# Quantum Information Theory - 67749
# Recitation 1, April 24, 2025

## 1 Two Qubit Gates and Quantum Circuits.

The standard computation model in the quantum setting is quantum circuits ('chips'), we describe it by associating a wire for each of the qubits, and on top of them, we lay operators (quantum gates). We think of the horizontal direction as our timeline, and the operators are set according to their time ordering. The gates can be either two-qubit gates, unitary, or a measurement in the computational basis. The **depth** of the circuits is the length of the longest line, and it quantifies the time complexity of the computation. The size of the circuit quantifies the space complexity. Since qubits are an expensive resource (e.g, IBM computers have at most 433 qubits), it's also interesting to talk about the width complexity - the number of additional ancillas that have to be paid.

A universal gate set is a set of gates that can generate an approximation (as good as we wish) of any operation in the computational model, in the classical model { `NAND` } and { `OR`, `AND` } are examples of universal gate set. In the quantum, we have, for example, the set $\{H, S, T, CNOT\}$, also called Clifford $+ T$. Where:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The CNOT -control not-, also called CX -control $X$- applies $X$ on the second (qu)bit conditioned on whether the first (qu)bit is turned on. Similarly, one can define CZ, CCX, and for a general unitary $U$: control-$U$. What's the inverse of control-$U$? (control-$U^\dagger$).

**EPR/BELL/GHZ-circuits:** In fig. 1 we have the circuit which when act on $|0^n\rangle$ gives the state $\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$. The circuit is composed of applying $H$ at the beginning on the first qubit and then xoring its value to the other qubits. At the end of the computation, in the ket associated with the value of the first qubit being 1, the 1 is spreading across all the qubits.

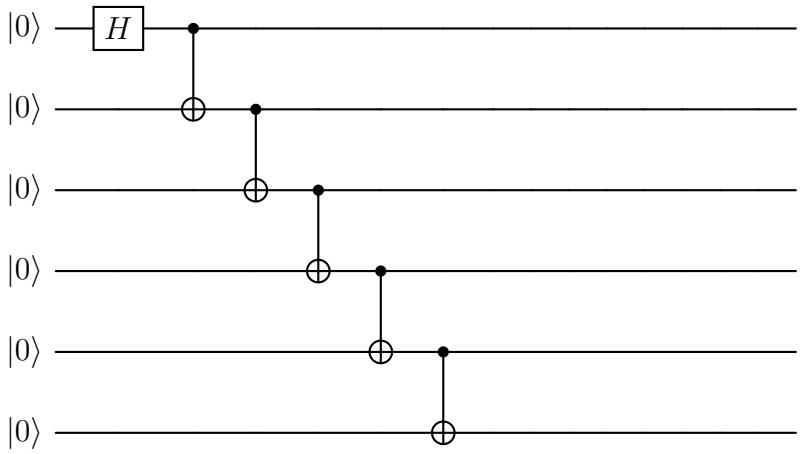
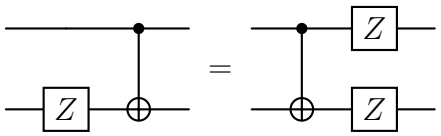



Figure 1: **GHZ**-generating circuit.

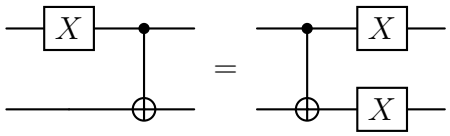
### 1.1 Quantum Circuits.

Prove equivalence for the following circuit pairs. You can do it by either showing the equivalence of the matrices products or by shifting the graphs according to the commutation rules.

(a) Bit flip propagation:




(b) Phase flip propagation:




**Solution.** On one hand $(I \otimes Z)\, CX$ equals:

$$\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right) \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix} \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{bmatrix}$$

On the other hand $CX\, (Z \otimes Z)$:

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right) = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{bmatrix}$$

## 2 Quantum Measurements

1. We would like to measure in an orthonormal basis $\{|v_i\rangle\}$, but the measuring apparatus works with the orthonormal basis $\{|w_i\rangle\}$. Show that the

measurement can be performed by applying a unitary transformation $U$ to the system before measuring using the apparatus, followed by applying $U^\dagger$.

**Hint:** Try to understand first how one can measure in $\{|+\rangle, |-\rangle\}$ base while having an apparatus to measure in $\{|0\rangle, |1\rangle\}$ base. What would be $H$ in that case?

