THE UNIVERSITY OF WARWICK

Examination: Summer 2022

Paper Code: CS9390_B

Quantum Computing

Time allowed: 3 hours.

Exam type: Standard Examination.

Answer **BOTH** questions from Section A and **ONE** question from Section B.

Read carefully the instructions on the answer book.

Calculators are not allowed.

Section A Answer **BOTH** questions.

1. (a) Describe the difference between an *entangled* and a *separable* state. [2]

(b) You are given a qubit in state $|\psi\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$, and another qubit in state $|\phi\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$. Express the joint state of both qubits in the computational basis. [3]

(c) Describe the difference between an *pure* and a *mixed* state. Explain how to express a mixed state as a *density matrix*, and describe the three conditions a density matrix must satisfy. [5]

(d) For each of the following states, write whether the state is entangled or separable. Then write the mixed state obtained by discarding the second qubit (either as a distribution or as a density matrix). Justify your answers in each case. [20]

i. $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

ii. $\frac{|00\rangle+|01\rangle}{\sqrt{2}}$.

iii. $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

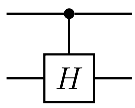
iv. $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$.

v. $\frac{1}{2}(|00\rangle + i\,|01\rangle + i\,|10\rangle - |11\rangle)$.

2. In this question you will show how to attack Wiesner's quantum money scheme if the bank always returns banknotes to the client (even when the verification fails).

   (a) Describe how an n-qubit banknote is generated and verified in Wiesner's quantum money scheme. [8]

   (b) Design a quantum circuit which, on input the state $|0\rangle^{\otimes 3}$, outputs a random 1-qubit banknote $|\$_k\rangle$ along with its corresponding key k. Explain why your circuit works. (Note: your circuit can output any representation of k.)

   Hint: use the controlled-H gate, $C_H(|b\rangle \otimes |\psi\rangle) = |b\rangle \otimes H^b |\psi\rangle$, written  .

   [7]

   (c) Suppose you are given a 1-qubit banknote $|\$_k\rangle$. You apply an X gate to $|\$_k\rangle$, obtaining a state $|\phi\rangle$, and then you send $|\phi\rangle$ to the bank. The bank runs the verification procedure on $|\phi\rangle$ and sends you the outcome (VALID or INVALID) along with the post-measurement state. Describe what happens for each possible k. [8]

   (d) Describe how to recover the key k from an n-qubit banknote $|\$_k\rangle$. [7]

Section B Answer **ONE** question.

3. For a function $f\colon \{0,1\}^n \to \{0,1\}^n$, denote by U_f the unitary $|x, y\rangle \mapsto |x, (y \oplus f(x))\rangle$.

   (a) Suppose $n = 1$. Show how to build a circuit that computes the unitary $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$ (known as the phase oracle). You may use Z gates, ancilla qubits initialized to $|0\rangle$, and **two** U_f gates. You must ensure that any ancilla qubits return to the state $|0\rangle$ so that they can be safely discarded. Prove that your circuit is correct. [6]

   (b) Suppose now (and for the remaining parts of this question) that $n = 2$. The gate S maps $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto i\,|1\rangle$. Show that $S^2 = Z$. [2]

   (c) Show how to build a circuit that computes the unitary that maps $|x\rangle \mapsto \omega^{2f(x)_1 + f(x)_2} |x\rangle$, where $f(x)_1, f(x)_2$ are the first and second bits of $f(x)$, respectively. You may use S gates, ancilla qubits initialised to $|0\rangle$, and **two** U_f gates. You must ensure that any ancilla qubits return to the state $|0\rangle$ so that they can be safely discarded. Prove that your circuit is correct. [12]

   (d) Design a circuit that determines whether f is constant or one-to-one. You may use:

      - any number of qubits initialized to $|0\rangle$,
      - Hadamard (H) gates,
      - S gates,
      - measurements in the computational basis, and
      - **two** U_f gates.

      Prove that your circuit is correct. [20]

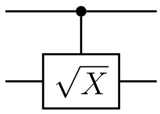
Continued

4. (a) Describe the CNOT and Toffoli (CCNOT) gates. [6]

   (b) What are the eigenvectors and eigenvalues of the matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$? [4]

   (c) Using your answer to the above, or otherwise, find a matrix $\sqrt{X}$ such that $(\sqrt{X})^2 = X$. (Hint: observe that X is Hermitian.) [6]

   (d) The controlled-$\sqrt{X}$ gate $C_{\sqrt{X}}$ is drawn like this:



   and operates as follows:

$$C_{\sqrt{X}} |0\rangle \otimes |\psi\rangle = |0\rangle \otimes |\psi\rangle \qquad C_{\sqrt{X}} |1\rangle \otimes |\psi\rangle = |1\rangle \otimes \sqrt{X} |\psi\rangle$$

   for any qubit state $|\psi\rangle$.

   i. Show how to implement a CNOT gate using only $C_{\sqrt{X}}$ gates. [4]

   ii. Show how to implement the gate $(C_{\sqrt{X}})^\dagger$ using only $C_{\sqrt{X}}$ gates. [4]

   iii. Show how to implement the unitary U that maps

$$|ab\rangle \otimes |\psi\rangle \mapsto |ab\rangle \otimes (\sqrt{X})^a (\sqrt{X})^b |\psi\rangle$$

   for all $a, b \in \{0, 1\}$ and qubit states $|\psi\rangle$ using only $C_{\sqrt{X}}$ gates. [6]

   iv. Show how to implement a Toffoli gate using only $C_{\sqrt{X}}$, $(C_{\sqrt{X}})^\dagger$ and CNOT gates. (Hint: start with your circuit from part (iii).) [10]

   (In each part, you should draw a circuit and show that it is correct.)