CSC518 **HW #3**
NAME: Alexander Jansing and Brittany Zeo **December 14, 2015**

Problem 1 Euclidean Algorithm: 15 pts

Let $a, b \in \mathbb{Z}^+$ (we're ignoring the negative integers, because they could result in thte same gcd and ignoring 0 because the gcd in all cases would be 0),

By the Division Algorithm $a = b(q_1) + r_1$, where b goes into a q_1 times with a remainder r_1 and both $q_1, r_1 \in \mathbb{Z}^+$ and $r < b$.

This repeats now for finding $\gcd(b, r_1)$ and we get $b = r_1(q_2)+r_2$, where $q_2, r_2 \in \mathbb{Z}^+$ and $r_2 < r_1$.

$$\vdots$$

This repeats now for finding $\gcd(r_{n-2}, r_{n-1})$ and we get $r_{n-2} = r_{n-1}(q_n) + r_n$, where $q_n, r_n \in \mathbb{Z}^+$ and $r_n = 0$.

Since $r_n = 0$, $r_{n-1} = \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-4}, r_{n-3}) = \cdots = \gcd(a, b)$.

Problem 2 Shor's Algorithm: 5 + 15 + 10 + 5 pts

a.) N is of the order $2^n \approx N$, so we set $n = \lceil \log_2 N \rceil$ as to not lose any data.

b.) $N^2 < q = 2^l \leq 2N^2$ is required because we need to be able to break the quantum register into two registers. You need l inputs and $q = 2^l$. We need to find a power of 2 value for q such that the first register has enough qubits to represent $q - 1$ in binary (covering all the values that could possibly be divisors of N).

If we wrote q as strictly between N and $2N$ (or even between N and N^2) then q could lack the scope needed to find all possible divisors.

c.) Find the period, showing all intermediate steps.

$l^x \mod 10$

$7^x \mod 10$

$$|\psi_1\rangle = \frac{1}{\sqrt{128}} \sum_{x=0}^{127} |x\rangle|0\rangle^{\otimes n} = \frac{1}{\sqrt{128}} \sum_{x=0}^{127} |x\rangle|0000\rangle$$

$$n = \lceil \log_2 10 \rceil = 4$$

$$|\psi_2\rangle = \frac{1}{\sqrt{128}} \sum_{x=0}^{127} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{128}} \begin{pmatrix} |0\rangle|f(0)\rangle + \\ |1\rangle|f(1)\rangle + \\ |2\rangle|f(2)\rangle + \cdots \\ \cdots + |127\rangle|f(127)\rangle \end{pmatrix}$$

$m = \lfloor \frac{q}{r} \rfloor$

$$\begin{aligned} f(0) &= 7^0 \equiv 1 \mod 10 \\ f(1) &= 7^1 \equiv 7 \mod 10 \\ f(2) &= 7^2 \equiv 9 \mod 10 \\ f(3) &= 7^3 \equiv 3 \mod 10 \\ \text{-----} &\quad \text{----------} \quad \text{----------} \\ f(4) &= 7^4 \equiv 1 \mod 10 \\ f(5) &= 7^5 \equiv 7 \mod 10 \\ &\vdots \quad\quad \vdots \quad\quad \vdots \end{aligned}$$

Period is 4.

d.) In the second case, the algorithm's complexity is to be blamed on the recursive nature of continued functions and how by definition may not terminate. And after so many layers of recursion, data needs to be stored somewhere to guarantee there is no loss of data.

Problem 3 Grover's Algorithm: 15 + 5 + 5 + 5 pts

a.)

$$G = \begin{array}{c} \\ \end{array} \begin{array}{c} \begin{array}{cc} \big|G\big\rangle & \big|B\big\rangle \end{array} \\ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{array}$$

N = size space
M = number of solutions,

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}.$$

$$\text{Then, } \sin^2\theta = \frac{4M(N-M)}{N^2}.$$

$$\cos^2\theta + \sin^2\theta = 1.$$

$$\text{So, } \cos^2\theta = 1 - \frac{4M(N-M)}{N^2},$$

$$\text{and } \cos\theta = \sqrt{1 - \frac{4M(N-M)}{N^2}}.$$

So now we can rewrite G and bind it between
the minimums and maximums ($0 < \theta < \frac{\pi}{2}$):

$$\begin{array}{ccccc} min & \leq & G & \leq & max \\ \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} & \leq & \begin{pmatrix} \sqrt{1-\frac{4M(N-M)}{N^2}} & -\frac{2\sqrt{M(N-M)}}{N} \\ \frac{2\sqrt{M(N-M)}}{N} & \sqrt{1-\frac{4M(N-M)}{N^2}} \end{pmatrix} & \leq & \begin{pmatrix} \cos\frac{\pi}{2} & -\sin\frac{\pi}{2} \\ \sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \leq & \begin{pmatrix} \sqrt{1-\frac{4M(N-M)}{N^2}} & -\frac{2\sqrt{M(N-M)}}{N} \\ \frac{2\sqrt{M(N-M)}}{N} & \sqrt{1-\frac{4M(N-M)}{N^2}} \end{pmatrix} & \leq & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \end{array}$$

