Introduction to Quantum Computation

Guojing Tian 田国敬

Institute of Computing Technology, Chinese Academy of Sciences

5.30, 2019

Outline

1. Course overview
   - Background
   - Course arrangement
2. Quantum mechanics under algebra
   - Vector
   - Operator
   - Postulates of quantum mechanics
3. Quantum circuit
   - Single qubit operations
   - Controlled operations
   - Measurement
   - Universal quantum gates

Background——Why

- Theory: Up to now, some quantum algorithms have been come up with and have shown strong computing power.

quantum algorithm	problem	speed up
Shor algorithm	factorization	exponential
Grover algorithm	searching	quadratic
HHL algorithm	linear system of equations	exponential
......	......	......

Background——Why

- Theory: Up to now, some quantum algorithms have been come up with and have shown strong computing power.

quantum algorithm	problem	speed up
Shor algorithm	factorization	exponential
Grover algorithm	searching	quadratic
HHL algorithm	linear system of equations	exponential
......	......	......

- Application: Several corporations have set up quantum computing labs to remain competitive.

Background——What

- Definition: Quantum computing is the use of quantum mechanical phenomena such as superposition and entanglement to perform computation.

Background——What

- Definition: Quantum computing is the use of quantum mechanical phenomena such as superposition and entanglement to perform computation.
- Take 1-(qu)bit operation as an example to have a glance at quantum computation.

	Input	Operation	Output
Classical "**NOT**"	0	$\neg$	1
Quantum "**NOT**"	$\alpha\|0\rangle + \beta\|1\rangle$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\alpha\|1\rangle + \beta\|0\rangle$
	(superposition)	(unitary)	(measurement)

Course arrangement

- Introduction to quantum computation **(2, 4)**
    - Quantum mechanics under algebra
    - Quantum circuit
- Shor algorithm **(5)**
    - Quantum Fourier Transformation
    - Phase estimation
    - Order finding
- Grover algorithm **(6)**
    - Amplitude amplification
    - Quantum counting

Please refer to ”Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.”

Dirac notation

The standard quantum mechanical notationquantum mechanical notation for a vector in a vector space is $|\psi\rangle$.

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\varphi\|\psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

Bases

Def 1. A set of non-zero vectors

$$|v_1\rangle, \cdots, |v_n\rangle, \tag{1}$$

is a basis for the vector space $\mathbb{V}$, if there exists a set of complex numbers $a_1, \cdots, a_n$ with $a_i \neq 0$ for at least one value of i, such that $a_1|v_1\rangle + \cdots + a_n|v_n\rangle = 0$.

Bases

Def 1. A set of non-zero vectors

$$|v_1\rangle, \cdots, |v_n\rangle, \tag{1}$$

is a basis for the vector space $\mathbb{V}$, if there exists a set of complex numbers $a_1, \cdots, a_n$ with $a_i \neq 0$ for at least one value of i, such that $a_1|v_1\rangle + \cdots + a_n|v_n\rangle = 0$.

Take $\mathbb{C}^2$ as an example, its two common bases are

$$|0\rangle \triangleq \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle \triangleq \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

$$|+\rangle \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |-\rangle \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{3}$$

Vector——Inner product

Def 2. A function $(\cdot,\cdot)$ from $\mathbb{V}\times\mathbb{V}$ to $\mathbb{C}$ is an inner product if it satisfies the requirements that:

- $(\cdot,\cdot)$ is linear in the second argument, i.e.,

$$(|\nu\rangle, \sum_i \lambda_i|\omega_i\rangle) = \sum_i \lambda_i(|\nu\rangle, |\omega_i\rangle)$$

- $(|\nu\rangle, |\omega\rangle) = (|\omega\rangle, |\nu\rangle)^*$
- $(|\nu\rangle, |\nu\rangle) \geq 0$ with equality if and only if $|\nu\rangle = 0$.

Vector——Inner product

Def 2. A function $(\cdot,\cdot)$ from $\mathbb{V}\times\mathbb{V}$ to $\mathbb{C}$ is an inner product if it satisfies the requirements that:

- $(\cdot,\cdot)$ is linear in the second argument, i.e.,

$$(|\nu\rangle, \sum_i \lambda_i|\omega_i\rangle) = \sum_i \lambda_i(|\nu\rangle, |\omega_i\rangle)$$

- $(|\nu\rangle, |\omega\rangle) = (|\omega\rangle, |\nu\rangle)^*$
- $(|\nu\rangle, |\nu\rangle) \geq 0$ with equality if and only if $|\nu\rangle = 0$.

