QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F15)

Assignment 2
Due date: October 13, 2015

1. **Entangled states and product states [9 points; 3 for each part].** For each two-qubit state below, either express it as a product of two one-qubit states or show that such a factorization is impossible (in the latter case, the qubits are *entangled*).

   (a) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

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

   (c) $\frac{1}{2}|00\rangle + i\frac{1}{2}|01\rangle + i^2\frac{1}{2}|10\rangle + i^3\frac{1}{2}|11\rangle \qquad (i = \sqrt{-1})$

2. **Determining the "slope" of a linear function over $\mathbb{Z}_4$ [12 points; 3 each].** Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, with arithmetic operations of addition and multiplication defined with respect to modulo 4 arithmetic on this set. Suppose that we are given a black-box computing a linear function $f : \mathbb{Z}_4 \to \mathbb{Z}_4$, which of the form $f(x) = ax + b$, with unknown coefficients $a, b \in \mathbb{Z}_4$ (throughout this question, multiplication and addition mean these operations in modulo 4 arithmetic). Let our goal be to determine the coefficient a (the "slope" of the function). We will consider the number of quantum and classical queries needed to solve this problem.

   Assume that what we are given is a black box for the function f that is in reversible form in the following sense. For each $x, y \in \mathbb{Z}_4$, the black box 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 (which is unitary).

   Also, note that we can encode the elements of $\mathbb{Z}_4$ into 2-bit strings, using the usual representation of integers as a binary strings ($00 = 0$, $01 = 1$, $10 = 2$, $11 = 3$). With this encoding, we can view f as a function on 2-bit strings $f : \{0, 1\}^2 \to \{0, 1\}^2$. When refering to the elements of $\mathbb{Z}_4$, we use the notation $\{0, 1, 2, 3\}$ and $\{00, 01, 10, 11\}$ interchangeably.

   (a) Prove that every classical algorithm for solving this problem must make two queries.

   (b) Consider the 2-qubit unitary operation A corresponding to "add 1", such that $A|x\rangle = |x + 1\rangle$ for all $x \in \mathbb{Z}_4$. It is easy to check that

   $$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (1)$$

   Let $|\psi\rangle = \frac{1}{2}(|00\rangle + i|01\rangle + i^2|10\rangle + i^3|11\rangle)$, where $i = \sqrt{-1}$. Prove that $A|\psi\rangle = -i|\psi\rangle$.

   (c) Show how to create the state $\frac{1}{2}\big((-i)^{f(00)}|00\rangle + (-i)^{f(01)}|01\rangle + (-i)^{f(10)}|10\rangle + (-i)^{f(11)}|11\rangle\big)$ with a single query to U_f. (Hint: you may use the result in part (b) for this.)

   (d) Show how to solve the problem (i.e., determine the coefficient $a \in \mathbb{Z}_4$) with a single quantum query to f. (Hint: you may use the result in part (c) for this.)

3. **Can a function be evaluated at two points with one quantum query? [12 points; 4 each].** Here we consider the problem where we have a query oracle for a function $f : \{0,1\} \to \{0,1\}$ and the goal is to obtain information about both $f(0)$ and $f(1)$ with a single query. We assume that the query oracle is in the usual form of a unitary operator U_f that, for all $a, b \in \{0,1\}$, maps $|a\rangle|b\rangle$ to $|a\rangle|b \oplus f(a)\rangle$. For simplicity, we consider methods that employ only two qubits in all and are expressible by a circuit of the form

$|0\rangle$

V U_f W

$|0\rangle$

where V and W are two-qubit unitaries and the D-shaped gates are measurements in the computational basis. Therefore, it can be assumed that the input state to the query is a two-qubit state of the form $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

(a) For each of the four functions of the form $f : \{0,1\} \to \{0,1\}$, give the quantum state right after the query has been performed.

(b) If there is a measurement procedure that perfectly distinguishes between the four states in part (a) then they must be mutually orthogonal. Show that, for a measurement to be able to perfectly determine the value of $f(0)$, it must be the case that $\alpha_{10} = \alpha_{11}$. (Hint: think of the orthogonality relationships that need to hold.)

(c) Show that, if the states are such that $f(0)$ can be determined perfectly from them, then $f(1)$ cannot be determined with probability better than $1/2$ (which is no better than random guessing). (Hint: You may use the result in part (b) for this.)

4. **A qubit cannot be used to communicate a trit [15 points; 5 each].** Suppose that Alice wants to convey a trit of information (an element of $\{0,1,2\}$) to Bob and all she is allowed to do is prepare one qubit and send it to Bob. Bob is allowed to prepare $n-1$ additional qubits, each in state $|0\rangle$, and apply an n-qubit unitary U operation to the entire n qubit system followed by a measurement in the computational basis.

qubit from Alice $\qquad x_1 \mapsto f(x_1, \ldots, x_n) \in \{0,1,2\}$

$|0\rangle \qquad x_2$

U

$\vdots \qquad \vdots$

$|0\rangle \qquad x_n$

Bob's more complex measurement of a qubit

The outcome will be an element of $\{0,1\}^n$. It is conceivable that such a scheme exists where Bob can determine the trit from these n bits. We shall prove that this is impossible.

The framework is that Alice starts with a trit $j \in \{0,1,2\}$ (unknown to Bob) and, based on j, prepares a one-qubit state, $\alpha_j|0\rangle + \beta_j|1\rangle$, and sends it to Bob. In summary:

Alice's trit j	state that Alice sends to Bob
0	$\alpha_0\|0\rangle + \beta_0\|1\rangle$
1	$\alpha_1\|0\rangle + \beta_1\|1\rangle$
2	$\alpha_2\|0\rangle + \beta_2\|1\rangle$

Then Bob applies some n-qubit unitary U to $(\alpha_j|0\rangle + \beta_j|1\rangle)|00\ldots0\rangle$ and measures each qubit in the computational basis, obtaining some $x \in \{0,1\}^n$ as outcome. Finally, Bob applies some function $f : \{0,1\}^n \to \{0,1,2\}$ to x to obtain a trit. The scheme *works* if and only if, starting with any $j \in \{0,1,2\}$, the resulting x will satisfy $f(x) = j$.

(a) Note that each row of the matrix U is a 2^n-dimensional vector. For $j \in \{0,1,2\}$, define the space V_j to be the span of all rows of U that are indexed by an element of the set $f^{-1}(j) \subseteq \{0,1\}^n$. Prove that V_0, V_1, and V_2 are mutually orthogonal spaces.

(b) Explain why, for a scheme to work, $(\alpha_j|0\rangle + \beta_j|1\rangle)|00\ldots0\rangle \in V_j$ must hold for all $j \in \{0,1,2\}$.

(c) Prove that it is impossible for $(\alpha_j|0\rangle+\beta_j|1\rangle)|00\ldots0\rangle \in V_j$ to hold for all $j \in \{0,1,2\}$.

5. **A version of Simon's problem modulo p [12 points; 6 each].** Let p be some large n-bit prime number ($2^{n-1} < p < 2^n$) and assume that we are given a black box computing $f : \mathbb{Z}_p\times\mathbb{Z}_p \to \mathbb{Z}_p$ that is promised to have the property: $f(a_1,a_2) = f(b_1,b_2)$ if and only if $(a_1,a_2) - (b_1,b_2) \in S$, where $S = \{k(r_1,r_2) : k \in \mathbb{Z}_p\}$ for some unknown non-zero $(r_1,r_2) \in \mathbb{Z}_p\times\mathbb{Z}_p$ (*non-zero* means $(r_1,r_2) \neq (0,0)$). Our goal is to determine an (r_1,r_2) that generates S. Note that S does not uniquely determine (r_1,r_2) (for example, $(2r_1,2r_2)$ also generates the same S), so any non-zero multiple of (r_1,r_2) is an acceptable output.

   Also, assume that we have a good implementation of F_p, the quantum Fourier transform modulo p, and its inverse $F_p^\dagger$. Technically, F_p can be defined in a qubit setting as an n-qubit unitary operation (where on the basis states that are out of range, namely $|a\rangle$ with $a \in \{p,\ldots,2^n-1\}$, some other arbitrary unitary operation is applied).

   (a) Describe and analyze a quantum algorithm that makes a single query to the (reversible) black box for f and produces an $(s_1,s_2) \in \mathbb{Z}_p\times\mathbb{Z}_p$ with uniform probability from the set $S^\perp := \{(s_1,s_2) \in \mathbb{Z}_p\times\mathbb{Z}_p : \text{such that } (s_1,s_2)\cdot(r_1,r_2) = 0\}$.

   (b) Give a one-query quantum algorithm that, with success probability $1-1/p$, produces a non-zero multiple of (r_1,r_2). (Hint: you can build on the algorithm in part(a).)

6. **Optional challenge question for bonus credit [12 points].** Consider the variation of Question 2, 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 $a \in \mathbb{Z}_3$ (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 $x,y \in \mathbb{Z}_3$). 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) [3 points] Give a quantum algorithm that solves this problem with two queries to f.

   (c) [8 points] Prove that this problem cannot be solved by a quantum algorithm that makes only one query.