x = y$$

Thus, f is one-one in this case

Case 2: $d \neq 0^n$

To prove that f is two-one, we need to show that $\forall z \in \text{range}(f)$, we have exactly two elements x, y such that $f(x) = f(y) = z$

$$\forall x, y \in \{0,1\}^n \ f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, d\}$$

(i) $x \oplus y = 0^n$

$x = y$, thus $f(x) = f(y)$

(ii) $x \oplus y = d$ with $d \neq 0^n$

$$y = d \oplus x$$

Since $d \neq 0^n$, we get $y \neq x$, and $f(x) = f(y)$

Clearly, two distinct values x and y give the same output. Now, we need to prove that no more than two distinct inputs give the same output.

Consider distinct $a, b, c \in \{0,1\}^n$ such that $f(a) = f(b) = f(c)$

Since a, b, c are distinct, their xor cannot be 0^d, thus we have

$$a \oplus b = b \oplus c = d$$

$$a = d \oplus b, c = d \oplus b$$

$$a = c$$

This is a contradiction. Thus, there only exist exactly two input values for each output value.

Thus, f is a two-one function in this case

Hence, proven

(b)

To Find: $|\psi'\rangle_{QR}$

Solution:

Initially, the state is

$$|0^n\rangle_Q \otimes |O^n\rangle_R$$

After the first Hadamard, the state is

$$H^{\otimes n}|0^n\rangle_Q \otimes |0^n\rangle_R$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_Q \otimes |0^n\rangle_R$$

After the oracle, the state is

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_Q \otimes |0^n\rangle_R$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle_Q \otimes |0^n\rangle_R$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_Q \otimes |0^n \oplus f(x)\rangle_R$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_Q \otimes |f(x)\rangle_R$$

After the second Hadamard, the required state is

$$|\psi'\rangle_{QR} = H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_Q \otimes |f(x)\rangle_R$$

$$|\psi'\rangle_{QR} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} H^{\otimes n}|x\rangle_Q \otimes |f(x)\rangle_R$$

$$|\psi'\rangle_{QR} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle_Q \otimes |f(x)\rangle_R$$

$$|\psi'\rangle_{QR} = \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle_Q \otimes |f(x)\rangle_R$$

(c)

To Prove: Probability of getting outcome $j = j_1 ... j_n$ is given by

$$p(j) = \| \frac{1}{2^n} \sum_{z\in\ \mathrm{range}(f)} \left(1 + (-1)^{j\cdot d}\right)|z\rangle\|^2$$

Proof:

$$|\psi'\rangle_{QR} = \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle_Q \otimes |f(x)\rangle_R$$

The coefficient of $|j\rangle$ is

$$|\varphi\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot j} |f(x)\rangle$$

Thus, the probability of measuring outcome $|j\rangle$ is

$$\langle \varphi | \varphi \rangle$$

$$\left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot j} \langle f(x)| \right) \left(\frac{1}{2^n} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot j} |f(y)\rangle \right)$$

$$\frac{1}{2^{2n}} \sum_{x, y \in \{0,1\}^n} (-1)^{x \cdot j + y \cdot j} \langle f(x) | f(y) \rangle$$

(d)

To Prove: $p(j)$ is nonzero only if $j \cdot z = 0$

Proof:

We know that

$$j \cdot z = \oplus_{i=1}^{n} j_i z_i$$

Thus, either $j \cdot z = 0$ or $j \cdot z = 1$, since the xor of bits can only be a bit.

If $j \cdot z = 0$,

$$p(j) = \| \frac{1}{2^n} \sum_{z \in \text{ range}(f)} \left(1 + (-1)^0\right) |z\rangle \|^2$$

$$p(j) = \| \frac{1}{2^{n-1}} \sum_{z \in \text{ range}(f)} |z\rangle \|^2$$

If otherwise, i.e, $j \cdot z = 1$

$$p(j) = \| \frac{1}{2^n} \sum_{z \in \text{ range}(f)} \left(1 + (-1)^1\right) |z\rangle \|^2$$

$$p(j) = \| \frac{1}{2^n} \sum_{z \in \text{ range}(f)} 0 |z\rangle \|^2$$

$$p(j) = 0$$

Clearly, if $j \cdot z = 0$, only then $p(j)$ can be non-zero.

Hence, proven.

(e)

To Find: The number of queries to f to determine d classically

Solution: We can use the fact that the function is either one-one or two-one depending on the choice of d.

If we perform $2^{n-1} + 1$ queries, there are two cases

1. If all the outputs are distinct, the function can't be two-one, as one of the outputs must have been repeated if it was. Thus, the function is one-one. Thus, d is 0^n.
2. If any two outputs are same, say $f(x) = f(y) = z$, then we have $d = x \oplus y$

Thus, always within $2^{n-1} + 1$ queries to f, one can determine d classically.