Quantum Computing and Information - Problem Set 2 **Due Mon, Feb 7, 2011**

Exercise 1. **Constructing a Toffoli gate from CNOT and single-qubit gates** This exercise will prove that two-qubit unitary gates are universal. For a single-qubit unitary U, define the controlled-U operation to be $C_U := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$. Note that $\textsc{cnot} = C_X$. To indicate the systems that these gates act on we use the notation $[C_X]_{i,j}$ to mean a controlled-U operation where qubit i is the control and qubit j is the target.

a) Show that

$$[C_U]_{1,3}[C_X]_{2,1}[C_U^\dagger]_{13}[C_X]_{21}[C_U]_{23}$$

implements a doubly-controlled U^2: i.e. applies $[U^2]_3$ only if qubits 1 and 2 are both in the $|1\rangle$ state. Thus if $U = e^{i\varphi}\sqrt{X}$ for some φ then this implements gate that is related to the Toffoli gate.

b) Now we need to construct a controlled-$\sqrt{X}$ gate from CNOTs and single-qubit gates. Show that

$$[V]_3[C_X]_{1,3}[V^\dagger]_3[W]_3[C_X]_{1,3}[W^\dagger]_3 = [C_U]_{1,3},$$

where $U = VXV^\dagger WXW^\dagger$.

c) Find V, W such that $VXV^\dagger WXW^\dagger = e^{i\varphi}\sqrt{X}$ for some φ. (Part (d) of question 2 on problem set 1 may help here, although you will need to calculate $(\vec{v}\cdot\vec{\sigma})\cdot(\vec{w}\cdot\vec{\sigma})$ rather than the commutator.)

Exercise 2. **The hybrid argument** The *operator norm* is defined as follows. If M is a matrix, then define

$$\|M\| := \max |\langle\alpha| M |\beta\rangle|,$$

where the max is taken over all unit vectors $|\alpha\rangle$ and $|\beta\rangle$.

a) Show that the operator norm obeys the triangle inequality: $\|A+B\| \leq \|A\| + \|B\|$.

b) Show that the norm is right and left unitarily-invariant. That is, for any unitary U and any matrix M, $\|M\| = \|MU\| = \|UM\|$.

c) Suppose that we would like to perform a quantum circuit $U_{(T)} := U_1 U_2 \cdots U_T$ but only are able to apply each gate approximately. Thus, we instead perform $\tilde{U}_{(T)} := \tilde{U}_1 \cdots \tilde{U}_T$ for some unitaries $\tilde{U}_1, \ldots, \tilde{U}_T$ satisfying $\|U_i - \tilde{U}_i\| \leq \epsilon_i$ for $i = 1, \ldots, T$. Prove that $\|U_{(T)} - \tilde{U}_{(T)}\| \leq \epsilon_{(T)} := \sum_{i=1}^{T} \epsilon_i$.

Exercise 3. **A lazier Quantum Fourier Transform (QFT)**
When implementing the QFT, a lot of time is spent on $R_k = \exp(\frac{2\pi i|1\rangle\langle 1|}{2^k})$ rotations that, for large values of k, are very close to I. Suppose we replace R_k with the identity whenever $k \geq k_0$ for some cut-off value k_0.

a) The standard QFT uses $O(n^2)$ gates. Give an asymptotic estimate for the number of gates in the lazy QFT described here, noting that identity gates don't count.

b) Give an upper bound on the error in the resulting approximate QFT.

c) How many gates suffice to achieve an error that scales as $1/n^{100}$?

