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

Problem 1

This problem will demonstrate an important aspect in designing quantum algorithms. Suppose we have some "oracle" that implements a unitary $O_{x,\pm}$ based on a classical 2-bit string $x = x_0x_1$. The action of the unitary on the computational basis is

$$O_{x,\pm} : |b\rangle \to (-1)^{x_b} |b\rangle \text{ for } b \in \{0, 1\}$$

a) Say that we run the 1-qubit circuit $HO_{x,\pm}H$ on the initial state $|0\rangle$ and then measure in the computational basis. What is the probability distribution on the output bit as a function of x?

Solution: Carrying out the calculation:

$$\begin{aligned} HO_{x,\pm}H|0\rangle &= HO_{x,\pm}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\ &= H \cdot \left(\frac{(-1)^{x_0}|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Now, depending on the identity of x, this state before acting H will change. So, we need to treat this on a case-by-case basis:

$$\begin{aligned} x = 00 &\longrightarrow H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left[|0\rangle + |1\rangle + |0\rangle - |1\rangle\right] = |0\rangle \\ x = 01 &\longrightarrow H\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left[|0\rangle + |1\rangle - (|0\rangle - |1\rangle)\right] = |1\rangle \\ x = 10 &\longrightarrow H\left(\frac{-|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left[-(|0\rangle + |1\rangle) + |0\rangle - |1\rangle\right] = -|1\rangle \\ x = 11 &\longrightarrow H\left(\frac{-|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left[-(|0\rangle + |1\rangle - (|0\rangle - |1\rangle)\right] = -|0\rangle \end{aligned}$$

So, the output bit from this process is entirely determined by the value of x. □

---

b) Now suppose we have a second implementation $O'_{x,\pm}$ that copies the value of the classical bit b over to a second register. That is, $O'_{x,\pm}$ is implemented as

$$O;_{x,\pm} : |b, 0\rangle \to (-1)^{x_b} |b, b\rangle$$

Suppose we ignore the second qubit and run the algorithm of (a) on the first qubit with $O'_{x,\pm}$ instead of $O_{x,\pm}$ (and $H \otimes I$ instead of H and initial state $|00\rangle$). What is now the probability distribution on the output bit (i.e. if we measure the first of the two qubits).

The point is to show the importance of "cleaning up" additional computational resources that were used in the computation. By leaving "garbage" in an ancillary register that is coupled to a sub-register one wishes to measure, the residual entnalgement between the two registers can corrupt measurement outcome distributions.

Solution: Applying the first two gates to the state, we get:

$$(H \otimes I)O'_{x,\pm}(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(H \otimes I)\left[(-1)^{x_0}|00\rangle + (-1)^{x_1}|11\rangle\right]$$

(I'm too lazy to write out the intermediate steps). Again, we do the same process as the previous problem:

$$\begin{aligned}
x = 00 &\longrightarrow \frac{1}{\sqrt{2}}(H \otimes I)(\left|00\right\rangle + \left|11\right\rangle) = \frac{1}{2}(\left|00\right\rangle + \left|10\right\rangle + \left|01\right\rangle + \left|11\right\rangle) \\
x = 01 &\longrightarrow \frac{1}{\sqrt{2}}(H \otimes I)(\left|00\right\rangle - \left|11\right\rangle) = \frac{1}{2}(\left|00\right\rangle + \left|10\right\rangle - \left|01\right\rangle - \left|11\right\rangle) \\
x = 10 &\longrightarrow \frac{1}{\sqrt{2}}(H \otimes I)(-\left|00\right\rangle + \left|11\right\rangle) = \frac{1}{2}(-\left|00\right\rangle - \left|10\right\rangle + \left|01\right\rangle + \left|11\right\rangle) \\
x = 11 &\longrightarrow \frac{1}{\sqrt{2}}(H \otimes I)(-\left|00\right\rangle - \left|11\right\rangle) = \frac{1}{2}(-\left|00\right\rangle - \left|10\right\rangle - \left|01\right\rangle - \left|10\right\rangle)
\end{aligned}$$

In all of these states, the probability of measuring 0 from the first qubit is $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, which is different than what we have in part (a). $\square$

Problem 2

a) Prove that any classical algorithm requires at least two calls to f to solve the Deutsch Josza problem with probability greater than $1/2$.

Solution: A simple randomized algorithm, where we pick a random input to f, will be able to determine the identity of f with a success rate of $\frac{2}{3}$ after two calls, this fact was proven in lecture.

