Introduction to Quantum Information Processing
Assignment 4
Due at 11:59pm on Friday March 8 2013 using the LEARN dropbox, or the dropbox located outside the tutorial centre, MC 4066, BOX 2, Slot 11 (please submit a confirmation of submission online in this case)
(will constitute 10% out of the 50% assignment marks)

1. Quantum searching **2 marks**

   (a) What is the smallest probability p for which quantum search via amplitude amplification finds a solution with certainty using two iterations of the quantum search iterate? Also give a three decimal approximation to p.

   Solution:

   Suppose we have an algorithm $A = \sin(\theta)|X_1\rangle + \cos(\theta)|X_0\rangle$, that finds a solution with probability $p = \sin^2(\theta)$.

   After 2 iterations of amplitude amplification, the resulting state will be $\sin(5\theta)|X_1\rangle + \cos(5\theta)|X_0\rangle$. In order to find a solution with certainty, we need $|\sin(5\theta)| = 1$, or in other words $5\theta = m\pi + \frac{\pi}{2}$, for some integer m. Thus $\theta = \frac{m}{5}\pi + \frac{\pi}{10}$ for some integer m. The value of θ (modulo 2π) such that $p = \sin^2\theta$ is minimum is $\theta = \frac{\pi}{10}$ (or $\theta = -\frac{\pi}{10}$ or $\theta = \pi \pm \frac{\pi}{10}$, which lead to the same p), and thus $p = \sin^2(\arcsin(\pi/10))$, which is roughly 0.099 (or $0.0986960440\ldots$).

   (b) Suppose we have a quantum algorithm A that produces a solution to $f(x) = 1$ with probability $\frac{1}{10000}$. What is the smallest positive integer k so that $k+1$ iterations of the quantum search iterate finds a solution with probability less than k iterations would?

   Solution:

   The probability of success is $p = \frac{1}{10000}$. We can let θ be the smallest positive value such that $p = \sin^2(\theta)$. Thus $\theta = \arcsin(\frac{1}{100}) = 0.010\ldots$.

   We know that after k iterations of the quantum search iteration, the amplitude of the solution states is $\sin((2k+1)\theta)$.

   Solving $(2k+1)\theta = \frac{\pi}{2}$ gives $k = 78.0385073\ldots$, which is not an integer. Up until $k = 78$, the value of $\sin^2((2k+1)\theta)$ will keep increasing, up to the value $\sin^2(157\theta) = \sin^2(157\arcsin(\frac{1}{100})) = 0.99999940\ldots$. For $k = 79$, the probability of finding a solution is $sin^2(159\theta) = \sin^2(159\arcsin(\frac{1}{100})) = 0.999630246\ldots$, and thus the probability of success is starting to decrease for $k = 79$.

   Thus the answer is $k = 78$.

2. Square-root of a unitary **3 marks**

   Let U be a unitary operation with eigenvalues ± 1. That is, $U^2 = I$.

   Let $U = P_0 - P_1$ be the spectral decomposition of U.

We have seen in previous work how to implement the eigenvalue estimation circuit (using one application of the controlled-U) that will map

$$|0\rangle|\psi\rangle \mapsto \alpha_+|0\rangle|\psi_+\rangle + \alpha_-|1\rangle|\psi_-\rangle$$

where $|\psi\rangle = \alpha_+|\psi_+\rangle + \alpha_-|\psi_-\rangle$ is an input state to U, the state $|\psi_+\rangle$ is a $+1$ eigenvector of U, and $|\psi_-\rangle$ is a -1 eigenvalue of U. In other words, $|\psi_+\rangle = P_0|\psi\rangle$ and $|\psi_-\rangle = P_1|\psi\rangle$.

Let $V = P_0 + iP_1$.

(a) Show that V is a square root of U. That is, $V^2 = U$.

Solution:

Let $V^2 = (P_0 + iP_1)(P_0 + iP_1) = P_0^2 + iP_0P_1 + iP_1P_0 - P_1^2 = P_0 - P_1 = U$ (since for projectors, we have $P_0^2 = P_0$ and $P_1^2 = P_1$, and for projectors onto orthogonal eigenspaces we have $P_0P_1 = 0 = P_1P_0$).

