18.435/2.111 Homework 4 Solutions

1: To define the change of basis operators, we wish to find $U_{x\to y}$ such that $U_{x\to y}|x+\rangle = |y+\rangle$ and $U_{x\to y}|x-\rangle = |y-\rangle$. Viewing this in terms of bras and kets, we should see the desired $U_{x\to y}$ (as well as $U_{z\to y}$) quite simply as:

$$U_{x\to y} = |y+\rangle\langle x+| + |y-\rangle\langle x-| = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{1}$$

$$U_{z\to y} = |y+\rangle\langle z+| + |y-\rangle\langle z-| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix} \tag{2}$$

Notice that I have written down the matrices in the $|z\pm\rangle$ basis, which is our standard computational basis.

There was a fair amount of confusion on the next section, so I will derive this very precisely, first in the general case. (Such a general derivation was not required for full credit on this problem.) Let $A_{ij} = \langle v_i| A |v_j\rangle$ be the matrix elements of the operator A in the $\{v_i\}$ basis. What we want are the matrix elements of A in the $\{w_i\}$ basis: $A'_{ij} = \langle w_i| A |w_j\rangle$. U be the change of basis operator to a basis $\{w_i\}$ (*i.e.* $w_i = Uv_i \Rightarrow U = \sum_i |w_i\rangle\langle v_i|$). We can write the matrix elements of U in the $\{v_i\}$ basis as $U_{ij} = \langle v_i| U |v_j\rangle = \langle v_i|w_j\rangle$.

Now to calculate A'_{ij}. We will write this out and twice use the trick of inserting a complete set of states $I = \sum_k |v_k\rangle\langle v_k|$.

$$\begin{aligned} A'_{ij} &= \langle w_i| A |w_j\rangle & (3) \\ &= \sum_{kl} \langle w_i|v_k\rangle \langle v_k| A |v_l\rangle \langle v_l|w_j\rangle & (4) \\ &= \sum_{kl} U^*_{ki} A_{kl} U_{lj}. & (5) \end{aligned}$$

The last line tells us how to use the matrix elements of the change of basis operator to convert A_{ij} in the $\{v_i\}$ basis to A'_{ij} in $\{w_i\}$. Since we're accustomed to seeing matrix equations instead of index sums, I will write this out as a matrix equation:

$$[A]_w = [U]_v^\dagger [A]_v [U]_v, \tag{6}$$

where I have used $[\cdot]$ to remind us that these are now matrices in the specified basis. (Notice that the † operator comes in the front.)

With the general framework in place, we can write down CNOT in the

$|y\pm\rangle$ basis. We know that $[CNOT]_z$ in the $|z\pm\rangle$ basis is given by

$$[CNOT]_z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{7}$$

We can change the basis by writing this as

$$\begin{aligned} [CNOT]_y &= [U_{z\to y} \otimes U_{z\to y}]_z^\dagger [CNOT]_z [U_{z\to y} \otimes U_{z\to y}]_z && (8) \\ &= \frac{1}{2}\begin{bmatrix} 1 & -i & 1 & i \\ i & 1 & -i & 1 \\ 1 & i & 1 & -i \\ -i & 1 & i & 1 \end{bmatrix} && (9) \end{aligned}$$

2: First, we show that $\|e_i\| \leq 1$. Let $|\hat{e}_i\rangle = |e_i\rangle / \|e_i\|$. Then

$$\begin{aligned} 1 &= \langle \hat{e}_i | \hat{e}_i \rangle = \langle \hat{e}_i | \left(\sum_k |e_k\rangle \langle e_k| \right) |\hat{e}_i\rangle && (10) \\ &= \sum_k \langle \hat{e}_i | e_k \rangle \langle e_k | \hat{e}_i \rangle = \|e_i\|^2 + \sum_{k\neq i} |\langle e_k | \hat{e}_i \rangle|^2 && (11) \\ &\geq \|e_i\|^2. && (12) \end{aligned}$$

Using the trace, we see that

$$\begin{aligned} n &= \mathrm{tr} I = \mathrm{tr} \sum_k |e_k\rangle \langle e_k| = \sum_k \langle e_k | e_k \rangle && (13) \\ &= \|e_1\|^2 + \|e_2\|^2 + \cdots + \|e_n\|^2 \leq n. && (14) \end{aligned}$$

The inequality at the end is a result of what we proved above. Obviously, we must achieve equality, which implies $\|e_i\| = 1$.