Notations:

- We call a vector space equipped with an inner product an inner product space.
- In the finite dimensional complex vector spaces that come up in QCQI, a Hilbert space is exactly the same thing as an inner product space.
- In the following, we prefer the term Hilbert space.

- Orthogonal: Vectors $|\omega\rangle$ and $|\nu\rangle$ are orthogonal, if their inner product is zero, that is, $(|\nu\rangle, |\omega\rangle) = \langle\nu|\omega\rangle = 0$.
- Norm: $\| |\nu\rangle \| \equiv \sqrt{\langle\nu|\nu\rangle}$.
- Normalized: If $\| |\nu\rangle \| = 1$, then we say $|\nu\rangle$ is normalized.

- Orthogonal: Vectors $|\omega\rangle$ and $|\nu\rangle$ are orthogonal, if their inner product is zero, that is, $(|\nu\rangle, |\omega\rangle) = \langle\nu|\omega\rangle = 0$.
- Norm: $\||\nu\rangle\| \equiv \sqrt{\langle\nu|\nu\rangle}$.
- Normalized: If $\||\nu\rangle\| = 1$, then we say $|\nu\rangle$ is normalized.

Suppose $|\omega_1\rangle, \cdots, |\omega_d\rangle$ is a basis for some vector space $\mathbb{V}$, then we can use inner product to produce an orthonormal basis through the Gram-Schmidt procedure.

1. Define $|\nu_1\rangle \equiv |\omega_1\rangle / \||\omega_1\|$,
2. for $1 \leq k \leq d-1$, define

$$|\nu_{k+1}\rangle \equiv \frac{|\omega_{k+1}\rangle - \sum_{i=1}^{k}\langle\nu_i|\omega_{k+1}\rangle|\nu_i\rangle}{\||\omega_{k+1}\rangle - \sum_{i=1}^{k}\langle\nu_i|\omega_{k+1}\rangle|\nu_i\rangle\|}$$

The Cauchy-Schwarz inequality

The *Cauchy–Schwarz inequality* is an important geometric fact about Hilbert spaces. It states that for any two vectors $|v\rangle$ and $|w\rangle$, $|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle$. To see this, use the Gram–Schmidt procedure to construct an orthonormal basis $|i\rangle$ for the vector space such that the first member of the basis $|i\rangle$ is $|w\rangle/\sqrt{\langle w|w\rangle}$. Using the completeness relation $\sum_i |i\rangle\langle i| = I$, and dropping some non-negative terms gives

$$\begin{aligned}
\langle v|v\rangle\langle w|w\rangle &= \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \\
&\geq \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle \\
&= \langle v|w\rangle\langle w|v\rangle = |\langle v|w\rangle|^2,
\end{aligned}$$

as required. A little thought shows that equality occurs if and only if $|v\rangle$ and $|w\rangle$ are linearly related, $|v\rangle = z|w\rangle$ or $|w\rangle = z|v\rangle$, for some scalar z.

Vector——Outer product

Outer product is a useful way of representing linear operators.

Def 3. Suppose $|\nu\rangle$ is a vector in $\mathbb{V}$ and $|\omega\rangle$ is a vector in $\mathbb{W}$, then $|\omega\rangle\langle\nu|$ is the linear operator from $\mathbb{V}$ to $\mathbb{W}$, whose action is defined by

$$(|\omega\rangle\langle\nu|)(|\nu'\rangle) \equiv |\omega\rangle\langle\nu|\nu'\rangle = \langle\nu|\nu'\rangle|\omega\rangle$$

Vector——Outer product

Outer product is a useful way of representing linear operators.

Def 3. Suppose $|\nu\rangle$ is a vector in $\mathbb{V}$ and $|\omega\rangle$ is a vector in $\mathbb{W}$, then $|\omega\rangle\langle\nu|$ is the linear operator from $\mathbb{V}$ to $\mathbb{W}$, whose action is defined by

$$(|\omega\rangle\langle\nu|)(|\nu'\rangle) \equiv |\omega\rangle\langle\nu|\nu'\rangle = \langle\nu|\nu'\rangle|\omega\rangle$$

Explanations:

- the result when the operator $|\omega\rangle\langle\nu|$ acts on $|\nu'\rangle$
- the result of multiplying $|\omega\rangle$ by the complex number $\langle\nu|\nu'\rangle$
- Indeed, we define the former in terms of the latter.

