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 $-x \in \mathbb{F}$.

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

(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 $xv_2 \in \mathcal{V}$.
(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 $v_1, v_2 \in \mathcal{V}$,

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

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

$$(xy)v_2 = x(yv_2) \,. \tag{A.1c}$$

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 quarternions ($\mathbb{H}$). 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 $v_1, \ldots, v_n$ in $\mathcal{V}$ are said to be *linearly dependent* of each other if there exits a solution $z_1, \ldots, z_n \in \mathbb{C}$ to the equation

$$z_1 v_1 + \cdots + z_n v_n = 0 \,. \tag{A.2}$$

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

A.1.2 Hermitian Product

In a vector space, the multiplication of vectors has not be 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

$$|\langle v, w\rangle|^2 \leq \langle v, v\rangle\langle w, w\rangle \tag{A.3}$$

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

$$u := v - w\frac{\langle w, v\rangle}{\langle w, w\rangle}\,. \tag{A.4}$$

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

$$\langle u, u\rangle = \langle v, v\rangle - \frac{\langle v, w\rangle\langle w, v\rangle}{\langle w, w\rangle}\,. \tag{A.5}$$

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

$$v = w\frac{\langle w, v\rangle}{\langle w, w\rangle}\,. \tag{A.6}$$

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

$$\|v\| := \sqrt{\langle v, v\rangle}. \tag{A.7}$$

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*

$$\|v + w\| \le \|v\| + \|w\| \tag{A.8}$$

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,

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

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,

$$\|u - w\| \le \|u - v\| + \|v - w\| \tag{A.10}$$

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 $v_1, \ldots, v_n$, then $v_1, \ldots, v_n$ are said to *span* (or *generate*) the vector space $\mathcal{V}$. The set $\{v_1, \ldots, v_n\} \subset \mathcal{V}$ is called a *basis* of $\mathcal{V}$ if $v_1, \ldots, v_n$ 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) $\{v_1, v_2, \ldots, v_n\}$ spanning $\mathcal{V}$ satisfies

$$\langle v_i, v_j \rangle = \delta_{ij} , \tag{A.11}$$

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 $\mathcal{A} = \{v_1, v_2, \ldots, v_n\}$ and $\mathcal{B} = \{w_1, w_2, \ldots, w_n\}$ 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):

$$w_j = \sum_i v_i U_{ij} , \tag{A.12}$$

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

$$U_{ij} = \langle v_i, w_j \rangle . \tag{A.13}$$

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

A.1.4 Representations

Given a fixed basis $\{v_1, v_2, \ldots, v_n\}$ 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

$$\alpha = v_1\alpha_1 + v_2\alpha_2 + \cdots v_n\alpha_n . \tag{A.14}$$

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

$$\alpha \doteq \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} . \tag{A.15}$$

When the basis $\{v_1, v_2, \ldots, v_n\}$ 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

$$\alpha = \sum_j v_j \langle v_j, \alpha \rangle \tag{A.16}$$

or, equivalently, by the column vector

$$\alpha \doteq \begin{bmatrix} \langle v_1, \alpha \rangle \\ \langle v_2, \alpha \rangle \\ \vdots \\ \langle v_n, \alpha \rangle \end{bmatrix} . \tag{A.17}$$

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

$$\langle \alpha, \beta \rangle = \sum_j \alpha_j^* \beta_j = \begin{bmatrix} \alpha_1^* \; \alpha_2^* \; \cdots \; \alpha_n^* \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} , \tag{A.18}$$

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

$$\alpha \doteq \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \tag{A.19}$$

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

$$\alpha \doteq \begin{bmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{bmatrix} \tag{A.20}$$

in the basis $\left\{ w_j \right\}$. 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

$$\alpha_k' = \langle w_k, \alpha \rangle = \sum_{j=1}^n \langle w_k, v_j \rangle \langle v_j, \alpha \rangle = \sum_k U_{kj} \alpha_j , \tag{A.21}$$

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

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

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)

$$\hat{L} : \mathcal{V} \to \mathcal{W} , \quad v \mapsto \hat{L}v \tag{A.23}$$

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 $\hat{L} : \mathcal{V} \to \mathcal{W}$ 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 $\hat{A} : \mathcal{V} \to \mathcal{W}$ by the associations

$$\hat{A}v_j \mapsto w_j \tag{A.24}$$

and

$$\hat{A}(v_1 z_1 + \cdots v_n z_n) = w_1 z_1 + \cdots w_n z_n \tag{A.25}$$

for all $z_1, \ldots, z_n \in \mathbb{C}$. $\hat{A}$ 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 $v = v_1 z_1 + \cdots v_n z_n \in \mathcal{V}$ with $z_j \in \mathbb{C}$. Note that

$$\hat{B}v = (\hat{B}v_1)z_1 + \cdots + (\hat{B}v_n)z_n = w_1 z_1 + \cdots + w_n z_n = \hat{A}v\,. \tag{A.26}$$

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

A.2.2 Representations

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

$$\hat{L}v_j = \sum_i w_i L_{ij}\,, \tag{A.27}$$

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 $\left\{v_j\right\}$ and $\{w_i\}$. $\hat{L}$ being represented by the matrix L is denoted by

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

When the bases $\left\{v_j\right\}$ 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

$$\hat{L}v_j = \sum_i w_i \langle w_i, \hat{L}v_j\rangle. \tag{A.29}$$

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:

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

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

$$w_j = \hat{U}v_j = \sum_i v_i U_{ij}\,, \tag{A.31}$$

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

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

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

$$L' = U^\dagger L U\,. \tag{A.33}$$

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 $\hat{L} : \mathcal{V} \to \mathcal{W}$ be a linear map. Then, the following statements hold true:*

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

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

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 $\hat{L} : \mathcal{V} \to \mathcal{W}$ be represented by

$$\hat{L} v_j = \sum_i w_i L_{ij} \,. \tag{A.35}$$

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

$$\hat{L}^\dagger w_j = \sum_i v_i L^*_{ji} \,. \tag{A.36}$$

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

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

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*

$$\hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = 1\,. \tag{A.38}$$

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 $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ 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 $j = 1, \ldots, n$.*

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

$$w_j = \hat{U} v_j = \sum_i v_i U_{ij}\,. \tag{A.39}$$

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 $\hat{U} : \mathcal{U} \to \mathcal{V}$ is a linear operator which preserves the Hermitian product. That is, for any $u, u' \in \mathcal{U}$,*

$$\langle \hat{U} u, \hat{U} u' \rangle = \langle u, u' \rangle\,. \tag{A.40}$$

There exists a unitary operator $\hat{V} : \mathcal{V} \to \mathcal{V}$ which extents $\hat{U}$. 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 $\mathbb{C}$, $\mathcal{V}^* := \{\phi : \mathcal{V} \to \mathbb{C}\}$. 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 $\phi_v : \mathcal{V} \to \mathbb{C}$ 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

$$\langle\alpha_i|\alpha_j\rangle = \delta_{ij} \,. \tag{A.41}$$

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

$$|v\rangle = \sum_j \left|\alpha_j\right\rangle v_j \,, \quad v_j \in \mathbb{C} \,. \tag{A.42}$$

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

$$\langle v| = \sum_j v_j^* \left\langle\alpha_j\right| \,. \tag{A.43}$$

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

$$|v\rangle \left\langle v'\right| : |u\rangle \mapsto |v\rangle \left\langle v'|u\right\rangle \tag{A.44}$$

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

$$(|v\rangle \left\langle v'\right|)^\dagger = \left|v'\right\rangle \langle v| \,. \tag{A.45}$$

If one constructs $|\alpha_i\rangle \left\langle\alpha_j\right|$ out of a basis $\left\{\left|\alpha_j\right\rangle\right\}$ 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 $\left\{\left|\alpha_j\right\rangle\right\}$ is *orthonormal*, then a linear operator $\hat{L}$ on $\mathcal{V}$ with the matrix representation L in the same basis is equivalent to

$$\hat{L} = \sum_{ij} |\alpha_i\rangle L_{ij} \left\langle\alpha_j\right| \,, \tag{A.46}$$

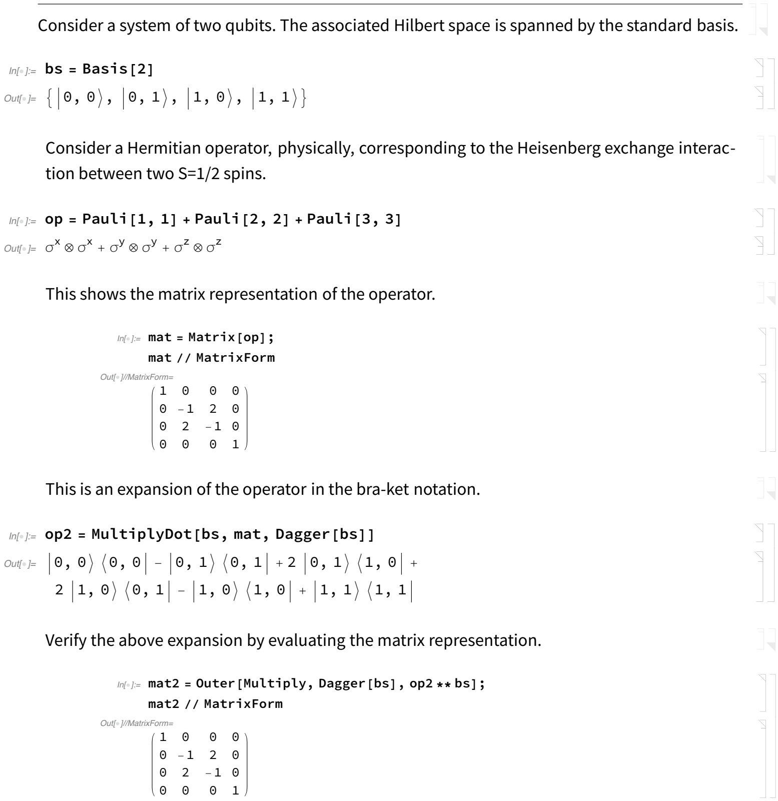
and, accordingly, its Hermitian conjugate $\hat{L}^\dagger$ to

$$\hat{L}^\dagger = \sum_{ij} |\alpha_i\rangle L_{ji}^* \left\langle\alpha_j\right| \,. \tag{A.47}$$

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

$$\hat{I} = \sum_j |\alpha_j\rangle\langle\alpha_j| \tag{A.48}$$

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[◦]= $\sigma^x \otimes \sigma^x + \sigma^y \otimes \sigma^y + \sigma^z \otimes \sigma^z$

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 $\mathcal{V} \to \mathcal{W}$ with an association similar to that in Eq. (A.44). Its Hermitian conjugate, $(|w\rangle\,\langle v|)^\dagger : \mathcal{W} \to \mathcal{V}$, 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 $\hat{L} : \mathcal{V} \to \mathcal{W}$ and examine $\hat{L}\,|\alpha_j\rangle$: Let $\{|\alpha_j\rangle : j = 1, \ldots, m\}$ and $\{|\beta_k\rangle : k = 1, \ldots, n\}$ 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 $\mathcal{W}$, $\hat{L}\left|\alpha_j\right\rangle = \hat{I}_{\mathcal{W}}\hat{L}\left|\alpha_j\right\rangle$. Using the completeness relation (A.48) (replacing $\left|\alpha_j\right\rangle$ with $|\beta_k\rangle$), one can get

$$\hat{L}\left|\alpha_j\right\rangle = \hat{I}_{\mathcal{W}}\hat{L}\left|\alpha_j\right\rangle = \sum_k |\beta_k\rangle\langle\beta_k|\,\hat{L}\left|\alpha_j\right\rangle. \tag{A.49}$$

Noting that $L_{kj} = \langle\beta_k|\,\hat{L}\left|\alpha_j\right\rangle$ 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)]

$$\hat{L}\left|\alpha_j\right\rangle = \sum_k |\beta_k\rangle\, L_{kj} \tag{A.50}$$

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

$$\hat{L} = \sum_{kj} |\beta_k\rangle\, L_{kj}\left\langle\alpha_j\right| . \tag{A.51}$$

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

$$\hat{L}^\dagger = \sum_{kj} \left|\alpha_j\right\rangle L^*_{kj}\,\langle\beta_k| . \tag{A.52}$$

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

$$\hat{A} = \sum_a |a\rangle\, a\, \langle a| \ , \tag{A.53}$$

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

$$\hat{A} = |\psi\rangle\, \langle\psi| \tag{A.54}$$

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

$$\hat{A} := \sum_j |\psi_j\rangle\langle\psi_j| \tag{A.55}$$

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

$$\langle v|\,\hat{A}^\dagger\hat{A}\,|v\rangle = \|\hat{A}\,|v\rangle\,\|^2 \geq 0 \tag{A.56}$$

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

$$\hat{A} = \sum_a |a\rangle\,\langle a|\,, \tag{A.57}$$

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

$$\hat{U} \doteq \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix} \tag{A.58}$$

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

$$|L/R\rangle := \frac{|0\rangle \pm i\,|1\rangle}{\sqrt{2}} \tag{A.59}$$

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

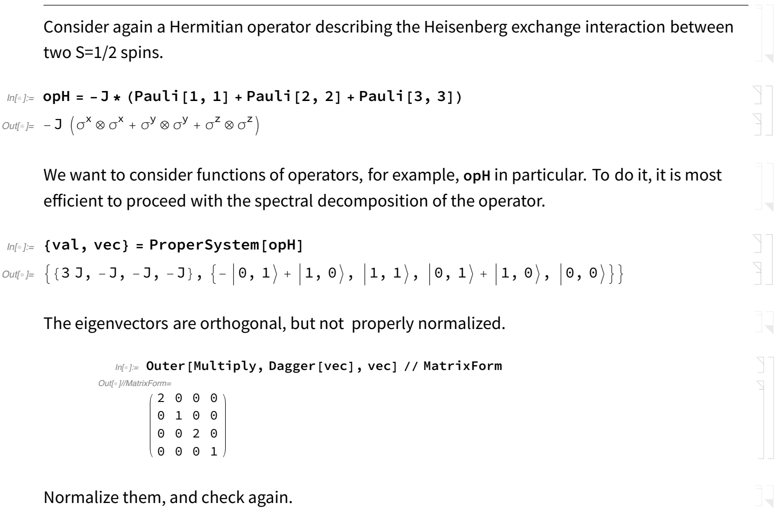
$$\hat{U} = |L\rangle\, e^{-i\phi}\,\langle L| + |R\rangle\, e^{+i\phi}\,\langle R|\,. \tag{A.60}$$

A.4.2 Functions of Operators

The spectral decomposition provides a convenient way to define *functions of a normal operator*. Let $f : \mathcal{D} \to \mathbb{C}$ 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)]

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

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}]
        Outer[Multiply, Dagger[nvec], nvec] // MatrixForm
```

Out[∘]=
$$\left\{\frac{-\left|0,1\right\rangle+\left|1,0\right\rangle}{\sqrt{2}},\ \left|1,1\right\rangle,\ \frac{\left|0,1\right\rangle+\left|1,0\right\rangle}{\sqrt{2}},\ \left|0,0\right\rangle\right\}$$

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[∘]= $e^{i J t\,(\sigma^x\otimes\sigma^x+\sigma^y\otimes\sigma^y+\sigma^z\otimes\sigma^z)}$

This uses the spectral decomposition.

```
In[∘]:= newU = Total@Multiply[nvec, Exp[-I t val], Dagger[nvec]]
```

Out[∘]=
$$e^{i J t}\left|0,0\right\rangle\left\langle 0,0\right| + \frac{1}{2}e^{i J t}\left|0,1\right\rangle\left\langle 0,1\right| + \frac{1}{2}e^{-3 i J t}\left|0,1\right\rangle\left\langle 0,1\right| + \frac{1}{2}e^{i J t}\left|0,1\right\rangle\left\langle 1,0\right| - \frac{1}{2}e^{-3 i J t}\left|0,1\right\rangle\left\langle 1,0\right| + \frac{1}{2}e^{i J t}\left|1,0\right\rangle\left\langle 0,1\right| - \frac{1}{2}e^{-3 i J t}\left|1,0\right\rangle\left\langle 0,1\right| + \frac{1}{2}e^{i J t}\left|1,0\right\rangle\left\langle 1,0\right| + \frac{1}{2}e^{-3 i J t}\left|1,0\right\rangle\left\langle 1,0\right| + e^{i J t}\left|1,1\right\rangle\left\langle 1,1\right|$$

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

```
In[∘]:= newU2 = Elaborate@ExpressionFor@Matrix[newU]
```

Out[∘]=
$$\frac{1}{4}e^{-3 i J t}\left(1+3\,e^{4 i J t}\right)\sigma^0\otimes\sigma^0 + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^x\otimes\sigma^x + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^y\otimes\sigma^y + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^z\otimes\sigma^z$$

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

```
In[∘]:= opU2 = Elaborate@Elaborate[opU]
```

Out[∘]=
$$\frac{1}{4}e^{-3 i J t}\left(1+3\,e^{4 i J t}\right)\sigma^0\otimes\sigma^0 + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^x\otimes\sigma^x + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^y\otimes\sigma^y + \frac{1}{4}e^{-3 i J t}\left(-1+e^{4 i J t}\right)\sigma^z\otimes\sigma^z$$

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*

$$A = USV^{\dagger}\,, \tag{A.62}$$

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

$$S = \begin{bmatrix} s_1 & & \\ & s_2 & \\ & & \ddots \end{bmatrix} \tag{A.63}$$

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,

$$\hat{A} = \sum_{ij} |i\rangle\, A_{ij}\, \langle j| = \sum_{ijk} |i\rangle\, U_{ij} s_j V^{\dagger}_{jk}\, \langle k|\,. \tag{A.64}$$

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

$$\hat{A} = \hat{U}\hat{S}\hat{V}^{\dagger}\,, \tag{A.65}$$

where

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

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

$$\hat{A} = \sum_{j} \left|u_j\right\rangle s_j \left\langle v_j\right|\,, \tag{A.67}$$

where

$$\left|u_j\right\rangle := \sum_{i} |i\rangle\, U_{ij}\,, \quad \left\langle v_j\right| := \sum_{i} |i\rangle\, V_{ij}\,. \tag{A.68}$$

The unitarity of the matrices U and V implies that

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

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

$$A = UP = QV\,, \tag{A.70}$$

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

$$\hat{A} = \hat{U}\hat{P} = \hat{Q}\hat{V}, \tag{A.71}$$

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

$$\hat{A} = \hat{U}'\hat{S}\hat{V}'^\dagger \tag{A.72}$$

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

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

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

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

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

$$\sqrt{\hat{C}} = \sum_c |c\rangle \sqrt{c}\, \langle c|\,. \tag{A.75}$$

Similarly, we rearrange the factors as

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

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.

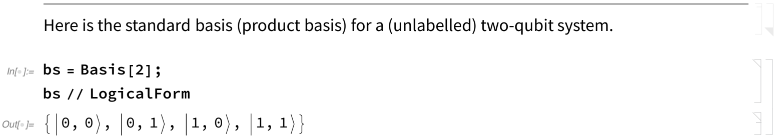
Then the vector space of the total system should be constructed by the vector spaces associated with the individual systems or degrees of freedom. Mathematically, such a construction is called the tensor product of the constituent vector spaces.

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

$$\left\{|v_i\rangle \otimes |w_j\rangle : i = 1, \ldots, \dim \mathcal{V};\;\; j = 1, \ldots, \dim \mathcal{W}\right\} \tag{A.77}$$

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 '⊗' 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

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

Expanded in the standard basis, a vector

$$|\Psi\rangle = \sum_{ij} |v_i\rangle \otimes |w_j\rangle\, \Psi_{ij} \in \mathcal{V} \times \mathcal{W} \tag{A.79}$$

involves $M \times N$ terms in general, where $M := \dim \mathcal{V}$ and $N := \mathcal{W}$. 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)

$$\Psi = U \Sigma V^\dagger, \tag{A.80}$$

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*

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

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

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

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

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

Then it follows from (A.82) that

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

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,

$$\hat{C}\,|v_k w_l\rangle = \sum_{ij} |v_i v_j\rangle\, C_{ij;kl}\,, \tag{A.85}$$

or equivalently,

$$\hat{C} = \sum_{ij;kl} |v_i w_j\rangle \langle v_k w_l|\; C_{ij;kl} = \sum_{ij;kl} |v_i\rangle \langle v_k| \otimes |w_j\rangle \langle w_l|\; C_{ij;kl}\,. \tag{A.86}$$

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

$$G_{ik;jl} = \sum_\mu U_{ik;\mu} \gamma_\mu V^\dagger_{\mu;jl}\,, \quad \gamma_\mu \geq 0. \tag{A.87}$$

Defining

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

leads to the expression

$$\hat{C} = \sum_{\mu} \hat{A}_{\mu} \otimes \hat{B}_{\mu} \gamma_{\mu} \,, \tag{A.89}$$

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 $\min(M^2, N^2)$.

Appendix B
Superoperators

A superoperator is a linear operator acting on a vector space of linear operators. As the concept of vectors is completely general, at a first glance there seems to be no reason why one should reserve a distinctive name for such operators and devote additional discussions. A considerable amount of interest in superoperators came with the booming of quantum information theory in the 1990s when it became clear that superoperators are important in the study of entanglement. Since then, mathematical theories on superoperators have been developed at a notably fast pace and have been applied to a wide range of subjects in quantum computation and quantum information. In this appendix, we briefly survey the properties of superoperators and provide some mathematical tools for the studies of entanglement and decoherence (see Chap. 5).

B.1 Operators as Vectors

The addition of two operators acting on a vector space as well as the multiplication of an operator by a scalar are defined in a natural and straightforward way. That is, operators on a vector space form a vector space themselves. The vector space of operators is not merely a mathematical generalization, but has an important physical relevance. In quantum physics, a mixed state, a statistical mixture of pure quantum states, is described by a so-called density operator.

There is another rather mathematically motivated and yet physically important fact that makes regarding operators as vectors very useful: Any unitary operator $\hat{U}$ can be written in the form $\hat{U} = \exp(i\hat{H})$, where $\hat{H}$ is an Hermitian operator. To describe any physical process, one has to deal with unitary operators. Because of the defining constraint, $\hat{U}^\dagger\hat{U} = \hat{I}$, it is often difficult to directly handle unitary operators. In most case, it is much more convenient and easier to handle Hermitian operators and to consider the exponential function of them. As there is no constraint—apart from the rather trivial Hermiticity condition—for Hermitian operators, it is natural to

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

express them as linear combinations of some basis elements. It makes the handling of physically relevant operators much more tractable.

In this appendix, we will discuss the general structure of the vector space of all linear operators on a vector space. Before we discuss more general vector spaces of linear operators, let us first consider vector spaces of matrices.

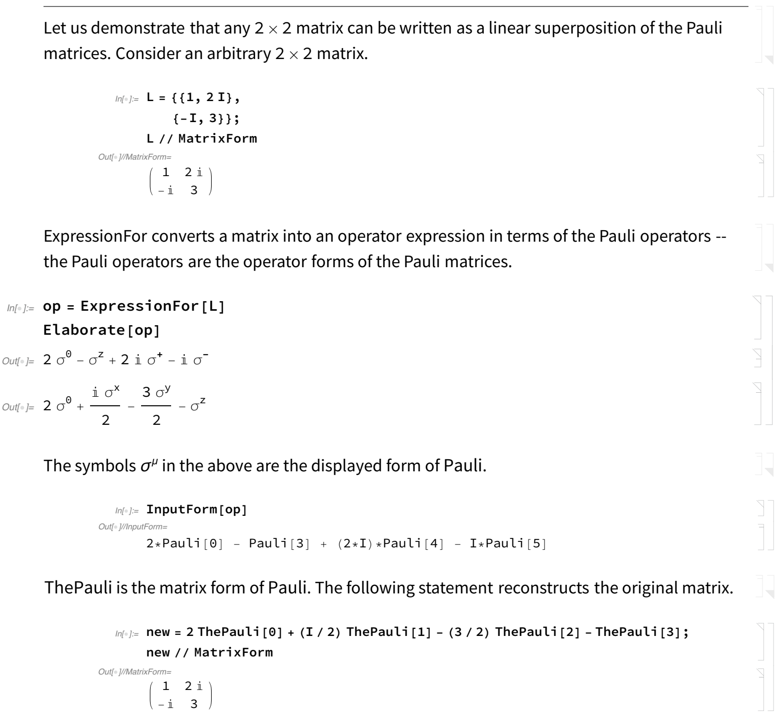
Exercise B.1 (*matrices as vectors*) Consider the set $\mathcal{M}_n$ of all $n \times n$ complex matrices.

(a) Show that $\mathcal{M}_n$ is a vector space.
(b) What is the dimension of $\mathcal{M}_n$.
(c) Define a *Hermitian product* in $\mathcal{M}_n$.
(d) Construct an *orthogonal basis* of $\mathcal{M}_n$.

Here is an even more specific example.

Example B.2 (*Pauli decomposition*) Consider $\mathcal{M}_2$.

(a) Show that the four Pauli matrices $\hat{\sigma}^\mu$ ($\mu = 0, 1, 2, 3$) form an orthogonal basis.
(b) Given an arbitrary matrix $L \in \mathcal{M}_2$, expand it in terms of the Pauli matrices. That is, find the most general form of L in terms of the Pauli matrices.
(c) Find the most general form of a Hermitian matrix $H \in \mathcal{M}_2$.
(d) Find the most general form of a unitary matrix $U \in \mathcal{M}_2$.



Let us demonstrate that any 2×2 matrix can be written as a linear superposition of the Pauli matrices. Consider an arbitrary 2×2 matrix.

