CS/Ph120 Homework 1 Solutions

October 22, 2016

Problem 1: State discrimination

Suppose you are given two distinct states of a single qubit, $|\psi_1\rangle$ and $|\psi_2\rangle$.

(a) Argue that if there is a φ such that $|\psi_2\rangle = e^{i\varphi}|\psi_1\rangle$ then no measurement will distinguish between the two states: for any choice of a basis, the probabilities of obtaining either outcome will be the same when performing the measurement on $|\psi_1\rangle$ or on $|\psi_2\rangle$.

Assuming $|\psi_1\rangle$ and $|\psi_2\rangle$ can be distinguished, we are interested in finding the optimal measurement to tell them apart. Here we need to make precise our notion of "optimal". We would like to find a basis $\{|b_1\rangle, |b_2\rangle\}$ of $\mathbb{C}^2$ such that the expression

$$\Pr\left(|b_1\rangle \mid |\psi_1\rangle\right) + \Pr\left(|b_2\rangle \mid |\psi_2\rangle\right) = \left|\langle b_1|\psi_1\rangle\right|^2 + \left|\langle b_2|\psi_2\rangle\right|^2 \tag{1}$$

is maximized.

(b) Show that for the purposes of this problem we can assume without loss of generality that $|\psi_1'\rangle = |0\rangle$ and $|\psi_2'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, for some $\theta \in [0, \pi)$. That is, given any $|\psi_1\rangle, |\psi_2\rangle$, determine an angle θ such that, given a basis $\{|b_1'\rangle, |b_2'\rangle\}$ which maximizes (1) for the pair $(|\psi_1'\rangle, |\psi_2'\rangle)$, lets you recover a basis $\{|b_1\rangle, |b_2\rangle\}$ which achieves the same value in (1) when $(|\psi_1\rangle, |\psi_2\rangle)$ is being measured. Say explicitly how to determine θ from $(|\psi_1\rangle, |\psi_2\rangle)$ and how to recover $\{|b_1\rangle, |b_2\rangle\}$ from $\{|b_1'\rangle, |b_2'\rangle\}$.

(c) Show that the optimal basis $\{|b_1'\rangle, |b_2'\rangle\}$ will always be of the form

$$|b_1'\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle, \qquad |b_1'\rangle = \sin\varphi|0\rangle - \cos\varphi|1\rangle$$

for some angle $\varphi \in [0, 2\pi)$. (The reason this may not be immediate is that in general the coefficients of $|b_1'\rangle$ and $|b_2'\rangle$ in the standard basis may involve complex numbers.)

(d) Determine the optimal φ as a function of θ.

(e) Conclude: what is the maximum value of (1), as a function of the original states $|\psi_1\rangle$ and $|\psi_2\rangle$? What is the basis which achieves the optimum?

Solution: (Due to De Huang)

(a) For any basis $|b_1\rangle, |b_2\rangle$, we have

$$\mathbf{Pr}(|b_1\rangle \mid |\psi_2\rangle) = \left|\langle b_1|\psi_2\rangle\right|^2 = \left|\langle b_1|e^{i\varphi}|\psi_1\rangle\right|^2 = \left|e^{i\varphi}\langle b_1||\psi_1\rangle\right|^2 = \left|\langle b_1|\psi_1\rangle\right|^2 = \mathbf{Pr}(|b_1\rangle \mid |\psi_1\rangle),$$

$$\mathbf{Pr}(|b_2\rangle \mid |\psi_2\rangle) = \left|\langle b_2|\psi_2\rangle\right|^2 = \left|\langle b_2|e^{i\varphi}|\psi_1\rangle\right|^2 = \left|e^{i\varphi}\langle b_2||\psi_1\rangle\right|^2 = \left|\langle b_2|\psi_1\rangle\right|^2 = \mathbf{Pr}(|b_2\rangle \mid |\psi_1\rangle),$$

thus no measurement will distinguish between these two states.