Vector——Outer product

Outer product is a useful way of representing linear operators.

Def 3. Suppose $|\nu\rangle$ is a vector in $\mathbb{V}$ and $|\omega\rangle$ is a vector in $\mathbb{W}$, then $|\omega\rangle\langle\nu|$ is the linear operator from $\mathbb{V}$ to $\mathbb{W}$, whose action is defined by

$$(|\omega\rangle\langle\nu|)(|\nu'\rangle) \equiv |\omega\rangle\langle\nu|\nu'\rangle = \langle\nu|\nu'\rangle|\omega\rangle$$

Explanations:

- the result when the operator $|\omega\rangle\langle\nu|$ acts on $|\nu'\rangle$
- the result of multiplying $|\omega\rangle$ by the complex number $\langle\nu|\nu'\rangle$
- Indeed, we define the former in terms of the latter.
- Let $|i\rangle$ be any orthonormal basis for some $\mathbb{V}$, then $\sum_i |i\rangle\langle i| = I$ (Completeness relation).

Vector——Tensor product

Tensor product is a way of putting vector spaces together to form larger vector spaces, i.e., composite systems. This construction is crucial to understanding the quantum mechanics of multiparticle systems.

Def 4. Suppose $\mathbb{V}$ and $\mathbb{W}$ are Hilbert spaces of dimension *m* and *n* respectively, then $\mathbb{V} \otimes \mathbb{W}$ is an *mn* dimensional Hilbert space, and the elements are linear combinations of tensor products $|\nu\rangle \otimes |\omega\rangle$.

Vector——Tensor product

Tensor product is a way of putting vector spaces together to form larger vector spaces, i.e., composite systems. This construction is crucial to understanding the quantum mechanics of multiparticle systems.

Def 4. Suppose $\mathbb{V}$ and $\mathbb{W}$ are Hilbert spaces of dimension *m* and *n* respectively, then $\mathbb{V} \otimes \mathbb{W}$ is an *mn* dimensional Hilbert space, and the elements are linear combinations of tensor products $|\nu\rangle \otimes |\omega\rangle$.

Properties:

- $z(|\nu\rangle \otimes |\omega\rangle) = z(|\nu\rangle) \otimes |\omega\rangle = |\nu\rangle \otimes (z|\omega\rangle)$
- $(|\nu_1\rangle + |\nu_2\rangle) \otimes |\omega\rangle = |\nu_1\rangle \otimes |\omega\rangle + |\nu_2\rangle \otimes |\omega\rangle$
- $|\nu\rangle \otimes |\omega\rangle \equiv |\nu\omega\rangle$ (for short)
- $|\psi\rangle^{\otimes k}$ (tensored with itself *k* times)

Operator

Def 5. A linear operator between $\mathbb{V}$ and $\mathbb{W}$ is defined to be any function A:

$$A(\sum_i a_i|\nu_i\rangle) = \sum_i a_i A(|\nu_i\rangle).$$

Operator

Def 5. A linear operator between $\mathbb{V}$ and $\mathbb{W}$ is defined to be any function A:

$$A\left(\sum_i a_i|\nu_i\rangle\right) = \sum_i a_i A(|\nu_i\rangle).$$

Eg. **Pauli matrices:**

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_1 = \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_2 = \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The outer product representation of Pauli matrices:

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\sigma_1 = \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$$

$$\sigma_2 = \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1|$$

$$\sigma_3 = \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Operator——Eigenvectors and Eigenvalues

Def 6. An **eigenvector** of a linear operator A on $\mathbb{V}$ is a non-zero vector $|\nu\rangle$ such that $A|\nu\rangle = \nu|\nu\rangle$, where ν is a complex number known as the **eigenvalue** of A corresponding to $|\nu\rangle$.

Operator——Eigenvectors and Eigenvalues

Def 6. An **eigenvector** of a linear operator A on $\mathbb{V}$ is a non-zero vector $|\nu\rangle$ such that $A|\nu\rangle = \nu|\nu\rangle$, where ν is a complex number known as the **eigenvalue** of A corresponding to $|\nu\rangle$.