```
In[•]:= L = {{1, 2 I},
            {-I, 3}};
        L // MatrixForm
Out[•]//MatrixForm=
```

$$\begin{pmatrix} 1 & 2\,i \\ -i & 3 \end{pmatrix}$$

ExpressionFor converts a matrix into an operator expression in terms of the Pauli operators -- the Pauli operators are the operator forms of the Pauli matrices.

```
In[•]:= op = ExpressionFor[L]
        Elaborate[op]
```

Out[•]= $2\,\sigma^0 - \sigma^z + 2\,i\,\sigma^+ - i\,\sigma^-$

Out[•]= $2\,\sigma^0 + \dfrac{i\,\sigma^x}{2} - \dfrac{3\,\sigma^y}{2} - \sigma^z$

The symbols σ^μ in the above are the displayed form of Pauli.

```
In[•]:= InputForm[op]
Out[•]//InputForm=
        2*Pauli[0] - Pauli[3] + (2*I)*Pauli[4] - I*Pauli[5]
```

ThePauli is the matrix form of Pauli. The following statement reconstructs the original matrix.

```
In[•]:= new = 2 ThePauli[0] + (I / 2) ThePauli[1] - (3 / 2) ThePauli[2] - ThePauli[3];
        new // MatrixForm
Out[•]//MatrixForm=
```

$$\begin{pmatrix} 1 & 2\,i \\ -i & 3 \end{pmatrix}$$

The conversion of Pauli to the corresponding matrix -- ThePauli -- can be achieved by simply using Matrix.

```
In[ ]:= new2 = Matrix[op];
        new2 // MatrixForm
Out[ ]//MatrixForm=
        ( 1   2 i )
        ( -i  3   )
```

Let us analyse the above demonstration in more detail. Here are the Pauli matrices. They form a basis of $\mathcal{M}_2$.

```
In[ ]:= bs = ThePauli /@ {0, 1, 2, 3};
        MatrixForm /@ bs
Out[ ]= {(1 0), (0 1), (0 -i), (1  0)}
         (0 1)  (1 0)  (i  0)   (0 -1)
```

The function PauliDecompose returns the expansion coefficients in the Pauli basis.

```
In[ ]:= cc = PauliDecompose[L]
Out[ ]= {2, i/2, -3/2, -1}
```

Indeed, the coefficients reconstructs the original matrix.

```
In[ ]:= new = cc.bs;
        new // MatrixForm
Out[ ]//MatrixForm=
        ( 1   2 i )
        ( -i  3   )
```

```
In[ ]:= L - new // Chop
Out[ ]= {{0, 0}, {0, 0}}
```

Let us further consider a 2 × 2 Hermitian matrix.

```
In[ ]:= H = RandomHermitian[];
        H // MatrixForm
Out[ ]//MatrixForm=
        (    0.558658 + 0. i       -0.89873 - 0.66087 i )
        ( -0.89873 + 0.66087 i       0.120512 + 0. i    )
```

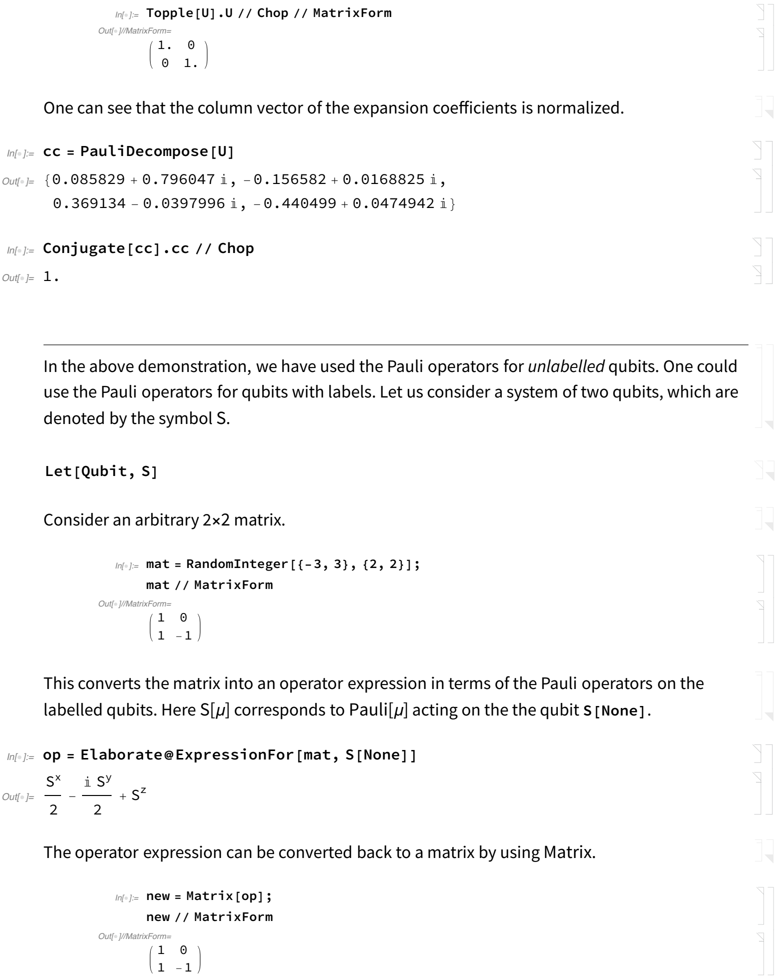
```
In[ ]:= H - Topple[H] // Chop // MatrixForm
Out[ ]//MatrixForm=
        ( 0 0 )
        ( 0 0 )
```

It is noted that the expansion coefficients are all real.

```
In[ ]:= cc = PauliDecompose[H] // Chop
Out[ ]= {0.339585, -0.89873, 0.66087, 0.219073}
```

Finally, consider a 2 × 2 unitary matrix.

```
In[ ]:= U = RandomUnitary[];
        U // MatrixForm
Out[ ]//MatrixForm=
        (  -0.35467 + 0.843542 i   -0.196382 - 0.352251 i )
        ( -0.116783 + 0.386016 i    0.526328 + 0.748553 i )
```



```
In[∘]:= Topple[U].U // Chop // MatrixForm
Out[∘]//MatrixForm=
        ( 1.  0  )
        ( 0   1. )
```

One can see that the column vector of the expansion coefficients is normalized.

```
In[∘]:= cc = PauliDecompose[U]
Out[∘]= {0.085829 + 0.796047 𝕚, -0.156582 + 0.0168825 𝕚,
         0.369134 - 0.0397996 𝕚, -0.440499 + 0.0474942 𝕚}
```

```
In[∘]:= Conjugate[cc].cc // Chop
Out[∘]= 1.
```

In the above demonstration, we have used the Pauli operators for *unlabelled* qubits. One could use the Pauli operators for qubits with labels. Let us consider a system of two qubits, which are denoted by the symbol S.

```
Let[Qubit, S]
```

Consider an arbitrary 2×2 matrix.

```
In[∘]:= mat = RandomInteger[{-3, 3}, {2, 2}];
        mat // MatrixForm
Out[∘]//MatrixForm=
        ( 1   0 )
        ( 1  -1 )
```

This converts the matrix into an operator expression in terms of the Pauli operators on the labelled qubits. Here S[μ] corresponds to Pauli[μ] acting on the the qubit `S[None]`.

```
In[∘]:= op = Elaborate@ExpressionFor[mat, S[None]]
```

$$\text{Out}[\circ]= \frac{S^x}{2} - \frac{\mathbb{i}\, S^y}{2} + S^z$$

The operator expression can be converted back to a matrix by using Matrix.

```
In[∘]:= new = Matrix[op];
        new // MatrixForm
Out[∘]//MatrixForm=
        ( 1   0 )
        ( 1  -1 )
```

Definition B.1 (*vector space of linear maps*) Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces. Let $\mathcal{L}(\mathcal{V}, \mathcal{W})$ be the set of all linear maps $\hat{L} : \mathcal{V} \to \mathcal{W}$. Equip it with a natural multiplication of linear map $\hat{L}$ by scalars $x \in \mathbb{C}$ as

$$(x\hat{L})\,|v\rangle := x(\hat{L}\,|v\rangle) \tag{B.1}$$

for all $|v\rangle \in \mathcal{V}$. Also define the sum of two linear maps by

$$(\hat{L} + \hat{M})\,|v\rangle := \hat{L}\,|v\rangle + \hat{M}\,|v\rangle \tag{B.2}$$

for all $|v\rangle \in \mathcal{V}$. Then the set $\mathcal{L}(\mathcal{V}, \mathcal{W})$ forms a vector space. When $\mathcal{V} = \mathcal{W}$, $\mathcal{L}(\mathcal{V}) := \mathcal{L}(\mathcal{V}, \mathcal{V})$ is the vector space of all linear *operators* on $\mathcal{V}$.

Let $\{|v_1\rangle, \dots, |v_m\rangle\}$ and $\{|w_1\rangle, \dots, |w_n\rangle\}$ be orthonormal bases of $\mathcal{V}$ and $\mathcal{W}$, respectively. A natural choice for basis of $\mathcal{L}(\mathcal{V}, \mathcal{W})$ is

$$\left\{ \left|w_j\right\rangle \langle v_i| : i = 1, \dots, m;\ j = 1, \dots, n \right\}. \tag{B.3}$$

$\mathcal{L}(\mathcal{V}, \mathcal{W})$ also needs a Hermitian product. In the same spirit as the Hilbert-Schmidt inner product[2] of matrices, a natural choice of the Hermitian product in $\mathcal{L}(\mathcal{V}, \mathcal{W})$ inherited from the Hermitian products in $\mathcal{V}$ and $\mathcal{W}$ is that

$$\langle \hat{A}, \hat{B} \rangle := \mathrm{Tr} \hat{A}^\dagger \hat{B} = \sum_j \langle v_j, \hat{A}^\dagger \hat{B} v_j \rangle_{\mathcal{V}} = \sum_j \langle \hat{A} v_j, \hat{B} v_j \rangle_{\mathcal{W}}. \tag{B.4}$$

It is called the *Hilbert-Schmidt inner product* or *Frobenius inner product*. With respect to this Hermitian product, the basis in (B.3) is orthonormal.

For the vector space $\mathcal{L}(\mathcal{V})$ of all *operators* on $\mathcal{V}$, equipped with the Hilbert-Schmidt inner product in (B.4), another choice of basis other than the standard basis (B.3) is widely used. It is to pick the identity operator $\hat{I}$ as an element of the basis. Then every other element in the basis must be *traceless*. For example, let $\mathcal{S}$ be a two-dimensional Hilbert space, and in $\mathcal{L}(\mathcal{S})$ the four Pauli operators form such a basis, $\left\{ \hat{I} \equiv \hat{S}^0, \hat{S}^x, \hat{S}^y, \hat{S}^z \right\}$. Obviously, the non-identity three Pauli operators are traceless, $\mathrm{Tr}\hat{S}^\mu = 0$ for $\mu = x, y, z$. Any operator $\hat{A} \in \mathcal{L}(\mathcal{S})$ is expanded in the four Pauli operators

$$\hat{A} = \hat{S}^0 \alpha_0 + \hat{S}^x \alpha_x + \hat{S}^y \alpha_y + \hat{S}^z \alpha_z \quad (\alpha_\mu \in \mathbb{C}). \tag{B.5}$$

The expansion coefficients can be obtained using the orthogonality of the basis and the Hilbert-Schmidt inner product,

$$\alpha_\mu = \frac{1}{2} \mathrm{Tr} \hat{S}^x \hat{A} \tag{B.6}$$

(recall that the Pauli operators are all Hermitian). We have already observed this fact in Exercise B.2 using the matrix form of the Pauli operators.

Example B.3 Consider the Hilbert space $\mathcal{S} \otimes \mathcal{S}$ associated with a system of two qubits. Show that the products of the Pauli operators

$$\left\{ \hat{S}_1^\mu \otimes \hat{S}_2^\nu \right\} \tag{B.7}$$

form an orthogonal basis of $\mathcal{L}(\mathcal{S} \otimes \mathcal{S})$.

Solution: Consider an arbitrary 4×4 matrix.

[2] In mathematics, it is often called the *Frobenius inner product*.

```
In[∘]:= mat = RandomInteger[{-3, 3}, {4, 4}];
        mat // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} -2 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ 2 & 2 & 0 & 2 \\ -2 & -3 & 0 & -3 \end{pmatrix}$$

This converts the matrix into an operator expression in terms of the products of the Pauli operators, which are represented by `Pauli[μ,ν,...]`.

```
In[∘]:= op = Elaborate@ExpressionFor[mat]
```

Out[∘]=

$$-\frac{5}{4}\,\sigma^0\otimes\sigma^0+\frac{\sigma^0\otimes\sigma^x}{2}+\frac{\sigma^0\otimes\sigma^z}{4}-\frac{3\,\sigma^x\otimes\sigma^0}{4}+\frac{\sigma^x\otimes\sigma^x}{2}+i\,\sigma^x\otimes\sigma^y+\frac{5\,\sigma^x\otimes\sigma^z}{4}-\frac{1}{4}\,i\,\sigma^y\otimes\sigma^0+$$
$$\frac{1}{2}\,i\,\sigma^y\otimes\sigma^x+\sigma^y\otimes\sigma^y-\frac{5}{4}\,i\,\sigma^y\otimes\sigma^z+\frac{\sigma^z\otimes\sigma^0}{4}-\frac{\sigma^z\otimes\sigma^x}{2}-i\,\sigma^z\otimes\sigma^y-\frac{5\,\sigma^z\otimes\sigma^z}{4}$$

This converts the operator expression back into the original matrix.

```
In[∘]:= new = Matrix[op];
        new // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} -2 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ 2 & 2 & 0 & 2 \\ -2 & -3 & 0 & -3 \end{pmatrix}$$

In the above demonstration, we have used the Pauli operators for *unlabelled* qubits. One could use the Pauli operators for qubits with labels. Let us consider a system of two qubits, which are denoted by the symbol S and the flavor indices.

```
Let[Qubit, S]
```

This converts the matrix into an operator expression in terms of the Pauli operators on the labelled qubits. Here S[1,*μ*] corresponds to Pauli[*μ*,0] acting on the first qubit and S[2,*μ*] to Pauli[0,*μ*] on the second qubit.

```
In[∘]:= op = ExpressionFor[mat, S[{1, 2}, None]]
        Elaborate[op]
```

Out[∘]=

$$-\frac{5}{4}-\frac{5}{4}\,S_1^z\,S_2^z-\frac{3}{2}\,S_1^z\,S_2^+ +\frac{1}{2}\,S_1^z\,S_2^- +S_1^+\,S_2^+ +S_1^+\,S_2^- +$$
$$\frac{5}{2}\,S_1^-\,S_2^z+2\,S_1^-\,S_2^+ -2\,S_1^-\,S_2^- +\frac{S_1^z}{4}-S_1^+ -\frac{S_1^-}{2}+\frac{S_2^z}{4}+\frac{S_2^+}{2}+\frac{S_2^-}{2}$$

Out[∘]=

$$-\frac{5}{4}+\frac{1}{2}\,S_1^x\,S_2^x+i\,S_1^x\,S_2^y+\frac{5}{4}\,S_1^x\,S_2^z+\frac{1}{2}\,i\,S_1^y\,S_2^x+S_1^y\,S_2^y-$$
$$\frac{5}{4}\,i\,S_1^y\,S_2^z-\frac{1}{2}\,S_1^z\,S_2^x-i\,S_1^z\,S_2^y-\frac{5}{4}\,S_1^z\,S_2^z-\frac{3\,S_1^x}{4}-\frac{i\,S_1^y}{4}+\frac{S_1^z}{4}+\frac{S_2^x}{2}+\frac{S_2^z}{4}$$

The operator expression can be converted back to a matrix by using Matrix.

```
In[∘]:= new = Matrix[op];
        new // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} -2 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ 2 & 2 & 0 & 2 \\ -2 & -3 & 0 & -3 \end{pmatrix}$$

B.2 Superoperators

As the operators on vector spaces are vectors themselves, one can consider a linear map $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ from operators on $\mathcal{V}$ to those on $\mathcal{W}$. We call it a *supermapping* or *supermap* to distinguish it from one between simple vectors. Physically, supermaps are most relevant when input operators represent mixed states, that is, when they are density operators.

In many cases, the input and output spaces are identical, $\mathcal{V} = \mathcal{W}$. In such a case, $\mathscr{F}$ itself is an operator—an operator on operators—and is called a *superoperator* on $\mathcal{V}$. Superoperators are useful to mathematically describe the evolution of open quantum systems, i.e., systems interacting with other surrounding systems.

