Appendix A
Linear Algebra for Quantum Computation

The purpose of this appendix is to compile the definitions, notations, and facts of linear algebra that are important for this book. This appendix also serves as a quick reference for the main operations in vector spaces, for instance, the *inner* and *tensor products*. Quantum computation inherited linear algebra from quantum mechanics as the supporting language for describing this area. Therefore, it is essential to have a solid knowledge of the basic results of linear algebra to understand quantum computation and quantum algorithms. If the reader does not have this base knowledge, we suggest reading some of the basic references recommended at the end of this appendix.

A.1 Vector Spaces

A *vector space* V over the field of complex numbers $\mathbb{C}$ is a non-empty set of elements called vectors. In V, it is defined the operations of vector addition and multiplication of a vector by a scalar in $\mathbb{C}$. The addition operation is associative and commutative. It also obeys properties

- There is an element $\mathbf{0} \in V$, such that, for each $\mathbf{v} \in V$, $\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}$ (existence of neutral element)
- For each $\mathbf{v} \in V$, there exists $\mathbf{u} = (-1)\mathbf{v}$ in V such that $\mathbf{v} + \mathbf{u} = \mathbf{0}$ (existence of inverse element)

$\mathbf{0}$ is called zero vector. The scalar multiplication operation obeys properties

- $a.(b.\mathbf{v}) = (a.b).\mathbf{v}$ (associativity)
- $1.\mathbf{v} = \mathbf{v}$ (1 is the neutral element of multiplication)
- $(a + b).\mathbf{v} = a.\mathbf{v} + b.\mathbf{v}$ (distributivity of sum of scalars)
- $a.(\mathbf{v} + \mathbf{w}) = a.\mathbf{v} + a.\mathbf{w}$ (distributivity in V)

where $\mathbf{v}, \mathbf{w} \in V$ and $a, b \in \mathbb{C}$.

R. Portugal, *Quantum Walks and Search Algorithms*, Quantum Science and Technology, DOI 10.1007/978-1-4614-6336-8,

A vector space can be infinite, but in most applications in *quantum computation*, *finite vector spaces* are used and are denoted by $\mathbb{C}^n$. In this case, the vectors have n complex entries. In this book, we rarely use infinite spaces, and in these few cases, we are interested only in finite subspaces. In the context of *quantum mechanics*, *infinite vector spaces* are used more frequently than finite spaces.

A *basis* for $\mathbb{C}^n$ consists of exactly n linearly independent vectors. If $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis for $\mathbb{C}^n$, then a generic vector $\mathbf{v}$ can be written as

$$\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{v}_i,$$

where coefficients a_i are complex numbers. The *dimension* of a vector space is the number of basis vectors.

A.2 Inner Product

The *inner product* is a binary operation $(\cdot, \cdot) : V \times V \mapsto \mathbb{C}$, which obeys the following properties:

1. $(\cdot, \cdot)$ is linear in the second argument

$$\left(\mathbf{v}, \sum_{i=1}^{n} a_i \mathbf{v}_i\right) = \sum_{i=1}^{n} a_i \,(\mathbf{v}, \mathbf{v}_i).$$

2. $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_2, \mathbf{v}_1)^*$.
3. $(\mathbf{v}, \mathbf{v}) \geq 0$. The equality holds if and only if $\mathbf{v} = \mathbf{0}$.

In general, the inner product is not linear in the first argument. The property in question is called *conjugate-linear*.

There is more than one way to define an inner product on a vector space. In $\mathbb{C}^n$, the most used inner product is defined as follows: If

$$\mathbf{v} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \quad \mathbf{w} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix},$$

then

$$(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^{n} a_i^* b_i.$$

This expression is equivalent to the matrix product of the transpose-conjugate vector, which is usually denoted by $\mathbf{v}^\dagger$, by $\mathbf{w}$.

If an inner product is introduced in a vector space, we can define the notion of orthogonality. Two vectors are *orthogonal* if the inner product is zero. We also introduce the notion of *norm* using the inner product. The norm of $\mathbf{v}$, denoted by $\|\mathbf{v}\|$, is defined as

$$\|\mathbf{v}\| = \sqrt{(\mathbf{v}, \mathbf{v})}.$$

A *normalized vector* or *unit vector* is a vector whose norm is equal to 1. A basis is said *orthonormal* if all vectors are normalized and mutually orthogonal.

A finite vector space with an inner product is called a *Hilbert space*. In order to an infinite vector space be a Hilbert space, it must obey additional properties besides having an inner product. Since we will deal primarily with finite vector spaces, we use the term *Hilbert space* as a synonym for *vector space with an inner product*. A *subspace* W of a finite Hilbert space V is also a Hilbert space. The set of vectors orthogonal to all vectors of W is the Hilbert space $W^{\perp}$ called *orthogonal complement*. V is the direct sum of W and $W^{\perp}$, that is, $V = W \oplus W^{\perp}$. An N-dimensional Hilbert space will be denoted by $\mathcal{H}^N$ to highlight its dimension. A Hilbert space associated with a system A will be denoted by $\mathcal{H}_A$.

A.3 The Dirac Notation

In this review of linear algebra, we will systematically be using the *Dirac* or *bra-ket notation*, which was introduced by the English physicist Paul Dirac in the context of quantum mechanics to aid algebraic manipulations. This notation is very simple. Several notations are used for vectors, such as $\mathbf{v}$ and $\vec{v}$. The Dirac notation uses

$$\mathbf{v} \equiv |v\rangle.$$

Up to this point, instead of using bold or putting an arrow over letter v, we put letter v between a vertical bar and a right angle bracket. If we have an indexed basis, that is, $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, in the Dirac notation we use the form $\{|v_1\rangle, \dots, |v_n\rangle\}$ or $\{|1\rangle, \dots, |n\rangle\}$. Note that if we are using a single basis, letter $\mathbf{v}$ is unnecessary in principle. Computer scientists usually start counting from 0. So, the first basis vector is usually called $\mathbf{v}_0$. In the Dirac notation we have

$$\mathbf{v}_0 \equiv |0\rangle.$$

Vector $|0\rangle$ is not the zero vector, it is only the first vector in a collection of vectors. In the Dirac notation, the zero vector is an exception, whose notation is not modified. Here we use the notation $\mathbf{0}$.