(Eigendecomposition of the Pauli matrices) Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices X, Y and Z.

Several specific operators

Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

Several specific operators

Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

1. Hermitian operator: $A^\dagger = A$.
2. projector: $P \equiv \sum_{i=0}^{k} |i\rangle\langle i|$.

Several specific operators

Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

1. Hermitian operator: $A^\dagger = A$.
2. projector: $P \equiv \sum_{i=0}^{k} |i\rangle\langle i|$.
3. normal operator: $AA^\dagger = A^\dagger A$.

Several specific operators

Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

1. Hermitian operator: $A^\dagger = A$.
2. projector: $P \equiv \sum_{i=0}^{k} |i\rangle\langle i|$.
3. normal operator: $AA^\dagger = A^\dagger A$.
4. unitary: $UU^\dagger = U^\dagger U = I$.

Several specific operators

Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

1. Hermitian operator: $A^\dagger = A$.
2. projector: $P \equiv \sum_{i=0}^{k} |i\rangle\langle i|$.
3. normal operator: $AA^\dagger = A^\dagger A$.
4. unitary: $UU^\dagger = U^\dagger U = I$.
5. positive operator: $(|\nu\rangle, A|\nu\rangle) \geq 0, \forall|\nu\rangle$.
   positive definite operator: $(|\nu\rangle, A|\nu\rangle) > 0, \forall|\nu\rangle \neq 0$.

Several specific operators

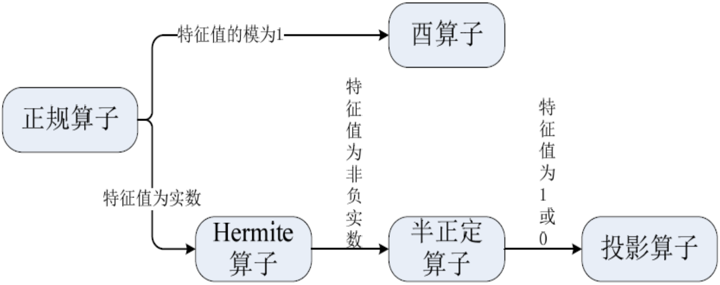
Suppose A is any linear operator on a Hilbert space $\mathbb{V}$, then there exists a unique linear operator $A^\dagger$ on $\mathbb{V}$ such that for all vectors $|\nu\rangle, |\omega\rangle \in \mathbb{V}$,

$$(|\nu\rangle, A|\omega\rangle) = (A^\dagger|\nu\rangle, |\omega\rangle),$$

we call this linear operator the adjoint or Hermitian conjugate of the operator A.

1. Hermitian operator: $A^\dagger = A$.
2. projector: $P \equiv \sum_{i=0}^{k} |i\rangle\langle i|$.
3. normal operator: $AA^\dagger = A^\dagger A$.
4. unitary: $UU^\dagger = U^\dagger U = I$.
5. positive operator: $(|\nu\rangle, A|\nu\rangle) \geq 0, \forall|\nu\rangle$.
   positive definite operator: $(|\nu\rangle, A|\nu\rangle) > 0, \forall|\nu\rangle \neq 0$.
6. density operator: $Tr(A) = 1$ and positive operator

The relationship among different operators is as follows.



Two important theorems are "the spectral decomposition" and "simultaneous diagonalization theorem".

Spectral decomposition: Any normal operator M on a vector space $\mathbb{V}$ is diagonal with respect to some orthonormal basis for $\mathbb{V}$. Conversely, any diagonalizable operator is normal.

Two important theorems are "the spectral decomposition" and "simultaneous diagonalization theorem".

Spectral decomposition: Any normal operator M on a vector space $\mathbb{V}$ is diagonal with respect to some orthonormal basis for $\mathbb{V}$. Conversely, any diagonalizable operator is normal.