(b) State another square-root of U (that isn't equal to V up to global phases).

Solution:

Let $V' = P_0 - iP_1$ is another square-root of U.

(c) Show how to implement V using the controlled-U twice.

Solution:

If on input $|\psi\rangle = \alpha|\psi_+\rangle + \beta|\psi_-\rangle$ (where $U|\psi\rangle = |\psi_+\rangle$ and $U|\psi_-\rangle = -|\psi_-\rangle$), we first apply the eigenvalue estimation circuit for distinguishing eigenvalue $+1$ from -1, we will be left in the state $\alpha|0\rangle|\psi_+\rangle + \beta|1\rangle|\psi_-\rangle$.

If we apply the gate $T = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ on the control qubit, then we will have $\alpha|0\rangle|\psi_+\rangle + \beta i|1\rangle|\psi_-\rangle$.

If we apply the inverse of the eigenvalue estimation algorithm (which is the same as the eigenvalue estimation algorithm in this case), we will "uncompute" the eigenvalue information in the control qubit and be left in the state $|0\rangle(\alpha|\psi_+\rangle + \beta i|\psi_-\rangle)$.

In other words, the net effect of this circuit, with a one-qubit ancilla initialized to $|0\rangle$ is to effect the operation V (returning the ancilla qubit to the state $|0\rangle$).

3. Exact one-out-of-four searching **2 marks**

Let $f : \{0,1\}^n \mapsto \{0,1\}$. Suppose we wish to find a string $x \in \{0,1\}^n$ such that $f(x) = 1$. Suppose further that exactly one quarter of all the strings x in $\{0,1\}^n$ satisfy $f(x) = 1$.

Show how to find a string x with certainty using exactly one evaluation of the black-box $U_f : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$.

Solution:

Notice that $H^{\otimes n}|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ will give a solution with probability exactly $\frac{1}{4}$. In other words $H^{\otimes n}|00\ldots0\rangle = \frac{1}{2}|X_1\rangle + \frac{\sqrt{3}}{2}|X_0\rangle$, where $|X_1\rangle$ is a uniform superposition

of values x such that $f(x) = 1$ and $|X_0\rangle$ is a uniform superposition of values x such that $f(x) = 0$.

We can also express this as $H^{\otimes n}|00\ldots0\rangle = \sin(\frac{\pi}{6})|X_1\rangle + \cos(\frac{\pi}{6})|X_0\rangle$.

After one iteration of the quantum search iteration we have
$-H^{\otimes n}U_{00\ldots0}H^{\otimes n}U_f H^{\otimes n}|00\ldots0\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) = \sin(\frac{3\pi}{6})|X_1\rangle + \cos(\frac{3\pi}{6})|X_0\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) = \sin(\frac{\pi}{2})|X_1\rangle + \cos(\frac{\pi}{2})|X_0\rangle = |X_1\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$.

(We use the ancilla qubit initialized to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ in order to effect $|x\rangle \mapsto (-1)^{f(x)}|x\rangle$ on the first n qubits.)

Measuring the first n qubits will yield a solution to $f(x) = 1$ with certainty.

4. **2 marks**

   Show how to use quantum searching to exactly create the superposition

   $$\frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$$

   starting from $|0000\rangle$, using ancillas initialized to $|0\rangle$ (as needed), and using only Hadamard gates and reversible classical operations. You may assume you have classical reversible circuits for elementary arithmetic operations (you do not need to derive them).

   Solution:

   For $x \in \{0,1\}^4$, let us define $f(x) = 1$ if and only if the Hamming weight of x is 1 (i.e. there is exactly one 1 in x).

   Note that $H^{\otimes 4}|0000\rangle = \frac{1}{4}\sum_{x\in\{0,1\}^4}|x\rangle = \frac{1}{2}\left(\frac{1}{2}|0001\rangle + \frac{1}{2}|0010\rangle + \frac{1}{2}|0100\rangle + \frac{1}{2}|1000\rangle\right) + \frac{\sqrt{3}}{2}|X_0\rangle$ where $|X_0\rangle$ is a uniform superposition of the strings with Hamming weight different from 1.

