Advanced Linear Algebra for Quantum Error Correction

Sam Burdick

Topological Quantum Error Correction

December 28, 2025

Agenda

1. Vector spaces
2. Basis vectors
3. Linear maps
4. Change of basis
5. Dirac notation
6. Subspaces
7. Orthonormal basis
8. Eigenstates
9. Unitary matrices
10. The Kronecker product
11. The commutator
12. Matrix trace
13. Projection operators
14. Clifford gate conjugation
15. Stabilizers
16. A five-qubit code
17. Spectral Theorem
18. * Linear functionals and dual spaces
19. * Riesz Representation Theorem
20. * Application: the uncertainty principle

* indicates supplemental content

To the reader

We assume existing familiarity with sets, functions, matrices, vectors, summation notation, probabilities, and complex numbers. I recommend Dr. Beezer's free textbook A First Course in Linear Algebra to newcomers. We also assume familiarity with the mathematical basics of quantum error correction (including quantum gates and the Pauli matrices) which is given in Dr. Fowler's free Coursera course on the subject.

> *Narrative is linear, but action has breadth*
> *and depth as well as height and is solid.*
> —Thomas Carlyle

> *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 $\mathbf{v} \in V, \alpha \in \mathbb{C}$.

Example

An *n*-qubit system's state vector occupies the vector space $\mathbb{C}^{2^n}$. A single qubit comprises the state vector $\binom{\alpha}{\beta}$, where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$.

Remark

Vector spaces have numerous other properties that show that vector space operations (vector addition and scalar multiplication) obey commutativity and associativity laws; they can be found here.

Linear independence and basis vectors

Definition

Given a set of vectors $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ 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 $\mathcal{B} \subseteq V$ that is linearly independent and spans V is a basis of V.

Linear maps

Definition

A linear map is a function $T : U \to V$, 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 $H : \mathbb{C}^2 \to \mathbb{C}^2$ acting on a single qubit $\binom{\alpha}{\beta}$.

Linear maps (cont'd)

Remark

In quantum computing, operators and observables are both represented as linear maps and $2^n \times 2^n$ matrices that act on state vectors of dimension 2^n.

Exercise

Show that the Pauli operators X and Z as well as the Clifford-T gates CNOT, H, S and T are linear maps.

Exercise

Linearity is also a property of sets of certain functions over other fields, including $\mathbb{R}$ and $\mathbb{C}$. Suppose $f(x)$ is differentiable for all $x \in \mathbb{R}$. Show that differentiation and integration of $f(x)$ are linear maps over sets of all such $f(x)$.

> *The map is not the territory.*
>
> —Alfred Korzybski

Change of basis

Definition

Given two vector spaces V and W, each of dimension n, the change of basis matrix is an $n \times n$ matrix $\mathcal{C}$. Let $\mathcal{V}$ and $\mathcal{W}$ denote matrices comprised of the basis vectors of V and basis vectors W expressed in terms of the basis vectors of V, respectively. Then $\mathcal{V} = \mathcal{C}\mathcal{W}\mathcal{C}^{-1}$.

Exercise

Verify that the Hadamard matrix H functions as a change of basis matrix between vectors in the X basis and the Z basis, and vice versa.

> *Change in all things is sweet.*
>
> —Aristotle

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 ψ_k is the kth 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 $|\psi\rangle$. The bra is the conjugate transpose of the corresponding ket.

Dirac notation (cont'd)

Theorem (Cauchy-Schwarz Inequality)

For any two state vectors $|\phi\rangle$ 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)

$$|\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} \left(\psi_1^*, \ldots, \psi_n^*\right) = \begin{pmatrix} \phi_1\psi_1^* & \cdots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \cdots & \phi_n\psi_n^* \end{pmatrix}$$

Remark

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

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

Dirac notation (cont'd)

Exercise

Demonstrate the Cauchy-Schwarz inequality for the state vectors $|+\rangle$ and $|-\rangle$.

Exercise

Compute the operator $|0\rangle \langle 1|$.

Exercise

Compute the ket $\langle - | \, H \, | + \rangle$.

Exercise

Show that for any state vector $|\psi\rangle$ that $\langle \psi | \psi \rangle = 1$. (Use the identity $zz^* = |z|^2$ for all $z \in \mathbb{C}$.)

Pick a flower on Earth and you move the farthest star.
—Paul Dirac

Subspaces

Definition

A set W is a subspace of a vector space V if W is itself a vector space and $W \subseteq V$.