(b) Given a distinguishable pair $(|\psi_1\rangle, |\psi_2\rangle)$, aussume that $\langle\psi_1|\psi_2\rangle = e^{i\phi}\cos\theta$ for some $\theta \in (0, \pi)$. We may also assume that $\phi = 0$ since adding a phase $e^{-i\phi}$ to $|\psi_1\rangle$ won't change the optimal solution. Let $|\psi_1^\perp\rangle$ be a state such that $\langle\psi_1|\psi_1^\perp\rangle = 0$, then it's obvious that $\left|\langle\psi_1^\perp|\psi_2\rangle\right| = \sin\theta$, since $\{|\psi_1\rangle, |\psi_1^\perp\rangle\}$ is a basis. By adding a proper phase to $|\psi_1^\perp\rangle$ we may further assume that $\langle\psi_1^\perp|\psi_2\rangle = \sin\theta$. Now consider the operator

$$U = |0\rangle\langle\psi_1| + |1\rangle\langle\psi_1^\perp|,$$

then it's easy to check that U is unitary and

$$U|\psi_1\rangle = |0\rangle \triangleq |\psi_1'\rangle, \quad U|\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle \triangleq |\psi_2'\rangle.$$

Provided that $\{|b_1'\rangle, |b_2'\rangle\}$ is a basis that maximizes (1) for the pair $(|\psi_1'\rangle, |\psi_2'\rangle)$, we may recover $\{|b_1\rangle, |b_2\rangle\}$ as

$$|b_1\rangle = U^*|b_1'\rangle, \quad |b_2\rangle = U^*|b_2'\rangle.$$

It's easy to check that $\{|b_1\rangle, |b_2\rangle\}$ is a basis, and we have

$$\begin{aligned}
\mathbf{Pr}(|b_1\rangle \mid |\psi_1\rangle) + \mathbf{Pr}(|b_2\rangle \mid |\psi_2\rangle) &= \left|\langle b_1|\psi_1\rangle\right|^2 + \left|\langle b_2|\psi_2\rangle\right|^2 \\
&= \left|\langle b_1'|UU^*|\psi_1'\rangle\right|^2 + \left|\langle b_2'|UU^*|\psi_2'\rangle\right|^2 \\
&= \left|\langle b_1'|\psi_1'\rangle\right|^2 + \left|\langle b_2'|\psi_2'\rangle\right|^2 \\
&= \mathbf{Pr}(|b_1'\rangle \mid |\psi_1'\rangle) + \mathbf{Pr}(|b_2'\rangle \mid |\psi_2'\rangle).
\end{aligned}$$

And for any basis $\{|\tilde{b}_1\rangle, |\tilde{b}_2\rangle\}$, we have

$$\begin{aligned}
\mathbf{Pr}(|\tilde{b}_1\rangle \mid |\psi_1\rangle) + \mathbf{Pr}(|\tilde{b}_2\rangle \mid |\psi_2\rangle) &= \left|\langle \tilde{b}_1|\psi_1\rangle\right|^2 + \left|\langle \tilde{b}_2|\psi_2\rangle\right|^2 \\
&= \left|\langle \tilde{b}_1|U^*|\psi_1'\rangle\right|^2 + \left|\langle \tilde{b}_2|U^*|\psi_2'\rangle\right|^2 \\
&= \mathbf{Pr}(U|\tilde{b}_1\rangle \mid |\psi_1'\rangle) + \mathbf{Pr}(U|\tilde{b}_2\rangle \mid |\psi_2'\rangle) \\
&\le \mathbf{Pr}(|b_1'\rangle \mid |\psi_1'\rangle) + \mathbf{Pr}(|b_2'\rangle \mid |\psi_2'\rangle) \\
&= \mathbf{Pr}(|b_1\rangle \mid |\psi_1\rangle) + \mathbf{Pr}(|b_2\rangle \mid |\psi_2\rangle).
\end{aligned}$$

Therefore the basis $\{|b_1\rangle, |b_2\rangle\}$ maximizes value (1) for the pair $(|\psi_1\rangle, |\psi_2\rangle)$.