B.2.1 Matrix Representation

How can a supermap be characterized? Recall that a linear map of simple vectors is characterized by its matrix representation. Upon a choice of bases $\left\{\left|v_j\right\rangle\right\}$ and $\{|w_i\rangle\}$ of $\mathcal{V}$ and $\mathcal{W}$, respectively, $\hat{L} : \mathcal{V} \to \mathcal{W}$ is completely specified by

$$\hat{L}\left|v_j\right\rangle = \sum_i |w_i\rangle\, L_{ij}\,. \tag{B.8}$$

For a supermap $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$, the involved spaces $\mathcal{L}(\mathcal{V})$ and $\mathcal{L}(\mathcal{W})$ have additional algebraic structures, and there are several ways to characterize it at different levels. One straightforward way to characterize a supermap is to take a plain analogy of the above matrix representation. Recall that $|v_k\rangle\,\langle v_l|$ and $|w_i\rangle\left\langle w_j\right|$ form the standard bases of $\mathcal{L}(\mathcal{V})$ and $\mathcal{L}(\mathcal{W})$, respectively. For each $|v_k\rangle\,\langle v_l|$, $\mathscr{F}(|v_k\rangle\,\langle v_l|)$ belongs to $\mathcal{L}(\mathcal{W})$ and is expanded in the standard basis $\left\{|w_i\rangle\left\langle w_j\right|\right\}$ [see Eq. (B.3)] as (notice the order of indices in $C_{ik;jl}$)

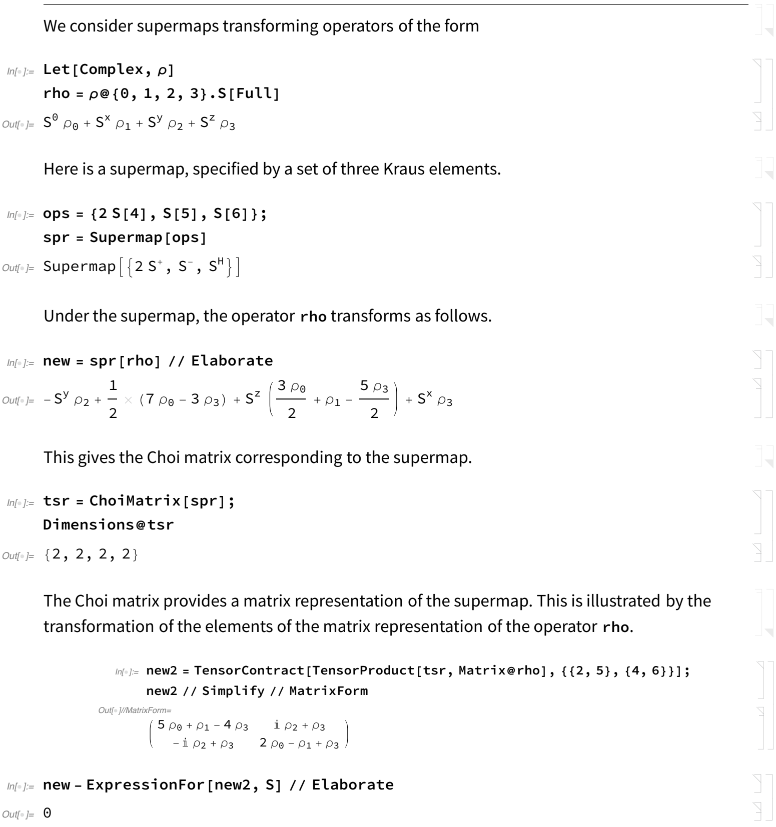
$$\mathscr{F}(|v_k\rangle\,\langle v_l|) = \sum_{ij} |w_i\rangle\left\langle w_j\right| C_{ik;jl}\,, \quad C_{ik;jl} \in \mathbb{C}\,. \tag{B.9}$$

Here the matrix C—regarding (ik) and (jl) as collective indices—is called the *Choi matrix* associated with the supermap $\mathscr{F}$, and it completely characterizes the supermap $\mathscr{F}$. For an arbitrary linear operator $\hat{\rho} := \sum_{kl} |v_k\rangle\,\langle v_l|\,\rho_{kl} \in \mathcal{L}(\mathcal{V})$, its image through $\mathscr{F}$ is given by

$$\hat{\sigma} := \mathscr{F}(\hat{\rho}) = \sum_{kl} \mathscr{F}(|v_k\rangle\,\langle v_l|)\rho_{kl} = \sum_{ij}\sum_{kl} |w_i\rangle\left\langle w_j\right| C_{ik;jl}\,\rho_{kl}\,. \tag{B.10}$$

This implies that the matrix elements (in the standard tensor-product basis) of $\hat{\sigma}$ and $\hat{\rho}$ are related to each other by the Choi matrix as

$$\sigma_{ij} = \sum_{kl} C_{ik;jl}\,\rho_{kl}. \tag{B.11}$$



We consider supermaps transforming operators of the form

```
In[•]:= Let[Complex, ρ]
        rho = ρ@{0, 1, 2, 3}.S[Full]
```

$$\text{Out[•]=}\quad S^{0}\,\rho_0 + S^{x}\,\rho_1 + S^{y}\,\rho_2 + S^{z}\,\rho_3$$

Here is a supermap, specified by a set of three Kraus elements.

```
In[•]:= ops = {2 S[4], S[5], S[6]};
        spr = Supermap[ops]
```

$$\text{Out[•]=}\quad \text{Supermap}\left[\left\{2\,S^{+},\ S^{-},\ S^{H}\right\}\right]$$

Under the supermap, the operator **rho** transforms as follows.

```
In[•]:= new = spr[rho] // Elaborate
```

$$\text{Out[•]=}\quad -S^{y}\,\rho_2 + \frac{1}{2} \times (7\,\rho_0 - 3\,\rho_3) + S^{z}\left(\frac{3\,\rho_0}{2} + \rho_1 - \frac{5\,\rho_3}{2}\right) + S^{x}\,\rho_3$$

This gives the Choi matrix corresponding to the supermap.

```
In[•]:= tsr = ChoiMatrix[spr];
        Dimensions@tsr
Out[•]= {2, 2, 2, 2}
```

The Choi matrix provides a matrix representation of the supermap. This is illustrated by the transformation of the elements of the matrix representation of the operator **rho**.

```
In[•]:= new2 = TensorContract[TensorProduct[tsr, Matrix@rho], {{2, 5}, {4, 6}}];
        new2 // Simplify // MatrixForm
```

$$\text{Out[•]//MatrixForm=}\quad \begin{pmatrix} 5\,\rho_0 + \rho_1 - 4\,\rho_3 & i\,\rho_2 + \rho_3 \\ -i\,\rho_2 + \rho_3 & 2\,\rho_0 - \rho_1 + \rho_3 \end{pmatrix}$$

```
In[•]:= new - ExpressionFor[new2, S] // Elaborate
Out[•]= 0
```

Let us take a few examples: First, consider a supermap of the simplest form

$$\mathscr{F}(\hat{\rho}) = \hat{A}\hat{\rho}\hat{B}^{\dagger}\,, \tag{B.12}$$

where $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{V}, \mathcal{W})$. Then the Choi matrix of $\mathscr{F}$ is given by

$$C_{ij;kl} = A_{ij}\,B^{*}_{kl}\,. \tag{B.13}$$

Next, consider a supermap of the form

$$\mathscr{F}(\hat{\rho}) = -i[\hat{H}, \hat{\rho}]. \tag{B.14}$$

It is the coherent part of the Lindblad equation (see Sect. 5.4). One can use the result in (B.13) putting either $\hat{A} = \hat{I}$ or $\hat{B} = \hat{I}$. It immediately follows that the Choi matrix for the supermap specified in (B.14)

$$C_{ij;kl} = -i(H_{ij}\delta_{kl} - \delta_{ij}H^*_{kl})\,. \tag{B.15}$$

B.2.2 Operator-Sum Representation

Another method to characterize a supermap is the so-called operator-sum representation, and it turns out to be extremely useful in many areas of physics, including quantum information theory and quantum statistical mechanics. Putting the identity $\rho_{kl} = \langle v_k|\hat{\rho}|v_l\rangle$ back into (B.10), one gets

$$\mathscr{F}(\hat{\rho}) = \sum_{ij}\sum_{kl} |w_i\rangle \langle v_k|\hat{\rho}|v_l\rangle \left\langle w_j\right| C_{ik;jl}\,. \tag{B.16}$$

Now identify $\hat{E}_{ik} := |w_i\rangle\langle v_k|$ as a linear map from $\mathcal{V}$ to $\mathcal{W}$, $\hat{E}_{ik} \in \mathcal{L}(\mathcal{V}, \mathcal{W})$. Similarly, $|v_l\rangle\left\langle w_j\right| \in \mathcal{L}(\mathcal{W}, \mathcal{V})$ and it is identical to $\hat{E}^\dagger_{jl}$. Hence

$$\mathscr{F}(\hat{\rho}) = \sum_{ij}\sum_{kl} \hat{E}_{ik}\hat{\rho}\hat{E}^\dagger_{jl}C_{ik;jl}\,. \tag{B.17$'$}$$

With the notation of collective indices $\mu \equiv (ik)$ and $\nu \equiv (jl)$, the supermap $\mathscr{F}$ takes the operator-sum representation

$$\mathscr{F}(\hat{\rho}) = \sum_{\mu=1}^{MN}\sum_{\nu=1}^{MN} \hat{E}_\mu\hat{\rho}\hat{E}^\dagger_\nu C_{\mu\nu}\,, \tag{B.17}$$

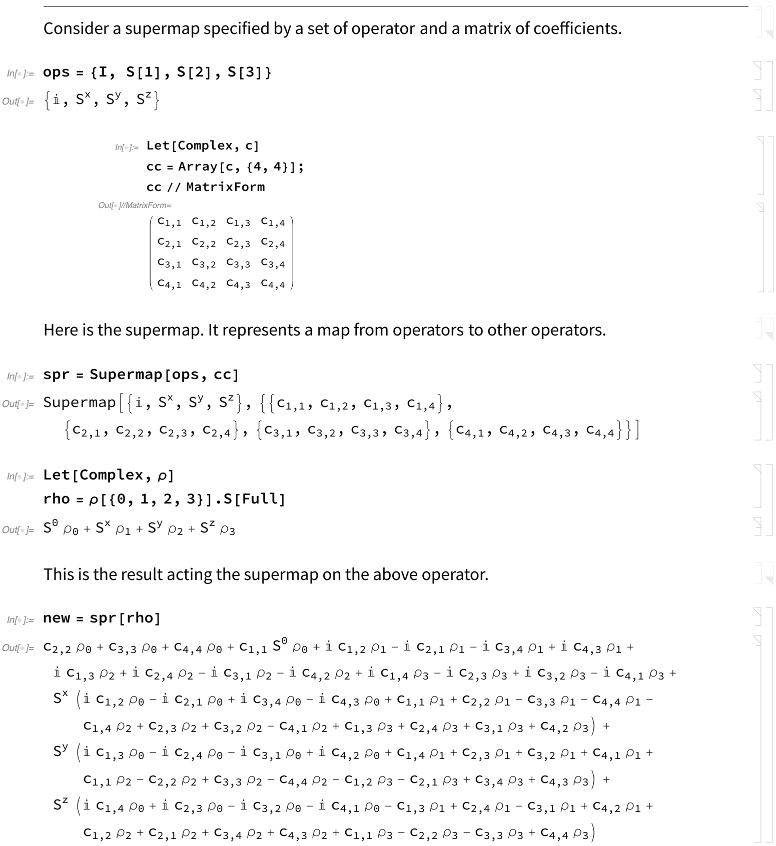
where $M := \dim\mathcal{V}$ and $N := \dim\mathcal{W}$. Diagrammatically, it is depicted as

$$\begin{tikzcd}
\mathcal{V} \arrow[d, "\hat{\rho}"] & \mathcal{W} \arrow[l, "\hat{E}^\dagger_\nu"'] \arrow[d, "\mathscr{F}(\hat{\rho})"] \\
\mathcal{V} \arrow[r, "\hat{E}_\mu"] & \mathcal{W}
\end{tikzcd} \tag{B.18}$$

In Eqs. (B.17) and (B.17$'$), a standard basis $\left\{\hat{E}_\mu\right\}$ has been chosen in $\mathcal{L}(\mathcal{V}, \mathcal{W})$. But one can choose any basis, which leads to the following theorem.

Theorem B.2 *Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces. If $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ is a supermap, then there exist $\hat{F}_\mu \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ such that*

$$\mathscr{F}(\hat{\rho}) = \sum_{\mu=1}^{MN}\sum_{\nu=1}^{MN} \hat{F}_\mu \hat{\rho} \hat{F}_\nu^\dagger \, C_{\mu\nu} \,, \quad C_{\mu\nu} \in \mathbb{C} \,. \tag{B.19}$$



Consider a supermap specified by a set of operator and a matrix of coefficients.

```
In[∘]:= ops = {I, S[1], S[2], S[3]}
```

Out[∘]= $\{\mathbb{i}, S^x, S^y, S^z\}$

```
In[∘]:= Let[Complex, c]
        cc = Array[c, {4, 4}];
        cc // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} \\ c_{3,1} & c_{3,2} & c_{3,3} & c_{3,4} \\ c_{4,1} & c_{4,2} & c_{4,3} & c_{4,4} \end{pmatrix}$$

Here is the supermap. It represents a map from operators to other operators.

```
In[∘]:= spr = Supermap[ops, cc]
```

Out[∘]= $\text{Supermap}\left[\{\mathbb{i}, S^x, S^y, S^z\}, \{\{c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}\}, \{c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}\}, \{c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}\}, \{c_{4,1}, c_{4,2}, c_{4,3}, c_{4,4}\}\}\right]$

```
In[∘]:= Let[Complex, ρ]
        rho = ρ[{0, 1, 2, 3}].S[Full]
```

Out[∘]= $S^0 \rho_0 + S^x \rho_1 + S^y \rho_2 + S^z \rho_3$

This is the result acting the supermap on the above operator.

```
In[∘]:= new = spr[rho]
```

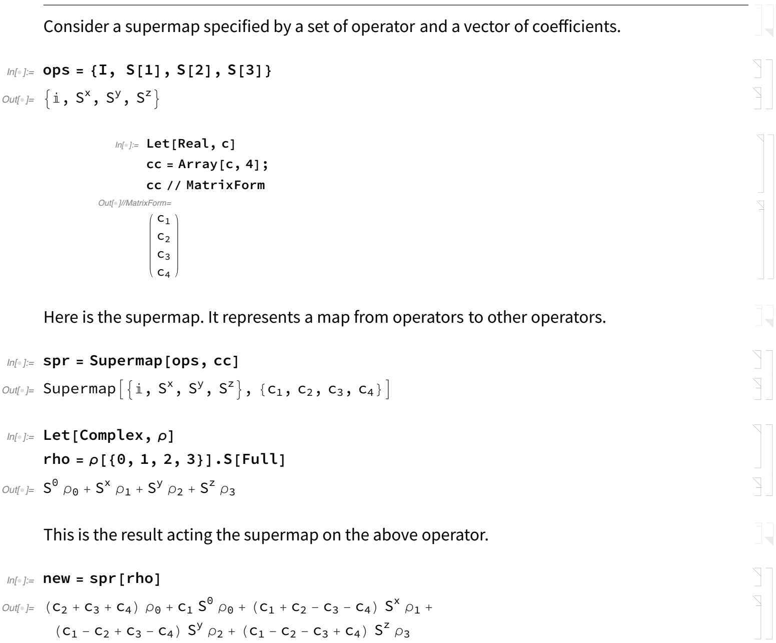
Out[∘]=
$$\begin{aligned}
&c_{2,2}\,\rho_0 + c_{3,3}\,\rho_0 + c_{4,4}\,\rho_0 + c_{1,1}\,S^0\,\rho_0 + \mathbb{i}\,c_{1,2}\,\rho_1 - \mathbb{i}\,c_{2,1}\,\rho_1 - \mathbb{i}\,c_{3,4}\,\rho_1 + \mathbb{i}\,c_{4,3}\,\rho_1 + \\
&\mathbb{i}\,c_{1,3}\,\rho_2 + \mathbb{i}\,c_{2,4}\,\rho_2 - \mathbb{i}\,c_{3,1}\,\rho_2 - \mathbb{i}\,c_{4,2}\,\rho_2 + \mathbb{i}\,c_{1,4}\,\rho_3 - \mathbb{i}\,c_{2,3}\,\rho_3 + \mathbb{i}\,c_{3,2}\,\rho_3 - \mathbb{i}\,c_{4,1}\,\rho_3 + \\
&S^x\,(\mathbb{i}\,c_{1,2}\,\rho_0 - \mathbb{i}\,c_{2,1}\,\rho_0 + \mathbb{i}\,c_{3,4}\,\rho_0 - \mathbb{i}\,c_{4,3}\,\rho_0 + c_{1,1}\,\rho_1 + c_{2,2}\,\rho_1 - c_{3,3}\,\rho_1 - c_{4,4}\,\rho_1 - \\
&\quad c_{1,4}\,\rho_2 + c_{2,3}\,\rho_2 + c_{3,2}\,\rho_2 - c_{4,1}\,\rho_2 + c_{1,3}\,\rho_3 + c_{2,4}\,\rho_3 + c_{3,1}\,\rho_3 + c_{4,2}\,\rho_3) + \\
&S^y\,(\mathbb{i}\,c_{1,3}\,\rho_0 - \mathbb{i}\,c_{2,4}\,\rho_0 - \mathbb{i}\,c_{3,1}\,\rho_0 + \mathbb{i}\,c_{4,2}\,\rho_0 + c_{1,4}\,\rho_1 + c_{2,3}\,\rho_1 + c_{3,2}\,\rho_1 + c_{4,1}\,\rho_1 + \\
&\quad c_{1,1}\,\rho_2 - c_{2,2}\,\rho_2 + c_{3,3}\,\rho_2 - c_{4,4}\,\rho_2 - c_{1,2}\,\rho_3 - c_{2,1}\,\rho_3 + c_{3,4}\,\rho_3 + c_{4,3}\,\rho_3) + \\
&S^z\,(\mathbb{i}\,c_{1,4}\,\rho_0 + \mathbb{i}\,c_{2,3}\,\rho_0 - \mathbb{i}\,c_{3,2}\,\rho_0 - \mathbb{i}\,c_{4,1}\,\rho_0 - c_{1,3}\,\rho_1 + c_{2,4}\,\rho_1 - c_{3,1}\,\rho_1 + c_{4,2}\,\rho_1 + \\
&\quad c_{1,2}\,\rho_2 + c_{2,1}\,\rho_2 + c_{3,4}\,\rho_2 + c_{4,3}\,\rho_2 + c_{1,1}\,\rho_3 - c_{2,2}\,\rho_3 - c_{3,3}\,\rho_3 + c_{4,4}\,\rho_3)
\end{aligned}$$

We are often interested in mapping density operators—not just any operators. In this case, the relevant supermaps are required to preserve the properties of density operators—density operators are *Hermitian* and in particular *positive* (Definition A.19). The condition to preserve Hermiticity simplifies the representation (B.17) further.

Theorem B.3 *Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces, equipped with Hermitian products. Let $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ be a supermap. If $\mathscr{F}(\hat{\rho})$ is Hermitian for every Hermitian $\hat{\rho} \in \mathcal{L}(\mathcal{V})$, then there exist $\hat{F}_\mu \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ such that*

$$\mathscr{F}(\hat{\rho}) = \sum_{\mu=1}^{MN} \epsilon_\mu \hat{F}_\mu \hat{\rho} \hat{F}_\mu^\dagger \,, \tag{B.20}$$

where $\epsilon_\mu = \pm 1$ *and the linear maps* $\hat{F}_\mu$ *are orthogonal to each other,* $Tr\hat{F}_\mu^\dagger \hat{F}_\nu = 0$ *for* $\mu \neq \nu$.



Consider a supermap specified by a set of operator and a vector of coefficients.

```
In[∘]:= ops = {I, S[1], S[2], S[3]}
```

Out[∘]= $\{\mathbb{i}, S^x, S^y, S^z\}$

```
In[∘]:= Let[Real, c]
        cc = Array[c, 4];
        cc // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$$

Here is the supermap. It represents a map from operators to other operators.

```
In[∘]:= spr = Supermap[ops, cc]
```

Out[∘]= $\text{Supermap}\left[\{\mathbb{i}, S^x, S^y, S^z\}, \{c_1, c_2, c_3, c_4\}\right]$

```
In[∘]:= Let[Complex, ρ]
        rho = ρ[{0, 1, 2, 3}].S[Full]
```

Out[∘]= $S^0 \rho_0 + S^x \rho_1 + S^y \rho_2 + S^z \rho_3$

This is the result acting the supermap on the above operator.

```
In[∘]:= new = spr[rho]
```

Out[∘]= $(c_2 + c_3 + c_4)\ \rho_0 + c_1 S^0 \rho_0 + (c_1 + c_2 - c_3 - c_4)\ S^x \rho_1 +$
$(c_1 - c_2 + c_3 - c_4)\ S^y \rho_2 + (c_1 - c_2 - c_3 + c_4)\ S^z \rho_3$

In the representation (B.20), all numerical factors have been absorbed into the operators $\hat{F}_\mu$ leaving only possibly negative signs in ϵ_μ. An immediate question is, what condition should a supermap satisfy to have $\epsilon_\mu = 1$ for all μ? Would the condition to preserve positivity be sufficient to guarantee it? Unfortunately, the positivity-preserving condition does not bring any meaningful simplification, and a much stronger condition is required:

Definition B.4 (*completely positive supermap*) Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces and $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ a supermap. $\mathscr{F}$ is said to be *completely positive* if $\mathscr{F} \otimes \mathscr{I} : \mathcal{L}(\mathcal{V} \otimes \mathcal{E}) \to \mathcal{L}(\mathcal{W} \otimes \mathcal{E})$ is positive[3] for any vector space $\mathcal{E}$, where $\mathscr{I}$ denotes the identity superoperator on $\mathcal{L}(\mathcal{E})$.

Physically, the vector space $\mathcal{E}$ is associated with an environment (Sect. 5.2). $\mathscr{F} \otimes \mathscr{I}$ acts non-trivially only on $\mathcal{V}$ associated with the system but trivially on $\mathcal{E}$. To be physically meaningful, $\mathscr{F} \otimes \mathscr{I}$ is expected preserve the properties, especially positivity, of density operators $\hat{\rho}$ on $\mathcal{V} \otimes \mathcal{E}$. Note that $\hat{\rho}$ may contain a considerable amount of entanglement due to prior interactions between the system and the environment.