Example

Consider the Bell pair $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. The state vector $|\Phi^+\rangle$ is a member of the (maximally entangled) subspace defined as

$$B = \left\{ \alpha\,|00\rangle + \beta\,|11\rangle : \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

Exercise

Show that B is a vector space, and then show that $B \subseteq \mathbb{C}^4$.

Happiness is a vector, it is movement.
—Neal Shusterman

Orthonormal basis

Definition

An orthonormal basis is a set of basis vectors $\mathcal{B}$ in a vector space with a Euclidean norm of 1, meaning $\sqrt{\sum_{k=1}^{n} |\psi_k|^2} = 1$ for all $|\psi\rangle \in \mathcal{B}$, and every pair of distinct vectors $|\phi\rangle, |\psi\rangle \in \mathcal{B}$ is orthogonal, meaning $\langle\phi|\psi\rangle = 0$.

Exercise

Show that the sets $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are both orthonormal bases of the single-qubit vector space $\mathbb{C}^2$.

> *The orthogonal features, when combined,*
> *can explode into complexity.*
> —Yukihiro Matsumoto

> *The endeavor to understand is the first and only basis of virtue.*
> —Baruch Spinoza

Eigenstates

Definition

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

Example

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

Exercise

Show that $|+\rangle$ and $|-\rangle$ are the $+1$ and -1 eigenstates of $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, respectively.

Exercise

Show that $|0\rangle$ and $|1\rangle$ are the $+1$ and -1 eigenstates of $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, respectively.

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, denoted $U^\dagger$, 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 the S and T gates are unitary but not Hermitian.

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.

The Kronecker product

Definition

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

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

and is sometimes denoted $|\phi\rangle\,|\psi\rangle$ or $|\phi\psi\rangle$.

Remark

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

The Kronecker product (cont'd)

Definition

The Kronecker product of two 2 × 2 matrices A and B can be computed as

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix},$$

which is a 4 × 4 matrix.

Exercise

Compute the Kronecker products $X \otimes X$ and $T \otimes T$, where $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$.

Remark

Stabilizers are Kronecker products of many Pauli operators, for example $XXXX$ or $ZZZZ$ which have a more compact binary representation we'll explore later.

> *God created the integers; all else is the work of man.*
>
> —Leopold Kronecker

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 $[X, Z] = -2iY$, where $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

> *... policies that can make commuting shorter ... would be a straightforward way to reduce minor but widespread suffering.*
>
> —Daniel Kahneman

Matrix trace

Definition

The trace of an $n \times n$ matrix A is the sum of its diagonal elements; that is

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

Remark

Trace is "commutativity-preserving," meaning $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ 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 $\mathrm{tr}(A) = \mathrm{tr}(B)$.

Matrix trace (cont'd)

Exercise

Show that $\mathrm{tr}(P) = 0$ for each non-identity Pauli operator P.

Exercise

Show that $\mathrm{tr}(XZ) = \mathrm{tr}(ZX)$.

> *It is by tracing things to their origin,*
> *that we learn to understand them …*
> —Thomas Paine

Projection operators

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 projection operator, denoted $\hat{P}$, when applied to a quantum state $|\psi\rangle \in \mathcal{H}$, where $\mathcal{H}$ is a Hilbert space, returns a vector in a subspace of $\mathcal{H}$ defined with respect to a specific state $|a\rangle$, and is defined as

$$\hat{P}_a = |a\rangle \langle a| ,$$

where $|a\rangle$ is in an orthonormal basis of $\mathcal{H}$.

Remark

Projection operators are used to model quantum measurement; in quantum computing, they project a qubit into a specific basis, such as the X or Z basis (where only one of two outcomes are possible).

Projection operators (cont'd)

Remark

Projection operators are idempotent, meaning that $\hat{P}^2 = \hat{P}$, and Hermitian, meaning that $\hat{P}^\dagger = \hat{P}$.

Example

For a single qubit in the general state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, a measurement in the Z basis $\{|0\rangle\,, |1\rangle\}$ is described by two projection operators:

- Projection operator for outcome $|0\rangle$: $\hat{P}_0 = |0\rangle\,\langle 0|$; note that $p(0) = |\alpha|^2$
- Projection operator for outcome $|1\rangle$: $\hat{P}_1 = |1\rangle\,\langle 1|$; note that $p(1) = |\beta|^2$

Remark

The probability of measuring $|\psi\rangle$ as $|a\rangle$ can be computed as

$$p(a) = |\,\langle a|\psi\rangle\,|^2 = \langle\psi|\,\hat{P}_a\,|\psi\rangle\,.$$

Projection operators (cont'd)

Exercise

Compute the matrices $\hat{P}_0$ and $\hat{P}_1$, then show that any projection operator is not unitary.