To prove orthogonality, we see that

$$\begin{aligned} 1 &= \langle e_i | e_i \rangle = \langle e_i | \left(\sum_k |e_k\rangle \langle e_k| \right) |e_i\rangle && (15) \\ &= 1 + \sum_{k\neq i} |\langle e_i | e_k \rangle|^2, && (16) \end{aligned}$$

which implies that $\langle e_i | e_k \rangle = \delta_{ik}$.

3a: If we define $A = \sum_i r_i E_i$, then the expected value of this observable when in state $|\psi\rangle$ is

$$\langle \psi | A | \psi \rangle = \sum_i r_i \langle \psi | E_i | \psi \rangle, \tag{17}$$

which is the desired result. We see that A is Hermitian by noting that each E_i is Hermitian and r_i is real.

3b: Let A and B be observables whose expected value is the same for all states $|\psi\rangle$ as the POVM in part (a). Then $\langle\psi| A |\psi\rangle = \langle\psi| B |\psi\rangle \Rightarrow \langle\psi| A - B |\psi\rangle = 0$ for all $|\psi\rangle$. This can only be true if $A - B = 0 \Rightarrow A = B$.

3c: There are two simple classes of examples. The first notes that a POVM on an n-dimensional system can have more than n elements. Since an observable can only have n outcomes, any such POVM cannot be duplicated by an observable. The second simple class of examples found cases where an n element POVM still yielded different outcomes. A simple example would be a POVM of elements

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & .5 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & .5 \end{bmatrix} \right\} \tag{18}$$

associated with outcomes $\{1, 0\}$ respectively. Notice that the corresponding observable is simply $\begin{bmatrix} 1 & 0 \\ 0 & .5 \end{bmatrix}$, which has outcomes $\{1, .5\}$ (the eigenvalues).

4a: Let's first do the Bell states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle$:

$$\begin{aligned} & \frac{1}{2}(\langle 00| \pm \langle 11|)M \otimes I(|00\rangle \pm |11\rangle) \\ = \; & \frac{1}{2}(\langle 0| M |0\rangle \langle 0|0\rangle \pm \langle 0| M |1\rangle \langle 0|1\rangle \pm \langle 0| M |1\rangle \langle 0|1\rangle + \langle 1| M |1\rangle \langle 1|1\rangle) \\ = \; & \frac{1}{2}(\langle 0| M |0\rangle + \langle 1| M |1\rangle). \end{aligned}$$

Similarly, for $\frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle$:

$$\begin{aligned} & \frac{1}{2}(\langle 10| \pm \langle 01|)M \otimes I(|10\rangle \pm |01\rangle) \\ = \; & \frac{1}{2}(\langle 0| M |0\rangle \langle 1|1\rangle \pm \langle 0| M |1\rangle \langle 1|0\rangle \pm \langle 0| M |1\rangle \langle 1|0\rangle + \langle 1| M |1\rangle \langle 0|0\rangle) \\ = \; & \frac{1}{2}(\langle 0| M |0\rangle + \langle 1| M |1\rangle). \end{aligned}$$

4b: The most general measurement Eve can make will be a POVM with elements of the form $\{E_i \otimes I\}$. The probability of any of these outcomes is given by $\langle B| E_i \otimes I |B\rangle$, where $|B\rangle$ is one of the Bell states. As we showed in (a), these probabilities are identical for any operator E_i, so Eve cannot distinguish anything about the state.