Proof

The converse is a simple exercise, so we prove merely the forward implication, by induction on the dimension d of V. The case $d = 1$ is trivial. Let λ be an eigenvalue of M, P the projector onto the λ eigenspace, and Q the projector onto the orthogonal complement. Then $M = (P+Q)M(P+Q) = PMP + QMP + PMQ + QMQ$. Obviously $PMP = \lambda P$. Furthermore, $QMP = 0$, as M takes the subspace P into itself. We claim that $PMQ = 0$ also. To see this, let $|v\rangle$ be an element of the subspace P. Then $MM^\dagger|v\rangle = M^\dagger M|v\rangle = \lambda M^\dagger|v\rangle$. Thus, $M^\dagger|v\rangle$ has eigenvalue λ and therefore is an element of the subspace P. It follows that $QM^\dagger P = 0$. Taking the adjoint of this equation gives $PMQ = 0$. Thus $M = PMP + QMQ$. Next, we prove that QMQ is normal. To see this, note that $QM = QM(P+Q) = QMQ$, and $QM^\dagger = QM^\dagger(P+Q) = QM^\dagger Q$. Therefore, by the normality of M, and the observation that $Q^2 = Q$,

$$\begin{aligned} QMQQM^\dagger Q &= QMQM^\dagger Q && (2.37)\\ &= QMM^\dagger Q && (2.38)\\ &= QM^\dagger MQ && (2.39)\\ &= QM^\dagger QMQ && (2.40)\\ &= QM^\dagger QQMQ\,, && (2.41) \end{aligned}$$

so QMQ is normal. By induction, QMQ is diagonal with respect to some orthonormal basis for the subspace Q, and PMP is already diagonal with respect to some orthonormal basis for P. It follows that $M = PMP + QMQ$ is diagonal with respect to some orthonormal basis for the total vector space. □

中科院计算所 INSTITUTE OF COMPUTING TECHNOLOGY, CAS

The commutator between two operators A and B is defined to be $[A, B] \equiv AB - BA$. Similarly, the anti-commutator between two operators A and B is defined to be $\{A, B\} \equiv AB + BA$.

Simultaneous diagonalization theorem: Suppose A and B are Hermitian operations. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis. We say that A and B are simultaneously diagonalized in this case.

The commutator between two operators A and B is defined to be $[A, B] \equiv AB - BA$. Similarly, the anti-commutator between two operators A and B is defined to be $\{A, B\} \equiv AB + BA$.

Simultaneous diagonalization theorem: Suppose A and B are Hermitian operations. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis. We say that A and B are simultaneously diagonalized in this case.

Proof

You can (and should!) easily verify that if A and B are diagonal in the same orthonormal basis then $[A, B] = 0$. To show the converse, let $|a, j\rangle$ be an orthonormal basis for the eigenspace V_a of A with eigenvalue a; the index j is used to label possible degeneracies. Note that

$$AB|a, j\rangle = BA|a, j\rangle = aB|a, j\rangle, \tag{2.71}$$

and therefore $B|a, j\rangle$ is an element of the eigenspace V_a. Let P_a denote the projector onto the space V_a and define $B_a \equiv P_a B P_a$. It is easy to see that the restriction of B_a to the space V_a is Hermitian on V_a, and therefore has a spectral decomposition in terms of an orthonormal set of eigenvectors which span the space V_a. Let's call these eigenvectors $|a, b, k\rangle$, where the indices a and b label the eigenvalues of A and B_a, and k is an extra index to allow for the possibility of a degenerate B_a. Note that $B|a, b, k\rangle$ is an element of V_a, so $B|a, b, k\rangle = P_a B|a, b, k\rangle$. Moreover we have $P_a|a, b, k\rangle = |a, b, k\rangle$, so

$$B|a, b, k\rangle = P_a B P_a|a, b, k\rangle = b|a, b, k\rangle. \tag{2.72}$$

It follows that $|a, b, k\rangle$ is an eigenvector of B with eigenvalue b, and therefore $|a, b, k\rangle$ is an orthonormal set of eigenvectors of both A and B, spanning the entire vector space on which A and B are defined. That is, A and B are simultaneously diagonalizable. □

Postulates of quantum mechanics

- origin: The postulates of quantum mechanics were derived after a long process of trial and (mostly) error.
- motivation: not always clear
- expectation: how to apply them, and when

Postulates of quantum mechanics

- origin: The postulates of quantum mechanics were derived after a long process of trial and (mostly) error.
- motivation: not always clear
- expectation: how to apply them, and when

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of system. The system is completely described by its state vector, which is a unit vector in the system's state space.

