18.435/2.111 Homework # 3

Due Thursday, October 5

1: Suppose that you have an n-dimensional Hilbert space $\mathcal{H}_n$. Now, suppose that it is embedded into a d-dimensional Hilbert space $\mathcal{H}_d$ by adding $d-n$ basis vectors. Let $\mathcal{H}_d$ now be measured using with a projective measurement, projecting onto one of the subspaces Π_1, Π_2, Π_3, ..., $\Pi_k \in \mathcal{H}_d$. (So $\Pi_i \Pi_j = 0$ if $i \neq j$ and $\sum_{i=1}^{k} \Pi_i = I_d$, the $d \times d$ identity matrix). Let T be the $n \times d$ matrix

$$T = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \dots & 0 \end{pmatrix}$$

with n ones along a diagonal at the left, and the rest zero's.

1a: Show that if we define $E_i = T \Pi_i T^\dagger$, then

$$\sum_{i=1}^{k} E_i = I_n.$$

1b: Show that if $|\, v\rangle$ is a vector which is in the subspace of $\mathcal{H}_d$ generated by the first n basis vectors, then

$$\langle v \,|\, \Pi_i \,|\, v \rangle = \langle v \,|\, E_i \,|\, v \rangle .$$

1c: Suppose that we have a state $|\, \psi\rangle \in \mathcal{H}_d$ and first project the state either onto the space generated by the first n basis vectors (corresponding to the projection matrix $T^\dagger T$) or its complement. If we obtain the result that it is projected onto the first n basis vectors, we follow this measurement by a subsequent projective measurement using projectors Π_i. This sequence of measurements then has $k+1$ possible outcomes. Find a POVM with $k+1$ elements (Hermitian matrices) that is a single measurement giving the same probabilities of outcomes.

Problem 1 shows that the probability outcomes of a projective measurement on the larger quantum state space $\mathcal{H}_d$ can be mapped to a POVM measurement on $\mathcal{H}_n$. Problem 2 shows what can happen to the state vector during a POVM.

2: (Problem 2.64 in Nielsen and Chuang.) Suppose that $E = A^\dagger A$, where E and A are square matrices. Show that there is a unitary matrix U so that

$$UA = E^{1/2}$$

(and thus $UA\,|\,v\rangle = E^{1/2}\,|\,v\rangle$ for all $|\,v\rangle$).
Hint: You might want to use a basis where E is diagonal, and you might want to use the singular value decomposition[1].

Along with the techniques used in class, problems 1 and 2 can be used to prove that any POVM can be peformed by embedding the quantum space in a larger space, performing a projective measurement, and then applying a unitary transformation depending on the outcome of the projective measurement. I'm not going to make you do this as homework, but you've seen the hardest parts.

3. This is Nielsen and Chuang, problem 2.3. Prove Tsirelsen's inequality. Suppose Q, R, S and T are observables on a single qubit, each having two eigenvalues $\{-1, +1\}$. Prove that

$$(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 = 4I + [Q, R] \otimes [S, T],$$

where

$$[A, B] = AB - BA$$

is the *commutator* of A and B. Use this result to prove that

$$\langle Q \otimes S\rangle + \langle R \otimes S\rangle + \langle R \otimes T\rangle - \langle Q \otimes T\rangle \leq 2\sqrt{2}$$

This inequality shows that the amount of violation of local realism for the (second) example I gave in class is tight.

4. Do the first part of Exercise 4.25 from Nielsen and Chuang. This shows that Fredkin gates are not much more expensive to construct that Toffoli gates.
4a. Give a quantum circuit which uses three Toffoli gates to construct a Fredkin gate.
4b. Show that two of these Toffoli gates can be replaced by CNOT gates.

5. Suppose U is a one-qubit unitary. Find a circuit for a multiply controled U gate, controlled by $n-1$ qubits, which uses a linear number (in n) of gates and a sublinear number of work qubits. This is probably too open-ended as is, so I will post a hint sometime before Monday. Feel free to work on it without the hints, if you want a challenge.

[1]Nielsen and Chuang give the singular value decomposition only for square matrices. While these are enough for this exercise, the SVD is such a useful theorem you really should learn its statement for rectangular matrices as well.