Midterm 2

Graded

Student

Sujith Potineni

Total Points

15 / 20 pts

Question 1

Question 1

5 / 5 pts

- ✔ **+ 5 pts** Correct
- **+ 1 pt** (a) got the correct joint state after the cswp.
- **+ 2 pts** (a) got the correct final joint state.
- **+ 2.5 pts** (a) Correct
- **+ 2.5 pts** (b)
- **+ 0 pts** Incorrect

Question 2

Question 2

0 / 5 pts

- **+ 5 pts** Correct
- **+ 3.5 pts** Recalled the Grover search algorithm, but failed to find the right reflection.
- **+ 2.5 pts** Recalled correctly he Grover search algorithm.
- **+ 1.5 pts** Recalled the first three gates in the Grover search algorithm.
- **+ 1 pt** Recalled the first two gates in the Grover search algorithm.
- **+ 1 pt** Recalled correctly how the sign-implementation affects the amplitudes graph
- ✔ **+ 0 pts** Incorrect

Question 3

Question 3

5 / 5 pts

- ✔ **+ 5 pts** Correct
- **+ 4 pts** Did the correct calculation for several N and guessed the right answer without justification
- **+ 1 pt** Correctly recalled the DFT
- **+ 0.5 pts** Did correctly the calculation for N = 2
- **+ 0 pts** Incorrect

Question 4

Question 4

5 / 5 pts

✔ **+ 5 pts** Correct

+ 2.5 pts Found the right order of a

+ 1 pt Considered a+1 and a-1, but did not use gcd

+ 0 pts Incorrect

CSE 598 Quantum Computation
Midterm #2, Fall 2024

Instructor: Zilin Jiang

October 31, 2024

Full name: Bala Sujith Potineni

Time: 75 minutes. **Four problems** worth 5 points each.

Instructions

1. Closed book. No notes or any electronic devices during the exam.
2. You must provide justification in your solutions (not just answers).
3. You may quote theorems and facts proved in class, course textbook/notes, or homework, provided that you state the facts that you are using.
4. This exam will be scanned before grading, so please ensure your writing is clear and legible.

$$\begin{bmatrix}1&1&1\\1&\omega^{-1}&\omega^{-2}\\1&\omega^{-2}&\omega^{-4}\end{bmatrix}\begin{bmatrix}1&1&1\\1&\omega^{-1}&\omega^{-2}\\1&\omega^{-2}&\omega^{-4}\end{bmatrix}$$

(-1)

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&(-1)\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&(-1)\end{bmatrix}$$

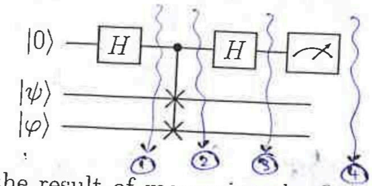
$(M-1)$

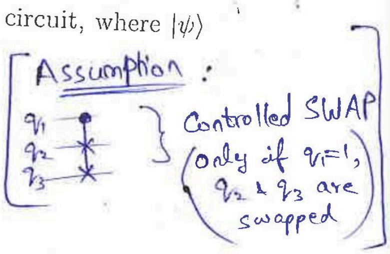
M

$$\begin{bmatrix}2&0\\0&2\end{bmatrix}$$

"To read our email, how mean of the spies and their quantum machine; be comforted though, they do not yet know how to factorize twelve or fifteen." — *Volker Strassen*

Problem 1 The SWAP gate performs the map $|x\rangle|y\rangle \mapsto |y\rangle|x\rangle$ for $x, y \in \{0, 1\}$, and is denoted in quantum circuit by [SWAP symbol]. Consider the following quantum circuit, where $|\psi\rangle$ and $|\varphi\rangle$ are arbitrary states of one qubit.





What is the probability that the result of measuring the first qubit is $|1\rangle$ in each of these two cases?

(i) $|\psi\rangle = |0\rangle, \quad |\varphi\rangle = |1\rangle$.

(ii) $|\psi\rangle = |\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Solution:

(i) At 1, J.S. = $|+\rangle \otimes |0\rangle \otimes |1\rangle$

~~At 2, J.S. = $|+\rangle \otimes |1\rangle \otimes |0\rangle$~~

~~At 3, J.S. = $|0\rangle \otimes |1\rangle \otimes |0\rangle$~~

~~At 4, Readout = { $|0\rangle$ with 100% probability; 2nd & 3rd qubits are $|10\rangle$.~~

~~$\Rightarrow$ Probability [Measuring 1st qubit is $|1\rangle$] = 0~~

~~(ii) At 1, J.S. = $|+\rangle \otimes |+\rangle \otimes |+\rangle$~~

~~At 2, J.S. = $|+\rangle \otimes |+\rangle \otimes |+\rangle$~~

~~At 3, J.S. = $|0\rangle \otimes$~~

At 2, J.S. = $\frac{1}{\sqrt{2}}|0\rangle \otimes |01\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |10\rangle$

At 3, J.S. = $\frac{1}{\sqrt{2}}|+\rangle \otimes |01\rangle + \frac{1}{\sqrt{2}}|-\rangle \otimes |10\rangle$

