CS 151 Quantum Computer Science

Lecture 7: Tensor product

February 07, 2027

Lecturer: Saeed Mehraban *Scribe: Preliminary notes*

1 Logistics

- Problem set 3 is now released. Problem set 2 is due tonight.

2 Overview

Last time, we gave a thorough description of single-qubit quantum operations. We then initiated our discussion about multi-qubit systems. We defined tensor products and entangled states. In this lecture, we will continue our discussion about tensor product formulation and use this formalism to analyze simple quantum circuits.

3 Multi-qubit systems:

3.1 Tensor product of operations

Next we talk about tensor product of operations on different parts of a system.

- Tensor product of operators: $A \otimes B$.

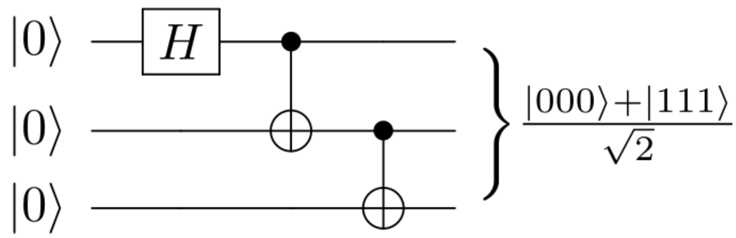
$$A \otimes B = \begin{pmatrix} & .. & \\ .. & A_{ij}B & .. \\ & .. & \end{pmatrix}$$

  - $(A + A') \otimes B = A \otimes B + A' \otimes B$
  - $(\alpha A) \otimes B = \alpha(A \otimes B)$
  - $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$
  - Example $(X \otimes X)(|0\rangle\langle 1| \otimes H)$

- Tensor product of operation $(A \otimes B)(|a\rangle \otimes |b\rangle) = (A|a\rangle \otimes B|b\rangle)$

Example 3.1. *Apply $H \otimes H$ to $|11\rangle$. Then apply CNOT. Then SWAP. Then apply the phase gate on the first qubit.*

Figure 1: Quantum Circuit for the GHZ state



Example 3.2. *Consider the three-qubit state* $|000\rangle$. *If we apply Hadamard to the first qubit we obtain:* $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |00\rangle$. *Now if we apply* $CNOT_{1,2}$ *we obtain* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle$. *If we next apply* $CNOT_{2,3}$, *we obtain* $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. *This state is known as the GHZ state. See Figure 1*

3.1.1 Hadamard test

Hadamard test is an important quantum subroutine to measure amplitudes of quantum experiments. Suppose we have a quantum experiment according to the unitary matrix U. We also have a quantum state $|\psi\rangle$ stored in a quantum memory. Our objective is to estimate the amplitude $\langle\psi, U\psi\rangle$. Similar to $CNOT$, we can implement controlled-U operations. See Figure 2. In particular, if the control bit is set to $|0\rangle$, then the gate applies identity to the second bit, and if the control bit is set to $|1\rangle$, it applies U. Using the tensor product notation, the controlled U operations is $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$.

Now we analyze the circuit in Figure 2. We start with $|0\rangle|\psi\rangle$. After the application of the first Hadamard we obtain $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\psi\rangle$. Next we apply controlled U and obtain $\frac{|0\rangle|\psi\rangle+|1\rangle U|\psi\rangle}{\sqrt{2}}$. Next we apply Hadamard another time and obtain:

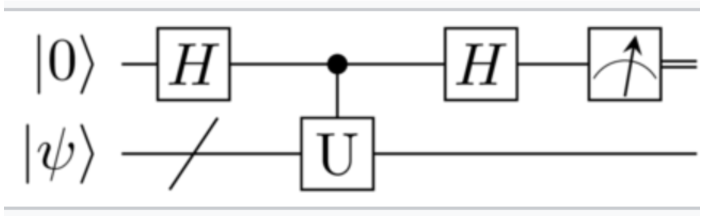
$$\frac{|0\rangle|\psi\rangle + |1\rangle|\psi\rangle + |0\rangle U|\psi\rangle - |0\rangle U|\psi\rangle}{2} = |0\rangle(\frac{I+U}{2})|\psi\rangle + |1\rangle(\frac{I-U}{2})|\psi\rangle$$

What is the probability of obtaining 0 from this experiment? We now tell you an important rule. Suppose we have quantum state that can be written as $|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle$. We can show that the probability of obtaining 0 is $\langle\phi_0, \phi_0\rangle$ and the probability of obtaining 1 is $\langle\phi_1, \phi_1\rangle$.

Exercise: Prove this!