(c) Let $|b_1'\rangle, |b_2'\rangle$ ba a basis that maximizes (1) for the pair $(|\psi_1'\rangle, |\psi_2'\rangle)$. It's easy to check that applying any phases to $|b_1'\rangle$ or $|b_2'\rangle$ will not change value (1). Thus without loss of generality, we may assume that

$$\begin{aligned}
|b_1'\rangle &= \cos\varphi|0\rangle + e^{i\alpha}\sin\varphi|1\rangle, \\
|b_2'\rangle &= \sin\varphi|0\rangle - e^{i\alpha}\cos\varphi|1\rangle,
\end{aligned}$$

for some $\varphi \in [0, 2\pi)$ and $\alpha \in [0, 2\pi)$ such that $(\cos\theta \sin\theta \cos\varphi \sin\varphi) \leq 0$ (otherwise we may take $\varphi \to \pi - \varphi$, $\alpha \to \alpha + \pi$). Then we have

$$\begin{aligned}
\mathbf{Pr}(|b_1'\rangle \mid |\psi_1'\rangle) + \mathbf{Pr}(|b_2'\rangle \mid |\psi_2'\rangle) &= \left|\langle b_1'|\psi_1'\rangle\right|^2 + \left|\langle b_2'|\psi_2'\rangle\right|^2 \\
&= \cos^2\varphi + |\cos\theta \sin\varphi - e^{-i\varphi} \sin\theta \cos\varphi|^2 \\
&= \cos^2\varphi + \cos^2\theta \sin^2\varphi + \sin^2\theta \cos^2\varphi \\
&\quad - \cos\theta \sin\theta \cos\varphi \sin\varphi (e^{i\alpha} + e^{-i\alpha}) \\
&\leq \cos^2\varphi + \cos^2\theta \sin^2\varphi + \sin^2\theta \cos^2\varphi \\
&\quad - 2\cos\theta \sin\theta \cos\varphi \sin\varphi.
\end{aligned}$$

Since we assume that $(\cos\theta \sin\theta \cos\varphi \sin\varphi) \leq 0$, we should always take $\alpha = 0$ so that the value is maximized. Then we have then wanted form

$$|b_1'\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle,$$

$$|b_2'\rangle = \sin\varphi|0\rangle - \cos\varphi|1\rangle.$$

(d) Using the result of (c), we have

$$\begin{aligned}
\mathbf{Pr}(|b_1'\rangle \mid |\psi_1'\rangle) + \mathbf{Pr}(|b_2'\rangle \mid |\psi_2'\rangle) &= \left|\langle b_1'|\psi_1'\rangle\right|^2 + \left|\langle b_2'|\psi_2'\rangle\right|^2 \\
&= \cos^2\varphi + (\cos\theta \sin\varphi - \sin\theta \cos\varphi)^2 \\
&= \cos^2\varphi + \sin^2(\varphi - \theta) \\
&= 1 + \frac{1}{2}[\cos(2\varphi) - \cos(2\varphi - 2\theta)] \\
&= 1 + \sin(\theta - 2\varphi) \sin\theta \\
&\leq 1 + \sin\theta.
\end{aligned}$$

Recall that we assume $(\cos\theta \sin\theta \cos\varphi \sin\varphi) \leq 0$, to make the inequality to become equality, we can take

$$\varphi = \frac{\theta}{2} + \frac{3\pi}{4}, \quad \theta \in (0, \pi).$$

Then the basis

$$\{|b_1'\rangle, |b_2'\rangle\} = \{\cos\varphi|0\rangle + \sin\varphi|1\rangle,\ \sin\varphi|0\rangle - \cos\varphi|1\rangle\}$$

maximizes value (1) for the pair $(|\psi_1'\rangle, |\psi_2'\rangle)$, and the maximum is $1 + \sin\theta$.

(e) Since $\cos\theta = |\langle\psi_1|\psi_2\rangle|$, the previous results conclude that the maximum of value (1) is

$$1 + \sin\theta = 1 + \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2},$$

and the basis that achieves the optimum is

$$\{|b_1\rangle, |b_2\rangle\} = \{U^*|b_1'\rangle, U^*|b_2'\rangle\},$$

where U is defined in (a) and $\{|b_1'\rangle, |b_2'\rangle\}$ is defined in (d).

