CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

1

Mathematical Preliminaries

This chapter is intended to serve as a review of mathematical concepts to be used throughout this book, and also as a reference to be consulted as subsequent chapters are studied, if the need should arise. The first section focuses on linear algebra, and the second on analysis and related topics. Unlike the other chapters in this book, the present chapter does not include proofs, and is not intended to serve as a primary source for the material it reviews – a collection of references provided at the end of the chapter may be consulted by readers interested in a proper development of this material.

1.1 Linear Algebra

The theory of quantum information relies heavily on linear algebra in finite-dimensional spaces. The subsections that follow present an overview of the aspects of this subject that are most relevant within the theory of quantum information. It is assumed that the reader is already familiar with the most basic notions of linear algebra, including those of linear dependence and independence, subspaces, spanning sets, bases, and dimension.

1.1.1 Complex Euclidean Spaces

The notion of a complex Euclidean space is used throughout this book. One associates a complex Euclidean space with every discrete and finite system; and fundamental notions such as states and measurements of systems are represented in linear-algebraic terms that refer to these spaces.

Definition of Complex Euclidean Spaces

An *alphabet* is a finite and nonempty set, whose elements may be considered to be *symbols*. Alphabets will generally be denoted by capital Greek letters,

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

including Σ, Γ, and Λ, while lower-case Roman letters near the beginning of the alphabet, including a, b, c, and d, will be used to denote symbols in alphabets. Examples of alphabets include the *binary alphabet* $\{0,1\}$, the n-fold Cartesian product $\{0,1\}^n$ of the binary alphabet with itself, and the alphabet $\{1,\ldots,n\}$, for n being a fixed positive integer.

For any alphabet Σ, one denotes by $\mathbb{C}^\Sigma$ the set of all functions from Σ to the complex numbers $\mathbb{C}$. The set $\mathbb{C}^\Sigma$ forms a vector space of dimension $|\Sigma|$ over the complex numbers when addition and scalar multiplication are defined in the following standard way:

1. Addition: for vectors $u, v \in \mathbb{C}^\Sigma$, the vector $u + v \in \mathbb{C}^\Sigma$ is defined by the equation $(u+v)(a) = u(a) + v(a)$ for all $a \in \Sigma$.
2. Scalar multiplication: for a vector $u \in \mathbb{C}^\Sigma$ and a scalar $\alpha \in \mathbb{C}$, the vector $\alpha u \in \mathbb{C}^\Sigma$ is defined by the equation $(\alpha u)(a) = \alpha u(a)$ for all $a \in \Sigma$.

A vector space defined in this way will be called a *complex Euclidean space*.[1] The value $u(a)$ is referred to as the *entry* of u indexed by a, for each $u \in \mathbb{C}^\Sigma$ and $a \in \Sigma$. The vector whose entries are all zero is simply denoted 0.

Complex Euclidean spaces will be denoted by scripted capital letters near the end of the alphabet, such as $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. Subsets of these spaces will also be denoted by scripted letters, and when possible this book will follow a convention to use letters such as $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ near the beginning of the alphabet when these subsets are not necessarily vector spaces. Vectors will be denoted by lower-case Roman letters, again near the end of the alphabet, such as u, v, w, x, y, and z.

When n is a positive integer, one typically writes $\mathbb{C}^n$ rather than $\mathbb{C}^{\{1,\ldots,n\}}$, and it is also typical that one views a vector $u \in \mathbb{C}^n$ as an n-tuple of the form $u = (\alpha_1, \ldots, \alpha_n)$, or as a column vector of the form

$$u = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \tag{1.1}$$

for complex numbers $\alpha_1, \ldots, \alpha_n$.

