

Appendix A

Linear Algebra

Linear algebra is an elementary language to mathematically describe quantum mechanics. This appendix summarizes the concepts, definitions, theorems, and properties of linear algebra that are frequently used in quantum information physics. In most cases, we omit rigorous proofs to focus on main concepts.

Many textbooks on linear algebra focus on arithmetic techniques related to the properties of matrices, such as the Gauss elimination and the formula of determinant. In most areas of physics, notably in quantum mechanics, more relevant are the fundamental concepts and algebraic structures of vector spaces and linear operators. Lang (1987)—an abridged edition Lang (1986) is also available—is one of the textbooks that introduce and discuss the latter subjects.

A.1 Vectors

A.1.1 Vector Space

One of the most distinguished features of quantum states compared to classical states is superposition inherited from the wave-particle duality. It is thus natural to describe quantum states mathematically by vectors. Vectors can be multiplied by numbers (called scalars) and added with each other, exactly the way the superposition principle dictates. We first need a field, a set of scalars with addition and multiplication.

Definition A.1 (*field*) A set $\mathbb{F}$ of elements is called a *field* if it satisfies the following conditions:

- (a) (addition) If $x, y \in \mathbb{F}$, then $x + y \in \mathbb{F}$.
- (b) (multiplication) If $x, y \in \mathbb{F}$, then $xy \in \mathbb{F}$.
- (c) (zero) $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$.
- (d) (inverse) If $x \in \mathbb{F}$, then $-x \in \mathbb{F}$.

(e) (inverse) If $x \in \mathbb{F}$ and $x \neq 0$, then $x^{-1} \in \mathbb{F}$.

The elements of the given field are called the *scalars*.

In the simplest terms, vectors represent physical quantities with both magnitude and direction. In quantum mechanics, more important feature of vectors is superposition. Here is the formal definition with mathematical rigor.

Definition A.2 (*vector space*) A set $\mathcal{V}$ of elements is called a *vector space* over a field $\mathbb{F}$, if it satisfies the following conditions:

- (a) If $v_1, v_2 \in \mathcal{V}$, then $v_1 + v_2 \in \mathcal{V}$.
- (b) If $v_1 \in \mathcal{V}$ and $x \in \mathbb{F}$, then $xv_1 \in \mathcal{V}$.
- (c) If $v_1, v_2, v_3 \in \mathcal{V}$, then $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$.
- (d) There is an element $0 \in \mathcal{V}$ (a *null vector*) such that for all $v_2 \in \mathcal{V}$ $0 + v_2 = v_2 + 0 = v_2$. Note that both “zero” in $\mathbb{F}$ or the null vector in $\mathcal{V}$ are denoted by ‘0’.
- (e) For a given $v_2 \in \mathcal{V}$, there exists $-v_2 \in \mathcal{V}$ such that $v_2 + (-v_2) = 0$. The subtraction between vectors are defined by $v_1 - v_2 := v_1 + (-v_2)$.
- (f) For $x, y \in \mathbb{F}$ and $v_1, v_2 \in \mathcal{V}$,

$$x(v_1 + v_2) = xv_1 + xv_2, \quad (\text{A.1a})$$

$$(x + y)v_2 = xv_2 + yv_2, \quad (\text{A.1b})$$

$$(xy)v_2 = x(yv_2). \quad (\text{A.1c})$$

The elements of a vector space are called *vectors*.

Common examples include vector spaces over the fields of rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$), complex numbers ($\mathbb{C}$), and quaternions ($\mathbb{H}$). Note that the set of integer numbers ($\mathbb{Z}$) with the standard arithmetic rules is not a field. As is the case mostly in quantum mechanics, *vector spaces will be assumed to be over the field of complex numbers $\mathbb{C}$ throughout this book unless mentioned otherwise.*

Definition A.3 (*linear independence*) Let $\mathcal{V}$ be a vector space. Vectors $v_1, \dots, v_n$ in $\mathcal{V}$ are said to be *linearly dependent* of each other if there exists a solution $z_1, \dots, z_n \in \mathbb{C}$ to the equation

$$z_1v_1 + \dots + z_nv_n = 0. \quad (\text{A.2})$$

If not, they are said to be *linearly independent*.

A.1.2 Hermitian Product

In a vector space, the multiplication of vectors has not been defined. The *inner product* gives a special kind of multiplication between vectors and provides the vector space with a geometric structure, i.e., the *orthogonality* of vectors.

The inner product is usually a bilinear mapping. In many fields of physics (e.g., quantum mechanics), however, we will be dealing with vector spaces over $\mathbb{C}$ (the field of complex numbers). To preserve the notion of positive definiteness, we need to adopt a slightly different definition of the inner product. This modified inner product is called a Hermitian product to distinguish it from a usual inner product.

Definition A.4 (*Hermitian product*) Let $\mathcal{V}$ be a vector space. A *Hermitian product* on $\mathcal{V}$ is a function $\langle \cdot, \cdot \rangle$ from $\mathcal{V} \times \mathcal{V}$ to $\mathbb{C}$ satisfying the following conditions:

- (a) For all $u, v, w \in \mathcal{V}$, $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$.
- (b) For all $z \in \mathbb{C}$ and $v, w \in \mathcal{V}$, $\langle zv, w \rangle = z^* \langle v, w \rangle$ and $\langle v, zw \rangle = z \langle v, w \rangle$.
- (c) For all $v, w \in \mathcal{V}$, $\langle v, w \rangle = \langle w, v \rangle^*$.
- (d) $\langle v, v \rangle \geq 0$ for all $v \in \mathcal{V}$, and $\langle v, v \rangle > 0$ if $v \neq 0$.¹

Two vectors v and w are said to be *orthogonal* if $\langle v, w \rangle = 0$. On the other hand, they are said to be *parallel* if they are linearly dependent.

One of the most fundamental properties of Hermitian product is the following inequality.

Theorem A.5 (Cauchy-Schwarz inequality) *Let $\langle \cdot, \cdot \rangle$ be a Hermitian product on a vector space $\mathcal{V}$. The so-called Cauchy-Schwarz inequality*

$$|\langle v, w \rangle|^2 \leq \langle v, v \rangle \langle w, w \rangle \quad (\text{A.3})$$

holds for any vectors v and w in $\mathcal{V}$. Equality holds if and only if v and w are linearly dependent (i.e., parallel).

To prove the Cauchy-Schwarz inequality, consider the vector defined by

$$u := v - w \frac{\langle w, v \rangle}{\langle w, w \rangle}. \quad (\text{A.4})$$

Geometrically, it corresponds to the difference between v and the component of v projected onto $|w\rangle$. Whence u is orthogonal to w , $\langle u, w \rangle = 0$. We have

$$\langle u, u \rangle = \langle v, v \rangle - \frac{\langle v, w \rangle \langle w, v \rangle}{\langle w, w \rangle}. \quad (\text{A.5})$$

Since $\langle u, u \rangle \geq 0$, the above equation leads to the inequality. Furthermore, we recall that $\langle u, u \rangle = 0$ if and only if $u = 0$. It immediately implies that the equality in (A.5) holds if and only if

$$v = w \frac{\langle w, v \rangle}{\langle w, w \rangle}. \quad (\text{A.6})$$

Therefore, v and w must be linearly dependent.

¹ A Hermitian product satisfying this condition is said to be *positive definite*. We include this condition here because it is required for most applications in quantum mechanics.

The geometric structure due to the Hermitian product allows defining the *magnitude* or *norm* of the vectors. For a vector v , we let $\|v\|$ denote the norm of v and define it by

$$\|v\| := \sqrt{\langle v, v \rangle}. \quad (\text{A.7})$$

This norm is called the *canonical norm* associated with the Hermitian product $\langle \cdot, \cdot \rangle$. It satisfies, as it should as a norm, the *triangle inequality*

$$\|v + w\| \leq \|v\| + \|w\| \quad (\text{A.8})$$

for all vectors v and w . In quantum mechanics, a norm is essential for the probabilistic interpretation (Sect. 1.3).

A norm, in turn, provides a *distance* measure. A natural way to measure the distance $D(v, w)$ between two vectors v and w is to use the norm,

$$D(v, w) := \|v - w\| \equiv \sqrt{\langle v - w, v - w \rangle}. \quad (\text{A.9})$$

The above distance measure is called the *canonical distance* associated with the Hermitian product $\langle \cdot, \cdot \rangle$. The triangle inequality (A.8) for the norm directly implies the analogous inequality for the distance,

$$\|u - w\| \leq \|u - v\| + \|v - w\| \quad (\text{A.10})$$

for all vectors u , v , and w . A distance measure is useful in quantifying the closeness of two quantum states (Sects. 5.5.1 and 5.5.2).

A Hermitian product provides another way of measuring how close two state vectors are through the notion of *fidelity* (Sect. 5.5.3). The fidelity between two vectors v and w is defined to be $|\langle v, w \rangle|$.

A.1.3 Basis

Definition A.6 (*basis*) Let $\mathcal{V}$ be a vector space. If every element of $\mathcal{V}$ is a linear combination of $v_1, \dots, v_n$, then $v_1, \dots, v_n$ are said to *span* (or *generate*) the vector space $\mathcal{V}$. The set $\{v_1, \dots, v_n\} \subset \mathcal{V}$ is called a *basis* of $\mathcal{V}$ if $v_1, \dots, v_n$ span $\mathcal{V}$ and are linearly independent. The number of elements in a basis of $\mathcal{V}$ is called the *dimension* of $\mathcal{V}$ and denoted by $\dim \mathcal{V}$.

Quantum states are described by a state vector in a *Hilbert space*. A Hilbert space is a vector space, usually infinite dimensional, with additional analytic properties provided by the notion of completeness. However, as long as the dimension is finite, there is no distinction between the Hilbert space and the vector space. Unless mentioned otherwise explicitly, we assume that vector spaces are finite dimensional.

When a basis (recall Definition A.6) $\{v_1, v_2, \dots, v_n\}$ spanning $\mathcal{V}$ satisfies

$$\langle v_i, v_j \rangle = \delta_{ij}, \quad (\text{A.11})$$

it is called an *orthonormal basis*. For a finite dimensional vector space $\mathcal{V}$, one can always find an orthogonal basis as long as $\mathcal{V} \neq \{0\}$.

A choice of basis is arbitrary and one can change the basis to another: Suppose that $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ and $\mathcal{B} = \{w_1, w_2, \dots, w_n\}$ are two bases of the same vector space $\mathcal{V}$. As both $\mathcal{A}$ and $\mathcal{B}$ are bases, one can expand each vector w_j in $\mathcal{B}$ in the vectors v_i in $\mathcal{A}$ (and vice versa):

$$w_j = \sum_i v_i U_{ij}, \quad (\text{A.12})$$

where U_{ij} are complex coefficients. The matrix $U := [U_{ij}]$ composed of these coefficients characterizes the relation between the two bases, and it must be invertible since the elements in each basis are linearly independent of each other. The relation is particularly simple when the bases are *orthonormal*: As $\mathcal{A}$ is orthonormal, the coefficients U_{ij} can be obtained by

$$U_{ij} = \langle v_i, w_j \rangle. \quad (\text{A.13})$$

More importantly, one can show that U is a *unitary* matrix (see also Theorem A.15).

A.1.4 Representations

Given a fixed basis $\{v_1, v_2, \dots, v_n\}$ of a vector space $\mathcal{V}$, any vector $\alpha \in \mathcal{V}$ is *uniquely* specified by the coefficients $\alpha_j \in \mathbb{C}$ in the expansion

$$\alpha = v_1 \alpha_1 + v_2 \alpha_2 + \dots + v_n \alpha_n. \quad (\text{A.14})$$

The column vector consisting of $\alpha_1, \dots, \alpha_n$ is said to be the *representation* of the vector α in the basis, and denoted by

$$\alpha \doteq \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}. \quad (\text{A.15})$$

When the basis $\{v_1, v_2, \dots, v_n\}$ is *orthonormal*, the expansion coefficients α_j are obtained directly by means of the Hermitian product, $\alpha_j = \langle v_j, \alpha \rangle$. Hence, the vector is represented by the expansion

$$\alpha = \sum_j v_j \langle v_j, \alpha \rangle \quad (\text{A.16})$$

or, equivalently, by the column vector

$$\alpha \doteq \begin{bmatrix} \langle v_1, \alpha \rangle \\ \langle v_2, \alpha \rangle \\ \vdots \\ \langle v_n, \alpha \rangle \end{bmatrix}. \quad (\text{A.17})$$

Consider another vector $\beta \in \mathcal{V}$ and suppose that $\beta_j := \langle v_j, \beta \rangle$ is its representation in the same orthonormal basis. Then, the Hermitian product $\langle \alpha, \beta \rangle$ can be evaluated using their column-vector representations

$$\langle \alpha, \beta \rangle = \sum_j \alpha_j^* \beta_j = [\alpha_1^* \alpha_2^* \cdots \alpha_n^*] \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}, \quad (\text{A.18})$$

where we have used the identity $\langle \alpha, v_j \rangle = \langle v_j, \alpha \rangle^* = \alpha_j^*$.

