School of Mathematics **Spring 2019**

QUANTUM COMPUTATION

Exercise sheet 2

Ashley Montanaro, University of Bristol
ashley.montanaro@bristol.ac.uk

1. **A simple case of Grover's algorithm.** Consider the unstructured search problem in the 4-element set $\{0,1\}^2$, where there is a unique marked element $x_0 = 10$.

   (a) Write down the matrix for the oracle operation U_f for this value of x_0, with respect to the computational basis.

   Answer: For $x_0 = 10$, by direct calculation the matrix for U_f is

   $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

   (b) Write down the matrix for the operator D occurring in Grover's algorithm for $N = 4$, with respect to the computational basis.

   Answer: We have $D = -H^{\otimes 2} U_0 H^{\otimes 2}$, so

   $$\begin{aligned} D &= -\frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}. \end{aligned}$$

   (c) Multiply out all the matrices and vectors occurring for one step of Grover's algorithm, to verify the claim in the lecture notes that the algorithm finds the marked element with certainty.

   Answer: One step of Grover's algorithm corresponds to applying the sequence of operations $DU_f H^{\otimes 2}$ to the initial state $|00\rangle$. So, written as a column vector, the final state is

   $$\frac{1}{4} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

So measuring the final state returns the outcome 10 with certainty.

(d) What is the final state if another step is made? What is the probability that the marked element is found if this state is measured?

Answer: Another step of the algorithm corresponds to applying DU_f. So the next state is

$$\frac{1}{2}\begin{pmatrix}-1\\-1\\1\\-1\end{pmatrix}.$$

Measuring this state in the computational basis will return the marked element with probability 1/4.

2. **Grover's algorithm for larger input sizes.** Here we consider Grover's algorithm with a search space of size 2^n for arbitrary integer n, and a unique marked element x_0.

(a) Calculate an expression for $\langle x|D|y\rangle$ for arbitrary $x, y \in \{0,1\}^n$.

Answer: Using the expression $D = -(I - 2|+\rangle\langle+|)$ from the lecture notes, we have

$$\langle x|D|y\rangle = \begin{cases} \frac{2}{N} - 1 & \text{if } x = y \\ \frac{2}{N} & \text{if } x \neq y \end{cases}.$$

(b) What is the probability that the marked element is found if the qubits are measured after only one step of the algorithm? Is this larger or smaller than we can achieve using a classical algorithm that makes one query?

Answer: From the definition of D, the state after one step of the algorithm is

$$DU_f|+\rangle = -(I - 2|+\rangle\langle+|)(I - 2|x_0\rangle\langle x_0|)|+\rangle = \left(1 - \frac{4}{N}\right)|+\rangle + \frac{2}{\sqrt{N}}|x_0\rangle,$$

where we use $\langle x_0|+\rangle = 1/\sqrt{N}$. So the probability that we see x_0 when we measure is

$$\left|\langle x_0|\left(\left(1 - \frac{4}{N}\right)|+\rangle + \frac{2}{\sqrt{N}}|x_0\rangle\right)\right|^2 = \left(\frac{3}{\sqrt{N}} - \frac{4}{N^{3/2}}\right)^2 = \frac{1}{N}\left(9 - \frac{24}{N} + \frac{16}{N^2}\right).$$

So the probability of success is roughly $9/N$, which is larger than the $1/N$ success probability we would achieve using a classical algorithm that makes just one query and then outputs the result. Note that we can do a bit better than this using a classical algorithm that checks one element, and if it is not marked, then picks another random element and returns that one; then the success probability is $2/N$.

3. **Grover's algorithm with errors.** Imagine we are attempting to run Grover's algorithm, but with an oracle U_f which sometimes fails to work. That is, sometimes it does nothing on every state (performs the identity operation), rather than the intended operation of mapping $|x_0\rangle$ to $-|x_0\rangle$, and leaving all other states $|x\rangle$ unchanged.

   (a) What is the effect on the algorithm if the oracle fails the first time it is used, but works on all subsequent occasions?

   Answer: The effective algorithm we obtain is to replace the first use of U_f with the identity operator, so the final state produced by the algorithm is of the form $(DU_f)^{T-1}D|+\rangle$. As $D|+\rangle = |+\rangle$, the new algorithm is equivalent to doing $T-1$ iterations of Grover's algorithm. The result is that the success probability is marginally reduced (by $O(1/N)$).

   (b) Assume that the overall algorithm makes T uses of U_f. What is the effect on the algorithm if the oracle fails the $\lceil T/2 \rceil$'th time it is used, but works on all other occasions?

   Answer: The answer depends on whether T is odd or even. Grover's algorithm corresponds to applying the unitary operator $(DU_f)^T$. If T is odd, we replace the middle U_f in this string of DU_f's with the identity operator I. But as $U_f^2 = I$ and also $D^2 = I$, this means that almost the entire string of DU_f's cancels out, and we are left with the operator D. As noted previously, $D|+\rangle = |+\rangle$, so the algorithm returns a random result. If T is even, after this cancellation we are left with the string DU_fD. So we finish with the effective algorithm DU_f, which is equivalent to running just one iteration of Grover's algorithm. So (using the bound of Q2b) the success probability is also $O(1/N)$.

4. **Running Grover's algorithm on a real quantum computer (optional).**

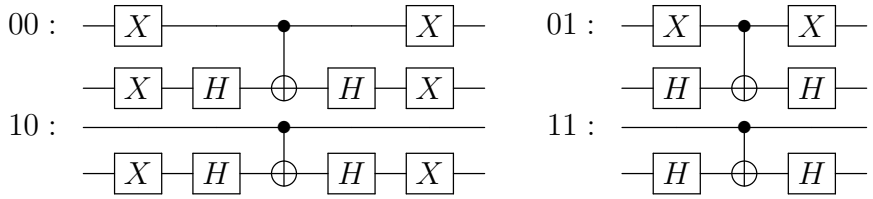
   The IBM Q Experience (`www.research.ibm.com/quantum/`) is a web interface to a real quantum computing experiment at IBM. In this question you will use it to implement and run Grover's algorithm for $N = 4$ and a unique marked element x_0.

   (a) Sign up for an account on the IBM Q Experience website, log in and familiarise yourself with the interface.

   (b) Find quantum circuits containing only H, X and CNOT gates for the operations U_0 and U_f occurring in Grover's algorithm, for the four different possible values for x_0. Hint: exercise sheet 1, Q2c could be useful.

   Answer: First note that U_0 is the same as U_f for $x_0 = 00$, and also note that U_f for $x_0 = 11$ is the same as CZ, for which a circuit of the desired form was obtained in exercise sheet 1, Q2c. To obtain the operators corresponding to the other values for x_0, we can permute the rows and columns using X gates. The

circuits obtained corresponding to different values of x_0 are:



(c) Use your answer to part (b) to implement the quantum circuits corresponding to one iteration of Grover's algorithm, for these different possible choices for x_0, on the IBM Q Experience. (Note that a $-I$ gate is not available, so replace D with $-D$ in the definition of the algorithm.) Run the circuits on the simulator. Check that the answer is what you expect.

(d) Run the same circuits on the real quantum computer. Note that this has restrictions on the allowed topology of gates. Is the answer what you expect?

(e) Work through the tutorials for the IBM Q Experience and experiment with other circuits (for example, Grover's algorithm with $N = 8$).