

# Advanced Linear Algebra for Quantum Computing

Sam Burdick

Topological Quantum Error Correction

November 5, 2025

# Agenda

- ▶ Vector spaces
- ▶ Basis vectors
- ▶ Linear maps
- ▶ Dirac notation
- ▶ Linear functionals and dual spaces
- ▶ Eigenstates
- ▶ Unitary matrices
- ▶ Tensor products
- ▶ The commutator
- ▶ Matrix trace
- ▶ Riesz representation theorem
- ▶ Spectral theorem

We assume existing familiarity with sets, functions, matrices, vectors, summation notation, and complex numbers.

*I discovered that the library is the real school.*

—Ray Bradbury

# Vector spaces

## Definition

$V$  is a vector space if it is a set of vectors coupled with the addition of vectors and scalar multiplication.

Vector addition:  $\mathbf{u}, \mathbf{v} \in V$  means that  $\mathbf{u} + \mathbf{v} \in V$ .

Scalar multiplication:  $\alpha \mathbf{v} \in V$  for any  $\mathbf{v} \in V, \alpha \in \mathbb{C}$ .

## Remark

The vector space we often use in quantum computing is  $\mathbb{C}^n$ , where  $n$  is a power of 2.

## Example

$$\begin{pmatrix} 42 \\ 1.618 \\ e^{i\pi/3} \\ 1 + i \end{pmatrix} \in \mathbb{C}^4$$

# Linear independence and basis vectors

## Definition

Given a set of vectors  $S = \{\mathbf{v}_1, \dots, \mathbf{v}_m\}$  we say that  $S$  is linearly independent if

$$\sum_{k=1}^m \alpha_k \mathbf{v}_k = \mathbf{0},$$

where  $\mathbf{0}$  is the zero vector, if  $\alpha_k = 0$  for all  $1 \leq k \leq m$ .

## Definition

If a set of vectors  $T$  can be combined in a linear fashion to produce every element of  $S$ , we say that  $T$  spans  $S$ .

## Definition

Suppose  $V$  is a vector space. Then a minimum cardinality subset  $B \subseteq V$  that is linearly independent and spans  $V$  is a basis of  $V$ .

# Linear maps

## Definition

A linear map is a function  $T : U \rightarrow V$ , where  $U$  and  $V$  are vector spaces, such that

$$T(\mathbf{u}_1 + \mathbf{u}_2) = T(\mathbf{u}_1) + T(\mathbf{u}_2) \text{ for all } \mathbf{u}_1, \mathbf{u}_2 \in U$$

and

$$T(\alpha \mathbf{u}) = \alpha T(\mathbf{u}) \text{ for all } \mathbf{u} \in U, \alpha \in \mathbb{C}.$$

## Example

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a linear map  $H : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ .

# Dirac notation

## Definition

A ket (or state vector)  $|\psi\rangle$  is a normalized vector in the vector space  $\mathbb{C}^n$ , meaning that  $\sum_{k=1}^n |\psi_k|^2 = 1$  and  $\psi_k$  is the  $k$ th element of  $|\psi\rangle$ .

## Definition

A bra-ket  $\langle\phi|\psi\rangle$  is the inner product of  $|\phi\rangle$  and  $|\psi\rangle$ ,

$$\langle\phi|\psi\rangle = \sum_{k=1}^n \phi_k^* \psi_k,$$

where the bra  $\langle\phi|$  acts as a functional map (from a ket to a scalar; more on this later) on  $|\psi\rangle$ .

## Example

For any quantum state  $|\psi\rangle$ ,  $\langle\psi|\psi\rangle = 1$ , since  $\psi_k \psi_k^* = |\psi_k|^2$ .

# Dirac notation (cont'd)

## Theorem (Cauchy-Schwarz Inequality)

For any two quantum states  $|\phi\rangle$  and  $|\psi\rangle$ , we have  $|\langle\phi|\psi\rangle|^2 \leq 1$ .