Suppose that vector $|v\rangle$ has the following entries in a basis

$$|v\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

The dual vector is denoted by $\langle v|$ and is defined by

$$\langle v| = \left[a_1^* \cdots a_n^*\right].$$

Usual vectors and their duals can be seen as column and row matrices, respectively, for algebraic manipulation. The matrix product of $\langle v|$ by $|v\rangle$ is denoted by $\langle v|v\rangle$ and its value in terms of their entries is

$$\langle v|v\rangle = \sum_{i=1}^{n} a_i^* a_i .$$

This is an example of an inner product, which is naturally defined via the Dirac notation. If $\{|v_1\rangle, \ldots, |v_n\rangle\}$ is an orthonormal basis, then

$$\langle v_i|v_j\rangle = \delta_{ij},$$

where δ_{ij} is the *Kronecker delta*. The norm of a vector in this notation is

$$\| |v\rangle \| = \sqrt{\langle v|v\rangle}.$$

We use the terminology *ket* for vector $|v\rangle$ and *bra* for dual vector $\langle v|$. Keeping consistency, we use the terminology *bra-ket* for $\langle v|v\rangle$.

It is also very common to meet the matrix product of $|v\rangle$ by $\langle v|$, denoted by $|v\rangle\langle v|$, known as the *outer product*, whose result is an $n \times n$ matrix

$$\begin{aligned} |v\rangle\langle v| &= \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \cdot \left[a_1^* \cdots a_n^*\right] \\ &= \begin{bmatrix} a_1 a_1^* & \cdots & a_1 a_n^* \\ & \ddots & \\ a_n a_1^* & \cdots & a_n a_n^* \end{bmatrix}. \end{aligned}$$

The key to the Dirac notation is to always view *kets* as column matrices, *bras* as row matrices, and recognize that a sequence of *bras* and *kets* is a matrix product, hence associative, but non-commutative.

A.4 Computational Basis

The *computational basis* of $\mathbb{C}^n$, denoted by $\{|0\rangle, \ldots, |n-1\rangle\}$, is given by

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad |n-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}. \Big\} (n-1)$$

This basis is also known as *canonical basis*. A few times we will use the numbering of the computational basis beginning with $|1\rangle$ and ending with $|n\rangle$. In this book, when we use a small-caption *Latin letter* within a *ket* or *bra*, we are referring to the computational basis. Then, the following expression will always be valid

$$\langle i | j \rangle = \delta_{ij}.$$

The normalized sum of all computational basis vectors defines vector

$$|\mathrm{D}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle,$$

which we will call *diagonal state*. When $n = 2$, the diagonal state is given by $|\mathrm{D}\rangle = |+\rangle$ where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Exercise A.1. Explicitly calculate the values of $|i\rangle\langle j|$ and

$$\sum_{i=0}^{n-1} |i\rangle\langle i|$$

in $\mathbb{C}^3$.

A.5 Qubit and the Bloch Sphere

The *qubit* is a *unit vector* in vector space $\mathbb{C}^2$. A generic qubit $|\psi\rangle$ is represented by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle,$$

where coefficients α and β are complex numbers and obey the constraint

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

The set $\{|0\rangle, |1\rangle\}$ is the computational basis of $\mathbb{C}^2$ and α, β are called amplitudes of state $|\psi\rangle$. The term *state* (or *state vector*) is used as a synonym for *unit vector in a Hilbert space*.

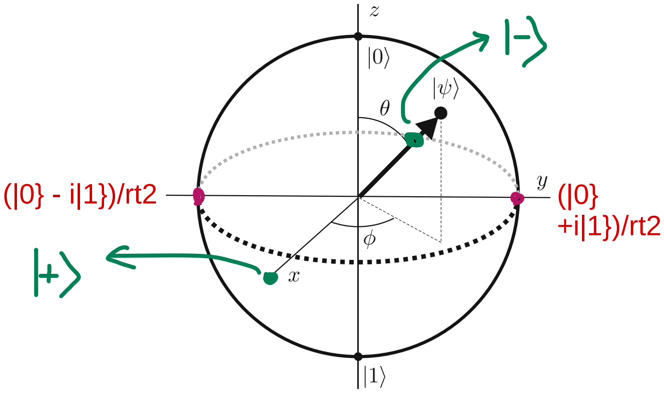

Fig. A.1 Bloch Sphere. The state $|\psi\rangle$ of a qubit is represented by a point on the sphere

In principle, we need four real numbers to describe a qubit, two for α and two for β. The constraint $|\alpha|^2 + |\beta|^2 = 1$ reduces to three numbers. In quantum mechanics, two vectors that differ from a *global phase factor* are considered equivalent. A global phase factor is a complex number of unit modulus multiplying the state. By eliminating this factor, a qubit can be described by two real numbers θ and ϕ as follows:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle,$$

where $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$. In the above notation, state $|\psi\rangle$ can be represented by a point on the surface of a sphere of unit radius, called *Bloch sphere*. Numbers θ and ϕ are spherical angles that locate the point that describes $|\psi\rangle$, as shown in Fig. A.1. The vector showed there is given by

$$\begin{bmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{bmatrix}.$$

When we disregard global phase factors, there is a one-to-one correspondence between the quantum states of a qubit and the points on the Bloch sphere. State $|0\rangle$ is in the *north pole* of the sphere, because it is obtained by taking $\theta = 0$. State $|1\rangle$ is in the *south pole*. States

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

$|+\rangle$ & $|-\rangle$ are the intersection points of the x-axis and the sphere, and states $(|0\rangle \pm i|1\rangle)/\sqrt{2}$ are the intersection points of the y-axis with the sphere.

The representation of *classical bits* in this context is given by the poles of the Bloch sphere and the representation of the *probabilistic classical bit*, that is, 0 with probability p and 1 with probability $1 - p$, is given by the point in z-axis with coordinate $2p - 1$. The interior of the Bloch sphere is used to describe the states of a qubit in the presence of *decoherence*.

Exercise A.2. Using the Dirac notation, show that opposite points in the Bloch sphere correspond to orthogonal states.

Exercise A.3. Suppose you know that a qubit is either is in state $|+\rangle$ with probability p or in state $|-\rangle$ with probability $1 - p$. If this is the best you know about the qubit's state, where in the Bloch sphere would you represent this qubit?

Exercise A.4. Does the outside of Bloch sphere play any role?

