Hidden Subgroups and Quantum Computation

Lecture 03

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

July 03, 2025

Overview

Today we will investigate a way to "multiply" Hilbert spaces using the tensor product $(-) \otimes (-) : \mathsf{FdHilb}_{\mathbb{C}} \times \mathsf{FdHilb}_{\mathbb{C}} \to \mathsf{FdHilb}_{\mathbb{C}}$.

Then, we will look at the four postulates or axioms of quantum mechanics. We will delay our discussion of group representations until the relevant theory is necessary for our study of the HSP.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Let $\mathsf{FdHilb}_{\mathbb{C}}$ denote the collection of all finite dimensional Hilbert spaces.[1] Remember, up to isomorphism, $\mathsf{FdHilb}_{\mathbb{C}}$ contains copies of the Hilbert space $(\mathbb{C}^n, (-,-))$ for different n.

In particular, between every pair of spaces $\mathcal{H}, \mathcal{K} \in \mathsf{FdHilb}_{\mathbb{C}}$, we have a set of linear transformations

$$\mathrm{Hom}_{\mathbb{C}}(\mathcal{H}, \mathcal{K}).$$

[1] We are intentionally being ambiguous about what "collection" means here. Any sort of size issues can be taken care of formally.

A function $\varphi : \mathcal{H} \times \mathcal{K} \to \mathcal{J}$ between Hilbert spaces is called bilinear if both

(i) for all $k \in \mathcal{K}$, the function $h \mapsto \varphi(h, k)$ is a linear transformation $\mathcal{H} \to \mathcal{J}$.

(ii) for all $h \in \mathcal{H}$, the function $k \mapsto \varphi(h, k)$ is a linear transformation $\mathcal{K} \to \mathcal{J}$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Define the tensor product bifunctor to be the function which assigns to each pair of spaces $(\mathcal{H}, \mathcal{K}) \in \mathsf{FdHilb}_{\mathbb{C}} \times \mathsf{FdHilb}_{\mathbb{C}}$

(i) a finite dimensional space $\mathcal{H} \otimes \mathcal{K}$.

(ii) a bilinear function $h : \mathcal{H} \times \mathcal{K} \to \mathcal{H} \otimes \mathcal{K}$

such that for all bilinear functions $\varphi : \mathcal{H} \times \mathcal{K} \to \mathcal{J}$, there is a unique linear transformation $\widetilde{\varphi} : \mathcal{H} \otimes \mathcal{K} \dashrightarrow \mathcal{J}$ such that $\varphi = \widetilde{\varphi} \circ h$.

Theorem

The tensor product $\mathcal{H} \otimes \mathcal{K}$ *exists for any pair* $\mathcal{H}, \mathcal{K} \in \mathsf{FdHilb}_{\mathbb{C}}$.

You may see the notation $\mathcal{H} \otimes_{\mathbb{C}} \mathcal{K}$ for the tensor product, which is perhaps more precise. The $\mathbb{C}$ tells us that our relevant Hilbert spaces are all $\mathbb{C}$-linear.

The "reason" we call $(-) \otimes (-) : \mathsf{FdHilb}_{\mathbb{C}} \times \mathsf{FdHilb}_{\mathbb{C}} \to \mathsf{FdHilb}_{\mathbb{C}}$ a bifunctor is due to the following observation.

If $\varphi \in \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}, \mathcal{J})$ and $\psi \in \mathrm{Hom}_{\mathbb{C}}(\mathcal{K}, \mathcal{L})$, then there is actually a unique homomorphism

$$\varphi \otimes \psi : \mathcal{H} \otimes \mathcal{K} \to \mathcal{J} \otimes \mathcal{L}$$

such that $(\varphi \otimes \psi)(h \otimes k) = \varphi(h) \otimes \psi(k)$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Further, if we have compositions

$$\mathcal{H} \xrightarrow{\varphi_1} \mathcal{K} \xrightarrow{\varphi_2} \mathcal{M}$$

and

$$\mathcal{J} \xrightarrow{\psi_1} \mathcal{L} \xrightarrow{\psi_2} \mathcal{N},$$

then

$$(\varphi_2 \circ \varphi_1) \otimes (\psi_2 \circ \psi_1) : \mathcal{H} \otimes \mathcal{M} \to \mathcal{J} \otimes \mathcal{N}$$

is the same as

$$(\varphi_2 \otimes \psi_2) \circ (\varphi_1 \otimes \psi_1) : \mathcal{H} \otimes \mathcal{M} \to \mathcal{J} \otimes \mathcal{N}.$$

Since $\mathcal{H} \times \mathcal{K} \to \mathcal{H} \otimes \mathcal{K}$ is bilinear, sending pairs $(h, k) \mapsto h \otimes k$, we can always compute in the following way:

$$\begin{aligned} \alpha((h+g) \otimes k) &= \alpha(h+g) \otimes k \\ &= \alpha h + \alpha g \otimes k \\ &= \alpha(h \otimes k) + \alpha(g \otimes k) \\ &= h \otimes \alpha k + g \otimes \alpha k. \end{aligned}$$

If β is a basis for $\mathcal{H}$ of size n, and γ is a basis for $\mathcal{K}$ of size m, then it can be shown that the set

$$\delta = \{b \otimes g : b \in \beta \text{ and } g \in \gamma\}$$

is a basis for $\mathcal{H} \otimes \mathcal{K}$. Thus,

$$\dim(\mathcal{H} \otimes \mathcal{K}) = |\delta| = nm.$$

Taking the tensor product of finite dimensional spaces multiplies their dimensions!