[3] Here “positive” actually means “positivity-preserving”.

An important example of a supermap that is *not* completely positive is *transposition*. For an operator $\hat{A} = \sum_{ij} |v_i\rangle A_{ij} \langle v_j|$ on $\mathcal{V}$, the transposition $\hat{A}^T$ of $\hat{A}$ is defined by the matrix transposition of A,

$$\hat{A}^T := \sum_{ij} |v_i\rangle A_{ji} \langle v_j| = \sum_{ij} |i\rangle A^T_{ij} |v_j\rangle . \tag{B.21}$$

The corresponding superoperator $\mathscr{F}$ is thus given by

$$\mathscr{F}(|v_i\rangle \langle v_j|) := |v_j\rangle \langle v_i| . \tag{B.22}$$

Consider an entangled state $|\Phi\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ in $\mathcal{V} \otimes \mathcal{E}$. Clearly,

$$|\Phi\rangle \langle\Phi| = |00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11| \tag{B.23}$$

is positive (Definition A.19). Now let us inspect

$$(\mathscr{F} \otimes \mathscr{I})(|\Phi\rangle \langle\Phi|) = |00\rangle \langle 00| + |10\rangle \langle 01| + |01\rangle \langle 10| + |11\rangle \langle 11| . \tag{B.24}$$

The superoperator $\mathscr{F} \otimes \mathscr{I}$ corresponds to partial transposition (further details to be discussed in Appendix B.4). The matrix representation in the tensor-product basis

$$(\mathscr{F} \otimes \mathscr{I})(|\Phi\rangle \langle\Phi|) \doteq \left[\begin{array}{c|cc|c} 1 & & & \\ \hline & 0 & 1 & \\ & 1 & 0 & \\ \hline & & & 1 \end{array}\right] \tag{B.25}$$

reveals that the resulting operator has an eigenvalue -1 and cannot be positive by Theorem A.20. This concludes that transposition is not a completely positive superoperator.

The operator-sum representation in (B.19) or (B.20) is further simplified for completely positive supermaps. The following example exhibits the motivation.

Exercise B.4 For any linear maps $\hat{F}_\mu \in \mathcal{L}(\mathcal{V}, \mathcal{W})$, the supermap $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ defined by

$$\mathscr{F}(\hat{\rho}) := \sum_\mu \hat{F}_\mu \hat{\rho} \hat{F}_\mu^\dagger \tag{B.26}$$

is completely positive.

Note that the linear maps $\hat{F}_\mu$ in (B.26) are completely arbitrary. They do not have to be orthogonal to each other, $\mathrm{Tr}\hat{F}_\mu^\dagger \hat{F}_\nu \neq 0$, nor to span the space $\mathcal{L}(\mathcal{V}, \mathcal{W})$. The following theorem confirms that any supermap takes the above form in Eq. (B.26). In fact, for a given supermap, one can find a more compact and refined linear maps to represent it with.

Theorem B.5 (Kraus representation theorem) *Let $\mathcal{V}$ and $\mathcal{W}$ be vector spaces, and $\mathscr{F} : \mathcal{L}(\mathcal{V}) \to \mathcal{L}(\mathcal{W})$ be a supermap. Then the following statement are equivalent:*

(a) $\mathscr{F}$ is completely positive.

(b) For any $\hat{\rho} \in \mathcal{L}(\mathcal{V})$, the effect $\mathscr{F}(\hat{\rho})$ can be written as

$$\mathscr{F}(\hat{\rho}) = \sum_{\mu=0}^{m-1} \hat{F}_\mu \hat{\rho} \hat{F}_\mu^\dagger\,, \tag{B.27}$$

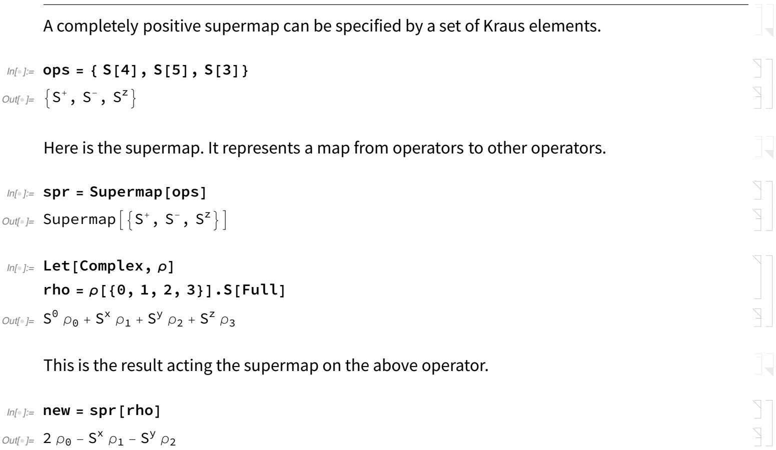
where $m \leq (\dim \mathcal{V})(\dim \mathcal{W})$ and $\hat{F}_\mu : \mathcal{V} \to \mathcal{W}$ are mutually orthogonal *linear maps—$\mathrm{Tr}\hat{F}_\mu^\dagger \hat{F}_\nu = 0$ for all $\mu \neq \nu$.*

(c) For any $\hat{\rho} \in \mathcal{L}(\mathcal{V})$, the effect $\mathscr{F}(\hat{\rho})$ can be written as a finite sum of the form

$$\mathscr{F}(\hat{\rho}) = \sum_{\mu} \hat{F}_\mu \hat{\rho} \hat{F}_\mu^\dagger\,, \tag{B.28}$$

where $\hat{F}_\mu : \mathcal{V} \to \mathcal{W}$ are (arbitrary) linear maps.

The expressions (B.27) and (B.28) are called the *Kraus operator-sum representation* or simply the *Kraus representation* of the completely positive supermap $\mathscr{F}$. The linear maps $\hat{F}_\mu$ are called the *Kraus elements* or the *Kraus maps* (the *Kraus operators* when $\mathcal{V} = \mathcal{W}$). The *orthogonal* Kraus elements in Eq. (B.27) are optimal in the sense that the sum has the least possible number of terms.



A completely positive supermap can be specified by a set of Kraus elements.

```
In[ ]:= ops = { S[4], S[5], S[3]}
```

Out[ ]= $\{S^{+}, S^{-}, S^{z}\}$

Here is the supermap. It represents a map from operators to other operators.

```
In[ ]:= spr = Supermap[ops]
```

Out[ ]= $\mathrm{Supermap}[\{S^{+}, S^{-}, S^{z}\}]$

```
In[ ]:= Let[Complex, ρ]
        rho = ρ[{0, 1, 2, 3}].S[Full]
```

Out[ ]= $S^{0}\rho_0 + S^{x}\rho_1 + S^{y}\rho_2 + S^{z}\rho_3$

This is the result acting the supermap on the above operator.

```
In[ ]:= new = spr[rho]
```

Out[ ]= $2\rho_0 - S^{x}\rho_1 - S^{y}\rho_2$

It is fairly obvious that a supermap expressed in the form (B.27) or (B.28) is completely positive. One can prove the converse starting from (B.17′).

Exercise B.5 Using the representation in (B.17′) and requiring the positivity of $(\mathscr{F} \otimes \mathscr{I})(|\Phi\rangle \langle\Phi|)$ with

$$|\Phi\rangle := \sum_j \left|v_j\right\rangle \otimes \left|v_j\right\rangle \in \mathcal{V} \otimes \mathcal{V}, \tag{B.29}$$

prove that a completely positive map has the Kraus representation of the form (B.27).

B.2.3 Choi Isomorphism

A less widely known yet intriguing method to characterize a supermap is provided by the *Choi isomorphism* (also known as Jamiolkowski, Choi-Jamiolkowski or Jamiolkowski-Choi isomorphism).[4]

Before we discuss the Choi isomorphism of supermaps, let us first examine the same isomorphism of linear maps. Let $\hat{A} : \mathcal{V} \to \mathcal{W}$ be a linear map. Recall that it is completely characterized by the $n \times m$ matrix A such that

$$\hat{A} = \sum_{kj} |w_k\rangle \, A_{kj} \left\langle v_j \right| , \tag{B.30}$$

where $\left\{v_j\right\}$ and $|w_k\rangle$ are bases of $\mathcal{V}$ and $\mathcal{W}$, respectively. Now note that the same matrix defines a vector

$$|A\rangle := \sum_{kj} |w_k\rangle \otimes \left|v_j\right\rangle A_{kj} \tag{B.31}$$

in the tensor-product space $\mathcal{W} \otimes \mathcal{V}$. The correspondence $\hat{A} \leftrightarrow |A\rangle$ turns out to be an isomorphism between $\mathcal{L}(\mathcal{V}, \mathcal{W})$ and $\mathcal{W} \otimes \mathcal{V}$. The isomorphism is called the Choi isomorphism and $|A\rangle$ is called the *Choi vector* associated with the linear map $\hat{A}$. Looking almost trivial at a first glance, the isomorphism brings about several interesting things. To see it, consider a maximally entangled state

$$|\Phi\rangle := \sum_k |v_k\rangle \otimes |v_k\rangle \in \mathcal{V} \otimes \mathcal{V} . \tag{B.32}$$

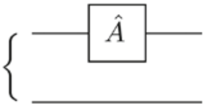
in the tensor-product space $\mathcal{V} \otimes \mathcal{V}$. First, observe that the Choi vector $|A\rangle$ of a linear map $\hat{A}$ is given by

$$|A\rangle = (\hat{A} \otimes \hat{I}) \, |\Phi\rangle \ . \tag{B.33}$$

This is depicted in the following quantum circuit

[4] There are subtle but important differences between the Choi and Jamiolkowski isomorphism; see Jiang et al. (2013).

$$|A\rangle = |\Phi\rangle$$



(B.34)

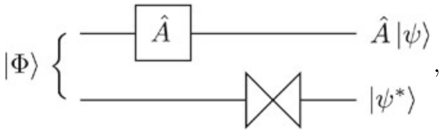
The isomorphism preserves the Hermitian products in $\mathcal{L}(\mathcal{V}, \mathcal{W})$ and $\mathcal{W} \otimes \mathcal{V}$, that is, $\langle \hat{A}, \hat{B} \rangle = \mathrm{Tr}\hat{A}^\dagger \hat{B} = \langle A|B \rangle$ for all linear maps $\hat{A}$ and $\hat{B}$. Furthermore, for an arbitrary state $|\psi\rangle = \sum_j \left|v_j\right\rangle \psi_j \in \mathcal{V}$, define its conjugate state by

$$\left|\psi^*\right\rangle := \sum_j \left|v_j\right\rangle \psi_j^* . \tag{B.35}$$

Then, it follows that

$$\hat{A}\,|\psi\rangle = \left\langle\psi^*\right| (\hat{A} \otimes \hat{I})\,|\Phi\rangle = \langle \psi^* | A \rangle\,, \tag{B.36}$$

where the Hermitian product on the right-hand side is applied partially and only on $\mathcal{V}$, and the remaining part is a vector belonging to $\mathcal{W}$. In quantum circuit model, it is depicted as



(B.37)

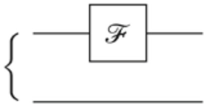
where the quantum circuit element —⋈— represents the projection onto the state specified at the output port. Interestingly, the result is not affected whether the projection onto $|\psi^*\rangle$ is made before or after the operation $\hat{A}$. This does not violate any physical principle as the two parts in $\mathcal{V} \otimes \mathcal{V}$ are separated spacelike.

Now let us turn to the Choi isomorphism between supermaps and operators: Consider again the maximally entangled state in Eq. (B.32) and operate an extended supermap $\mathscr{F} \otimes \mathcal{I} : \mathcal{L}(\mathcal{V} \otimes \mathcal{V}) \to \mathcal{L}(\mathcal{W} \otimes \mathcal{V})$ on $|\Phi\rangle\,\langle\Phi|$ to get

$$\begin{aligned} \hat{C}_{\mathscr{F}} := (\mathscr{F} \otimes \mathscr{I})(|\Phi\rangle\,\langle\Phi|) = \sum_{kl} \mathscr{F}(|v_k\rangle\,\langle v_l|) \otimes |v_k\rangle\,\langle v_l| \\ = \sum_{ij} \sum_{kl} |w_i v_k\rangle \left\langle w_j v_l\right| C_{ik;jl}\,, \end{aligned} \tag{B.38}$$

where C is the Choi matrix of $\mathscr{F}$; see Eq. (B.9). In quantum circuit model, it reads as

$$\hat{C}_{\mathscr{F}} = |\Phi\rangle$$



(B.39)

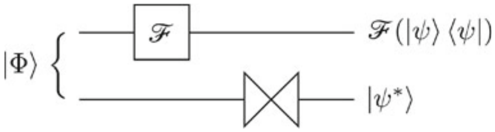
Clearly $\hat{C}_{\mathscr{F}}$ is an operator (not a superoperator) on $\mathcal{W} \otimes \mathcal{V}$ and the Choi matrix C is nothing but its matrix representation in the standard tensor-product basis. Hence $\hat{C}_{\mathscr{F}}$ is called the *Choi operator* associated with $\mathscr{F}$. It turns out that the correspondence $\mathscr{F} \leftrightarrow \hat{C}_{\mathscr{F}}$ by means of (B.38) is one-to-one and an isomorphism.[5] For any state $|\psi\rangle \in \mathcal{V}$, the effect $\mathscr{F}(|\psi\rangle\langle\psi|)$ of supermap $\mathscr{F}$ on the pure state can be obtained by means of the conjugate state $|\psi^*\rangle$ [see Eq. (B.35)] as

$$\mathscr{F}(|\psi\rangle\langle\psi|) = \left\langle\psi^*\right| \hat{C}_{\mathscr{F}} \left|\psi^*\right\rangle , \tag{B.40}$$

or, more generally, for any $\hat{\rho} = \sum_{ij} |v_i\rangle \left\langle v_j\right| \rho_{ij}$

$$\mathscr{F}(\hat{\rho}) = \mathrm{Tr}_{\mathcal{V}} \hat{\rho}^* \hat{C}_{\mathscr{F}} , \tag{B.41}$$

where $\hat{\rho}^* := \sum_{ij} |v_i\rangle \left\langle v_j\right| \rho^*_{ij}$. This has been depicted in the quantum circuit



(B.42)

Furthermore, taking the matrix representation of each entity in the relation (B.41) confirms the linear transformation rule (B.11) between the matrix elements of $\hat{\rho}$ and $\hat{\sigma} := \mathscr{F}(\hat{\rho})$ The transformation rule in (B.11) is another illustration of the Choi isomorphism.

The Choi operator plays a key role in the *gate teleportation* protocol, and it provides an interesting proof of the Kraus-representation theorem (see Sect. 5.2).

B.3 Partial Trace

The tensor product (Appendix A.6) extends vectors and operators. A partial trace is effectively an inverse procedure and reduces operators on a tensor-product space to one of the component spaces.

Consider an operator $\hat{T}$ on a tensor product space $\mathcal{V} \otimes \mathcal{W}$. The *partial trace* over the space $\mathcal{W}$ is defined by

$$\mathop{\mathrm{Tr}}_{\mathcal{W}} \hat{T} := \sum_{ijk} |v_i\rangle \left\langle v_i w_j\right| \hat{T} \left|v_k w_j\right\rangle \langle v_k| , \tag{B.43}$$

[5] Here we have just defined an association $\mathscr{F} \mapsto \hat{C}_{\mathscr{F}}$. Given an operator $\hat{C} \in \mathcal{L}(\mathcal{W} \otimes \mathcal{V})$, one can also find the corresponding supermap $\mathscr{F}_{\hat{C}}$, that is, the association $\hat{C} \to \mathscr{F}_{\hat{C}}$ in the reverse direction; see Størmer (2013).

where $\{|v_i\rangle\}$ and $\left\{\left|w_j\right\rangle\right\}$ are given bases of $\mathcal{V}$ and $\mathcal{W}$, respectively. The partial trace over $\mathcal{V}$ is defined analogously. The procedure is said to *trace out* the vector space $\mathcal{W}$, and the resulting operator is called a *reduced operator* of $\hat{T}$. The reduced operator acts on $\mathcal{V}$. Often Eq. (B.43) is casually written as

$$\operatorname*{Tr}_{\mathcal{W}} \hat{T} = \sum_j \left\langle w_j \right| \hat{T} \left| w_j \right\rangle . \tag{B.44}$$

It should be understood that on the right-hand side, the Hermitian product is applied partially and only on $\mathcal{W}$. The expression remains to be an operator on $\mathcal{V}$, rather than a complex number.

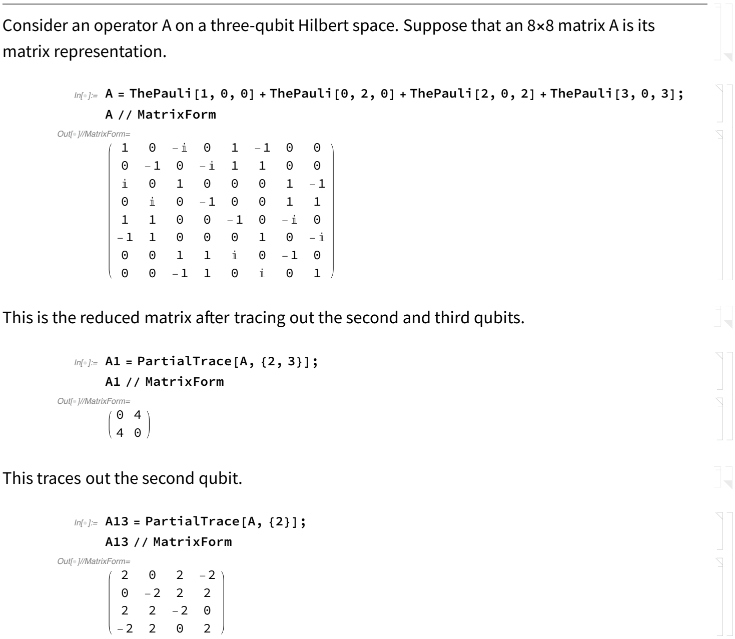
Given the matrix representation $T_{ij;kl}$ of $\hat{T}$ in the tensor-product basis

$$\hat{T} \left| v_k w_l \right\rangle = \sum_{ij} \left| v_i w_j \right\rangle T_{ij;kl} , \tag{B.45}$$

one can obtain the matrix representation of the reduced operator $\hat{A} := \mathrm{Tr}_{\mathcal{W}} \hat{T}$ in the basis $\{|v_i\rangle\}$ by

$$A_{ik} = \sum_j T_{ij;kj} . \tag{B.46}$$

Although we have defined partial trace in a chosen basis, it does not depend on the basis.



Consider an operator A on a three-qubit Hilbert space. Suppose that an 8×8 matrix A is its matrix representation.

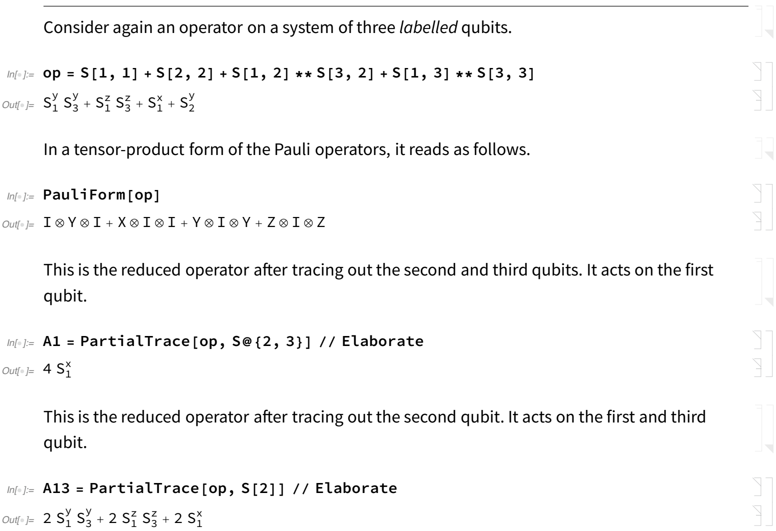
```
In[•]:= A = ThePauli[1, 0, 0] + ThePauli[0, 2, 0] + ThePauli[2, 0, 2] + ThePauli[3, 0, 3];
        A // MatrixForm
Out[•]//MatrixForm=
         1   0  -i   0   1  -1   0   0
         0  -1   0  -i   1   1   0   0
         i   0   1   0   0   0   1  -1
         0   i   0  -1   0   0   1   1
         1   1   0   0  -1   0  -i   0
        -1   1   0   0   0   1   0  -i
         0   0   1   1   i   0  -1   0
         0   0  -1   1   0   i   0   1
```

This is the reduced matrix after tracing out the second and third qubits.

```
In[•]:= A1 = PartialTrace[A, {2, 3}];
        A1 // MatrixForm
Out[•]//MatrixForm=
        0  4
        4  0
```

This traces out the second qubit.

```
In[•]:= A13 = PartialTrace[A, {2}];
        A13 // MatrixForm
Out[•]//MatrixForm=
         2   0   2  -2
         0  -2   2   2
         2   2  -2   0
        -2   2   0   2
```



Consider again an operator on a system of three *labelled* qubits.

```
In[∘]:= op = S[1, 1] + S[2, 2] + S[1, 2] ** S[3, 2] + S[1, 3] ** S[3, 3]
```

Out[∘]= $S_1^y S_3^y + S_1^z S_3^z + S_1^x + S_2^y$

In a tensor-product form of the Pauli operators, it reads as follows.

```
In[∘]:= PauliForm[op]
```

Out[∘]= $I \otimes Y \otimes I + X \otimes I \otimes I + Y \otimes I \otimes Y + Z \otimes I \otimes Z$

This is the reduced operator after tracing out the second and third qubits. It acts on the first qubit.

```
In[∘]:= A1 = PartialTrace[op, S@{2, 3}] // Elaborate
```

Out[∘]= $4\, S_1^x$

This is the reduced operator after tracing out the second qubit. It acts on the first and third qubit.

```
In[∘]:= A13 = PartialTrace[op, S[2]] // Elaborate
```

Out[∘]= $2\, S_1^y S_3^y + 2\, S_1^z S_3^z + 2\, S_1^x$

Partial trace is a *completely positive* supermap (Definition B.4). By Theorem B.5, one can prove it simply by constructing an operator-sum representation. In accordance with the definition of the partial trace in (B.43), we define Kraus elements

$$\hat{F}_j := \sum_i |v_i\rangle \langle v_i w_j| \,. \tag{B.47}$$

Then it follows that

$$\operatorname*{Tr}_{\mathcal{W}} \hat{T} = \sum_j \hat{F}_j \hat{T} \hat{F}_j^\dagger . \tag{B.48}$$

B.4 Partial Transposition

We conclude this appendix with a rather unusual mathematical tool—the *partial transposition*. As the name suggests, it applies the matrix transposition to the part of the matrix representation of an operator that corresponds to a certain subsystem. The resulting matrix gives a new operator associated with it. Roughly speaking,[6] the partial transformation would correspond to a time-reversal transformation only on the subsystem.