Upon the change of basis, the representations of vectors also change. Suppose that a vector $\alpha \in \mathcal{V}$ is represented by

$$\alpha \doteq \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \quad (\text{A.19})$$

in the basis $\{v_i\}$, and by

$$\alpha \doteq \begin{bmatrix} \alpha'_1 \\ \alpha'_2 \\ \vdots \\ \alpha'_n \end{bmatrix} \quad (\text{A.20})$$

in the basis $\{w_j\}$. The relation between the two representations is fixed by the relation between the two bases. Let us take a closer look at the relation when the two bases are orthonormal. We note from (A.16) that

$$\alpha'_k = \langle w_k, \alpha \rangle = \sum_{j=1}^n \langle w_k, v_j \rangle \langle v_j, \alpha \rangle = \sum_k U_{kj} \alpha_j, \quad (\text{A.21})$$

where we have put $U_{kj} := \langle w_k, v_j \rangle$. We have seen in Eq. (A.13) that the matrix U is unitary. Therefore, we see that the representations in two different orthonormal bases are related by a unitary matrix as

$$\begin{bmatrix} \alpha'_1 \\ \alpha'_2 \\ \vdots \\ \alpha'_n \end{bmatrix} = \begin{bmatrix} U_{11} & U_{12} & \cdots & U_{1n} \\ U_{21} & U_{22} & \cdots & U_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ U_{n1} & U_{n2} & \cdots & U_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}. \quad (\text{A.22})$$

A.2 Linear Operators

In quantum mechanics, the evolution of quantum states and the properties of physical quantities are described by linear operators. Linear operators are special kind of linear mappings.

A.2.1 Linear Maps

As already mentioned, the most important algebraic property of a vector space is the superposition. Therefore, the mapping preserving this property from one vector space to another plays an important role in the theory of linear algebra.

Definition A.7 (*linear map*) Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces. A mapping (or simply map)

$$\hat{L} : \mathcal{V} \rightarrow \mathcal{W}, \quad v \mapsto \hat{L}v \quad (\text{A.23})$$

is said to be *linear* if it satisfies the following two properties:

- (a) For any $v, w \in \mathcal{V}$, we have $\hat{L}(v + w) = \hat{L}v + \hat{L}w$.
- (b) For all $z \in \mathbb{C}$ and $v \in \mathcal{V}$ we have $\hat{L}(zv) = z(\hat{L}v)$.

When $\mathcal{V} = \mathcal{W}$, the map is called a *linear operator* on $\mathcal{V}$.

Since a linear map preserves superposition, it is completely determined by specifying how it maps just the basis vectors. The following theorem summarizes the property.

Theorem A.8 *Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces. Let $\{v_1, \dots, v_n\}$ be a basis of $\mathcal{V}$, and $w_1, \dots, w_n \in \mathcal{W}$ be arbitrary vectors—not to be necessarily distinctive nor to form a basis. Then there exists a unique linear map $\hat{L} : \mathcal{V} \rightarrow \mathcal{W}$ such that $w_j = \hat{L}v_j$ for all $j = 1, \dots, n$.*

Proof of the theorem highlights the implications of linearity. Let us take a look at a proof. Define a map $\hat{A} : \mathcal{V} \rightarrow \mathcal{W}$ by the associations

$$\hat{A}v_j \mapsto w_j \quad (\text{A.24})$$

and

$$\hat{A}(v_1z_1 + \cdots v_nz_n) = w_1z_1 + \cdots w_nz_n \quad (\text{A.25})$$

for all $z_1, \dots, z_n \in \mathbb{C}$. $\hat{A}$ is linear by construction, and we have shown that there exists a linear map satisfying the required condition. Now suppose that two linear maps $\hat{A}$ and $\hat{B}$ satisfy the condition. Let $v = v_1z_1 + \cdots v_nz_n \in \mathcal{V}$ with $z_j \in \mathbb{C}$. Note that

$$\hat{B}v = (\hat{B}v_1)z_1 + \cdots + (\hat{B}v_n)z_n = w_1z_1 + \cdots + w_nz_n = \hat{A}v. \quad (\text{A.26})$$

Since v is arbitrary, we conclude that $\hat{A} = \hat{B}$.

A.2.2 Representations

As asserted by Theorem A.8, a linear map $\hat{L} : \mathcal{V} \rightarrow \mathcal{W}$ is completely determined by specifying how it maps each element of a basis $\{v_j : j = 1, \dots, n\}$ of $\mathcal{V}$. Expanding the result $\hat{L}v_j$ in a basis $\{w_i : i = 1, \dots, m\}$ of $\mathcal{W}$ as

$$\hat{L}v_j = \sum_i w_i L_{ij}, \quad (\text{A.27})$$

we can equivalently say that $\hat{L}$ is *uniquely* specified by the coefficients $L_{ij} \in \mathbb{C}$. The $m \times n$ matrix composed of the coefficients is called the matrix representation of $\hat{L}$ in the bases $\{v_j\}$ and $\{w_i\}$. $\hat{L}$ being represented by the matrix L is denoted by

$$\hat{L} \doteq \begin{bmatrix} L_{11} & L_{12} & \cdots \\ L_{21} & L_{22} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}. \quad (\text{A.28})$$

When the bases $\{v_j\}$ and $\{w_i\}$ are *orthonormal*, the matrix elements L_{ij} can be obtained by means of the Hermitian product, $L_{ij} = \langle w_i, \hat{L}v_j \rangle$, and hence

$$\hat{L}v_j = \sum_i w_i \langle w_i, \hat{L}v_j \rangle. \quad (\text{A.29})$$

In quantum mechanics, one has to frequently calculate the matrix representations of linear maps in orthonormal bases, and the procedure is summarized in the following table:

$$\hat{L} \doteq \begin{array}{c|ccc} & v_1 & v_2 & \cdots \\ \hline w_1 & \langle w_1, \hat{L}v_1 \rangle & \langle w_1, \hat{L}v_2 \rangle & \cdots \\ w_2 & \langle w_2, \hat{L}v_1 \rangle & \langle w_2, \hat{L}v_2 \rangle & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array} \quad (\text{A.30})$$

When $\mathcal{V} = \mathcal{W}$, a linear operator is represented by a square matrix.

It is important to note that the matrix representation of a linear map depends on the choice of bases of $\mathcal{V}$ and $\mathcal{W}$. How does the matrix representation change when we choose different bases? Here let us focus on linear operators ($\mathcal{V} = \mathcal{W}$). Suppose that $\{v_i\}$ and $\{w_j\}$ are two different orthonormal bases of $\mathcal{V}$. Since they are both orthonormal, there must be a unitary operator (Definition A.13) $\hat{U}$ such that

$$w_j = \hat{U}v_j = \sum_i v_i U_{ij}, \quad (\text{A.31})$$

where $U_{ij} := \langle v_i, w_j \rangle$ is a unitary matrix (see Eq. (A.12)). Suppose that L_{ij} be the matrix representation of a linear operator $\hat{L}$ in the basis $\{v_i\}$. What is the matrix representation L'_{ij} of $\hat{L}$ in the new basis $\{w_j\}$? Using the relation (A.31), we obtain the new matrix representation

$$L'_{ij} = \langle w_i, \hat{L}w_j \rangle = \sum_{kl} U_{ik}^* \langle v_i, \hat{L}v_l \rangle U_{lj} = \sum_{kl} U_{ik}^* L_{il} U_{lj}. \quad (\text{A.32})$$

In other words, the matrix representations in two different bases are related with each other by

$$L' = U^\dagger L U. \quad (\text{A.33})$$

A.2.3 Hermitian Conjugate of Operators

On a vector space equipped with a Hermitian product, given a linear operator $\hat{L}$ one can define another linear operator $\hat{L}^\dagger$ naturally related to $\hat{L}$. Hermitian conjugates of operators greatly simplify the evaluations of operator-related expressions and the spectral analysis of them.

Theorem A.9 (Hermitian conjugate) *Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces over $\mathbb{C}$ equipped with Hermitian products. Let $\hat{L} : \mathcal{V} \rightarrow \mathcal{W}$ be a linear map. Then, the following statements hold true:*

(a) *There exists a unique linear map $\hat{L}^\dagger : \mathcal{W} \rightarrow \mathcal{V}$ such that*

$$\langle w, \hat{L}v \rangle_{\mathcal{W}} = \langle \hat{L}^\dagger w, v \rangle_{\mathcal{V}} \quad (\text{A.34})$$

for all $v \in \mathcal{V}$ and $w \in \mathcal{W}$.

(b) $(\hat{L}^\dagger)^\dagger$ exists as well, and is identical to $\hat{L}$, $(\hat{L}^\dagger)^\dagger = \hat{L}$.

The linear operator $\hat{L}^\dagger$ is called the Hermitian conjugate of $\hat{L}$.

The matrix representation of a linear map is unique, and one can also define the Hermitian conjugate in terms of the matrix representation. Let $\hat{L} : \mathcal{V} \rightarrow \mathcal{W}$ be represented by

$$\hat{L}v_j = \sum_i w_i L_{ij}. \quad (\text{A.35})$$

Then, $\hat{L}^\dagger : \mathcal{W} \rightarrow \mathcal{V}$ is defined by

$$\hat{L}^\dagger w_j = \sum_i v_i L_{ji}^*. \quad (\text{A.36})$$

That is, the matrix representation of $\hat{L}^\dagger$ is the conjugate-transposition of the matrix representation of $\hat{L}$. For finite-dimensional vector spaces, the two definitions are equivalent.

For an operator on a vector space, its Hermitian conjugate also acts on the same vector space and enables to characterize the operator itself.

Definition A.10 (*normal operator*) A linear operator $\hat{L}$ on a vector space $\mathcal{V}$ is said to be *normal* if $[\hat{L}^\dagger, \hat{L}] = 0$.

The two most important examples of normal operators are Hermitian operators and unitary operators.

In quantum mechanics, the linear operator representing a physical quantity should be Hermitian:

Definition A.11 (*Hermitian operator*) A linear operator $\hat{H}$ on a vector space is called *Hermitian* if

$$\langle \hat{H}v, w \rangle = \langle v, \hat{H}w \rangle, \quad \forall v, w \in \mathcal{V}. \quad (\text{A.37})$$

There is a simple test for a Hermitian operator on a finite dimensional vector space:

Theorem A.12 Let $\mathcal{V}$ be a vector space. An operator $\hat{H}$ on $\mathcal{V}$ is Hermitian if and only if $\langle v, \hat{H}v \rangle \in \mathbb{R}$ for all $v \in \mathcal{V}$.

Another type of operators one encounters very frequently in quantum mechanics are unitary operators, *norm-preserving and invertible* linear maps.

Definition A.13 (*unitary operator*) Let $\mathcal{V}$ be a vector space $\mathcal{V}$ equipped with a Hermitian product. A linear operator $\hat{U}$ is said to be *unitary* when it maps $\mathcal{V}$ onto the whole of $\mathcal{V}$ and preserve the norm. That is, $\hat{U}\mathcal{V} = \mathcal{V}$ and $\langle \hat{U}v, \hat{U}v \rangle = \langle v, v \rangle$ for all $v \in \mathcal{V}$.

A unitary operator is characterized by the fact that its Hermitian conjugate is identical to its inverse.

Theorem A.14 *If $\hat{U}$ is a unitary operator on $\mathcal{V}$, then*

$$\hat{U}^\dagger \hat{U} = \hat{U} \hat{U}^\dagger = 1. \quad (\text{A.38})$$

In fact, Eq. (A.38) can be used as an alternative definition of a unitary operator.

The unique linear map in Theorem A.8 becomes a unitary operator when the image vectors form another orthonormal basis of the same vector space.

