**CS903 Quantum Computing and Quantum Information Theory**

# Final Exam

*Due Date : May 14, 2004*

1. A pure quantum state on $n$ qubits is said to be *separable* or *disentagled* if it can be written as a tensor product of single qubit states. A mixed state is said to be *unentangled* if it is a probability distribution over separable pure states. However, since different mixtures can be equivalent (i.e., have the same density matrix), a mixed quantum state that looks entangled, might actually be separable, since it might have an equivalent representation as a probability distribution over separable pure states.

   (a) Prove that the mixed state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with probability half and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ with probability half is a separable mixed state.

   (b) Challenge : Prove that the following state is separable : let $C \subseteq Z_2^n$ be a subgroup of the group $Z_2^n$. Consider a uniform mixture of coset states $|C + x\rangle$. Prove that this is a separable mixed state.

2. Consider a bipartite quantum state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Show that if $A$ performs an arbitrary unitary operation on her part of $|\psi\rangle$ and then $B$ measures his qubits in the standard basis, then the result of $B$'s measurement is independent of $A$'s actions.

   Now show that there is no measurement that $B$ can perform to tell which unitary operation $A$ performed on her qubits.

3. Generalize quantum teleportation to qutrits – $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$. (**Hint :** use a Fourier transform gate $F_3$ in place of Hadamard gate – $F_3$ maps the basis states of a qutrit as follows : $|j\rangle \rightarrow \sum_k \omega^{jk}|k\rangle$, where $w = e^{2\pi i/3}$ is the principal third root of unity. Also use the sum modulo 3 gate in place of the CNOT gate – this gate maps $|j\rangle \otimes |k\rangle$ to $|j\rangle \otimes |j + k \mod 3\rangle$).

4. Suppose you are given a $4-1$ function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, such that there exist $a \neq b$, $a, b \neq 0$ such that $f(x) = f(x+a) = f(x+b) = f(x+a+b)$. Give an efficient quantum algorithm to compute $a, b$.

5. Let $a|q$ and $b|q$. What is the Fourier transform mod$q$ of the uniform superposition on all $0 \leq x < q$ such that $a|x$ or $b|x$.

6. Consider the geometric series $\frac{1}{N}\sum_{j=1}^{N}\beta^j$, where $\beta \in \mathcal{C}$ has unit magnitude. If $\beta^N$ wraps around $k$ times (i.e., $N$ times the phase of $\beta$ is at least $2\pi k$), and if the phase of $\beta$ lies between 0 and $\pi$, then show that the sum is at most $k$.

7. Suppose $f(x + r) = f(x)$, and $0 \leq x < N$, for $N$ an integer multiple of $r$. Also suppose that you are given a unitary operator $U_y$ which performs the transformation $U_y|f(x)\rangle \rightarrow |f(x+y)\rangle$. Show how $U_y$ can be used to solve the period finding problem.

8. Show, in detail, the steps involved in factoring $N = 15$ using both Shor's and Kitaev's methods.

9. Consider the task of constructing a quantum circuit to compute $|x\rangle \rightarrow |x+y \ \ mod \ \ 2^n\rangle$, where $y$ is a fixed constant. Show that one efficient way of doing this, for values of $y$ such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of $y$ can be added this way, and how many operations are required?

10. Give a quantum algorithm for finding the minimum element in a list of $N$ numbers with query complexity $O(\sqrt{N} \log N)$.

11. Given a 2 to 1 function $f : [N] \rightarrow [N]$, we wish to find a collision pair, i.e., $x$ and $y$ such that $f(x) = f(y)$. Show that the quantum query complexity for this collision pair problem is $O(N^{1/3} \log N)$.

12. Give a linear time quantum algorithm for the following problem – given $N$ numbers $x_1, \ldots, x_N$, decide whether they are all distinct (i.e., no two of them are equal).

13. Consider the classical seven bit linear code $C_1$ defined by the following parity check matrix

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Let $C_2$ be the dual code of $C_1$, i.e., $C_2 = C_1^{\perp}$.

(a) Show that $C_2 \subseteq C_1$.

(b) What is the number of cosets of $C_2$ in $C_1$ ?

(c) How many errors can the CSS code constructed by these two codes correct ?

(d) How many qubits can be encoded using this CSS code ?

(e) Let $b$ and $f$ be two arbitrary seven bit strings. Let $E_b = X^{b_1} \otimes X^{b_2} \otimes \cdots \otimes X^{b_7}$ be an operator applying bit flips on those qubits in which the string $b$ is 1. Let $E_f$ be defined similarly but with phase flips. Consider the subspace in the Hilbert space of seven qubits which one gets when applying $E_b E_f$ to the $CSS$ code. How many errors can this subspace correct, when used as a quantum code ? How many qubits can it encode ?

## Some classical information theory.

1. Consider again the problem of finding the odd ball among a dozen balls where all the balls have the same weight except one, with as few as possible uses of a weighing machine that can tell us whether the balls on the left pan are heavier than those on the right, are equal in weight, or lighter.

(a) Convince yourself that the strategy discussed in the class is indeed optimal. Derive a lower bound for the problem using both information theoretic and combinatorial arguments.

(b) Some people argue that 'weighing six balls against six balls' is a good first weighing, some others say that 'no, weighing six against six gives no information at all'! Explain to each group why they are wrong by computing the information gained about *which is the odd ball* and *whether it is heavier or lighter*.

(c) Is it possible to solve the above problem using a sequence of three fixed weighings, such that the balls chosen for the second weighing do not depend on the first, and the third weighing does not depend on the first or the second?

(d) Suppose you have a bizzare two-pan balance that can report only two outcomes: 'the two sides balance' or 'the two sides do not balance'. Design a strategy to find the odd ball among 16.

(e) Find a solution to the general $N$ ball weighing problem in which exactly one of the $N$ balls is odd. Show that in $W$ weighings, an odd ball can identified from among $N = (3^W - 3)/2$ balls.

2. Suppose there are twenty-four people in a room.

(a) What is the probability that there are at least two people present who have the same birthday (i.e, one of the 365 days in a year, with apologies to leapyearians)?

(b) What is the expected number of pairs of people with the same birthday?

(c) Suppose we wish to convey a message to an outsider identifying one of the twenty-four people. We could simply communicate a number from $\mathcal{A}_S = \{1, 2, \ldots, 24\}$, alternatively, we could convey a number from $\mathcal{A}_X = \{1, 2, \ldots, 365\}$ conveying the person's birthday [the receiver is assumed to know everybody's birthdays]. What, roughly, is the probability of error of this communication scheme, assuming it is used for a single transmission? What is the capacity of the communication chaanel, and what is the rate of communication attempted by this scheme?