Exercise 4. **Phase estimation**

a) Suppose we start with the state

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

apply the conditional phase $\sum_{x=0}^{2^n-1} e^{2\pi i\varphi x}|x\rangle\langle x|$ and then the inverse QFT $\frac{1}{\sqrt{2^n}}\sum_{x,y=0}^{N-1} e^{-\frac{2\pi i xy}{N}} |x\rangle\langle y|$. Finally we measure the state in the computational basis and obtain outcome y. Calculate $\Pr[y]$.

b) Assume that $0 \leq \varphi \leq 1$. Define $\Delta := y/N - \varphi$ and $\delta = \min(|\Delta|, 1 - |\Delta|)$. This definition is meant to express the idea that δ is the error in the phase estimation procedure. Show that there exists a constant $c > 0$ such that

$$\Pr\left[\delta \geq \frac{k}{N}\right] \leq \frac{c}{k},$$

for any positive integer k. *Hint: For $\alpha \geq 0$, it may be helpful to use the bounds $\alpha - \alpha^3/6 \leq \sin\alpha \leq \alpha$.*

c) *Optional:* Now suppose we do the same procedure but replace the state in Eq. (1) with

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{x=0}^{2^n-1} \sin\frac{\pi(x+\frac{1}{2})}{2^n} |x\rangle . \tag{2}$$

Check that this state is normalized, calculate $\Pr[y]$ for this strategy, and show that it satisfies

$$\Pr\left[\delta \geq \frac{k}{N}\right] \leq \frac{c}{k^3},$$

for any positive integer k and for a possibly different constant c. Thus, while the width of this distribution cannot be substantially improved, the tails can be made to drop off faster. This question relates to the construction of optimal quantum clocks.

Exercise 5. **Collision detection**
Suppose we are given a black-box function $f : \{0,1\}^n \to \{0,1\}^{n-1}$ that is 2-to-1: i.e. exactly two inputs go to each output. Our goal is to find $x, y \in \{0,1\}^n$ such that $f(x) = f(y)$. However, unlike in Simon's algorithm, we now have no promise about any periodicity of f. As a result it turns out that quantum computers cannot achieve exponential speedups in this case. Define $N = 2^n$.

a) Give a classical algorithm that finds a collision with high probability ($\geq 1/2$) using only $O(\sqrt{N})$ queries to f.

b) Suppose now that only $O(N^{1/3}\log(N))$ bits of memory are available. (Note that $\log(N)$ bits can store one integer between 1 and N.) Now describe a classical algorithm that finds a collision with high probability that uses $O(N^{2/3})$ queries.

c) Give a quantum algorithm that finds a collision in $O(\sqrt{N})$ queries and uses $O(\log(N))$ space. *Hint: Use Grover's algorithm.*

d) Give a quantum algorithm that finds a collision in $O(M + \sqrt{N/M})$ queries and uses $O(M\log(N))$ space for any choice of M. Choosing $M = N^{1/3}$ will then yield a $\tilde{O}(N^{1/3})$-query algorithm, where $\tilde{O}$ neglects log factors. *Hint: combine parts (b) and (c).*

Exercise 6. *Optional, but recommended:* **Quantum counting**
We are given a black-box function $f : \{0,1\}^n \to \{0,1\}$ and would like to estimate $|f^{-1}(1)|$: that is, the number of $x \in \{0,1\}^n$ such that $f(x) = 1$. Let $M = |f^{-1}(1)|$ and $N = 2^n$.

a) Suppose we are given access to $U_f = \sum_{x\in\{0,1\}^n} \sum_{y\in\{0,1\}} |x\rangle\langle x| \otimes |y \oplus f(x)\rangle \langle y|$. We would like to use U_f to apply the phase $(-1)^{f(x)}$ conditioned on an additional qubit. This operation is defined as

$$V_f = I \otimes |0\rangle\langle 0| + \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x| \otimes |1\rangle\langle 1|.$$

Show how we can use U_f to implement V_f.

b) Define $|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N-1} |x\rangle$. Define the Grover iteration

$$G = (I - 2|s\rangle\langle s|) \cdot \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x|.$$

Find the eigenvalues of G.

c) Show how the construction of part (a) can be used to perform

$$\sum_{t=0}^{T-1} |t\rangle\langle t| \otimes G^t$$

using $T-1$ queries to U_f.

d) Assume that M divides N. Show that quantum phase estimation can be used to determine M/N up to accuracy $O(1/T)$ with high probability. How large does T have to be in order to have a $\geq 1/2$ probability of determining M exactly? How many queries are necessary to achieve this classically?