   Thus if we implement one iteration of quantum searching, we get
   $-H^{\otimes 4}U_{0000}H^{\otimes 4}U_f H^{\otimes 4}|0000\rangle = \frac{1}{2}|0001\rangle + \frac{1}{2}|0010\rangle + \frac{1}{2}|0100\rangle + \frac{1}{2}|1000\rangle$ as required, where $U_f|x\rangle = (-1)^{f(x)}|x\rangle$.

   In order to implement U_f, we can use a reversible circuit, ADD, for computing the sum of four bits: $ADD : |x_1x_2x_3x_400\rangle \mapsto |x_1x_2x_3x_4y_1y_2\rangle$ where $y = 2y_1 + y_2 = x_1 + x_2 + x_3 + x_4$.

   Using a third ancilla qubit initialized to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, plus a Toffoli gate and two NOT gates (or alternatively, a Toffoli-gate controlled on the first bit being 0 and the second bit being 1), we can implement a -1 phase shift if and only if $f(x) = 1$ (i.e. the total number of 1s in x is one). And lastly, we "uncompute" the ADD operation.

   The net effect is to map $|x\rangle|00\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \mapsto (-1)^{f(x)}|x\rangle|00\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ as required.

5. Collision-finding **3 marks**

   Let $f : \{1, 2, \ldots, N\} \to X$ for some finite set of strings X, with the property that f is two-to-one. That is, for each value y occurring in the range of f, there are two distinct inputs, x_1, x_2 such that $f(x_1) = f(x_2) = y$.

Suppose you are given a black-box for implementing $U_f : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$, where $x \in \{1, 2, \ldots, N\}$ and $b \in \{0, 1\}$.

Consider the following collision-finding algorithm:

- Query $f(1), f(2), \ldots, f(M)$, for some $M << N$.
- If $f(x_1) = f(x_2)$ for distinct $x_1, x_2 \in \{1, 2, \ldots, M\}$, then output the collision pair (x_1, x_2).
- Otherwise, perform a quantum search for a value $x_2 \in \{M+1, M+2, \ldots, N\}$ such that $f(x_2) = f(x_1)$ for some $x_1 \in \{1, 2, \ldots, M\}$. Output (x_1, x_2).

(a) Assuming $f(1), f(2), \ldots, f(M)$ are distinct, what is the probability p that a value x sampled uniformly at random from $\{M+1, M+2, \ldots, N\}$ will satisfy $f(x) = f(x_1)$ for some $x_1 \in \{1, 2, \ldots, M\}$.

Solution:

There are $N-M$ values to choose from, and exactly M of them will lead to a collision with some $x_1 \in \{1, 2, \ldots, M\}$.
Thus the probability of a collision is $\frac{M}{N-M}$.

(b) How many quantum queries does this algorithm need in order to find a collision with constant probability? Express your answer in terms of N and M and using big-O notation. (Do not forget about the queries to compute $f(1), f(2), \ldots, f(M)$ in the first step.)

Solution:

Since the probability of finding a solution is $\frac{M}{N-M}$, we know the number of iterations of the quantum search iterate needed in order to find a solution with constant probability is in $O\left(\sqrt{\frac{N-M}{M}}\right) = O\left(\sqrt{\frac{N}{M}}\right)$ (since $M << N$).
Combined with the M queries needed to determine $f(1), f(2), \ldots, f(M)$, this gives a total number of queries in $O(\sqrt{\frac{N}{M}}) + M$.

(c) Let $M = N^\epsilon$ for some constant $\epsilon > 0$. Find the value of the constant ϵ that minimizes the number of queries (up to constant factors) needed to find a collision with high probability.

Solution:

The number of queries is $O(\sqrt{N^{1-\epsilon}}) + N^\epsilon = O(N^{\frac{1-\epsilon}{2}}) + N^\epsilon \in O(N^{\max(\frac{1-\epsilon}{2}, \epsilon)})$.
In order to minimize the exponent, we set $\frac{1-\epsilon}{2} = \epsilon$ (since one value gets larger as the other gets smaller), and solve to get $\epsilon = \frac{1}{3}$.

6. **3 marks** Parallelizing phase-queries

Let U_ϕ denote the unitary operation that maps $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\phi}|1\rangle$.