Theorem A.15 *Let $\mathcal{V}$ be a vector space. Let $\{v_1, \dots, v_n\}$ and $\{w_1, \dots, w_n\}$ be orthonormal bases of $\mathcal{V}$. Then there exists a unique unitary operator $\hat{U}$ on $\mathcal{V}$ such that $w_j = \hat{U}v_j$ for all $j = 1, \dots, n$.*

We have already seen in Eq. (A.12) that two orthonormal bases are related by a unitary matrix. Theorem A.15 just asserts it again. Indeed, if U is the matrix representation of $\hat{U}$ in the basis $\{v_i\}$, then

$$w_j = \hat{U}v_j = \sum_i v_i U_{ij}. \quad (\text{A.39})$$

Theorem A.15 is even more general and hold for any orthonormal subsets:

Theorem A.16 *Let $\mathcal{V}$ is a Hilbert space equipped with a Hermitian product $\langle \cdot, \cdot \rangle$, and $\mathcal{U} \subset \mathcal{V}$ a subspace. Suppose $\hat{U} : \mathcal{U} \rightarrow \mathcal{V}$ is a linear operator which preserves the Hermitian product. That is, for any $u, u' \in \mathcal{U}$,*

$$\langle \hat{U}u, \hat{U}u' \rangle = \langle u, u' \rangle. \quad (\text{A.40})$$

There exists a unitary operator $\hat{V} : \mathcal{V} \rightarrow \mathcal{V}$ which extends $\hat{U}$. That is, $\hat{V}u = \hat{U}u$ for all $u \in \mathcal{U}$ and $\hat{V}$ is defined on the entire space $\mathcal{V}$.

An immediate consequence of Theorem A.16 is that for any pair of vectors v and w one can always find a unitary operator $\hat{U}$ such that $w = \hat{U}v$.

A.3 Dirac's Bra-Ket Notation

For a given vector space $\mathcal{V}$, one can construct another special vector space $\mathcal{V}^*$ associated with $\mathcal{V}$, consisting of all linear mappings from $\mathcal{V}$ to $\mathbb{C}$, $\mathcal{V}^* := \{\phi : \mathcal{V} \rightarrow \mathbb{C}\}$. It is called the *dual space* of $\mathcal{V}$. With a fixed vector $v \in \mathcal{V}$ and the Hermitian product, one can define a linear mapping $\phi_v : \mathcal{V} \rightarrow \mathbb{C}$ by the relation $\phi_v(w) := \langle v, w \rangle$. Certainly, ϕ_v is an element of $\mathcal{V}^*$. This way, by choosing different vectors from $\mathcal{V}$, one can define a particular kind of linear mappings belonging to $\mathcal{V}^*$. Now the key observation is that in fact, any linear mapping in $\mathcal{V}^*$ is of this kind. That is, there is a one-to-one correspondence $v \leftrightarrow \phi_v$ between $\mathcal{V}$ and $\mathcal{V}^*$. ϕ_v is called the *dual vector* of v .

In Dirac's bra-ket notation, the dual ϕ_v is denoted by $\langle v|$ whereas the native vector v is denoted by $|v\rangle$; hence the name. It is just a simple notational change. However, it simplifies most evaluations in quantum mechanics so greatly that it is widely used. *Throughout the book, we will almost always be using the bra-ket notation.*

When $\{|\alpha_1\rangle, \dots, |\alpha_n\rangle\}$ is an orthonormal basis of $\mathcal{V}$, $\{\langle\alpha_1|, \dots, \langle\alpha_n|\}$ is also an orthonormal basis of $\mathcal{V}^*$ and is called the *dual basis* of the former. More importantly, the two bases satisfy the relation

$$\langle\alpha_i|\alpha_j\rangle = \delta_{ij}. \quad (\text{A.41})$$

Suppose that a vector $|v\rangle \in \mathcal{V}$ is expanded as

$$|v\rangle = \sum_j |\alpha_j\rangle v_j, \quad v_j \in \mathbb{C}. \quad (\text{A.42})$$

Then, its dual vector $\langle v|$ is given by

$$\langle v| = \sum_j v_j^* \langle\alpha_j|. \quad (\text{A.43})$$

Armed with the basic properties of the bra-ket notation, now consider a combination of the form $|v\rangle\langle v'|$, where $|v\rangle, |v'\rangle \in \mathcal{V}$: We regard it as an operator on $\mathcal{V}$ defined by the association

$$|v\rangle\langle v'| : |u\rangle \mapsto |v\rangle\langle v'|u\rangle \quad (\text{A.44})$$

for all $|u\rangle \in \mathcal{V}$. A simple inspection (see Definition A.9) shows that its Hermitian conjugate $(|v\rangle\langle v'|)^\dagger$ is just given by

$$(|v\rangle\langle v'|)^\dagger = |v'\rangle\langle v|. \quad (\text{A.45})$$

If one constructs $|\alpha_i\rangle\langle\alpha_j|$ out of a basis $\{|\alpha_j\rangle\}$ of $\mathcal{V}$, then any linear map on $\mathcal{V}$ can be expressed in terms of them, and they form a basis of the vector space $\mathcal{L}(\mathcal{V})$ of linear operators (Appendix B.1). In particular, if the basis $\{|\alpha_j\rangle\}$ is *orthonormal*, then a linear operator $\hat{L}$ on $\mathcal{V}$ with the matrix representation L in the same basis is equivalent to

$$\hat{L} = \sum_{ij} |\alpha_i\rangle L_{ij} \langle\alpha_j|, \quad (\text{A.46})$$

and, accordingly, its Hermitian conjugate $\hat{L}^\dagger$ to

$$\hat{L}^\dagger = \sum_{ij} |\alpha_i\rangle L_{ji}^* \langle\alpha_j|. \quad (\text{A.47})$$

Both expansions can be verified by evaluating the matrix elements in the basis and applying the orthogonality relation (A.41). An interesting result is that for *any* orthonormal basis $\{|\alpha_j\rangle\}$ of $\mathcal{V}$, the linear combination

$$\hat{I} = \sum_j |\alpha_j\rangle\langle\alpha_j| \quad (\text{A.48})$$

is equal to the identity operator on $\mathcal{V}$. It is called the *completeness relation*. The orthogonality relation (A.41) and the completeness relation (A.48), which are mutually complementary, together empower the bra-ket notation.

Consider a system of two qubits. The associated Hilbert space is spanned by the standard basis.

```
In[ ]:= bs = Basis[2]
```

```
Out[ ]:= { |0, 0⟩, |0, 1⟩, |1, 0⟩, |1, 1⟩ }
```

Consider a Hermitian operator, physically, corresponding to the Heisenberg exchange interaction between two $S=1/2$ spins.

```
In[ ]:= op = Pauli[1, 1] + Pauli[2, 2] + Pauli[3, 3]
```

```
Out[ ]:= σx ⊗ σx + σy ⊗ σy + σz ⊗ σz
```

This shows the matrix representation of the operator.

```
In[ ]:= mat = Matrix[op];
mat // MatrixForm
```

```
Out[ ]//MatrixForm=

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

```

This is an expansion of the operator in the bra-ket notation.

```
In[ ]:= op2 = MultiplyDot[bs, mat, Dagger[bs]]
```

```
Out[ ]:= |0, 0⟩⟨0, 0| - |0, 1⟩⟨0, 1| + 2|0, 1⟩⟨1, 0| +
2|1, 0⟩⟨0, 1| - |1, 0⟩⟨1, 0| + |1, 1⟩⟨1, 1|
```

Verify the above expansion by evaluating the matrix representation.

```
In[ ]:= mat2 = Outer[Multiply, Dagger[bs], op2 ** bs];
mat2 // MatrixForm
```

```
Out[ ]//MatrixForm=

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

```

More generally, given two vector spaces $\mathcal{V}$ and $\mathcal{W}$, the combination $|w\rangle\langle v|$ with for $|v\rangle \in \mathcal{V}$ and $|w\rangle \in \mathcal{W}$ is a linear map $\mathcal{V} \rightarrow \mathcal{W}$ with an association similar to that in Eq. (A.44). Its Hermitian conjugate, $(|w\rangle\langle v|)^\dagger : \mathcal{W} \rightarrow \mathcal{V}$, is given by $(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$.

To illustrate the power of the bra-ket notation, let us consider a linear map $\hat{L} : \mathcal{V} \rightarrow \mathcal{W}$ and examine $\hat{L}|\alpha_j\rangle$: Let $\{|\alpha_j\rangle : j = 1, \dots, m\}$ and $\{|\beta_k\rangle : k = 1, \dots, n\}$ be orthonormal bases of $\mathcal{V}$ and $\mathcal{W}$, respectively. As $\hat{L}|\alpha_j\rangle$ is an element of $\mathcal{W}$, it

should not be affected by the identity operator $\hat{I}_{\mathcal{W}}$ on $\mathcal{W}$, $\hat{L}|\alpha_j\rangle = \hat{I}_{\mathcal{W}}\hat{L}|\alpha_j\rangle$. Using the completeness relation (A.48) (replacing $|\alpha_j\rangle$ with $|\beta_k\rangle$), one can get

$$\hat{L}|\alpha_j\rangle = \hat{I}_{\mathcal{W}}\hat{L}|\alpha_j\rangle = \sum_k |\beta_k\rangle \langle\beta_k| \hat{L}|\alpha_j\rangle. \quad (\text{A.49})$$

Noting that $L_{kj} = \langle\beta_k| \hat{L}|\alpha_j\rangle$ is the matrix elements of the representation of $\hat{L}$ in the given bases [see Eq. (A.29)], one recovers the defining relation [see Eq. (A.27)]

$$\hat{L}|\alpha_j\rangle = \sum_k |\beta_k\rangle L_{kj} \quad (\text{A.50})$$

for the matrix representation of $\hat{L}$. Given the matrix representation L_{kj} , one can further expand $\hat{L}$ in terms of the bra-ket notation as

$$\hat{L} = \sum_{kj} |\beta_k\rangle L_{kj} \langle\alpha_j|. \quad (\text{A.51})$$

Once expanded in the bra-ket notation, its Hermitian conjugate $\hat{L}^\dagger : \mathcal{W} \rightarrow \mathcal{V}$ reads as

$$\hat{L}^\dagger = \sum_{kj} |\alpha_j\rangle L_{kj}^* \langle\beta_k|. \quad (\text{A.52})$$

A.4 Spectral Theorems

The eigenvalues and eigenvectors of normal operators (Definition A.10) exhibit particularly useful properties. They are frequently used in quantum mechanics and simplify many calculations and analyses. Here we summarize the properties of the eigenvalues and eigenvectors of normal operators, especially, Hermitian and unitary operators. Although we will mainly focus on the spectral properties, we will also discuss some other related properties.

A.4.1 Spectral Decomposition

The following theorems summarize the properties of the eigenvectors and eigenvalues of normal operators, especially, Hermitian, positive, and unitary operators:

Theorem A.17 *Let $\hat{A}$ be a normal operator (Definition A.10) on a vector space $\mathcal{V}$.*

- (a) *Eigenstates of $\hat{A}$ belonging to distinct eigenvalues are orthogonal to each other.*
- (b) *The set of all eigenvectors of $\hat{A}$ spans $\mathcal{V}$.*

Theorem A.17 enables to expand a normal operator in terms of its eigenvectors and eigenvalues using Dirac's bra-ket notation. Suppose that a normal operator $\hat{A}$ on a vector space $\mathcal{V}$ has eigenvectors $|a\rangle$ and the corresponding eigenvalues a . If some eigenvalues are degenerate, that is, there are more than one linearly independent eigenvectors belonging to the same eigenvalue, we choose mutually orthogonal eigenvectors, which is always possible. Then, the normalized eigenvectors form an orthonormal basis, which is called the *eigenbasis* from $\hat{A}$ of the vector space $\mathcal{V}$. Then the matrix representation of $\hat{A}$ in the eigenbasis from itself must be diagonal with the diagonal elements given by the eigenvalues. Hence, in Dirac's bra-ket notation, $\hat{A}$ can be expanded as

$$\hat{A} = \sum_a |a\rangle a \langle a|, \quad (\text{A.53})$$

where the sum is over all eigenvalues of $\hat{A}$. The expansion is called the *spectral decomposition* of $\hat{A}$.

Theorem A.18 (a) A Hermitian operator $\hat{H}$ is normal.
 (b) Every eigenvalue of a Hermitian operator is real.

In quantum mechanics, the operators usually describe the changes of state of a system in terms of the transformation of vectors. However, there is also a class of operators, called density operators, that describe the mixed state of the system (Sect. 1.1.2). For a proper statistical interpretation of mixed states, the density operators are required to satisfy certain properties. They are Hermitian and positive among other properties. It motivates the following definition.

Definition A.19 (*positive operator*) Let $\hat{H}$ be a Hermitian operator on a vector space $\mathcal{V}$.