The simplest quantum mechanical system is the qubit. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for this two-dimensional state space, then an arbitrary state vector can be written

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

where a, b are complex numbers, and $|a|^2 + |b|^2 = 1$.

The simplest quantum mechanical system is the qubit. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for this two-dimensional state space, then an arbitrary state vector can be written

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

where a, b are complex numbers, and $|a|^2 + |b|^2 = 1$.

Notations:

- computational basis states: $\{|0\rangle, |1\rangle\}$
- superposition: $|\psi\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$.
- amplitude: a, b is the amplitude for $|0\rangle, |1\rangle$, respectively.
- probability: $|a|^2$ for measuring result is 0, and $|b|^2$ for measuring result is 1.

Geometric representation for a qubit is as follows.

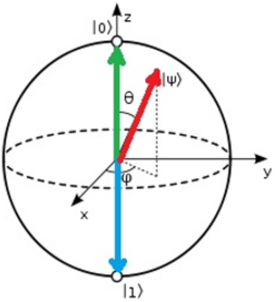
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

normalization

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$$

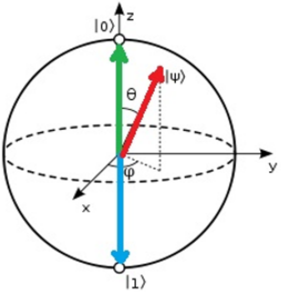
up to global phase

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



Block sphere representation of a qubit

Some common used qubit states.



Block sphere representation of a qubit

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

Axis-Z

If $\varphi = 0, \theta = 0$, then $|\psi\rangle = |0\rangle$;

If $\varphi = 0, \theta = \pi$, then $|\psi\rangle = |1\rangle$;

Axis-X

If $\varphi = 0, \theta = \frac{\pi}{2}$, then $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \triangleq |+\rangle$;

If $\varphi = 0, \theta = \frac{3\pi}{2}$, then $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \triangleq |-\rangle$.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

Notations:

- closed: This system is not interacting in any way with other systems.
- Egs.:
  bit flip: X
  phase flip: Z
  Hadamard gate: H

Postulate 2′: The time evolution of a state of a closed quantum system is described by the Schrodinger equation,

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

In this equation, $\hbar$ is a physical constant known as Plank's constant whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor $\hbar$ into H, effectively setting $\hbar = 1$. H is a fixed Hermitian operator known as the Hamiltonian of the closed system.

Think about the connection between this Hamiltonian and the above unitary operator.

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle,$$

and the state of the system after the measurement is

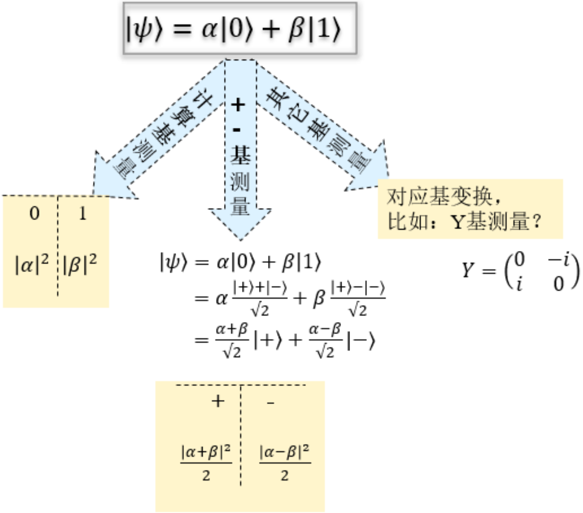
$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

The measurement operators satisfy the completeness equations,

$$\sum_m M_m^\dagger M_m = I.$$

- The measurement of a qubit in the computational basis is $\{M_0, M_1\}$, where $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$.

- The measurement of a qubit in the computational basis is $\{M_0, M_1\}$, where $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$.
- Dfferent measurements act on a fixed qubit state.