Note that $U_{k\phi} = U_\phi^k$. However, if a black-box process for implementing U_ϕ takes time t then implementing $U_{k\phi}$ in this serial way takes time kt.

Show that it is possible to parallelize the implementation of $U_{k\phi}$ in such a way that all k of the U_ϕ gates are applied in parallel (on different qubits). You may perform standard quantum gates on the qubits before and after the application of the k parallel phase gates.

Solution:

We can use $k-1$ ancilla qubits initialized to $|00\ldots0\rangle$, and then use $k-1$ CNOT gates to map $|0\rangle|00\ldots0\rangle \mapsto |0\rangle|00\ldots0\rangle$ and $|1\rangle|00\ldots0\rangle \mapsto |1\rangle|11\ldots1\rangle$.

Applying the k gates U_ϕ in parallel on these k qubits gives $U_\phi^{\otimes k}|0\rangle|00\ldots0\rangle \mapsto |0\rangle|00\ldots0\rangle$ and $U_\phi^{\otimes k}|1\rangle|11\ldots1\rangle \mapsto e^{ik\phi}|1\rangle|11\ldots1\rangle$.

Lastly, we can apply $k-1$ CNOT gates again to map $|0\rangle|00\ldots0\rangle \mapsto |0\rangle|00\ldots0\rangle$ and $|1\rangle|11\ldots1\rangle \mapsto |1\rangle|00\ldots0\rangle$.

The net effect of this circuit is to map $|0\rangle|00\ldots0\rangle \mapsto |0\rangle|00\ldots0\rangle$ and $|1\rangle|00\ldots0\rangle \mapsto e^{ik\phi}|1\rangle|00\ldots0\rangle$, as required.

7. Hidden shifts **2 marks**

Let $f : \{0,1,\ldots,2^n-1\} \to X$ and $g : \{0,1,\ldots,2^n-1\} \to X$ be one-to-one functions to a finite set X with the property that $g(x) = f(x+s)$ for some secret value $s \in \{0,1,\ldots 2^n-1\}$.

Let U_f map $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ and U_g map $|x\rangle|0\rangle \mapsto |x\rangle|g(x)\rangle$. Assume you have the controlled-U_f and controlled-U_g as black-boxes.

(a) Show how to create the state $\frac{1}{\sqrt{2}}|0\rangle|x\rangle + \frac{1}{\sqrt{2}}|1\rangle|x+s\rangle$ for some value $x \in \{0,1,\ldots,2^n-1\}$ (x can be random).

Solution:

Using $n+1$ Hadamard gates we can prepare

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle)|00\ldots0\rangle.$$

If we apply the controlled-U_f we get

$$\frac{1}{\sqrt{2}}|0\rangle \left(\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle\right)|00\ldots0\rangle + \frac{1}{\sqrt{2}}|1\rangle \left(\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle|f(x)\rangle\right).$$

If we apply a NOT gate on the control bit, followed by the controlled-U_g, and then another NOT gate, we get

$$\frac{1}{\sqrt{2}}|0\rangle \left(\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle|g(x)\rangle\right) + \frac{1}{\sqrt{2}}|1\rangle \left(\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle|f(x)\rangle\right).$$

If we measure the right-most register, we will obtain some value $y = g(x) = f(x+s)$ for some random value of x, and the rest of the qubits will be left in the state $\frac{1}{\sqrt{2}}|0\rangle|x\rangle + \frac{1}{\sqrt{2}}|1\rangle|x+s\rangle$, as requested.

(b) Given the state $\frac{1}{\sqrt{2}}|0\rangle|x\rangle + \frac{1}{\sqrt{2}}|1\rangle|x+s\rangle$ for some value $x \in \{0, 1, \ldots, 2^n - 1\}$, show how to create the state

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{sk}{2^n}}|1\rangle)|k\rangle$$

for a uniformly random $k \in \{0, 1, \ldots 2^n - 1\}$.