$= \frac{1}{2}|001\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|010\rangle - \frac{1}{2}|110\rangle = \left[\frac{1}{\sqrt{2}}|0\rangle \otimes \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle \otimes \left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right)\right]$

At 4, Readout = $\begin{cases} |0\rangle \text{ with 50\% probability; Next qubits are } \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) \quad \left(\because \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}\right) \\ |1\rangle \text{ with 50\% probability; Next qubits are } \left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) \quad \left(\because \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}\right) \end{cases}$

$\Rightarrow$ Probability [Measuring 1st qubit is $|1\rangle$] = 0.5

(ii) At ①, J.S. = $|{+}{+}{+}\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |{+}{+}\rangle$

~~At ②, J.S. =~~ $\cancel{\frac{|0\rangle}{\sqrt{2}} \otimes |{+}{+}\rangle + \frac{|1\rangle}{\sqrt{2}}}$ $\cancel{\frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle}$ ~~[i is binary coded]~~

~~(by uniform superposition)~~

At ②, J.S. = $\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |{+}{+}\rangle$ [∵ $SWAP(|{+}{+}\rangle) = |{+}{+}\rangle$]

At ③, J.S. = $|0\rangle \otimes |{+}{+}\rangle$

At ④, 1st-qubit Readout = $\begin{cases} |0\rangle & \text{with } 100\% \text{ probability; Next qubits are } |{+}{+}\rangle \\ |1\rangle & \text{with } 0\% \text{ probability} \end{cases}$

⇒ Probability [1st qubit measurement = $|1\rangle$] = 0

Problem 2 We would like to solve the Grover search problem for the Boolean function $F: \{0,1\}^n \to \{0,1\}$, where we know that exactly M elements $x \in \{0,1\}^n$ satisfy $F(x) = 1$. Show that, if $M = N/4$, where $N = 2^n$, the Grover search problem can be solved with one use of the sign-implementation $Q_F^{\pm}$ of F.

Using Basic Adversary Method of Ambaini's 2000 paper,

Promise: Exactly 'M' elements $x \in \{0,1\}^n$ satisfy $F(x)=1$ for $F: \{0,1\}^n \to \{0,1\}$

$\Rightarrow$ string $w =$ "01...0111..." has exactly 'M' 1's & $(N-M)$ 0's.

(Here $N = 2^n$)

$Y \subseteq YES = \{\underbrace{111111}_{M}\underbrace{000}_{N-M}, \underbrace{11111}_{M-1}01000..., ...\}$

$N \leq NO$ ~~$\{0,1\}^n / YES$~~ & $N =$ strings of exactly $(M-1)$ 1's.

$m =$ Number of strings z in $z \in N$ s.t. for every $y \in Y$; $dist(y,z) = 1$
$= M + (N-M) = N$

$m' =$ Number of strings y in $y \in Y$ s.t. for every $z \in N$; $dist(y,z) = 1$
$= N - M + 1$

$l =$ Number of strings z in $z \in N$ s.t. for every $y \in Y$ & j; $y_j \neq z_j$
$= 1$

$l' =$ Number of strings y in $y \in Y$ s.t. for every $z \in N$ & j; $y_j \neq z_j$
$= N - M + 1$

$\sqrt{\frac{N}{k}} = \sqrt{\frac{N}{\frac{N}{4}}} = 2$

Extra space for Problem 2

Problem 3 Using the formula for a geometric series, or otherwise, write down an expression for $(\mathrm{DFT}_N)^2$ for any N, where DFT_N is the discrete Fourier transform.

$$\mathrm{DFT}_N = \frac{1}{\sqrt{N}}\begin{bmatrix} \omega^{-0} & \omega^{-0} & \omega^{-0} & \cdots & \omega^{-0} \\ \omega^{-0} & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-16} \\ \omega^{-0} & \omega^{-2} & \omega^{-4} & \cdots & \omega^{-32} \\ \vdots & & & & \vdots \\ \omega^{-0} & \omega^{-(N-1)} & \omega^{-2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}_{N\times N}$$

(In this matrix, element $a_{sx} = \frac{\omega^{-sx}}{\sqrt{N}}$ where $s, x \in \{0, 1, \ldots, (N-1)\}$)

Here $\omega = N^{th}$ root of unity $= \left[e^{\frac{2\pi i}{N}}\right]$

$$\Rightarrow (\mathrm{DFT}_N)^2 = (\mathrm{DFT}_N)(\mathrm{DFT})_N$$

The element a_{sx} of $(\mathrm{DFT}_N)^2$ is given by $\frac{1}{(\sqrt{N})^2}\sum_{i=0}^{(N-1)}(a_{si}\cdot a_{ix})$

$$= \frac{1}{N}\sum_{i=0}^{(N-1)}\left(\omega^{-si}\cdot\omega^{-ix}\right) = \frac{1}{N}\sum_{i=0}^{(N-1)}\left(\omega^{-i(s+x)}\right) = \frac{1}{N}\left[\omega^{-0} + \omega^{-(s+x)} + \omega^{-2(s+x)} + \cdots + \omega^{-(N-1)(s+x)}\right]$$

