

Solution homework 3

Question a. No M does not satisfy all constraints (check column 3). We have $L_1 = L_2 = L_3 = 1$ and $C_1 = C_2 = C_3 = -1$ so $L_1 L_2 L_3 = 1$ and $C_1 C_2 C_3 = -1$. But $C_1 C_2 C_3 = L_1 L_2 L_3$, hence the contradiction.

Question b. Using the algebraic rules for Pauli matrices seen in the course, for instance:

$$\begin{aligned} (\sigma_x \otimes \sigma_x)(\sigma_y \otimes \sigma_y) &= (\sigma_x \sigma_y) \otimes (\sigma_x \sigma_y) \\ &= (-\sigma_y \sigma_x) \otimes (-\sigma_y \sigma_x) \\ &= (\sigma_y \sigma_x) \otimes (\sigma_y \sigma_x) \\ &= (\sigma_y \otimes \sigma_y)(\sigma_x \otimes \sigma_x) \end{aligned}$$

So the matrices in the box $(1,1)$ and $(2,1)$ commute. All other checks for commutation proceed similarly through these algebraic rules with Pauli matrices or explicit matrix product calculations.

Using also that the squares of Pauli matrices equal the identity matrix, we find that the product of observables in rows is $\mathbf{I} \otimes \mathbf{I}$ while it is $-\mathbf{I} \otimes \mathbf{I}$ in columns.

Question c. Essentially A and B have to agree on some prior filling of the magic square before playing, which is as good as possible, except for one box. It is easy to find one where the products of all three rows for Alice is fine (equal $+1$) and for Bob only two columns work out (say the first two). Now if the verifier asks to Bob his values in third column (with prob $1/3$) he has to flip one bit before sending his answer to the verifier. But then the verifier has a chance $1/3$ to ask to Alice for the values in the row where Bob flipped the bit. Then the bit in the intersection of row and column sent by Alice and Bob will not be the same and they lose the game.

One can see that with this strategy Alice and Bob will win if the bad box is not in the intersection of the row and column chosen by the verifier. So they can hope to win with probability $Prob(win) = 1 - \frac{1}{3} \cdot \frac{1}{3} = \frac{8}{9}$.

Question d. Let's take the case where V sends A the row index $i = 1$ and B the column index $j = 2$ (all other cases are similar). The observables on row $i = 1$ commute (as checked before) and thus Alice can indeed measure them simultaneously (meaning with the same apparatus or measurement basis). Similarly all observables on column $j = 2$ commute and thus B can measure them simultaneously (with the same apparatus or measurement basis). Now let's look at the outcome of the particular observable in box $(i = 1, j = 2)$. The shared state $|\Psi\rangle_{AB}$ is the tensor product of a Bell state $|\Psi^+\rangle_{A_1 B_1}$ and a Bell state $|\Psi^+\rangle_{A_2 B_2}$. Thus (given that they both measure $(i = 1, j = 2)$) the outcome state for qubit A_1 and B_1 is the same, and the outcome for qubit A_2 and B_2 is the same. The eigenvalue outcome is a common binary eigenvalue $\in \{+1, -1\}$ as we are dealing exclusively with Pauli matrices and the identity matrix.

More precisely we can check all this explicitly from many points of view.

Imagine Alice does a measurement. For the observable ($i = 1, j = 2$) in other words $\sigma_x \otimes I$ a good choice of eigenbasis for A is

$$|+\rangle_{A_1} \otimes |+\rangle_{A_2}, \quad |-\rangle_{A_1} \otimes |+\rangle_{A_2}, \quad |+\rangle_{A_1} \otimes |-\rangle_{A_2}, \quad |-\rangle_{A_1} \otimes |-\rangle_{A_2}$$

Note this basis diagonalises simultaneously all observables in the row $i = 1$. When A does the measurement the possible outcomes are (you can use that the state can be written $(|+\rangle_{A_1 B_1} + |-\rangle_{A_1 B_1}) \otimes (|+\rangle_{A_2 B_2} + |-\rangle_{A_2 B_2})$ to convince yourself)

$$|+\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |+\rangle_{B_2}$$

$$|-\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |+\rangle_{B_2}$$

$$|+\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |-\rangle_{B_2}$$

$$|-\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |-\rangle_{B_2}$$

with eigenvalue -1 . Other basis outcomes have probability zero. Inspecting these states we see that Alice and Bob each time get the same state. We also see that for each state $\sigma_x^{A_1} \otimes I^{A_2}$ and $\sigma_x^{B_1} \otimes I^{B_2}$ take the same value (eigenvalue). For the above measurement outcomes the common eigenvalues are respectively $(+1), (-1), (+1), (-1)$. Thus Alice and Bob will send the same eigenvalue to the verifier.