Definition

The CNOT gate has the following matrix representation:

$$\text{CNOT} = \begin{pmatrix} I & \mathcal{O} \\ \mathcal{O} & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Exercise

Show that the conditional action of the CNOT gate can be written as

$$\text{CNOT} = (|0\rangle\langle 0| \otimes I) + (|1\rangle\langle 1| \otimes X).$$

Clifford gate conjugation

Definition

A Clifford operator C "conjugates within" the Pauli operators $\{I, X, Y, Z\}$; that is:

$$P' = CPC^\dagger$$

where P and P' are Kronecker products of Pauli operators in equal dimension to C.

Remark

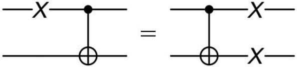
Any Clifford operator can be generated from Hadamard, CNOT, and/or S operators. The Pauli operators are themselves Clifford operators. The "Clifford + T" gates suffice to construct any quantum circuit.

> *In our implementation of a quantum [CNOT] logic gate, the target qubit $|S\rangle$ is spanned by two $^2S_{1/2}$ hyperfine ground states of a single $^9\mathrm{Be}^+$ ion ...*
>
> —C. Monroe *et al* [1995]

Clifford gate conjugation (cont'd)

Example

The movement of an X error through the control of a CNOT gate looks like:



Using stabilizer notation, we represent this as

$$(X_1 I_2) \xrightarrow{\text{CNOT}_{1,2}} (X_1 X_2).$$

To demonstrate, let's use gate conjugation. The Clifford gate is CNOT and the Pauli operators are X and I:

$$\text{CNOT}(X \otimes I)\text{CNOT}^\dagger = \begin{pmatrix} I & \mathcal{O} \\ \mathcal{O} & X \end{pmatrix} \begin{pmatrix} \mathcal{O} & I \\ I & \mathcal{O} \end{pmatrix} \begin{pmatrix} I & \mathcal{O} \\ \mathcal{O} & X \end{pmatrix} = X \otimes X$$

Clifford gate conjugation (cont'd)

Exercise

Use Clifford gate conjugation to demonstrate the following error propagation rules:

$$X \xrightarrow{H} Z \xrightarrow{H} X$$

$$X \xrightarrow{S} Y \xrightarrow{S} -X$$

$$I_1 Z_1 \xrightarrow{\mathrm{CNOT}_{1,2}} Z_1 Z_2$$

$$I_1 X_2 \xrightarrow{\mathrm{CNOT}_{1,2}} I_1 X_2$$

Still round the corner there may wait
A new road or a secret gate.
—J. R. R. Tolkien, *The Hobbit*

Stabilizers

Definition

Each of the four Pauli operators can be encoded symplectically, using two bits as such:

$$I \rightarrow (0|0),\ X \rightarrow (1|0),\ Y \rightarrow (1|1),\ Z \rightarrow (0|1).$$

Definition

A stabilizer comprises the Kronecker product of n Pauli operators represented in symplectic notation, written as a vector in block format as

$$\mathbf{v} = (x_1 \cdots x_n | z_1 \cdots z_n) \in \mathbb{F}_2^{2n}.$$

The left side of the vector is the X sector and the right side is the Z sector. $\mathbb{F}_2$ is the binary field $\{0, 1\}$ (also denoted $GF(2)$), making $\mathbb{F}_2^{2n}$ a vector space over $\mathbb{F}_2$ of dimension $2n$.

Stabilizers (cont'd)

Example

The 4-qubit stabilizer with Pauli string $XXXX$ can be represented as the bit vector $(1111|0000)$, and $XZXZ$ is $(1010|0101)$.

Definition

The symplectic inner product of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^{2n}$ is defined as

$$\mathbf{u} \odot \mathbf{v} = \sum_{k=1}^{n} \left[x_k^{(\mathbf{u})} z_k^{(\mathbf{v})} + z_k^{(\mathbf{v})} x_k^{(\mathbf{u})} \right] \mod 2,$$

where $x_k^{(\mathbf{u})}$ denotes the kth element of the X sector of $\mathbf{u}$, and so on.

Theorem

Two stabilizers represented symplectically by $\mathbf{u}$ and $\mathbf{v}$ commute if and only if $\mathbf{u} \odot \mathbf{v} = 0$.