(Geometric Series)

$$= \begin{cases} \frac{1}{N}\left[\frac{\omega^{-N(s+x)} - 1}{\omega^{-(s+x)} - 1}\right] = 0, & \text{when } \omega^{-(s+x)} \neq 1 \\ \frac{N}{N} = 1, & \text{when } \omega^{-(s+x)} = 1 \end{cases}$$

[Here $\omega^{-N(s+x)} = 1 \Rightarrow \left(\frac{\omega^{-N(s+x)} - 1}{\omega^{-(s+x)} - 1}\right) = 0$]

Cases when $\omega^{-(s+x)} = 1$:

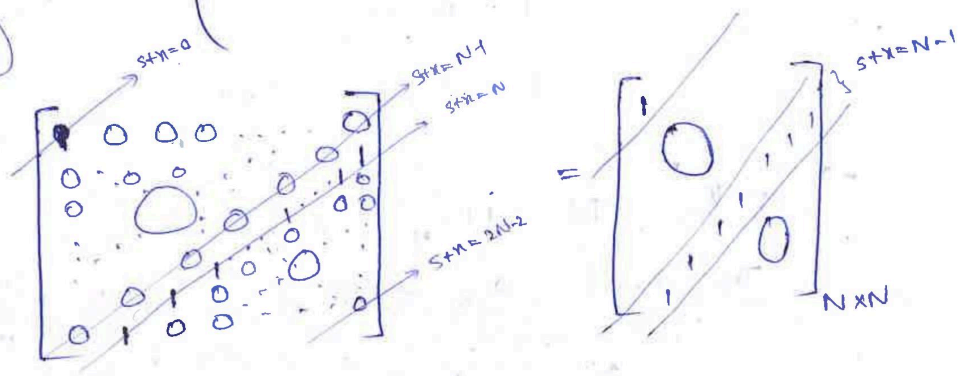
$$\omega^{-(s+x)} = e^{\frac{-2\pi i}{N}(s+x)} = 1 \Rightarrow (s+x) = Nk \text{ for } k \in \mathbb{Z}$$

$$\Rightarrow (\mathrm{DFT}_N)^2 = \left(\frac{1}{\sqrt{N}}\right)^2 \begin{bmatrix} N & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & & & & & N \\ 0 & & & & & N & 0 \\ \vdots & & & & & & \vdots \\ 0 & N & N & N & 0 & \cdots & 0 \end{bmatrix}_{N\times 1}$$

$$\text{So, } \left\{ \left(DFT_N\right)^2 \right\}_{(s,x)} = \begin{cases} 0, & \text{if } s+x \neq Nk \text{ for } k \in \mathbb{Z} \\ 1, & \text{if } s+x = Nk \text{ for } k \in \mathbb{Z} \end{cases}$$

$\underbrace{s,x}_{\text{indices}} \in \{0,1,\ldots,(N-1)\}$

$\Rightarrow \left(DFT_N\right)^2 =$



Problem 4 Assume that we would like to factorize $N = 33$ and pick $a = 10$. Determine the order of a mod N and use this information to factorize N.

Remark: It's important to note that directly expressing $33 = 3 \times 11$ is not sufficient. The factorization must be achieved using the order of a to derive the factors of N.

Assumption: $33 = P \times Q$ (product of 2 primes)

~~10 Mod 33~~ Here $a = 10 \Rightarrow a \bmod N = 10 \equiv 10 \bmod 33$

$a^2 \bmod N = 100 \equiv 1 \bmod 33$

$\Rightarrow \boxed{\text{Order} = 2}$ & its even.

$\Rightarrow$ For $L = \frac{2}{2} = 1$, $a^{\frac{L}{2}} \equiv \pm 1 \bmod P$ (p is one of the 2 prime factors of 33)

$\Rightarrow$ $10^1 \equiv \pm 1 \bmod p$

$\Rightarrow$ $9 \bmod p$ (or) $11 \bmod p$

Taking $11 \bmod p$:

Here $p = \gcd(11, 33)$

So, by euclid's algorithm,

$33 = 11 \times 3 + 0 \Rightarrow 11 = \gcd(11, 33)$

$\Rightarrow p = 11 \Rightarrow q = \frac{33}{p} = 3$

$\therefore N = 33 = 11 \times 3$

Because under the assumption that $N = P \times Q$ where P, Q are primes.

Since $a^L \equiv 1 \pmod N \Rightarrow (a^{\frac{L}{2}} - 1)(a^{\frac{L}{2}} + 1) \equiv 0 \pmod N$

$\Rightarrow a^{\frac{L}{2}} \equiv 1$ or $a^{\frac{L}{2}} \equiv -1$ ~~mod N~~ $\pmod P$

$\Rightarrow \gcd(a^{\frac{L}{2}} - 1, N)$ or $\gcd(a^{\frac{L}{2}} + 1, N) = P$

Extra space for Problem 4