Eric Du — Physics C191

HW 05 — Introduction to Quantum Computing — February 26, 2024

Header styling inspired by CS 70: https://www.eecs70.org/

Collaborators

I worked closely with **Teja Nivarthi** on this assignment.

Problem 1

Alice has a pair of qubits a_1, a_2 which have been prepared in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alie would like to teleport this entangled state to Bob and Charlie such that they will share an entangled state $|\Phi^+\rangle$ between their respective qubits.

She follows the standard quantum teleportation protocol. A source sends an entangled qubit pair b_1, b_2 to Alice and Bob, respectively, and also sends an entangled qubit pair c_1, c_2 to Alice and Charlie, respectively. Each qubit pair is in the Bell state $|\Phi^+\rangle$. The following eleportation scheme is then executed (note that this is the same scheme that was presented in lecture, only now we are applying it twice because alice wants to teleport two qubits): (Diagram clarifications: The measuremet icon refers to a standard basis measurement. The standard notation for CNOT is used here, where the filled in circle • is the control qubit and the open circle $\oplus$ is the target qubit.)

Since each of the three pairs of qubits is initially in the state $|\Phi^+\rangle$, the initial six-qubit state can be written as:

$$\begin{aligned}|\Phi^+\rangle\,|\Phi^+\rangle\,|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\ &= \frac{1}{2\sqrt{2}}(|000000\rangle + |000011\rangle + |001100\rangle + |001111\rangle + |110000\rangle + |110011\rangle + |111100\rangle + |111111\rangle)\end{aligned}$$

where the qubit ordering we have used in writing out these states is $|a_1a_2b_1b_2c_1c_2\rangle$.

a) What is the state of the system after both CNOT gates have been executed?

Solution: The CNOT gate applies to bits a_1, b_1 and a_2, c_1, so therefore the state looks like:

$$|\psi\rangle = \frac{1}{2\sqrt{2}}(|000000\rangle + |000011\rangle + |001100\rangle + |001111\rangle + |111010\rangle + |111001\rangle + |110110\rangle + |110101\rangle)$$

□

b) What is the state of the system after both Hadamard gates have been executed?

Solution: Now we need to apply the Hadamard gates. Recall that a hadamard gate turns the states:

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |1\rangle \to \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Now, we'll be applying the Hadamard gate to a_1 and a_2, so therefore:

$$\begin{aligned}|\psi\rangle = \frac{1}{4\sqrt{2}}\Bigg[&\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^2(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)\\ &+ \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^2(|1010\rangle + |1001\rangle + |0110\rangle + |0101\rangle)\Bigg]\end{aligned}$$

I refuse to write down all 32 possible states. □

c) Now assume that the measurements all contain a result of 0, such that the X and Z gates are not executed. What is the final state of the system? Was alice successful in teleporting the entangled state to Bob and Charlie?

Solution: If both measurements return zero, the final state of the system is acutally very simple, and consists only of two terms, since the measurements ensure that a_1, a_2, b_1, c_1 are all zero. Therefore, this corresponds to the states:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|000000\rangle + |000101\rangle) = \frac{1}{\sqrt{2}}|00\rangle\,(\,|0000\rangle + |0101\rangle)$$

This final state is precisely the entangled state we wanted (b_2 and c_2) are entangled with each other, so Alice was indeed successful in this case. □

Problem 2

In this question, we will show the following fact about the quantum Fourier transform applied to quantum states with periodic amplitudes:

Suppose that you have a quantum state

$$|\psi\rangle = \sum_{k=1}^{N-1} \alpha_k |k\rangle$$

with periodic amplitudes ($\alpha_k = \alpha_{k+t} \bmod N$ for some $1 \leq t \leq N-1$). Note that periodicity requires that t divides N.

We will show that

$$\mathrm{QFT}_N |\psi\rangle = \sum_{k=1}^{N-1} \beta_k |k\rangle$$

where $\beta_k \neq 0$ only if k is an integer multiple of N/t.

a) Show that if $|\psi\rangle$'s amplitudes are periodic with period t (i.e., $\alpha_k = \alpha_{k+t \bmod N}$), then it is equivalent to the state $|\psi + t\rangle$:

$$|\psi + t\rangle = \sum_{k=1}^{N-1} \alpha_k |k + t \bmod N\rangle$$

Solution: Since we know that $\alpha_k = \alpha_{k+t \bmod N}$, then we know that the coefficient attached to $|k + t \bmod N\rangle$ is the same as α_k. Thus, for all states $|k + t \bmod N\rangle$, they all share the same α_k. □

b) Recall that the N'-th root of unity $\omega_N = e^{i\frac{2\pi}{N}}$. Show that $\omega_N^r = 1$ if and only if r is an integer multiple of N.