A.6 Linear Operators

Let V and W be vector spaces, $\{|v_1\rangle, \ldots, |v_n\rangle\}$ a basis for V, and $\mathcal{A}$ a function $\mathcal{A} : V \mapsto W$ that satisfies

$$\mathcal{A}\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i \mathcal{A}(|v_i\rangle),$$

for any complex numbers a_i. $\mathcal{A}$ is called a *linear operator* from V to W. The term *linear operator in* V means that both the domain and codomain of $\mathcal{A}$ is V. The composition of linear operators $\mathcal{A} : V_1 \mapsto V_2$ and $\mathcal{B} : V_2 \mapsto V_3$ is also a linear operator $\mathcal{C} : V_1 \mapsto V_3$ obtained through the composition of their functions: $\mathcal{C}(|v\rangle) = \mathcal{B}(\mathcal{A}(|v\rangle)$. The sum of two linear operators, both from V to W, is naturally defined by formula $(\mathcal{A} + \mathcal{B})(|v\rangle) = \mathcal{A}(|v\rangle) + \mathcal{B}(|v\rangle)$.

The identity operator $\mathcal{I}$ in V is a linear operator such that $\mathcal{I}(|v\rangle) = |v\rangle$ for all $|v\rangle \in V$. The null operator $\mathcal{O}$ in V is a linear operator such that $\mathcal{O}(|v\rangle) = \mathbf{0}$ for all $|v\rangle \in V$.

The *rank* of a linear operator $\mathcal{A}$ in V is the dimension of the image of $\mathcal{A}$. The *kernel* or *nullspace* of a linear operator $\mathcal{A}$ in V is the set of all vectors $|v\rangle$ for which $\mathcal{A}(|v\rangle) = \mathbf{0}$. The dimension of the kernel is called the *nullity* of the operator. The *rank-nullity theorem* states that rank $\mathcal{A}$ + nullity $\mathcal{A}$ = dim V.

Fact

If we specify the action of a linear operator on a basis of vector space V, its action on any vector in V can be straightforwardly determined.

A.7 Matrix Representation

Linear operators can be represented by matrices. Let $\mathcal{A} : V \mapsto W$ be a linear operator, $\{|v_1\rangle, \ldots, |v_n\rangle\}$ and $\{|w_1\rangle, \ldots, |w_m\rangle\}$ orthonormal bases for V and W, respectively. A *matrix representation* of $\mathcal{A}$ is obtained by applying $\mathcal{A}$ to every vector in the basis of V and expressing the result as a linear combination of basis vectors of W, as follows:

$$\mathcal{A}\left(\left|v_j\right\rangle\right) = \sum_{i=1}^{m} a_{ij}\,|w_i\rangle,$$

where index j run from 1 to n. Therefore, a_{ij} are entries of an $m \times n$ matrix, which we call A. In this case, expression $\mathcal{A}\left(\left|v_j\right\rangle\right)$, which means function $\mathcal{A}$ applied to argument $\left|v_j\right\rangle$, is equivalent to the matrix product $A\left|v_j\right\rangle$. Using the outer product notation, we have

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\,|w_i\rangle\langle v_j|.$$

Using the above equation and the fact that the basis of V is orthonormal, we can verify that the matrix product of A by $\left|v_j\right\rangle$ is equal to $\mathcal{A}\left(\left|v_j\right\rangle\right)$. The key to this calculation is to use the associativity of matrix multiplication:

$$\begin{aligned}\big(|w_i\rangle\langle v_j|\big)|v_k\rangle &= |w_i\rangle\big(\langle v_j|v_k\rangle\big)\\ &= \delta_{jk}|w_i\rangle.\end{aligned}$$

In particular, the matrix representation of the identity operator $\mathcal{I}$ in any orthonormal basis is the identity matrix I and the matrix representation of the null operator $\mathcal{O}$ in any orthonormal basis is the *zero matrix*.

If the linear operator $\mathcal{C}$ is the composition of the linear operators $\mathcal{B}$ and $\mathcal{A}$, the matrix representation of $\mathcal{C}$ will be obtained by multiplying the matrix representation of $\mathcal{B}$ with that of $\mathcal{A}$, that is, $C = BA$.

When we fix orthonormal bases for the vector spaces, there is a one-to-one correspondence between linear operators and matrices. In $\mathbb{C}^n$, we use the computational basis as a reference basis, so the terms *linear operator* and *matrix* are taken as synonyms. We will also use the term *operator* as a synonym for *linear operator*.

Exercise A.5. Suppose B is an operator whose action on the computational basis of the n-dimensional vector space V is

$$B|j\rangle = \left|\psi_j\right\rangle,$$

where $\left|\psi_j\right\rangle$ are vectors in V for all j.

1. Obtain the expression of B using the outer product.
2. Show that $\left|\psi_j\right\rangle$ is the j-th column in the matrix representation of B.

3. Suppose that B is the Hadamard operator

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

Redo the previous items using operator H.

A.8 Diagonal Representation

Let $\mathcal{O}$ be an operator in V. If there exists an orthonormal basis $\{|v_1\rangle, \ldots, |v_n\rangle\}$ of V such that

$$O = \sum_{i=1}^{n} \lambda_i |v_i\rangle\langle v_i|,$$

we say that $\mathcal{O}$ admits a *diagonal representation* or, equivalently, $\mathcal{O}$ is *diagonalizable*. The complex numbers λ_i are the *eigenvalues* of $\mathcal{O}$ and $|v_i\rangle$ are the corresponding *eigenvectors*. Any multiple of an eigenvector is also an eigenvector. If two eigenvectors are associated with the same eigenvalue, then any linear combination of these eigenvectors is an eigenvector. The number of linearly independent eigenvectors associated with the same eigenvalue is the *multiplicity* of that eigenvalue.

If there are eigenvalues with multiplicity greater than one, the diagonal representation can be factored out as follows:

$$O = \sum_{\lambda} \lambda P_\lambda,$$

where index λ runs only on the distinct eigenvalues and P_λ is the projector on the eigenspace of $\mathcal{O}$ associated with eigenvalue λ. If λ has multiplicity 1, $P_\lambda = |v\rangle\langle v|$, where $|v\rangle$ is the unit eigenvector associated with λ. If λ has multiplicity 2 and $|v_1\rangle, |v_2\rangle$ are linearly independent unit eigenvectors associated with λ, $P_\lambda = |v_1\rangle\langle v_1| + |v_2\rangle\langle v_2|$ and so on. The projectors P_λ satisfy

$$\sum_{\lambda} P_\lambda = I.$$

An alternative way to define a diagonalizable operator is by requiring that O is *similar* to a diagonal matrix. Matrices O and O' are similar if $O' = M^{-1}OM$ for some invertible matrix M. We have interest only in the case when M is a unitary matrix. The term *diagonalizable* we use here is narrower than the one used in the literature, because we are demanding that M be a unitary matrix.

