
Problem set 2 — Solutions

CSE 534 Autumn 2026

Problem 1.

1. The bank looks up $L(s) = (a, b)$ (rejecting if not listed) and measures qubit i in the computational basis if $b_i = 0$, or the Hadamard basis if $b_i = 1$. It accepts exactly when every outcome is a_i . Equivalently, it measures the POVM $\{\Pi_s, \mathbb{I} - \Pi_s\}$, where $\Pi_s = |\psi_s\rangle\langle\psi_s|$. On acceptance, the returned state is $|\psi_s\rangle$.
2. Let $|\phi\rangle$ be Alice's purported bill. For a fixed choice of $|\psi_s\rangle$, the probability that the bank accepts is

$$\Pr[\text{accept} \mid \psi_s] = |\langle\phi|\psi_s\rangle|^2 = \langle\phi|\psi_s\rangle\langle\psi_s|\phi\rangle. \quad (1)$$

Averaging over the bank's uniformly random choices of a, b , the overall success probability (using linearity) is

$$\Pr[\text{accept}] = \langle\phi| \left(\mathbb{E}_{a,b} [|\psi_s\rangle\langle\psi_s|] \right) |\phi\rangle. \quad (2)$$

Recall that $|\psi_s\rangle = \bigotimes_{i=1}^n H^{b_i} |a_i\rangle$. Thus, the projector $|\psi_s\rangle\langle\psi_s|$ is a tensor product of the individual qubit projectors. Since the pairs (a_i, b_i) are sampled independently, the expectation factors as

$$\begin{aligned} \mathbb{E}_{a,b} [|\psi_s\rangle\langle\psi_s|] &= \bigotimes_{i=1}^n \mathbb{E}_{a_i, b_i} [H^{b_i} |a_i\rangle\langle a_i| H^{b_i}] \\ &= \bigotimes_{i=1}^n \frac{|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|}{4} \\ &= \bigotimes_{i=1}^n \frac{\mathbb{I}}{2} = \frac{\mathbb{I}}{2^n}. \end{aligned} \quad (3)$$

Substituting back, we obtain

$$\Pr[\text{accept}] = \langle\phi| \frac{\mathbb{I}}{2^n} |\phi\rangle = 2^{-n}. \quad (4)$$

Therefore, Alice's success probability is at most 2^{-n} , independently of her choice of $|\phi\rangle$.

Part 3. The CNOT gate simultaneously clones $|0\rangle$ and $|1\rangle$, since $\text{CNOT} |00\rangle = |00\rangle$ and $\text{CNOT} |10\rangle = |11\rangle$. Now consider the quantity

$$F(U) = |\langle 0, 0 | U | 0, 0 \rangle|^2 + |\langle +, + | U | +, 0 \rangle|^2. \quad (5)$$

Since each term is at most 1, we have $F(U) \leq 2$. Equality would require U to perfectly clone both $|0\rangle$ and $|+\rangle$ (up to global phases). However, unitaries preserve the absolute value of inner products, whereas

$$|\langle 0, 0 | +, 0 \rangle| = \frac{1}{\sqrt{2}} \neq \frac{1}{2} = |\langle 0, 0 | +, + \rangle|. \quad (6)$$

Thus, $F(U) < 2$ for every unitary U . Therefore, $\max_{U \text{ unitary}} F(U) < 2$. The remaining two cloning fidelities are each at most 1, so we conclude that

$$\boxed{\max_{U \text{ unitary}} \sum_{|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}} |\langle \phi, \phi | U | \phi, 0 \rangle|^2 < 4.} \quad (7)$$

3. For each $i = 1, \dots, n$, apply X_i to the genuine bill and submit it for verification. If $b_i = 1$, then $X_i |\psi_s\rangle = \pm |\psi_s\rangle$, so the bank accepts with certainty since the global phase is not detected. If $b_i = 0$, the state $X_i |\psi_s\rangle$ is orthogonal to $|\psi_s\rangle$, so the bank rejects with certainty. Therefore, in either case, the bank's measurement does not change the state. Thus the verdict reveals b_i with certainty. In the rejection case the bank returns $X_i |\psi_s\rangle$, which we restore by applying X_i again; on acceptance it already returns $|\psi_s\rangle$.

After n such tests, measure each qubit in its known basis b_i to learn a_i without disturbing the bill. Prepare a second copy $\bigotimes_i H^{b_i} |a_i\rangle$. This produces two genuine bills with certainty, using n bank queries and $O(n)$ total operations.