**Solution.** Let's consider first the case we would like to measure in $\{|+\rangle, |-\rangle\}$ base. In other words, we are willing to engineer a protocol for which:

(a) The probability to measure $|\pm\rangle$ is $|| \langle \pm|\psi\rangle ||^2$.

(b) The output state at the end of the protocol is $|\pm\rangle$ upon the measurement result.

Consider the circuit at fig. 3[1].

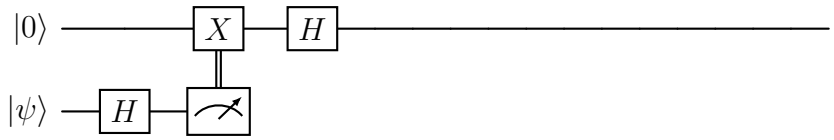



Figure 3: Measuring the single-qubit state $|\psi\rangle$ at the $\{|+\rangle, |-\rangle\}$ base.

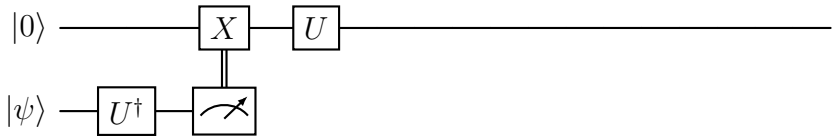



Figure 4: Measuring the single-qubit state $|\psi\rangle$ at the $\{U|0\rangle, U|1\rangle\}$ base.

2. Recall that we said in the class that one can distinguish between only two nonorthogonal states $|\psi\rangle$ and $|\phi\rangle$. only with probability at most $\frac{1+\sin\theta}{2}$ when $\cos^2\theta = \langle\psi||\phi\rangle$

   (a) Show that the statement above is false given a machine which can copy $|\psi\rangle$ and $|\phi\rangle$

   (b) Prove that a quantum circuit that can copy doesn't exist.

   **Solution.**

[1]Here we think of the measuring mechanism as a machine which outputs a classical bit which can't be used again as a fresh qubit. Otherwise, we could use a single wire by applying $U$ immediately after the measurement.

(a) Given a state $|\psi\rangle$ one can duplicate it $t$ times and get the tensor $|\psi\rangle^{\otimes t}$, Then by applying the measurement we saw in class [2]. And take the majority of the results. We bound the failure probability by the scenario that the mean of the results is $\varepsilon$ far from $\frac{1+\sin\theta}{2}$. By the Chernoff bound, it happened with probability less than $\sim e^{-\varepsilon t}$.

(b) Assume trough contradiction that $U$ is the cloning gate. Namely $U|\psi\rangle|0\rangle \mapsto |\psi\rangle|\psi\rangle$. Then:

$$\begin{aligned} U|+\rangle|0\rangle &= U\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(U|0\rangle|0\rangle + U|1\rangle|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \neq |+\rangle|+\rangle \end{aligned}$$

## 2.1 Quantum Operations and POVMs

1. Consider the POVM given by the operators:

$$E_1 = \frac{1}{2}|0\rangle\langle 0|, \quad E_2 = \frac{1}{2}|1\rangle\langle 1|,$$
$$E_3 = \frac{1}{2}|+\rangle\langle +|, \quad E_4 = \frac{1}{2}|-\rangle\langle -|.$$

**Verify** that this is an eligible POVM and **find** a realization of the POVM above as an orthogonal measurement in a two-qubit state space, by adding an ancilla qubit.

**Solution.** First, observe that any rank-1 matrix $M = \alpha|v\rangle\langle v|$ with positive coefficients is a PSD. That's because:

$$\langle u|M|u\rangle = \langle u\alpha|v\rangle\langle v|u\rangle = \begin{cases} 0 & \text{if } |u\rangle \in (|v\rangle)^{\perp} \\ \alpha||\langle u,v\rangle||^2 & \text{otherwise} \end{cases}$$

So all the $E_i$ are PSD's, and now it's only left to show that they sum up to the identity. Also observe that:

$$|+\rangle\langle +| = \frac{1}{\sqrt{2}}[1,1]\frac{1}{\sqrt{2}}([1,1])^{\top} = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$$
$$|-\rangle\langle -| = \frac{1}{2}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}$$

So we have that:

$$\begin{aligned} E_1+E_2+E_3+E_4 &= \frac{1}{2}\left(\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}\right) \\ &= \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \end{aligned}$$

[2] projecting over orthogonal base for which the crossing angle between the base element is the same as the one which cross the angle between $|\psi\rangle$ and $|\phi\rangle$

To realize the measurement, we are going to 'controlize' the measurement based on ancilla. Using almost the same apparatus we developed earlier, but we will condition the $U$-rotation by a thread qubit ancilla.

