Quantum information and quantum computation

Xiaodi Li

January 4, 2022

Contents

1 Classical Computation

1.1 Classical computation models

1.1.1 Turing machine

1.1.2 Circuit

1.2 Computational complexity

1.3 The physics of classical computation

2 Quantum computation

Quantum computation is composed of three basic steps: preparation of the input state, implementation of the desired unitary transformation acting on input state, measurement of the output state. More explicitly, in order to perform a quantum computation, we should be able to:

- *prepare* the quantum computer in a well-defined initial state $|\psi_i\rangle$, which we call the fiducial state of the computer, for instance the state $|0\cdots 0\rangle$.
- *manipulate* the quantum-computer wave function, that is, derive any given unitary transformation U, leading to $|\psi_f\rangle = U|\psi_i\rangle$;
- perform, at the end of the algorithm, a standard *measurement* in the computational basis, that is, measure the polarization σ_z of each qubit.

Even the evolution of the n-qubit system is described by $2^n \times 2^n$ unitary matrix, this matrix can be decomposed into a product of unitary operations acting only on one or two qubits. And these operations are the elementary *quantum gates* of the circuit model of quantum computation.

The output of the measurement is inherently *probabilistic* and the probabilities of different outputs are given by the basic laws of quantum mechanics. In a quantum algorithm, we must *repeat the algorithm several times* to obtain the correct solution of our problem with probability as close to one.

2.1 Single qubit and single qubit operations

2.1.1 Single qubit

The elementary unit of quantum information and the basic building block of quantum computation is the *qubit*. A qubit is a 2-dimensional Hilbert space. The pure state of a qubit is represented by a vector

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1}$$

with $|a|^2 + |b|^2 = 1$. Since $|\psi\rangle \sim e^{i\phi}|\psi\rangle$, the state is described by 2 real parameters. The state $|\psi\rangle = a|0\rangle + b|1\rangle$ can be parameterized by $a = \cos(\theta/2), b = e^{i\phi}\sin(\theta/2)$

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \tag{2}$$

with $0 \leq \theta \leq \pi, 0 \leq \phi < 2\pi$. Then a pure state of qubit corresponds to a point (θ, ϕ) on the unit sphere, which is called *Bloch sphere*. The point is described by a unit 3-vector

$$(x, y, z) = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta), \tag{3}$$

which is called the *Bloch vector*. The density operator of a generic pure state of qubit is given by

$$\rho(\theta, \phi) = |\psi(\theta, \rho)\rangle\langle\psi(\theta, \rho)| = \left[\begin{array}{cc} \cos^2(\theta/2) & \sin(\theta/2)\cos(\theta/2)e^{-i\phi} \\ \sin(\theta/2)\cos(\theta/2)e^{-i\phi} & \cos^2(\theta/2) \end{array}\right]. \tag{4}$$

The density operator ρ for the mixed state of a qubit should be 2×2 Hermitian matrix and satisfies $\mathrm{Tr}(\rho) = 1$ and $\det(\rho) \geq 0$. Then ρ is parameterized as

$$\rho = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z) = \frac{1}{2}\left[\begin{array}{cc} 1+z & x-iy \\ x+iy & 1-z \end{array}\right]. \tag{5}$$

Since $\det(\rho) \geq 0$, we get $\det(\rho) = \frac{1}{4}(1 - x^2 - y^2 - z^2) \geq 0$, then $\vec{r} = (x, y, z)$ corresponds to a point on the unit ball, which is called the *Bloch ball*. Pure states are located on the boundary of the Bloch ball, and the density matrix $\rho = 1/2I$ corresponds to the centre of the Bloch ball.

2.1.2 Single qubit operation

Operations on a qubit are described by 2×2 unitary matrices, which constitute the U(2) group. For example, the Pauli matrices $\{X, Y, Z\}$, the Hadamard gate H, phase gate S, $\pi/8$ gate T,

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{6}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \tag{7}$$

Since $\mathrm{U}(2) = \mathrm{U}(1) \times \mathrm{SU}(2)$, then for any 2×2 unitary matrix $U \in \mathrm{U}(2)$,

$$U = e^{i\alpha} \widetilde{U}, \tag{8}$$

with $\widetilde{U} \in \mathrm{SU}(2)$. SU(2) is the double-covering group of SO(3) and has the same Lie algebra as SO(3), then $\widetilde{U}$ can be interpreted as a rotation transformation of a 3-vector corresponding to a state of a qubit. $\widetilde{U}$ has two different parameterization. The first is

$$\widetilde{U} = R_{\hat{n}}(\theta) = \exp(-i\theta\hat{n} \cdot \vec{\sigma}/2), \tag{9}$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli matrices, we can interpret it as a rotation by θ around the $\hat{n}$ axis. While the second is the Euler angle representation

$$\widetilde{U} = R_z(\beta) R_y(\gamma) R_z(\delta). \tag{10}$$

We get the conclusion that for any unitary operation on a single qubit, there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \tag{11}$$