Exercise A.6. Suppose that O is a diagonalizable operator with eigenvalues ± 1. Show that

$$P_{\pm 1} = \frac{I \pm O}{2}.$$

A.9 Completeness Relation

The *completeness relation* is so useful that it deserves to be highlighted. Let $\{|v_1\rangle$, . . ., $|v_n\rangle\}$ be an orthonormal basis of V. Then,

$$I = \sum_{i=1}^{n} |v_i\rangle\langle v_i|.$$

The completeness relation is the diagonal representation of the identity matrix.

Exercise A.7. If $\{|v_1\rangle, \ldots, |v_n\rangle\}$ is an orthonormal basis, it is straightforward to verify the validity of equations

$$A\big|v_j\big\rangle = \sum_{i=1}^{m} a_{ij}\,|w_i\rangle$$

from equation

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\,|w_i\rangle\big\langle v_j\big|.$$

Verify in the reverse direction using the completeness relation, that is, assuming that expressions $A\big|v_j\big\rangle$ are given for all $1 \le j \le n$, obtain A.

A.10 Cauchy–Schwarz Inequality

Let V be a Hilbert space and $|v\rangle, |w\rangle \in V$. Then,

$$\big|\langle v|w\rangle\big| \le \sqrt{\langle v|v\rangle\langle w|w\rangle}.$$

A more explicit way of presenting the Cauchy–Schwarz inequality is

$$\left|\sum_i v_i w_i\right|^2 \le \left(\sum_i |v_i|^2\right)\left(\sum_i |w_i|^2\right),$$

which is obtained when we take $|v\rangle = \sum_i v_i^* |i\rangle$ and $|w\rangle = \sum_i w_i |i\rangle$.

A.11 Special Operators

Let A be a linear operator in Hilbert space V. Then, there exists a unique linear operator $A^\dagger$ in V, called *adjoint operator*, that satisfies

$$(|v\rangle, A|w\rangle) = \left(A^\dagger|v\rangle, |w\rangle\right),$$

for all $|v\rangle, |w\rangle \in V$.

The matrix representation of $A^\dagger$ is the transpose-conjugate matrix $(A^*)^{\mathrm{T}}$. The main properties of the *dagger* or *transpose-conjugate* operation are

1. $(A\,B)^\dagger = B^\dagger A^\dagger$
2. $|v\rangle^\dagger = \langle v|$
3. $\big(A|v\rangle\big)^\dagger = \langle v|A^\dagger$
4. $\big(|w\rangle\langle v|\big)^\dagger = |v\rangle\langle w|$
5. $\big(A^\dagger\big)^\dagger = A$
6. $\big(\sum_i a_i A_i\big)^\dagger = \sum_i a_i^* A_i^\dagger$

The last property shows that the dagger operation is *conjugate-linear* when applied on a linear combination of operators.

Normal Operator

An operator A in V is *normal* if $A^\dagger A = A A^\dagger$.

Spectral Theorem

An operator A in V is diagonalizable if and only if A is normal.

Unitary Operator

An operator U in V is *unitary* if $U^\dagger U = U U^\dagger = I$.

Facts About Unitary Operators

Unitary operators are normal, so they are diagonalizable with respect to an orthonormal basis. Eigenvectors of a unitary operator associated with different eigenvalues are orthogonal. The eigenvalues have unit modulus, that is, their form is $\mathrm{e}^{\mathrm{i}\alpha}$, where α is a real number. Unitary operators preserve the inner product, that is, the inner product of $U|v_1\rangle$ by $U|v_2\rangle$ is equal to the inner product of $|v_1\rangle$ by $|v_2\rangle$. The application of a unitary operator on a vector preserves its norm.

Hermitian Operator

An operator A in V is *Hermitian* or *self-adjoint* if $A^\dagger = A$.

Facts About Hermitian Operators

Hermitian operators are normal, so they are diagonalizable with respect to an orthonormal basis. Eigenvectors of a Hermitian operator associated with different eigenvalues are orthogonal. The eigenvalues of a Hermitian operator are real numbers. A real symmetric matrix is Hermitian.

Orthogonal Projector

An operator P in V is an *orthogonal projector* if $P^2 = P$ and $P^\dagger = P$.

Facts About Orthogonal Projectors

The eigenvalues are equal to 0 or 1. If P is an orthogonal projector, then the *orthogonal complement* $I - P$ is also an orthogonal projector. Applying a projector on a vector either decreases its norm or maintains invariant. In this book, we use the term *projector* as a synonym for *orthogonal projector*. We will use the term *non-orthogonal projector* explicitly to distinguish this case. An example of a non-orthogonal projector on a qubit is $P = |1\rangle\langle+|$.

Positive Operator

An operator A in V is said *positive* if $\langle v|A|v\rangle \geq 0$ for any $|v\rangle \in V$. If the inequality is strict for any nonzero vector in V, then the operator is said *positive definite*.

Facts About Positive Operators

Positive operators are Hermitian. The eigenvalues are nonnegative real numbers.

Exercise A.8. Consider matrix

$$M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

1. Show that M is not normal.
2. Show that the eigenvectors of M generate a one-dimensional space.

Exercise A.9. Consider matrix

$$M = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}.$$

1. Show that the eigenvalues of M are ± 1.
2. Show that M is neither unitary nor Hermitian.
3. Show that the eigenvectors associated with distinct eigenvalues of M are not orthogonal.
4. Show that M has a diagonal representation.

Exercise A.10.

1. Show that the product of two unitary operators is a unitary operator.
2. The sum of two unitary operators is necessarily a unitary operator? If not, give a counterexample.

Exercise A.11.

1. Show that the sum of two Hermitian operators is a Hermitian operator.
2. The product of two Hermitian operators is necessarily a Hermitian operator? If not, give a counterexample.

Exercise A.12. Show that $A^\dagger A$ is a positive operator for any operator A.

A.12 Pauli Matrices

The *Pauli matrices* are

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix},$$

$$\sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

These matrices are unitary and Hermitian, and hence their eigenvalues are equal to ± 1. Putting in another way: $\sigma_j^2 = I$ and $\sigma_j^\dagger = \sigma_j$ for $j = 0, \ldots, 3$.

The following facts are extensively used:

$$X|0\rangle = |1\rangle, \; X|1\rangle = \; |0\rangle,$$

$$Z|0\rangle = |0\rangle, \; Z|1\rangle = -|1\rangle.$$

Pauli matrices form a basis for the vector space of 2 × 2 matrices. Therefore, a generic operator that acts on a qubit can be written as a linear combination of Pauli matrices.