## Definition

A ket-bra  $|\phi\rangle\langle\psi|$  is a linear map (or outer product)

$$\begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} (\psi_1^*, \dots, \psi_n^*) = \begin{pmatrix} \phi_1\psi_1^* & \dots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \dots & \phi_n\psi_n^* \end{pmatrix}$$

## Remark

Given a linear map  $A$  and bra  $\langle\phi|$ ,  $\langle\phi|A$  is also a bra defined by the function composition rule

$$(\langle\phi|A)|\psi\rangle = \langle\phi|(A|\psi\rangle) = \langle\phi|A|\psi\rangle$$

# Linear functionals and dual spaces

## Definition

A linear functional  $f$  is a mapping between elements of a vector space into the complex plane (ie,  $f : V \rightarrow \mathbb{C}$ ) such that

$$f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) \text{ and } f(\alpha\mathbf{u}) = \alpha f(\mathbf{u})$$

for any  $\mathbf{u}, \mathbf{v} \in V$  and  $\alpha \in \mathbb{C}$ .

## Definition

The dual space of a vector field  $V$  is the set of all linear functionals over  $V$ .

## Remark

The bra  $\langle\phi|$  is a member of the dual space of the vector space containing  $|\phi\rangle$ . As stated previously, the bra-ket represents the mapping of state vectors in  $\mathbb{C}^n$  into  $\mathbb{C}$ .



# Eigenstates

## Definition

A state vector  $|\psi\rangle$  is the  $\lambda$ -eigenstate (or eigenvector) of a linear map  $U$  if  $U|\psi\rangle = \lambda|\psi\rangle$  for some  $\lambda \in \mathbb{R}$ , where  $\lambda$  is said to be an eigenvalue of  $U$  (and corresponds to a measurement of a quantum gate).

## Example

If  $U|\psi\rangle = |\psi\rangle$ , we say that  $|\psi\rangle$  is the  $+1$  eigenstate of  $U$ .

## Exercise

Show that  $|+\rangle$  is the  $+1$  eigenstate of  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

## Exercise

Show that  $|0\rangle$  and  $|1\rangle$  are the  $+1$  and  $-1$  eigenstates of  $Z$ .

# Unitary matrices

## Definition

The conjugate of a matrix  $U$  is denoted  $U^*$  and obtained by conjugating each of its elements.

## Definition

The transpose of a matrix  $U$  is denoted  $U^T$  and is obtained by systematically exchanging (i.e., swapping) the values of the rows with the values in the columns in  $U$ .

## Definition

The adjoint of a matrix  $U$  is the conjugate transpose

$$U^\dagger = (U^*)^T = \begin{pmatrix} u_{1,1}^* & \cdots & u_{1,n}^* \\ \vdots & \ddots & \vdots \\ u_{n,1}^* & \cdots & u_{n,n}^* \end{pmatrix}^T = \begin{pmatrix} u_{1,1}^* & \cdots & u_{n,1}^* \\ \vdots & \ddots & \vdots \\ u_{1,n}^* & \cdots & u_{n,n}^* \end{pmatrix}$$

# Unitary matrices (cont'd)

## Definition

A matrix  $U$  is hermitian if it is self-adjoint, that is,  $U = U^\dagger$ .

## Definition

A matrix  $U$  is unitary if  $UU^\dagger = U^\dagger U = I$ .

## Exercise

Show that every quantum operator is unitary.

*Hint.* Use the fact that  $\langle\psi|\psi\rangle = 1$  and substitute  $|\psi\rangle$  for  $U|\psi\rangle$  for an arbitrary operator  $U$ . Then use function composition rules.

# Tensor products

## Definition

For two-dimensional, normalized quantum states  $|\phi\rangle$   $|\psi\rangle$ , the tensor product between them is

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} \otimes \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} = \begin{pmatrix} \phi_1 \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \\ \phi_2 \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \phi_1\psi_1 \\ \phi_1\psi_2 \\ \phi_2\psi_1 \\ \phi_2\psi_2 \end{pmatrix}$$

## Remark

You can take tensor products of matrices as well; the new object's dimension is the product of the dimensions of the objects multiplied, meaning that tensor products of higher-dimensional objects quickly become unmanageable to compute by hand.

