

QUANTUM COMPUTATION

Exercise sheet 1

Ashley Montanaro, University of Bristol

ashley.montanaro@bristol.ac.uk

1. Revision.

- (a) Imagine we have a quantum state $|\psi\rangle$ of n qubits, where $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$, and we measure the first qubit of $|\psi\rangle$ in the computational basis. What is the probability that the measurement outcome is 1, in terms of the α_x coefficients?

Answer: $\sum_{x, x_1=1} |\alpha_x|^2$.

- (b) What is the state of the system after the measurement?

Answer: $\frac{1}{\sqrt{\sum_{x, x_1=1} |\alpha_x|^2}} \sum_{x, x_1=1} \alpha_x |x\rangle$.

- (c) Let M be the matrix defined by $M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ -1 & 1 \end{pmatrix}$. Is M unitary?

Answer: No, because $M^\dagger M \neq I$.

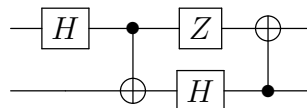
- (d) Write down the matrix corresponding to the operator $H \otimes H$, in the computational basis, where H is the Hadamard operator.

Answer:

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

2. The quantum circuit model.

- (a) Consider the following quantum circuit C :



- i. Calculate the matrix of the unitary operation U corresponding to C , with respect to the computational basis.

Answer: The answer can be obtained either by just multiplying out the matrices corresponding to the gates, or by tracking each computational basis state through the circuit, e.g.:

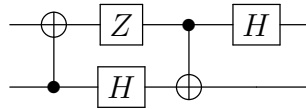
$$\begin{aligned}
 |0\rangle|0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 &\mapsto \frac{1}{2}(|0\rangle(|0\rangle + |1\rangle) - |1\rangle(|0\rangle - |1\rangle)) \\
 &\mapsto \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle).
 \end{aligned}$$

The final answer is

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

ii. Write down a quantum circuit corresponding to the inverse operation U^{-1} .

Answer: As each gate in the circuit is its own inverse, U^{-1} can be implemented by running the circuit in reverse order, i.e.:



iii. If C is applied to the initial state $|0\rangle|0\rangle$ and is followed by a measurement of each qubit in the computational basis, what is the distribution on measurement outcomes?

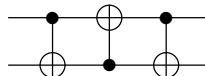
Answer: The distribution on measurement outcomes is obtained by squaring the first column of U , and is hence uniform on $\{0, 1\}^2$.

(b) The SWAP gate for 2 qubits is defined as $\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$ for $x, y \in \{0, 1\}$ and is denoted by the circuit element $\begin{array}{c} \times \\ \text{---} \\ \times \end{array}$. Show that SWAP can be implemented as a product of CNOT gates and write down the corresponding circuit.

Answer: The matrix for SWAP in the computational basis is

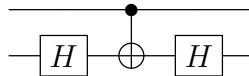
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

By direct calculation, the following circuit corresponds to the same matrix:



- (c) Show that a CZ gate can be implemented using a CNOT gate and Hadamard gates and write down the corresponding circuit.

Answer: Recall from Quantum Information Theory that $Z = HXH$. As CNOT is a controlled- X operation, we would expect that $CZ = (I \otimes H) \text{CNOT} (I \otimes H)$. And indeed this is the case, as can be verified from writing out the matrices and multiplying them together. The corresponding circuit is



- (d) The classical OR gate takes as input a pair of bits $x, y \in \{0, 1\}$ and outputs 1 if either x or y is equal to 1, and 0 otherwise. Use the generic construction of reversible functions discussed in the lecture notes to write down a unitary operation on 3 qubits which corresponds to a reversible implementation of the OR gate.

Answer: Following the same construction as for AND, we obtain the map $|x\rangle|y\rangle|z\rangle \mapsto |x\rangle|y\rangle|z \oplus (x \text{ OR } y)\rangle$. Written explicitly as a matrix with respect to the computational basis, this is

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

3. The Bernstein-Vazirani algorithm.

A parity function $f_s : \{0, 1\}^n \rightarrow \{0, 1\}$, for some $s \in \{0, 1\}^n$, is a function of the form $f_s(x) = x \cdot s$, where the inner product is taken modulo 2. For example, with $n = 3$, $f_{110}(x)$ is the function $x_1 \oplus x_2$.