Three elementary but important measurement scenarios:

- Distinguishing quantum states

Proof that non-orthogonal states can't be reliably distinguished

A proof by contradiction shows that no measurement distinguishing the non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ is possible. Suppose such a measurement is possible. If the state $|\psi_1\rangle$ ($|\psi_2\rangle$) is prepared then the probability of measuring j such that $f(j) = 1$ ($f(j) = 2$) must be 1. Defining $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$, these observations may be written as:

$$\langle\psi_1|E_1|\psi_1\rangle = 1; \quad \langle\psi_2|E_2|\psi_2\rangle = 1.$$

Since $\sum_i E_i = I$ it follows that $\sum_i \langle\psi_1|E_i|\psi_1\rangle = 1$, and since $\langle\psi_1|E_1|\psi_1\rangle = 1$ we must have $\langle\psi_1|E_2|\psi_1\rangle = 0$, and thus $\sqrt{E_2}|\psi_1\rangle = 0$. Suppose we decompose $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, where $|\varphi\rangle$ is orthonormal to $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, and $|\beta| < 1$ since $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal. Then $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$, which implies a contradiction with (2.99), as

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\langle\varphi|E_2|\varphi\rangle \le |\beta|^2 < 1,$$

where the second last inequality follows from the observation that

$$\langle\varphi|E_2|\varphi\rangle \le \sum_i \langle\varphi|E_i|\varphi\rangle = \langle\varphi|\varphi\rangle = 1.$$

- Projective measurements

Projective measurements: A projective measurement is described by an *observable*, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m m P_m ,$$

where P_m is the projector onto the eigenspace of M with eigenvalue m.

POVM measurements

Suppose a measurement described by measurement operators M_m is performed upon a quantum system in the state $|\psi\rangle$. Then the probability of outcome m is given by $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Suppose we define

$$E_m \equiv M_m^\dagger M_m.$$

Then from Postulate 3 and elementary linear algebra, E_m is a positive operator such that $\sum_m E_m = I$ and $p(m) = \langle\psi|E_m|\psi\rangle$. Thus the set of operators E_m are sufficient to determine the probabilities of the different measurement outcomes. The operators E_m are known as the *POVM elements* associated with the measurement. The complete set $\{E_m\}$ is known as a *POVM*.

- POVM measurements

Suppose a measurement described by measurement operators M_m is performed upon a quantum system in the state $|\psi\rangle$. Then the probability of outcome m is given by $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Suppose we define

$$E_m \equiv M_m^\dagger M_m.$$

Then from Postulate 3 and elementary linear algebra, E_m is a positive operator such that $\sum_m E_m = I$ and $p(m) = \langle\psi|E_m|\psi\rangle$. Thus the set of operators E_m are sufficient to determine the probabilities of the different measurement outcomes. The operators E_m are known as the *POVM elements* associated with the measurement. The complete set $\{E_m\}$ is known as a *POVM*.

Eg: $\{|\psi_1\rangle = |0\rangle, |\psi_2\rangle = |+\rangle\}$

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then then joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

- entangled state: it cannot be written as a product of states of its component systems.
- Bell states:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Psi_{01}\rangle = (I \otimes Z)|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi_{10}\rangle = (I \otimes X)|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi_{11}\rangle = (I \otimes XZ)|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Review the four postulates and try to place them in some kind of global perspective.

- Postulate 1 sets the area for quantum mechanics.
- Postulate 2 tells the dynamics of closed quantum system.
- Postulate 3 describes how to extract information from quantum systems.
- Postulate 4 shows how to combine different quantum systems to generate a composite one.

Single qubit operations

Operations on a qubit must preserve normalization, thus are described by 2×2 unitary matrices.

Single qubit operations

Operations on a qubit must preserve normalization, thus are described by 2×2 unitary matrices.

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Rotation operators about the $\hat{x}$, $\hat{y}$ and $\hat{z}$ axes are defined as follows.

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

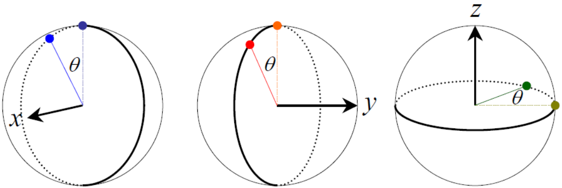
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

Rotation operators about the $\hat{x}$, $\hat{y}$ and $\hat{z}$ axes are defined as follows.

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$



An arbitrary unitary operator on a single qubit can be written as a combination of rotations, together with global phase shifts.

($Z - Y$ decomposition for a single qubit)

Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

An arbitrary unitary operator on a single qubit can be written as a combination of rotations, together with global phase shifts.