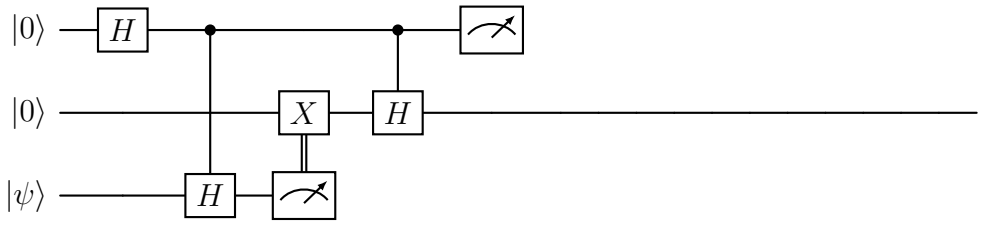



Figure 5: realizing the POVM-measurement $\{E_1, E_2, E_3, E_4\}$.

Complete proof would also require explicitly computing probabilities, yet we will give up on the fun.

# 3 Diagonalize Noisy State.

Let $|A_+\rangle$ and $|A_-\rangle$ be two orthogonal pure states over single qubit, i.e $\langle A_+|A_-\rangle = 0$ and let $\rho$ be the mixed state such that $\langle A_+|\rho|A_+\rangle = 1-p$ for some $p < 1$. We would like to design a channel $\mathcal{E}_A : \mathcal{L}(\mathcal{H}_2) \to \mathcal{L}(\mathcal{H}_2)$ that takes $\rho$ into:

$$\rho' = \mathcal{E}_A(\rho) = (1-p)\,|A_+\rangle\langle A_+| + p\,|A_-\rangle\langle A_-|$$

1. Give an explicit example for which $\mathcal{E}$ is not trivial, namely $\rho$ satisfies the constraint, yet doesn't have the form of $\rho'$.

   **Solution.** Consider, for example, the mixed state:

   $$\rho = \frac{2}{3}|0\rangle\langle 0| + \frac{i}{3}|1\rangle\langle 0| - \frac{i}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 1|$$

   On one hand, it's clear that the matrix is Hermitian, and since its eigenvalues are $\frac{1}{2}\left(1 \pm \frac{\sqrt{5}}{3}\right) > 0$, the matrix is definite positive, hence $\rho$ is density matrix. On the other hand, $\rho$ has non-zero off-diagonal elements.

2. Solve it for $|A_\pm\rangle = |\pm\rangle$.

   **Solution.** So in let's define the channel which is probability $\frac{1}{2}$ do nothing and with probability $\frac{1}{2}$ apply $X$. So in total we got:

   $$\rho \to \frac{1}{2}\rho + \frac{1}{2}X\rho X$$

   Notice that the channel acts trivially on $|\pm\rangle\langle\pm|$:

   $$\begin{aligned}|\pm\rangle\langle\pm| \to &\frac{1}{2}|\pm\rangle\langle\pm| + \frac{1}{2}X|\pm\rangle\langle\pm|X \\ &\frac{1}{2}|\pm\rangle\langle\pm| + \frac{1}{2}(\pm)|\pm\rangle\langle\pm|(\pm) = |\pm\rangle\langle\pm|\end{aligned}$$

However on $|\pm\rangle\langle\mp|$ we have that:

$$|\pm\rangle\langle\mp| \rightarrow \frac{1}{2}|\pm\rangle\langle\mp| + \frac{1}{2}X|\pm\rangle\langle\mp|X$$
$$\frac{1}{2}|\pm\rangle\langle\mp| + \frac{1}{2}(\pm)|\pm\rangle\langle\mp|(\mp) = \frac{1}{2}|\pm\rangle\langle\mp| - \frac{1}{2}|\pm\rangle\langle\mp| = 0$$

So in total, we have that any $\rho$ such $\langle+|\rho|+\rangle = p$ and $\langle+|\rho|+\rangle = 1-p$ would be map to a mixed state

$$\rho' = p|+\rangle\langle+| + (1-p)|-\rangle\langle-|$$

3. [**At home.**] Solve it for the general case. (Hint: What does the orthogonality condition guarantee?).