For an arbitrary alphabet Σ, the complex Euclidean space $\mathbb{C}^\Sigma$ may be viewed as being equivalent to $\mathbb{C}^n$ for $n = |\Sigma|$; one simply fixes a bijection

$$f\colon \{1,\ldots,n\} \rightarrow \Sigma \tag{1.2}$$

and associates each vector $u \in \mathbb{C}^\Sigma$ with the vector in $\mathbb{C}^n$ whose k-th entry

[1] Many quantum information theorists prefer to use the term *Hilbert space*. The term *complex Euclidean space* will be preferred in this book, however, as the term *Hilbert space* refers to a more general notion that allows the possibility of infinite index sets.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

is $u(f(k))$, for each $k \in \{1, \ldots, n\}$. This may be done implicitly when there is a natural or obviously preferred choice for the bijection f. For example, the elements of the alphabet $\Sigma = \{0,1\}^2$ are naturally ordered 00, 01, 10, 11. Each vector $u \in \mathbb{C}^\Sigma$ may therefore be associated with the 4-tuple

$$(u(00), u(01), u(10), u(11)), \tag{1.3}$$

or with the column vector

$$\begin{pmatrix} u(00) \\ u(01) \\ u(10) \\ u(11) \end{pmatrix}, \tag{1.4}$$

when it is convenient to do this. While little or no generality would be lost in restricting one's attention to complex Euclidean spaces of the form $\mathbb{C}^n$ for this reason, it is both natural and convenient within computational and information-theoretic settings to allow complex Euclidean spaces to be indexed by arbitrary alphabets.

Inner Products and Norms of Vectors

The *inner product* $\langle u, v \rangle$ of two vectors $u, v \in \mathbb{C}^\Sigma$ is defined as

$$\langle u, v \rangle = \sum_{a \in \Sigma} \overline{u(a)}\, v(a). \tag{1.5}$$

It may be verified that the inner product satisfies the following properties:

1. Linearity in the second argument:

$$\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle \tag{1.6}$$

   for all $u, v, w \in \mathbb{C}^\Sigma$ and $\alpha, \beta \in \mathbb{C}$.
2. Conjugate symmetry:

$$\langle u, v \rangle = \overline{\langle v, u \rangle} \tag{1.7}$$

   for all $u, v \in \mathbb{C}^\Sigma$.
3. Positive definiteness:

$$\langle u, u \rangle \geq 0 \tag{1.8}$$

   for all $u \in \mathbb{C}^\Sigma$, with equality if and only if $u = 0$.

It is typical that any function satisfying these three properties is referred to as an inner product, but this is the only inner product for vectors in complex Euclidean spaces that is considered in this book.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

The *Euclidean norm* of a vector $u \in \mathbb{C}^\Sigma$ is defined as

$$\|u\| = \sqrt{\langle u, u\rangle} = \sqrt{\sum_{a\in\Sigma} |u(a)|^2}. \tag{1.9}$$

The Euclidean norm possesses the following properties, which define the more general notion of a norm:

1. Positive definiteness: $\|u\| \geq 0$ for all $u \in \mathbb{C}^\Sigma$, with $\|u\| = 0$ if and only if $u = 0$.
2. Positive scalability: $\|\alpha u\| = |\alpha| \|u\|$ for all $u \in \mathbb{C}^\Sigma$ and $\alpha \in \mathbb{C}$.
3. The triangle inequality: $\|u + v\| \leq \|u\| + \|v\|$ for all $u, v \in \mathbb{C}^\Sigma$.

The *Cauchy–Schwarz inequality* states that

$$|\langle u, v\rangle| \leq \|u\| \, \|v\| \tag{1.10}$$

for all $u, v \in \mathbb{C}^\Sigma$, with equality if and only if u and v are linearly dependent. The collection of all unit vectors in a complex Euclidean space $\mathcal{X}$ is called the *unit sphere* in that space, and is denoted

$$\mathcal{S}(\mathcal{X}) = \{u \in \mathcal{X} \colon \|u\| = 1\}. \tag{1.11}$$

The Euclidean norm represents the case $p = 2$ of the class of *p-norms*, defined for each $u \in \mathbb{C}^\Sigma$ as

$$\|u\|_p = \biggl(\sum_{a\in\Sigma} |u(a)|^p\biggr)^{\frac{1}{p}} \tag{1.12}$$

for $p < \infty$, and

$$\|u\|_\infty = \max\{|u(a)| \colon a \in \Sigma\}. \tag{1.13}$$

The above three norm properties (positive definiteness, positive scalability, and the triangle inequality) hold for $\|\cdot\|$ replaced by $\|\cdot\|_p$ for any choice of $p \in [1, \infty]$.

