

This problem set is due *Wednesday, October 7th, at 11:59 PM ET*. It will be graded for completion: for every problem, give as much of a solution as you can. If you get stuck, explain where you got stuck, what you are confused about, and what you tried to get around it.

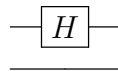
See the AI policy and the collaboration statement in the syllabus. In short, do not use AI. Feel free to collaborate with others, but your write-up must be your own, and you must disclose your collaborators and any outside sources.

Here are some definitions of matrices for reference.

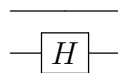
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Problem 1 (Quantum circuits). The following are questions to familiarize you with quantum circuits.

- (a) (Nielsen–Chuang, Exercise 4.16) What is the 4×4 unitary matrix for the circuit

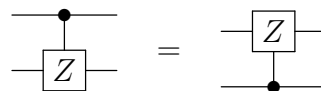


in the computational basis? What is the unitary matrix for the circuit

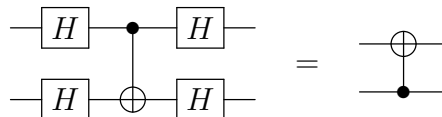


in the computational basis? Here, let's read the wires top to bottom: for example, $|01\rangle$ would correspond to putting $|0\rangle$ on the top wire and $|1\rangle$ on the bottom wire.

- (b) (Nielsen–Chuang, Exercise 4.18) Show that



- (c) (Nielsen–Chuang, Exercise 4.20) Unlike ideal classical gates, ideal quantum gates do not have (as electrical engineers say) ‘high-impedance’ inputs. In fact, the roles of ‘control’ and ‘target’ are arbitrary – they depend on what basis you think of a device as operating in. We have described how the CNOT behaves with respect to the computational basis, and in this description the state of the control qubit is not changed. However, if we work in a different basis then the control qubit does change: we will show that its phase is flipped depending on the state of the ‘target’ qubit! Show that

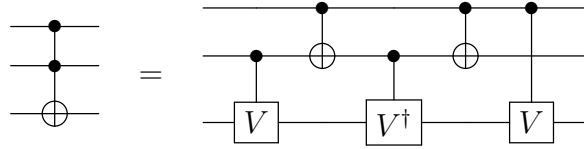


Thus, with respect to the Hadamard basis, the state of the target qubit is not changed, while the state of the control qubit changes: it is flipped if the target starts as $|-\rangle$, and left alone if the target is $|+\rangle$. That is, in this basis, the target and control have essentially interchanged roles!

- (d) (Nielsen–Chuang, p. 182) The Toffoli gate is the one which performs NOT on the third register if the first and second registers are $|1\rangle$:

$$|b_1\rangle |b_2\rangle |b_3\rangle \mapsto |b_1\rangle |b_2\rangle |b_3 \text{ XOR } (b_1 \text{ AND } b_2)\rangle.$$

Show that the matrix $V = (1 - i)(I + iX)/2$ satisfies $V^2 = X$. Then, use this to show that the Toffoli gate can be implemented as follows:



Problem 2 (Partial trace). For a density matrix on two qubits, the partial trace over the first qubit is the linear map which satisfies the following property:¹

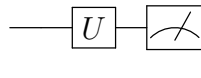
$$\text{tr}_1(|a_1\rangle\langle b_1|)(|a_2\rangle\langle b_2|) = \text{tr}(|a_1\rangle\langle a_2|)|b_1\rangle\langle b_2| = \langle a_2|a_1\rangle|b_1\rangle\langle b_2|.$$

We can compute the partial trace for a general density matrix by expanding it out into terms like $|00\rangle\langle 00|$, $|00\rangle\langle 01|$, and so on. Similarly, we can define

$$\text{tr}_2(|a_1\rangle\langle b_1|)(|a_2\rangle\langle b_2|) = |a_1\rangle\langle a_2|\text{tr}(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2|\langle b_2|b_1\rangle.$$

See Box 2.6 of Nielsen–Chuang for more details on the motivation for this definition.

- (a) Compute the density matrix $\sigma = \text{tr}_1(|\psi\rangle\langle\psi|)$, where $|\psi\rangle = \frac{1}{\sqrt{10}}(|00\rangle + 2|01\rangle + 2|10\rangle - |11\rangle)$, and compute the probabilities you get when measuring σ in the $\{|+\rangle, |-\rangle\}$ basis. Then, confirm that the probability you get of measuring $|+\rangle$ from σ is equal to the probability of measuring either $|++\rangle$ or $|+-\rangle$ when measuring both qubits of $|\psi\rangle\langle\psi|$ in the $\{|+\rangle, |-\rangle\}$ basis.
- (b) Let ρ and σ be one-qubit density matrices. Show that $\text{tr}_1(\rho \otimes \sigma) = \sigma$ and $\text{tr}_2(\rho \otimes \sigma) = \rho$.
- (c) Consider a two-qubit pure state $|\phi\rangle$. Consider applying a unitary to the first qubit and then measuring it:



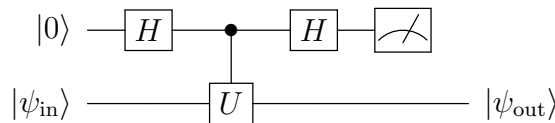
The measurement outcomes will be $|0\rangle$ and $|1\rangle$, with probabilities (say) of p_0 and p_1 , and leave the remaining qubit in the states $|\phi_0\rangle$ and $|\phi_1\rangle$, respectively. Suppose I have the first qubit, you have the second qubit, and I do not tell you which outcome I measured, so that to you, the state of the second qubit is $|\phi_0\rangle$ with probability p_0 and $|\phi_1\rangle$ with probability p_1 . Show that the density matrix that corresponds to this distribution over outcomes equals $\text{tr}_1(|\phi\rangle\langle\phi|)$, regardless of what U is. This is the substance of the no-communication theorem: my actions on the first qubit do not affect the density matrix of your qubit, unless I communicate to you in some way.

- (d) Let ρ be the density matrix of a two-qubit state. When is $\text{tr}_1(\rho)$ pure? Justify your answer; a formal proof is not required.

¹This same definition works beyond two qubits, to “tracing out” a register of any dimension from a larger space.

Problem 3 (Learning states). Suppose you have many copies of a one-qubit state with density matrix ρ . (In this situation, you don't know what ρ is; suppose it's the outcome of an experiment, and you don't know what the output is but you can repeat the experiment to generate new copies.) One copy is not enough to determine an arbitrary unknown ρ , but sufficiently many independent copies allow us to estimate it to arbitrary accuracy. This type of procedure is known as *state tomography*.

- (a) Suppose I tell you three values, $\text{tr}(X\rho) = E_X$, $\text{tr}(Y\rho) = E_Y$, and $\text{tr}(Z\rho) = E_Z$. Then describe how to find ρ . I tell you that the state ρ has the property that $E_X = 1/4$, $E_Y = 1/4$, and $E_Z = 1/2$. What is ρ ?
- (b) (Nielsen–Chuang, Exercise 4.34) Suppose we have a single qubit operator U which is unitary and Hermitian. Show that the following circuit implements a measurement of U :



That is, show that the outcome of the measurement can be used to produce a random variable $z \in \{+1, -1\}$ such that $E[z] = \text{tr}(U\rho)$ and $\text{Var}[z] = E[|z - E[z]|^2] \leq 1$.

- (c) Show that, with $3k$ independent copies of ρ , we can produce estimates for $\text{tr}(X\rho)$, $\text{tr}(Y\rho)$, and $\text{tr}(Z\rho)$ whose means equal the respective quantities and whose variances are at most $1/k$. (Use $E[z_1 + z_2] = E[z_1] + E[z_2]$ and, for independent random variables, $\text{Var}[z_1 + z_2] = \text{Var}[z_1] + \text{Var}[z_2]$.) Thus, with enough copies of the state, we can estimate its density matrix.

Problem 4 (Distinguishing states). Suppose you are given a state $|\psi\rangle$ that is either $|0\rangle$ or $|1\rangle$, but you do not know which. You can distinguish them by measuring in the $\{|0\rangle, |1\rangle\}$ basis.

- (a) Suppose instead that $|\psi\rangle$ is either $|0\rangle$ or $|+\rangle$, with equal probability. Give a protocol that distinguishes the two states with failure probability $\sin^2(\frac{\pi}{8}) \approx 0.146$. (This is optimal!) Show explicitly that your protocol achieves this failure probability.

A protocol is a step-by-step procedure that ends by outputting either “I think this was $|0\rangle$ ” or “I think this was $|+\rangle$ ”.

Hint: Read Section 5.2 of the lecture notes.

- (b) What is the failure probability if you measure in the $\{|0\rangle, |1\rangle\}$ basis and then choose which state to guess based on the outcome?
- (c) Now suppose that you get two copies of the state that you want to distinguish: you are given $|\phi\rangle$ which is either $|00\rangle$ or $|++\rangle$ with equal probability. Give a protocol which measures the qubits one at a time to distinguish the two states with failure probability $1/8$.
- (d) Find a method to distinguish the two states with failure probability smaller than $1/8$. (*Hint: Again, Section 5.2 will be your friend. First, change your basis into one which makes the problem easier to understand.*)
- (e) Now suppose that you are given ρ which is either $|+\rangle\langle+|$ or a fair coin $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ with equal probability. Give a protocol to distinguish them with failure probability $1/4$.