Partial transposition has attracted considerable attention thanks to the seminal work on the separability test of mixed states of a composite quantum system by Peres (1996) and Horodecki et al. (1996). Ever since then, it has been widely used

[6] Rigorously speaking, this statement is wrong because no anti-unitary transformation such as time reversal can be applied on a subpart of the system.

to study the structure of the tensor-product space of composite systems concerning various entanglement properties.

Consider an operator $\hat{A}$ on a tensor product space $\mathcal{V} \otimes \mathcal{W}$ with the matrix representation

$$\hat{A} = \sum_{ij;kl} \left|v_i w_j\right\rangle \langle v_k w_l| \, A_{ij;kl} \tag{B.49}$$

in the standard tensor-product basis, $\left\{\left|v_i w_j\right\rangle \equiv |v_i\rangle \otimes \left|w_j\right\rangle\right\}$. The *partial transposition* $\hat{A}^{T_\mathcal{V}}$ of $\hat{A}$ with respect to the subspace $\mathcal{V}$ is defined by

$$\hat{A}^{T_\mathcal{V}} := \sum_{ij;kl} \left|v_i w_j\right\rangle \langle v_k w_l| \, A_{kj;il} \,. \tag{B.50}$$

Equivalently, we define

$$\left\langle v_i w_j\right| \hat{A}^{T_\mathcal{V}} \left|v_k w_l\right\rangle = \left\langle v_k w_j\right| \hat{A} \left|v_i w_l\right\rangle . \tag{B.51}$$

The partial transposition with respect to $\mathcal{W}$ is defined analogously. In a fixed basis, partial transposition is defined entirely by the matrix representations. For the above case,

$$A^{T_\mathcal{V}}_{ij;kl} = A_{kj;il} \,. \tag{B.52}$$

For example, consider a linear operator on two qubits with the matrix representation

$$\hat{A} \doteq \left[\begin{array}{cc|cc} A_{0,0;0,0} & A_{0,0;0,1} & A_{0,0;1,0} & A_{0,0;1,1} \\ A_{0,1;0,0} & A_{0,1;0,1} & A_{0,1;1,0} & A_{0,1;1,1} \\ \hline A_{1,0;0,0} & A_{1,0;0,1} & A_{1,0;1,0} & A_{1,0;1,1} \\ A_{1,1;0,0} & A_{1,1;0,1} & A_{1,1;1,0} & A_{1,1;1,1} \end{array}\right] . \tag{B.53}$$

we have

$$\hat{A}^{T_\mathcal{V}} \doteq \left[\begin{array}{cc|cc} A_{0,0;0,0} & A_{0,0;0,1} & A_{1,0;0,0} & A_{1,0;0,1} \\ A_{0,1;0,0} & A_{0,1;0,1} & A_{1,1;0,0} & A_{1,1;0,1} \\ \hline A_{0,0;1,0} & A_{0,0;1,1} & A_{1,0;1,0} & A_{1,0;1,1} \\ A_{0,1;1,0} & A_{0,1;1,1} & A_{1,1;1,0} & A_{1,1;1,1} \end{array}\right] \tag{B.54}$$

$$\hat{A}^{T_\mathcal{W}} \doteq \left[\begin{array}{cc|cc} A_{0,0;0,0} & A_{0,1;0,0} & A_{0,0;1,0} & A_{0,1;1,0} \\ A_{0,0;0,1} & A_{0,1;0,1} & A_{0,0;1,1} & A_{0,1;1,1} \\ \hline A_{1,0;0,0} & A_{1,1;0,0} & A_{1,0;1,0} & A_{1,1;1,0} \\ A_{1,0;0,1} & A_{1,1;0,1} & A_{1,0;1,1} & A_{1,1;1,1} \end{array}\right] . \tag{B.55}$$

It is important to remember that the partial transposition is basis-dependent.

Consider an operator on two qubits.

```
In[∘]:= op = S[1, 1] ** S[2, 2] + 3 I S[1, 2] ** S[2, 3]
```

Out[∘]= $S_1^x S_2^y + 3\,i\, S_1^y S_2^z$

Here is the partial transpose with respect to the second qubit.

```
In[∘]:= new = PartialTranspose[op, S[2]] // Elaborate
```

Out[∘]= $-S_1^x S_2^y + 3\,i\, S_1^y S_2^z$

Here is the partial transposition with respect to the both qubits.

```
In[∘]:= new = PartialTranspose[op, S@{1, 2}] // Elaborate
```

Out[∘]= $-S_1^x S_2^y - 3\,i\, S_1^y S_2^z$

It must coincide with the (overall) transposition. It is indeed the case as one can see below.

```
In[∘]:= ExpressionFor[Transpose@Matrix[op], S@{1, 2}] // Elaborate
```

Out[∘]= $-S_1^x S_2^y - 3\,i\, S_1^y S_2^z$

Consider again the above demonstration, now in terms of matrix representations.

```
In[∘]:= mat = ThePauli[1, 2] + 3 * I * ThePauli[2, 3];
        mat // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} 0 & 0 & 3 & -i \\ 0 & 0 & i & -3 \\ -3 & -i & 0 & 0 \\ i & 3 & 0 & 0 \end{pmatrix}$$

Here is the partial transpose with respect to the second qubit.

```
In[∘]:= new = PartialTranspose[mat, {2}];
        new // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} 0 & 0 & 3 & i \\ 0 & 0 & -i & -3 \\ -3 & i & 0 & 0 \\ -i & 3 & 0 & 0 \end{pmatrix}$$

Here is the partial transposition with respect to the both qubits. It must coincide with the (overall) transposition. It is indeed the case as one can see below.

```
In[∘]:= new = PartialTranspose[mat, {1, 2}];
        new // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} 0 & 0 & -3 & i \\ 0 & 0 & -i & 3 \\ 3 & i & 0 & 0 \\ -i & -3 & 0 & 0 \end{pmatrix}$$

A noteworthy property of partial transposition is that the partial transposition of a positive operator is not always positive (Definition A.19). For example, consider an entangled state $|\Phi\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ in $\mathcal{V} \otimes \mathcal{W}$, and an associate operator

$$\hat{A} := |\Psi\rangle \langle\Psi| = |00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11| \,. \tag{B.56}$$

Clearly, $\hat{A}$ is positive [see Eqs. (A.54) and (A.55)]. However, the partial transposition $\hat{A}^{T_\mathcal{V}}$

$$\hat{A}^{T_\mathcal{V}} = |00\rangle \langle 00| + |10\rangle \langle 01| + |01\rangle \langle 10| + |11\rangle \langle 11| \tag{B.57}$$

has a negative eigenvalue -1 as one can see from the matrix representation

$$\hat{A}^{T_\mathcal{V}} \doteq \left[\begin{array}{c|cc|c} 1 & & & \\ \hline & 0 & 1 & \\ & 1 & 0 & \\ \hline & & & 1 \end{array}\right]. \tag{B.58}$$

By Theorem A.20, $\hat{A}^{T_\mathcal{V}}$ cannot be positive. On the other hand, the partial transposition preserves the positivity of any operator of the form

$$\hat{A} = \sum_j p_j \hat{\rho}_j \otimes \hat{\sigma}_j \,, \tag{B.59}$$

where where $\hat{\rho}_j$ and $\hat{\sigma}_j$ are positive operators on $\mathcal{V}$ and $\mathcal{W}$, respectively, and p_j are non-negative. The operator in (B.59) is a convex linear superposition of products of positive operators. Such operators represent *separable* mixed states (Sect. 1.1.2). Consequently, partial transposition provides a convenient necessary condition for separability of mixed states. Unfortunately, the condition is not a sufficient condition for the separability. In other words, the partial transpositions of some entangled states are positive.

Partial transposition naturally arises when one regards transposition as a supermap. For an operator $\hat{A} = \sum_{ij} |v_i\rangle\, A_{ij} \langle v_j|$ on $\mathcal{V}$, the transposition $\hat{A}^T$ of $\hat{A}$ is defined by the matrix transposition of A,

$$\hat{A}^T := \sum_{ij} |v_i\rangle\, A_{ji} \langle v_j| = \sum_{ij} |i\rangle\, A^T_{ij} \,|v_j\rangle \,. \tag{B.60}$$

The corresponding superoperator $\mathscr{T}$ is thus given by

$$\mathscr{T}(|v_i\rangle \langle v_j|) := |v_j\rangle \langle v_i| \,. \tag{B.61}$$

The extended superoperator $\mathscr{T} \otimes \mathscr{I}$ corresponds to partial transposition. As shown above, partial transposition does not preserve the positivity of an operator. Whence, transposition is not a completely positive supermap (Definition B.4).

Appendix C
Group Theory

Group theory is the study of algebraic structures called groups. It has emerged as an abstraction unifying ideas of number theory, geometry, and the theory of algebraic equations. It forms the core part of abstract algebra.

The notion of group suits well the physical conception of symmetry, and group theory has provided valuable theoretical tools to exploit the symmetry of physical problems. Crystallography was the first in physics to use group theory extensively. With the advent of quantum mechanics, group theory has occupied a key position at the center stage of physical theories in various areas ranging from condensed matter physics to high-energy physics.

In quantum information and related areas, the use of group theory is not restricted to symmetry considerations. It facilitates and boosts investigations into the algebraic structures of multi-partite quantum states and quantum operations. For example, group theory lays out elegant and efficient algebraic tools to develop quantum algorithms, construct quantum error-correction codes, and analyze quantum cryptosystems.

In this appendix, we introduce briefly elementary concepts and theorems concerning groups. A great number of textbooks are available for more complete accounts, including Cornwell (1984)—or Cornwell (1997) if an abridged version is preferred—as well as Wigner (1959) for physicists.

C.1 The Concept

Mathematically, a group is a set of algebraic objects that must obey certain *axioms*. The development of the theory does not depend on the specific nature of the elements themselves, but in most physical applications these elements are transformations of one kind or another. The *multiplication* between objects is key to determine the structure of a group. Physically, it corresponds to the composition—successive application—of transformations.

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

Definition C.1 (*group*) A set $\mathcal{G}$ of elements is called *group* if the following four *group axioms* are satisfied:

(a) There exists an operation which associates with every pair of elements $G_1 \in \mathcal{G}$ and $G_2 \in \mathcal{G}$ another element $G_3 \in \mathcal{G}$. This operation is called *multiplication* and is written as $G_3 = G_1 G_2$, G_3 being described as the "product of G_1 and G_2."

(b) For any three elements $G_1, G_2, G_3 \in \mathcal{G}$,

$$(G_1 G_2) G_3 = G_1 (G_2 G_3)\,, \tag{C.1}$$

i.e., the multiplication is *associative*.

(c) There exists an *identity element* $e \in \mathcal{G}$ such that

$$GE = EG = G \tag{C.2}$$

for every element $G \in \mathcal{G}$.

(d) For each element $G \in \mathcal{G}$ there exists an *inverse element* $G^{-1} \in \mathcal{G}$ such that

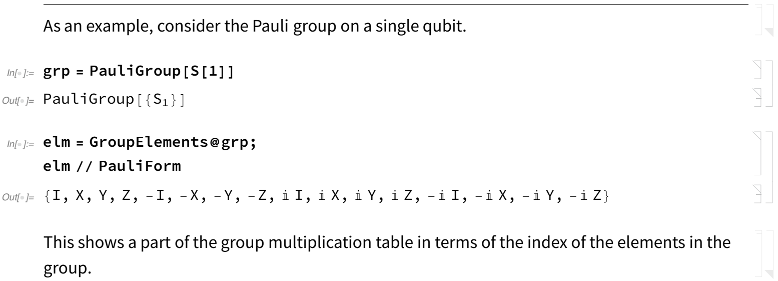
$$GG^{-1} = G^{-1}G = E\,. \tag{C.3}$$

The *order* of a group $\mathcal{G}$ is defined to be the number of elements in $\mathcal{G}$, which may be finite, countably infinite, or even non-countably infinite. It is denoted by $|\mathcal{G}|$. A group with finite order is called a *finite group*.

One of the most frequently appearing examples of group in quantum information is *Pauli group*. The Pauli group on a single qubit consists of the Pauli operators I, X, Y, and Z. Explicitly, it is given by

$$\mathcal{P}(1) = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}\ . \tag{C.4}$$

The additional phase factors ± 1 and $\pm i$ are included because a multiplication of two Pauli operators may result in another Pauli operator with one of such phase factors.

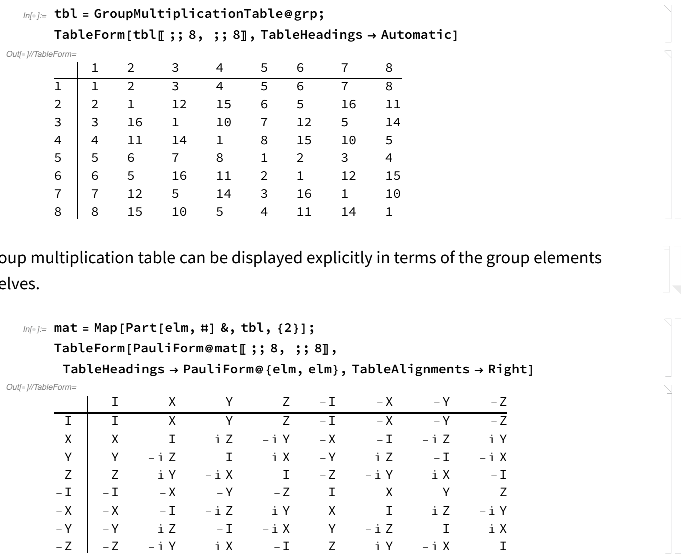


As an example, consider the Pauli group on a single qubit.

```
In[]:= grp = PauliGroup[S[1]]
Out[]= PauliGroup[{S1}]
```

```
In[]:= elm = GroupElements@grp;
       elm // PauliForm
Out[]= {I, X, Y, Z, -I, -X, -Y, -Z, i I, i X, i Y, i Z, -i I, -i X, -i Y, -i Z}
```

This shows a part of the group multiplication table in terms of the index of the elements in the group.



```
In[]:= tbl = GroupMultiplicationTable@grp;
       TableForm[tbl[[ ;; 8,  ;; 8]], TableHeadings → Automatic]
Out[]//TableForm=
     | 1   2    3    4    5   6    7    8
  ---+----------------------------------
  1  | 1   2    3    4    5   6    7    8
  2  | 2   1    12   15   6   5    16   11
  3  | 3   16   1    10   7   12   5    14
  4  | 4   11   14   1    8   15   10   5
  5  | 5   6    7    8    1   2    3    4
  6  | 6   5    16   11   2   1    12   15
  7  | 7   12   5    14   3   16   1    10
  8  | 8   15   10   5    4   11   14   1
```

The group multiplication table can be displayed explicitly in terms of the group elements themselves.

```
In[]:= mat = Map[Part[elm, #] &, tbl, {2}];
       TableForm[PauliForm@mat[[ ;; 8,  ;; 8]],
        TableHeadings → PauliForm@{elm, elm}, TableAlignments → Right]
Out[]//TableForm=
     |  I     X     Y     Z    -I    -X    -Y    -Z
  ---+-----------------------------------------------
   I |  I     X     Y     Z    -I    -X    -Y    -Z
   X |  X     I    i Z  -i Y   -X    -I  -i Z   i Y
   Y |  Y  -i Z     I   i X    -Y   i Z    -I  -i X
   Z |  Z   i Y  -i X     I    -Z  -i Y   i X    -I
  -I | -I    -X    -Y    -Z     I     X     Y     Z
  -X | -X    -I  -i Z   i Y     X     I   i Z  -i Y
  -Y | -Y   i Z    -I  -i X     Y  -i Z     I   i X
  -Z | -Z  -i Y   i X    -I     Z   i Y  -i X     I
```

Definition C.2 (*generators*) Let $\mathcal{G}$ be a group. The elements $G_1, G_2, \ldots, G_k$ of $\mathcal{G}$ are said to *generate* the group $\mathcal{G}$ and are denoted by

$$\mathcal{G} = \langle\{G_1, G_2, \ldots, G_k\}\rangle \tag{C.5}$$

if every element of $\mathcal{G}$ can be expressed as a multiplication of them. The elements are called *generators* of $\mathcal{G}$.

The description of a group can be drastically simplified by the use of generators. For example, consider the Pauli group in (C.4). It contains 16 elements but is generated by three elements,

$$\mathcal{P}(1) = \langle\{X, Y, Z\}\rangle\,. \tag{C.6}$$

It is more pronounced when we consider the Pauli group $\mathcal{P}(2)$ on two qubits,

$$\mathcal{P}(2) = \{\pm I \otimes I, \pm iI \otimes I, \pm X \otimes I, \pm iX \otimes I, \pm X \otimes X, \pm iX \otimes X, \ldots\}\,. \tag{C.7}$$

There are 64 elements in $\mathcal{P}(2)$ whereas it is generated by just 6 elements

$$\mathcal{P}(2) = \langle\{X \otimes I, Y \otimes I, Z \otimes I, I \otimes X, I \otimes Y, I \otimes Z\}\rangle\,. \tag{C.8}$$

For a given group $\mathcal{G}$, the set of generators is not unique. For example, the Pauli group on a single qubit can also be generated by iI, X, and Z; $\mathcal{P}(1) = \langle\{iI, X, Z\}\rangle$.

Theorem C.3 *Let $\mathcal{G}$ be a finite group. There exists a set of* $\log_2 |\mathcal{G}|$ *elements that generates $\mathcal{G}$.*

The description of a group can be drastically simplified by using generators.

```
In[ ]:= gnr = GroupGenerators@grp;
        PauliForm[gnr]
Out[ ]= {X, Y, Z}
```

For another example, consider the Pauli group on two qubits.

```
In[ ]:= elm = GroupElements@PauliGroup[S@{1, 2}];
        PauliForm[elm]
Out[ ]= {I⊗I, I⊗X, I⊗Y, I⊗Z, X⊗I, X⊗X, X⊗Y, X⊗Z, Y⊗I, Y⊗X, Y⊗Y, Y⊗Z,
         Z⊗I, Z⊗X, Z⊗Y, Z⊗Z, -(I⊗I), -(I⊗X), -(I⊗Y), -(I⊗Z), -(X⊗I),
         -(X⊗X), -(X⊗Y), -(X⊗Z), -(Y⊗I), -(Y⊗X), -(Y⊗Y), -(Y⊗Z), -(Z⊗I),
         -(Z⊗X), -(Z⊗Y), -(Z⊗Z), ⅈ I⊗I, ⅈ I⊗X, ⅈ I⊗Y, ⅈ I⊗Z, ⅈ X⊗I, ⅈ X⊗X,
         ⅈ X⊗Y, ⅈ X⊗Z, ⅈ Y⊗I, ⅈ Y⊗X, ⅈ Y⊗Y, ⅈ Y⊗Z, ⅈ Z⊗I, ⅈ Z⊗X, ⅈ Z⊗Y, ⅈ Z⊗Z,
         -ⅈ I⊗I, -ⅈ I⊗X, -ⅈ I⊗Y, -ⅈ I⊗Z, -ⅈ X⊗I, -ⅈ X⊗X, -ⅈ X⊗Y, -ⅈ X⊗Z,
         -ⅈ Y⊗I, -ⅈ Y⊗X, -ⅈ Y⊗Y, -ⅈ Y⊗Z, -ⅈ Z⊗I, -ⅈ Z⊗X, -ⅈ Z⊗Y, -ⅈ Z⊗Z}
```

It has 64 elements. That is, the order of the Pauli group on two qubits is 64.

```
In[ ]:= Length[elm]
Out[ ]= 64
```

```
In[ ]:= GroupOrder@PauliGroup[S@{1, 2}]
Out[ ]= 64
```

The Pauli group on two qubits can be generated by just 6 elements.