Problem 2: Improving Wiesner's Quantum Money

Consider the following six single-qubit states:

$$\left\{ |\psi_1\rangle = |0\rangle\,,\ |\psi_2\rangle = |1\rangle\,,\ |\psi_3\rangle = |+\rangle\,,\ |\psi_4\rangle = |-\rangle\,,\ |\psi_5\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}},\ |\psi_6\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \right\}.$$

Suppose we create a money scheme in which each bit of a bill's serial number is encoded into one of these six states, chosen uniformly at random (so with probability 1/6 each) by the bank.

(a) Consider the attack on this scheme which attempts to copy the bill in the standard basis, using the unitary $U : |0\rangle\,|0\rangle \mapsto |0\rangle\,|0\rangle$, $U : |1\rangle\,|0\rangle \mapsto |1\rangle\,|1\rangle$. What is its success probability? Recall that the success probability is defined as

$$\sum_{k=1}^{6} \frac{1}{6} \Big| \big(\langle\psi_k| \otimes \langle\psi_k| \big)\, U \big(|\psi_k\rangle \otimes |0\rangle \big) \Big|^2.$$

What if we choose U to copy in the Hadamard basis instead?

(a) Can you improve on the attack described in the previous question? Give any attack that does better. [Bonus points: describe an attack with success probability 2/3.]

(b) Find a quantum money scheme which uses only four possible single-qubit states but is better than Wiesner's scheme (i.e. the scheme which uses the four states $\{|\psi_1\rangle = |0\rangle\,,\ |\psi_2\rangle = |1\rangle\,,\ |\psi_3\rangle = |+\rangle\,,\ |\psi_4\rangle = |-\rangle\}$), in the sense that the optimal attack has success probability $< 3/4$. (You do not need to prove completely formally that your scheme is better than Wiesner's, but describe the four states you would use, and argue why you think it would be better than Wiesner's.) *[Hint: Think about the Bloch sphere — use all the available space!]*

Solution: (Due to the TAs)

(a) By linearity, we can compute the action of U on all 6 quantum money states.

$$U : |\psi_1\rangle\,|0\rangle \mapsto |0\rangle\,|0\rangle\,; \qquad U : |\psi_2\rangle\,|0\rangle \mapsto |1\rangle\,|1\rangle$$
$$U : |+\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\right); \qquad U : |-\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle - |1\rangle\,|1\rangle\right)$$
$$U : |\psi_5\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle + i\,|1\rangle\,|1\rangle\right); \qquad U : |\psi_6\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle - i\,|1\rangle\,|1\rangle\right)$$

It is instructive to carry out each of the inner products in the sum by hand in full detail

$$\begin{aligned} &\langle 0|\,\langle 0|\,U\,|0\rangle\,|0\rangle \\ &= \langle 0|\,\langle 0|\,(U\,|0\rangle\,|0\rangle) \\ &= (\langle 0| \otimes \langle 0|)\,(|0\rangle \otimes |0\rangle) \\ &= \langle 0|0\rangle\,\langle 0|0\rangle = \boxed{1} \\ &|\langle\psi_1|\,\langle\psi_1|\,U\,|\psi_1\rangle\,|0\rangle|^2 = 1 \end{aligned} \qquad \begin{aligned} &\langle 1|\,\langle 1|\,U\,|1\rangle\,|1\rangle \\ &= \langle 1|\,\langle 1|\,(U\,|1\rangle\,|1\rangle) \\ &= (\langle 1| \otimes \langle 1|)\,(|1\rangle \otimes |1\rangle) \\ &= \langle 1|1\rangle\,\langle 1|1\rangle = \boxed{1} \\ &|\langle\psi_2|\,\langle\psi_2|\,U\,|\psi_2\rangle\,|0\rangle|^2 = 1 \end{aligned}$$

$$\begin{aligned}
&\langle +|\langle +|U|+\rangle|0\rangle \\
&= (\langle +|\langle +|)\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\langle +|0\rangle\langle +|0\rangle + \langle +|1\rangle\langle +|1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2\right) = \boxed{\frac{1}{\sqrt{2}}} \\
&|\langle\psi_3|\langle\psi_3|U|\psi_3\rangle|0\rangle|^2 = \frac{1}{2}
\end{aligned}$$

