Problem set 4

CSE 534 Autumn 2026

Due date: November 2nd 11:59 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.

Practice problems (not graded)

These problems are not graded. Do not submit a solution, but do ensure that you can solve the problem.

Problem 1 (Partial trace)**.**

1. Consider a quantum state $\rho_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Prove that

$$\mathrm{tr}_B(\mathrm{tr}_C(\rho_{ABC})) = \mathrm{tr}_C(\mathrm{tr}_B(\rho_{ABC})) = \mathrm{tr}_{BC}(\rho_{ABC}).$$

2. Prove that for a density matrix $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ that $\sigma_A \stackrel{\text{def}}{=} \mathrm{tr}_B(\sigma_{AB})$ is a density matrix (i.e. that it is a positive Hermitian matrix of trace 1).

3. Assume $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$. Prove that any single-qubit standard basis measurement of σ_A has the same distribution as that obtained by measuring the same qubit of σ_{AB}.

Graded problems

Problem 2. Define the 1-norm of a matrix:

$$\|\rho\|_1 \stackrel{\text{def}}{=} \mathrm{tr}\sqrt{\rho^\dagger \rho}.$$

Let ρ be a density matrix and $\{\Pi, \mathbb{I} - \Pi\}$ be a POVM with $\Pi^2 = \Pi$ such that $\mathrm{tr}(\Pi\rho) \geq 1 - \epsilon$. Let ρ' be the post-measurement state: $\rho' = \frac{\Pi\rho\Pi}{\mathrm{tr}(\Pi\rho)}$.

1. **(3 points)** State and prove an upper bound on $\|\rho - \rho'\|_1$.

   Hint: First calculate the statement for a pure state. Then, generalize to density matrices by expressing a density matrix as a linear combination of pure states. Cauchy-Schwarz is your friend! Lastly, it may help to note that

$$\||a\rangle\langle a| - |b\rangle\langle b|\|_1 = \||a\rangle + |b\rangle\| \cdot \||a\rangle - |b\rangle\|$$

   when $\langle a|b\rangle$ is real. You can use this without proof.

2. **(2 points)** Argue by constructing an example that the upper bound is asymptotically tight (as in the scaling is the correct function of ϵ).

Problem 3. Let ρ and σ be two density matrices $\in \mathcal{H}_A \otimes \mathcal{H}_B$.

(3 points) Prove that

$$\|\mathrm{tr}_A(\rho) - \mathrm{tr}_A(\sigma)\|_1 \leq \|\rho - \sigma\|_1. \tag{1}$$

Problem 4 (Simultaneous change of basis)**.** In this problem, we are going to prove the following statement which is very useful in characterizing the behavior of quantum devices:

> For any two Hermitian operators A, B acting on a Hilbert space $\mathcal{H} \cong \mathbb{C}^d$ such that $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$, there exists a change of basis U on $\mathcal{H}$ such that
>
> $$UAU^\dagger = X \otimes \mathbb{I}_{d/2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \mathbb{I}_{d/2}, \qquad UBU^\dagger = Z \otimes \mathbb{I}_{d/2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \mathbb{I}_{d/2} \tag{2}$$
>
> where the $\mathbb{I}$ action is on the remaining $d/2$ dimensions. Therefore, A and B identify a decomposition of $\mathcal{H} \cong \mathbb{C}^2 \otimes \mathbb{C}^{d/2}$.

The following setup breaks down the proof into manageable parts. *However, you do not have to use this particular proof strategy.*

1. First, solve the $d = 2$ case. Meaning, you can assume that A and B are 2×2 matrices and you want to explicitly show the existence of a 2×2 unitary U such that $UAU^\dagger = X$ and $UBU^\dagger = Z$.
   (a) **(1 point)** Calculate the eigenvalues of A and B.
   (b) **(1 point)** Write B in its eigenbasis. What does $AB = -BA$ imply about A?
   (c) **(1 point)** Show the existence of a U satisfying eq. (2) in the case that $d = 2$.
2. Consider matrices A and B such that there exists a unitary V such that $VAV^\dagger$ and $VBV^\dagger$ are block-diagonal with each block being a 2×2 matrix – i.e.

$$VAV^\dagger = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{d/2} \end{pmatrix}, \quad VBV^\dagger = \begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_{d/2} \end{pmatrix}. \tag{3}$$

   (2 points) Show that for such matrices, a simultaneous change of basis according to eq. (2) exists.
3. Show that eq. (3) is sufficiently general. Namely, that if general $d \times d$ Hermitian matrices exist satisfying $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$, then there exists a unitary V such that eq. (3) holds.