Solution: We show first that $\omega_N^r = 1$ if r is a multiple of N. This means we can write $r = kN$ for some k, and therefore:

$$\omega_N^r = e^{i\frac{2\pi}{N} \cdot kN} = e^{i2\pi k}$$

And since k is an integer, then we know that $\omega_N^r = 1$. For the reverse side, we we know ω_N^r can be written as:

$$\omega_N^r = e^{i\frac{2\pi}{N}r}$$

If this must equal 1, then it must be the case that $i\frac{2\pi}{N}r = k(2\pi i)$, which implies that r must be a multiple of N. □

c) Using that the quantum Fourier transforms of $|\psi\rangle$ and $|\psi + t\rangle$ are related in the following way. If

$$\mathrm{QFT}_N |\psi\rangle = \sum_{k=1}^{N-1} \beta_k |k\rangle$$

then

$$\mathrm{QFT}_N |\psi + t\rangle = \sum_{k=1}^{N-1} \omega_N^{kt} \beta_k |k\rangle$$

Show that if $|\psi\rangle = |\psi + t\rangle$, then $\mathrm{QFT}_N |\psi\rangle$ has nonzero amplitudes only on integer multiples of N/t. That is, show that if $\beta_k \neq 0$, then $k = \ell(N/t)$ for some integer ℓ.

Solution: If $|\psi\rangle = |\psi + t\rangle$, then we also know that applying QFT_N on both states should return the same values. Therefore, we have:

$$\sum_{k=1}^{N-1} \beta_k |k\rangle = \sum_{k=1}^{N-1} \omega_N^{kt} \beta_k |k\rangle$$

If $\beta_k \neq 0$, then we have:

$$\omega_N^{kt} = 1$$

Then from part (b), we know that this implies that kt must be a multiple of N, and one way to guarantee that is to let $k = \ell(N/t)$ for some integer ℓ, as desired. □

Problem 3

In this question, we will go through a small example of Schor's factoring algoritihm. Use the following facts about the quantum Fourier transform (QFT_M) applies to periodic and shifted states:

1) QFT on periodic states: Let $1 < r < M$ be an integer that divides M. QFT_M applied to the state $\sqrt{\frac{r}{M}}(\,|0\rangle + |r\rangle + |2r\rangle + \cdots + |M-r\rangle)$ results in
$$\frac{1}{\sqrt{r}}(\,|0\rangle + \,|M/r\rangle + \,|2M/r\rangle + \cdots + \,|(r-1)M/r\rangle)$$

2) QFT on shifted states: If $|\psi\rangle = \sum_{k=0}^{M-1} \alpha_k\,|k\rangle$ and $|\psi + t\rangle = \sum_{k=0}^{M-1} \alpha_k\,|k + t \bmod N\rangle$, then QFT_M applied to the two states are related by: If
$$\text{QFT}_M\,|\psi\rangle = \sum_{k=0}^{M-1} \beta_k\,|k\rangle$$
then
$$\text{QFT}_M\,|\psi + t\rangle \sum_{k=0}^{M-1} \omega_M^{kt}\beta_k\,|k\rangle$$
We will work through an example of factoring $N = 21$ using QFT_M with $M = 12$.

a) Let $a = 2$. Calculate the state $|\psi\rangle = \sum_{x=0}^{M-1}\,|x\rangle\,|a^x \bmod N\rangle$.

Solution: Written out, since $M = 12$, and $N = 21$, this state is equal to:
$$|\psi\rangle = \,|0\rangle\,|1\rangle + \,|1\rangle\,|2\rangle + \,|2\rangle\,|4\rangle + \cdots + \,|10\rangle\,|16\rangle + \,|11\rangle\,|11\rangle$$
The higher powers of 2 were computed using Mathematica. □

---

b) Suppose we measure the second register of $|\psi\rangle$ and obtain "1". What is the resulting state on the first register, then perform QFT_M on the first register. What is the resulting state on the first register? Now measure this state in the standard basis. What are the possible measurement outcomes?