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

It is important to note that while the set δ of tensors forms a basis for $\mathcal{H} \otimes \mathcal{K}$, i.e., every $v \in \mathcal{H} \otimes \mathcal{K}$ can be written as a combination

$$v = \sum_{i=1}^{nm} \alpha_i (b \otimes g)_i, \quad (b \otimes g) \in \delta,$$

it is *not* the case that every v is of the form $h \otimes k$, where $h \in \mathcal{H}$ and $k \in \mathcal{K}$. When this is possible, we call such a tensor simple.

We will often care about spaces of the form

$$\mathcal{H} \simeq \mathbb{C}^2 \underbrace{\otimes \cdots \otimes}_{n \text{ times}} \mathbb{C}^2.$$

For this, we have a shorthand $(\mathbb{C}^2)^{\otimes n}$.

Let $\varphi : \mathbb{C}^2 \to \mathbb{C}^2$ and $\psi : \mathbb{C}^2 \to \mathbb{C}^2$ be linear transformations. Then, we have the transformation

$$\varphi \otimes \psi : (\mathbb{C}^2)^{\otimes 2} \to (\mathbb{C}^2)^{\otimes 2}.$$

But what does $\varphi \otimes \psi$ do?

Write

$$\varphi \doteq \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} \text{ and } \psi \doteq \begin{pmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{pmatrix}.$$

Then, $\varphi \otimes \psi$ takes on the form of the Kronecker product

$$\varphi \otimes \psi \doteq \begin{pmatrix} \varphi_{11} \begin{pmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{pmatrix} & \varphi_{12} \begin{pmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{pmatrix} \\ \varphi_{21} \begin{pmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{pmatrix} & \varphi_{22} \begin{pmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{pmatrix} \end{pmatrix}.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

$$\varphi \otimes \psi \doteq \begin{pmatrix} \varphi_{11}\psi_{11} & \varphi_{11}\psi_{12} & \varphi_{12}\psi_{11} & \varphi_{12}\psi_{12} \\ \varphi_{11}\psi_{21} & \varphi_{11}\psi_{22} & \varphi_{12}\psi_{21} & \varphi_{12}\psi_{22} \\ \varphi_{21}\psi_{11} & \varphi_{21}\psi_{12} & \varphi_{22}\psi_{11} & \varphi_{22}\psi_{12} \\ \varphi_{21}\psi_{21} & \varphi_{21}\psi_{22} & \varphi_{22}\psi_{21} & \varphi_{22}\psi_{22} \end{pmatrix}$$

The same process works for arbitrary, finite dimensions.

In Dirac notation, you will often see the shorthands

$$|\varphi\rangle \otimes |\psi\rangle = |\varphi\rangle\,|\psi\rangle = |\varphi\psi\rangle\,.$$

We know that $\{|0\rangle, |1\rangle\}$ is a basis for $\mathbb{C}^2$. Then,

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

should be a basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$. The Kronecker product will make this obvious.

First, we know that $\dim(\mathbb{C}^2)^{\otimes 2} = 2^2 = 4$, so $(\mathbb{C}^2)^{\otimes 2} \simeq \mathbb{C}^4$.
Further, we know we can write

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Using the Kronecker product, we see

$$|00\rangle \doteq \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle \doteq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle \doteq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ and } |11\rangle \doteq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Thus, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is effectively just the standard basis for $\mathbb{C}^4$, which we know is isomorphic to $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Recall that given a square matrix representing $\varphi : \mathbb{C}^n \to \mathbb{C}^n$, its trace $\mathrm{tr}(\varphi)$ is the sum along its diagonal.

We say that $\varphi : \mathcal{H} \to \mathcal{H}$ is positive (semi-definite) if for all $h \in \mathcal{H}$, the inner product $(\varphi h, h) \geq 0$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Axiom I: State Space

Any finite quantum system Q is represented by a complex Hilbert space $\mathcal{H}^Q \in \mathsf{FdHilb}_{\mathbb{C}}$, called the state space. States of the system are represented by unit-trace, positive operators acting on $\mathcal{H}$, called the density operators $\mathcal{D}(\mathcal{H}) \subseteq \mathrm{Hom}_{\mathbb{C}}(\mathcal{H})$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Axiom II: Multiple System

Any pair of quantum systems A and B can be represented as a joint system AB via the tensor product in $\mathsf{FdHilb}_{\mathbb{C}}$:

$$\mathcal{H}^{AB} = \mathcal{H}^{A} \otimes \mathcal{H}^{B}.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

That is, in our framework, the tensor product bifunctor $(-) \otimes (-)$ is precisely a way to join quantum systems.