- (a) $\hat{H}$ is said to be *positive* (or more specifically, *positive definite*) if $\langle v|\hat{H}|v\rangle > 0$ for all non-vanishing vectors $|v\rangle \in \mathcal{V}$. A positive operator is denoted as $\hat{H} > 0$.
- (b) $\hat{H}$ is said to be *positive semidefinite* or *non-negative* if $\langle v|\hat{H}|v\rangle \geq 0$ for all non-vanishing vectors $|v\rangle \in \mathcal{V}$. It is denoted as $\hat{H} \geq 0$.

Very often in physics, positive definite and positive semidefinite operators are not distinguished, and both types are simply called positive operators.

Theorem A.20 Let $\hat{H}$ be a Hermitian operator on a vector space. Then,

- (a) $\hat{H}$ is positive if and only if every eigenvalue of it is positive;
- (b) $\hat{H}$ is positive-semidefinite if and only if the eigenvalues are non-negative.

A common example of positive operator is an operator of the form

$$\hat{A} = |\psi\rangle \langle \psi| \quad (\text{A.54})$$

for some vector $|\psi\rangle$. It has a single non-zero eigenvalue 1, and the corresponding eigenvector is $|\psi\rangle$. Any vector $|\varphi\rangle$ orthogonal to $|\psi\rangle$ is an eigenvector of $\hat{A}$ belonging to the (degenerate) eigenvalue 0, $\hat{A}|\varphi\rangle = 0$. Whence, $\hat{A} \geq 0$. More generally, consider an operator of the form

$$\hat{A} := \sum_j |\psi_j\rangle\langle\psi_j| \quad (\text{A.55})$$

for an arbitrary set $\{|\psi_j\rangle\}$ of vectors (not necessarily orthogonal nor normalized). One can show that $\hat{A} \geq 0$.

For any linear operator $\hat{A}$, the compositions $\hat{A}^\dagger \hat{A}$ and $\hat{A} \hat{A}^\dagger$ give positive operators as well. To see it, note that

$$\langle v | \hat{A}^\dagger \hat{A} | v \rangle = \|\hat{A} | v \rangle\|^2 \geq 0 \quad (\text{A.56})$$

for any $|v\rangle$. Therefore, $\hat{A}^\dagger \hat{A} \geq 0$. One can use a similar argument to convince oneself that $\hat{A} \hat{A}^\dagger \geq 0$.

Sometimes, it is useful to normalize the eigenvectors $|a\rangle$ of a *positive operator* (Definition A.19 and Theorem A.20) with their own (positive) eigenvalues a so that $\langle a | a \rangle = a$. In this case, the spectral decomposition of a positive operator $\hat{A}$ is given by

$$\hat{A} = \sum_a |a\rangle \langle a|, \quad (\text{A.57})$$

This form of the spectral decomposition for a positive operator should not be confused with the completeness relation (A.48), where an orthonormal basis is used. For a *positive semidefinite operator*, there only appear eigenvectors with positive eigenvalues in the summation in (A.57), and the eigenvectors with zero eigenvalue are automatically dropped.

Theorem A.21 *Let $\hat{U}$ be a unitary operator on a vector space $\mathcal{V}$. Then, every eigenvalue of $\hat{U}$ is of the form $e^{i\phi}$ with $\phi \in \mathbb{R}$.*

For example, consider an operator $\hat{U}$ with the matrix representation

$$\hat{U} \doteq \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix} \quad (\text{A.58})$$

in the logical basis $|0\rangle$ and $|1\rangle$. It has two eigenvectors

$$|L/R\rangle := \frac{|0\rangle \pm i |1\rangle}{\sqrt{2}} \quad (\text{A.59})$$

with eigenvalues ± 1 . $\hat{U}$ has the spectral decomposition

$$\hat{U} = |L\rangle e^{-i\phi} \langle L| + |R\rangle e^{+i\phi} \langle R|. \quad (\text{A.60})$$

A.4.2 Functions of Operators

The spectral decomposition provides a convenient way to define *functions of a normal operator*. Let $f : \mathcal{D} \rightarrow \mathbb{C}$ be a function of complex variable defined in a domain $\mathcal{D} \subset \mathbb{C}$. Suppose that $\hat{A}$ be a normal operator with all eigenvalues $a \in \mathcal{D}$. Then the function $f(\hat{A})$ of the operator $\hat{A}$ —another operator on the same vector space derived from $\hat{A}$ —is defined by [to be compared with (A.53)]

$$f(\hat{A}) := \sum_a |a\rangle f(a) \langle a|. \quad (\text{A.61})$$

Surprisingly, most students try to define a function of an operator by means of the Taylor series expansion involving multiple powers of the operator. In most cases, however, it is very difficult to convince oneself whether the series is actually converging or not. Even if it does, it is tremendously difficult to figure out the behavior of the resulting operator, not to speak of the evaluation of the series itself. In contrast, the definition in (A.61) is well-defined as long as $f(z)$ of complex variable z is well defined, and often provides clear physical meaning of the resulting operator $f(\hat{A})$. Above all, the evaluation is straightforward and, in many cases, simple. The definition applies only to normal operators. However, it is not a serious restriction since in most physics applications, it is normal operators that we want to transform by means of already existing functions.

Consider again a Hermitian operator describing the Heisenberg exchange interaction between two $S=1/2$ spins.

```
In[ ]:= opH = -J * (Pauli[1, 1] + Pauli[2, 2] + Pauli[3, 3])
Out[ ]:= -J (σx ⊗ σx + σy ⊗ σy + σz ⊗ σz)
```

We want to consider functions of operators, for example, `opH` in particular. To do it, it is most efficient to proceed with the spectral decomposition of the operator.

```
In[ ]:= {val, vec} = ProperSystem[opH]
Out[ ]:= {{3 J, -J, -J, -J}, {{0, 1}, {1, 0}, {1, 1}, {0, 1} + {1, 0}, {0, 0}}}
```

The eigenvectors are orthogonal, but not properly normalized.

```
In[ ]:= Outer[Multiply, Dagger[vec], vec] // MatrixForm
Out[ ]:= MatrixForm[
  {
    {2 0 0 0},
    {0 1 0 0},
    {0 0 2 0},
    {0 0 0 1}
  ]
]
```

Normalize them, and check again.

```

In[ ]:= nvec = vec / Sqrt[{2, 1, 2, 1}]
Out[ ]:= Outer[Multiply, Dagger[nvec], nvec] // MatrixForm
Out[ ]:= 
$$\left\{ \frac{-|\langle 0, 1 \rangle + |1, 0\rangle}{\sqrt{2}}, |1, 1\rangle, \frac{|\langle 0, 1 \rangle + |1, 0\rangle}{\sqrt{2}}, |\langle 0, 0 \rangle\right\}$$

Out[ ]:= MatrixForm[

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$


```

Suppose we want to get the exponential function of `opH`. For example, the time-evolution operator is given by

```

In[ ]:= opU = MultiplyExp[-I t opH]
Out[ ]:= 
$$e^{i \int t (\sigma^x \otimes \sigma^x + \sigma^y \otimes \sigma^y + \sigma^z \otimes \sigma^z)}$$


```

This uses the spectral decomposition.

```

In[ ]:= newU = Total@Multiply[nvec, Exp[-I t val], Dagger[nvec]]
Out[ ]:= 
$$e^{i \int t} |\langle 0, 0 \rangle \langle 0, 0 | + \frac{1}{2} e^{i \int t} |\langle 0, 1 \rangle \langle 0, 1 | + \frac{1}{2} e^{-3 i \int t} |\langle 0, 1 \rangle \langle 0, 1 | - \frac{1}{2} e^{-3 i \int t} |\langle 1, 0 \rangle \langle 1, 0 | - \frac{1}{2} e^{-3 i \int t} |\langle 1, 0 \rangle \langle 0, 1 | - \frac{1}{2} e^{-3 i \int t} |\langle 1, 0 \rangle \langle 1, 0 | + \frac{1}{2} e^{-3 i \int t} |\langle 1, 0 \rangle \langle 0, 1 | + \frac{1}{2} e^{-3 i \int t} |\langle 1, 0 \rangle \langle 1, 0 | + e^{i \int t} |\langle 1, 1 \rangle \langle 1, 1 |$$


```

This converts the bra-ket expression into a form in terms of the Pauli operators.

```

In[ ]:= newU2 = Elaborate@ExpressionFor@Matrix[newU]
Out[ ]:= 
$$\frac{1}{4} e^{-3 i \int t} (1 + 3 e^{4 i \int t}) \sigma^0 \otimes \sigma^0 + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^x \otimes \sigma^x + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^y \otimes \sigma^y + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^z \otimes \sigma^z$$


```

In many cases, `MultiplyExp` can be further evaluated by means of `Elaborate`.

```

In[ ]:= opU2 = Elaborate@Elaborate[opU]
Out[ ]:= 
$$\frac{1}{4} e^{-3 i \int t} (1 + 3 e^{4 i \int t}) \sigma^0 \otimes \sigma^0 + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^x \otimes \sigma^x + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^y \otimes \sigma^y + \frac{1}{4} e^{-3 i \int t} (-1 + e^{4 i \int t}) \sigma^z \otimes \sigma^z$$


```

A.5 Factorization of Operators

Matrices can be decomposed into several factors. As linear operators are represented by matrices, the methods directly also applies to linear operators. We have already seen one form, the spectral decomposition, in Sect. A.4.1. Here we introduce a few more forms.

Theorem A.22 (singular-value decomposition) *Let A be an $m \times n$ matrix of complex numbers. It can be written in the form*

$$A = USV^\dagger, \quad (\text{A.62})$$

where U and V are $m \times m$ and $n \times n$ unitary matrices, respectively, and S is an $m \times n$ diagonal matrix of the form

$$S = \begin{bmatrix} s_1 & & \\ & s_2 & \\ & & \ddots \end{bmatrix} \quad (\text{A.63})$$

with $s_j \geq 0$. Positive values of s_j are called the singular values of A .

For a linear operator $\hat{A}$ on a vector space $\mathcal{V}$, one can apply the above theorem to its matrix representation A ,

$$\hat{A} = \sum_{ij} |i\rangle A_{ij} \langle j| = \sum_{ijk} |i\rangle U_{ij} s_j V_{jk}^\dagger \langle k|. \quad (\text{A.64})$$

It results in the singular-value decomposition of the operator $\hat{A}$

$$\hat{A} = \hat{U} \hat{S} \hat{V}^\dagger, \quad (\text{A.65})$$

where

$$\hat{U} := \sum_{ij} |i\rangle U_{ij} \langle j|, \quad \hat{S} := \sum_j |j\rangle s_j \langle j|, \quad \hat{V} := \sum_{ij} |i\rangle V_{ij} \langle j|. \quad (\text{A.66})$$

Since the both matrices U and V are unitary, the operators $\hat{U}$ and $\hat{V}$ are also unitary. Another useful form of the singular-value decomposition is

$$\hat{A} = \sum_j |u_j\rangle s_j \langle v_j|, \quad (\text{A.67})$$

where

$$|u_j\rangle := \sum_i |i\rangle U_{ij}, \quad \langle v_j| := \sum_i \langle i| V_{ij}. \quad (\text{A.68})$$

The unitarity of the matrices U and V implies that

$$\langle u_i | u_j \rangle = \delta_{ij}, \quad \langle v_i | v_j \rangle = \delta_{ij}. \quad (\text{A.69})$$

Theorem A.23 (polar decomposition) *Any $n \times n$ matrix A of complex numbers can be written in the form*

$$A = UP = QV, \quad (\text{A.70})$$

where U and V are unitary matrices, and $P := \sqrt{A^\dagger A}$ and $Q := \sqrt{AA^\dagger}$ are positive-definite matrices.

The above theorem has been stated for matrices. However, it is directly translated to linear operators. In other words, any linear operator $\hat{A}$ on a vector space $\mathcal{V}$ can be written in the form

$$\hat{A} = \hat{U} \hat{P} = \hat{Q} \hat{V}, \quad (\text{A.71})$$

where $\hat{P} := \sqrt{\hat{A}^\dagger \hat{A}}$ and $\hat{Q} := \sqrt{\hat{A} \hat{A}^\dagger}$ and positive operators, and $\hat{U}$ and $\hat{V}$ are unitary operators.