Orthogonality and Orthonormality

Two vectors $u, v \in \mathbb{C}^\Sigma$ are said to be *orthogonal* if $\langle u, v\rangle = 0$. The notation $u \perp v$ is also used to indicate that u and v are orthogonal. More generally, for any set $\mathcal{A} \subseteq \mathbb{C}^\Sigma$, the notation $u \perp \mathcal{A}$ indicates that $\langle u, v\rangle = 0$ for all vectors $v \in \mathcal{A}$.

A collection of vectors

$$\{u_a \colon a \in \Gamma\} \subset \mathbb{C}^\Sigma, \tag{1.14}$$

indexed by an alphabet Γ, is said to be an *orthogonal set* if it holds that

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

$\langle u_a, u_b \rangle = 0$ for all choices of $a, b \in \Gamma$ with $a \neq b$. A collection of nonzero orthogonal vectors is necessarily linearly independent.

An orthogonal set of *unit* vectors is called an *orthonormal set*, and when such a set forms a basis it is called an *orthonormal basis*. It holds that an orthonormal set of the form (1.14) is an orthonormal basis of $\mathbb{C}^\Sigma$ if and only if $|\Gamma| = |\Sigma|$. The *standard basis* of $\mathbb{C}^\Sigma$ is the orthonormal basis given by $\{e_a : a \in \Sigma\}$, where

$$e_a(b) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases} \tag{1.15}$$

for all $a, b \in \Sigma$.

Direct Sums of Complex Euclidean Spaces

The *direct sum* of n complex Euclidean spaces $\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n}$ is the complex Euclidean space

$$\mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n = \mathbb{C}^{\Sigma_1 \sqcup \cdots \sqcup \Sigma_n}, \tag{1.16}$$

where $\Sigma_1 \sqcup \cdots \sqcup \Sigma_n$ denotes the *disjoint union* of the alphabets $\Sigma_1, \ldots, \Sigma_n$, defined as

$$\Sigma_1 \sqcup \cdots \sqcup \Sigma_n = \bigcup_{k \in \{1,\ldots,n\}} \{(k, a) : a \in \Sigma_k\}. \tag{1.17}$$

For vectors $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$, the notation $u_1 \oplus \cdots \oplus u_n \in \mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n$ refers to the vector for which

$$(u_1 \oplus \cdots \oplus u_n)(k, a) = u_k(a), \tag{1.18}$$

for each $k \in \{1, \ldots, n\}$ and $a \in \Sigma_k$. If each u_k is viewed as a column vector of dimension $|\Sigma_k|$, the vector $u_1 \oplus \cdots \oplus u_n$ may be viewed as a column vector

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \tag{1.19}$$

having dimension $|\Sigma_1| + \cdots + |\Sigma_n|$.

Every element of the space $\mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n$ can be written as $u_1 \oplus \cdots \oplus u_n$ for a unique choice of vectors $u_1, \ldots, u_n$. The following identities hold for

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

every choice of $u_1, v_1 \in \mathcal{X}_1, \ldots, u_n, v_n \in \mathcal{X}_n$, and $\alpha \in \mathbb{C}$:

$$u_1 \oplus \cdots \oplus u_n + v_1 \oplus \cdots \oplus v_n = (u_1 + v_1) \oplus \cdots \oplus (u_n + v_n), \tag{1.20}$$

$$\alpha(u_1 \oplus \cdots \oplus u_n) = (\alpha u_1) \oplus \cdots \oplus (\alpha u_n), \tag{1.21}$$

$$\langle u_1 \oplus \cdots \oplus u_n, v_1 \oplus \cdots \oplus v_n \rangle = \langle u_1, v_1 \rangle + \cdots + \langle u_n, v_n \rangle. \tag{1.22}$$

Tensor Products of Complex Euclidean Spaces

The *tensor product* of n complex Euclidean spaces $\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n}$ is the complex Euclidean space

$$\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n = \mathbb{C}^{\Sigma_1 \times \cdots \times \Sigma_n}. \tag{1.23}$$

For vectors $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$, the notation $u_1 \otimes \cdots \otimes u_n \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ refers to the vector for which

$$(u_1 \otimes \cdots \otimes u_n)(a_1, \ldots, a_n) = u_1(a_1) \cdots u_n(a_n). \tag{1.24}$$

Vectors of the form $u_1 \otimes \cdots \otimes u_n$ are called *elementary tensors*. They span the space $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$, but not every element of $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ is an elementary tensor.

