2.111J/18.435J Quantum Computation Problem Set 5 Solutions
(Due: Tuesday, October 25, 2005)

1) Consider the quantum phase estimation algorithm for an operator U when the algorithm's input is a particular eigenvector of U. Let $|\psi_\theta\rangle$ denote the eigenvector and let $e^{i\theta}$ denote its eigenvalue. At the end of the algorithm, right before measurement, the computer's state will be:

$$|\psi\rangle_{output} = \frac{1}{2^n}\sum_{k=0}^{2^n-1}\left(\sum_{j=0}^{2^n-1} e^{-2\pi ij\left(\frac{k}{2^n}-\frac{\theta}{2\pi}\right)}\right)|k\rangle \otimes |\psi_\theta\rangle$$

where $|k\rangle$ denotes the state of the n-qubit register that contains the eigenvalue estimate. Explicitly evaluate the geometric sum over j appearing in parentheses to make quantitative the following statement:

With very high probability, measurement of the n-qubit register will yield only those integers k such that $2\pi k/2^n \approx \theta$.

Solution: Let $b = b_1 b_2 \ldots b_n$ be the n-bit string giving the best binary fraction approximation $\frac{b}{2^n} = 0.b_1 b_2 \ldots b_n$ to $\frac{\theta}{2\pi} \in [0, 1)$. In other words, $\frac{\theta}{2\pi}$ rounded to the nearest n-bit binary fraction is $\frac{b}{2^n}$, and thus

$$\frac{b}{2^n} = \frac{\theta}{2\pi} + \delta \text{ where } |\delta| \leq \frac{1}{2^{n+1}}$$

Plugging this expression for $\frac{\theta}{2\pi}$ into $|\psi\rangle_{output}$ yields

$$|\psi\rangle_{output} = \frac{1}{2^n}\sum_{k=0}^{2^n-1}\left(\sum_{j=0}^{2^n-1} e^{-2\pi ij\left(\frac{k-b}{2^n}+\delta\right)}\right)|k\rangle \otimes |\psi_\theta\rangle$$

The magnitude squared of the scalar in front of $|k\rangle \otimes |\psi_\theta\rangle)$ gives the probability the algorithm outputs $\frac{k}{2^n}$ as its n-bit binary fraction approximation to $\frac{\theta}{2\pi}$.

$$\text{Prob}(k) = \left|\frac{1}{2^n}\left(\sum_{j=0}^{2^n-1} e^{-2\pi ij\left(\frac{k-b}{2^n}+\delta\right)}\right)\right|^2$$

Recalling the formula for summing geometric series

$$\sum_{x=0}^{M} z^x = \frac{1-z^{M+1}}{1-z}$$

and noting that in this case $z = e^{-2\pi i\left(\frac{k-b}{2^n}+\delta\right)}$ and $M + 1 = 2^n$, we find

$$\text{Prob}(k) = \frac{1}{2^{2n}}\left|\frac{1-e^{-2\pi i(k-b+2^n\delta)}}{1-e^{-2\pi i\left(\frac{k-b}{2^n}+\delta\right)}}\right|^2$$

As for analytically evaluating this formula, let us satisfy ourselves with an analytical argument that $\text{Prob}(k = b)$, the probability of obtaining the best possible n-bit approximation with just one run of the algorithm, is quite high just by itself (at least 40.5%, in fact).

From our formula on the last page,

$$\text{Prob}(k = b) = \frac{1}{2^{2n}} \left| \frac{1 - e^{-2\pi i 2^n \delta}}{1 - e^{-2\pi i \delta}} \right|^2$$

We lower bound this expression for $\text{Prob}(k = b)$ by lower bounding the numerator and upper bounding the denominator. We get the needed bounds from simple geometric arguments based on the fact e^{-iz} can be represented as a point $(\cos z, -\sin z)$ on the unit circle. First, we invoke the simple fact that the length of the straight line connecting the points $e^{i0} = (1, 0)$ and $e^{-iz} = (\cos z, -\sin z)$ of the unit circle is never longer than the length of the arc between them on the unit circle itself. Thus, we have the bound

$$|1 - e^{-iz}| \leq |z| \text{ with equality only when } z = 0.$$

Second, the straight line connecting the points $e^{i0} = (1, 0)$ and $e^{-iz} = (\cos z, -\sin z)$ of the unit circle is at least as long as the projection of that line onto the circle's diameter. If $0 \leq z \leq \pi$, then we may express the length of this projection onto the diameter as $\frac{2|z|}{\pi}$, that is, the length of the diameter—2 for the unit circle—multiplied by ratio of the arc length $|z|$ to the total arc length π of the unit half-circle. Thus, we have the bound,

$$\text{If } 0 \leq z \leq \pi, \text{ then } |1 - e^{-iz}| \geq \frac{2|z|}{\pi} \text{ with equality only when } z = 0 \text{ or } \pi.$$