# The commutator

## Definition

Two matrices  $A$  and  $B$  are said to commute if  $AB = BA$ .

## Remark

For quantum operators  $A$  and  $B$ ,  $(AB)|\psi\rangle$  means “apply  $B$  first, then  $A$ , on  $|\psi\rangle$ .”

## Definition

The commutator of two matrices is defined as  $[A, B] = AB - BA$ .

## Corollary

For commuting matrices,  $[A, B] = \mathcal{O}$  (the zero matrix).

## Exercise

Show that  $[X, Z] = -2iY$ .

# Matrix trace

## Definition

The trace of a matrix  $A$  is the sum of its diagonal elements; that is

$$\operatorname{tr}(A) = \sum_{k=1}^n A_{k,k}$$

## Remark

Trace is “commutativity-preserving,” meaning  $\operatorname{tr}(AB) = \operatorname{tr}(BA)$  for any matrices  $A, B$ .

## Remark

The trace is independent of a chosen basis, meaning that if a linear map  $A$ , represented by a matrix, has a “change-of-basis” matrix  $P$  such that  $B = P^{-1}AP$ , then  $\operatorname{tr}(A) = \operatorname{tr}(B)$ .

# Riesz Representation Theorem

## Definition

A Hilbert space  $\mathcal{H}$  in quantum computing is a complex inner product space, that is, a vector space over  $\mathbb{C}^n$  endowed with an inner product operation.

## Definition

A linear map  $T$  is anti-linear if

$$T(\alpha |\psi\rangle + \beta |\psi\rangle) = \alpha^* T |\psi\rangle + \beta^* T |\psi\rangle.$$

## Definition

Two vector spaces  $V$  and  $W$  are isomorphic if there exists a bijective linear map  $T : V \rightarrow W$ , meaning that

- ▶ (it's injective) every unique vector in  $V$  maps to a unique vector in  $W$  (that is, if  $T(\mathbf{u}) = T(\mathbf{v})$  then  $\mathbf{u} = \mathbf{v}$ ) and
- ▶ (it's surjective) that for every vector  $\mathbf{w} \in W$  there exists a vector  $\mathbf{v} \in V$  such that  $T(\mathbf{v}) = \mathbf{w}$ .

# Riesz Representation Theorem (cont'd)

## Definition

An isomorphism is canonical if it is defined by the intrinsic mathematical properties of the vector spaces it acts on, that is, no additional change-of-basis matrix is necessary to perform it.

## Theorem (Riesz)

For any Hilbert space  $\mathcal{H}$  there exists its canonical anti-linear isomorphism between  $\mathcal{H}$  and its dual space  $\mathcal{H}^*$ .

## Remark

The Riesz representation theorem is how we ensure a bijective, normalization-preserving correspondence between bras and kets; we will often write  $|\psi\rangle = (\langle\psi|)^\dagger$ , where the Hermitian conjugate operator  $\dagger$  represents the conversion between a row and a column vector and conjugation of vector elements.



# Spectral Theorem

## Definition

A diagonal matrix is a matrix such that all entries outside the main diagonal are zero.

## Definition

The spectrum of a matrix  $A$  is the set of all eigenvalues of  $A$ .

## Definition

A matrix  $A$  is normal if  $[A, A^\dagger] = \mathcal{O}$ .

## Theorem

If a matrix  $A$  is normal, then  $A$  is unitarily diagonalizable, meaning that  $A = UDU^\dagger$  for some unitary matrix  $U$  comprising the eigenvectors of  $A$ , and a diagonal matrix  $D$ , where the diagonal values of  $D$  is the spectrum of  $A$ . Such a factorization is called the spectral decomposition of  $A$ .

# Spectral Theorem (cont'd)

## Example

## Remark

The spectral theorem tells us that, since the Pauli matrices  $\{X, Y, Z\}$  are hermitian, their eigenvalues are  $\pm 1$  and their eigenvectors form a mutually orthogonal ( $\langle \phi | \psi \rangle = 0$ ) and complete basis, justifying their use as the fundamental observables of a qubit.