Solution: If we obtain 2 in the second register, then the state after this measurement corresponds to the states $|x\rangle$ where $2^x \equiv 1 \pmod N$. It turns out that this refers to every multiple of 6, so therefore the state for the first register is now:
$$|\psi'\rangle = \frac{1}{2}(\,|0\rangle + \,|6\rangle + \,|12\rangle + \,|18\rangle)$$
Then, performing QFT_M on this, we use rule 1:
$$\text{QFT}_M\,|\psi'\rangle = \frac{1}{\sqrt{6}}(\,|0\rangle + \,|21/6\rangle + \,|42/6\rangle + \,|63/6\rangle + \,|84/6\rangle)$$
□

---

c) Suppose we repeat the above experiment, now the first step (when measuring the second register) gives "4". Answer the same questions as above.

Solution: Repeating what was done above, the state is now:
$$|\psi'\rangle = (\,|2\rangle + \,|8\rangle + \,|14\rangle + \,|20\rangle)$$
□

---

d) Suppose we repeat the above experiment 4 times in total. Each time we record a measurement outcome of the first register (after performing QFT_M). Suppose the recorded outcomes are all different. What is their greatest common divisor g?

e) Calculate $\gcd(N, a^{M/2g} - 1)$ and $\gcd(N, a^{M/2g} + 1)$. Are they prime factors of N?

Problem 4

In this question, we'll try to get a geometric understanding of Grover's algorithm. In Grover's algorithm we have some distinguished, marked element $a \in \{1, \ldots, N\} = [N]$ and have access to some function $f : [N] \to \{0, 1\}$ that recognized a, i.e., $f(a) = 1$ and $f(x) = 0$ if $x \neq a$. Our goal is to use f to find a.

Let $|a\rangle$ be the standard basis state labelled with a and define

$$|e\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \,\in\, [N] \text{ and } x \,\neq\, a} |x\rangle$$

At all times, we will maintain a quanutm state in the two-dimensinoal subspace spanned by $|a\rangle$ and $|e\rangle$. That is, our state can be written as $\alpha\,|a\rangle + \beta\,|e\rangle\, i\ (\alpha, \beta \in \mathbb{R})$ and therefore we can understand the algorithm in a two dimensional space.

a) We start with the state $|u\rangle = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |x\rangle$. Express $|u\rangle$ in terms of $|a\rangle$ and $|e\rangle$. What is the angle θ between $|u\rangle$ and $|e\rangle$ in the following two dimensional space?

Solution: We have the state $|u\rangle$, which we can write as:

$$|u\rangle = \frac{1}{\sqrt{N}}(\,|a\rangle + |e\rangle) = \frac{1}{\sqrt{N}}\,|a\rangle + \sqrt{\frac{N-1}{N}}\,|e\rangle$$

Now, the angle between $|u\rangle$ and $|e\rangle$ is given by the equation:

$$\sin\theta = \frac{1}{\sqrt{N}} \implies \theta = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right)$$

□

b) Apply the oracle U_f (defined as $U_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$) to $|u\rangle$, obtaining the state $|\psi\rangle$. Draw $|\psi\rangle$ in the above two dimensional space.

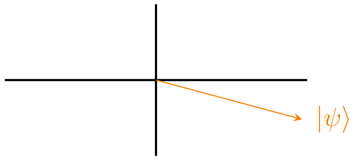
Solution: We do as instructed, and compute $U_f\,|u\rangle$:

$$U_f\,|u\rangle = \frac{1}{\sqrt{N}}(-1)^{f(a)}\,|a\rangle + \sqrt{\frac{N-1}{N}} \sum_{x \neq a} (-1)^{f(x)}\,|x\rangle$$

Then, since we have that $f(a) = 1$ and 0 for all other values everything in the state $|e\rangle$ will evaluate to 1, and hence that part will remain unchanged. Therefore, we have:

$$U_f\,|u\rangle = -\frac{1}{\sqrt{N}}\,|a\rangle + \sqrt{\frac{N-1}{N}}\,|e\rangle$$

The state in the diagram would look like:



□

c) Apply the unitary $2\,|u\rangle\,\langle u| - I$ to the state $|\psi\rangle$. Draw the resulting state in the above two dimensional space.

