CSC518 **HW #3**
NAME: Alexander Jansing and Brittany Zeo **November 19, 2015**

Problem 1 Simon's Algorithm: 28 pts

Suppose we run Simon's algorithm on the following input x (with $N = 8$ and hence $n = 3$): We have

$$x_{000} = x_{111} = 000 \quad x_{001} = x_{110} = 001$$
$$x_{010} = x_{101} = 010 \quad x_{011} = x_{100} = 011$$

Note that x is 2-to-1 and $x_i = x_{i \oplus 111}$ for all $i \in \{0,1\}^3$, so $s = 111$.

a Give the starting state of Simon's algorithm.

$$\begin{aligned} U_f\big|x\big\rangle\big|0\big\rangle^{\otimes n} &= \big|x\big\rangle\big|0 \oplus f(x)\big\rangle \\ \otimes_{l=0}^{n}\big|0\big\rangle &= \otimes_{l=0}^{3}\big|0\big\rangle \end{aligned}$$

b Give the state after the first Hadamard transforms on the first 3 qubits.

$$\begin{aligned} H^{\otimes n}\big|x\big\rangle &= \tfrac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}\big|z\big\rangle, \\ H^{\otimes 3}\big|x\big\rangle &= \tfrac{1}{\sqrt{8}} \sum_{z\in\{0,1\}^3} (-1)^{x\cdot z}\big|z\big\rangle \otimes \big|0\big\rangle. \end{aligned}$$

c Give the state after applying the oracle.

$$\tfrac{1}{\sqrt{2^{n-1}}} \sum_{x\in 1} \tfrac{1}{\sqrt{2}}(\big|x\big\rangle + \big|x \oplus s\big\rangle)\big|f(x)\big\rangle$$
$$\tfrac{1}{2} \sum_{x\in 1} \tfrac{1}{\sqrt{2}}(\big|x\big\rangle + \big|x \oplus s\big\rangle)\big|f(x)\big\rangle$$

d Give the state after measuring the second register (the measurement gave $\big|001\big\rangle$). Measurement collapses the state and since the measurement gave $\big|001\big\rangle$, it is also the state; normalizing to 1.

e Use $H^{\otimes n}\big|i\big\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\cdot j}\big|j\big\rangle$ to give the state after the final Hadamard.
$H^{\otimes n}\big|i\big\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\cdot j}\big|j\big\rangle$
$H^{\otimes n}(\frac{1}{\sqrt{2}}\left[\big|000...0\big\rangle + \big|s\big\rangle\right]) = \frac{1}{\sqrt{2^{n+1}}} \sum_{j\in\{0,1\}^n} (2)\big|j\big\rangle$
$\frac{1}{\sqrt{2^n)}} \sum_{j\in s^\perp} \big|j\big\rangle$

f Why does measurement of the first 3 qubits of the final state give the information about s?
Because the bits in the first register are in a superpositioned state and as they pass through U_f they output the state that is the `XOR` of the second register and s.

g Suppose the first run of the algorithm give $j = 011$ and the second run gives $j = 101$. Show that, assuming $s \neq 000$, those two runs already determine s.

Problem 2 Fourier Transform: 30 pts

a For $\omega = e^{\frac{2\pi i}{3}}$ and $F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$, calculated $F_3 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $F_3 \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix}$.

- $F_3 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}$
- $F_3 \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega + \omega^2 + 1 \\ 2\omega^3 + 1 \\ \omega^2 + \omega^4 + 1 \end{pmatrix}$

b Let the Fourier transform defined as what we described in class, *i.e.* $\omega = e^{\frac{2\pi i}{N}}$ and entry at location (i, j) is $e^{\frac{2\pi ijk}{N}}$ where $0 \leq j, k < N$. Let $\left|C_k\right\rangle$ be the k^{th} column of F_N. Please show that

$$\left\langle C'_k \middle| C_k \right\rangle = \begin{cases} 1 \text{ if } k = k' \\ 0 \text{ if } k \neq k' \end{cases}$$

A Fourier transform square matrix of size N can be seen as such,

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & \cdots & \cdots & 1 \\ 1 & \omega & \omega^{1*2} & \ddots & & & \omega^{1*(N-1)} \\ 1 & \omega^{2*1} & \omega^{2*2} & & \ddots & & \omega^{2*(N-1)} \\ \vdots & \vdots & \vdots & & & \ddots & \vdots \\ 1 & \omega^{(N-1)*1} & & & \cdots & & \omega^{(N-1)*(N-1)} \end{pmatrix}$$