Axiom III: System Evolution

A quantum system Q undergoing closed evolution is described by a unitary transformation on the state space $\mathcal{H}^Q$.

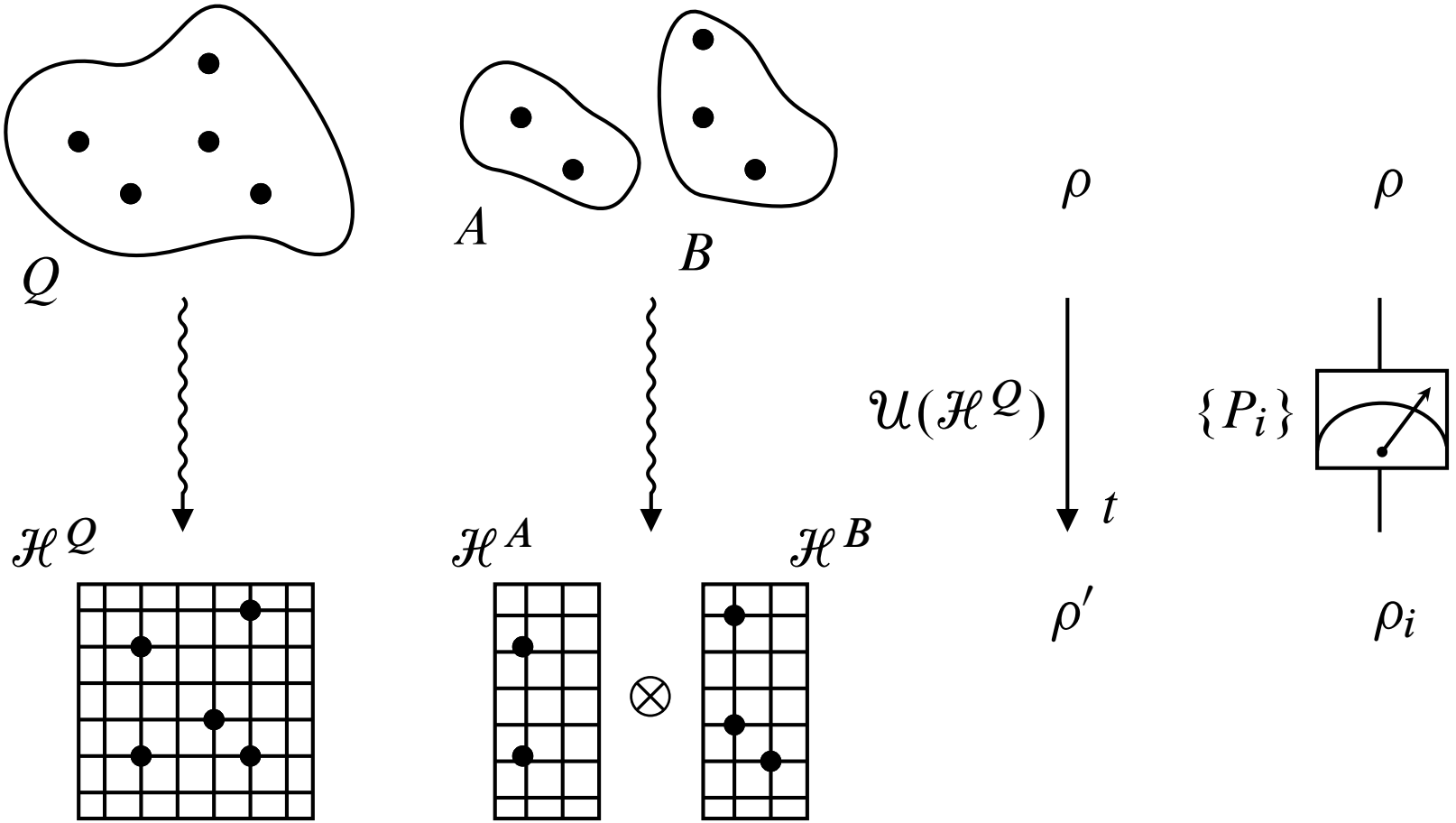
Remember, a unitary $U \in \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}^Q)$ means $UU^\dagger = U^\dagger U = I^Q$.

Axiom IV: Measurement

Every measurement of a finite dimensional quantum system is described by a set of orthogonal projectors $\{P_i\}_{i=1}^r$ such that $\sum_{i=1}^r P_i = I^Q$. If ρ is the state of Q prior to measurement, then with probability $\mathbb{P}(i) = \mathrm{tr}(P_i \rho)$, the post-measurement state is

$$\rho_i = \frac{P_i \rho P_i}{\mathbb{P}(i)}.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN


Q
A
B
$\mathcal{H}^Q$
$\mathcal{H}^A$
$\mathcal{H}^B$
$\otimes$
ρ
$\mathcal{U}(\mathcal{H}^Q)$
t
ρ'
ρ
$\{P_i\}$
ρ_i

Next time we will discuss

(i) the (unitary) quantum circuit model.

(ii) the preliminary definitions and motivation for the hidden subgroup problem.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN