Introduction to Quantum Information Processing
(CS 467/667, C&0 481/681, PHYS 467/767)

Fall 2005

Assignment 3

Due date: December 1, 2005

1. **Converting quantum operations from unitary form to Krauss form.** In each case below, consider the one-qubit to one-qubit quantum operation that results from the following process. First, the input quantum state is extended by a one-qubit "ancilla" in state $|\psi\rangle$ (as given below), then a CNOT gate is applied to the two-qubit system (with the ancilla as target), and then the ancilla is discarded (i.e., traced out).

   For each case below, give a set of 2×2 matrices $A_1, \ldots, A_m$ satisfying $\sum_{k=1}^{m} A_k^\dagger A_k = I$ such that, for any input qubit with density matrix ρ, the density matrix of the corresponding output qubit is $\sum_{k=1}^{m} A_k \rho A_k^\dagger$.

   (a) $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

   (b) $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

   (c) $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

2. **Converting quantum operations from Krauss form to unitary form.** Since the matrices

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

   satisfy $A_1^\dagger A_1 + A_2^\dagger A_2 = I$, they define a two-qubit to two-qubit quantum operation that maps the state with density matrix ρ to the state with density matrix $A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger$. We explore this quantum operation here.

   (a) For each of the computational basis states, $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, give the corresponding output state of the operation.

   Based on your results so far, can you deduce whether or not the operation is unitary?

   (b) What is the output state for input state $\frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle)$? What about the output state for input state $\frac{1}{\sqrt{2}}|1\rangle(|0\rangle + |1\rangle)$? (Hint: in one case you should get a pure state and in the other case a mixed state.)

   (c) If you did part (a) correctly, the output for each computational basis state is also a computational basis state (possibly a different one). For computational basis states, give a simple boolean expression for each bit of the output state $|a'b'\rangle$ (where $a', b' \in \{0, 1\}$) in terms of the bits of the input state $|ab\rangle$ (where $a, b \in \{0, 1\}$).

   (d) Describe a unitary operation U acting on three qubits such that the quantum operation $\rho \mapsto A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger$ is equivalent to first extending the input state by an ancilla qubit in state $|0\rangle$, and then applying U to the three qubit system, followed by tracing out the third qubit. You may specify U in terms of its quantum circuit (for which a simple solution exists), or as an 8×8 matrix.

3. **Three-qutrit erasure code.** This question utilizes qutrits (basis states $|0\rangle$, $|1\rangle$, $|2\rangle$). We will use the two-qutrit gate SUM_3 that maps $|a\rangle|b\rangle$ to $|a\rangle|a+b \bmod 3\rangle$ and F_3, the one-qutrit Fourier transform modulo 3.

   Consider the following "encoding" of one-qutrit states

$$\begin{aligned}\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle \quad \mapsto \quad & \alpha(|000\rangle+|111\rangle+|222\rangle)\\ & +\beta(|012\rangle+|120\rangle+|201\rangle)\\ & +\gamma(|021\rangle+|102\rangle+|210\rangle).\end{aligned}$$

   (a) Explain how to compute the above encoding by adding a two-qutrit ancilla and using SUM_3 and F_3 gates. (Hint: if you're stuck then try again after doing part (b).)

   (b) Given an encoding (of some unknown pure state $\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle$) of the above form, what is the state that arises if one first performs a SUM_3 on the first two qutrits with the *second* qutrit as target and then another SUM_3 on the first two qutrits with the *first* qutrit as target?

   (c) Suppose that some unknown pure state $\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle$ is encoded in the above manner and that one of the three qutrits is then lost (thus we have two qutrits left and we know which ones they are—for example, they might be the first two qutrits). Show how to reconstruct the original state from any two of the three qutrits.

4. **Distinguishing between 1-to-3 balanced and zero.** For $n \geq 2$, call a function $f : \{0,1\}^n \to \{0,1\}$ *1-to-3 balanced*, if for 2^{n-2} values of x, $f(x) = 1$ and, for the remaining $3 \cdot 2^{n-2}$ values of x, $f(x) = 0$. (Thus the ratio of 1s to 0s for such an f is 1 to 3.) **Note:** this is different from 3-to-1 balanced, as defined in Assignment 2. Intuitively, a 1-to-3 balanced function is harder to distinguish from a zero function than a 3-to-1 balanced function is (since the two functions are different in fewer places). (Recall that a function $f : \{0,1\}^n \to \{0,1\}$ is *zero* if, for all x, $f(x) = 0$.)

   The *1-to-3 vs. zero* problem has as input a black-box computing a function $f : \{0,1\}^n \to \{0,1\}$ that is promised to be either 1-to-3 balanced or zero and the goal is to determine which of the two types f is.

   (a) How many queries to f must a classical algorithm make to solve 1-to-3 vs. zero with certainty on a worst-case input?

   (b) Show how, for the case where f is 1-to-3 balanced, the state

$$\frac{1}{\sqrt{2^{n-2}}} \sum_{\substack{x \in \{0,1\}^n \\ f(x)=1}} |x\rangle.$$

   can be exactly constructed from a single f-query. (Hint: try the approach used in Grover's algorithm to reach a satisfying assignment of f.)

   (c) Give a quantum algorithm that solves 1-to-3 vs. zero with *two* queries to f, with certainty on a worst-case input.

5. **Evolution of Hermitian operations.** Recall that, for any $d \times d$ Hermitian matrix A, e^{-iA} is a $d \times d$ unitary matrix (corresponding to evolution by the Hamiltonian A for one time unit).

   (a) Is $e^{-i(A+B)} = e^{-iA}e^{-iB}$ true in general? Either prove it or give a counterexample.

   (b) Is $e^{-i(A\otimes I)} = e^{-iA} \otimes I$ true in general? Either prove it or give a counterexample.

   (c) Is $e^{-i(A\otimes B)} = e^{-iA} \otimes e^{-iB}$ true in general? Either prove it or give a counterexample.