(Note that this bound applies to our numerator since $|\delta| \leq \frac{1}{2^{n+1}}$ and thus $2\pi 2^n |\delta| \leq \pi$.)

So, in conclusion,

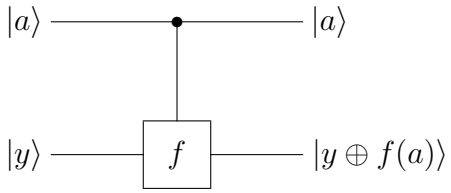
$$\text{Prob}(k = b) = \frac{1}{2^{2n}} \left| \frac{1 - e^{-2\pi i 2^n \delta}}{1 - e^{-2\pi i \delta}} \right|^2 \geq \frac{1}{2^{2n}} \left| \frac{\frac{2}{\pi}(2\pi 2^n \delta)}{2\pi\delta} \right|^2 = \frac{4}{\pi^2} = 0.40528\ldots$$

and therefore, as promised, a single run of the phase estimation algorithm using an n-qubit register for the eigenvalue produces the best possible n-bit binary fraction approximation to that eigenvalue at least 40.5% of the time.

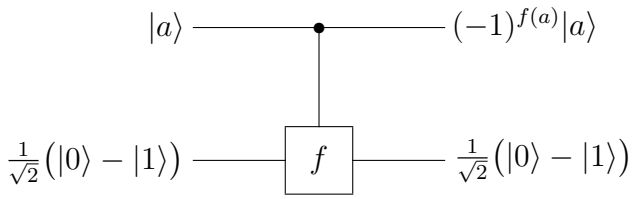
If you desire a more detailed analysis, then please see Nielsen and Chuang, Section 5.2.1.

---

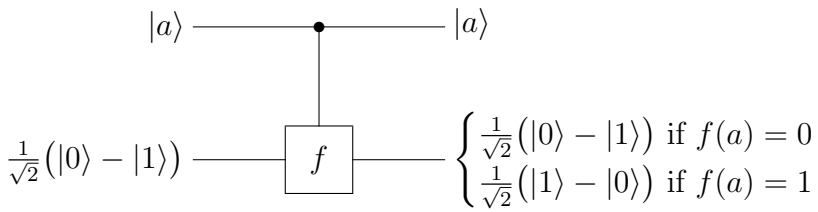
2) Verify that if one has a controlled-f gate,



then the following trick is valid:



Solution: By our definition of the controlled-f gate,



As we are free to write $|a\rangle \otimes [(-1)|y\rangle]$ as $[(-1)|a\rangle] \otimes |y\rangle$, we free to associate the $(-1)^{f(a)}$ phase factor obtained from the controlled-f with the $|a\rangle$ register rather than with the ancilla qubit in state $\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$ even though it is this ancilla qubit on which the controlled-f gate acts.

---

3) Let $H^{\otimes n}$ denote Hadamard gates applied individually to n qubits. Let $P = 2|0\rangle\langle 0| - I$ where I denotes the identity on n qubits and $|0\rangle\langle 0|$ denotes the projector onto the n-qubit state $\otimes_{i=1}^{n}|0\rangle_i$. Prove that

$$H^{\otimes n} P H^{\otimes n} = 2|\psi_u\rangle\langle\psi_u| - I$$

where $|\psi_u\rangle = \dfrac{1}{2^{n/2}} \displaystyle\sum_{j=0}^{2^n-1} |j\rangle$, the uniform superposition over the computational basis states.

