QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F19)

Assignment 2
Due date: October 3, 2019

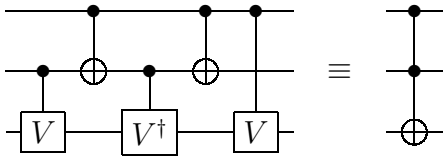
1. **Measuring individual qubits [12 points].** Let the state of a 3-qubit system be

$$\tfrac{1}{\sqrt{3}}|100\rangle + \tfrac{1}{\sqrt{3}}|010\rangle + \tfrac{1}{\sqrt{3}}|001\rangle. \tag{1}$$

   (a) [6 points] Suppose the first qubit is measured (in the computational basis). Give the probability of each possible outcome. Also, for each possible outcome, give the state of the two remaining qubits after the measurement.

   (b) [6] Suppose the first qubit and third qubit are both measured (in the computational basis). Give the probability of each possible outcome. Also, for each possible outcome, give the state of the remaining qubit after the measurement.

2. **Constructing a Toffoli gate out of two-qubit gates [12 points].** The Toffoli gate (controlled-controlled-NOT) is a 3-qubit gate, and here we show how to implement it with 2-qubit gates. The construction is given by the following quantum circuit



where

$$V = \tfrac{1}{\sqrt{2}} \begin{pmatrix} \omega & \overline{\omega} \\ \overline{\omega} & \omega \end{pmatrix}, \quad \text{with } \omega = e^{i\pi/4} \text{ and } \overline{\omega} = e^{-i\pi/4} \text{ (ω's conjugate).}$$

   We *could* verify this by multiplying 8×8 matrices; however, we take a simpler approach.

   (a) [2 points] Show that $V^2 = X$ (this means V is a square root of NOT).

   (b) [8] Prove each of the following, where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is an arbitrary 1-qubit state:

      i. The circuit maps $|00\rangle|\psi\rangle$ maps to $|00\rangle|\psi\rangle$.
      ii. The circuit maps $|01\rangle|\psi\rangle$ maps to $|01\rangle|\psi\rangle$.
      iii. The circuit maps $|10\rangle|\psi\rangle$ maps to $|10\rangle|\psi\rangle$.
      iv. The circuit maps $|11\rangle|\psi\rangle$ maps to $|11\rangle V^2|\psi\rangle$.

   (c) [2] Based on parts (a) and (b), give the 8×8 unitary matrix of the above circuit.

3. **Classifying multilinear functions [12 points, 6 each].** For each $a_1a_2b \in \{0,1\}^3$, define the function $f_{a_1a_2b} : \{0,1\}^2 \to \{0,1\}$ as

$$f_{a_1a_2b}(x_1, x_2) = a_1x_1 + a_2x_2 + b \bmod 2. \tag{2}$$

   (This is equivalent to defining $f_{a_1a_2b}(x_1, x_2) = (a_1 \wedge x_1) \oplus (a_2 \wedge x_2) \oplus b$.) Note that these eight functions can be classified into four categories as follows

CONTINUED ON NEXT PAGE

- **Constant**: $f_{000}(x_1, x_2) = 0$; and $f_{001}(x_1, x_2) = 1$.
- **Varying with respect to** x_2: $f_{010}(x_1, x_2) = x_2$; and $f_{011}(x_1, x_2) = x_2 + 1 \bmod 2$.
- **Varying with respect to** x_1: $f_{100}(x_1, x_2) = x_1$; and $f_{101}(x_1, x_2) = x_1 + 1 \bmod 2$.
- **Varying with respect to** $x_1 + x_2 \bmod 2$:
  $f_{110}(x_1, x_2) = x_1 + x_2 \bmod 2$; and $f_{111}(x_1, x_2) = x_1 + x_2 + 1 \bmod 2$.

Let the goal be to determine a_1 and a_2 (in other words, which of the four categories).

(a) What is the minimum number of classical queries required to solve this problem? (Include a proof that it cannot be fewer.)

(b) Show that one quantum query suffices to solve this problem. (Include the algorithm.)

4. **Distinguishing between pairs of unitaries [12 points, 4 each].** In each case, you are given a black box gate that computes one of the two given unitaries, but you are not told which one. It is chosen uniformly: each is selected with probability $\frac{1}{2}$. Your goal is to guess which of the two unitaries it is with as high a probability as you can. To help you do this, you can create any one-qubit quantum state, apply the black box gate to this qubit, and then measure the answer in some basis (that is, you can apply a unitary of your choosing and then measure in the computational basis). You can only use the black-box gate once.

   For example, consider the case where the two unitaries are $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In this case, setting the initial state to $|+\rangle$, applying the black-box unitary, followed by H and measuring yields 0 in the first case and 1 in the second case. So this is a perfect distinguishing procedure (it succeeds with probability 1).

   Give the best distinguishing procedure (i.e., highest success probability) you can find in each case below. You do not have to prove optimality.

   (a) $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ (the latter is a rotation by $\pi/4$).

   (b) I and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

   (c) I and H.

   (Hint: in two out of the above three cases there is a perfect distinguishing procedure.)

5. **Zero vs. 3/4-weight [12 points].** For $n \geq 2$, call a function $f : \{0,1\}^n \to \{0,1\}$ 3/4-*weight* if the number of $x \in \{0,1\}^n$ for which $f(x) = 1$ is $(3/4)2^n$. Suppose you're promised that function f is *either* 3/4-weight *or* zero (i.e., $f(x) = 0$, for all $x \in \{0,1\}^n$) and your goal is to distinguish between the two cases with as few queries to f as possible.

   (a) [3 points] What is the minimum number of classical queries needed to solve this problem (with no error probability permitted)? (Include a proof that it cannot be fewer.)

   (b) [9] Show that one quantum query suffices to solve this problem (with no error probability permitted). (Include the algorithm.)

6. **Optional question for bonus credit [10 points].** Deutsch's problem can be viewed as the problem where one is given a function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ that is linear, of the form $f(x) = ax + b$ (arithmetic mod-2), for unknown coefficients $a, b \in \mathbb{Z}_2$, and the goal is to determine the value of coefficient a.

   Consider the variation of Deutsch's problem, where there is a function $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ that is quadratic, of the form $f(x) = ax^2 + bx + c$ (all arithmetic is mod 3), for unknown coefficients $a, b, c \in \mathbb{Z}_3$, and the goal is to determine the value of coefficient a (the "leading coefficient").

   The black box for f that we are given maps (x, y) to $(x, y + f(x))$ in the classical case; and $|x\rangle|y\rangle$ to $|x\rangle|y + f(x)\rangle$ in the quantum case (for each $x, y \in \mathbb{Z}_3$, and with arithmetic mod-3). For simplicity, assume here that the registers contain trits or qutrits.

   (a) [1 point] Show that any classical algorithm solving this problem must make at least three queries to f. (Note that the algorithm *only* has to determine a; not b or c.)

   (b) [4] Give a quantum algorithm that solves this problem with two queries to f.

   (c) [5] Prove that this problem cannot be solved by a quantum algorithm that makes only one query.