The polar decomposition is easily conceivable in terms of the singular-value decomposition. Suppose that

$$\hat{A} = \hat{U}' \hat{S} \hat{V}'^\dagger \quad (\text{A.72})$$

is a singular-value decomposition of a linear operator $\hat{A}$. Then we observe that

$$\hat{A} = \hat{U}' \hat{V}'^\dagger \hat{V}' \hat{S} \hat{V}'^\dagger = (\hat{U}' \hat{V}'^\dagger) \sqrt{\hat{A}^\dagger \hat{A}}, \quad (\text{A.73})$$

which is of the first form in (A.71). Here recall from Sect. A.4.2 that for a positive operator $\hat{C}$ (such as $\hat{A}^\dagger \hat{A}$ and $\hat{A} \hat{A}^\dagger$) with spectral decomposition

$$\hat{C} = \sum_c |c\rangle c \langle c| \quad (c \geq 0), \quad (\text{A.74})$$

the new operator $\sqrt{\hat{C}}$ is given by

$$\sqrt{\hat{C}} = \sum_c |c\rangle \sqrt{c} \langle c|. \quad (\text{A.75})$$

Similarly, we rearrange the factors as

$$\hat{A} = \hat{U}' \hat{S} \hat{U}'^\dagger \hat{U}' \hat{V}'^\dagger = \sqrt{\hat{A} \hat{A}^\dagger} (\hat{U}' \hat{V}'^\dagger). \quad (\text{A.76})$$

It is of the second form in (A.71).

A.6 Tensor-Product Spaces

When there are more than one systems, each system is associated with a different vector space. Even for a single system, independent degrees of freedom (such as external and internal degrees of freedom) are associated with different vector spaces.

Then the vector space of the total system should be constructed by the vector spaces associated with the individual systems or degrees of freedom. Mathematically, such a construction is called the tensor product of the constituent vector spaces.

A.6.1 Vectors in a Product Space

Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces, and $\{|v_i\rangle\}$ and $\{|w_j\rangle\}$ their respective bases. The tensor product $\mathcal{V} \otimes \mathcal{W}$ is a vector space spanned by the basis

$$\{|v_i\rangle \otimes |w_j\rangle : i = 1, \dots, \dim \mathcal{V}; j = 1, \dots, \dim \mathcal{W}\} \quad (\text{A.77})$$

We call it the *standard tensor-product basis* or simply *standard basis* of $\mathcal{V} \otimes \mathcal{W}$. Obviously, the dimension of $\mathcal{V} \otimes \mathcal{W}$ is given by $\dim(\mathcal{V} \otimes \mathcal{W}) = (\dim \mathcal{V})(\dim \mathcal{W})$. The symbol ‘ $\otimes$ ’ in the basis states separates $|v_i\rangle$ and $|w_j\rangle$ from each other clearly indicating which vector space they are from. In many cases, when there is no risk of confusion, it is dropped and the product states are simply written as $|v_i\rangle |w_j\rangle$ or even $|v_i w_j\rangle$.

Here is the standard basis (product basis) for a (unlabelled) two-qubit system.

```
In[ ]:= bs = Basis[2];
      bs // LogicalForm
Out[ ]:= { |0, 0⟩, |0, 1⟩, |1, 0⟩, |1, 1⟩ }
```

The Hermitian products $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ and $\langle \cdot, \cdot \rangle_{\mathcal{W}}$ in the corresponding spaces are inherited to the tensor-product space to give the standard Hermitian product

$$(\langle v_i | \otimes \langle w_j |)(|v_k\rangle \otimes |w_l\rangle) = \langle v_i | v_k \rangle_{\mathcal{V}} \langle w_j | w_l \rangle_{\mathcal{W}}. \quad (\text{A.78})$$

Expanded in the standard basis, a vector

$$|\Psi\rangle = \sum_{ij} |v_i\rangle \otimes |w_j\rangle \Psi_{ij} \in \mathcal{V} \times \mathcal{W} \quad (\text{A.79})$$

involves $M \times N$ terms in general, where $M := \dim \mathcal{V}$ and $N := \dim \mathcal{W}$. It can be reduced to a form with much less terms. To see this, rewrite the matrix Ψ consisting of the expansion coefficients Ψ_{ij} by means of the singular-value decomposition (Theorem A.22)

$$\Psi = U \Sigma V^\dagger, \quad (\text{A.80})$$

where U is a $M \times M$ unitary matrix, V a $N \times N$ matrix, and Σ a $M \times N$ diagonal matrix. The diagonal elements s_j of Σ are all non-negative, and the number R of non-zero elements cannot be greater than $\min(M, N)$. Putting (A.80) back into (A.79)

leads to the so-called *Schmidt decomposition*

$$|\Psi\rangle = \sum_{j=1}^R |\alpha_j\rangle \otimes |\beta_j\rangle s_j, \quad |\alpha_j\rangle := \sum_i |v_i\rangle U_{ij}, \quad |\beta_j\rangle := \sum_i |w_i\rangle V_{ij}^*. \quad (\text{A.81})$$

Note that $\langle \alpha_i | \alpha_j \rangle = \delta_{ij}$ and $\langle \beta_i | \beta_j \rangle = \delta_{ij}$ because U and V are unitary, and that $\sum_{j=1}^R s_j^2 = 1$ ($0 < s_j < 1$) if $|\Psi\rangle$ is normalized.

The number R is called the *Schmidt rank* or *Schmidt number* of the vector $|\Psi\rangle$. When $R = 1$, $|\Psi\rangle$ is factorized as $|\Psi\rangle = |\alpha_1\rangle \otimes |\beta_1\rangle$, and is said to be *separable*. Otherwise, it cannot be factorized and it is called an *entangled vector*. The Schmidt decomposition is a convenient method to test whether a vector is separable or entangled.

Consider an arbitrary vector in the tensor-product space.

```
In[ ]:= cc = Re@RandomVector[4];
vec = bs.cc;
vec // LogicalForm
```

```
Out[ ]:= -0.392437 |0, 0> + 0.309225 |0, 1> - 0.352869 |1, 0> + 0.733405 |1, 1>
```

This is its Schmidt decomposition and shows that the state vector is entangled.

```
In[ ]:= {ww, uu, vv} = SchmidtDecomposition[vec, {1}, {2}];
ww // Normal
uu
vv
```

```
Out[ ]:= {0.935711, 0.190978}
```

```
Out[ ]:= {0.504017 |0> + 0.863694 |1>, -0.863694 |0> + 0.504017 |1>}
```

```
Out[ ]:= {-0.537096 |0> + 0.843521 |1>, 0.843521 |0> + 0.537096 |1>}
```

SchmidtForm presents the Schmidt decomposition in a more intuitively-appealing form. For a thorough analysis of the result, use **SchmidtDecomposition**.

```
In[ ]:= new = SchmidtForm[vec, {1}, {2}]
```

```
Out[ ]:= 0.190978 (-0.863694 |0> + 0.504017 |1>) ⊗ (0.843521 |0> + 0.537096 |1>) +
0.935711 (0.504017 |0> + 0.863694 |1>) ⊗ (-0.537096 |0> + 0.843521 |1>)
```

Check whether the two vectors are the same or not.

```
In[ ]:= vec - ReleaseTimes[new] // Garner // Chop
```

```
Out[ ]:= 0
```

A.6.2 Operators on a Product Space

Let $\hat{A}$ and $\hat{B}$ be linear operators on $\mathcal{V}$ and $\mathcal{W}$, respectively. Then the *tensor-product operator* $\hat{A} \otimes \hat{B}$ is a linear operator on the tensor-product space $\mathcal{V} \otimes \mathcal{W}$ defined by the association

$$(\hat{A} \otimes \hat{B})(|v_i\rangle \otimes |w_j\rangle) = (\hat{A}|v_i\rangle) \otimes (\hat{B}|w_j\rangle). \quad (\text{A.82})$$

Suppose that $\hat{A}$ and $\hat{B}$ are represented by matrices A and B , respectively, i.e.,

$$\hat{A}|v_j\rangle = \sum_i |v_i\rangle A_{ij}, \quad \hat{B}|w_j\rangle = \sum_i |w_i\rangle B_{ij}. \quad (\text{A.83})$$

Then it follows from (A.82) that

$$(\hat{A} \otimes \hat{B})(|v_i\rangle \otimes |w_j\rangle) = \left(\sum_k |v_k\rangle A_{ki} \right) \otimes \left(\sum_l |w_l\rangle B_{lj} \right) = \sum_{kl} |v_k\rangle \otimes |w_l\rangle A_{ki} B_{lj}. \quad (\text{A.84})$$

This implies that the matrix representation of $\hat{A} \otimes \hat{B}$ in the standard product basis is given by the *direct product* $A \otimes B$ of the two matrices.

In general, a linear operator $\hat{C}$ on $\mathcal{V} \otimes \mathcal{W}$ is not a single product but a sum of such products. How many terms are there? Suppose that the matrix $C_{ij;kl}$ is the matrix representation of $\hat{C}$ in the standard product basis,

$$\hat{C}|v_k w_l\rangle = \sum_{ij} |v_i w_j\rangle C_{ij;kl}, \quad (\text{A.85})$$

or equivalently,

$$\hat{C} = \sum_{ij;kl} |v_i w_j\rangle \langle v_k w_l| C_{ij;kl} = \sum_{ij;kl} |v_i\rangle \langle v_k| \otimes |w_j\rangle \langle w_l| C_{ij;kl}. \quad (\text{A.86})$$

The $M^2 \times N^2$ matrix $G_{ik;jl} := C_{ij;kl}$ with collective indices (ik) and (jl) has a singular value decomposition

$$G_{ik;jl} = \sum_{\mu} U_{ik;\mu} \gamma_{\mu} V_{\mu;jl}^{\dagger}, \quad \gamma_{\mu} \geq 0. \quad (\text{A.87})$$

Defining

$$\hat{A}_{\mu} := \sum_{ik} |v_i\rangle \langle v_k| U_{ik;\mu}, \quad \hat{B}_{\mu} := \sum_{jl} |w_j\rangle \langle w_l| V_{jl;\mu}^*, \quad (\text{A.88})$$

leads to the expression

$$\hat{C} = \sum_{\mu} \hat{A}_{\mu} \otimes \hat{B}_{\mu} \gamma_{\mu} , \quad (\text{A.89})$$

which is in direct analogy with the Schmidt decomposition (A.81) of a vector in the tensor-product space. Here the number of non-vanishing singular values γ_{μ} is less than or equal to $\min(M^2, N^2)$.

Bibliography

- Aaronson, S., & Gottesman, D. (2004). Improved simulation of stabilizer circuits. *Physical Review A*, 70(5). <https://doi.org/10.1103/physreva.70.052328>. arXiv:quant-ph/0406196.
- Aharonov, Y., & Anandan, J. (1987). Phase change during a cyclic quantum evolution. *Physical Review Letters*, 58(16), 1593. <https://doi.org/10.1103/PhysRevLett.58.1593>.
- Alicea, J., Oreg, Y., Refael, G., von Oppen, F., & Fisher, M. P. A. (2011). Non-Abelian statistics and topological quantum information processing in 1D wire networks. *Nature Physics*, 7(5), 412. <https://doi.org/10.1038/nphys1915>.
- Anandan, J. (1988). Non-adiabatic non-abelian geometric phase. *Physics Letters A*, 133(4-5), 171. [https://doi.org/10.1016/0375-9601\(88\)91010-9](https://doi.org/10.1016/0375-9601(88)91010-9).
- Aspect, A., Grangier, P., & Roger, G. (1981). Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47(7), 460.
- Barenco, A., Bennett, C. H., Cleve, R., et al. (1995). Elementary gates for quantum computation. *Physical Review A*, 52(5), 3457. <https://doi.org/10.1103/physreva.52.3457>. arXiv:quant-ph/9503016.
- Bell, J. S. (1966). On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3), 447.
- Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., & Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5), 3824. <https://doi.org/10.1103/PhysRevA.54.3824>. arXiv:quant-ph/9604024.
- Bennett, C. H., & Wiesner, S. J. (1992). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20), 2881.
- Bergou, J. A., Herzog, U., & Hillery, M. (2004). Discrimination of quantum states. In Paris & Rehacek (Chap. 11, pp. 417–465). https://doi.org/10.1007/978-3-540-44481-7_11.
- Bernstein, E., & Vazirani, U. (1993). Quantum complexity theory. In *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing* (pp. 11–20). New York: ACM Press.
- Bernstein, E., & Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal on Computing*, 26(5), 1411. <https://doi.org/10.1137/s0097539796300921>.
- Berry, M. V. (1984). Quantal phase factors accompanying adiabatic changes. *Proceedings of the Royal Society London A*, 392, 45.
- Blum, K. (2012). *Density matrix theory and applications*, Springer series on atomic, optical, and plasma physics (Vol. 64, 3rd ed.). Berlin, Heidelberg: Springer. ISBN 978-3-642-20560-6.
- Bohr, N. (1949). Discussion with Albert Einstein on epistemological problems in atomic physics. In P. A. Schilpp (Ed.), *Albert Einstein, philosopher-scientist*, The library of living philosophers (Vol. VII, pp. 200–241, 1st ed.). Evanston: Harper.
- Born, M. (1926). Zur Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik*, 37(12), 863.