Solution: Recall that $H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Thus, we have the trio of facts:

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big); \quad H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big); \quad HH^\dagger = I$$

Since $H^{\otimes n}$ denotes Hadamard gates applied individually to each of the n qubits, it immediately follows that

$$H^{\otimes n} P H^{\otimes n} \equiv 2H^{\otimes n}|0\rangle\langle 0|(H^{\otimes n})^\dagger - H^{\otimes n} I (H^{\otimes n})^\dagger = 2|\psi_u\rangle\langle\psi_u| - I.$$

---

4) Let O be the oracle operator for the unsorted search problem with a single search target $|w\rangle$ among N possibilities, That is, let $O = I - 2|w\rangle\langle w|$. Additionally, let $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{a \neq w} |a\rangle$

denote the uniform superposition over all the possibilities other than the search target. Define $H^{\otimes n}$ and P as in Problem 3. Finally, let $G = OH^{\otimes n}PH^{\otimes n}$ be the Grover operator. Prove that

$$G = \cos\theta\big(|w\rangle\langle w| + |r\rangle\langle r|\big) - \sin\theta\big(|w\rangle\langle r| - |r\rangle\langle w|\big) = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$$

where $\cos\theta = 1 - \dfrac{2}{N}$.

Solution: Using the result of Problem 3 for $H^{\otimes n}PH^{\otimes n}$ and the above definition of O, we expand the Grover operator as

$$\begin{aligned} G &= OH^{\otimes n}PH^{\otimes n} \\ &= \big(I - 2|w\rangle\langle w|\big)\big(2|\psi_u\rangle\langle\psi_u| - I\big) \\ &= 2|\psi_u\rangle\langle\psi_u| - I - 4|w\rangle\langle w|\psi_u\rangle\langle\psi_u| + 2|w\rangle\langle w| \end{aligned}$$

At this point, let us simply invoke without proof the result we shall prove in Problem 6,

$$|\psi_u\rangle = \sqrt{\frac{1}{N}}\,|w\rangle + \sqrt{1 - \frac{1}{N}}\,|r\rangle.$$

Plugging this result into our explicit expansion of the Grover operator along with the simple fact $I = |w\rangle\langle w| + |r\rangle\langle r|$ yields

$$\begin{aligned} G &= 2\left[\frac{1}{N}|w\rangle\langle w| + \frac{\sqrt{N-1}}{N}\big(|w\rangle\langle r| + |r\rangle\langle w|\big) + \frac{N-1}{N}|r\rangle\langle r|\right] - |w\rangle\langle w| \\ &\quad - |r\rangle\langle r| - 4|w\rangle\left(\sqrt{\frac{1}{N}}\right)\left(\sqrt{\frac{1}{N}}\,\langle w| + \sqrt{\frac{N-1}{N}}\,\langle r|\right) + 2|w\rangle\langle w| \\ &= \left(1 - \frac{2}{N}\right)\big(|w\rangle\langle w| + |r\rangle\langle r|\big) + \frac{2\sqrt{N-1}}{N}\big(|r\rangle\langle w| - |w\rangle\langle r|\big) \end{aligned}$$

Defining $\cos\theta = 1 - \dfrac{2}{N}$ and using $\sin\theta = \sqrt{1 - \cos^2\theta}$ then establishes the expression for G.

---

5) Verify that

$$GG\ldots G = \begin{pmatrix}\cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta\end{pmatrix}$$

where $GG\ldots G$ denotes the product of k Grover operators G, defined as in Problem 4.

Solution: This result follows immediately from the fact

$$\begin{aligned} \begin{pmatrix}\cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}\cos\beta & -\sin\beta \\ \sin\beta & \cos\beta\end{pmatrix} &= \begin{pmatrix}\cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \cos\alpha\sin\beta + \sin\alpha\cos\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta\end{pmatrix} \\ &= \begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix} \end{aligned}$$

6) Referring to the definitions of Problems 3 and 4, verify that

$$|\psi_u\rangle = \sqrt{\frac{1}{N}}\,|w\rangle + \sqrt{1-\frac{1}{N}}\,|r\rangle = \begin{pmatrix} \sqrt{\frac{1}{N}} \\ \sqrt{1-\frac{1}{N}} \end{pmatrix}.$$

Solution: By definition, $|\psi_u\rangle$ is the normalized uniform superposition over all computational basis states

$$|\psi_u\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^n-1} |j\rangle,$$

and by definition $|r\rangle$ is the normalized uniform superposition over all computational basis states *except* the search target $|w\rangle$

$$|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{j\in\{0,\ldots,2^n-1\}-\{w\}} |j\rangle.$$

The desired result immediately follows.