And if $M \leq \frac{N}{2}$, then $0 \leq M \leq \frac{N}{2}$:

$$M := 0; \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$M := \tfrac{N}{2}; \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} \sqrt{1-\frac{4\frac{N}{2}(N-\frac{N}{2})}{N^2}} & -\frac{2\sqrt{\frac{N}{2}(N-\frac{N}{2})}}{N} \\ \frac{2\sqrt{\frac{N}{2}(N-\frac{N}{2})}}{N} & \sqrt{1-\frac{4\frac{N}{2}(N-\frac{N}{2})}{N^2}} \end{pmatrix} \leq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$M := \tfrac{N}{2}; \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} \sqrt{1-\frac{2N(\frac{N}{2})}{N^2}} & -\frac{2\sqrt{\frac{N}{2}(\frac{N}{2})}}{N} \\ \frac{2\sqrt{\frac{N}{2}(\frac{N}{2})}}{N} & \sqrt{1-\frac{2N(\frac{N}{2})}{N^2}} \end{pmatrix} \leq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$M := \tfrac{N}{2};\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ \leq\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ \leq\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

b.) 1.) We were unsure how to solve this without the direct method in the notes. Classically requires $\frac{N}{t}$ calls.

Quantumly, there is a quadratic speed up, so there need to be

$$\sqrt{\frac{N}{t}} = \sqrt{\frac{2^{10}}{2^2}} = \sqrt{2^8} = 2^4 = 32 \text{ calls.}$$

2.) will do easily for $N = 100$, $M = 4$:

$$\begin{pmatrix} \sqrt{1 - \frac{16(96)}{10000}} - \lambda & -\frac{2\sqrt{4(96)}}{100} \\ \frac{2\sqrt{4(96)}}{100} & \sqrt{1 - \frac{4M(N-M)}{10000}} - \lambda \end{pmatrix}$$

$$\begin{aligned} p(\lambda) &= det \begin{pmatrix} \sqrt{1 - \frac{16(96)}{10000}} - \lambda & -\frac{2\sqrt{4(96)}}{100} \\ \frac{2\sqrt{4(96)}}{100} & \sqrt{1 - \frac{16(96)}{10000}} - \lambda \end{pmatrix} \\ &= (.92 - \lambda)^2 + (.3919)(-.3919) \\ 0 &= (.92 - \lambda)^2 + (.3919)(-.3919) \\ \lambda &= .92 \pm .3919i \end{aligned}$$

3.) $\frac{4*32}{1024} = \frac{128}{1024} = \frac{2^7}{2^10} = \frac{1}{8}$

Problem 4 Quantum Phase Estimation (QPE): 15+ 5 pts

a.)

$$\begin{gathered} |k_1\rangle - H - R_1 - R_3 - - - - \\ |k_2\rangle - - - - - | - - | - HR_2 - - \\ |k_3\rangle - - - - - - - - | - - - | - H - \end{gathered}$$

$$U|\psi\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_1x_2x_3)}|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_2x_3)}|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_3)}|1\rangle)$$

$$\begin{gathered} |0\rangle - H - R_1 - R_3 - - - - \\ |0\rangle - - - - - | - - | - HR_2 - - \\ |0\rangle - - - - - - - - | - - - | - H - \end{gathered}$$

$$U|\psi\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.000)}|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.00)}|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.0)}|1\rangle)$$

$$U|\psi\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

b.) Eigenvalues:

$$\begin{pmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos 0\theta - \lambda \end{pmatrix}$$

$0 = (\cos\theta - \lambda)^2 + (\sin\theta)(-\sin\theta) \rightarrow \lambda = \cos\theta \pm i\sin\theta.$

Eigenvectors: First with $\lambda = \cos\theta - i\sin\theta$,

$$\begin{pmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos\theta - \lambda \end{pmatrix} = \begin{pmatrix} \cos\theta - (\cos\theta - i\sin\theta) & -\sin\theta \\ \sin\theta & \cos\theta - (\cos\theta - i\sin\theta) \end{pmatrix}$$

$$= \begin{pmatrix} i\sin\theta & -\sin\theta \\ \sin\theta & i\sin\theta \end{pmatrix}$$

$$i\sin\theta v_1 - \sin\theta v_2 = 0 \sin\theta v_1 - i\sin\theta v_2 = 0$$

Let $v_2 = t$, then we have $i\sin\theta v_1 = \sin\theta t \Rightarrow v_1 = -it$ and $\sin\theta v_1 = i\sin\theta t \Rightarrow v_1 = it$, this gives us one eigenvector, $\begin{pmatrix} -i \\ i \end{pmatrix}$.

Similarly, $\lambda = \cos\theta - +i\sin\theta$,

$$\begin{pmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos\theta - \lambda \end{pmatrix} = \begin{pmatrix} \cos\theta - (\cos\theta + i\sin\theta) & -\sin\theta \\ \sin\theta & \cos\theta - (\cos\theta + i\sin\theta) \end{pmatrix}$$

$$= \begin{pmatrix} -i\sin\theta & -\sin\theta \\ \sin\theta & -i\sin\theta \end{pmatrix}$$

Let $v_2 = t$, then we have $-i\sin\theta v_1 = \sin\theta t \Rightarrow v_1 = it$ and $\sin\theta v_1 = i\sin\theta t \Rightarrow v_1 = it$, this gives us one eigenvector, $\begin{pmatrix} i \\ i \end{pmatrix}$.

Problem 5 Random Walk: +5 points

Given a symmetric matrix of all real entries, $g_{ij} \in \mathbb{R}, \forall i, j \in \{1, \cdots, n\}$:

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{12} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ g_{1n} & g_{2n} & \cdots & g_{nn} \end{pmatrix}$$

$G^* = G^T$, so $G^*G = G^2$ and therefore G is normal[1].

[1]It is also easy to show that one can perform Gaussian Elimination upon a symmetric matrix to reduce to an identity matrix.