$$\begin{aligned}
&\langle -|\langle -|U|-\rangle|0\rangle \\
&= (\langle -|\langle -|)\frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\langle -|0\rangle\langle -|0\rangle - \langle -|1\rangle\langle -|1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}\right)^2 - \left(\frac{1}{\sqrt{2}}\right)^2\right) = \boxed{0} \\
&|\langle\psi_4|\langle\psi_4|U|\psi_4\rangle|0\rangle|^2 = 0
\end{aligned}$$

$$\begin{aligned}
&\langle\psi_5|\langle\psi_5|U|\psi_5\rangle|0\rangle \\
&= (\langle\psi_5|\langle\psi_5|)\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + i|1\rangle|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\langle\psi_5|0\rangle\langle\psi_5|0\rangle + i\langle\psi_5|1\rangle\langle\psi_5|1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}\right)^2 + i\left(\frac{i}{\sqrt{2}}\right)^2\right) = \boxed{\frac{1-i}{2\sqrt{2}}} \\
&|\langle\psi_5|\langle\psi_5|U|\psi_5\rangle|0\rangle|^2 = \frac{1}{4}
\end{aligned}$$

$$\begin{aligned}
&\langle\psi_6|\langle\psi_6|U|\psi_6\rangle|0\rangle \\
&= (\langle\psi_6|\langle\psi_6|)\frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\langle\psi_6|0\rangle\langle\psi_6|0\rangle - i\langle\psi_6|1\rangle\langle\psi_6|1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}\right)^2 - i\left(\frac{i}{\sqrt{2}}\right)^2\right) = \boxed{\frac{1+i}{2\sqrt{2}}} \\
&|\langle\psi_6|\langle\psi_6|U|\psi_6\rangle|0\rangle|^2 = \frac{1}{4}
\end{aligned}$$

The overall success probability is

$$\frac{1}{6}\left(1+1+\frac{1}{2}+0+\frac{1}{4}+\frac{1}{4}\right) = \boxed{\frac{1}{2}}. \tag{2}$$

WHat if we copy in the Hadamard basis instead? First, we define the copying map:

$$U' : |+\rangle|+\rangle \mapsto |+\rangle|+\rangle U' : |-\rangle|+\rangle \mapsto |-\rangle|-\rangle$$

We see that this definition is symmetric with respect to switching $|0\rangle$ with $|+\rangle$ and $|1\rangle$ with $|-\rangle$. This symmetry is given concretely by the Hadamard change of basis. Let's examine the action of H on our money states

$$H|\psi_1\rangle = |\psi_3\rangle \qquad H|\psi_2\rangle = |\psi_4\rangle \qquad H|\psi_5\rangle = -|\psi_5\rangle \qquad H|\psi_6\rangle = -|\psi_6\rangle \tag{3}$$

To see these identities visually, recall that H is the rotation by π about the $X+Z$ axis on the Bloch sphere. Note that since $H = H^\dagger$, the corresponding identities for bras hold.

$$\langle\psi_1|H = \langle\psi_3| \qquad \langle\psi_2|H = \langle\psi_4| \qquad \langle\psi_5|H = -\langle\psi_5| \qquad \langle\psi_6|H = -\langle\psi_6|$$

All of this suggests that we should be able to express U' in terms of U and H. Let's rewrite with the equations defining U' in terms of H and the standard basis.

$$U|0\rangle|0\rangle = |0\rangle|0\rangle \quad \Longrightarrow \quad U(H\otimes H)|+\rangle|+\rangle = (H\otimes H)|+\rangle|+\rangle \tag{4}$$

Multiplying both sides of this equation by $(H\otimes H)$ gives us that $(H\otimes H)U(H\otimes H)$ acts on $|+\rangle|+\rangle$ in the same way as U'. In fact, these two maps also have the same action on $|1\rangle|0\rangle$. Now we can apply this symmetry term-by-term:

$$\begin{aligned}|\langle\psi_k|\langle\psi_k|U'|\psi_k\rangle|+\rangle|^2 &= |\langle\psi_k|\langle\psi_k|(H\otimes H)U(H\otimes H)|\psi_k\rangle|+\rangle|^2 \\ &= |\langle\psi_{k'}|\langle\psi_{k'}|U|\psi_{k'}\rangle|0\rangle|^2\end{aligned}$$