We know that QFT matrices are *unitary* and therefore the column vectors are linearly independent. Therefore each column vector is "parallel" to itself, and its $\left\langle C'_k \middle| C_k \right\rangle = 1$, and is orthogonal to the other column vectors in N-space, so $\left\langle C'_k \middle| C_k \right\rangle = 0$.

c Prove the identity in equation 7.1.18 in the textbook.
Identity 7.1.18 states, for some binary $w = 0.x_1x_2\cdots$

Is it a typo in the book when it says, "$\sum_{y=0}^{2^n-1}$?" Shouldn't it be $\sum_{y=0}^{2^{n-1}}$?

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}} e^{2\pi iwy}\big|y\big\rangle = \left(\frac{\big|0\big\rangle+e^{2\pi i(2^{n-1}w)}\big|1\big\rangle}{\sqrt{2}}\right)\otimes\left(\frac{\big|0\big\rangle+e^{2\pi i(2^{n-2}w)}\big|1\big\rangle}{\sqrt{2}}\right)\otimes\cdots$$
$$\cdots\otimes\left(\frac{\big|0\big\rangle+e^{2\pi i(w)}\big|1\big\rangle}{\sqrt{2}}\right).$$

So, we know in a general case from the notes,

$$\begin{aligned}
\mu^{2^0}\big|\psi\big\rangle &= e^{2\pi i(w)} &= e^{2\pi i(0.x_1x_2\cdots)} &= \left(\frac{\big|0\big\rangle+e^{2\pi i(0.x_1x_2\cdots)}\big|1\big\rangle}{\sqrt{2}}\right)\\
\mu^{2^1}\big|\psi\big\rangle &= e^{2\pi i(2^1w)} &= e^{2\pi i(x_1.x_2x_3\cdots)} &= \left(\frac{\big|0\big\rangle+e^{2\pi i(0.x_2x_3\cdots)}\big|1\big\rangle}{\sqrt{2}}\right)\\
&\vdots\\
\mu^{2^{n-1}}\big|\psi\big\rangle &= e^{2\pi i(2^{n-1}w)} &= e^{2\pi i(x_1\cdots x_{n-1}.x_n)} &= \left(\frac{\big|0\big\rangle+e^{2\pi i(0.x_n)}\big|1\big\rangle}{\sqrt{2}}\right)
\end{aligned}$$

So $\sum_{y=0}^{2^{n-1}} e^{2\pi iwy}\big|y\big\rangle = \left(\frac{\big|0\big\rangle+e^{2\pi i(2^{n-1}w)}\big|1\big\rangle}{\sqrt{2}}\right)\otimes\left(\frac{\big|0\big\rangle+e^{2\pi i(2^{n-2}w)}\big|1\big\rangle}{\sqrt{2}}\right)\otimes\cdots\otimes\left(\frac{\big|0\big\rangle+e^{2\pi i(w)}\big|1\big\rangle}{\sqrt{2}}\right)$
easily follows.

Problem 3 Euclidean distance: 12 pts

The Euclidean distance between two states $\big|\phi\big\rangle = \sum_i \alpha_i\big|i\big\rangle$ and $\big|\psi\big\rangle = \sum_i \beta_i\big|i\big\rangle$ and $\big|\big|\big|\phi\big\rangle - \big|\psi\big\rangle\big|\big| = \sqrt{\sum_i |\alpha_i - \beta_i|^2}$. Assume the states are unit vectors with real amplitudes. Suppose the distance is small: $\big|\big|\big|\phi\big\rangle - \big|\psi\big\rangle\big|\big| = \epsilon$. Show that the probabilities resulting from a measurement on the two states are also close: $\sqrt{\sum_i |\alpha_i^2 - \beta_i^2|} \le 2\epsilon$ (Hint: use *Cauchy-Schwarz* inequality).