5. We construct a subroutine for learning the basis bit b_i for each $i = 1, \dots, n$. Learning the basis bit requires introducing a new “probe qubit”. The probe qubit will slowly pivot like the state in a bomb tester experiment. Let R_θ be the rotation unitary used in class and apply the controlled rotation (bill qubit i first, probe second)

$$U_i = |0\rangle\langle 0|_i \otimes \mathbb{I} + |1\rangle\langle 1|_i \otimes R_\theta. \quad (8)$$

Let m be an integer we specify later and set $\theta = \pi/m$. Our algorithm for learning b_i is

Initialize the probe to $|0\rangle$, and repeat m times: apply U_i , submit the bill for verification, and stop if the bank rejects. If every verification accepts, measure the probe in the computational basis.

If $b_i = 0$: The bill qubit is $|0\rangle$ or $|1\rangle$. Inductively, argue that after t iterations the state of the bill and the probe is exactly

$$\bigotimes_i (H^{b_i} |a_i\rangle) \otimes R_{a_i t \theta} |0\rangle. \quad (9)$$

Notice that the probe and the bill are always unentangled and the bill never changes. Thus the bank always accepts and the final probe is $|0\rangle$ or $R_{m\theta}|0\rangle = -|0\rangle$. Its outcome is 0 with certainty.

If $b_i = 1$: The bill qubit is $|+\rangle$ or $|-\rangle$. Suppose current state of bill and probe is $|\psi_s\rangle \otimes R_Y|0\rangle$ for some γ . After applying U_i , the other qubits of the bill will remain unentangled and the joint state of the bill qubit and probe becomes

$$U_i(H|a_i\rangle \otimes R_Y|0\rangle) = \frac{1}{\sqrt{2}} (|0\rangle \otimes R_Y|0\rangle + (-1)^{a_i} |1\rangle \otimes R_{\theta+\gamma}|0\rangle) \quad (10)$$

with unentanglement with the remainder of the bill. When the bank measures and accepts the bill, it projects the bill back onto $|\psi_s\rangle$, removing any entanglement with the probe. The resulting unnormalized state of the probe is

$$(\langle a_i| H \otimes \mathbb{I}) \frac{1}{\sqrt{2}} (|0\rangle \otimes R_Y|0\rangle + (-1)^{a_i} |1\rangle \otimes R_{\theta+\gamma}|0\rangle) \quad (11)$$

$$= \frac{1}{2} (\langle 0| \otimes \mathbb{I} + (-1)^{a_i} \langle 1| \otimes \mathbb{I}) (|0\rangle \otimes R_Y|0\rangle + (-1)^{a_i} |1\rangle \otimes R_{\theta+\gamma}|0\rangle) \quad (12)$$

$$= \frac{1}{2} (R_Y|0\rangle + R_{\gamma+\theta}|0\rangle) \quad (13)$$

$$= \cos \frac{\theta}{2} \cdot R_{\gamma+\theta/2}|0\rangle. \quad (14)$$

Thus the probability of acceptance is

$$\Pr[\text{accept}] = \cos^2(\theta/2), \quad (15)$$

and conditioned on acceptance, the probe is in state $R_{\gamma+\theta/2}|0\rangle$. In other words, each successful verification rotates the probe by $\theta/2$, rather than θ . Starting with the probe in $|0\rangle$, after m successful rounds its state is

$$R_{m\theta/2}|0\rangle = R_{\pi/2}|0\rangle = |1\rangle, \quad (16)$$

where $\theta = \pi/m$. Hence the probe measurement returns 1 with certainty, conditioned on avoiding jail. Since the probability of acceptance in each round is $\cos^2(\theta/2)$, the probability of being sent to jail during these m rounds is

$$\begin{aligned} \Pr[\text{jail}] &= 1 - \cos^{2m}(\theta/2) \\ &\leq m \sin^2(\theta/2) \\ &\leq \frac{\pi^2}{4m}. \end{aligned} \quad (17)$$

Combining the two cases, conditioned on avoiding jail, outcome 0 identifies $b_i = 0$ and outcome 1

identifies $b_i = 1$ exactly. Moreover, each successful verification restores the original bill to $|\psi_s\rangle$, so we can reuse it to learn the remaining basis bits.

For a total risk of ϵ , bound the probability of jail in each round to be ϵ/n . So choose m such that $\pi^2/(4m) \leq \epsilon/n$. Then, the algorithm is to repeat this procedure for all n qubits, using a fresh probe each time. Conditioned on avoiding jail, we know the entire basis string b exactly and retain the original bill $|\psi_s\rangle$. We can measure each qubit in its known basis to recover a without disturbing the bill, then prepare a second copy of $\bigotimes_{i=1}^n H^{b_i} |a_i\rangle$. Thus, whenever jail is avoided, both bills are exact. The procedure uses at most $nm = \boxed{O(n^2/\epsilon)}$ bank queries and elementary operations which also bounds the running time.