Imagine Bob does a measurement. Another way to see this is to think of the measurements Bob does. For Bob a good choice is

$$|+\rangle_{B_1} \otimes |0\rangle_{B_2}, \quad |+\rangle_{B_1} \otimes |1\rangle_{B_2}, \quad |-\rangle_{B_1} \otimes |0\rangle_{B_2}, \quad |-\rangle_{B_1} \otimes |1\rangle_{B_2}$$

This is a common eigenbasis of the observables in his column $j = 2$. The possible outcomes (again use the rotation invariance property of the Bell state) are

$$|+\rangle_{B_1} \otimes |0\rangle_{B_2} \otimes |+\rangle_{A_1} \otimes |0\rangle_{A_2}$$

$$|+\rangle_{B_1} \otimes |1\rangle_{B_2} \otimes |+\rangle_{A_1} \otimes |1\rangle_{A_2}$$

$$|-\rangle_{B_1} \otimes |0\rangle_{B_2} \otimes |-\rangle_{A_1} \otimes |0\rangle_{A_2}$$

$$|-\rangle_{B_1} \otimes |1\rangle_{B_2} \otimes |-\rangle_{A_1} \otimes |1\rangle_{A_2}$$

All other outcomes have probability zero. As before, inspecting these states we see that Alice and Bob each time get the same state. We also see that for each state $\sigma_x^{A_1} \otimes I^{A_2}$ and $\sigma_x^{B_1} \otimes I^{B_2}$ take the same value (eigenvalue). For the above measurement outcomes the common eigenvalues are respectively $(+1), (+1), (-1), (-1)$. Thus Alice and Bob will send the same eigenvalue to the verifier.

Imagine Alice and Bob do a "simultaneous" measurement, each of them in their above "good" basis. The global measurement basis is the tensor product of the above two basis: an 16 dimensional basis.

Let us compute the probability that Alice and Bob convey different eigenvalues to the verifier. We should hopefully find this probability is zero

$$Prob(\lambda_A \neq \lambda_B) = Prob(\lambda_A = +1, \lambda_B = -1) + Prob(\lambda_A = -1, \lambda_B = +1)$$

The first event $(\lambda_A = +1, \lambda_B = -1)$ correspond to the measurement outcomes

$$|+\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |0\rangle_{B_2}$$

$$|+\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |1\rangle_{B_2}$$

$$|+\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |0\rangle_{B_2}$$

$$|+\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |-\rangle_{B_1} \otimes |1\rangle_{B_2}$$

and the second event $(\lambda_A = -1, \lambda_B = +1)$ corresponds to the measurement outcomes

$$|-\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |0\rangle_{B_2}$$

$$|-\rangle_{A_1} \otimes |+\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |1\rangle_{B_2}$$

$$|-\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |0\rangle_{B_2}$$

$$|-\rangle_{A_1} \otimes |-\rangle_{A_2} \otimes |+\rangle_{B_1} \otimes |1\rangle_{B_2}$$

We can check (careful with the labels) that the inner product of all these states with the shared state

$$\frac{1}{\sqrt{2}}(|++\rangle_{A_1 B_1} + |--\rangle_{A_1 B_1}) \otimes \frac{1}{\sqrt{2}}(|++\rangle_{A_2 B_2} + |--\rangle_{A_2 B_2})$$

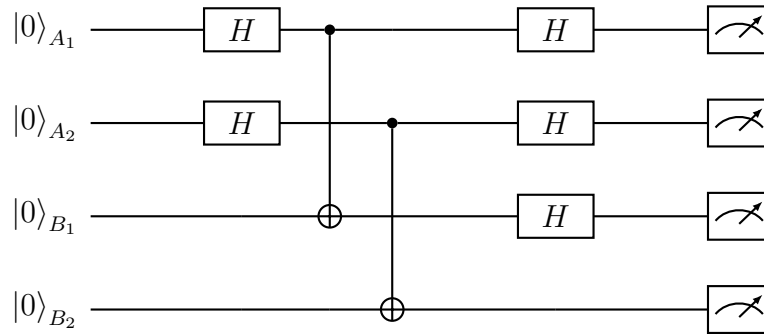
is zero. Thus $Prob(\lambda_A \neq \lambda_B) = 0$.

Question e. We just give the solution here for the case $i = 1, j = 2$. The two appropriate measurement basis have been given above. A quantum circuit uses (by convention) the computational measurement basis. So when we need another basis we have to find the unitary operator which makes the appropriate change of basis.

For Alice's side: $\langle++| = \langle 00|(H \otimes H)$, $\langle+-| = \langle 01|(H \otimes H)$, $\langle-+| = \langle 10|(H \otimes H)$, $\langle--| = \langle 11|(H \otimes H)$.

For Bob's side: $\langle+0| = \langle 00|(H \otimes \mathbf{I})$, $\langle+1| = \langle 01|(H \otimes \mathbf{I})$, $\langle-0| = \langle 10|(H \otimes \mathbf{I})$, $\langle-1| = \langle 11|(H \otimes \mathbf{I})$.

The following circuit first builds the two Bell states (Hadamard and control nots) and then makes the change of basis.



Remark that the general principle for the change of basis in a quantum circuit is the following:
If

$$|basis\rangle = U|computational\rangle$$

then in the circuit you put a gate $U^\dagger$ just before the measurement box.

Indeed note that the outcome probability of a measurement in a general basis is of the form

$$|\langle basis|\Psi\rangle|^2 = |\langle computational|U^\dagger|\Psi\rangle|^2$$

where $|\Psi\rangle$ is the state produced by the circuit just before the gate $U^\dagger$.

Of course in the above question $H^\dagger = H$ so you don't see this (dagger) subtlety.