We can then make the argument that *any* classical algorithm must also do this becuase regardless of how our classical algorithm inquires about f, the probability of it receiving either 0 or 1 is $\frac{1}{2}$ if f is balanced. Therefore, the probability of error after two calls is going to be

$$P(\text{error}) = \frac{1}{2^2} = \frac{1}{4}$$

so the probability of success is greater than $\frac{1}{2}$, as desired. ☐

---

b) Prove that any classical algorithm requires $2^{n-1} + 1$ calls to f to solve the Deutsch-Josza problem with certainty.

Solution: A classical algorithm needs to check more than half the values of f to determine f with certainty, due to the pigeonhole principle (once we've covered more than half the values, then if f is balanced then both 0 and 1 would have been seen.). Therefore, for a bitstring of length n, the search space is 2^n, so we require at least $2^{n-1} + 1$ queries. ☐

---

c) Describe a classical approach to the Deutsch Josza problem that solves it with high probability using fewer than $2^{n-1}+1$ calls. Calculate the success probability of your approach as a function of the number of calls.

Solution: Consider a randomized algorithm that selects a random bitstring out of the 2^n possible ones and inquires about f. If f is balanced, then the probability that f outputs either 0 or 1 is $\frac{1}{2}$ on every call. Therefore, after k calls, the probability of error (i.e. we output that f is constant when in reality f is balanced) is:

$$P(\text{error}) = \frac{1}{2^k}$$

Note that this probability of error drops off very quickly; after just 10 queries, the probability of error is already less than 0.1%. ☐

Problem 3

The (classical) Fourier transform mod N is the $N \times N$ matrix given by

$$FT_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}$$

where $\omega = e^{2\pi i/N}$ has a primitive N th root of unity. So the i, j 'th element of FT_N is $\frac{1}{\sqrt{N}}\omega^{ij}$, for $i, j = 0, \dots, N-1$. Show that FT_N is unitary by evaluating the inner product between the i and j th columns of FT_N, i.e., show that

$$\langle i|FT_N^\dagger FT_N|j\rangle = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Your calculation will demonstrate a very important and useful result, namely that for ω a primitive N-th root of unity (i.e., $\omega^N = 1$ but $\omega^m \neq 1$ for $0 < m < N$),

$$\sum_{k=0}^{N-1} \omega^{kj} = \begin{cases} N & \text{if } j = 0 \pmod{N} \\ 0 & \text{otherwise} \end{cases}$$

Solution: Notice that the (i, j)-th element of the product $FT_N^\dagger FT_N$ is given by the dot product of the i-th row of $FT_N^\dagger$ and j-th column of FT_N. An element in the i-th row of $FT_N^\dagger$ is written as $\frac{1}{\sqrt{N}}\omega^{-ik}$, and an element in the j-th column of FT_N is written as $\frac{1}{\sqrt{N}}\omega kj$. Therefore, we can write the product as:

$$M_{ij} = \frac{1}{N}\sum_{k=1}^{N-1} \omega^{-ik}\omega^{kj} = \frac{1}{N}\sum_{k=1}^{N-1} \omega^{(j-i)k}$$

Now, let $m = j - i$, so we have

$$\frac{1}{N}\sum_{k=1}^{N-1} \omega^{km}$$

Since ω is an N-th root of unity, then it satisfies the equation $\omega^N - 1 = 0$. Factoring this, we get

$$(\omega - 1)(\omega^{N-1} + \omega^{N-2} + \dots + 1) = 0 \tag{1}$$

If $\omega - 1 = 0$, then this means that $m = 0$ or $i = j$, so then $\omega = 1$. This means that

$$\frac{1}{N}\sum_{k=1}^{N-1} \omega^{km} = \frac{1}{N}\sum_{k=1}^{N-1} N = 1$$

If the second term in eq. 1 is equal to zero, then this implies that $j \neq i$, and we notice that

$$\sum_{k=1}^{N-1} \omega^{km} = \omega^{N-1} + \omega^{N-2} + \dots + 1 = 0$$

so we immediately have that if $j \neq i$, then the summation is also zero. Therefore, we have:

$$M_{ij} = \frac{1}{N}\sum_{k=1}^{N-1} \omega^{km} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \implies M_{ij} = \delta_{ij}$$

as desired. $\square$

Problem 4

The uncertainty principle bounds how well a quantum state can be localized simultaneously in the standard basis and the Fourier basis. In this question, we will derive an uncertainty princpile for a discrete system of n-qubits.

