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) Find the smallest positive p so that 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.

   (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?

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, $\alpha_+|\psi_+\rangle = P_0|\psi\rangle$ and $\alpha_-|\psi_-\rangle = P_1|\psi\rangle$.

   Let $V = P_0 + iP_1$.

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

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

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

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 $U_f : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$.

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).

5. Collision-finding **3 marks**

   Let $f : \{1, 2, \dots, N\} \to X$ 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 $x \in \{1, 2, \dots, N\}$ and $b \in \{0, 1\}$.

   Consider the following collision-finding algorithm:

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

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

   (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 $f(1), f(2), \dots, f(M)$ in the first step.)

   (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.

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.

7. Hidden shifts **2 marks**

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

   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).

(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 $k \in \{0, 1, \ldots 2^n - 1\}$.

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.

(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.)*