Hidden Subgroups and Quantum Computation

Lecture 02

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

June 26, 2025

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Overview

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Today we will look at a restriction of the notion of an abelian group called a vector space. In particular, we will focus our attention to $\mathbb{C}$-linear spaces, developing the language of inner products and Dirac's bra-ket notation.

Quantum mechanics is traditionally framed in the language of Hilbert spaces. Since quantum computation considers finite dimensional systems with n physical qubits, we may restrict ourselves to the theory of finite dimensional Hilbert spaces.

Luckily for us, finite dimensional Hilbert spaces are only a slightly enriched version of finite dimensional vector spaces. This brings us to our discussion of linear algebra.

A complex vector space is a triple $(\mathcal{V}, +, \cdot)$, where $(-) + (-) : \mathcal{V}^2 \to \mathcal{V}$ is an operation and $(-)(-) : \mathbb{C} \times \mathcal{V} \to \mathcal{V}$ is an action $\mathbb{C} \curvearrowright \mathcal{V}$.

In particular, $(\mathcal{V}, +)$ must form an abelian group, and the action is a way to multiply vectors in $\mathcal{V}$ by scalars in $\mathbb{C}$. We require that

(i) for all $v \in \mathcal{V}$, $1v = v$.

(ii) for all $\alpha_1, \alpha_2 \in \mathbb{C}$ and $v \in \mathcal{V}$, $(\alpha_1\alpha_2)v = \alpha_1(\alpha_2 v)$.

(iii) for all $\alpha_1, \alpha_2 \in \mathbb{C}$ and $v \in \mathcal{V}$, $(\alpha_1 + \alpha_2)v = \alpha_1 v + \alpha_2 v$.

(iv) for all $\alpha \in \mathbb{C}$ and $v_1, v_2 \in \mathcal{V}$, $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

An element $v \in \mathcal{V}$ of the form

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_n v_n = \sum_{i=1}^{n} \alpha_i v_i ,$$

where $v_i \in \mathcal{V}$ and $\alpha_i \in \mathbb{C}$, is called a linear combination.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

A subset $S \subseteq \mathcal{V}$ is linearly independent if there does not exist an $s \in S$ so that s is a linear combination of elements in S.

A subspace $\mathcal{W} \subseteq \mathcal{V}$ is a nonempty subset which is closed under addition and scalar multiplication.

Let $S \subseteq \mathcal{V}$ be a subset. Then,

$$\operatorname{span} S = \left\{ \sum_{i=1}^{n} \alpha_i v_i : \alpha_i \in \mathbb{C} \text{ and } v_i \in \mathcal{V} \right\}.$$

That is, $\operatorname{span} S$ is the subspace of all linear combinations of elements in S. In fact, this is the smallest subspace of $\mathcal{V}$ containing S, so we could call it the subspace generated by S, as we did with subgroups.

A basis β of a vector space $\mathcal{V}$ is a linearly independent, minimal (with respect to cardinality) spanning set of $\mathcal{V}$.

Assuming the axiom of choice, we get the following.[1]

Theorem

Every vector space has a basis.

Without choice, we are restricted to "finite dimensional" spaces, though then we would have to define a finite dimensional vector space as one which is finitely generated, as opposed to the basis-dependent definition which follows.

[1] Andreas Blass showed (1984) that the existence of bases implies the axiom of choice, so the statements are, in fact, equivalent.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The dimension of a vector space $\mathcal{V}$ is the cardinality of any basis β of $\mathcal{V}$. We write $\dim \mathcal{V} = |\beta|$.

A vector space homomorphism (linear transformation) is an abelian group homomorphism $\varphi : \mathcal{V}_1 \to \mathcal{V}_2$ such that for all $\alpha \in \mathbb{C}$ and $v \in \mathcal{V}$,

$$\varphi(\alpha v) = \alpha\varphi(v).$$

That is, a linear transformation is a function which preserves the additive and scalar multiplicative structure.

As before, a bijective linear transformation $\varphi : \mathcal{V} \to \mathcal{W}$ is called an isomorphism. When such a φ exists, we write $\mathcal{V} \simeq \mathcal{W}$.

Theorem

Every finite dimensional (complex) vector space with $\dim \mathcal{V} = n$ *admits an isomorphism* $\mathcal{V} \simeq \mathbb{C}^n$.

