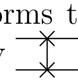
School of Mathematics **Spring 2017**

QUANTUM COMPUTATION

Practice questions

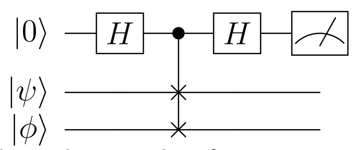
Ashley Montanaro, University of Bristol
`ashley.montanaro@bristol.ac.uk`

1. **Quantum circuits.** The SWAP gate performs the map $|x\rangle|y\rangle \mapsto |y\rangle|x\rangle$ for $x, y \in \{0,1\}$ and is denoted in a quantum circuit by .

   (a) Write down the matrix corresponding to SWAP with respect to the computational basis and hence, or otherwise, show that SWAP is unitary.

   (b) Show that, for any quantum states of one qubit $|\psi\rangle$, $|\phi\rangle$, SWAP$|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle$.

   (c) Consider the following quantum circuit, where $|\psi\rangle$, $|\phi\rangle$ are arbitrary states of one qubit.

   What is the probability that the result of measuring the first qubit is 1 in each of these two cases?

   i. $|\psi\rangle = |0\rangle$, $|\phi\rangle = |1\rangle$.

   ii. $|\psi\rangle = |\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

2. **Grover's algorithm.**

   (a) Imagine we would like to solve the unstructured search problem on a set of size N, where we know that there are M marked elements, for some M. Let S denote the set of marked elements and write $U_f = I - 2\Pi_S$, where $\Pi_S = \sum_{x \in S} |x\rangle\langle x|$.

   i. Show that $U_f^2 = I$ and hence that U_f is unitary.

   ii. Show that, if $M = N/4$, the unstructured problem can be solved with one use of the oracle operator U_f.

   (b) Imagine we apply standard Grover search for a unique marked element, but in fact every element is marked ($M = N$). Does the algorithm succeed? Why or why not?

3. **The QFT and periodicity.**

   (a) Using the formula for a geometric series, or otherwise, write down an expression for Q_N^2 for any N.

(b) Run through the steps of the periodicity-determination algorithm for the periodic function $f : \mathbb{Z}_4 \to \mathbb{Z}_2$ where $f(0) = 1$, $f(1) = 0$, $f(2) = 1$, $f(3) = 0$, choosing an arbitrary measurement outcome in step 3. What is the distribution on measurement outcomes? What is the probability that the algorithm succeeds?

4. **Shor's algorithm.**

   (a) Assume that we would like to factorise $N = 33$ and pick $a = 10$. Determine the order of a mod N and hence factorise N.

   (b) Write down the continued fraction expansion of 17/32 and the corresponding sequence of convergents.

   (c) Describe all the ways that Shor's algorithm can fail to factorise an integer N.

5. **Phase estimation and Hamiltonian simulation.**

   (a) Write down the full quantum circuit for phase estimation with $n = 3$.

   (b) What is the minimal k such that the Hamiltonian $H = 2X \otimes X \otimes I - 3Z \otimes I \otimes Z$ is k-local? What is the minimal k such that H^2 is k-local?

   (c) Let H be a Hamiltonian on n qubits, and imagine we can produce a state $|\psi\rangle$ such that $|\psi\rangle$ is an eigenvector of H with eigenvalue λ. Describe how phase estimation can be combined with Hamiltonian simulation to approximately determine λ.

6. **Noise, quantum channels and error-correction.**

   (a) The phase-damping channel $\mathcal{E}_P$ is described by Kraus operators

$$E_0 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \begin{pmatrix} \sqrt{p} & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{p} \end{pmatrix}$$

   for some p such that $0 \le p \le 1$.

      i. What is the result of applying $\mathcal{E}_P$ to a mixed state ρ of the form

$$\rho = \begin{pmatrix} \alpha & \beta \\ \beta^* & \gamma \end{pmatrix}$$

      in the computational basis?

      ii. Determine the representation of $\mathcal{E}_P$ as an affine map $v \mapsto Av + b$ on the Bloch sphere.

   (b) Imagine we encode the state $\alpha|0\rangle + \beta|1\rangle$ using the bit-flip code (i.e. $|0\rangle \mapsto |000\rangle$ and $|1\rangle \mapsto |111\rangle$) and a Y error occurs on the second qubit. What is the decoded state?

   (c) The code space of the bit-flip code is span$\{|000\rangle, |111\rangle\}$. Find three independent commuting Pauli matrices (on 3 qubits each) that preserve this subspace, i.e. that map each state in the subspace to another state in the subspace. Find a Pauli matrix that anticommutes with one of these matrices.