- Bouwmeester, D., Pan, J.-W., Daniell, M., Weinfurter, H., & Zeilinger, A. (1999). Observation of three-photon Greenberger-Horne-Zeilinger entanglement. *Physical Review Letters*, 82(7), 1345.
- Bravyi, S. B., & Kitaev, A. Y. (1998). Quantum codes on a lattice with boundary. [arXiv:quant-ph/9811052](https://arxiv.org/abs/quant-ph/9811052).
- Breuer, H.-P., & Petruccione, F. (2002). *The theory of open quantum systems*. New York: Oxford University Press.
- Browne, D., & Briegel, H. (2016) One-way quantum computation. In D. Bruß, & G. Leuchs (Eds.), *Quantum information: From foundations to quantum technology applications* (pp. 449–473, 2nd ed.). Wiley. <https://doi.org/10.1002/9783527805785.ch21>. [arXiv:quant-ph/0603226](https://arxiv.org/abs/quant-ph/0603226).
- Calderbank, A. R., & Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, 54(2), 1098.
- Caves, C. M. (1981). Quantum-mechanical noise in an interferometer. *Physical Review D*, 23(8), 1693.
- Chefles, A. (2004). Quantum states: Discrimination and classical information transmission. A review of experimental progress. In Paris & Rehacek (Chap. 12, pp. 467–511). https://doi.org/10.1007/978-3-540-44481-7_12.
- Chiaverini, J. (2005). Implementation of the semiclassical quantum Fourier transform in a scalable system. *Science*, 308(5724), 997. <https://doi.org/10.1126/science.1110335>.
- Choi, M.-S. (2003). Geometric quantum computation in solid-state qubits. *Journal of Physics: Condensed Matter*, 15(46), 7823. [arXiv:quant-ph/0111019](https://arxiv.org/abs/quant-ph/0111019).
- Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23, 880.
- Cleve, R., Ekert, A., Macchiavello, C., & Mosca, M. (1998). Quantum algorithms revisited. *Proceedings of the Royal Society A*, 454(1969), 339. <https://doi.org/10.1098/rspa.1998.0164>. [arXiv:quant-ph/9708016](https://arxiv.org/abs/quant-ph/9708016).
- Cleve, R., & Gottesman, D. (1997). Efficient computations of encodings for quantum error correction. *Physical Review A*, 56(1), 76. <https://doi.org/10.1103/physreva.56.76>. [arXiv:quant-ph/9607030](https://arxiv.org/abs/quant-ph/9607030).
- Cornwell, J. F. (1984). *Group theory in physics* (Vol. I). Orlando: Academic Press.
- Cornwell, J. F. (1997). *Group theory in physics: An introduction*. San Diego: Academic Press.
- Crease, R. P. (2002). The most beautiful experiment. *Physics World*, 15(9), 19. <https://doi.org/10.1088/2058-7058/15/9/22>.
- Das, A., Ronen, Y., Most, Y., Oreg, Y., Heiblum, M., & Shtrikman, H. (2012). Zero-bias peaks and splitting in an Al-InAs nanowire topological superconductor as a signature of Majorana fermions. *Nature Physics*, 8(12), 887.
- Deng, M. T., Yu, C. L., Huang, G. Y., Larsson, M., Caroff, P., & Xu, H. Q. (2012). Anomalous Zero-Bias Conductance Peak in a Nb–InSb Nanowire–Nb Hybrid Device. *Nano Letters*, 12(12), 6414.
- Dennis, E., Kitaev, A., Landahl, A., & Preskill, J. (2002). Topological quantum memory. *Journal of Mathematical Physics*, 43(9), 4452. <https://doi.org/10.1063/1.1499754>. [arXiv:quant-ph/0110143](https://arxiv.org/abs/quant-ph/0110143).
- Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400, 97. <https://doi.org/10.1098/rspa.1985.0070>.
- Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 439(1907), 553. <https://doi.org/10.1098/rspa.1992.0167>.
- Dirac, P. A. M. (1958). *The principles of quantum mechanics* (4th ed.). Oxford: Oxford University Press.
- DiVincenzo, D. P. (2000). The physical implementation of quantum computation. *Fortschritte der Physik*, 48, 771. [https://doi.org/10.1002/1521-3978\(200009\)48:9/11<771::AID-PROP771>3.0.CO;2-E](https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E). [arXiv:quant-ph/0002077](https://arxiv.org/abs/quant-ph/0002077).

- Dum, R., Parkins, A. S., Zoller, P., & Gardiner, C. W. (1992). Monte Carlo simulation of master equations in quantum optics for vacuum, thermal, and squeezed reservoirs. *Physical Review A*, 46(7), 4382.
- Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47, 777.
- Feynman, R., Leighton, R. B., & Sands, M. L. (1963). *The Feynman lectures on physics* (Vol. III, 1st ed.). Redwood City: Addison-Wesley.
- Fowler, A. G., Mariantoni, M., Martinis, J. M., & Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3), 032324. <https://doi.org/10.1103/physreva.86.032324>. [arXiv:1208.0928](https://arxiv.org/abs/1208.0928).
- Freedman, M. H. (2001). Quantum computation and the localization of modular functors. *Foundations of Computational Mathematics*, 1(2), 183. <https://doi.org/10.1007/s102080010006>.
- Giovannetti, V., Lloyd, S., & Maccone, L. (2006). Quantum metrology. *Physical Review Letters*, 96(1), 010401. <https://doi.org/10.1103/PhysRevLett.96.010401>. [arXiv:quant-ph/0509179](https://arxiv.org/abs/quant-ph/0509179).
- Gisin, N. (1989). Stochastic quantum dynamics and relativity. *Helvetica Physica Acta*, 62, 363. <https://doi.org/10.5169/seals-116034>.
- Goldstein, S. (1994). Nonlocality without inequalities for almost all entangled states for two particles. *Physical Review Letters*, 72(13), 1951.
- Gottesman, D. (1996). Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54(3), 1862. <https://doi.org/10.1103/physreva.54.1862>. [arXiv:quant-ph/9604038](https://arxiv.org/abs/quant-ph/9604038).
- Gottesman, D. (1997). *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, California Institute of Technology, Pasadena, California. [arXiv:quant-ph/9705052](https://arxiv.org/abs/quant-ph/9705052).
- Gottesman, D. (1998). Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1), 127. <https://doi.org/10.1103/PhysRevA.57.127>. [arXiv:quant-ph/9702029](https://arxiv.org/abs/quant-ph/9702029).
- Gottesman, D. (1999). The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, & P. D. Jarvis (Eds.), *Group22: Proceedings of XXII International Colloquium on Group Theoretical Methods in Physics: Hobart, July 13–17, 1998*. Cambridge, MA: International Press. ISBN 978-1571460547. [arXiv:quant-ph/9807006](https://arxiv.org/abs/quant-ph/9807006).
- Greenberger, D. M., Horne, M. A., Shimony, A., & Zeilinger, A. (1990). Bell's theorem without inequalities. *American Journal of Physics*, 58, 1131. <https://doi.org/10.1119/1.16243>.
- Greenberger, D. M., Horne, M. A., & Zeilinger, A. (1989). Going beyond Bell's theorem. In M. Kafatos (Ed.), *Bell's theorem, quantum theory, and conceptions of the universe*. Dordrecht, The Netherlands: Kluwer Academic. [arXiv:0712.0921](https://arxiv.org/abs/0712.0921).
- Griffiths, R. B., & Niu, C.-S. (1996). Semiclassical Fourier transform for quantum computation. *Physical Review Letters*, 76(17), 3228. <https://doi.org/10.1103/physrevlett.76.3228>. [arXiv:quant-ph/9511007](https://arxiv.org/abs/quant-ph/9511007).
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (p. 212). New York: ACM Press. [arXiv:quant-ph/9605043](https://arxiv.org/abs/quant-ph/9605043).
- Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2), 325.
- Hardy, L. (1992). Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Physical Review Letters*, 68(20), 2981.
- Hardy, L. (1993). Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71, 1665.
- Higgins, B. L., Berry, D. W., Bartlett, S. D., Wiseman, H. M., & Pryde, G. J. (2007). Entanglement-free Heisenberg-limited phase estimation. *Nature*, 450(7168), 393. <https://doi.org/10.1038/nature06257>. [arXiv:0709.2996](https://arxiv.org/abs/0709.2996).
- Horodecki, M., Horodecki, P., & Horodecki, R. (1996). Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A*, 223(1), 1. [https://doi.org/10.1016/0375-9601\(95\)00930-2](https://doi.org/10.1016/0375-9601(95)00930-2).

- Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Reviews of Modern Physics*, 81(2), 865. <https://doi.org/10.1103/RevModPhys.81.865>.
- Hughston, L. P., Jozsa, R., & Wootters, W. K. (1993). A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183(1), 14. [https://doi.org/10.1016/0375-9601\(93\)90880-9](https://doi.org/10.1016/0375-9601(93)90880-9).
- Jiang, M., Luo, S., & Fu, S. (2013). Channel-state duality. *Physical Review A*, 87(2). <https://doi.org/10.1103/physreva.87.022310>.
- Jönsson, C. (1961). Electron diffraction at multiple slits. *Zeitschrift für Physik*, 161, 454. <https://doi.org/10.1007/BF01342460>.
- Kitaev, A. Y. (1996). Quantum measurements and the Abelian stabilizer problem. *Electronic Colloquium on Computational Complexity*, 3, 3. [arXiv:quant-ph/9511026](https://arxiv.org/abs/quant-ph/9511026).
- Kitaev, A. Y. (1997). Quantum computations: Algorithms and error correction. *Russian Mathematical Surveys*, 52(6), 1191.
- Kitaev, A. Y. (2001). Unpaired Majorana fermions in quantum wires. *Physics-Uspekhi*, 44(10S), 131. <https://doi.org/10.1070/1063-7869/44/10S/S29>. [arXiv:cond-mat/0010440](https://arxiv.org/abs/cond-mat/0010440).
- Kitaev, A. Y. (2003). Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1), 2. [https://doi.org/10.1016/S0003-4916\(02\)00018-0](https://doi.org/10.1016/S0003-4916(02)00018-0). [arXiv:quant-ph/9707021](https://arxiv.org/abs/quant-ph/9707021).
- Laflamme, R., Miquel, C., Paz, J. P., & Zurek, W. H. (1996). Perfect quantum error correcting code. *Physical Review Letters*, 77(1), 198. <https://doi.org/10.1103/physrevlett.77.198>. [arXiv:quant-ph/9602019](https://arxiv.org/abs/quant-ph/9602019).
- Landauer, R. (1991). Information is physical. *Physics Today*, 44(5), 23.
- Lang, S. (1986). *Introduction to linear algebra*, Undergraduate texts in mathematics (2nd ed.). New York: Springer. ISBN 9781461210702. <https://doi.org/10.1007/978-1-4612-1070-2>.
- Lang, S. (1987). *Linear algebra* (3rd ed.). Berlin: Springer. ISBN 978-1-4757-1949-9. <https://doi.org/10.1007/978-1-4757-1949-9>.
- Loss, D., & DiVincenzo, D. P. (1998). Quantum computation with quantum dots. *Physical Review A*, 57(1), 120.
- Lundeen, J. S., Sutherland, B., Patel, A., Stewart, C., & Bamber, C. (2011). Direct measurement of the quantum wavefunction. *Nature*, 474(7350), 188. <https://doi.org/10.1038/nature10120>.
- Mourik, V., Zuo, K., Frolov, S. M., Plissard, S. R., Bakkers, E. P. A. M., & Kouwenhoven, L. P. (2012). Signatures of Majorana fermions in hybrid superconductor-semiconductor nanowire devices. *Science*, 336(6084), 1003.
- Nadj-Perge, S., Drozdov, I. K., Li, J., et al. (2014). Observation of Majorana fermions in ferromagnetic atomic chains on a superconductor. *Science*, 346(6209), 602. <https://doi.org/10.1126/science.1259327>. [arXiv:http://www.sciencemag.org/content/346/6209/602.full.pdf](https://arxiv.org/abs/http://www.sciencemag.org/content/346/6209/602.full.pdf).
- Nakazato, H., Hida, Y., Yuasa, K., Militello, B., Napoli, A., & Messina, A. (2006). Solution of the Lindblad equation in the Kraus representation. *Physical Review A*, 74(6), 062113. <https://doi.org/10.1103/physreva.74.062113>. [arXiv:quant-ph/0606193](https://arxiv.org/abs/quant-ph/0606193).
- Nielsen, M., & Chuang, I. L. (2011). *Quantum computation and quantum information* (10th anniversary ed.). New York: Cambridge University Press. ISBN 978-1107002173.
- Ozawa, M. (2000). Entanglement measures and the Hilbert–Schmidt distance. *Physics Letters A*, 268(3), 158. [https://doi.org/10.1016/s0375-9601\(00\)00171-7](https://doi.org/10.1016/s0375-9601(00)00171-7).
- Pan, J.-W., Bouwmeester, D., Daniell, M., Weinfurter, H., & Zeilinger, A. (2000). Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. *Nature*, 403, 515.
- Paris, M., & Rehacek, J. (Eds.). (2004). *Quantum state estimation*, Lecture notes in physics (Vol. 649). Berlin, Heidelberg: Springer. ISBN 9783540444817. <https://doi.org/10.1007/b98673>.
- Peres, A. (1996). Separability criterion for density matrices. *Physical Review Letters*, 77(8), 1413. <https://doi.org/10.1103/PhysRevLett.77.1413>. [arXiv:quant-ph/9604005](https://arxiv.org/abs/quant-ph/9604005).
- Pérez-García, D., Wolf, M. M., Petz, D., & Ruskai, M. B. (2006). Contractivity of positive and trace-preserving maps under L_p norms. *Journal of Mathematical Physics*, 47(8), 083506. <https://doi.org/10.1063/1.2218675>. [arXiv:math-ph/0601063](https://arxiv.org/abs/math-ph/0601063).