Solution:

If we apply the QFT_{2^n} to the state we obtain

$$\frac{1}{\sqrt{2}}|0\rangle\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i \frac{kx}{2^n}}|k\rangle + \frac{1}{\sqrt{2}}|1\rangle\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i \frac{k(x+s)}{2^n}}|k\rangle$$

$$= \sum_{k=0}^{2^n-1} \frac{1}{\sqrt{2}}(e^{2\pi i \frac{kx}{2^n}}|0\rangle + e^{2\pi i \frac{k(x+s)}{2^n}}|1\rangle)|k\rangle.$$

Thus, if we measure the register containing the "k" values, we obtain $|k\rangle$ uniformly at random for $k \in \{0, 1, \ldots, 2^n - 1\}$, and the remaining qubit is left in the state $\frac{1}{\sqrt{2}}(e^{2\pi i \frac{kx}{2^n}}|0\rangle + e^{2\pi i \frac{k(x+s)}{2^n}}|1\rangle)$ which equals $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{ks}{2^n}}|1\rangle)$ up to global phase.

8. Implementing controlled-black-boxes **3 marks**

Let $f : \{0, 1, \ldots, 2^n - 1\} \to \{0, 1, \ldots, 2^n - 1\}$.

Suppose you are given a black-box on $2n$ qubits for implementing

$$U_f : |x\rangle|b\rangle \mapsto |x\rangle|b + f(x) \bmod 2^n\rangle.$$

(a) Describe a state $|\psi\rangle$ such that $U_f : |x\rangle|\psi\rangle \mapsto |x\rangle|\psi\rangle$ for any input value x.

Solution:

Such a state should work, e.g. for the simple function $f(x) = 1$. The eigenstate of $|b\rangle \mapsto |b + 1 \bmod 2^n\rangle$ with eigenvalue $+1$ is $|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}|y\rangle$.

This state is thus a $+1$ eigenvalue (since $+1 = (+1)^{f(x)}$) of the map $|b\rangle \mapsto |b + f(x) \bmod 2^n\rangle$. Thus it follows that $U_f|x\rangle|\psi\rangle = |x\rangle|\psi\rangle$

(b) Given the n-qubit state $|\psi\rangle$ described in part a), and the black-box U_f, show how to implement the controlled-U_f on $2n+1$ qubits (plus the n-qubit ancilla state $|\psi\rangle$). Draw a circuit and explain why it works. *(Hint: you may use the controlled-SWAP gate.)*

Solution:

Consider the input state $|b\rangle|\phi\rangle|\psi\rangle$, where we wish to apply U_f to $|b\rangle|\phi\rangle$, and we use $|\psi\rangle$ as an ancilla state.

Suppose we first perform a controlled-SWAP of the n-qubits of $|\phi\rangle$ with the corresponding n-qubits of $|\psi\rangle$.

We then have the two possibilities:

$$|0\rangle|\phi\rangle|\psi\rangle \mapsto |0\rangle|\phi\rangle|\psi\rangle$$

and

$$|1\rangle|\phi\rangle|\psi\rangle \mapsto |1\rangle|\psi\rangle|\phi\rangle.$$

(Linear combinations of the control bit would lead to the corresponding linear combinations of the outputs: $(\alpha|0\rangle + \beta|1\rangle)|\phi\rangle|\psi\rangle \mapsto |0\rangle|\phi\rangle|\psi\rangle + |1\rangle|\psi\rangle|\phi\rangle$.)

If we then apply the U_f black-box to the ancilla register we get (using the fact that $U_f|\psi\rangle = |\psi\rangle$)

$$|0\rangle|\phi\rangle|\psi\rangle \mapsto |0\rangle|\phi\rangle|\psi\rangle \mapsto |0\rangle|\phi\rangle|\psi\rangle$$

and

$$|1\rangle|\phi\rangle|\psi\rangle \mapsto |1\rangle|\psi\rangle|\phi\rangle \mapsto |1\rangle|\psi\rangle U_f|\phi\rangle.$$

Another controlled-SWAP of the two registers results in the net transformation

$$|0\rangle|\phi\rangle|\psi\rangle \mapsto |0\rangle|\phi\rangle|\psi\rangle$$

and

$$|1\rangle|\phi\rangle|\psi\rangle \mapsto |1\rangle U_f|\phi\rangle|\psi\rangle$$

, or in general

$$(\alpha|0\rangle + \beta|1\rangle)|\phi\rangle|\psi\rangle \mapsto (|0\rangle|\phi\rangle + |1\rangle U_f|\phi\rangle)|\psi\rangle,$$

as required.