```
In[ ]:= gnr = GroupGenerators@PauliGroup[S@{1, 2}];
        PauliForm[gnr]
Out[ ]= {X⊗I, Y⊗I, Z⊗I, I⊗X, I⊗Y, I⊗Z}
```

Definition C.4 (*Abelian group*) If all the elements of a group commute, the group is said to be *Abelian*.

A special example of Abelian group are *cyclic groups*. A cyclic group $\mathcal{G}$ consists of elements which can be obtained by raising one of them to successive powers, i.e.,

$$\mathcal{G} = \left\{G, G^2, G^3, \ldots, G^n = E\right\}, \tag{C.9}$$

where n is some integer. It is thus generated by a single element, $\mathcal{G} = \langle\{G\}\rangle$; Any element of a cyclic group generates the group. A common example of cyclic group is

$$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\} \tag{C.10}$$

with addition modulo n as the group multiplication. In particular, $\mathbb{Z}_2$ appears very often in wide areas of science.

Theorem C.5 (rearrangement theorem) *Let $\mathcal{G}$ be a group. For any fixed element $G \in \mathcal{G}$, the set $G\mathcal{G} := \left\{GG' | G' \in \mathcal{G}\right\}$ contains every element of $\mathcal{G}$* once and only once. *The same holds for the set $\mathcal{G}G := \left\{G'G | G' \in \mathcal{G}\right\}$.*

Definition C.6 (*group homomorphism*) If $\phi : \mathcal{G} \to \mathcal{G}'$ is a mapping of a group $\mathcal{G}$ onto another group $\mathcal{G}'$ such that

$$\phi(G_1)\phi(G_2) = \phi(G_1 G_2) \tag{C.11}$$

for all $G_1, G_2 \in \mathcal{G}$, then ϕ is said to be a *homomorphic* mapping or a *homomorphism*. If ϕ is an one-to-one mapping, then it is called an *isomorphism*. When there exists an isomorphism from $\mathcal{G}$ onto $\mathcal{G}'$, $\mathcal{G}$ and $\mathcal{G}'$ are said to be *isomorphic* to each other and denoted by $\mathcal{G} \simeq \mathcal{G}'$.

C.2 Classes

A *class* of a group $\mathcal{G}$ is a subset of $\mathcal{G}$ having a certain property. This particular property makes classes play an important role in representation theory.

Definition C.7 (*conjugate elements and classes*) Let $\mathcal{G}$ be a group. An element $G' \in \mathcal{G}$ is said to be *conjugate* to another element G if there exists an element $H \in \mathcal{G}$ such that

$$G' = HGH^{-1} \,. \tag{C.12}$$

Obviously, if G' is conjugate to G, then G is also conjugate to G'. It is therefore permissible to talk of a set of *mutually* conjugate elements. A *class* of a group $\mathcal{G}$ is a set of mutually conjugate elements of $\mathcal{G}$.

Each class is completely determined by any member G of it. That is, given G, we obtain the whole class by forming the products

$$\mathcal{G}G\mathcal{G}^{-1} := \left\{HGH^{-1} | H \in \mathcal{G}\right\} \,. \tag{C.13}$$

Theorem C.8 *Classes have the following properties:*

(a) Every element of a group $\mathcal{G}$ is a member of some class of $\mathcal{G}$.
(b) No element of $\mathcal{G}$ an be a member of two different classes of $\mathcal{G}$.
(c) The identity E of $\mathcal{G}$ always forms a class on its own.

The conjugation relation between group elements as defined in (C.12) has physical implications when applied to quantum mechanics. For example, if $\mathcal{G}$ is a group consisting of rotations, no class of $\mathcal{G}$ contains both proper and improper rotations. Moreover, in each class of proper rotations all rotations are through the same angle. Similarly, in each class of improper rotations the proper parts are all through the same angle.

C.3 Invariant Subgroups

The notion of invariant subgroups is usually introduced together with the notion of *cosets* to construct *quotient groups*. It is also closely related to the concept of *classes* as will be seen shortly. Therefore, invariant subgroups also play an important role in representation theory.

Definition C.9 (*subgroup*) Let $\mathcal{G}$ be a group and $\mathcal{H} \subset \mathcal{G}$. If $\mathcal{H}$ itself is a group (with the multiplication among its elements given by that of $\mathcal{G}$), then $\mathcal{H}$ is called a subgroup of the group $\mathcal{G}$.

Definition C.10 (*invariant subgroups*) A subgroup $\mathcal{H}$ of a group $\mathcal{G}$ is said to be *invariant* if

$$GHG^{-1} \in \mathcal{H} \tag{C.14}$$

for every $H \in \mathcal{H}$ and $G \in \mathcal{G}$. In many cases the property in Eq. (C.14) is written in a more compact form as

$$\mathcal{G}\mathcal{H}\mathcal{G}^{-1} = \mathcal{H} \tag{C.15}$$

with the abbreviation $\mathcal{G}\mathcal{H}\mathcal{G}^{-1} := \left\{GHG^{-1} | H \in \mathcal{H}, G \in \mathcal{G}\right\}$.

Invariant subgroups are sometimes called *normal subgroups* or *normal divisors* because the defining property in Eq. (C.14) is of the same form as Eq. (C.12). The following theorem ensures the connection between the *classes* and the invariant subgroups.

Theorem C.11 *A subgroup $\mathcal{H}$ of a group $\mathcal{G}$ is an invariant subgroup if and only if $\mathcal{H}$ consists entirely of* complete *classes of $\mathcal{G}$.*

A special kind of invariant subgroup is the *centre* of the group. This notion is closely related to the notion of *quotient groups*.

Definition C.12 (*centre of a group*) The *centre* $\mathcal{Z}$ of a group $\mathcal{G}$ is defined to be the subgroup consisting of *all* elements of $\mathcal{G}$ that commute with every element of $\mathcal{G}$.

$\mathcal{Z}$ is an Abelian invariant subgroup of $\mathcal{G}$. Moreover, any subgroup of $\mathcal{Z}$ is an Abelian invariant subgroup of $\mathcal{G}$ and called a *central invariant subgroup* of $\mathcal{G}$.

C.4 Cosets and Quotient Groups

A subgroup of a group can be used to decompose the group (as a set) into disjoint subsets called *cosets*. We have already seen in Sect. C.2 that conjugacy classes is another way to do it. However, unlike conjugacy classes, all cosets of a group are of equal size.

Definition C.13 (*coset*) Let $\mathcal{H}$ be a subgroup (not necessarily an invariant subgroup) of a group $\mathcal{G}$. Then for any fixed $G \in \mathcal{G}$ (which may or may not be member of $\mathcal{H}$) the set $\mathcal{H}G := \{HG : H \in \mathcal{H}\}$ is called the *right coset* of $\mathcal{H}$ with respect to G. Similarly, the set $G\mathcal{H} := \{GH : H \in \mathcal{H}\}$ is called the *left coset* of $\mathcal{H}$ with respect to G.

The properties of cosets are summarized in the following two theorems:

Theorem C.14 *Let $\mathcal{H}$ be a subgroup of a group $\mathcal{G}$.*

(a) If $G \in \mathcal{H}$, then $\mathcal{H}G = \mathcal{H}$.
(b) If $G' \in \mathcal{H}G$, then $\mathcal{H}G' = \mathcal{H}G$.
(c) If $G \notin \mathcal{H}$, then $\mathcal{H}G$ is not a subgroup of $\mathcal{G}$.
(d) Every element of $\mathcal{G}$ is a member of some right coset.
(e) Two right cosets of $\mathcal{H}$ are either identical or have no elements in common.
(f) Any two elements HG and $H'G$ of $\mathcal{H}G$ are different provided that $H \neq H'$. In particular, if $\mathcal{H}$ is a finite subgroup of order $|\mathcal{H}|$, then $\mathcal{H}G$ contains $|\mathcal{H}|$ different elements.
(g) If $\mathcal{G}$ is a finite group of order $|\mathcal{G}|$ and $\mathcal{H}$ has order $|\mathcal{H}|$, then the number of distinct right cosets is $|\mathcal{G}|/|\mathcal{H}|$.

Above the statements are for the right cosets, but every statement applies equally to left cosets.

Theorem C.15 (cosets and invariant subgroups) *The right and left cosets of a subgroup $\mathcal{H}$ of a group $\mathcal{G}$ are* identical*, that is,*

$$\mathcal{H}G = G\mathcal{H} \tag{C.16}$$

for all $G \in \mathcal{G}$, if and only if $\mathcal{H}$ is an invariant *subgroup.*

The property (b) in Theorem C.14 is particularly important. It shows that the same coset is formed starting from *any* member of the coset. All members of a coset therefore appear on an equal footing, so that *any* member of the coset can be taken as the *coset representative* that labels the coset and from which the coset can be constructed. Accordingly, it may be useful to ignore the internal structure of each right coset of a subgroup $\mathcal{H}$ and consider each coset as an *element* of the *set of distinct right cosets*. Indeed, such a set of cosets forms a group with the suitable definition of multiplication as stated in the following theorem:

Theorem C.16 (quotient group $\mathcal{G}/\mathcal{H}$) *The set of right cosets of an* invariant *subgroup $\mathcal{H}$ of a group $\mathcal{G}$ forms a group with the group multiplication defined by*

$$G_1\mathcal{H} \cdot G_2\mathcal{H} = (G_1G_2)\mathcal{H} \tag{C.17}$$

for any $G_1, G_2 \in \mathcal{G}$. This group is called a quotient group *(or* factor group*) and is denoted by $\mathcal{G}/\mathcal{H}$. Furthermore, if $\mathcal{G}$ is* finite*, then*[7]

[7] It follows from Theorem C.14 (g).

$$|\mathcal{G}/\mathcal{H}| = |\mathcal{G}|/|\mathcal{H}| \,. \tag{C.18}$$

The key idea behind the notion of quotient group is that two elements G, G' of $\mathcal{G}$ are regarded equivalent as long as there exists $H \in \mathcal{H}$ such that $G = G'H$ (or $H' \in \mathcal{H}$ such that $G = H'G'$).

Note that unless the subgroup $\mathcal{H}$ is an invariant subgroup, it is not guaranteed that Eq. (C.17) provides a meaningful and consistent definition for the group multiplication. One has first to show that Eq. (C.17) provides a meaningful definition in that if alternative coset representatives are chosen for the cosets on the left-hand side of the equation, the coset on the right-hand side remains unchanged. Suppose that G_1' and G_2' are alternative coset representatives for $\mathcal{H}G_1$ and $\mathcal{H}G_2$, respectively, so that $G_1' \in \mathcal{H}G_1$ and $G_2' \in \mathcal{H}G_2$. It has to be proved that $\mathcal{H}(G_1'G_2') = \mathcal{H}(G_1G_2)$. As $G_1' \in \mathcal{H}G_1$ and $G_2' \in \mathcal{H}G_2$, there exist $H_1, H_2 \in \mathcal{H}$ such that $G_1' = H_1G_1$ and $G_2' = H_2G_2$ Furthermore, as $\mathcal{H}$ is invariant, $G_1\mathcal{H} = \mathcal{H}G_1$ and hence there exists $H_2' \in \mathcal{H}$ such that $G_1H_2 = H_2'G_1$. Consequently, one has

$$\mathcal{H}G_1' \cdot \mathcal{H}G_2' = \mathcal{H}(H_1G_1H_2G_2) = \mathcal{H}(H_1H_2'G_1G_2) = \mathcal{H}(G_1G_2) \,. \tag{C.19}$$

As an example, consider again the Pauli group on a single qubit

$$\mathcal{G} = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \,, \tag{C.20}$$

which we have already discussed in Eq. (C.4). $\mathcal{Z} = \{I, -I, iI, -iI\}$ is an invariant subgroup of $\mathcal{G}$. In fact, $\mathcal{Z}$ is the center of $\mathcal{G}$ (Definition C.12). The quotient group $\mathcal{G}/\mathcal{Z}$ is given by

$$\mathcal{G}/\mathcal{Z} = \{\mathcal{Z}, X\mathcal{Z}, Y\mathcal{Z}, Z\mathcal{Z}\} \,. \tag{C.21}$$

In the quotient group $\mathcal{G}/\mathcal{Z}$, the elements X, $-X$, iX, and $-iX$ are not distinguished and regarded as equivalent. Likewise, the elements Y, $-Y$, iY, and $-iY$ are regarded equivalent. This is convenient, for example, when one is only interested in the commutation relation but not the explicit multiplications between elements.

C.5 Product Groups

Given two or more sets, it is common to construct a new set consisting of tuples of the elements from the given sets. Given two or more groups, one can construct a new group in an analogous manner with the group multiplication inherited from the given groups.

Definition C.17 Let $\mathcal{G}$ and $\mathcal{G}'$ be groups. The *direct product group* or simply *product group*, $\mathcal{G} \times \mathcal{G}'$, is defined as follows:

(a) The underlying set of $\mathcal{G} \otimes \mathcal{G}'$ consists of the ordered pair of elements from $\mathcal{G}$ and $\mathcal{G}'$, that is,

$$\mathcal{G} \otimes \mathcal{G}' := \left\{ (G, G') | G \in \mathcal{G}, G' \in \mathcal{G}' \right\} \tag{C.22}$$

(b) For any $G_1, G_2 \in \mathcal{G}$ and $G'_1, G'_2 \in \mathcal{G}'$, the group multiplication is defined by

$$(G_1, G'_1)(G_2, G'_2) = (G_1 G_2, G'_1 G'_2). \tag{C.23}$$

It is straightforward to extend the definition to direct products of more than two groups by repeating the above operation.

The simplest example is the direct product of cyclic groups [see Eq. (C.10)], $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. The resulting group is Abelian (Definition C.4). In fact, one can show that any Abelian group is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ for some $n_1, n_2, \ldots, n_k$. Interestingly, $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ can also be regarded as a vector space over the field $\mathbb{Z}_2$. This fact provides convenient tools in studying the structure of the Pauli group (Sect. 6.3.1).

Appendix D
Mathematica Application Q3

Q3 is a Mathematica application to help study quantum information processing, quantum many-body systems, and quantum spin systems. It provides various tools and utilities for symbolic calculations and numerical simulations in these areas of quantum physics.

Q3 consists of several packages at different levels. Quisso, Fock, and Wigner are the three main packages, and they are devoted to the simulation of quantum information processing, quantum many-body systems, and quantum spin systems, respectively. They are based on another lower-level package, Pauli. Pauli itself provides useful tools to handle the Pauli matrices and operators for unlabelled qubits directly. However, it also lays out the programming structures and defines objects for the aforementioned three and other higher-level packages.

Q3 is distributed through the GitHub repository:

https://github.com/quantum-mob/Q3App

D.1 Installation

Q3 provides two installation methods: The first is based on the paclet system that has recently been introduced by Wolfram Research. It is not only fully automatic but also convenient to get updates later on. But it is supported only for Mathematica 12.1 or later. If your copy of Mathematica is compatible, then just copy the following code and run it on your Mathemtica Notebook:

```
Module[
  { ps },
  ps = PacletSiteRegister[
    "https://github.com/quantum-mob/PacletServer/raw/main",
    "Quantum Mob Paclet Server"
   ];
```

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

```
    PacletSiteUpdate[ps];
    PacletInstall["Q3"]
  ]
```

The other method is to download and copy the files to a proper folder—the traditional method. For details, take a look at the *installation guide* at:

https://github.com/quantum-mob/Q3App/blob/main/INSTALL.md

D.2 Quick Start

Once the application is installed, put

```
  "Q3" or "Q3/guide/Q3"
```

in the search field of the Wolfram Language Documentation Center (the help window of Mathematica) to get detailed technical information about the application.

Note that after installing the application, the first time you search for a keyword in Wolfram Language Documentation Center, Mathematica builds the search index of the new documentation files. It can take a few seconds to minutes depending on your computer. It happens only once (everytime you update the application).

Appendix E
Integrated Compilation of Demonstrations

QuantumWorkbook is a compilation of Mathematica Notebook files containing the Wolfram Language code files that have been used to generate the demonstrations in the book. Readers can try and modify the code themselves to build their own examples on the demonstrations and to experiment their fresh ideas.

QuantumWorkbook is distributed through the GitHub repository:

https://github.com/quantum-mob/QuantumWorkbook

E.1 Installation

Copy the following code, and just evaluate it in your Mathematica(R) Notebook:

```
Module[
  { ps },
  ps = PacletSiteRegister[
    "https://github.com/quantum-mob/PacletServer/raw/main",
    "Quantum Mob Paclet Server"
   ];
  PacletSiteUpdate[ps];
  PacletInstall["Q3"];
  PacletInstall["QuantumWorkbook"]
 ]
```

Note that along with QuantumWorkbook, it also installs the main application Q3 for your convenience.

This package may be modified for bug fixes and improvements. You may want to check for updates from time to time:

```
QuantumWorkbookCheckUpdate[]
```

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

In case there is an update, you can install it by using the following function:

```
QuantumWorkbookUpdate[]
```

E.2 Quick Start

Once QuantumWorkbook is installed, put

```
"QuantumWorkbook"
```

in the search field of the Wolfram Documentation Center (the Help window of Mathematica). You will see the table of contents of the workbook.

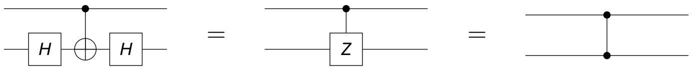
Appendix F
Solutions to Select Problems

F.1 The Postulates of Quantum Mechanics

F.2 Quantum Computation: Overview

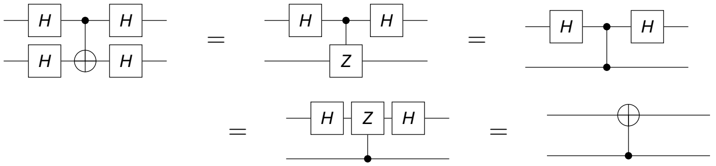
Problem 2.4

First, note that



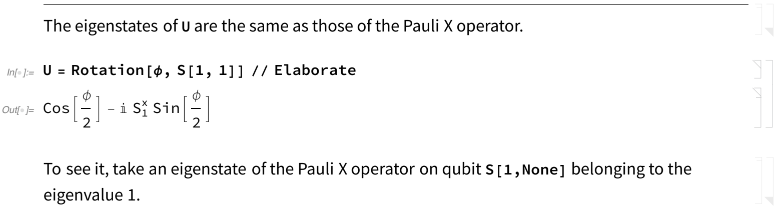
,

where note that the controlled-Z operation is "symmetric" in the roles of control and target; hence the circuit representation by two dots. Then it follows that



. (F.1)

Problem 2.7



The eigenstates of U are the same as those of the Pauli X operator.

```
In[◦]:= U = Rotation[ϕ, S[1, 1]] // Elaborate
```

```
Out[◦]= Cos[ϕ/2] - i S₁ˣ Sin[ϕ/2]
```

To see it, take an eigenstate of the Pauli X operator on qubit `S[1,None]` belonging to the eigenvalue 1.

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

```
In[•]:= vec = S[1, 6] ** Ket[];
        vec // LogicalForm
```

Out[•]= $\frac{\left|0_{S_1}\right\rangle}{\sqrt{2}} + \frac{\left|1_{S_1}\right\rangle}{\sqrt{2}}$

This confirms that the vector is indeed the intended eigenstate.

```
In[•]:= U ** vec // LogicalForm // TrigToExp // Simplify
```

Out[•]= $\frac{e^{-\frac{i\phi}{2}}\left(\left|0_{S_1}\right\rangle + \left|1_{S_1}\right\rangle\right)}{\sqrt{2}}$

This checks for the other eigenstate belonging to the eigenvalue -1.

```
In[•]:= vec = S[1, 6] ** Ket[S[1] → 1];
        vec // LogicalForm
```

Out[•]= $\frac{\left|0_{S_1}\right\rangle}{\sqrt{2}} - \frac{\left|1_{S_1}\right\rangle}{\sqrt{2}}$

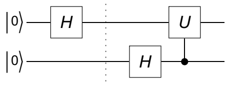
```
In[•]:= U ** vec // LogicalForm // TrigToExp // Simplify
```

Out[•]= $\frac{e^{\frac{i\phi}{2}}\left(\left|0_{S_1}\right\rangle - \left|1_{S_1}\right\rangle\right)}{\sqrt{2}}$

The ancillary qubit takes a relative phase shift depending on in which eigenstate the native qubit is.

```
In[•]:= Let[Real, ϕ];
        qc = QuantumCircuit[LogicalForm[Ket[], S@{1, 2}], S[1, 6], "Separator",
          S[2, 6], ControlledU[S[2], Rotation[ϕ, S[1, 1]], "Label" → "U"]]
```

Out[•]=



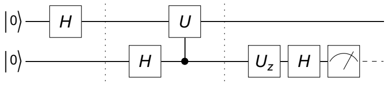
```
In[•]:= out = ExpressionFor[qc] // TrigToExp;
        KetFactor@out
```

Out[•]= $\frac{1}{2}\, e^{-\frac{i\phi}{2}}\left(\left|0_{S_1}\right\rangle + \left|1_{S_1}\right\rangle\right) \otimes \left(e^{\frac{i\phi}{2}}\left|0_{S_2}\right\rangle + \left|1_{S_2}\right\rangle\right)$

Make a basis change to detect it.

```
In[•]:= qc = QuantumCircuit[LogicalForm[Ket[], S@{1, 2}], S[1, 6], "Separator",
          S[2, 6], ControlledU[S[2], Rotation[ϕ, S[1, 1]], "Label" → "U"],
          "Separator", Rotation[ϕ / 2, S[2, 3]], S[2, 6], Measurement[S[2]]]
```

Out[•]=

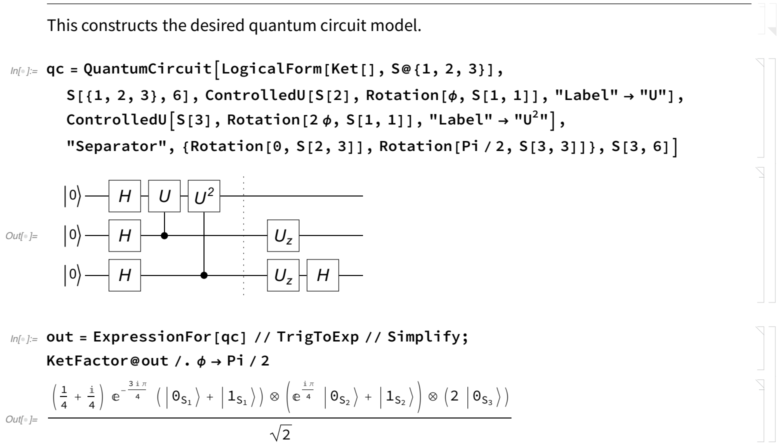


Finally, check the result.