- Plenio, M. B., & Knight, P. L. (1998). The quantum-jump approach to dissipative dynamics in quantum optics. *Reviews of Modern Physics*, 70(1), 101.
- Plenio, M. B., & Virmani, S. (2007). An introduction to entanglement measures. *Quantum Information & Computation*, 7(1&2), 1. [arXiv:quant-ph/0504163](https://arxiv.org/abs/quant-ph/0504163).
- Preskill, J. (1998). Lecture Notes on Quantum Information and Computation, unpublished.
- Raussendorf, R., & Briegel, H. J. (2001). A one-way quantum computer. *Physical Review Letters*, 86(22), 5188.
- Raussendorf, R., Browne, D., & Briegel, H. (2002). The one-way quantum computer—a non-network model of quantum computation. *Journal of Modern Optics*, 49(8), 1299. <https://doi.org/10.1080/09500340110107487>. [arXiv:quant-ph/0108118](https://arxiv.org/abs/quant-ph/0108118).
- Raussendorf, R., Browne, D. E., & Briegel, H. J. (2003). Measurement-based quantum computation on cluster states. *Physical Review A*, 68(2), 022312. <https://doi.org/10.1103/PhysRevA.68.022312>. [arXiv:quant-ph/0301052](https://arxiv.org/abs/quant-ph/0301052).
- Schwinger, J. (1959). The algebra of microscopic measurement. *Proceedings of the National Academy of Sciences*, 45(10), 1542. <https://doi.org/10.1073/pnas.45.10.1542>.
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). Washington, DC, USA: IEEE Computer Society. SFCS '94. <https://doi.org/10.1109/SFCS.1994.365700>.
- Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484. [arXiv:quant-ph/9508027](https://arxiv.org/abs/quant-ph/9508027).
- Simon, D. R. (1997). On the power of quantum computation. *SIAM Journal on Computing*, 26(5), 1474. <https://doi.org/10.1137/s0097539796298637>.
- Sjöqvist, E., Tong, D. M., Mauritz Andersson, L., Hessmo, B., Johansson, M., & Singh, K. (2012). Non-adiabatic holonomic quantum computation. *New Journal of Physics*, 14(10), 103035. <https://doi.org/10.1088/1367-2630/14/10/103035>. [arXiv:1107.5127](https://arxiv.org/abs/1107.5127).
- Smolin, J. A., & DiVincenzo, D. P. (1996). Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate. *Physical Review A*, 53(4), 2855. <https://doi.org/10.1103/PhysRevA.53.2855>.
- Steane, A. M. (1996). Error correcting codes in quantum theory. *Physical Review Letters*, 77(5), 793.
- Størmer, E. (2013). *Positive linear maps of operator algebras*. Berlin: Springer. ISBN 9783642343698. <https://doi.org/10.1007/978-3-642-34369-8>.
- Tonomura, A., Endo, J., Matsuda, T., Kawasaki, T., & Ezawa, H. (1989). Demonstration of single-electron buildup of an interference pattern. *American Journal of Physics*, 57(2), 117. <https://doi.org/10.1119/1.16104>.
- Vallone, G., & Dequal, D. (2016). Strong measurements give a better direct measurement of the quantum wave function. *Physical Review Letters*, 116(4), 040502. <https://doi.org/10.1103/physrevlett.116.040502>. [arXiv:1504.06551](https://arxiv.org/abs/1504.06551).
- Vedral, V., Barenco, A., & Ekert, A. (1996). Quantum networks for elementary arithmetic operations. *Physical Review A*, 54(1), 147. <https://doi.org/10.1103/physreva.54.147>. [arXiv:quant-ph/9511018](https://arxiv.org/abs/quant-ph/9511018).
- Vedral, V., Plenio, M. B., Rippin, M. A., & Knight, P. L. (1997). Quantifying entanglement. *Physical Review Letters*, 78(12), 2275. <https://doi.org/10.1103/physrevlett.78.2275>.
- Wang, C., Harrington, J., & Preskill, J. (2003). Confinement-Higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory. *Annals of Physics*, 303(1), 31. [https://doi.org/10.1016/s0003-4916\(02\)00019-2](https://doi.org/10.1016/s0003-4916(02)00019-2).
- Wehrl, A. (1978). General properties of entropy. *Reviews of Modern Physics*, 50(2), 221. <https://doi.org/10.1103/revmodphys.50.221>.
- Weyl, H. (1931). *The theory of groups and quantum mechanics*. London: Dover.
- Wigner, E. P. (1959). *Group theory and its application to the quantum mechanics of atomic spectra* (English translation ed.). New York: Academic Press.

- Wilczek, F., & Zee, A. (1984). Appearance of Gauge structure in simple dynamical systems. *Physical Review Letters*, 52(24), 2111. <https://doi.org/10.1103/PhysRevLett.52.2111>.
- Wilmut, I., Schnieke, A. E., McWhir, J., Kind, A. J., & Campbell, K. H. S. (1997). Viable offspring derived from fetal and adult mammalian cells. *Nature*, 385(6619), 810.
- Wooters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299, 802.
- Zanardi, P., & Rasetti, M. (1999). Holonomic quantum computation. *Physics Letters A*, 264(2-3), 94. [https://doi.org/10.1016/S0375-9601\(99\)00803-8](https://doi.org/10.1016/S0375-9601(99)00803-8). [arXiv:quant-ph/9904011](https://arxiv.org/abs/quant-ph/9904011).
- Zurek, W. H. (1991). Decoherence and the transition from quantum to classical. *Physics Today*, 44(10), 36.
- Zurek, W. H. (2000). Quantum cloning: Schrodinger's sheep. *Nature*, 404, 130. <https://doi.org/10.1038/35004684>.
- Zurek, W. H. (2002). Decoherence and the transition from quantum to classical: Revisited. *Los Alamos Science*, 27, 2.

Index

A

Abelian group, 279, 398, 403
Amplitude damping, 220
Ancillary qubit, 75

B

Basis, 352, 353
 orthonormal basis, 353, 354, 356, 359
Bayes' rule, 329
Bayes, T., 329
Bell basis, 133, *see also* Bell states
Bell, J., 130
Bell measurement, 83, 133, 208
Bell's inequality, 130
Bell states, 83, 133
Bell's test, 130
Bernstein-Vazirani algorithm, 136, 144
Bilinear mapping, 351
Birthday paradox, 145
Bit flip, 37
Bit-flip correction code, 301
Bit-flip error, 259, 261, 263–265, 299
Bitwise AND, 72
Bloch space, 93, 99, 182, 284
Bloch sphere, 4, 12, 43
Bloch states, 175
Bloch vector, 4, 12, 242
Bohr, Niels H. D., 191
Bra-ket notation, 35, 360
Bright state, 104

C

Calderbank-Shor-Steane codes, 305

Canonical distance, 352
Canonical norm, 236, 352
Cauchy–Schwarz inequality, 254, 255, 351, 416
Center, 277
Change of basis, 354, 357
Channel-state duality, 207
Choi isomorphism, 206–209, 388
Choi matrix, 206, 207, 379, *see also* Choi operator
Choi operator, 207, 252, 388, *see also* Choi matrix
Choi vector, 205, 209
Classical communication channel, 133
Classical feedback control, 291, *see also* semiclassical feedback control
Classical fidelity, 326
Clifford circuit, 289, 290
Clifford group, 283, 287, 321, 322
Clifford operators, 283, 301, 302, *see also* Pauli operators
Closed system, 2, 189, 196
Closure relation, 199
Cluster state, 86, 112, 124
CNOT gate, 46, 55, 57, 77, 81, 99, 113, 133, 176, 193, 283, 286, 288, 295
 controlled-NOT gate, 46
 multi-qubit controlled-NOT, 73
Code space, 258, 271
Code words, 264
Coherence, 91
Complementarity principle, 2
Completely positive and trace-preserving supermap, 197

Completely positive supermap, 196–198, 207, 383–385, 390, 393
 Completeness relation, 26, 216, 364
 Computational basis, 167, *see also* logical basis
 Concave function, 334, 347
 Concavity of entropy, 347
 Conditional entropy, 329
 Conjugation, 283, 286
 Continued fraction, 172
 Controlled-unitary gate, 46, 62, 161, 188
 multi-qubit controlled-unitary gate, 60, 70
 Controlled-Z gate, 52, *see also* CZ gate
 control qubit, 47
 Convergent of a continued fraction
 continued fraction, 172
 Convex function, 327, 347
 Convex linear, 197
 Coset, 277, 282, 400
 left coset, 401
 right coset, 401
 CSS codes, 305, *see also* Calderbank-Shor-Steane codes
 Cyclic evolution, 111
 Cyclic group, 284, 398, 403
 CZ gate, 52, 100, 101, 113, 125, 283

D

Damping operator, 218, 221, 228
 Dark state, 104, 125
 De Broglie, Louis, 191
 Decoherence, 7, 15, 21, 197, 257
 Density matrix, 8, *see also* density operator
 Density operator, 8, 9, 190, 196, 197, 207, 224, 241, 331, 363, 373
 Dephasing, 211, 212
 Depolarizing process, 221
 Deutsch-Jozsa algorithm, 136
 Deutsch-Jozsa problem, 145
 Dimension, 352
 Dirac, P. M. A., 191
 Direct product group, 402
 Discrete Fourier transform, 150, 151, 168
 Discrete logarithm, 150
 Distillable entanglement, 346
 DiVincenzo criteria, 90
 Double-slit experiment, 190, 193
 Dual basis, 360
 Dual vector, 359

E

Effective Hamiltonian, 217, 221, 228
 Eigenbasis, 363
 Eigenvalue, 362
 Eigenvector, 362
 Einstein, Albert, 7, 129, 191
 Elementary quantum logic gates, 34
 Elements, 1, 172
 Entangled state, 5, 7, 48, 339, 370
 Entanglement, 7, 15, 21, 26, 52, 123, 133, 139, 323, 338
 Entanglement cost, 346
 Entanglement distillation, 343
 Entanglement fidelity, 207
 Entanglement measure, 242
 Entanglement witness, 342
 Entropy, 323–325
 Entropy of entanglement, 345, 346
 Environment, 189, 257
 Error-detection, 259, 261
 Error operators, 270
 Error-recovery, 259
 Error syndrome, 259, 269, 298, 299, 316, 318, 319
 Euclidean algorithm, 172
 Euclidean distance, 326
 Euclid of Alexandria, 1, 172
 Euler, L., 44
 Euler rotation, 44, 117
 Euler angles, 44
 Exclusive OR, 50

F

Factor group, 401, *see also* quotient group
 Feynman, Richard P., 191
 Fidelity, 207, 234, 246–248, 352
 Field, 349
 Flux quantization, 89
 Fredkin gate, 77, 78
 Frobenius inner product, 377, *see also* Hilbert-Schmidt inner product