($Z-Y$ decomposition for a single qubit)

Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

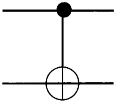
Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

Controlled operations

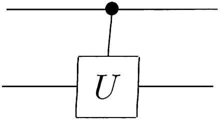
"If A is true, then do B".

- two input qubits, known as the control qubit and target qubit
- $|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$

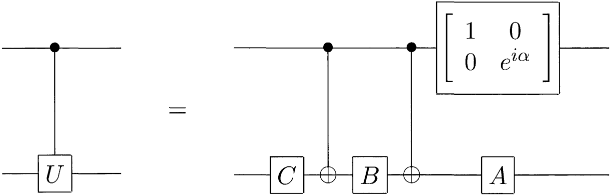
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



- $|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$



- how to implement the controlled-U operation for arbitrary single qubit U, using only single qubit operations and the CNOT gate.



Measurement

A final element used in quantum circuits.

We shall denote a projective measurement in the computational basis using a 'meter' symbol.

Two principles:

- Principle of deferred measurement
  Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.
- Principle of implicit measurement
  Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

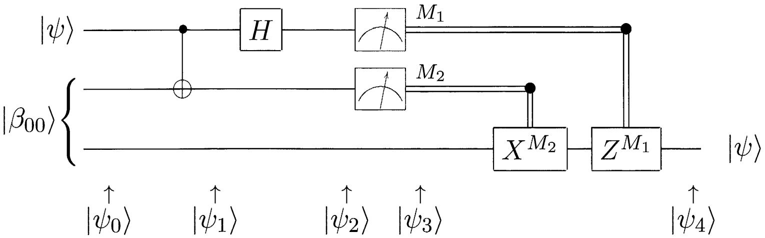
Quantum teleportation

Quantum teleportation is a technique for moving quantum states around, even in the absence of a quantum communications channel linking the sender of the quantum state to the recipient.

Setting:

- Alice and Bob met long ago and generated an EPR pair, but now live far apart with one qubit of the EPR pair.
- Many years later, Bob is in hiding, and Alice's mission is to deliver a qubit $|\psi\rangle$ to Bob.
- Alice does not knowdoes not know the state of the qubit, and moreover can only send classical information to Bob.

Alice can employ quantum teleportation as the way of sending $|\psi\rangle$ to Bob with only a small overhead of classical communication.



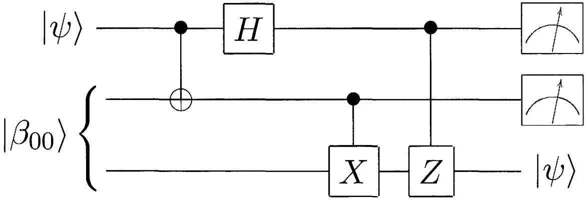
where

$$
\begin{aligned}
|\psi_0\rangle &= |\psi\rangle|\beta_{00}\rangle \\
&= \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big]
\end{aligned}
$$

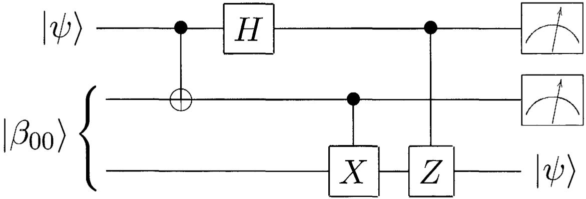
$$
|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big]
$$

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big] \\
&= \frac{1}{2}\Big[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) \\
&\quad + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\Big]
\end{aligned}
$$

Principle of deferred measurement



Principle of deferred measurement



- Bob can "fix up" his state to recover $|\psi\rangle$ according to the measurement result.
- faster than the speed of light?
- create a copy?
- EPR pair (entanglement) is a resource.

Universal quantum gates

A set of gates is said to be universal for quantum computation, if any unitary operation may be approximated to arbitrary accuracy by a quantum circuit involving only those gates.

Three universality constructions:

- an arbitrary unitary operator may be expressed exactly as a product of two-level unitary operators.
- an arbitrary unitary operator may be expressed exactly using single qubit and CNOT gates.
- any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, CNOT and $\pi/8$ gates.

Summary

1. Course overview
   - Background
   - Course arrangement
2. Quantum mechanics under algebra
   - Vector
   - Operator
   - Postulates of quantum mechanics
3. Quantum circuit
   - Single qubit operations
   - Controlled operations
   - Measurement
   - Universal quantum gates