The following identities hold for all vectors $u_1, v_1 \in \mathcal{X}_1, \ldots, u_n, v_n \in \mathcal{X}_n$, scalars $\alpha, \beta \in \mathbb{C}$, and indices $k \in \{1, \ldots, n\}$:

$$\begin{aligned} & u_1 \otimes \cdots \otimes u_{k-1} \otimes (\alpha u_k + \beta v_k) \otimes u_{k+1} \otimes \cdots \otimes u_n \\ & \quad = \alpha\, (u_1 \otimes \cdots \otimes u_{k-1} \otimes u_k \otimes u_{k+1} \otimes \cdots \otimes u_n) \\ & \quad\quad + \beta\, (u_1 \otimes \cdots \otimes u_{k-1} \otimes v_k \otimes u_{k+1} \otimes \cdots \otimes u_n), \end{aligned} \tag{1.25}$$

$$\langle u_1 \otimes \cdots \otimes u_n, v_1 \otimes \cdots \otimes v_n \rangle = \langle u_1, v_1 \rangle \cdots \langle u_n, v_n \rangle. \tag{1.26}$$

Tensor products are often defined in a way that is more abstract (and more generally applicable) than the definition above, which is sometimes known more specifically as the *Kronecker product*. The following proposition is a reflection of the more abstract definition.

Proposition 1.1 *Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}$ be complex Euclidean spaces and let*

$$\phi\colon \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \rightarrow \mathcal{Y} \tag{1.27}$$

be a multilinear function, meaning a function for which the mapping

$$u_k \mapsto \phi(u_1, \ldots, u_n) \tag{1.28}$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

is linear for all $k \in \{1, \dots, n\}$ *and every fixed choice of vectors* $u_1, \dots, u_{k-1}$, $u_{k+1}, \dots, u_n$. *There exists a unique linear mapping*

$$A \colon \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \to \mathcal{Y} \tag{1.29}$$

such that

$$\phi(u_1, \dots, u_n) = A(u_1 \otimes \cdots \otimes u_n) \tag{1.30}$$

for all choices of $u_1 \in \mathcal{X}_1, \dots, u_n \in \mathcal{X}_n$.

If $\mathcal{X}$ is a complex Euclidean space, $u \in \mathcal{X}$ is a vector, and n is a positive integer, then the notations $\mathcal{X}^{\otimes n}$ and $u^{\otimes n}$ refer to the n-fold tensor product of either $\mathcal{X}$ or u with itself. It is often convenient to make the identification

$$\mathcal{X}^{\otimes n} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \tag{1.31}$$

under the assumption that $\mathcal{X}_1, \dots, \mathcal{X}_n$ and $\mathcal{X}$ all refer to the same complex Euclidean space; this allows one to refer to the different tensor factors in $\mathcal{X}^{\otimes n}$ individually, and to express $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ more concisely.

Remark A rigid interpretation of the definitions above suggests that tensor products of complex Euclidean spaces (or of vectors in complex Euclidean spaces) are not associative, insofar as Cartesian products are not associative. For instance, given alphabets Σ, Γ, and Λ, the alphabet $(\Sigma \times \Gamma) \times \Lambda$ contains elements of the form $((a, b), c)$, the alphabet $\Sigma \times (\Gamma \times \Lambda)$ contains elements of the form $(a, (b, c))$, and the alphabet $\Sigma \times \Gamma \times \Lambda$ contains elements of the form (a, b, c), for $a \in \Sigma$, $b \in \Gamma$, and $c \in \Lambda$. For $\mathcal{X} = \mathbb{C}^\Sigma$, $\mathcal{Y} = \mathbb{C}^\Gamma$, and $\mathcal{Z} = \mathbb{C}^\Lambda$, one may therefore view the complex Euclidean spaces $(\mathcal{X} \otimes \mathcal{Y}) \otimes \mathcal{Z}$, $\mathcal{X} \otimes (\mathcal{Y} \otimes \mathcal{Z})$, and $\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$ as being different.

