CSE 599d Quantum Computing Problem Set 1

Author: Dave Bacon (*Department of Computer Science & Engineering, University of Washington*)
Due: January 20, 2006

Exercise 1: Majorization and Random Permutations

Let $x = (x_1, x_2, \ldots, x_n)$ denote a vector of n real numbers, $x \in \mathbb{R}^n$. Define $x^\downarrow$ as the vector x sorted such that the components of the vector are in decreasing order, $x^\downarrow = (x_1^\downarrow, x_2^\downarrow, \ldots, x_n^\downarrow)$ where $x_1^\downarrow \geq x_2^\downarrow \geq \cdots \geq x_n^\downarrow$. Thus, for example, $x_1^\downarrow$ is the largest component of x. We say that the vector x is majorized by the vector y if $\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow$ for all $k < n$ (i.e. $k = 1, 2, \ldots, n-1$) and $\sum_{i=1}^n x_i^\downarrow = \sum_{i=1}^n y_i^\downarrow$. When x is majorized by y we write $x \prec y$.

(a) Suppose that $p \in \mathbb{R}^n$ is such that $p_i \geq 0$ and $\sum_{i=1}^n p_i = 1$ (we say that p is a vector of probabilities). There is a single vector of probabilities which is majorized by all other vectors of probabilities. What is this vector and prove that it is the only vector which has this property.

(b) An $n \times n$ matrix $A = (a_{ij})$ is called doubly stochastic if $a_{ij} \geq 0$ for all i and j, $\sum_{i=1}^n a_{ij} = 1$ for all j and $\sum_{j=1}^n a_{ij} = 1$ for all i. Show that every convex combination of a doubly stochastic matrices is a doubly stochastic matrix (recall that a convex combination of matrices $A_1, A_2, \ldots, A_m$ is a sum of these matrices, $\sum_{j=1}^m q_j A_j$ with $q_j \geq 0$ and $\sum_{j=1}^m q_j = 1$.)

(c) Prove that if $Ax \prec x$ for all x then A must be doubly stochastic (hint consider the vector from part (a) as well as vectors like $(0, 0, 1, 0, \ldots, 0)$.)

(d) Prove that if A is doubly stochastic then $Ax \prec x$ for all vectors x.

(e) Suppose that we have a machine with N configurations. One operation we can perform on such a system is to permute (map in a one-to-one manner) these configurations. Suppose that at any given time we apply one of $N!$ different permutations to the system with a fixed probability for each possible permutation. If p is a vector of probabilities describing our machine the evolution described by these random permutations is given by $q = Ap$ where q is the new description of our machine. Show that for process of applying random permutations, the matrix A is doubly stochastic. Can the vector of probabilities for a four state machine $[\frac{1}{12}\ \frac{1}{2}\ \frac{1}{12}\ \frac{1}{3}]^T$ ever evolve under one of these random permutations into the vector of probabilities $[\frac{1}{2}\ \frac{1}{6}\ \frac{1}{6}\ \frac{1}{6}]^T$? Why or why not?

The notion of majorization occurs naturally in various contexts. For example, in economics if $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ denote incomes of individuals $1, \ldots, n$, then $x \prec y$ would mean that there is a more equal distribution of incomes in the state x than in y. We will encounter majorization later when we talk about transformations on entangled quantum states.

Exercise 2: Paulis, Cliffords, and Toffolis

Recall that the single qubit Pauli operators are given by

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Elements of the *Pauli group* are made up of tensor products of n of the Pauli matrices, along with a phase i^k, where $k \in \{0, 1, 2, 3\}$. Elements of the Pauli group can be parameterized by two n bit strings, a and b along with $k = 0, 1, 2, 3$ as

$$P(a, b, k) = i^k (X^{a_1} Z^{b_1}) \otimes (X^{a_2} Z^{b_2}) \otimes \cdots \otimes (X^{a_n} Z^{b_n})$$

(a) Show that all elements of the Pauli group on n qubits, $P(a, b, k)$, are unitary.