Let $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ be the state of an n-qubit system. A measure of the spread of $|\psi\rangle$ is $S(|\psi\rangle) \equiv \sum_x |\alpha_x|$. For example, a completely localized state $|\psi\rangle = |y\rangle\, (y \in \{0,1\}^n)$, the spread of $S(|\psi\rangle) = 1$. For a maximally spread state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, $S(|\psi\rangle) = 2^n \cdot \frac{1}{\sqrt{2^n}} = \sqrt{2^n}$.

a) Prove that for any quantum state $|\psi\rangle$ on n qubits, $S(|\psi\rangle) \leq 2^{n/2}$. (Hint: use the Cauchy-Schwarz inequality, $\langle v|w\rangle \leq \|v\| \cdot \|w\|$.

Solution: First, we use the triangle inequality to conclude:

$$\sum_x |\alpha_x| \leq \left|\sum_x \alpha_x\right| = \left|\sum_x \langle x|\psi\rangle\right|$$

Then, we apply Cauchy-Schwarz on the right hand side:

$$\left|\sum_x \langle x|\psi\rangle\right| \leq \left|\sum_x \|x\| \cdot \|\psi\|\right|$$

We know that $\|\psi\| = 1$, and since there are 2^n states, then we can write:

$$\sum_x |\alpha_x| \leq \sqrt{2^n} = 2^{n/2}$$

as desired. □

---

b) Suppose that $|\alpha_x| \leq a$ for all x. Prove that $S(|\psi\rangle) \geq \frac{1}{a}$. (Hint: think about normalization...)

Solution: Firstly, it's simpler to prove that $aS(|\psi\rangle) \geq 1$. This means we want to show:

$$aS(|\psi\rangle) = a\sum_x |\alpha_x| = \sum_x a|\alpha_x| \geq 1$$

Now, notice that from the normalization condition, we have:

$$\sum_x |\alpha_x|^2 \leq \sum_x a \cdot |\alpha_x| \leq \sum_x a^2$$

The first half of this equation is what we want, since $\sum_x |\alpha_x|^2 = 1$, so we have:

$$1 \leq \sum_x a \cdot |\alpha_x| = aS(|\psi\rangle)$$

as desired. □

---

c) Argue that $H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x\cdot y} |y\rangle$ ($x \cdot y \equiv \sum_{i=1}^n x_i y_i$). (Hint: you can use results from previous homeworks.)

Solution: We did this exact problem on the previous homework, so I'm going to copy-paste my solution from there:

First, consider the Hadamard on one qubit:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Now, consider acting H on an arbitrary state $|x\rangle$:

$$H|x\rangle = \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

Writing it more suggestively to match the desired form:

$$H|x\rangle = \frac{(-1)^{0\cdot x}|0\rangle + (-1)^{1\cdot x}|1\rangle}{\sqrt{2}}$$

So, we can write it as follows:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$$

as desired. $\square$

---

d) Using c), the action of $H^{\otimes n}$ on $|\psi\rangle$ can be written as $H^{\otimes n}|\psi\rangle = \sum_x \beta_x |x\rangle$, where $\beta_x = \frac{1}{2^{n/2}} \sum_y (-1)^{x\cdot y} \alpha_y$.

Use this to prove that for all y, $|\beta_y| \le \frac{1}{2^{n/2}} S(|\psi\rangle)$. (Hint: use the triangle inequality.)

Solution: We want to show:

$$|\beta_y| = \left| \frac{1}{\sqrt{2^n}} \sum_x (-1)^{x\cdot y} \alpha_x \right| \le \frac{1}{\sqrt{2^n}} S(|\psi\rangle)$$

Therefore, cancelling out the prefactors, we basically want to show:

$$\left| \sum_x (-1)^{x\cdot y} \alpha_x \right| \le \sum_x |\alpha_x|$$

But this sum is immediately true due to the triangle inequality, which says that $|a+b| \le |a| + |b|$, exactly what we have here. $\square$

---

e) Prove the uncertainty relation $S(|\psi\rangle) S(H^{\otimes n}|\psi\rangle) \ge 2^{n/2}$. Justify why it makes sense to call this an uncertianty relation.

Solution: Here, we leverage part (b) for this problem. In the earlier part, we proved that all the coefficients of $H^{\otimes n}|\psi\rangle$ are less than $\frac{1}{2^{n/2}} S(|\psi\rangle)$. From part (b), we know that if we have an upper bound on the coefficients, then that gives us a lower bound on the spread of $|\psi\rangle$. Therefore:

$$S(H^{\otimes n}|\psi\rangle) \ge \frac{1}{\frac{1}{2^{n/2}} S(|\psi\rangle)}$$

$$\therefore S(H^{\otimes n}|\psi\rangle) \cdot S(|\psi\rangle) \ge 2^{n/2}$$

as desired. $\square$