However, the alphabets $(\Sigma \times \Gamma) \times \Lambda$, $\Sigma \times (\Gamma \times \Lambda)$, and $\Sigma \times \Gamma \times \Lambda$ can of course be viewed as equivalent by simply removing parentheses. For this reason, there is a natural equivalence between the complex Euclidean spaces $(\mathcal{X} \otimes \mathcal{Y}) \otimes \mathcal{Z}$, $\mathcal{X} \otimes (\mathcal{Y} \otimes \mathcal{Z})$, and $\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$. Whenever it is convenient, identifications of this sort are made implicitly throughout this book. For example, given vectors $u \in \mathcal{X} \otimes \mathcal{Y}$ and $v \in \mathcal{Z}$, the vector $u \otimes v$ may be treated as an element of $\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$ rather than $(\mathcal{X} \otimes \mathcal{Y}) \otimes \mathcal{Z}$.

Although such instances are much less common in this book, a similar convention applies to direct sums of complex Euclidean spaces.

Real Euclidean Spaces

Real Euclidean spaces are defined in a similar way to complex Euclidean spaces, except that the field of complex numbers $\mathbb{C}$ is replaced by the field of real numbers $\mathbb{R}$ in each of the definitions and concepts in which it arises.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

Naturally, complex conjugation acts trivially in the real case, and therefore may be omitted.

Complex Euclidean spaces will play a more prominent role than real ones in this book. Real Euclidean spaces will, nevertheless, be important in those settings that make use of concepts from the theory of convexity. The space of Hermitian operators acting on a given complex Euclidean space is an important example of a real vector space that can be identified with a real Euclidean space, as is discussed in the subsection following this one.

1.1.2 Linear Operators

Given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, one writes $\mathrm{L}(\mathcal{X},\mathcal{Y})$ to refer to the collection of all linear mappings of the form

$$A\colon \mathcal{X} \rightarrow \mathcal{Y}. \tag{1.32}$$

Such mappings will be referred to as *linear operators*, or simply *operators*, from $\mathcal{X}$ to $\mathcal{Y}$ in this book. Parentheses are omitted when expressing the action of linear operators on vectors when no confusion arises in doing so. For instance, one writes Au rather than $A(u)$ to denote the vector resulting from the application of an operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ to a vector $u \in \mathcal{X}$.

The set $\mathrm{L}(\mathcal{X},\mathcal{Y})$ forms a complex vector space when addition and scalar multiplication are defined as follows:

1. Addition: for operators $A, B \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, the operator $A + B \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ is defined by the equation

$$(A + B)u = Au + Bu \tag{1.33}$$

for all $u \in \mathcal{X}$.

2. Scalar multiplication: for an operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ and a scalar $\alpha \in \mathbb{C}$, the operator $\alpha A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ is defined by the equation

$$(\alpha A)u = \alpha A u \tag{1.34}$$

for all $u \in \mathcal{X}$.

Matrices and Their Correspondence with Operators

A *matrix* over the complex numbers is a mapping of the form

$$M : \Gamma \times \Sigma \rightarrow \mathbb{C} \tag{1.35}$$

for alphabets Σ and Γ. For $a \in \Gamma$ and $b \in \Sigma$ the value $M(a, b)$ is called the (a, b) *entry* of M, and the elements a and b are referred to as *indices* in this

© in this web service Cambridge University Press www.cambridge.org

context: a is the *row index* and b is the *column index* of the entry $M(a,b)$. Addition and scalar multiplication of matrices are defined in a similar way to vectors in complex Euclidean spaces:

1. Addition: for matrices $M : \Gamma \times \Sigma \to \mathbb{C}$ and $N : \Gamma \times \Sigma \to \mathbb{C}$, the matrix $M + N$ is defined as
$$(M+N)(a,b) = M(a,b) + N(a,b) \tag{1.36}$$
for all $a \in \Gamma$ and $b \in \Sigma$.
2. Scalar multiplication: for a matrix $M : \Gamma \times \Sigma \to \mathbb{C}$ and a scalar $\alpha \in \mathbb{C}$, the matrix αM is defined as
$$(\alpha M)(a,b) = \alpha M(a,b) \tag{1.37}$$
for all $a \in \Gamma$ and $b \in \Sigma$.

In addition, one defines matrix multiplication as follows:

3. Matrix multiplication: for matrices $M : \Gamma \times \Lambda \to \mathbb{C}$ and $N : \Lambda \times \Sigma \to \mathbb{C}$, the matrix $MN : \Gamma \times \Sigma \to \mathbb{C}$ is defined as
$$(MN)(a,b) = \sum_{c \in \Lambda} M(a,c)N(c,b) \tag{1.38}$$
for all $a \in \Gamma$ and $b \in \Sigma$.

