CS419

THE UNIVERSITY OF WARWICK

MEng Examinations: Summer 2020

Quantum Computing MOCK

Time allowed: 3 hours.

Answer **THREE** questions: **Question 1** from Section A and **TWO** questions from Section B.

Read carefully the instructions on the answer book and make sure that the particulars required are entered on **each** answer book.

Calculators are not allowed.

Section A Answer the following question

1. (a) **(6 points)** Formally state two of the postulates of quantum computation.

   (b) **(6 points)** Suppose the quantum state $|\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |01\rangle + \alpha_3 |10\rangle + \alpha_4 |11\rangle$ is measured in the $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle\}$ basis. What is the probability of outcome $|{+}{+}\rangle$? How about $|{-}{-}\rangle$?

   (c) **(18 points)** For each of the following statements, indicate whether it is **true** or **false**. You will be awarded 3 points for each correct answer and -3 points for each incorrect answer. (Should the sum of awarded points be negative, you will receive 0 points for this part of the question.)

      i. Quantum computers enable exponential speedups as compared to classical ones because computing on a state in superposition is equivalent to making exponentially many classical computations in parallel.

      ii. If the pure quantum states $|\Psi\rangle, |\phi\rangle$ are indistinguishable, they differ by a global phase: there exists $c \in \mathbb{C}$ such that $|\phi\rangle = c\,|\Psi\rangle$.

      iii. If the mixed states with density matrices ρ, σ are indistinguishable, the pure states in each distribution differ by a global phase: there exist $|\Psi_1\rangle, \ldots |\Psi_m\rangle$, $|\phi_1\rangle, \ldots, |\phi_m\rangle$ and $c_1, \ldots, c_m \in \mathbb{C}$ such that $\rho = \sum_{i=1}^{m} p_i \,|\Psi\rangle_i \langle\Psi|_i$ and $\sigma = \sum_{i=1}^{m} p_i \,|\phi_i\rangle \langle\phi_i|$, with $|\phi_i\rangle = c_i\,|\Psi_i\rangle$ for all $i \leq m$.

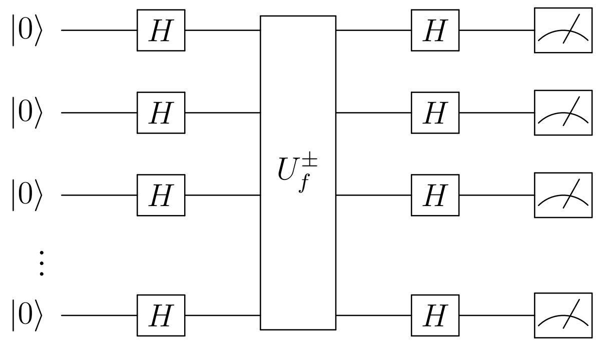
      iv. A measurement gate is given by a unitary matrix, but not all unitary matrices define a measurement.

      v. Fourier transforms are different on different groups, but each group has a unique Fourier basis.

      vi. The Hidden Subgroup Problem generalises all of the main quantum algorithms studied in the course: Deutsch-Josza, Bernstein-Vazirani, Simon's, Grover's and Shor's.

Section B Answer **TWO** questions (out of three)

1. Let $f : \{0,1\}^n \to \{0,1\}$ be any function, and $U_f^{\pm}$ a quantum circuit that sign-implements f. Consider the following circuit.



   (a) **(15 points)** Determine the state of the n qubits after applying each one of the gates.

   (b) **(10 points)** Determine the probabilities of the possible outcomes of the measurements.

   (c) **(10 points)** Describe at least one application that this circuit can be used for.

2. Let $F : \{0,1\}^2 \to \{0,1\}$ be the two-bit NOR (negated OR) function.

   (a) **(5 points)** Write the truth table of F as well as that of $f : \{0,1\}^2 \to \{1,-1\}$, the sign-implementation of F.

   (b) **(10 points)** Write the two-qubit quantum state $|f\rangle$ and the two-qubit quantum states of the Fourier basis $|\chi_{00}\rangle$, $|\chi_{01}\rangle$, $|\chi_{10}\rangle$ and $|\chi_{11}\rangle$.

   (c) **(10 points)** Compute the Fourier coefficients $\hat{f}(00), \hat{f}(01), \hat{f}(10)$ and $\hat{f}(11)$. Write the quantum state $\left|\hat{f}\right\rangle$.

   (d) **(10 points)** Write $|f\rangle$ as a linear combination of the Fourier basis. How does it relate to $\left|\hat{f}\right\rangle$ (written in the computational basis)?

3. Consider the following generalization of Simon's problem: the input is $F : \{0,1\}^n \to \{0,1\}$, with the property that there is some unknown *subspace* $V \subseteq \{0,1\}^n$ (where $\{0,1\}^n$ is the vector space of n-bit strings with entrywise addition modulo 2) such that $F(x) = F(y)$ if and only if there exists an element $v \in V$ such that $x = v \oplus y$ (recall that, in this case, a subspace V is simply a subset such that $u \oplus v \in V$ whenever $u, v \in V$).

   The goal is to determine V, and the usual definition of Simon's problem corresponds to the case where $V = \{0, s\}$ for some unknown $s \in \{0,1\}^n$ (which is equivalent to finding s).

   (a) **(5 points)** Show that $\{0, s\}$ is a subspace of $\{0,1\}^n$ for any fixed s.

   (b) **(20 points)** Show that one run of Simon's algorithm now produces a $z \in \{0,1\}^n$ that is orthogonal to the whole subspace V (i.e., $\sum_{i=0}^{n} z_i \cdot v_i = 0 \mod 2$ for every $v \in V$).

   (c) **(10 points)** Explain how we might extend Simon's algorithm to solve this generalised version of the problem.