Exercise A.13. Consider the representation of the state $|\psi\rangle$ of a qubit in the Bloch sphere. What is the representation of states $X|\psi\rangle$, $Y|\psi\rangle$, and $Z|\psi\rangle$ relative to $|\psi\rangle$? What is the geometric interpretation of the action of the Pauli matrices on the Bloch sphere?

A.13 Operator Functions

If we have an operator A in V, we can ask whether it is possible to calculate $\sqrt{A}$, that is, to find an operator the square of which is A? In general, we can ask ourselves whether it makes sense to use an operator as an argument of a usual function, such as, exponential or logarithmic function. If operator A is normal, it has a diagonal representation, that is, can be written in the form

$$A = \sum_i a_i |v_i\rangle\langle v_i|,$$

where a_i are the eigenvalues and the set $\{|v_i\rangle\}$ is an orthonormal basis of eigenvectors of A. We can extend the application of a function $f : \mathbb{C} \mapsto \mathbb{C}$ to A as follows

$$f(A) = \sum_i f(a_i)|v_i\rangle\langle v_i|.$$

The result is an operator defined in the same vector space V and it is independent of the choice of basis of V.

If the goal is to calculate $\sqrt{A}$, first A must be diagonalized, that is, we must determine a unitary matrix U such that $A = UDU^\dagger$, where D is a diagonal matrix. Then, we use the fact that $\sqrt{A} = U\sqrt{D}\,U^\dagger$, where $\sqrt{D}$ is calculated by taking the square root of each diagonal element.

If U is the evolution operator of an isolated quantum system that is initially in state $|\psi(0)\rangle$, the state at time t is given by

$$|\psi(t)\rangle \; = \; U^t|\psi(0)\rangle.$$

The most efficient way to calculate state $|\psi(t)\rangle$ is to obtain the diagonal representation of the unitary operator U

$$U = \sum_i \lambda_i |v_i\rangle\langle v_i|,$$

and to calculate the t-th power U, that is,

$$U^t = \sum_i \lambda_i^t |v_i\rangle\langle v_i|.$$

The system state at time t will be

$$|\psi(t)\rangle = \sum_i \lambda_i^t \left\langle v_i \middle| \psi(0) \right\rangle |v_i\rangle.$$

The *trace* of a matrix is another type of operator function. In this case, the result of applying the trace function is a complex number defined as

$$\mathrm{tr}(A) = \sum_i a_{ii},$$

where a_{ii} are the diagonal elements of A. In the Dirac notation

$$\mathrm{tr}(A) = \sum_i \langle v_i|A|v_i\rangle,$$

where $\{|v_1\rangle, \ldots, |v_n\rangle\}$ is an orthonormal basis of V. The trace function satisfies the following properties:

1. $\mathrm{tr}(aA + bB) = a\,\mathrm{tr}(A) + b\,\mathrm{tr}(B)$, (linearity)
2. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$,
3. $\mathrm{tr}(A\,B\,C) = \mathrm{tr}(CA\,B)$. (cyclic property)

The third property follows from the second one. Properties 2 and 3 are valid even when A, B, and C are not square matrices.

The trace function is invariant under *similarity transformations*, that is, $\mathrm{tr}(M^{-1}AM) = \mathrm{tr}(A)$, where M is an invertible matrix. This implies that the trace does not depend on the basis choice for the matrix representation of A.

A useful formula involving the trace of operators is

$$\mathrm{tr}(A|\psi\rangle\langle\psi|) = \left\langle \psi \middle| A \middle| \psi \right\rangle,$$

for any $|\psi\rangle \in V$ and any A in V. This formula can be easily proved using the cyclic property of the trace function.

Exercise A.14. Using the method of applying functions on matrices described in this section, find all matrices M such that

$$M^2 = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}.$$

A.14 Tensor Product

Let V and W be finite Hilbert spaces with basis $\{|v_1\rangle, \ldots, |v_m\rangle\}$ and $\{|w_1\rangle, \ldots, |w_n\rangle\}$, respectively. The *tensor product* of V by W, denoted by $V \otimes W$, is an mn-dimensional Hilbert space, for which set $\{|v_1\rangle \otimes |w_1\rangle, |v_1\rangle \otimes |w_2\rangle, \ldots, |v_m\rangle \otimes |w_n\rangle\}$ is a basis. The tensor product of a vector in V by a vector in W, such as $|v\rangle \otimes |w\rangle$, also denoted by $|v\rangle|w\rangle$ or $|v, w\rangle$ or $|v\,w\rangle$, can be calculated explicitly via the Kronecker product, defined ahead. A generic vector in $V \otimes W$ is a linear combination of vectors $|v_i\rangle \otimes |w_j\rangle$, that is, if $|\psi\rangle \in V \otimes W$ then

$$|\psi\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\,|v_i\rangle \otimes |w_j\rangle.$$

The tensor product is *bilinear*, that is, linear in each argument:

1. $|v\rangle \otimes \big(a\,|w_1\rangle + b\,|w_2\rangle\big) \;=\; a\,|v\rangle \otimes |w_1\rangle + b\,|v\rangle \otimes |w_2\rangle,$
2. $\big(a\,|v_1\rangle + b\,|v_2\rangle\big) \otimes |w\rangle \;=\; a\,|v_1\rangle \otimes |w\rangle + b\,|v_2\rangle \otimes |w\rangle.$

A scalar can always be factored out to the beginning of the expression:

$$a\big(|v\rangle \otimes |w\rangle\big) \;=\; \big(a|v\rangle\big) \otimes |w\rangle \;=\; |v\rangle \otimes \big(a|w\rangle\big).$$

The tensor product of a linear operator A in V by B in W, denoted by $A \otimes B$, is a linear operator in $V \otimes W$ defined by

$$\big(A \otimes B\big)\big(|v\rangle \otimes |w\rangle\big) \;=\; \big(A|v\rangle\big) \otimes \big(B|w\rangle\big).$$

A generic linear operator in $V \otimes W$ can be written as a linear combination of operators of the form $A \otimes B$, but an operator in $V \otimes W$ cannot be factored out in general. This definition can easily be extended to operators $A : V \mapsto V'$ and $B : W \mapsto W'$. In this case, the tensor product of these operators is of type $(A \otimes B) : (V \otimes W) \mapsto (V' \otimes W')$.