For instance, the space of matrices $\mathbb{M}_{m\times n}(\mathbb{C})$ is of dimension mn, so there is an isomorphism

$$\varphi : \mathbb{M}_{m\times n}(\mathbb{C}) \to \mathbb{C}^{nm}.$$

Denote by $\mathrm{Hom}_{\mathbb{C}}(\mathcal{V}_1, \mathcal{V}_2)$ the set of vector space homomorphisms from $\mathcal{V}_1$ to $\mathcal{V}_2$.

Then, $\mathrm{Hom}_{\mathbb{C}}(\mathcal{V}_1, \mathcal{V}_2)$ is a $\mathbb{C}$-linear space.

An inner product on $\mathcal{H}$ is a map

$$(-,-) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

satisfying, for all $v_1, v_2 \in \mathcal{H}$,

(i) $(v_1, v_2) = (v_2, v_1)^*$.

(ii) linearity in the second argument.

(iii) $(v_1, v_1) \geq 0$, where equality holds if and only if $v_1 = 0$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

An inner product space is a pair $(\mathcal{H}, (-,-))$ consisting of a vector space and an inner product.

For our purposes, a Hilbert space will be any finite dimensional inner product space.[2]

[2]The more analytic definition you may have seen arises when considering infinite dimensional spaces.

Let $(\mathcal{H}, (-,-))$ be a (finite dimensional) Hilbert space; let $\varphi : \mathcal{H} \to \mathcal{H}$ be a linear transformation. Then, the adjoint of φ is a transformation $\varphi^\dagger : \mathcal{H} \to \mathcal{H}$ such that

$$(\varphi v_1, v_2) = (v_1, \varphi^\dagger v_2), \quad v_1, v_2 \in \mathcal{H}.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

When $\dim \mathcal{H} = n < \infty$, we have that $\varphi^\dagger$ corresponds to taking the conjugate transpose of the matrix representing φ.

Given a space $\mathcal{H}$, the dual space $\mathcal{H}^*$ is the space $\mathrm{Hom}_{\mathbb{C}}(\mathcal{H}, \mathbb{C})$.

It is common to call such a homomorphism $\mathcal{H} \to \mathbb{C}$ a linear functional.

Given an element $v \in \mathcal{H}$, there is an induced functional $v^\dagger \in \mathcal{H}^*$ which, in finite dimension n, corresponds to taking

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}^\dagger = \begin{pmatrix} v_1^* & \cdots & v_n^* \end{pmatrix}.$$

The usual inner product on $\mathbb{C}^n$ is given by

$$(v_1, v_2) = v_1^\dagger v_2 = \sum_{i=1}^{n} v_{1_i}^* v_{2_i} .$$

In 1939, Paul Dirac introduced the bra-ket notation for doing linear algebra in the context of quantum mechanics.

While it remains unused (and often, unknown) by many mathematicians, it is ubiquitous in quantum.

Given a Hilbert space $\mathcal{H}$ associated to our quantum system, we call the vectors in $\mathcal{H}$ kets, denoting them by

$$|\psi\rangle \in \mathcal{H}.$$

The elements of $\mathcal{H}^*$ are called bras, denoting the functional associated to a ket $|\psi\rangle \in \mathcal{H}$ by

$$\langle\psi| \in \mathcal{H}^*.$$

We define the inner product (or braket) of $|\psi\rangle$ and $|\varphi\rangle$ in $\mathcal{H}$ by

$$|\psi\rangle^\dagger |\varphi\rangle = \langle\psi|\varphi\rangle .$$

The outer product (or ketbra) of $|\psi\rangle$ and $|\varphi\rangle$ in $\mathcal{H}$ is given by

$$|\psi\rangle\,|\varphi\rangle^{\dagger} = |\psi\rangle\langle\varphi|\,.$$

The braket $\langle -|-\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ is precisely the standard inner product, whereas the ketbra $|-\rangle\langle -| : \mathcal{H} \times \mathcal{H} \to \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}, \mathcal{H})$ corresponds, in finite dimension n, to the product

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}^{\dagger} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \begin{pmatrix} w_1^* & \cdots & w_n^* \end{pmatrix},$$

which is a matrix in $\mathbb{M}_n(\mathbb{C}) \simeq \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n, \mathbb{C}^n)$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The standard basis for $\mathbb{C}^n$, usually denoted by

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

is instead written $|1\rangle, |2\rangle, \ldots, |n\rangle$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

It is worth noting, however, that for $\mathbb{C}^2$ we usually write

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

Next time we will discuss

(i) tensor products $\mathcal{H} \otimes \mathcal{K}$.

(ii) group representations $\rho : G \to \mathrm{Aut}(\mathcal{V})$.

Then, we can begin discussing the postulates of quantum mechanics and rudiments of quantum computation.