(b) Show that $P(a, b, k)P(c, d, l) = (-1)^m P(c, d, k)P(a, b, l)$ where $m = \sum_{i=1}^n a_i d_i + \sum_{i=1}^n b_i c_i \bmod 2$. Thus you will have shown that any two elements of the Pauli group either commute $m = 0$ or anti-commute $m = 1$.

(c) Consider operators on n qubits of the form $R(P(a, b, k)) = \frac{1}{\sqrt{2}}(I + iP(a, b, k))$ where $P(a, b, k)$ is an element of the Pauli group. Show that if $P(a, b, k)$ is hermitian, then $R(P(a, b, k))$ is unitary. For the later parts of this problem, assume that $R(P(a, b, k))$ is indeed one of these unitary gates.

(d) Show that $R(P(a, b, k))P(c, d, l)R(P(a, b, k))^\dagger = P(c, d, l)$ if $P(a, b, k)$ commutes with $P(c, d, l)$.

(e) Show that $R(P(a, b, k))P(c, d, l)R(P(a, b, k))^\dagger = iP(a, b, k)P(c, d, l)$ if $P(a, b, k)$ anti-commutes with $P(c, d, l)$.

(f) The Toffoli gate on 3 qubits is a controlled-controlled-NOT gate. In the computational basis, it acts as

$$CC_X = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

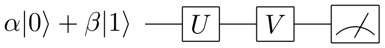
Show that no sequence of unitary operations $R(P(a,b,k))$ on 3 qubits can be used to reproduce the Toffoli gate (hint consider the effect of conjugating a Pauli operator by the Tofolli gate: $(CC_X)P(a,b,k)(CC_X)^\dagger$)

What you've demonstrated in the last part of this problem is that there is no way to use the R gates alone to perform a Tofolli gate. In fact, we will learn when we get to quantum error correction that the R gates are what are called Clifford gates and that they do not form a universal set of quantum gates.

Exercise 3: Distinguishing Paulis

Suppose we are given access to a black box which implements one of the four Pauli operators I, X, Y, Z (given explicitly in Exercise 2.) We don't know which of these four Pauli operators the box implements and confoundingly the black box explodes after we use it, so that we only get to use it one time! We will call the black box U (i.e. U is from the set $\{I, X, Y, Z\}$.)

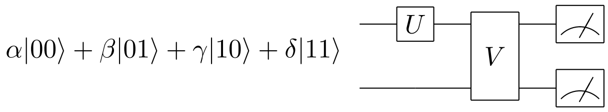
(a) Suppose that we are only allowed to use a single qubit pure state input into the black box, but that we can choose this single qubit state arbitrarily. After the black box U has acted, then we are allowed to make any single qubit unitary we wish and then measure in the computational ($|0\rangle$, $|1\rangle$) basis. In other words, we attempt to distinguish what U is by a circuit of the form



where V is an arbitrary unitary. Prove that it is impossible to choose a V and input $\alpha|0\rangle + \beta|1\rangle$ such that it is always possible to distinguish with perfect certainty which Pauli, I, X, Y, or Z, the black box U implements. This isn't as hard as it sounds.

(b) Show that $(P \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where P is one of the four single qubit Pauli matrices I, X, Y, or Z are orthogonal for the four different Ps.

(c) Now suppose that instead of the restricted circuit used in part (a), you are now allowed to input two-qubit states into the black box, then perform a two qubit gate after the evolution of the black box, and then perform a measurement in the computational basis. In other words the general circuit considered is now


$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$
U
V

where V is now a two-qubit unitary. Show that it is now possible to distinguish all for single qubit Paulis from each other with certainty by choosing the appropriate two qubit input state and two qubit unitary V.

What you've just demonstrated is that it is possible to use entangled quantum states to help distinguish between different unknown unitary gates. This idea, generalized, is one way to think about how quantum algorithms work.