In quantum mechanics, it is very common to use operators in the form of external products, for example, $A = |v\rangle\langle v|$ and $B = |w\rangle\langle w|$. The tensor product of A by B can be represented by the following equivalent ways:

$$\begin{aligned} A \otimes B &= \big(|v\rangle\langle v|\big) \otimes \big(|w\rangle\langle w|\big) \\ &= |v\rangle\langle v| \otimes |w\rangle\langle w| \\ &= |v, w\rangle\langle v, w|. \end{aligned}$$

If A_1, A_2 are operators in V and B_1, B_2 are operators in W, then the composition or the matrix product of the matrix representations obey the property

$$(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = (A_1 \cdot A_2) \otimes (B_1 \cdot B_2).$$

The inner product of $|v_1\rangle \otimes |w_1\rangle$ by $|v_2\rangle \otimes |w_2\rangle$ is defined as

$$\big(|v_1\rangle \otimes |w_1\rangle\,,\, |v_2\rangle \otimes |w_2\rangle\big) \;=\; \big\langle v_1\big|v_2\big\rangle\big\langle w_1\big|w_2\big\rangle.$$

The inner product of vectors written as a linear combination of basis vectors are calculated by applying the linear property in the second argument and the *conjugate-linear* property in the first argument of the inner product. For example,

$$\left(\left(\sum_{i=1}^{n} a_i\,|v_i\rangle\right) \otimes |w_1\rangle\,,\, |v\rangle \otimes |w_2\rangle\right) \;=\; \left(\sum_{i=1}^{n} a_i^*\,\big\langle v_i\big|v\big\rangle\right)\big\langle w_1\big|w_2\big\rangle.$$

The inner product definition implies that

$$\big\|\,|v\rangle \otimes |w\rangle\,\big\| \;=\; \big\|\,|v\rangle\,\big\| \,\cdot\, \big\|\,|w\rangle\,\big\|.$$

In particular, the norm of the tensor product of unit-norm vectors is a unit-norm vector.

When we use matrix representations for operators, the tensor product can be calculated explicitly via the *Kronecker product*. Let A be a $m \times n$ matrix and B a $p \times q$ matrix. Then,

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ & \ddots & \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

The dimension of the resulting matrix is $mp \times nq$. The Kronecker product can be used for matrices of any dimension, particularly for two vectors,

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \\ a_2 \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1b_1 \\ a_1b_2 \\ a_2b_1 \\ a_2b_2 \end{bmatrix}.$$

The tensor product is an associative and distributive operation, but noncommutative, that is, $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$ if $v \neq w$. Most operations on a tensor product are performed term by term, such as

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

If both operators A and B are special operators of the same type, as the ones defined in Sect. A.11, then the tensor product $A \otimes B$ is also a special operator of the same type. For example, the tensor product of Hermitian operators is a Hermitian operator.

The trace of a Kronecker product of matrices is

$$\text{tr}(A \otimes B) = \text{tr}A \ \text{tr}B,$$

while the determinant is

$$\det(A \otimes B) = (\det A)^m \, (\det B)^n,$$

where n is the dimension of A and m of B.

The direct sum of a vector space V with itself n times is a particular case of the tensor product. In fact, a matrix $A \oplus \cdots \oplus A$ in $V \oplus \cdots \oplus V$ is equal to $I \otimes A$ for any A in V, where I is the $n \times n$ identity matrix. This shows that, somehow, the tensor product is defined from the direct sum of vector spaces, analogous to the product of numbers which is defined from the sum of numbers. However, the tensor product is richer than the simple repetition of the direct sum of vector spaces. Anyway, we can continue generalizing definitions: It is natural to define tensor potentiation, in fact, $V^{\otimes n}$ means $V \otimes \cdots \otimes V$ with n terms.

If the *diagonal state* of the vector space V is $|\text{D}\rangle_V$ and of space W is $|\text{D}\rangle_W$, then the diagonal state of space $V \otimes W$ is $|\text{D}\rangle_V \otimes |\text{D}\rangle_W$. Therefore, the diagonal state of space $V^{\otimes n}$ is $|\text{D}\rangle^{\otimes n}$.

Exercise A.15. Let H be the Hadamard operator

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

Show that

$$\langle i | H^{\otimes n} | j \rangle = \frac{(-1)^{i \cdot j}}{\sqrt{2^n}},$$

where n represents the number of qubits and $i \cdot j$ is the binary inner product, that is, $i \cdot j = i_1 j_1 + \cdots + i_n j_n \mod 2$, where $(i_1, \ldots, i_n)$ and $(j_1, \ldots, j_n)$ are the binary decompositions of i and j, respectively.

A.15 Registers

A *register* is a set of qubits treated as a composite system. In many quantum algorithms, the qubits are divided into two registers: one for the main calculation from where the result comes out and the other for the draft (calculations that will be erased). Suppose we have a register with two qubits. The computational basis is

$$|0,0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |0,1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |1,0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |1,1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

A generic state of this register is

$$|\psi\rangle = \sum_{i=0}^{1}\sum_{j=0}^{1} a_{ij}\,|i,j\rangle$$

where coefficients a_{ij} are complex numbers that satisfy the constraint

$$\left|a_{00}\right|^2 + \left|a_{01}\right|^2 + \left|a_{10}\right|^2 + \left|a_{11}\right|^2 = 1.$$

To help generalizing to n qubits, it is usual to compress the notation by converting binary-base representation to decimal-base. The computational basis for two-qubit register in decimal-base representation is $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. In the binary-base representation, we can determine the number of qubits by counting the number of digits inside the *ket*, for example, $|011\rangle$ refers to three qubits. In the decimal-base representation, we cannot determine what is the number of qubits of the register. This information should come implicit. In this case, we can go back, write the numbers in the binary-base representation and explicitly retrieve the notation. In the compact notation, a generic state of a n-qubit register is

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i\,|i\rangle,$$

where coefficients a_i are complex numbers that satisfy the constraint

$$\sum_{i=0}^{2^n-1} \left|a_i\right|^2 = 1.$$

The *diagonal state* of a n-qubit register is the tensor product of the diagonal state of each qubit, that is, $|\mathrm{D}\rangle = |+\rangle^{\otimes n}$.

Exercise A.16. Let f be a function with domain $\{0,1\}^n$ and codomain $\{0,1\}^m$. Consider a 2-register quantum computer with n and m qubits, respectively. Function f can be implemented by using operator U_f defined in the following way:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle,$$

where x has n bits, y has m bits, and $\oplus$ is the binary sum (bitwise *xor*).

1. Show that U_f is a unitary operator for any f.
2. If $n = m$ and f is injective, show that f can be implemented on a 1-register quantum computer with n qubits.

Further Reading

There are many good books about linear algebra. For an initial contact, we suggest [11, 12, 37, 72]; for a more advanced approach, we suggest [36]; for those who have mastered the basics and are only interested in the application of linear algebra on quantum computation, we suggest [64].

References

1. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. Theory of Computing, **1**, 47–79 (2003)
2. Abal, G., Donangelo, R., Marquezino, F.L., Portugal, R.: Spatial search on a honeycomb network. Math. Struct. Comput. Sci. **20**(Special Issue 06), 999–1009 (2010)
3. Aharonov, D., Ambainis, A., Kempe, J., Vazirani, U.: Quantum walks on graphs. In: Proceedings of 33th STOC, pp. 50–59. ACM, New York (2001)
4. Aharonov, D.: Quantum computation – a review. In: Stauffer, D. (ed.) Annual Review of Computational Physics, vol. VI, pp. 1–77. World Scientific, Singapore (1998)
5. Aharonov, Y., Davidovich, L., Zagury, N.: Quantum random walks. Phys. Rev. A **48**(2), 1687–1690 (1993)
6. Aldous, D.J., Fill, J.A.: Reversible Markov Chains and Random Walks on Graphs. Book in preparation, http://www.stat.berkeley.edu/~aldous/RWG/book.html (2002)
7. Ambainis, A., Bach, E., Nayak, A., Vishwanath, A., Watrous, J.: One-dimensional quantum walks. In: Proceedings of 33th STOC, pp. 60–69. ACM, New York (2001)
8. Ambainis, A., Backurs, A., Nahimovs, N., Ozols, R., Rivosh, A.: Search by quantum walks on two-dimensional grid without amplitude amplification. arxiv:1112.3337 (2011)
9. Ambainis, A.: Quantum walk algorithm for element distinctness. In: FOCS '04: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, pp. 22–31. IEEE Computer Society, Washington, DC (2004)
10. Ambainis, A., Kempe, J., Rivosh, A.: Coins make quantum walks faster. In: Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 1099–1108. SIAM, Philadelphia (2005)
11. Apostol, T.M.: Calculus, vol. 1: One-Variable Calculus with an Introduction to Linear Algebra. Wiley, New York (1967)
12. Axler, S.: Linear Algebra Done Right. Springer, New York (1997)
13. Bednarska, M., Grudka, A., Kurzynski, P., Luczak, T., Wójcik, A.: Quantum walks on cycles. Phys. Lett. A **317**(1–2), 21–25 (2003)
14. Bednarska, M., Grudka, A., Kurzynski, P., Luczak, T., Wójcik, A.: Examples of non-uniform limiting distributions for the quantum walk on even cycles. Int. J. Quant. Inform. **2**(4), 453–459 (2004)
15. Benioff, P.: Space searches with a quantum robot. (ed.) Samuel J. Lomonaco, Jr. and Howard D. Brandt Contemporary Mathematics, AMS, as a special session about Quantum Computation and Information, vol. 305, pp. 1–12. Washington, D.C (2002)
16. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: Strengths and weaknesses of quantum computing. SIAM J. Comput. **26**(5), 1510–1523 (1997)

R. Portugal, *Quantum Walks and Search Algorithms*, Quantum Science
and Technology, DOI 10.1007/978-1-4614-6336-8,

17. Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. Forstschritte Der Physik **4**, 820–831 (1998)
18. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Quant. Comput. Quant. Inform. Sci., Comtemporary Mathematics **305**, 53–74, (2002), quant-ph/0005055
19. Carteret, H.A., Ismail, M.E.H., Richmond, B.: Three routes to the exact asymptotics for the one-dimensional quantum walk. J. Phys A: Math. General **36**(33), 8775–8795 (2003)
20. Childs, A.: On the relationship between continuous- and discrete-time quantum walk. Commun. Math. Phys. **294**, 581–603 (2010)
21. Childs, A.M.: Universal computation by quantum walk. Phys. Rev. Lett. **102**, 180501 (2009)
22. Childs, A.M., Farhi, E., Gutmann, S.: An example of the difference between quantum and classical random walks. Quant. Informa. Process. **1**(1), 35–43 (2002)
23. Diu, B., Cohen-Tannoudji, C., Laloe, F.: Quantum Mechanics. Wiley-Interscience, New York (2006)
24. Cover, T.M., Thomas, J.: Elements of Information Theory. Wiley, New York (1991)
25. d'Espagnat, B.: Conceptual Foundations of Quantum Mechanics. Westview Press, Boulder (1999)
26. Farhi, E., Gutmann, S.: Quantum computation and decision trees. Phys. Rev. A **58**, 915–928 (1998)
27. Feller, W.: An Introduction to Probability Theory and Its Applications, vol. 1, 3rd edn. Wiley, New York (1968)
28. Forets, M., Abal, G., Donangelo, R., Portugal, R.: Spatial quantum search in a triangular network. Math. Struct. Comput. Sci. **22**(03), 521–531 (2012)
29. Gould, H.W.: Combinatorial Identities. Morgantown Printing and Binding Co., Morgantown (1972)
30. Graham, R.L., Knuth, D.E., Patashnik, O.: Concrete Mathematics: A Foundation for Computer Science, 2nd edn. Addison-Wesley Professional, Reading (1994)
31. Griffiths, D.: Introduction to Quantum Mechanics, 2nd edn. Benjamin Cummings, Menlo Park (2005)
32. Grover, L.K.: Quantum computers can search arbitrarily large databases by a single query. Phys. Rev. Lett. **79**(23), 4709–4712 (1997)
33. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325–328 (1997)
34. Grover, L.K.: Quantum computers can search rapidly by using almost any transformation. Phys. Rev. Lett. **80**(19), 4329–4332 (1998)
35. Hein, B., Tanner, G.: Quantum search algorithms on a regular lattice. Phys. Rev. A **82**(1), 012326 (2010)
36. Hoffman, K.M., Kunze, R.: Linear Algebra. Prentice Hall, New York (1971)
37. Horn, R., Johnson, C.R.: Matrix Analysis. Cambridge University Press, Cambridge (1985)
38. Hughes, B.D.: Random Walks and Random Environments: Random Walks (Vol 1). Clarendon Press, Oxford (1995)
39. Hughes, B.D.: Random Walks and Random Environments: Random Environments (Vol 2). Oxford University Press, Oxford (1996)
40. Itakura, Y.K.: Quantum algorithm for commutativity testing of a matrix set. Master's thesis, University of Waterloo, Waterloo (2005)
41. Kaye, P., Laflamme, R., Mosca, M.: An Introduction to Quantum Computing. Oxford University Press, Oxford (2007)
42. Kempe, J.: Quantum random walks – an introductory overview. Contemp. Phys. **44**(4), 302–327 (2003) quant-ph/0303081
43. Kempe, J.: Discrete quantum walks hit exponentially faster. Probab. Theor. Relat. Field. **133**(2), 215–235 (2005), quant-ph/0205083
44. Konno, N.: Quantum random walks in one dimension. Quant. Inform. Process. **1**(5), 345–354 (2002)
45. Košík, J.: Two models of quantum random walk. Cent. Eur. J. Phys. **4**, 556–573 (2003)

