Header styling inspired by CS 70: https://www.eecs70.org/

Problem 1

A source repeatedly generates two entangled qubits in the state $|\Omega\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$,

$$|\Omega\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle) \tag{1}$$

One qubit is sent to Alice and one to Bob.

a) When Alice measures her qubit in the standard Z basis, she instantaneously knows whether Bob, who may be miles away, will observe outcome 0 or 1 when he measures his qubit in the Z basis. Explain why these correlations cannot be used for instantaneous communication but they can be used for generating cryptographic keys.

Solution: This cannot be used for instantaneous communication becuase in order for that to occur, Alice would need to send her measurement to Bob via a *classical* channel, which still follows the rules of causality – hence, it cannot be instantaneous. Further, there is no extra information gained by Alice once she measures her own qubit, since there is no communication with Bob.

It can, however, be used to generate cryptographic keys, since Alice and Bob can together agree the basis in which they want to measure the state in, and a third party cannot possibly know this information. Furthermore, even if a third party knows this information, they cannot interfere with the entangled state itself, since upon measurement the state immediately collapses, a procedure which is detectable via the Bell inequalities. □

---

b) Show that for any two operations $A, B \in \mathcal{B}(\mathbb{C}^2)$, we have

$$\langle\Omega|A \otimes B|\Omega\rangle = \frac{1}{2}\operatorname{tr} A^\top B \tag{2}$$

Solution: To do this, let's write out the matrix element:

$$\langle\Omega|A \otimes B|\Omega\rangle = \frac{1}{2}(\,\langle 00| + \langle 11|)(A \otimes B)(\,|00\rangle + |11\rangle) = \frac{1}{2}\langle 00|A \otimes B|00\rangle + \langle 11|A \otimes B|11\rangle = \frac{1}{2}(a_0b_0 + a_1b_1)$$

which is equal to $\frac{1}{2}\operatorname{tr} A^\top B$, as desired. □

---

c) Let A and B be two observables measured by Alice and Bob, respectively,

$$A = \cos\alpha Z + \sin\alpha X, \text{ and } B = \cos\beta Z + \sin\beta X \tag{3}$$

where X and Z are the Pauli operators. Using b) show that

$$\langle\Omega|A \otimes B|\Omega\rangle = \cos(\alpha - \beta) \tag{4}$$

Show that the eigenvalues and thus the observable values of A and B are both ± 1. Hence, $A \otimes B$ is an observable that will take the value $+1$ when the measurement outcomes of A and B are the same and -1 otherwise. Using this show that the probability that the results registered by Alice and Bob upon measuring these observables are identical is $\cos^2(\frac{\alpha-\beta}{2})$.

Solution: Firstly, we know that given these operators, we can express A and B as:

$$A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \quad B = \begin{pmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{pmatrix}$$

Now, using the identity from the previous part, we know that $\langle\Omega|A\otimes B|\Omega\rangle$ is easily calculated by the equation on the right hand side:

$$\frac{1}{2}\operatorname{Tr}\big(A^\top B\big) = \cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\alpha-\beta)$$

To show that the eigenvalue of A and B are both ±1, we just have to solve $\det(A-\lambda I)=0$. Solving for A:

$$\det(A-\lambda I) = 0 = \begin{vmatrix}\cos\alpha-\lambda & \sin\alpha \\ \sin\alpha & -\cos\alpha-\lambda\end{vmatrix} = -(\cos\alpha-\lambda)(\cos\alpha+\lambda) - \sin^2\alpha = -(\cos^2\alpha-\lambda^2)-\sin^2\alpha$$

This simplifies to the equation

$$\lambda^2 = 1 \implies \lambda = \pm 1$$

Since B is the same matrix but with the angle β, it will have the same eigenvalues. Unfortunately, I couldn't really figure out the second part of this problem. It seems that one way to approach finding the probability is to find the eigenvectors of A (and also B), then look at how we can re-express $|\Omega\rangle$ in this new eigenbasis, then look at the probability that they measure the same value.

