Quantum Computing Exercises # 6

Ronald de Wolf

Mar 8, 2011

(to be handed in before or at the start of the lecture on Mar 15)

1. (a) Suppose $n = 2$, and $x = x_{00}x_{01}x_{10}x_{11} = 0001$. Give the initial, intermediate, and final superpositions in Grover's algorithm, for $k = 1$ queries. What is the success probability?

   (b) Give the final superposition for the above x after $k = 2$ iterations. What is now the success probability?

2. Show that if the number of solutions is $t = N/4$, then Grover's algorithm always finds a solution with certainty after just one query. How many queries would a classical algorithm need to find a solution with certainty if $t = N/4$? And if we allow the classical algorithm error probability $1/10$?

3. Let $x = x_0 \dots x_{N-1}$ (where $N = 2^n$ and $x_i \in \{0,1\}^n$ is an n-bit number), be an input that we can query in the usual way, i.e., we can apply unitary $O_x : |i, 0^n\rangle \mapsto |i, x_i\rangle$. The *minimum* of x is defined as $\min\{x_i \mid i \in \{0, \dots, N-1\}\}$. Give a quantum algorithm that finds (with probability $\geq 2/3$) an index achieving the minimum, using $O(\sqrt{N} \log N)$ queries to the input.
   Hint: start with $m = x_i$ for a random i, and repeatedly use Grover's algorithm to find an index j such that $x_j < m$ and update $m = x_j$. Continue this until you can find no element smaller than m, and analyze the number of queries of this algorithm. You are allowed to argue about this algorithm on a high level (i.e., things like "use Grover to search for a j such that..." are OK), no need to write out complete circuits.
   Bonus: give a quantum algorithm that uses $O(\sqrt{N})$ queries.

4. Let $x = x_0 \dots x_{N-1}$, where $N = 2^n$ and $x_i \in \{0,1\}^n$, be an input that we can query in the usual way. We are promised that this input is 2-to-1: for each i there is exactly one other j such that $x_i = x_j$.[1] Such an (i, j)-pair is called a *collision*.

   (a) Suppose S is a randomly chosen set of s elements of $\{0, \dots, N-1\}$. What is the probability that there exists a collision in S?

   (b) Give a classical randomized algorithm that finds a collision (with probability $\geq 2/3$) using $O(\sqrt{N})$ queries to x. *Hint: What is the above probability if $s = 2\sqrt{N}$?*

   (c) Give a quantum algorithm that finds a collision (with probability $\geq 2/3$) using $O(N^{1/3})$ queries. *Hint: Choose a set S of size $s = N^{1/3}$, and classically query all its elements. First check if S contains a collision. If yes, you're done. If not, use Grover to find a $j \notin S$ that collides with an $i \in S$.*

[1] The 2-to-1 inputs for Simon's algorithm are a very special case of this, where x_i equals x_j if $i = j \oplus s$ for fixed but unknown $s \in \{0,1\}^n$.