- (a) Show that f_s is a balanced function for all $s \neq 0^n$.

Answer: We have $f_s(x) = \sum_i x_i s_i \pmod 2$. If $s \neq 0^n$, then there exists i such that $s_i \neq 0$. So, for all x , $f_s(x) \neq f_s(x^i)$, where x^i is the string obtained from x

by inverting bit i . Hence f_s is balanced.

- (b) Imagine we apply the circuit for the Deutsch-Jozsa algorithm with the oracle U_{f_s} . Show that the measured output is precisely the string s .

Answer: The final state in the Deutsch-Jozsa algorithm is

$$\sum_{y \in \{0,1\}^n} \frac{1}{2^n} \left(\sum_{x \in \{0,1\}^n} (-1)^{f_s(x)+x \cdot y} \right) |y\rangle.$$

We have

$$\sum_{x \in \{0,1\}^n} (-1)^{f_s(x)+x \cdot y} = \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s + x \cdot y} = \sum_{x \in \{0,1\}^n} (-1)^{x \cdot (s+y)}.$$

By the same argument as part (a), this evaluates to zero unless $s + y = 0^n \pmod{2}$, or in other words unless $s = y$.

- (c) Consider the following problem: given oracle access to a parity function f_s , determine s using the minimal number of queries to f_s .

- i. Conclude from (b) that there is a quantum algorithm that solves this problem with one query to f_s .

Answer: We perform the Deutsch-Jozsa algorithm, using the oracle U_{f_s} , and measure the final result. The answer is s with certainty and the algorithm uses one query to U_{f_s} and hence one query to f_s .

- ii. Give an exact bound on the number of queries to f_s required for a classical algorithm to solve the problem with certainty.

Answer: Each classical query has two outcomes, so reduces the space of possibilities for s by at most a factor of $1/2$. As there are 2^n possible strings s , the classical algorithm must make at least n queries. This is tight, because we can evaluate f_s on the strings $x^{(i)}$, $i = 1, \dots, n$ where $x^{(i)}$ is 1 at position i , and 0 elsewhere. Then $f_s(x^{(i)}) = s_i$, so each query reveals one bit of s .

4. Simulation of various kinds. (Optional)

- (a) Show that the phase oracle U_f as defined in the lecture notes cannot be used to implement the bit oracle O_f in general, even if f only has 1 bit output.

Answer: Consider the two functions on one bit $f(x) = 0$ and $f(x) = 1$. Then in the first case, $U_f|x\rangle = |x\rangle$, and in the second case $U_f|x\rangle = -|x\rangle$; thus either $U_f = I$ or $U_f = -I$. These two operations are indistinguishable by any operations we might perform around them, because they only differ by a global phase of -1 .

But in the case of the bit oracle $O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, these two functions are indeed distinguishable (we could simply query O_f on $x = 0$). So U_f cannot be used to implement O_f in general.

- (b) Imagine we are given a quantum circuit on n qubits which consists of $\text{poly}(n)$ gates picked from the (universal) set $\{H, X, \text{CNOT}, T\}$, followed by a final measurement of all the qubits. Assume that at each step in the computation the quantum state is unentangled (i.e. is a product state of the n qubits). Show that the circuit can be simulated efficiently classically: that is, there is an efficient classical algorithm for exactly sampling from the probability distribution on the final measurement outcomes.

Answer: Imagine we start with a product state $|\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle$. A description of this state can be written down in $O(n)$ space by writing down a description of each state $|\psi_i\rangle$ separately. We simulate the effect of each gate in the circuit on this state in turn. If we have H , X or T on qubit i , this can be done by multiplying $|\psi_i\rangle$ by the corresponding matrix, and updating the description of $|\psi_i\rangle$ accordingly. On the other hand, the CNOT gate involves two qubits i, j . So, once the gate has been applied, we need to find a new product state representation for the state of these qubits. This can be achieved by solving a system of equations in 4 variables corresponding to the amplitudes of the product states. At the end of the circuit, we have some product state of n qubits. To simulate sampling from the distribution on final outcomes x , we can sample each bit x_i from the distribution corresponding to state $|\psi_i\rangle$.