```
In[•]:= out = ExpressionFor[qc] // TrigToExp;
        LogicalForm[KetFactor@out, S@{1, 2}]
```

Out[•]= $\frac{e^{-\frac{i\phi}{4}}\left(\left|0_{S_1}0_{S_2}\right\rangle + \left|1_{S_1}0_{S_2}\right\rangle\right)}{\sqrt{2}}$

Problem 2.8



This constructs the desired quantum circuit model.

```
In[•]:= qc = QuantumCircuit[LogicalForm[Ket[], S@{1, 2, 3}],
          S[{1, 2, 3}, 6], ControlledU[S[2], Rotation[ϕ, S[1, 1]], "Label" → "U"],
          ControlledU[S[3], Rotation[2 ϕ, S[1, 1]], "Label" → "U²"],
          "Separator", {Rotation[0, S[2, 3]], Rotation[Pi / 2, S[3, 3]]}, S[3, 6]]
```

Out[•]=

```
In[•]:= out = ExpressionFor[qc] // TrigToExp // Simplify;
        KetFactor@out /. ϕ → Pi / 2
```

Out[•]=

$$\frac{\left(\frac{1}{4}+\frac{i}{4}\right) e^{-\frac{3 i \pi}{4}} \left(\left|0_{S_1}\right\rangle + \left|1_{S_1}\right\rangle\right) \otimes \left(e^{\frac{i\pi}{4}} \left|0_{S_2}\right\rangle + \left|1_{S_2}\right\rangle\right) \otimes \left(2 \left|0_{S_3}\right\rangle\right)}{\sqrt{2}}$$

Problem 2.10 Suppose that the statement (2.10a) holds. Then

$$\hat{A}\hat{B} = \hat{I}\,, \quad \hat{A}\hat{X}\hat{B} = \hat{U}\,. \tag{F.2}$$

The first condition in the above implies that $\hat{B} = \hat{A}^\dagger$. Then put $\hat{W} = \hat{A}\hat{H}$, where $\hat{H}$ is the Hadamard gate, so that

$$\hat{W}\hat{Z}\hat{W}^\dagger = \hat{A}\hat{X}\hat{A}^\dagger = \hat{U}\,. \tag{F.3}$$

That is, the statement (2.10b) holds. Furthermore, observe that

$$\mathrm{Tr}\hat{U} = \mathrm{Tr}\hat{W}\hat{Z}\hat{W}^\dagger = \mathrm{Tr}\hat{Z} = 0\,, \tag{F.4}$$

$$\det\hat{U} = \det\hat{W}\hat{Z}\hat{W}^\dagger = \det\hat{Z} = -1\,, \tag{F.5}$$

and hence the statement (2.10c) holds as well.

Next, suppose that $\hat{U} = \hat{W}\hat{Z}\hat{W}^\dagger$ for some unitary operator $\hat{W}$. Put $\hat{A} = \hat{W}\hat{H}$ and $\hat{B} = \hat{A}^\dagger$, which satisfy (F.2); that is, the statement (2.10a) holds. Furthermore, statement (2.10c) also holds as already shown above.

Finally, suppose that the statement (2.10c) holds: The condition $\mathrm{Tr}\hat{U} = 0$ implies that

$$\hat{U} = u_x\hat{X} + u_y\hat{Y} + u_z\hat{Z} \quad (u_x, u_y, u_z \in \mathbb{C}). \tag{F.6}$$

The unitarity condition of $\hat{U}$ implies that all the phases of u_μ must be the same and that $\sum_\mu |u_\mu|^2 = 1$. This implies in turn that

$$\hat{U} = e^{i\phi}\hat{W}\hat{Z}\hat{W}^\dagger \tag{F.7}$$

for some $\phi \in \mathbb{R}$ and some unitary operator $\hat{W}$. The condition $\det\hat{U} = -1$ leads to $\phi = n\pi$ with $n \in \mathbb{Z}$. For $e^{i\phi} = -1$ (n odd), simply replace $\hat{W}$ with $\hat{W}' = \hat{W}\hat{X}$.

Therefore, regardless of $e^{i\phi} = \pm 1$, the statement (2.10b) holds. As we have already shown above that the statement (2.10b) implies (2.10a), this completes the proof.

F.3 Quantum Computers

Problem 3.3 We define

$$|D\rangle := \frac{|1\rangle\,\Omega_1 + |2\rangle\,\Omega_2}{\Omega}. \tag{F.8}$$

where $\Omega := \sqrt{\Omega_1^2 + \Omega_2^2}$. Then the Hamiltonian reads as

$$\hat{H} = \epsilon\,|\epsilon\rangle\,\langle\epsilon| - \frac{1}{2}\Omega\,(|\Omega\rangle\,\langle\epsilon| + |\epsilon\rangle\,\langle\Omega|)\,. \tag{F.9}$$

(a) The expressions for the two eigenstates of $\hat{H}$ in (F.9) are formally the same as those in the main text (Sect. 3.3.1). The Hamiltonian involves only $|\epsilon\rangle$ and $|\Omega\rangle$. There must be one more state. It is the dark state of the system. We denote it by $|D\rangle$. The dark state must be orthogonal to the bright state $|\Omega\rangle$ as well as $|\epsilon\rangle$. Therefore, we can construct it as follows

$$|D\rangle = \frac{|1\rangle\,\Omega_2^* - |2\rangle\,\Omega_1^*}{\Omega}. \tag{F.10}$$

By inspection, one can confirm that it is orthogonal both to $|\Omega\rangle$ and trivially to $|\epsilon\rangle$. Using the parametrization suggested in the statement of the problem, we can rewrite $|D\rangle$ into the form

$$|D\rangle = \frac{|1\rangle\sin(\theta/2)e^{-\phi/2} - |2\rangle\cos(\theta/2)e^{i\phi/2}}{\Omega}. \tag{F.11}$$

(b) The Abelian gauge potential is given by

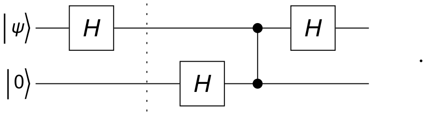
$$A^\phi := \langle D|\,\frac{\partial}{\partial\phi}\,|D\rangle = \frac{i\cos\theta}{2}. \tag{F.12}$$

As it is Abelian, it is customary to define the Berry phase as $\gamma = -iA^\phi = \frac{1}{2}\cos\theta$.

(c) For the path where ϕ varies from 0 to 2π with θ fixed, the Abelina geometric phase is given by

$$U(\mathcal{C}) = e^{-i\gamma} = e^{-i(\cos\theta)/2}. \tag{F.13}$$

Problem 3.4 A direct inspection would be sufficient. Here we slightly modify the quantum circuit into the form



(F.14)

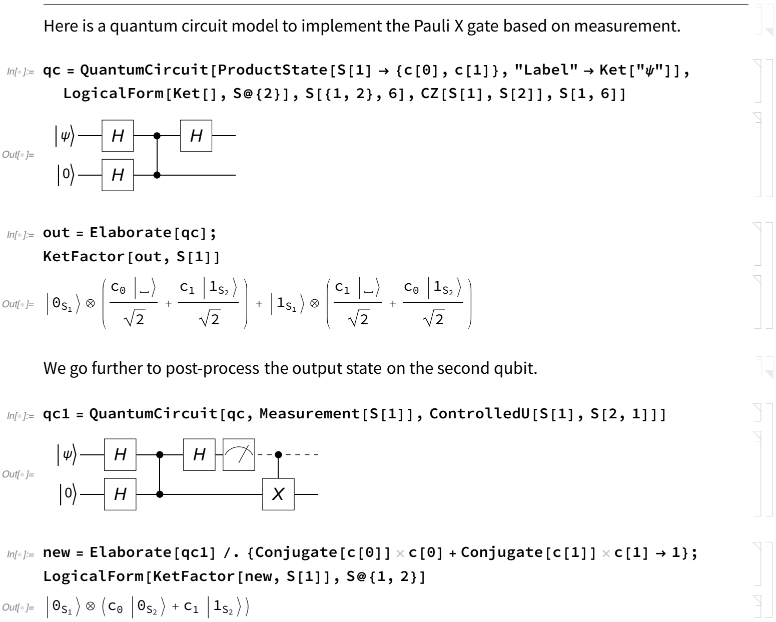
We then use the already known result in (3.70) for the quantum circuit in Eq. (3.69). In this case, $\hat{U}_z$ is trivial, $\hat{U}_z = \hat{I}$, and the input state is $\hat{H}\,|\psi\rangle$. It leads to the output state on the second qubit

$$\frac{|0\rangle \otimes (\hat{H}\hat{H}\,|\psi\rangle) + |1\rangle \otimes (\hat{H}\hat{Z}\hat{H}\,|\psi\rangle)}{\sqrt{2}}. \tag{F.15}$$

The identities, $\hat{H}^2 = \hat{I}$ and $\hat{H}\hat{Z}\hat{H} = \hat{X}$, lead to

$$\frac{|0\rangle \otimes |\psi\rangle + |1\rangle \otimes (\hat{X}\,|\psi\rangle)}{\sqrt{2}}. \tag{F.16}$$

as expected.



Here is a quantum circuit model to implement the Pauli X gate based on measurement.

```
In[∘]:= qc = QuantumCircuit[ProductState[S[1] → {c[0], c[1]}, "Label" → Ket["ψ"]],
          LogicalForm[Ket[], S@{2}], S[{1, 2}, 6], CZ[S[1], S[2]], S[1, 6]]
```

```
In[∘]:= out = Elaborate[qc];
        KetFactor[out, S[1]]
```

Out[∘]= $\left|0_{S_1}\right\rangle \otimes \left(\frac{c_0\,|\_\rangle}{\sqrt{2}} + \frac{c_1\,\left|1_{S_2}\right\rangle}{\sqrt{2}}\right) + \left|1_{S_1}\right\rangle \otimes \left(\frac{c_1\,|\_\rangle}{\sqrt{2}} + \frac{c_0\,\left|1_{S_2}\right\rangle}{\sqrt{2}}\right)$

We go further to post-process the output state on the second qubit.

```
In[∘]:= qc1 = QuantumCircuit[qc, Measurement[S[1]], ControlledU[S[1], S[2, 1]]]
```

```
In[∘]:= new = Elaborate[qc1] /. {Conjugate[c[0]] × c[0] + Conjugate[c[1]] × c[1] → 1};
        LogicalForm[KetFactor[new, S[1]], S@{1, 2}]
```

Out[∘]= $\left|0_{S_1}\right\rangle \otimes \left(c_0\,\left|0_{S_2}\right\rangle + c_1\,\left|1_{S_2}\right\rangle\right)$

Problem 3.6 Let $\hat{U}$ be a unitary operator on a finite-finite dimensional vector space $\mathcal{V}$. Then we have

$$\hat{U}\exp(\hat{A})\hat{U}^\dagger = \exp(\hat{U}\hat{A}\hat{U}^\dagger) \tag{F.17}$$

for any linear operator $\hat{A}$ on $\mathcal{V}$.

(a) We note that $\hat{X}$ is both unitary and Hermitian. Furthermore, $\hat{X}\hat{Z}\hat{X} = -\hat{Z}$. These observations lead to

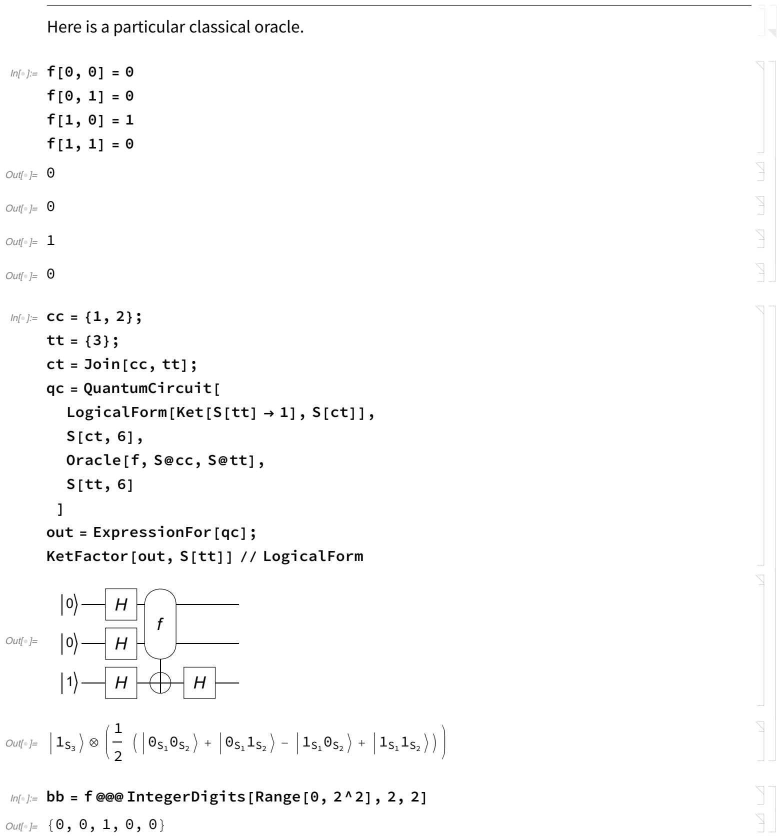
$$\hat{X}\exp(-i\hat{Z}\phi/2)\hat{X} = \exp(-i\hat{X}\hat{Z}\hat{X}\phi/2) = \exp(+i\hat{Z}\phi/2) = \hat{U}_z(-\phi). \quad \text{(F.18)}$$

(b) Similarly, $\hat{H}$ is both unitary and Hermitian. It also satisfies $\hat{H}\hat{Z}\hat{H} = \hat{X}$. It follows that

$$\hat{H}\exp(-i\hat{Z}\phi/2)\hat{H} = \exp(-i\hat{H}\hat{Z}\hat{H}\phi/2) = \exp(-i\hat{X}\phi/2) = \hat{U}_x(\phi). \quad \text{(F.19)}$$

F.4 Quantum Algorithms

Problem 4.1



Here is a particular classical oracle.

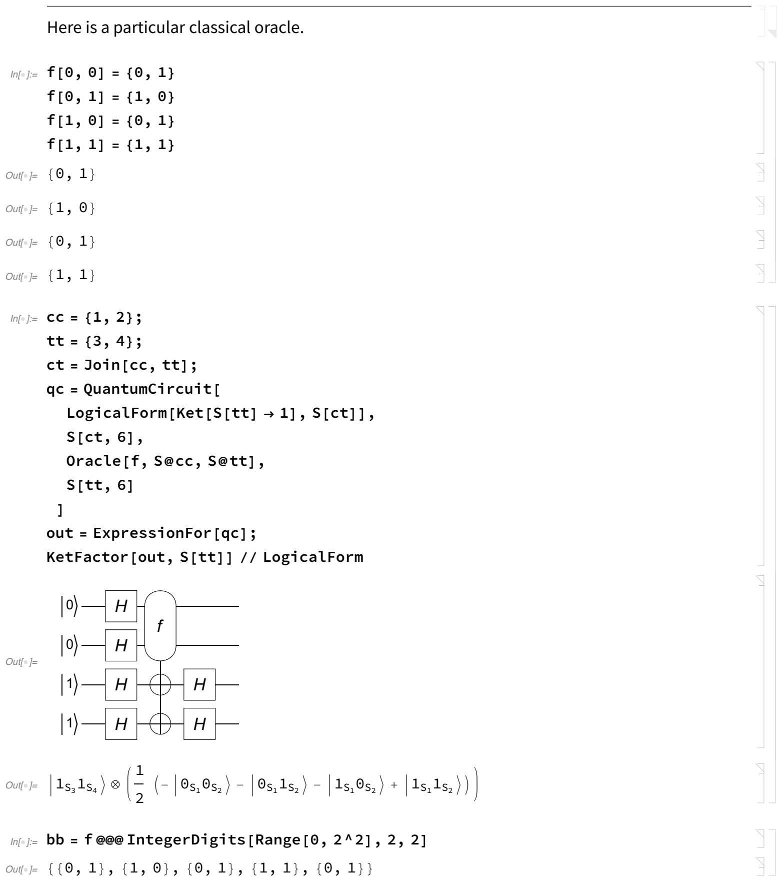
```
In[ ]:= f[0, 0] = 0
        f[0, 1] = 0
        f[1, 0] = 1
        f[1, 1] = 0
Out[ ]= 0
Out[ ]= 0
Out[ ]= 1
Out[ ]= 0
```

```
In[ ]:= cc = {1, 2};
        tt = {3};
        ct = Join[cc, tt];
        qc = QuantumCircuit[
          LogicalForm[Ket[S[tt] → 1], S[ct]],
          S[ct, 6],
          Oracle[f, S@cc, S@tt],
          S[tt, 6]
         ]
        out = ExpressionFor[qc];
        KetFactor[out, S[tt]] // LogicalForm
```

Out[ ]=

Out[ ]= $|1_{S_3}\rangle \otimes \left(\frac{1}{2}\left(|0_{S_1}0_{S_2}\rangle + |0_{S_1}1_{S_2}\rangle - |1_{S_1}0_{S_2}\rangle + |1_{S_1}1_{S_2}\rangle\right)\right)$

```
In[ ]:= bb = f @@@ IntegerDigits[Range[0, 2^2], 2, 2]
Out[ ]= {0, 0, 1, 0, 0}
```



Here is a particular classical oracle.

```
In[◦]:= f[0, 0] = {0, 1}
        f[0, 1] = {1, 0}
        f[1, 0] = {0, 1}
        f[1, 1] = {1, 1}
Out[◦]= {0, 1}
Out[◦]= {1, 0}
Out[◦]= {0, 1}
Out[◦]= {1, 1}
```

```
In[◦]:= cc = {1, 2};
        tt = {3, 4};
        ct = Join[cc, tt];
        qc = QuantumCircuit[
          LogicalForm[Ket[S[tt] → 1], S[ct]],
          S[ct, 6],
          Oracle[f, S@cc, S@tt],
          S[tt, 6]
         ]
        out = ExpressionFor[qc];
        KetFactor[out, S[tt]] // LogicalForm
```

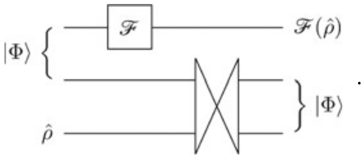
Out[◦]=

Out[◦]= $\left|1_{S_3}1_{S_4}\right\rangle \otimes \left(\frac{1}{2}\left(-\left|0_{S_1}0_{S_2}\right\rangle - \left|0_{S_1}1_{S_2}\right\rangle - \left|1_{S_1}0_{S_2}\right\rangle + \left|1_{S_1}1_{S_2}\right\rangle\right)\right)$