$$\begin{aligned}
\sqrt{\textstyle\sum_i |\alpha_i - \beta_i|^2} &\le \sqrt{\textstyle\sum_i |\alpha_i^2 - \beta_i^2|^2}\\
\sqrt{\textstyle\sum_i |\alpha_i^2 - \beta_i^2|^2} &= \sqrt{\textstyle\sum_i \left(|\alpha_i - \beta_i| * |\alpha_i + \beta_i|\right)^2}\\
\sqrt{\textstyle\sum_i \left(|\alpha_i - \beta_i| * |\alpha_i + \beta_i|\right)^2} &\le \sqrt{\textstyle\sum_i |\alpha_i - \beta_i|^2 * \sum_i |\alpha_i + \beta_i|^2}\\
\cdots & \quad \sqrt{\epsilon^2 * \textstyle\sum_i |\alpha_i + \beta_i|^2}\\
\sqrt{\epsilon^2 * \textstyle\sum_i |\alpha_i + \beta_i|^2} &= \epsilon\sqrt{\textstyle\sum_i |\alpha_i + \beta_i|^2}\\
\epsilon\sqrt{\textstyle\sum_i |\alpha_i + \beta_i|^2} &\le \epsilon * \left(\textstyle\sum_i |\alpha_i|^2 + \sum_i |\beta_i|^2\right)\\
\epsilon * \left(\textstyle\sum_i |\alpha_i|^2 + \sum_i |\beta_i|^2\right) &= \epsilon * 2
\end{aligned}$$

Problem 4 Analysis Technique Proof: 10 pts

In quantum counting or the hard case analysis of Shors algorithm, the following analysis technique is commonly used: $\left|1-e^{i\theta}\right| = 2\left|\sin(\frac{\theta}{2})\right|$ Please prove this equality.

$$
\begin{array}{rcll}
\left|1-e^{i\theta}\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
|1-(\cos(\theta)+i\sin(\theta))| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
|1-\cos(\theta)-i\sin(\theta))| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
\left|1-\cos\left(\frac{2\theta}{2}\right)-i\sin\left(\frac{2\theta}{2}\right)\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
\left|1-1+2\sin^2\left(\frac{\theta}{2}\right)-2i\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
2\left|\sin\left(\frac{\theta}{2}\right)\right|\left|\sin\left(\frac{\theta}{2}\right)-i\cos\left(\frac{\theta}{2}\right)\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
2\left|\sin\left(\frac{\theta}{2}\right)\right|\left|\cos\left(\frac{\pi}{2}-\theta\right)-i\sin\left(\frac{\pi}{2}-\theta\right)\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
2\left|\sin\left(\frac{\theta}{2}\right)\right|\left|e^{-i\left(\frac{\pi}{2}-\theta\right)}\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
2\left|\sin\left(\frac{\theta}{2}\right)\right|1 & = & 2\left|\sin(\frac{\theta}{2})\right| & \\
2\left|\sin\left(\frac{\theta}{2}\right)\right| & = & 2\left|\sin(\frac{\theta}{2})\right| & \checkmark
\end{array}
$$

Problem 5 Root of Unity: 10 pts

Prove that if a operator U satisfies $U^r = I$, then the eigenvalues of U must be r^{th} roots of 1.
If U was unitary, then $U^1\left|\psi\right\rangle = \lambda\left|\psi\right\rangle$ and since U would be unitary λ (the eigenvalue(s) of similar $1's$ we're looking for) would have a magnitude of 1, so $\lambda = e^{2\pi i\phi}$ where $\phi \in [0,1)$.

$$\vdots$$

Now if U is r-nary, then $U^r\left|\psi\right\rangle = \lambda\left|\psi\right\rangle$ and since U would be r-nary λ would have a magnitude of r, so $\lambda = e^{2\pi i\phi}$ where $\phi \in [0,r)$; for some $r \in \mathbb{Z}$ and $\phi \in \mathbb{R}$.

Problem 6 Gate Approximation: 10 pts

As mentioned in class that the implementation of QFT inverse will be difficult if the precision requirement is high for the control rotation gates. Based on the Solovay-Kitaevs decomposition theorem, there is always a way to approximate a single qubit gate with error at most using $O(log^c \frac{1}{\epsilon})$ gates from the universal gate where the optimal c is some number slightly less than 2. Please describe (sketch) the proof of this theorem.
This we're both unsure of how to begin without just copying the material from here within the time we have; and already being late with this. So I will reference material from here and admit that I'd look here for at someone who has gone through the work to prove the theorem.

URL for paper version: http://home.lu.lv/ sd20008/papers/essays/Solovay-Kitaev.pdf