The map $k \mapsto k'$ is the permutation given in (3). Therefore, we can derive the below equality by rearranging terms.

$$\frac{1}{6}\sum_{k=1}^{6}|\langle\psi_k|\langle\psi_k|U|\psi_k\rangle|0\rangle|^2 = \frac{1}{6}\sum_{k=1}^{6}|\langle\psi_k|\langle\psi_k|U'|\psi_k\rangle|0\rangle|^2 = \frac{1}{2}. \tag{5}$$

(b) For a scheme achieving $\frac{2}{3}$, see [1].

(c) Suppose that $|\psi\rangle$ and $|\phi\rangle$ have an angle of θ between them when considered as points on the Bloch sphere. Then $|\langle\psi|\phi\rangle|^2 = \cos^2\frac{\theta}{2}$. The spatial distance between the points is $2\sin\frac{\theta}{2}$. Therefore, any configuration which maximizes the sum of squares of pairwise distance between points on the Bloch sphere also minimizes the sum of pairwise overlaps of the corresponding qubits. In other words, this choice maximizes the distinguishability of the states. For four points, this arrangement is achieved by the tetrahedron.

For any attack scheme, say given by a cptp map T, the distinguishability of the $|\psi_k\rangle$ gives an upper bound on the distinguishability of the "copied" states $T(|\psi_k\rangle\langle\psi_k|)$.

Problem 3: Quantum Teleportation

In class we saw that the no-cloning theorem forbids us from copying arbitrary quantum states, i.e. implementing a unitary U that takes $|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle$ for any state $|\psi\rangle$.

(a) In general show that if there exists a unitary U taking $|\Psi\rangle \to |\Phi\rangle$, there must exist another unitary V independent of $|\Psi\rangle$ and $|\Phi\rangle$ that takes $|\Phi\rangle \to |\Psi\rangle$. In other words, no information is lost when applying a unitary to a quantum state.

(b) Suppose Alice holds a qubit in the state $|\psi\rangle = a|0\rangle + b|1\rangle$ and wants Bob to have that state as well. Why doesn't the following work? Alice measures her qubit in some basis of her choice, then prepares another qubit in the state she obtains and sends that to Bob. (Please answer without making explicit use of the no-cloning theorem.)

We now introduce a scheme by which Alice can prepare $|\psi\rangle$ on Bob's side without sending him her qubit—in fact, without sending any quantum information at all!—provided they share a Bell

state. To be precise, the initial setup is as follows: Alice holds $|\psi\rangle_S$, and Alice and Bob each have a qubit of

$$\left|\phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\big(\,|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B\,\big),$$

so that the joint state of all three qubits is

$$|\Psi\rangle_{SAB} = |\psi\rangle_S \otimes \left|\phi^+\right\rangle_{AB} = \big(a\,|0\rangle_S + b\,|1\rangle_S\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|00\rangle_{AB} + |11\rangle_{AB}\,\big). \tag{6}$$

(c) As with a single qubit, any state of a two-qubit system can be written in terms of an orthonormal basis, and also measured in such a basis. One example is the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Find a state $|\psi^-\rangle$ that, together with the following three states,

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \quad \left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB})$$
$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}),$$

$|\psi^-\rangle$ forms an orthonormal basis of the two-qubit space $\mathbb{C}^4$. This basis is called the *Bell basis*.

(d) Rewrite the joint state (6) as a linear combination of the form $\sum_{i=1}^4 |\alpha_i\rangle_{SA}\,|\beta_i\rangle_B$, where $|\alpha\rangle$ ranges over the four possible Bell states on Alice's two qubits S and A, and $|\beta\rangle$ is a single-qubit state on Bob's qubit.

(e) Suppose Alice measures her two qubits SA in the Bell basis and sends the result to Bob. Show that for each of the four possible outcomes, Bob can use this (classical!) information to determine a unitary, independent of $|\psi\rangle_S$, on his qubit that will map it, in all cases, to the original state $|\psi\rangle_B$ that Alice had.