Therefore with probability $\frac{1}{4}\langle\psi|(I + U^\dagger)(I + U)|\psi\rangle = \frac{1}{2}(1 + Re(\langle\psi|U|\psi\rangle))$ we obtain 0 and with probability $\frac{1}{4}\langle\psi|(I - U^\dagger)(I - U)|\psi\rangle = \frac{1}{2}(1 - Re(\langle\psi|U|\psi\rangle))$ we obtain 1. We claim that if we output $X = +1$ upon measuring 0 and $X = -1$ upon measuring 1, then the expectation value of X will be $Re(\langle\psi|U|\psi\rangle)$. To see this let $\alpha = Re(\langle\psi|U|\psi\rangle)$. Then $Pr(X = 0) = \frac{1+\alpha}{2}$ and $Pr(X = 1) = \frac{1-\alpha}{2}$. Therefore $E(X) = Pr(X = 0) - Pr(X = 1) = \alpha$. To recover α, we repeat the experiment a few times to obtain $X_1, \ldots, X_k$. We then compute $\frac{X_1+\ldots+X_k}{k}$ and output it as an estimation to α. From basis probability theory we know that the probability of error decays as $O(\frac{1}{\sqrt{k}}$. So, in order to make the error ϵ, we need to repeat the experiment at least $\Omega(1/\epsilon^2)$.

Figure 2: The Hadamard circuit



This experiment yields the real part of the amplitude $\langle\psi|U|\psi\rangle$. To obtain the imaginary part we can design a similar experiment. We leave it as an exercise for your practice.

Exercise: Design a quantum algorithm to estimate the imaginary part of a quantum amplitude.

3.1.2 Multi-qubit Pauli strings

An important class of multi-qubit operations are Pauli strings. A Pauli string is a tensor product of Pauli operators such as $X \otimes X$, $X \otimes Y$, $I \otimes Y$, etc. In general, any operator like $P_1 \otimes \ldots \otimes P_n$ for $P_i \in \{I, X, Y, Z\}$ is a Pauli string.

Recall the Clifford gate set is the group of operators that can be generated by $S, H, CNOT$. We know that this gate set generates the Pauli string. To se this we note that $Z = S^2$, $X = HZH$ and $Y = iZX$. We can show that the set of Pauli strings (up to a global phase) is closed under conjugation by Pauli strings. We can see this using the following exercise.

Exercise: The conjugation of a matrix A by another matrix B is according to BAB^{-1}. In this exercise, we want to study the conjugation of Pauli strings by Clifford circuits. Let P be the tensor product of any two Pauli strings and let C be any Clifford operations. Show that, up to a global phase, CPC^{-1} is a Pauli string. (Hint: You only need to show this for XI, ZI, IX, IZ, because these four operators generate all Pauli strings. Can you see why that is enough?)

Remark 3.3. Mathematically speaking, the Clifford group is the normalizer of the Pauli group. The Pauli group is the group of Pauli strings under multiplication. The Pauli group $\mathcal{P}$ includes four copies of each Pauli string, one for either of the four global phases $1, -1, i$ or $-i$. In other words, $\mathcal{P} = \{e^{im\pi/2} P_1 \otimes \ldots \otimes P_n : P_i \in \{I, X, Y, Z\}, m = 0, 1, 2, 3\}$. We previously discussed in class that according to a well-known theorem of Gottesman and Knill, the Clifford circuits are classically simulable. The proof of this theorem heavily relies on the Clifford group being the normalizer of the Pauli group. We will discuss more details about this theorem in future lectures.

4 No cloning theorem

Now that we learned about multi-qubit systems, we can ask a basic question: can we use quantum operations to produce multiple copies of a quantum state? One of the main features of classical computing is the capability to copy quantum states. Can we copy quantum states? In particular, is there a quantum operation to clone an arbitrary quantum state $|\psi\rangle$: $|\psi\rangle|0\rangle \rightarrow |\psi\rangle|\psi\rangle$? It turns out the answer is no. For instance, suppose you have a quantum state, and you don't know if it is the state $|0\rangle$ or $|+\rangle$. How can we copy this quantum state if it is either of the two incompatible bases? There is a simple reason to see why quantum operations are not capable of cloning quantum states. The reason is simply that cloning is a nonlinear operation, and quantum mechanics is a linear theory.

We can show the no-cloning theorem in a different way. Suppose there existed a cloning quantum operation U such that $U(|\psi\rangle \otimes |0\rangle) = (|\psi\rangle \otimes |\psi\rangle)$. For any other state $|\phi\rangle$ we have $U(|\phi\rangle \otimes |0\rangle) = (|\phi\rangle \otimes |\phi\rangle)$. What is the inner product of the two sides of each equation? $(\langle\psi| \otimes \langle 0|)U^\dagger U(|\phi\rangle \otimes |0\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle)$. Hence $\langle\psi, \phi\rangle = |\langle\psi, \phi\rangle|^2$. Which is a contradiction (for instance, let $|\psi\rangle = |0\rangle$ and $|\phi\rangle = |+\rangle$). However, cloning is possible only on an orthonormal basis (which is not more powerful than classical computations).