
Problem set 2

CSE 534 Autumn 2026

Due date: October 16th 5:00 pm

Instructions: Solutions should be legibly handwritten or typeset. Mathematically rigorous solutions are expected for all problems unless explicitly stated. You are encouraged to collaborate on problems in small teams; however, each team member must write and submit their own individual solution. Read the AI tools policy on the course webpage and adhere to it. For grading purposes, start each problem on a new page.

Problem 1 (Wiesner’s quantum money). In this problem, we are going to study a cryptographic scheme developed by Wiesner for information-theoretically unclonable money. Wiesner was annoyed by the fact that paper money was counterfeitable—given enough time and resources, one could emulate a dollar bill exactly. This also holds for any notion of a “bill” being a classical string; copying is easy. Wiesner wanted 3 key properties for any purported currency:

- **Verifiability:** Anyone can take a purported bill to the bank that issued it, and the bank has a method for verifying its legitimacy.
- **Transferability:** A bill can be transferred from Alice to Bob without the bank being involved. If Alice’s bill was legitimate, then Bob has a legitimate bill as well.
- **Unclonability:** It should be computationally intractable to generate two valid bills from one valid bill.

Today we will study Wiesner’s scheme, which attempts to achieve all 3 properties using quantum information. The idea is that each bill consists of a classical string s and a quantum state $|\psi_s\rangle$. Anyone can read the classical string s and so it is easy to duplicate, but the quantum state $|\psi_s\rangle$ should be considerably harder to duplicate. In what follows, n will be the size of the quantum bill measured in number of bits/qubits.

To issue a bill, the bank chooses a fresh public serial number $s \in \{0, 1\}^n$ and independently and uniformly chooses two secret strings $a, b \in \{0, 1\}^n$. It prepares the state

$$|\psi_s\rangle \stackrel{\text{def}}{=} \bigotimes_{i=1}^n H^{b_i} |a_i\rangle.$$

A *bill* is the pair $(s, |\psi_s\rangle)$. The bank keeps a private classical ledger of each serial number s and the corresponding secret strings $L : s \mapsto (a, b)$. An equivalent way of looking at the state $|\psi_s\rangle$ is that each of the n qubits of $|\psi_s\rangle$ is chosen i.i.d. from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The bank knows the sequence of qubits from the classical information (a, b) , but the owner of the bill only knows s .

1. **(1 point)** Write down a description of how a bank verifies a purported bill $(s, |\psi\rangle)$.

2. **(2 points)** Say Alice knows that the bank has issued a bill with serial number s but does not have the corresponding quantum state. Argue an upper bound on the success probability of Alice generating a state $|\psi\rangle$ such that $(s, |\psi\rangle)$ is accepted by the verification procedure. Your bound should scale like c^n for some constant $c < 1$.

Hint: Observe that

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|}{4} = \frac{\mathbb{I}}{2}.$$

3. **(2 points)** We say a unitary clones a single-qubit state $|\phi\rangle$ if $U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$. Show that there exists a unitary that simultaneously clones $|0\rangle$ and $|1\rangle$, but show that there does not exist a unitary that simultaneously clones $|0\rangle, |1\rangle, |+\rangle$, and $|-\rangle$. This is known as the no-cloning theorem.

For full credit, prove that

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

(Optional challenge) show that the maximum achieves a value of $\frac{3}{2} + \sqrt{2}$.

The no-cloning theorem suggests that duplicating a quantum bill $(s, |\psi_s\rangle)$ should be difficult. In fact, a stronger quantitative statement holds: the optimal probability of producing two bills from one genuine bill such that both pass the bank's verification is c^n for some constant $c < 1$. Note the exponential scaling—this gets progressively harder as the security parameter increases. This probability is averaged over the bank's random choice of secret strings and all measurement outcomes. The bound holds even for an attacker with unlimited computation, provided that the attacker starts with only one genuine bill and cannot query the bank during the counterfeiting procedure.

Proving this statement requires more than applying the single-qubit no-cloning theorem separately to each qubit: an attacker might act jointly on all the qubits and introduce auxiliary registers. Later in the course, we will introduce density matrices, which provide a convenient language for describing and analyzing such general attacks. You are not asked to prove the bound here, but we invite you to return to this question once we have developed that language.

For now, let us note a key assumption required in this security guarantee: the attacker cannot query the bank while preparing the counterfeit bills. What happens when we give the attacker access to the bank's verification procedure? In the next part of this problem, we will see that counterfeiting security does not hold if the attacker is allowed to query the bank's verification procedure.

Imagine that you start with one genuine bill $(s, |\psi_s\rangle)$. Your goal is to produce two genuine bills with the same serial number: two registers in the joint state $|\psi_s\rangle \otimes |\psi_s\rangle$. You may introduce auxiliary qubits, apply

quantum gates, perform measurements, and repeatedly submit an n -qubit register to the bank. You may retain auxiliary registers while the bank verifies the submitted register. The bank will verify the submission and reveal only the overall verdict, not the individual measurement outcomes. Whenever it returns a bill, it returns the post-measurement state with the same serial number and the same secret strings. The bank will additionally verify the same bill as many times as a user desires.

4. **(2 points)** First suppose the bank returns the post-measurement state together with its verdict whether the bill is legitimate or not accepted. Construct a procedure that starts with one copy of $(s, |\psi_s\rangle)$ and that exploits access to this bank to produce two copies of $(s, |\psi_s\rangle)$ bills with certainty. Prove its correctness and analyze its number of bank queries and expected running time in terms of n .
5. **(3 points)** Now suppose the bank returns the post-measurement state only if it accepts. If it rejects, it sounds an alarm and sends the submitter to jail, ending your procedure. For every $\epsilon \in (0, 1)$, construct a procedure that has a max probability of going to jail of ϵ and, conditioned on avoiding jail, produces two copies of $(s, |\psi_s\rangle)$. Prove both guarantees and analyze its number of bank queries and expected running time in terms of n and ϵ .

Hint: Take inspiration from the Elitzur–Vaidman bomb tester. For each $i = 1, \dots, n$, in sequence learn the basis encoding b_i encoding the i -th bit of $|\psi_s\rangle$. *[This part is challenging; come ask us for hints in office hours if stuck!]*

For the running-time analysis, count each bank query as one operation and count each one- and two-qubit gates and single-qubit measurements as one operation. Single-qubit rotations by arbitrary specified angles are allowed.