Quantum Computing Problem Set 5

Author: Dave Bacon (*Department of Computer Science & Engineering, University of Washington*)
Due: August 3, 2005

Problem 1: A Simple Run of Simon's Algorithm

Here we will work through a small scale example of Simon's algorithm. Define the following two bit function:

$$f(0,0) = 0, \quad f(0,1) = 1, \quad f(1,0) = 1, \quad f(1,1) = 0$$

(a) This function has an xor-mask. That is there exist two bits, s_1 and s_2, such that $f(x_1, x_2) = f(x_1 \oplus s_1, x_2 \oplus s_2)$, where $\oplus$ is the exclusive or operation and s_1 and s_2 are both not equal to 0. What are s_1 and s_2?

(b) Suppose we have a unitary which implements this function as described in class:

$$U = \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \sum_{y=0}^{1} |x_1, x_2, y \oplus f(x_1, x_2)\rangle\langle x_1, x_2, y|$$

Suppose we have three qubits with the wave function $|v\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |0\rangle$. Calculate $U|v\rangle$. Express your answer as a sum over computational basis states.

(c) Suppose we now measure the third qubit (the one where the function "lives".) There will be two possible outcomes, corresponding to the computational basis states $|0\rangle$, and $|1\rangle$. Show that if you get outcome $|0\rangle$, then the state of the first two qubits is

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

.

(d) In part (c), we saw that if we got outcome $|0\rangle$ on the third qubit, then the wave function of the first two qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If we now take these first two qubits (conditional on measurement outcome $|0\rangle$ for measuring the third qubit), apply the two qubit Hadamard to this state, $H \otimes H$, and then measure the resulting two qubits in the computational basis (as we would do in Simon's algorithm), what are the (two) possible outcomes and what are their probabilities?

(e) In part (d), one of the possible outcomes you calculated should have been $|11\rangle$. Following along with Simon's algorithm, we know that this leads to the equation $s_1 + s_2 = 0 \mod 2$. What is the only nonzero solution to this equation (i.e. what are s_1 and s_2, assuming $s_1 \neq 0$ and $s_2 \neq 0$?) Compare with part (a).

Problem 2: One-in-Four Grover

In this problem we will solve what is called the one-in-four Grover problem (we haven't covered Grover's algorithm, yet, but while the problem is similar, we don't need to know anything about Grover's algorithm to solve it.) Suppose we have a function on two bits, which we define as $f_{a_1,a_2}(x_1, x_2) = 1$ if $x_1 = a_1$ and $x_2 = a_2$, but $f_{a_1,a_2}(x_1, x_2) = 0$ otherwise. Here a_1, a_2, x_1, and x_2 are all bits. Thus, for instance, if $a_1 = 0$ and $a_2 = 1$, then $f_{0,1}(x_1, x_2) = (1 - x_1)x_2$.

(a) Express $f_{0,0}(x_1, x_2)$, $f_{0,1}(x_1, x_2)$, $f_{1,0}(x_1, x_2)$, and $f_{1,1}(x_1, x_2)$ as multinomials of x_1 and x_2 (as we have done, just above, at the end of the intro paragraph, i.e. I've done the second one for you!)

(b) Suppose we have a unitary which implements this function as described in class:

$$U_{a_1,a_2} = \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \sum_{y=0}^{1} |x_1, x_2, y \oplus f_{a_1,a_2}(x_1, x_2)\rangle\langle x_1, x_2, y|$$

Here $\oplus$ is the exclusive or operation. If this unitary corresponds to the function $f_{1,0}(x_1, x_2)$ (i.e. $a_1 = 1$ and $a_2 = 0$), calculate what computational basis state is the result of applying $U_{1,0}$ to $|x_1 = 0, x_2 = 1, y = 1\rangle$.

(c) Suppose we start in a superposition over all inputs to the function and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the third qubit. In other words our initial state is

$$|v\rangle = \frac{1}{2\sqrt{2}} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} (|x_1, x_2, 0\rangle - |x_1, x_2, 1\rangle)$$

Show that if we apply the unitary U_{a_1,a_2} to this state we obtain the state

$$|v\prime\rangle = \frac{1}{2}\sum_{x_1=0}^{1}\sum_{x_2=0}^{1}(-1)^{f_{a_1,a_2}(x_1,x_2)}|x_1,x_2\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

(d) As we see above, the new wave function $U_{a_1,a_2}|v\rangle$, has the first two qubit wave function,

$$|a_1,a_2\rangle := \frac{1}{2}\sum_{x_1=0}^{1}\sum_{x_2=0}^{1}(-1)^{f_{a_1,a_2}(x_1,x_2)}|x_1,x_2\rangle$$

Show that these four states (corresponding to the four possible values of a_1, a_2) are orthogonal.

(e) (Harder) Since the $|a_1,a_2\rangle$ states are orthogonal, we can perform a measurement in this two qubit basis. This implies that there is a two qubit unitary transform such that performing a measurement in the computational basis for these two qubits will determine the bits a_1 and a_2 with one hundred percent certainty. What is this two qubit unitary operation?

In this problem, you've shown that if you have a two bit function which is 1 on only one possible two bit input, then by using a superposition, the phase kickback trick, querying the unitary corresponding to this function, and then performing a measurement in a particular basis, you can learn what the input to this function is which yields an output 1. You've found the one marked input out of 4 possible inputs in a single quantum query! The generalization of this problem, where only one n bit input to the function outputs 1 is called Grover's problem.