A five-qubit code

Example

We can use $m = 4$ stabilizers to perform error detection using $n = 5$ physical qubits. Let's tabulate:

Stabilizer	Pauli string	X bits (H_X)	Z bits (H_Z)
S_1	$XZZXI$	10010	01100
S_2	$IXZZX$	01001	00110
S_3	$XIXZZ$	10100	00011
S_4	$ZXIXZ$	01010	10001

This encodes $k = n - m = 1$ logical qubit.

Definition

The parity check (or, Hamming) matrix H_c for an n-qubit code is a $m \times 2n$ matrix defined via concatenation as $H_c = [H_X | H_Z]$.

A five-qubit code (cont'd)

Definition

The symplectic Gram matrix is defined as $\Omega = \begin{pmatrix} \mathcal{O}_n & I_n \\ I_n & \mathcal{O}_n \end{pmatrix}$.

Definition

The symplectic error vector $\mathbf{e} = (e_x | e_z)$ represents the location of errors. In e_x, a 1 at index i means an X error occurred on physical qubit i, and likewise for e_z and Z errors.

Definition

The symplectic syndrome vector $\mathbf{s}$ is defined as $\mathbf{s} = H_c \Omega \mathbf{e}^T$. Note that $\mathbf{s}$ is m-dimensional, corresponding to detection events of the m stabilizers in the code. Given a syndrome vector $\mathbf{s}$, we must compute the error vector $\mathbf{e}$ to locate the X and Z errors on any of the n physical qubits.

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)

Remark

The spectral decomposition of any $n \times n$ Hermitian matrix A is

$$A = \sum_{k=1}^{n} \lambda_k \left|\psi\right\rangle_k \left\langle\psi\right|_k ,$$

where λ_k is an eigenvalue of A and $\left|\psi\right\rangle_k$ is its corresponding orthonormal eigenstate.

Example

The spectral theorem yields the following decomposition of the Pauli Z matrix in terms of projection operators:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (1)\hat{P}_1 + (-1)\hat{P}_{-1}$$

since the eigenvalues of Z are $+1$ and -1.

Spectral Theorem (cont'd)

Remark

The spectral theorem tells us that, since the Pauli matrices $\{X, Y, Z\}$ are Hermitian, their eigenvalues are ± 1 and their eigenvectors form a mutually orthogonal and complete basis of the qubit state space $\mathbb{C}^2$, justifying their use as the fundamental observables of a qubit. The Pauli matrices create a basis for all 2×2 Hermitian matrices.

Exercise

Show that every unitary matrix and Hermitian matrix is normal.

> *I consider nature a vast chemical laboratory in which all kinds of composition and decompositions are formed.*
>
> —Antoine Lavoisier

> *This isn't right. This isn't even wrong.*
>
> —Wolfgang Pauli

Linear functionals and dual spaces

Definition

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

Adding functionality is not just a matter of adding code.

—Wietse Venema

Riesz Representation Theorem

Definition

A linear map T is anti-linear if

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

Definition

Two vector spaces V and W are isomorphic if there exists a bijective linear map $T : V \to W$, 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 define it.

Theorem (Riesz)

For any Hilbert space $\mathcal{H}$ there exists a unique 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.

> *We are servants rather than masters in mathematics.*
>
> —Charles Hermite

Application: the uncertainty principle

Definition

The expectation value of a Hermitian operator (or, observable) A with respect to a particular normalized state vector $|\psi\rangle$ of equal dimension to A is a scalar computed as:

$$\langle A\rangle = \langle\psi| A |\psi\rangle$$

Remark

The expectation value corresponds to the probabilistic expected value of an experiment measuring an observable A on $|\psi\rangle$.

Remark

The expectation value is analogous to the expected value of a random variable X which has a probability density function $f(x)$ satisfying

$$p(a \leq X \leq b) = \int_a^b f(x)dx \text{ and } \mathbb{E}[X] = \int_{-\infty}^{\infty} xf(x)dx.$$

Application: the uncertainty principle (cont'd)

Definition

The variance of an operator A, denoted $\mathrm{Var}(A)$, is computed as $\mathrm{Var}(A) = \langle A^2 \rangle - \langle A \rangle^2$

Definition

The standard deviation of an operator A, denoted ΔA or σ_A, is simply $\Delta A = \sqrt{\mathrm{Var}(A)}$.

Theorem (Robertson)

For any two non-commuting Hermitian operators A and B, we have

$$\Delta A \Delta B \geq \frac{1}{2} \left| \langle [A, B] \rangle \right| .$$

Application: the uncertainty principle (cont'd)

Exercise

Verify the Robertson uncertainty relation for each distinct pair of Pauli matrices. (Hint: compute the expectation values in terms of basis vectors.)

Information is the resolution of uncertainty.
—Claude Shannon