(a) **(2 points)** Consider any two Hermitian matrices such that $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$. Let $|v\rangle$ be any eigenvector of $A + B$. Then show that both A and B preserve the vector space spanned by $|v\rangle$ and $AB\,|v\rangle$.

(b) **(2 points)** Conclude that there exists a change of basis unitary V such that in this basis, A and B are simultaneously block-diagonal with blocks of size 1 or 2.

(c) **(1 point)** Argue that blocks of size 1 cannot exist due to the anti-commutation condition. Therefore, we have achieved the assumption of eq. (3).

4. Read the following text about why you had to prove this theorem. No response is required.

What is a bit? Let $V \subseteq \mathbb{F}_2^n$ be a subspace with $k = \dim V = \log_2 |V|$, so V can store k bits. But *which* k bits? The coordinates of $\mathbb{F}_2^n$ are not the answer: $V = \{000, 111\}$ has three coordinates but stores a single bit, and no single coordinate can be changed without leaving V.

To name a bit we need two things: a way to *flip* it and a way to *read* it. A flip is a vector $v \in V$, acting by $w \mapsto w + v$. A readout is a vector $u \in \mathbb{F}_2^n$, acting by $w \mapsto u \cdot w \pmod 2$. To name all k bits at once, collect the flips as the columns of a matrix M and the readouts as the rows of a matrix R:

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_k \\ | & & | \end{pmatrix}, \qquad R = \begin{pmatrix} - & u_1 & - \\ & \vdots & \\ - & u_k & - \end{pmatrix}, \qquad RM = I_k.$$

The condition $RM = I_k$ says $u_i \cdot v_j = \delta_{ij}$, and therefore

$$u_i \cdot (w + v_j) = u_i \cdot w + \delta_{ij}.$$

That is, flipping bit j changes the readout of bit j and of no other bit. This is exactly what it means for the k bits to be independent. The matrices also give the bijection $\{0,1\}^k \leftrightarrow V$: encode with $x \mapsto Mx$, and decode with $w \mapsto Rw$, since $R(Mx) = x$. The strings whose first bit is 0 form $V_0 = \{w \in V \,:\, u_1 \cdot w = 0\}$, those whose first bit is 1 form $V_1 = V_0 + v_1$, and the flip v_1 swaps the two halves.

The bits are in the eye of the beholder. Take $V = \mathbb{F}_2^2$. Two equally valid frames are

$$\text{Frame I:} \quad M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \text{Frame II:} \quad M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Both satisfy $RM = I_2$. In Frame II, flipping bit 1 flips *both* coordinates, and reading bit 2 computes their *parity*. The string $(1, 1)$ decodes to 11 in Frame I but to 10 in Frame II. Nothing about V

prefers one frame over the other. Notice also that bit 1 has the same readout in both frames but a different flip, so neither a flip nor a readout alone defines a bit.

What is a qubit? The same story holds for qubits, with operators in place of vectors. The flip of a qubit is an observable X. Its readout is an observable Z, whose eigenvalue ± 1 encodes $(-1)^{\text{bit}}$. The classical condition $u_i \cdot v_j = \delta_{ij}$ becomes

$$Z_i X_j = (-1)^{\delta_{ij}} X_j Z_i,$$

so X_j flips the eigenvalue of Z_i exactly when $i = j$. In addition, the flips commute with each other and the readouts commute with each other. (Classically this was automatic.)

Where the theorem from this problem fits in. The statement you just proved is precisely the one-qubit case of this picture. You were handed a flip A and a readout B that satisfy the qubit relations ($A^2 = B^2 = \mathbb{I}$, $AB = -BA$) but nothing else. They could be enormous matrices in an arbitrary basis of $\mathcal{H} \cong \mathbb{C}^d$, with no qubit in sight. The theorem says that any such pair *is* a qubit: there is a change of basis U under which A becomes $X \otimes \mathbb{I}_{d/2}$ and B becomes $Z \otimes \mathbb{I}_{d/2}$. The unitary U plays the role that the frame (M, R) played classically. It is the dictionary between the abstract space $\mathcal{H}$ and the "qubit coordinates" $\mathbb{C}^2 \otimes \mathbb{C}^{d/2}$.