I had thought about doing this, but the computation was far too complex for me to believe like this was the intended solution method. One other thing I tried was to notice that

$$\cos^2\left(\frac{\alpha-\beta}{2}\right) = \frac{1+\cos(\alpha-\beta)}{2}$$

and somehow relate this equation to the matrix element, but I couldn't come up with an argument as to why this was true besides being a coincidence. □

---

d) Let A_1, A_2, B_1 and B_2 be the observables defined by using the angles $\alpha_1 = \frac{\pi}{2}$, $\alpha_2 = 0$, $\beta_1 = \frac{\pi}{4}$ and $\beta_2 = \frac{3\pi}{4}$ (respectively) in Eqs. 3. Alice and Bob perform a statistical test (known as the CHSH test) in which Alice repeatedly measures either A_1 or A_2, and Bob either B_1 or B_2. For each run they choose, randomly and independently from each other, which observable to measure, then check whether the following conditinos are satisfied by the measurement outcomes:

$$A_1 = B_1,\ \ A_1 = B_2,\ \ A_2 = B_1,\ \ A_2 \neq B_2 \tag{5}$$

In each run they are able to check only one of the four conditions depending on the pair of observables they choose to measure. Show that their probability P_s of success (i.e. the asymptotic fraction of runs in which they find that the outcomes agree with the conditions in Eq. (3)) is given by $P_s = \cos^2\frac{\pi}{8}$.

Note: The CHSH test described above can be performed using two devices, $\mathcal{A}$ and $\mathcal{B}$ with $\mathcal{A}$ being a "black box" of unkonwn design that has two settings A_1 nad A_2, and similarly for $\mathcal{B}$ with the settings being B_1 and B_2. At each run of the device $\mathcal{A}$ or $\mathcal{B}$ for a given setting, an outcome of ±1 is generated. The probability of success is achieved only when the strings correspond to the measurements on qubits in state $|\omega\rangle$, as described above (modulo some simple relabelling). The test is rigid - there is no other way to maximise the probability of success.

Solution: The way I reasoned this is as follows: regardless of which observable Alice and Bob choose, they are looking for a specific condition in order for the measurement to be considered a success (i.e. only one of the four equalities in eq. 5 is measured). Therefore, all we have to show is that the probability of all four of these events is identical and eqal to P_s. To do this, we use the formula given in part (c):

$$\begin{aligned}
P(A_1 = B_1) &= \cos^2\left(\frac{\pi}{8}\right) \\
P(A_1 = B_2) &= \cos^2\left(\frac{\pi/2 - 3\pi/4}{2}\right) = \cos^2\left(\frac{\pi}{8}\right) \\
P(A_2 = B_1) &= \cos^2\left(\frac{0-\pi/4}{2}\right) = \cos^2\left(\frac{\pi}{8}\right) \\
P(A_2 \neq B_1) &= 1 - P(A_2 = B_2) = 1 - \cos^2\left(\frac{0-3\pi/4}{2}\right) = 1-\sin^2\left(\frac{\pi}{8}\right) = \cos^2\left(\frac{\pi}{8}\right)
\end{aligned}$$

They all match and are equal to $P_s = \cos^2\left(\frac{\pi}{8}\right)$, as desired. □

---

e) Now on the other hand let us assume the two devices were classically preprogrammed and had predetermined values for A_1, A_2, B_1, B_2. In each round Alice and Bob i.i.d. at random inquire A_1 or A_2 and B_1 or B_2 respectively and check the corresponding condition out of the 4 conditions in (Eq. 5) What is the maximal average success probability for the two variables of a round to fulfill the corresponding condition in (Eq. 5)?

Solution: I'm assuming that Alice and Bob have no knowledge of the values of A_1, A_2 and B_1, B_2 (they can be preprogrammed, but hidden to Alice and Bob). Then, when they choose an observable, they are essentially getting an outcome of ± 1 with probability $\frac{1}{2}$ each. Thus, the probability they match is going to be either if they both get 0 with probability $\frac{1}{4}$, or both 1, with probability $\frac{1}{4}$. Thus, the maximal probability they can achieve classically is $P_s = \frac{1}{2}$. □

Problem 2

The Hadamard gate on one qubit may be written as

$$H = \frac{1}{\sqrt{2}}[(\,|0\rangle + |1\rangle)\,\langle 0| + (\,|0\rangle - |1\rangle)\,\langle 1|]$$

a) Show explicitly that the Hadamard transform on n qubits, $H^{\otimes n}$ may be written as

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} \,|x\rangle\, \langle y|$$

Solution: First, consider the Hadamard on one qubit:

$$H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Now, consider acting H on an arbitrary state $|x\rangle$:

$$H\,|x\rangle = \frac{|0\rangle + (-1)^x\,|1\rangle}{\sqrt{2}}$$

Writing it more suggestively to match the desired form:

$$H\,|x\rangle = \frac{(-1)^{0\cdot x}\,|0\rangle + (-1)^{1\cdot x}\,|1\rangle}{\sqrt{2}}$$