For any choice of complex Euclidean spaces $\mathcal{X} = \mathbb{C}^\Sigma$ and $\mathcal{Y} = \mathbb{C}^\Gamma$, there is a bijective linear correspondence between the set of operators $\mathrm{L}(\mathcal{X},\mathcal{Y})$ and the collection of all matrices taking the form $M : \Gamma \times \Sigma \to \mathbb{C}$ that is obtained as follows. With each operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, one associates the matrix M defined as
$$M(a,b) = \langle e_a, A e_b \rangle \tag{1.39}$$
for $a \in \Gamma$ and $b \in \Sigma$. The operator A is uniquely determined by M, and may be recovered from M by the equation
$$(Au)(a) = \sum_{b \in \Sigma} M(a,b)u(b) \tag{1.40}$$
for all $a \in \Gamma$. With respect to this correspondence, matrix multiplication is equivalent to operator composition.

Hereafter in this book, linear operators will be associated with matrices implicitly, without the introduction of names that distinguish matrices from the operators with which they are associated. With this in mind, the notation
$$A(a,b) = \langle e_a, A e_b \rangle \tag{1.41}$$

© in this web service Cambridge University Press

CAMBRIDGE

Cambridge University Press
978-1-107-18056-7 — The Theory of Quantum Information
John Watrous
Excerpt
More Information

is introduced for each $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, $a \in \Gamma$, and $b \in \Sigma$ (where it is to be assumed that $\mathcal{X} = \mathbb{C}^\Sigma$ and $\mathcal{Y} = \mathbb{C}^\Gamma$, as above).

The Standard Basis of a Space of Operators

For every choice of complex Euclidean spaces $\mathcal{X} = \mathbb{C}^\Sigma$ and $\mathcal{Y} = \mathbb{C}^\Gamma$, and each choice of symbols $a \in \Gamma$ and $b \in \Sigma$, the operator $E_{a,b} \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ is defined as

$$E_{a,b}\, u = u(b) e_a \tag{1.42}$$

for every $u \in \mathcal{X}$. Equivalently, $E_{a,b}$ is defined by the equation

$$E_{a,b}(c,d) = \begin{cases} 1 & \text{if } (c,d) = (a,b) \\ 0 & \text{otherwise} \end{cases} \tag{1.43}$$

holding for all $c \in \Gamma$ and $d \in \Sigma$. The collection

$$\{E_{a,b} : a \in \Gamma,\; b \in \Sigma\} \tag{1.44}$$

forms a basis of $\mathrm{L}(\mathcal{X},\mathcal{Y})$ known as the *standard basis* of this space. The number of elements in this basis is, of course, consistent with the fact that the dimension of $\mathrm{L}(\mathcal{X},\mathcal{Y})$ is given by $\dim(\mathrm{L}(\mathcal{X},\mathcal{Y})) = \dim(\mathcal{X}) \dim(\mathcal{Y})$.

The Entry-Wise Conjugate, Transpose, and Adjoint

For every operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, for complex Euclidean spaces $\mathcal{X} = \mathbb{C}^\Sigma$ and $\mathcal{Y} = \mathbb{C}^\Gamma$, one defines three additional operators,

$$\overline{A} \in \mathrm{L}(\mathcal{X},\mathcal{Y}) \quad \text{and} \quad A^{\mathsf{T}}, A^* \in \mathrm{L}(\mathcal{Y},\mathcal{X}), \tag{1.45}$$

as follows:

1. The operator $\overline{A} \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ is the operator whose matrix representation has entries that are complex conjugates to the matrix representation of A:

$$\overline{A}(a,b) = \overline{A(a,b)} \tag{1.46}$$

   for all $a \in \Gamma$ and $b \in \Sigma$.
2. The operator $A^{\mathsf{T}} \in \mathrm{L}(\mathcal{Y},\mathcal{X})$ is the operator whose matrix representation is obtained by *transposing* the matrix representation of A:

$$A^{\mathsf{T}}(b,a) = A(a,b) \tag{1.47}$$

   for all $a \in \Gamma$ and $b \in \Sigma$.

© in this web service Cambridge University Press www.cambridge.org