```
In[◦]:= bb = f@@@IntegerDigits[Range[0, 2^2], 2, 2]
Out[◦]= {{0, 1}, {1, 0}, {0, 1}, {1, 1}, {0, 1}}
```

F.5 Decoherence

Problem 5.2 We analyse the quantum circuit



(F.20)

Before the projection onto $|\Phi\rangle := \frac{1}{\sqrt{d}}\sum_j \left|v_j\right\rangle \otimes \left|v_j\right\rangle$, where d is the dimension of each quantum register, the state reads as

$$\hat{R} = \frac{1}{d}\sum_{ij} \mathscr{F}(|v_i\rangle\langle v_j|) \otimes |v_i\rangle\langle v_j| \otimes \hat{\rho}. \tag{F.21}$$

The projection onto $|\Phi\rangle$ leads to the state for the first register

$$\begin{aligned}
\hat{R}' &= \frac{1}{d}\sum_{ij} \mathscr{F}(|v_i\rangle\langle v_j|)\mathrm{Tr}(|v_i\rangle\langle v_j| \otimes \hat{\rho})\,|\Phi\rangle\langle\Phi| \\
&= \frac{1}{d}\sum_{ij} \mathscr{F}(|v_i\rangle\langle v_j|)\frac{1}{d}\sum_{kl}(|v_i\rangle\langle v_j| \otimes \hat{\rho})(|v_k\rangle\langle v_l| \otimes |v_k\rangle\langle v_l|) \\
&= \frac{1}{d^2}\sum_{ij} \mathscr{F}(|v_i\rangle\langle v_j|)\,\langle v_i|\,\hat{\rho}\,|v_j\rangle
\end{aligned} \tag{F.22}$$

By the linearity of the supermap $\mathscr{F}$, one obtains

$$\hat{R}' = \frac{1}{d^2}\mathscr{F}\left(\textstyle\sum_{ij} |v_i\rangle\langle v_i|\,\hat{\rho}\,|v_j\rangle\langle v_j|\right) = \frac{1}{d^2}\mathscr{F}(\hat{\rho}). \tag{F.23}$$

The factor of $1/d^2$ indicates the success probability of the protocol.

Problem 5.10 We first prove (5.245). From the singular-value decomposition of $\hat{A}$

$$\hat{A} = \sum_j |u_j\rangle a_j \langle v_j| \quad (a_j \geq 0), \tag{F.24}$$

we have

$$\|\hat{A}\|_{\mathrm{HS}}^2 = \sum_j a_j^2, \tag{F.25}$$

and

$$\|\hat{A}^\dagger\hat{A}\|_{\mathrm{HS}}^2 = \sum_j a_j^4 \leq \left(\sum_j a_j^2\right)^2 = \|\hat{A}\|_{\mathrm{HS}}^2, \tag{F.26}$$

which proves (5.245).

Next, we prove (5.244). We note that

$$\|\hat{A}\hat{B}\|_{\mathrm{HS}}^2 = \mathrm{Tr}\hat{B}^\dagger\hat{A}^\dagger\hat{A}\hat{B} = \mathrm{Tr}\hat{A}^\dagger\hat{A}\hat{B}\hat{B}^\dagger = \langle\hat{A}^\dagger\hat{A}, \hat{B}\hat{B}^\dagger\rangle. \tag{F.27}$$

Using the Cauchy-Schwarz inequality and (5.245), we have

$$\|\hat{A}\hat{B}\|_{\mathrm{HS}}^2 = \langle\hat{A}^\dagger\hat{A}, \hat{B}\hat{B}^\dagger\rangle \leq \|\hat{A}^\dagger\hat{A}\|_{\mathrm{HS}}\|\hat{B}\hat{B}^\dagger\|_{\mathrm{HS}} \leq \|\hat{A}\|_{\mathrm{HS}}^2\|\hat{B}\|_{\mathrm{HS}}^2. \tag{F.28}$$

Problem 5.11 We first note that

$$\mathrm{Tr}\hat{G} = \sum_\mu \mathrm{Tr}\hat{F}_\mu \hat{F}_\mu^\dagger = \sum_\mu \mathrm{Tr}\hat{F}_\mu^\dagger \hat{F}_\mu = \mathrm{Tr}\hat{I} = \dim \mathcal{V}. \tag{F.29}$$

From (5.168), we have

$$|\mathrm{Tr}\hat{G}| = \dim \mathcal{V} \le \|\hat{G}\|_{\mathrm{tr}}. \tag{F.30}$$

On the other hand, from (5.183), we have

$$\|\hat{G} = \mathscr{F}(\hat{I})\|_{\mathrm{tr}} \le \|\hat{I}\|_{\mathrm{tr}} = \dim \mathcal{V}. \tag{F.31}$$

Problem 5.12 Consider the singular-value decomposition (Theorem A.22 and Eq. (A.67)) of $\hat{A}$ in the form

$$\hat{A} = \sum_j |u_j\rangle a_j \langle v_j| \ , \tag{F.32}$$

where $a_j \ge 0$ are the singular values of $\hat{A}$, $\langle u_i|u_j\rangle = \delta_{ij}$, and $\langle v_i|v_j\rangle = \delta_{ij}$.

(a) Then, it follows that

$$\begin{aligned} \sum_m \left|\langle m|\hat{A}|m\rangle\right|^2 &= \sum_{mj} \left|\langle m|u_j\rangle\right|^2 a_j^2 \left|\langle v_j|m\rangle\right|^2 \\ &\le \sum_{mj} \left|\langle m|u_j\rangle\right|^2 a_j^2 \\ &= \sum_j a_j^2 \\ &= \|\hat{A}\|^2. \end{aligned} \tag{F.33}$$

Here we have used the fact that $|u_i\rangle$ and $\left|v_j\right\rangle$ are normalized vectors, $|\langle m|u_j\rangle|^2 \le 1$, and $|\langle m|v_j\rangle|^2 \le 1$.
On the other hand, we note that

$$\begin{aligned} \sum_m \left|\langle m|\hat{A}|m\rangle\right| &= \sum_{mj} \left|\langle m|u_j\rangle a_j \langle v_j|m\rangle\right| \\ &= \sum_{mj} a_j \left|\langle m|u_j\rangle\right| \left|\langle v_j|m\rangle\right| \\ &\le \frac{1}{2}\sum_{mj} a_j \left(\left|\langle m|u_j\rangle\right|^2 + \left|\langle v_j|m\rangle\right|^2\right), \end{aligned} \tag{F.34}$$

where we have used the inequality

$$xy \le \frac{x^2+y^2}{2} \tag{F.35}$$

for any real numbers x and y. Note that

$$\sum_m \left|\langle m|u_j\rangle\right|^2 = \sum_m \langle u_j|m\rangle\langle m|u_j\rangle = \langle u_j|u_j\rangle = 1, \tag{F.36}$$

and similarly,

$$\sum_m \left|\langle m|v_j\rangle\right|^2 = 1. \tag{F.37}$$

Therefore we have

$$\sum_m |\langle m|\hat{A}|m\rangle| \le \sum_j a_j = \|\hat{A}\|_{\rm tr}\,. \tag{F.38}$$

(b) In addition to the singular-value decomposition (F.32) of $\hat{A}$, we also consider the spectral decomposition of $\hat{E}_m$

$$\hat{E}_m = \sum_k |\epsilon_{mk}\rangle\, \epsilon_{mk}\, \langle\epsilon_{mk}|\,. \tag{F.39}$$

Here note that

$$0 \le \epsilon_{mk} \le 1 \tag{F.40}$$

because the POVM elements satisfy the closure relation

$$\sum_m \hat{E}_m = \hat{I}. \tag{F.41}$$

Therefore, it follows that

$$\begin{aligned}
\sum_m ({\rm Tr}\hat{E}_m\hat{A})^2 &= \sum_{mkj} \epsilon_{mk}^2 \left|\langle\epsilon_{mk}|u_j\rangle\right|^2 a_j^2 \left|\langle v_j|\epsilon_{mk}\rangle\right|^2 \\
&\le \sum_{mkj} \epsilon_{mk} \left|\langle\epsilon_{mk}|u_j\rangle\right|^2 a_j^2 \\
&= \sum_j \sum_{mk} \langle u_j|\epsilon_{mk}\rangle\epsilon_{mk}\langle\epsilon_{mk}|u_j\rangle a_j^2 \\
&= \sum_j \sum_m \langle u_j|\, \hat{E}_m \,|u_j\rangle a_j^2 \\
&= \sum_j a_j^2 \\
&= \|\hat{A}\|^2.
\end{aligned} \tag{F.42}$$

On the other hand, we note that

$$\begin{aligned}\sum_m \left|\mathrm{Tr}\hat{E}_m\hat{A}\right| &= \sum_{mkj} \left|\epsilon_{mk}\langle\epsilon_{mk}|u_j\rangle a_j\langle v_j|\epsilon_{mk}\rangle\right| \\ &= \sum_{mkj} a_j\epsilon_{mk}\left|\langle\epsilon_{mk}|u_j\rangle\right|\left|\langle v_j|\epsilon_{mk}\rangle\right| \\ &\leq \frac{1}{2}\sum_{mkj} a_j\epsilon_{mk}\left(\left|\langle\epsilon_{mk}|u_j\rangle\right|^2 + \left|\langle v_j|\epsilon_{mk}\rangle\right|^2\right).\end{aligned} \tag{F.43}$$

Again, we have used the inequality (F.35). Note that

$$\begin{aligned}\sum_{mk}\epsilon_{mk}\left|\langle\epsilon_{mk}|u_j\rangle\right|^2 &= \sum_{mk}\langle u_j\epsilon_{mk}\rangle\epsilon_{mk}\langle\epsilon_{mk}|u_j\rangle \\ &= \sum_m \left\langle u_j\right|\hat{E}_m\left|u_j\right\rangle = \langle u_j|u_j\rangle = 1,\end{aligned} \tag{F.44}$$

and similarly,

$$\sum_{mk}\epsilon_{mk}\left|\langle\epsilon_{mk}|v_j\rangle\right|^2 = 1. \tag{F.45}$$

Therefore we have

$$\sum_m |\mathrm{Tr}\hat{E}_m\hat{A}| \leq \sum_j a_j = \|\hat{A}\|_{\mathrm{tr}}\,. \tag{F.46}$$

Problem 5.7 Consider a polar decomposition of $\hat{A}$,

$$\hat{A} = V\sqrt{\hat{A}^\dagger\hat{A}}\,. \tag{F.47}$$

Then we have

$$|\mathrm{Tr}\hat{A}\hat{U}| = \left|\mathrm{Tr}\hat{U}\hat{V}\sqrt{\hat{A}^\dagger\hat{A}}\right|. \tag{F.48}$$

Define a unitary operator $\hat{W} := \hat{U}\hat{V}$ and consider its spectral decomposition

$$\hat{W} = \sum_j \left|w_j\right\rangle e^{i\phi_j}\left\langle w_j\right|. \tag{F.49}$$

Putting it into (F.48), we have

$$\begin{aligned}|\mathrm{Tr}\hat{A}\hat{U}| &= \left|\sum_j \langle w_j|\sqrt{\hat{A}^\dagger\hat{A}}\,|w_j\rangle e^{i\phi_j}\right| \\ &\le \sum_j \left|\langle w_j|\sqrt{\hat{A}^\dagger\hat{A}}\,|w_j\rangle e^{i\phi_j}\right| \\ &= \mathrm{Tr}\sqrt{\hat{A}^\dagger\hat{A}} \\ &= \|\hat{A}\|_{\mathrm{tr}}\,.\end{aligned} \tag{F.50}$$

F.6 Quantum Error-Correction Codes

Problem 6.3 Let $\left|\hat{G}_1\right\rangle, \left|\hat{G}_2\right\rangle, \ldots, \left|\hat{G}_k\right\rangle$ be the Gottesman vectors of the generators $\hat{G}_1, \hat{G}_2, \ldots, \hat{G}_k$. As the generators are independent, the Gottesman vectors are linearly independent of each other. Construct a matrix M from the rows of $\left\langle\hat{G}_1\right|, \left\langle\hat{G}_2\right|, \ldots, \left\langle\hat{G}_k\right|$,

$$M = \begin{bmatrix} \left\langle\hat{G}_1\right| \\ \left\langle\hat{G}_2\right| \\ \vdots \\ \left\langle\hat{G}_k\right| \end{bmatrix} = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ & \vdots & & \\ M_{k1} & M_{k2} & \cdots & M_{kn} \end{bmatrix}. \tag{F.51}$$

Suppose that we want to find an operator $\hat{G}$ that anti-commutes with, say, $\hat{G}_1$ but commute with all others. Because the rows of M are linearly independent by construction, the equation

$$\begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ & \vdots & & \\ M_{k1} & M_{k2} & \cdots & M_{kn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{F.52}$$

has at least one solution. Define a Gottesman vector $\left\langle\hat{G}\right| := (y_1, y_2, y_3, \ldots, y_n)\hat{J}$ where the operator $\hat{J}$ on the Gottesman vector space is defined in Eq. (6.43). Then we have

$$\begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ & \vdots & & \\ M_{k1} & M_{k2} & \cdots & M_{kn} \end{bmatrix} \hat{J} \left|\hat{G}\right\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} . \tag{F.53}$$

That is,

$$\langle \hat{G}_1 | \hat{G} \rangle = 1 , \quad \langle \hat{G}_2 | \hat{G} \rangle = 0 , \quad \ldots , \quad \langle \hat{G}_k | \hat{G} \rangle = 0 . \tag{F.54}$$

Therefore, the operator $\hat{G}$ corresponding to the Gottesman vector $\left|\hat{G}\right\rangle$ must anti-commute with $\hat{G}_1$ but commute with $\hat{G}_2, \ldots, \hat{G}_k$.
Problem 6.5 See Problem 2.4.

Problem 6.6 Let

$$\hat{Z}' := \hat{U}(\hat{Z} \otimes \hat{J})\hat{U}^\dagger , \quad \hat{X}' := \hat{U}(\hat{X} \otimes \hat{J})\hat{U}^\dagger . \tag{F.55}$$

Note that they anti-commute. Therefore, there exists at least one qubit on which $\hat{Z}'$ and $\hat{X}'$ anti-commute. We rearrange the qubits so that the particular qubit comes at the first place. Now $\hat{Z}'$ and $\hat{X}'$ must be of the form

$$\hat{Z}' = \hat{P} \otimes \hat{A} , \quad \hat{X}' = \hat{Q} \otimes \hat{B} \tag{F.56}$$

with $\left\{\hat{P}, \hat{Q}\right\} = 0$. Then, one can apply the conjugation by a single-qubit operation in $\mathcal{C}(1)$ on the first qubit so that

$$\hat{P} \to \hat{X} , \quad \hat{Q} \to \hat{Z} . \tag{F.57}$$

Problem 6.7 Let $\hat{P}$ be an element of the n-qubit Pauli group $\mathcal{P}(n)$. Consider

$$\begin{aligned} \hat{P}\hat{V} |y\rangle &= \sum_x \hat{P} |x\rangle \left(\langle 0| \otimes \langle x|\right)\hat{U}(|0\rangle \otimes |y\rangle) \\ &= \sum_x \hat{P} |x\rangle \left(\langle 0| \otimes \langle x| \hat{P}^\dagger\right)(\hat{I} \otimes \hat{P})\hat{U}(|0\rangle \otimes |y\rangle) \\ &= \sum_x |x\rangle \left(\langle 0| \otimes \langle x|\right)(\hat{I} \otimes \hat{P})\hat{U}(|0\rangle \otimes |y\rangle) , \end{aligned}$$

where we have used the fact that $\hat{P}$ is invertible, and accordingly changed the dummy variable $\hat{P} |x\rangle \to |x\rangle$. Now as $\hat{U}$ is an element of the Clifford group and $\hat{I} \otimes \hat{P} \in \mathcal{P}(n+1)$, there must exist $\hat{P}' \in \mathcal{P}(n+1)$ such that $(\hat{I} \otimes \hat{P})\hat{U} = \hat{U}\hat{P}'$.

$$\hat{P}\hat{V}\,|y\rangle = \sum_x |x\rangle\,(\langle 0| \otimes \langle x|)\hat{U}\hat{P}'(|0\rangle \otimes |y\rangle).$$

(i) Suppose that $\hat{P}' = \hat{Z} \otimes \hat{P}''$ or $\hat{P} = \hat{I} \otimes \hat{P}''$ for some $\hat{P}'' \in \mathcal{P}(n)$. Then,

$$\begin{aligned}\hat{P}\hat{V}\,|y\rangle &= \sum_x |x\rangle\,(\langle 0| \otimes \langle x|)\hat{U}(|0\rangle \otimes \hat{P}''\,|y\rangle)\\ &= \hat{V}\hat{P}''\,|y\rangle\end{aligned}$$

for all $|y\rangle$. Therefore, $\hat{V} \in \mathcal{C}(n)$. (ii) Next, suppose that $\hat{P}' = \hat{X} \otimes \hat{P}''$; the case $\hat{P}' = \hat{Y} \otimes \hat{P}''$ can be treated by combining with the above argument. Then, using the property

$$\hat{U}(\hat{X} \otimes \hat{J})\hat{U}^\dagger = \hat{Z} \otimes \hat{P}''', \quad \hat{J} := \hat{I}^{\otimes n} \tag{F.58}$$

for some $\hat{P}''' \in \mathcal{P}(n)$, one can see that

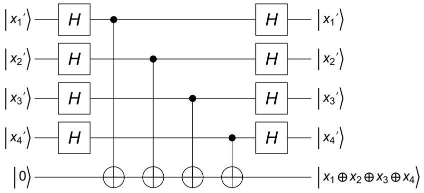
$$\hat{P}\hat{V}\,|y\rangle = \sum_x |x\rangle\,(\langle 0| \otimes \langle x|)(\hat{Z} \otimes \hat{W})\hat{U}(|0\rangle \otimes \hat{P}''\,|y\rangle).$$

This implies that for any $\hat{P} \in \mathcal{P}(n)$, there exist $\hat{P}''$, $\hat{P}''' \in \mathcal{P}(n)$ such that

$$\hat{P}'''\hat{P}\hat{V} = \hat{V}\hat{P}''. \tag{F.59}$$

As $\hat{P}'''$ is invertible, $\hat{P}'''\hat{P}$ covers whole $\mathcal{P}(n)$, and Eq. (F.59) proves the statement.

Problem 6.10 We start with the quantum circuit

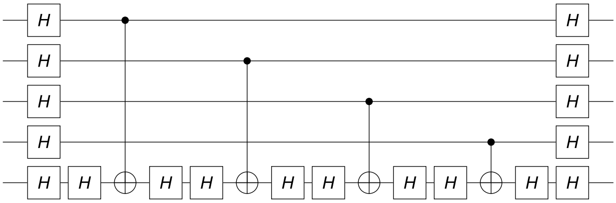


(F.60)

where the states $|x'\rangle$ with $x = 0, 1$ are defined by

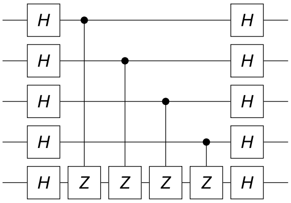
$$|0'\rangle \equiv |+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1'\rangle \equiv |-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{F.61}$$

As $\hat{H}^2 = \hat{I}$, it is equivalent to the following quantum circuit



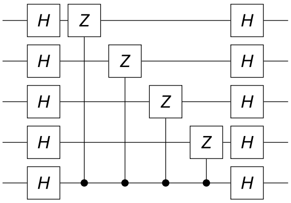
(F.62)

Now we use the identity in Eq. (2.44) to get



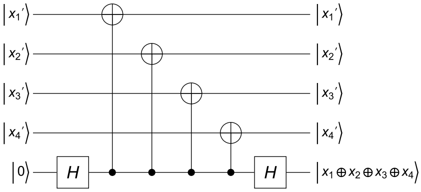
(F.63)

Since CZ gates are symmetric about control and target qubits, the above quantum circuit is equivalent to the following



(F.64)

Finally, we use the identity in Eq. (2.44) again to arrive at the following quantum circuit



(F.65)

F.7 Quantum Information Theory

Problem 7.2 Since N_{typical} is a huge number for large n, it is convenient to tame it with the logarithm function,

$$\log N_{\text{typical}} \approx \log n! - \log (np)! - \log (n - np)!. \tag{F.66}$$

Using *Stirling's approximation*, $\log x! \approx x \log x - x$, we obtain

$$\log N_{\text{typical}} \approx n\left[-p\log p - (1-p)\log(1-p)\right] = nH(\{p, 1-p\}). \tag{F.67}$$

Problem 7.3 Consider the spectral decompositions of $\hat{A}$ and $\hat{B}$,

$$\hat{A} = \sum_i |\alpha_i\rangle\, a_i\, \langle\alpha_i| \ , \quad \hat{B} = \sum_j \left|\beta_j\right\rangle b_j \left\langle\beta_j\right| \ . \tag{F.68}$$

For later use, define

$$P_{ij} := \left|\langle\alpha_i|\beta_j\rangle\right|^2 . \tag{F.69}$$

Note that P_{ij} are *doubly stochastic*, that is,

$$0 \le P_{ij} \le 1\, , \quad \sum_i P_{ij} = \sum_j P_{ij} = 1. \tag{F.70}$$

As $f(x)$ is convex, one has the inequalities

$$\sum_i f(a_i)P_{ij} \ge f(\textstyle\sum_i a_i P_{ij}) \ge f(b_j) + f'(b_j)\left(\displaystyle\sum_i a_i P_{ij} - b_j\right). \tag{F.71}$$

The first inequality is by the definition of a convex function, and the second follows from the property (7.95). Now note that

$$\sum_j \sum_i f(a_i) P_{ij} = \sum_i f(a_i) \sum_j P_{ij} = \sum_i f(a_i) = \mathrm{Tr} f(\hat{A})\, , \tag{F.72}$$

$$\sum_j f'(b_j) \sum_{ij} a_i P_{ij} = \sum_{ij} f'(b_j)\langle\beta_j|\alpha_i\rangle a_i \langle\alpha_i|\beta_j\rangle = \mathrm{Tr} f'(\hat{B})\hat{A}. \tag{F.73}$$

Therefore, the summation over j of both sides of (F.71) proves the inequality.

Problem 7.5 We use Klein's inequality (7.52) with $\hat{\rho} = \hat{\rho}_{AB}$ and $\hat{\sigma} = \hat{\rho}_A \otimes \hat{\rho}_B$. We observe that

$$\begin{aligned} S(\hat{\rho}_{AB}) &\le -\mathrm{Tr}\hat{\rho}\log\hat{\sigma} \\ &= -\mathrm{Tr}\hat{\rho}_{AB}\left(\log\hat{\rho}_A + \log\hat{\rho}_B\right) \\ &= -\mathrm{Tr}\hat{\rho}_A \log\hat{\rho}_A - \mathrm{Tr}\hat{\rho}_B \log\hat{\rho}_B \\ &= S(\hat{\rho}_A) + S(\hat{\rho}_B) \end{aligned} \tag{F.74}$$

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.

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 Stoß"vorgänge. *Zeitschriftfür Physik, 37*(12), 863.

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7

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.

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.

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.

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.

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.

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.

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. arXiv: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.

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.

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.

Gottesman, D. (1997). *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, California Institute of Technology, Pasadena, California. arXiv: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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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. arXiv: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.

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.

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.

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.

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.

Pérez-García, D., Wolf, M. M., Petz, D., & Ruskai, M. B. (2006). Contractivity of positive and trace-preserving maps under Lp norms. *Journal of Mathematical Physics, 47*(8), 083506. https://doi.org/10.1063/1.2218675. arXiv: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.

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.

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.

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.

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.

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.

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.

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.

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. arXiv: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

M.-S. Choi, *A Quantum Computation Workbook*,
https://doi.org/10.1007/978-3-030-91214-7