One way to see what your proof was doing is to compare it with the classical picture. Classically, the readout u_1 splits V into halves V_0 and V_1, and the flip v_1 swaps them. Quantumly, the readout B splits $\mathcal{H}$ into its $+1$ and -1 eigenspaces E_+ and E_-. Because $AB = -BA$, the flip A maps E_+ isomorphically onto E_-. Hence both eigenspaces have dimension $d/2$, and $\mathcal{H} = E_+ \oplus E_- \cong \mathbb{C}^2 \otimes E_+$. The $\mathbb{C}^2$ factor records "which half," and the $\mathbb{C}^{d/2}$ factor records everything else.

From one qubit to n qubits. Your theorem handles a single flip–readout pair. To handle n pairs, we iterate it.

Lemma. Let $\mathcal{H} \cong \mathbb{C}^d$, and let $A_1, \dots, A_n$ and $B_1, \dots, B_n$ be observables on $\mathcal{H}$ such that $A_i B_i = -B_i A_i$ for every i, and every other pair of these operators commutes. Then 2^n divides d, and there exists a change of basis U on $\mathcal{H}$ such that

$$U A_i U^\dagger = X_i \otimes \mathbb{I}_{d/2^n}, \qquad U B_i U^\dagger = Z_i \otimes \mathbb{I}_{d/2^n},$$

where X_i and Z_i denote X and Z acting on the i-th factor of $(\mathbb{C}^2)^{\otimes n}$, e.g. $X_i = \mathbb{I}^{\otimes(i-1)} \otimes X \otimes \mathbb{I}^{\otimes(n-i)}$. Therefore $\mathcal{H} \cong (\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^{d/2^n}$.

Characterizing $(\mathbb{C}^2)^{\otimes n}$. Conversely, the standard operators $X_1, \dots, X_n, Z_1, \dots, Z_n$ on $(\mathbb{C}^2)^{\otimes n}$ satisfy the hypotheses of the corollary. So the corollary is a characterization: *a Hilbert space carries n qubits exactly when it carries n flip–readout pairs obeying the qubit relations.* When $d = 2^n$ the leftover factor is trivial, so $\mathcal{H} \cong (\mathbb{C}^2)^{\otimes n}$, and A_i, B_i are literally the Pauli X and Z on the i-th

qubit.

Even the computational basis is recovered from the operators alone. The vectors $U^\dagger |x\rangle$ for $x \in \{0,1\}^n$ are the joint eigenvectors of the readouts, with B_i having eigenvalue $(-1)^{x_i}$. The flips act by addition: for $a \in \{0,1\}^n$, the product $A_1^{a_1} \cdots A_n^{a_n}$ sends $U^\dagger |x\rangle$ to $U^\dagger |x \oplus a\rangle$. This mirrors the classical encoding $x \mapsto Mx$, in which the flips v_i act by addition and the readouts u_i recover x. The tensor factors are not handed to us by $\mathcal{H}$. They are carved out by the operators we choose.

Entanglement is in the eye of the beholder. On $\mathbb{C}^2 \otimes \mathbb{C}^2$, consider the quantum version of Frame II:

$$\widetilde{X}_1 = X \otimes X, \quad \widetilde{Z}_1 = Z \otimes \mathbb{I}, \quad \widetilde{X}_2 = \mathbb{I} \otimes X, \quad \widetilde{Z}_2 = Z \otimes Z.$$

(Check that these satisfy the hypotheses of the corollary!) Since $d = 4 = 2^2$, the corollary says these operators carve $\mathbb{C}^2 \otimes \mathbb{C}^2$ into two qubits in a new way. One valid change of basis is $U = \text{CNOT}$, which maps $X \otimes X \mapsto X \otimes \mathbb{I}$ and $Z \otimes Z \mapsto \mathbb{I} \otimes Z$, and fixes $Z \otimes \mathbb{I}$ and $\mathbb{I} \otimes X$.

Why take this perspective? Often there is no trustworthy "physical" description of the qubits to fall back on. As we will see, in quantum error correction, the logical qubit of the three-qubit bit-flip code is defined by its logical operators $\bar{X} = XXX$ and $\bar{Z} = ZII$, exactly mirroring $M = (1,1,1)^T$ and $R = (1,0,0)$ for the classical repetition code. Restricted to the code space, these satisfy the hypotheses of your theorem, so they carve out a genuine qubit.

In non-local games and device-independent cryptography, we do not even know the Hilbert space or the measurements. Yet if the observed statistics force n pairs of observables to obey the qubit relations, the corollary lets us *find* n qubits inside the unknown device, up to the leftover factor. In each case, defining qubits by their flips and readouts is what lets us talk about qubits at all. This can all be made fully rigorous, and the mathematics, while daunting at first, is well within reach.