Solution: We are asked to compute $(2\,|u\rangle\,\langle u| - I)\,|\psi\rangle$. To do this, it's benefiical to rewirte $|\psi\rangle$ in terms of u, so that the outer product may be applied nicely. Rearranging:

$$|\psi\rangle = -\frac{1}{\sqrt{N}}\,|a\rangle + \sqrt{\frac{N-1}{N}}\,|e\rangle = |u\rangle - \frac{2}{\sqrt{N}}\,|a\rangle$$

Therefore, now applying the unitary:

$$\begin{aligned}
|\psi'\rangle = (2\,|u\rangle\,\langle u| - I)\,|\psi\rangle &= (2\,|u\rangle\,\langle u| - I)\,|u\rangle - \frac{2}{\sqrt{N}}(2\,|u\rangle\,\langle u| - I)\,|a\rangle \\
&= |u\rangle - \frac{2}{\sqrt{N}}\left(\frac{2}{\sqrt{N}}\,|u\rangle - |a\rangle\right) \\
&= \left(1 - \frac{4}{N}\right)\,|u\rangle + \frac{2}{\sqrt{N}}\,|a\rangle
\end{aligned}$$

□

---

d) Apply the operation $(2\,|u\rangle\,\langle u| - I)U_f$ two more times on the resulting state from 2.3 and draw the two resulting states in the above two dimensinoal space. What angle of rotation does $(2\,|u\rangle\,\langle u| - I)U_f$ perform in the space?

Solution: To preface, there's a lot of algebra that I'll skip in this problem, but it's basically the same thing we did in part (c) except twice. Applying the unitary to $|\psi'\rangle$:

$$\begin{aligned}
|\psi''\rangle = (2\,|u\rangle\,\langle u| - I)\,|\psi'\rangle &= (2\,|u\rangle\,\langle u| - I)\left(1 - \frac{4}{N}\right)\,|u\rangle - \frac{2}{\sqrt{N}}(2\,|u\rangle\,\langle u| - I)\,|a\rangle \\
&= \left(1 - \frac{4}{N}\right)\,|u\rangle - \frac{4}{N}\,|u\rangle + \frac{2}{N}\,|a\rangle \\
&= \left(1 - \frac{8}{N}\right)\,|u\rangle + \frac{2}{\sqrt{N}}\,|a\rangle
\end{aligned}$$

By this point we can start to notice a pattern: all this operator does is add another $-\frac{4}{N}\,|u\rangle$ to the state, so therefore we can extrapolate:

$$|\psi'''\rangle = (2\,|u\rangle\,\langle u| - I)\,|\psi''\rangle = |\psi''\rangle - \frac{4}{N}\,|u\rangle = \left(1 - \frac{12}{N}\right)\,|u\rangle + \frac{2}{\sqrt{N}}\,|a\rangle$$

Re-expressing this in terms of $|a\rangle$ and $|e\rangle$:

$$|\psi'''\rangle = \sqrt{\frac{N}{N-1}}\left(1 - \frac{12}{N}\right)\,|e\rangle + \frac{1}{\sqrt{N}}\left(3 - \frac{12}{N}\right)\,|a\rangle$$

So now our new angle is:

$$\theta = \sin^{-1}\left(\frac{3}{\sqrt{N}}\left(1 - \frac{4}{N}\right)\right)$$

In general, we can see that applying this operator rotates our state counterclockwise by $2\theta_0$ every time, where θ_0 is the initial angle we started with (in $|\psi\rangle$). □

---

e) Grover's algorithm repeatedly applies $(2\,|u\rangle\,\langle u| - I)U_f$ to $|u\rangle$ to get close to $|a\rangle$. How many times should you apply this operation to et closest to the state $|a\rangle$? (You can use the small angle approximation $\sin\theta \approx \theta$).

Solution: In order for us to get closest to $|a\rangle$, then the requirement is that we want to get an angle as close to $\frac{\pi}{2}$ as possible. From the previous part, we can deduce that after applying the operator k times, we have a total angle of $\theta = (2k+1)\theta_0$, meaning that we have to solve the equation:

$$(2k+1)\sin^{-1}\left(\frac{1}{\sqrt{N}}\right) = \frac{\pi}{2}$$

Using the small angle approximation (valid when N large), we can get rid of the sine, and also get rid of the 1 in from of $2k+1$, since when N is large we also implicitly assume that the initial angle is very close to zero. This means that:

$$k \approx \frac{\pi\sqrt{N}}{4}$$

□