Solution: (Due to Mandy Huang)

(a) Suppose there exists a unitary U mapping $|\Psi\rangle \to |\Phi\rangle$. Since U is unitary, we have $U^{-1} = U^*$ is unitary, so the operator $V := U^*$ is a unitary operator which maps $|\Phi\rangle \to |\Psi\rangle$.

(b) If Alice measures $|\psi\rangle$ in a basis of her choice, then $|\psi\rangle$ will collapse to some eigenstate of the basis so if she reproduces this state and sends it to Bob, Bob will have a state that is different than the original state unless $|\psi\rangle$ happens to be an element of the basis in which Alice is measuring.

(c) Let $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Then

$$\langle\psi^\pm|\psi^\pm\rangle = \frac{1}{2}(1+1) = 1 \quad \langle\phi^\pm|\phi^\pm\rangle = \frac{1}{2}(1+1) = 1$$
$$\langle\psi^\mp|\psi^\pm\rangle = \frac{1}{2}(1-1) = 0 \quad \langle\phi^\mp|\phi^\pm\rangle = \frac{1}{2}(1-1) = 0$$
$$\langle\psi^+|\phi^\pm\rangle = 0 \quad \langle\phi^+|\psi^\pm\rangle = 0$$

(d) Note

$$|\Psi\rangle_{SAB} = (a|0\rangle_S + b|1\rangle_S) \otimes \frac{1}{\sqrt{(2)}}(|00\rangle_{AB} + |11\rangle_{AB})$$
$$= \frac{1}{\sqrt{2}}(a|000\rangle_{SAB} + b|100\rangle_{SAB} + a|011\rangle_{SAB} + b|111\rangle_{SAB})$$

and

$$\frac{1}{2}\left(|\phi^+\rangle + |\phi^-\rangle\right) = \frac{1}{\sqrt{2}}|00\rangle \qquad \frac{1}{2}\left(|\phi^+\rangle - |\phi^-\rangle\right) = \frac{1}{\sqrt{2}}|11\rangle$$
$$\frac{1}{2}\left(|\psi^+\rangle + |\psi^-\rangle\right) = \frac{1}{\sqrt{2}}|01\rangle \qquad \frac{1}{2}\left(|\psi^+\rangle - |\psi^-\rangle\right) = \frac{1}{\sqrt{2}}|10\rangle$$

Then we have

$$|\Psi\rangle_{SAB} = \frac{1}{2}\left(a\left(|\phi^+\rangle + |\phi^-\rangle\right)|0\rangle + b\left(|\psi^+\rangle - |\psi^-\rangle\right)|0\rangle + a\left(|\psi^+\rangle + |\psi^-\rangle\right)|1\rangle + b\left(|\phi^+\rangle - |\phi^-\rangle\right)|1\rangle\right)$$
$$= \frac{1}{2}\left(|\phi^+\rangle(a|0\rangle + b|1\rangle) + |\phi^-\rangle(a|0\rangle - b|1\rangle) + |\psi^+\rangle(b|0\rangle + a|1\rangle) + |\psi^-\rangle(-b|0\rangle + a|1\rangle)\right)$$

(e) From part (d) The possible outcomes are $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, and $|\psi^-\rangle$ in which case Bob's qubit is $a|0\rangle + b|1\rangle$, $a|0\rangle - b|1\rangle$, $b|0\rangle + a|1\rangle$, and $-b|0\rangle + a|1\rangle$, respectively.

If Alice measures $|\phi^+\rangle$ then Bob should apply the identity.
If Alice measures $|\phi^-\rangle$ then Bob should apply $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
If Alice measures $|\phi^-\rangle$ then Bob should apply $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
If Alice measures $|\phi^-\rangle$ then Bob should apply $ZX = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

References

[1] Abel Molina, Thomas Vidick, and John Watrous. "Optimal counterfeiting attacks and generalizations for Wiesner's quantum money". In: *Conference on Quantum Computation, Communication, and Cryptography*. Springer. 2012, pp. 45–64.