So, we can write it as follows:

$$H\,|x\rangle = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y}\,|y\rangle$$

Finally, multiplying both sides by $\langle x|$, we get:

$$H = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y}\,|y\rangle\, \langle x|$$

Now that we have it in this form, consider what happens when we try to act H on a product state of n qubits. Then, we'll basically have this form for every single qubit, and because it's a product state the normalization factors of $\frac{1}{\sqrt{2}}$ will multiply together. Therefore, on n qubits, we have:

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y}\,|y\rangle\, \langle x|$$

Which is the exact same form that we wanted in the problme statement. Note that x and y are swapped in my answer compared to what we want to show, but this is an artifact of how I labeled x and y. □

---

b) Write out the explicit 4x4 matrix for $H^{\otimes 2}$ (in the computational basis). Do this in two ways: First by explicitly taking the elementwise tensor product of the two 2x2 matrices $H \otimes H$. Secondly use the formula derived above for $n = 2$ and deduce all 16 matrix elements explicitly!

Solution: First, we'll compute $H \otimes H$, with the help of our good friend Mathematica:

$$H \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Now, the other way is:

$$H^{\otimes 2} = \frac{1}{\sqrt{2^2}} \sum_{x,y \in \{0,1\}^2} (-1)^{x \cdot y} |y\rangle \langle x|$$

This way of writing it out leverages the vectors $|y\rangle$ and $\langle x|$, which is convenient when we're working with states. So, instead I'm just going to look at the sign of $x \cdot y$ and match it with $H \otimes H$ that we have above. To do this, we'll use a 2D multiplication table, where the entry in each cell denotes $(-1)^{x \cdot y}$, where $x \cdot y$ denotes the bitwise inner product of x and y.

	00	01	10	11
00	1	1	1	1
01	1	-1	1	-1
10	1	1	-1	-1
11	1	-1	-1	1

Note that the sign is exactly the same as the Hadamard gate, as expected. □

Problem 3

Similarly to Quantum teleportation, where two bits are sent to communicate one qubit using the resource of entangled qubits at a distance, it is possible to send one qubit to communicate two bits, again by using the resource of distant entangled qubits.

The process starts out with an EPR pair that is shared between the sender (Alice) and receiver (Bob).

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle)$$

The first of the two qubits is Alice's, the second is Bob's.

Alice wants to send a two bit message to Bob, e.g., 00, 01, 10, or 11. To do so, she first performs an operation on her qubit which transforms to the EPR pair according to which message she wants to send:

After having applied these operations according to the 2 bit message alice wants to send to Bob, Alice sends/gives her physical qubit to Bob.

For a message 00: Alice applies I (i.e., does nothing)
For a message 01: Alice applies X
For a message 10: Alice applies Z
For a message 11: Alice applies XZ (i.e. applies Z then X)

a) Calculate the 4 different states of the two qubits that Bob now has corresponding to each of the possible message Alice sent.

Solution: We'll go down the list:

- For 00, Alice applies I, so the state remains unchanged:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle)$$

- For 01, Alice applies X, which transforms as:

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to |0\rangle$$

Therefore, the state is now:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|10\rangle + |01\rangle)$$

- For 10, Alice applies Z, which transforms as:

$$|0\rangle \to |0\rangle$$
$$|1\rangle \to -|1\rangle$$

Therefore, the state is now:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle)$$

- For 11, Alice applies Z then X, so therefore we have:

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to -|0\rangle$$

Therefore, the final state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|10\rangle - |01\rangle)$$

□

b) Show how Bob can now extract Alice's message (i.e. her two bits) from measurements on the two qubits via one of the following two options. Bob could do this directly using a quantum measurement in a good choice of basis for the measurement and translate the measurements into Alice's 2 bit message. Or bob could apply further gates to map the 4 different staets to the 4 corresponding messages in the computational basis (i.e. $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$).

Solution: Notice that the four states that we've created are the bell states, which form a basis on two qubits. Therefore, if we just measure Alice's 2 qubits in the bell basis, then we'd recover the messages. Specifically:

$$|\Phi^+\rangle \longrightarrow 00$$
$$|\Phi^-\rangle \longrightarrow 01$$
$$|\Psi^+\rangle \longrightarrow 10$$
$$|\Psi^-\rangle \longrightarrow 11$$

□