4. [**At home.**] Let $|A_1\rangle, |A_2\rangle, |A_3\rangle, |A_4\rangle$ be four orthogonal states in $\mathcal{H}_4$. Suppose now that $\rho$ is supported on two qubits. And for $i \in \{1,2,3,4\}$ denote by $p_i$ the fidelity between $|A_i\rangle$ and $\rho$. Namely $\langle A_i|\rho|A_i\rangle = p_i$. Design a channel $\mathcal{E}_A$ that takes $\rho$ into:

$$\rho' = \mathcal{E}_A(\rho) = \sum_{i=1}^{4} p_i |A_i\rangle\langle A_i|$$

# 4 Partial Trace Transformation Under Local Operation.

Consider the mixed state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$. And let $M$ be an operator that acts on $\mathcal{H}_A$. Show that:

$$\mathbf{Tr}_B\left(M \otimes I_B \rho M^\dagger \otimes I_B\right) = M\mathbf{Tr}_B(\rho)M^\dagger$$

**Solution.** Let $M$ be an operation in $\mathcal{H}_A$-space, and consider the presentation of $\rho$ in the base of the eigen vectors of $M$, namely $\rho$ can be written as:

$$\rho = \sum_{ijkl} \alpha_{ijkl}|ij\rangle\langle kl|$$

When $\{|i,*\rangle\}$ (or $\langle k,*|$) are eigenvectors of $M$. Thus[3] :

$$\rho \rightarrow M\rho M^\dagger \rightarrow \sum_{ijkl} \sigma_i \sigma_k^* \alpha_{ijkl}|ij\rangle\langle kl|$$

Now tracing out $B$ gives:

[3]Notice that the result is an unnormolized state. We are going to show an equivalence between matrices; to get the actual density matrices, we would have to normalize by the trace.

$$\sum_{j'}\sum_{ijkl} I\otimes\langle j'|\left(\sum_{ik}\sigma_i\sigma_k^*\alpha_{ijkl}\,|ij\rangle\,\langle kl|\right)I\otimes|j'\rangle=\sum_{jik}\sigma_i\sigma_k^*\alpha_{ijkj}\,|i\rangle\,\langle k|$$

$$=\sum_{ik}\left(\sum_j\alpha_{ijkj}\right)\sigma_i\sigma_k^*\,|i\rangle\,\langle k|=\sum_{ik}\left(\sum_j\alpha_{ijkj}\right)M\,|i\rangle\,\langle k|\,M^\dagger$$

$$=M\left(\sum_{ijkl} I\otimes\langle j'|\,\alpha_{ijkl}\,|ij\rangle\,\langle kl|\,I\otimes|j'\rangle\right)M^\dagger=M\mathbf{Tr}_B\left(\rho\right)M^\dagger$$

**Example.** Let $\rho$ be the density matrix of the **EPR** state:

$$\begin{aligned}\rho&=\frac{1}{2}\left(|00\rangle+|11\rangle\right)\left(\langle 00|+\langle 11|\right)\\&=\frac{1}{2}\left(|00\rangle\,\langle 00|+|00\rangle\,\langle 11|+|11\rangle\,\langle 00|+|11\rangle\,\langle 11|\right)\end{aligned}$$

Now consider the experiment in which we first forget (tracing out) the $B$'s-part, and then apply $X$ on the first qubit:

$$\begin{aligned}\rho&\mapsto I\otimes\langle 0|\,\rho I\otimes|0\rangle+I\otimes\langle 1|\,\rho I\otimes|1\rangle=\frac{1}{2}|0\rangle\,\langle 0|+|1\rangle\,\langle 1|\\&\mapsto X(\cdot)X=\frac{1}{2}|1\rangle\,\langle 1|+|0\rangle\,\langle 0|\end{aligned}$$

On the other hand, if we were first to apply $X$ on the first qubit and then forget from $B$ then we would have:

$$\begin{aligned}\rho&\mapsto X\otimes I\rho X\otimes I=\frac{1}{2}\left(|10\rangle\,\langle 10|+|10\rangle\,\langle 01|+|01\rangle\,\langle 10|+|01\rangle\,\langle 01|\right)\\&\mapsto I\otimes\langle 0|\,(\cdot)I\otimes|0\rangle+I\otimes\langle 1|\,(\cdot)I\otimes|1\rangle=\frac{1}{2}\left(|1\rangle\,\langle 1|+|0\rangle\,\langle 0|\right)\end{aligned}$$

**Question.** Why don't we have to normalize the resulting mixed state?