G

Gate teleportation, 208
 Gauge transformation, 112
 Generalized interaction picture, 228
 Generalized measurement, 215
 Geometric phase, 103
 Geometric quantum computation, 109, 111, 112
 GHZ state, 52, 85
 Gibbs' inequality, 327, 336

Gibbs, J. W., 326
 Gisin-Hughston-Jozsa-Wooters (GHJW) theorem, 14
 Golden ratio, 173
 Gottesman-Knill theorem, 289
 Gottesman vector, 278, 279, 282, 321, 420
 Graph state, 112, 122–124, 290, *see also* cluster state
 Gray code, 60, 71
 Gray code sequence, 72
 Greenberger-Horne-Zeilinger experiment, 289
 Greenberger-Horne-Zeilinger state, 52, 85
 Group, 395
 Group generators, 275, 291, 397
 Group theory, 274, 395
 Grover, L. K., 178
 Grover operator, 181
 Grover rotation, 183
 Grover's algorithm, 178, *see also* quantum search algorithm
 Grover's diffusion operator, 178

H

Hadamard gate, 39, 81, 84, 85, 100, 113, 116, 133, 283, 286–288
 Hadamard matrix, 39
 Hardy's test, 131
 Heisenberg exchange interaction, 99, 101
 Heisenberg limit, 26
 Hermitian, 235
 Hermitian conjugate, 358
 Hermitian operator, 196, 358, 362, 382
 Hermitian product, 351, 352, 354, 357, 359, 377
 Hidden subgroup problem, 150, 160, 168, 170
 Hilbert–Schmidt distance, 234, 241
 Hilbert–Schmidt inner product, 198, 203, 236, 377
 Hilbert–Schmidt norm, 238, 239, 253
 Hilbert space, 2, 3, 90, 352
 Homomorphism, 399
 Householder reflection, 178, *see also* Householder transformation
 Householder transformation, 178, 183

I

Inertial force, 95
 Inertial frame, 94
 Information theory, 323
 Initialization, 91

Inner product, 350, 351
 Invariant subgroup, 277, 401
 Inverse quantum Fourier transform
 quantum Fourier transform, 156
 Irreversible population loss, 218
 Ising exchange interaction, 100, 101
 Isomorphism, 399

J

Joint entropy, 328
 Joint probability distribution, 328
 Josephson inductance, 89

K

Kinetic inductance, 89
 Klein, O., 336, 347
 Klein's inequality, 336, 338, 347, 424
 Klein's trace inequality, 347
 Kolmogorov, A., 244
 Kolmogorov distance, 244, 326
 Kraus elements, 198, 212, 220, 252, 291, 385
 orthogonal Kraus elements, 385
 Kraus maps, 385, *see also* Kraus elements
 Kraus operators, 385, *see also* Kraus elements
 Kraus operator-sum representation, 385, *see also* Kraus representation
 Kraus representation, 197, 203, 385

L

Larmor precession, 93
 Lindblad basis, 224
 Lindblad equation, 217, 223, 228, 381
 Lindblad generator, 217, 218, 220, 225
 Lindblad operators, 217, 218
 Linear algebra, 349
 Linear dependent, 351
 Linearly dependent, 350
 linearly independent, 350
 Linear map, 355
 Linear operator, 355
 Logarithmic negativity, 346
 Logical basis, 3, 282
 Logical operators, 281–283, 290–292, 301

M

Mach–Zender interferometer, 191, 192
 Markov approximation, 217
 Markov assumption, 219
 Maximally entangled state, 29, 86, 194, 206, 207, 255

Maximally mixed state, 332, 336
 Measurement, 33, 91, 197
 Measurement-based quantum computation, 112, 271
 Measurement operators, 26, 216
 Metric, 234
 Mixed state, 7, 12, 13, 19, 210, 363
 Modular exponentiation, 167, 175, 176
 Modular multiplication, 162, 175, 176
 Momentum basis, 167
 Mutual information, 329

N

Newton, Isaac, 1
 Newton's laws of motion, 1
 No-cloning theorem, 22, 50, 132, 257
 Noiseless coding theorem, 331
 Non-Abelian gauge potential, 112
 Non-Abelian geometric phase, 103
 Non-Hermitian Hamiltonian, 217, 228
 Non-inertial effect, 95, 110
 Nonlocality, 7, 129, 130
 Non-negative operator, 363, *seealso* positive semidefinite operator
 Non-selective measurement, 216
 Norm, 235, 352
 Normalizer, 283
 Normal operator, 358, 362, 363
 NOT gate, 99
 Null space, 335

O

Observable, 347
 Octant phase gate, 45, 81, 289
 One-way quantum computation, 112, *seealso* measurement-based quantum computation
 Open quantum system, 189, 196, 379
 Operation time, 93
 Operator-sum representation, 207, 381, 384
 Oracle, 180
 Order-finding algorithm, 175, 177
 order-finding problem, 150, 162, 175
 Orthogonality, 350
 Orthonormal basis, 29, 364

P

Parallel transport, 112
 Partial trace, 13, 199, 207, 210, 388–390
 Partial transposition, 340, 384, 390, 391, 393
 Path ordering, 111

Pauli gates, 34, *seealso* Pauli operators
 Pauli group, 274, 275, 279, 283, 297, 396, 402, 403
 Pauli operators, 34, 85, 91, 125, 133, 274, 275, 278, 283
 Pauli X, 34
 Pauli Y, 37
 Pauli Z, 36
 Period-finding algorithm, 168, 175, 176
 Phase damping, 212, 220
 Phase flip, 37
 Phase-flip correction code, 301
 Phase-flip error, 261–263, 265
 Phase gate, 84
 Planar codes, 309, 314
 Planar exchange interaction, 100, *seealso* XY exchange interaction
 Plaquette defect, 319, 320
 Plaquette operator, 310–315
 Point group, 284
 Polar decomposition, 253, 255, 269, 368, 419
 Position basis, 167
 Positive definite Hermitian product, 351
 Positive definite operator, 363, *seealso* positive operator
 Positive operator, 10, 196, 207, 241, 332, 363, 364, 368, 382, 384, 392
 Positive partial transposition criterion, 340, 346
 Positive semidefinite operator, 199, 363, 364
 Postulates of quantum mechanics, 2
 POVM, 27, 28, 254, 418
 POVM elements, 27, 28
 Principle of complementarity, 191
 Principle of deferred measurement, 157
 Product group, 402
 Projection operator, 208, 387
 Projective measurement, 26
 Pure state, 3, 7, 12, 13, 19, 23
 Purification, 9, 13, 14, 248, 338

Q

Quadrant phase gate, 45, 81, 284, 286–288
 Quantum channel, 197
 Quantum circuit model
 quantum circuit diagram, 33
 Quantum communication, 22
 Quantum computer, 89
 quantum computer architecture, 89
 Quantum decoherence, 197, *seealso* decoherence

Quantum efficiency, 91
 Quantum entanglement, 7, *see also* entanglement
 Quantum entangler circuit, 48, 83
 Quantum entropy, 337, *see also* von Neumann entropy
 Quantum error-correction conditions, 268, 270, 271, 298
 Quantum factorization algorithm, 127, 145, 150, 160, 175, 177
 Quantum Fourier transform, 152, 161, 163, 166, 167
 inverse quantum Fourier transform, 156
 Quantum gate teleportation, 209, 251
 Quantum information theory, 323, 381
 Quantum jump approach, 218, 227
 Quantum jump operators, 217, 222, *see also* Lindblad operators
 Quantum logic gate, 46, 89
 Quantum logic gate operation, 33
 Quantum Markovian dynamics, 217
 Quantum master equation, 223, *see also* Lindblad equation
 Quantum mutual information, 338
 Quantum operation, 190, 196, 207, 216, 239, 252, 270
 Quantum operation formalism, 21
 Quantum oracle, 136, 137, 142, 146, 168, 169, 183, 188
 Quantum parallelism, 136, 142
 Quantum phase estimation, 60, 86, 150, 160, 161, 167, 169, 175, 176
 Quantum register, 40, 49
 Quantum search algorithm, 178
 Quantum state, 2
 Quantum statistical mechanics, 381
 Quantum teleportation, 7, 52, 128, 132, 208, 292
 Qubit, 3, 33, 90
 quantum bit, 33
 Quotient group, 277, 400, 401

R

Rabi oscillation, 95, 110
 Rabi frequency, 95
 Random variable, 324
 Reduced density matrix, 86, *see also* reduced density operator
 Reduced density operator, 337
 Reference space, 206
 Relative entropy, 326
 Relative Shannon entropy, 326, 334, 336

Representation, 353–356, 358
 Resonance, 95
 Rotating frame, 94
 Hamiltonian in the rotating frame, 95
 time-evolution operator in the rotating frame, 95
 Rotating-wave approximation, 99
 Rotation operator, 43, 93

S

Scalable system, 90
 Scalar, 349
 Schmidt decomposition, 5, 339, 370, 372
 Schmidt, E., 370
 Schmidt number, 370, *see also* Schmidt rank
 Schmidt rank, 6, 344, 370
 Selective measurement, 216
 Semiclassical feedback control, 291, *see also* classical feedback control
 Separable state, 5, 370
 Shannon, C. E., 324
 Shannon entropy, 324, 331, 332, 334, 337
 Shor, Peter W., 127
 Shor's algorithm, 127, *see also* quantum factorization algorithm
 Simon's algorithm, 136, 145
 Simon's problem, 145
 Singular-value decomposition, 238, 253, 367–369, 416
 singular values, 238, 253
 Special theory of relativity, 130
 Spectral decomposition, 13, 199, 208, 237, 253, 363, 366
 Spin, 90
 Stabilizer, 272–274, 276, 290, 291, 321
 Stabilizer circuit, 289, 290
 Stabilizer codes, 271, 276, 280, 305
 Stabilizer formalism, 123, 271, 290
 Stabilizer subgroup, 272, *see also* stabilizer
 Standard quantum limit, 26
 Standard tensor-product basis, 369
 State vector, 2
 Statistical ensemble, 7
 Statistical mixture, 373
 Stirling, J., 347, 424
 Stirling's approximation, 347, 424
 Subadditivity, 338, 347
 Superdense coding, 128
 Supermap, 196, 207, 379, 381
 Super-mapping, 379, *see also* supermap
 Superoperator, 217, 373, 379, 384, 393
 Superposition, 257, 268, 349, 350, 355

Support of operator, 335
 Surface codes, 309, 318, 319
 SWAP gate, 54, 55, 77, 99, 125, 128
 $\sqrt{\text{SWAP}}$ gate, 56, 100, 125

T

Target qubit, 47
 Taylor series expansion, 365
 Tensor product, 369, 388
 Tensor-product basis, 5
 Tensor-product space, 5, 28, 369, 372
 Time ordering, 111
 Time-evolution operator, 17
 Toffoli gate, 75, 78, 81, 289
 Topological quantum computation, 112
 Toric codes, 309, 315
 Trace, 197
 Trace distance, 234, 241, 242, 244
 Trace norm, 236, 238, 246, 253, 346
 Translational freedom of Lindblad operators, 218
 Transposition, 384, 393
 matrix transposition, 384, 393
 Triangle inequality, 338, 352
 Two-level unitary transformation, 63, 66, 74, 79
 two-level unitary matrix, 69, 71

U

Uhlmann, A., 248, 249
 Uhlmann's theorem, 248, 249
 Uhlmann's formula, 248, 254
 Uncertainty principle, 22
 Unconditional security, 22
 Unitary freedom, 10
 Unitary freedom in purification, 9, 14
 Unitary freedom of density operator, 10, 14

Unitary freedom of Kraus elements, 204, 218
 Unitary freedom of Lindblad operators, 218, 220
 Unitary group, 34
 Unitary matrix, 34, 357
 Unitary operator, 357, 358, 362
 Unitary representation, 197
 Universal quantum computation, 34, 63, 71, 81
 universal set of quantum logic gates, 79, 91
 Universal set of classical logic gates, 79
 Unstructured search, 178, 180

V

Vector, 350
 orthogonal vectors, 351
 parallel vectors, 351
 Vector space, 350
 Vector space of linear maps, 376
 Vector space of linear operators, 9, 373, 376
 Vertex defect, 319–320
 Vertex operator, 310–311, 314, 315, 320
 von Neumann entropy, 16, 332
 von Neumann, J., 23
 von Neumann measurement, 23, *see also* von Neumann scheme of measurement
 Von Neumann scheme of measurement, 23, 166

W

Wave-particle duality, 2, 191, 349

X

XOR, 50, *see also* exclusive OR
 XY exchange interaction, 100