46. Krovi, H., Magniez, F., Ozols, M., Roland, J.: Finding is as easy as detecting for quantum walks. In: Automata, Languages and Programming. Lecture Notes in Computer Science, vol. 6198, pp. 540–551. Springer, Berlin (2010)
47. Lovász, L.: Random walks on graphs: a survey. Bolyai Society Mathematical Studies, Vol. 2, pp. 1–46. Springer (1993)
48. Lovett, N.B., Cooper, S., Everitt, M., Trevers, M., Kendon, V.: Universal quantum computation using the discrete-time quantum walk. Phys. Rev. A **81**, 042330 (2010)
49. Mackay, T.D., Bartlett, S.D., Stephenson, L.T., Sanders, B.C.: Quantum walks in higher dimensions. J. Phys. A: Math. General **35**(12), 2745 (2002)
50. Magniez, F., Nayak, A.: Quantum complexity of testing group commutativity. Algorithmica **48**(3), 221–232 (2007)
51. Magniez, F., Nayak, A., Richter, P., Santha, M.: On the hitting times of quantum versus random walks. In: Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 86–95. Philadelphia (2009)
52. Magniez, F., Nayak, A., Roland, J., Santha, M.: Search via quantum walk. In: Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing, pp. 575–584. New York (2007)
53. Magniez, F., Santha, M., Szegedy, M.: Quantum algorithms for the triangle problem. SIAM J. Comput. **37**(2), 413–424. New York (2007)
54. Marquezino, F.L., Portugal, R., Abal, G.: Mixing times in quantum walks on two-dimensional grids. Phys. Rev. A **82**(4), 042341 (2010)
55. Marquezino, F.L., Portugal, R., Abal, G., Donangelo, R.: Mixing times in quantum walks on the hypercube. Phys. Rev. A **77**, 042312 (2008)
56. Marquezino, F.L., Portugal, R.: The QWalk simulator of quantum walks. Comput. Phys. Commun. **179**(5), 359–369 (2008), arXiv:0803.3459
57. Mermin, N.D.: Quantum Computer Science: An Introduction. Cambridge University Press, New York (2007)
58. Meyer, C.D.: Matrix Analysis and Applied Linear Algebra. SIAM, Philadelphia (2001)
59. Moore, C., Russell, A.: Quantum walks on the hypercube. In: Rolim, J.D.P., Vadhan, S. (eds.) Proceedings of Random 2002, pp. 164–178. Springer, Cambridge (2002)
60. Moore, C., Mertens, S.: The Nature of Computation. Oxford University Press, New York (2011)
61. Mosca, M.: Counting by quantum eigenvalue estimation. Theor. Comput. Sci. **264**(1), 139–153 (2001)
62. Motwani, R., Raghavan, P.: Randomized algorithms. ACM Comput. Surv. **28**(1), 33–37 (1996)
63. Nayak, A., Vishwanath, A.: Quantum walk on a line. DIMACS Technical Report 2000-43, quant-ph/0010117 (2000)
64. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, New York (2000)
65. Omnès, R.: Understanding Quantum Mechanics. Princeton University Press, Princeton (1999)
66. Peres, A.: Quantum Theory: Concepts and Methods. Springer, Berlin (1995)
67. Preskill, J.: Lecture Notes on Quantum Computation. http://www.theory.caltech.edu/~preskill/ph229 (1998)
68. Rieffel, E., Polak, W.: Quantum Computing, a Gentle Introduction. MIT, Cambridge (2011)
69. Sakurai, J.J.: Modern Quantum Mechanics. Addison Wesley, Reading (1993)
70. Santos, R.A.M., Portugal, R.: Quantum hitting time on the complete graph. Int. J. Quant. Inform. **8**(5), 881–894 (2010), arXiv:0912.1217
71. Shenvi, N., Kempe, J., Whaley, K.B.: A quantum random walk search algorithm. Phys. Rev. A **67**(5), 052307 (2003), quant-ph/0210064
72. Strang, G.: Linear Algebra and Its Applications. Brooks Cole, Belmont (1988)
73. Strauch, F.W.: Connecting the discrete- and continuous-time quantum walks. Phys. Rev. A **74**(3), 030301 (2006)
74. Szegedy, M.: Quantum speed-up of markov chain based algorithms. In: Proceedings of the Fourty-fifth Annual IEEE Symposium on the Foundations of Computer Science, pp. 32–41 (2004). DOI: 10.1109/FOCS.2004.53

75. Szegedy, M.: Spectra of Quantized Walks and a $\sqrt{\delta\epsilon}$ Rule. (2004), quant-ph/0401053
76. Travaglione, B.C., Milburn, G.J.: Implementing the quantum random walk. Phys. Rev. A **65**(3), 032310 (2002)
77. Tregenna, B., Flanagan, W., Maile, R., Kendon, V.: Controlling discrete quantum walks: coins and initial states. New J. Phys. **5**(1), 83 (2003), quant-ph/0304204
78. Tulsi, A.: Faster quantum-walk algorithm for the two-dimensional spatial search. Phys. Rev. A **78**(1), 012310 (2008)
79. Venegas-Andraca, S.E.: Quantum walks: a comprehensive review. Quantum Information Processing **11**(5), 1015–1106 (2012), arXiv:1201.4780
80. Venegas-Andraca, S.E.: Quantum Walks for Computer Scientists. Morgan and Claypool Publishers, San Rafael (2008)
81. Štefaňák, M., Kollár, B., Kiss, T., Jex, I.: Full revivals in 2d quantum walks. Phys. Scripta **2010**(T140), 014035 (2010)
82. Štefaňák, M.: Interference phenomena in quantum information. PhD thesis, Czech Technical University (2010), arXiv:1009.0200
83. Zalka, C.: Grover's Quantum Searching Algorithm is Optimal. Phys. Rev. A **60**, 2746–2751 (1999)

Index

R. Portugal, *Quantum Walks and Search Algorithms*, Quantum Science
and Technology, DOI 10.1007/978-1-4614-6336-8,
© Springer Science+Business Media New York 2013