And there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$ with

$$A = R_z(\beta) R_y(\gamma/2), \quad B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2), \quad C = R_z((\delta-\beta)/2). \tag{12}$$

2.2 Controlled operations

CNOT (controlled-NOT) gate is a quantum gate with two input qubits, the control qubit and target qubit. In the computational basis, the action of the CNOT is given by $|c\rangle|t\rangle \to |c\rangle|c \oplus t\rangle$. The matrix representation of CNOT is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{13}$$

A controlled-U operation is a two qubit operation with a control and a target qubit. Its action is $|c\rangle|t\rangle \to |c\rangle U^c |t\rangle$.

2.3 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.

Any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, CNOT, and $\pi/8$ gates. To prove the above conclusion, there are two steps.

- Exactness:

  An arbitrary unitary operator may be expressed *exactly* as a product of two-level unitary operators.

  An arbitrary two-level unitary operator may be expressed *exactly* using only single qubit and CNOT gates.

- Approximation:

  Single qubit operation may be approximated to *arbitrary accuracy* using the Hadamard, phase, and $\pi/8$ gates.

2.3.1 Exact realization

There are two steps to construct the exact realization.

- Two-level unitary gates are universal.

  Two-level unitary operators are those operators act non-trivially only on a subspace spanned by two computational basis states.

- Single qubit and CNOT gates are universal.

2.3.2 Approximate realization

A discrete set of gates can't be used to implement an arbitrary unitary operation exactly, since the set of unitary operations is continuous. But a discrete set can be used to approximate any unitary operation.

How to approximate unitary operators? The *error* of utilizing V to approximate U is defined by

$$E(U,V) \equiv \max_{|\psi\rangle} ||(U-V)|\psi\rangle||. \tag{14}$$

There are two important points.

- Suppose M is a POVM element, and P_U or P_V are the probability distributions of the measurement M following the action of U or V on a initial state $|\psi\rangle$, then

$$|P_U - P_V| \leq 2E(U,V). \tag{15}$$

- If we use a sequence of gates $V_1, \cdots, V_m$ to approximate another sequence $U_1, \cdots, U_m$, the errors accumulate linearly as

$$E(U_m \cdots U_1, V_m \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j). \tag{16}$$

There are two different sets of universal gates, the first is: Hadamard, phase, CNOT and $\pi/8$, and the second is: Hadamard, phase, CNOT and Toffoli gates. They both rely on the fact: the Hadamard and $\pi/8$ gates can be used to approximate any single qubit unitary operation to arbitrary accuracy.

3 Quantum algorithms

3.1 Classical computation on a quantum computer

A classical circuit may not be able to simulated by quantum circuits is because unitary quantum logic gates are inherently *reversible*, whereas many classical logic gates such as the NAND gate are inherently *irreversible*.

Any classical circuit can be replaced by an equivalent circuit containing only reversible elements by making use of the reversible gate, *Toffoli gate.* The Toffoli gate can be used to simulate the NAND gate and FANOUT gates, and with these two gates it becomes possible to construct an equivalent reversible circuit.

The quantum Toffoli gate simply permute computational basis states in the same way as the classical Toffoli gate, and can be used to simulate irreversible classical logic gates just as the classical Toffoli gate. So quantum computers are capable of performing any classical computation. It's easy for quantum computer to simulate non-deterministic classical computer.

3.2 Quantum parallelism and Deutsch's algorithm

Informally, quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many different values of x simultaneously. To implement quantum parallelism, the *Hadamard transform* need to be applied to the input n qubits

$$H^{\otimes n} : |0\rangle^{\otimes n} \to \frac{1}{2^{n/2}} \sum_x |x\rangle, \tag{17}$$

where the sum is over all possible computational basis. The Hadamard transform produces an equal superposition of all computational basis states.

Suppose a quantum circuit apply the unitary operation to n input qubit $|x\rangle$ and 1 output qubit $|y\rangle$ as $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$, i.e., U_f evaluates the function $f(x)$. Prepare the initial state $|0\rangle^{\otimes n}|0\rangle$, apply the Hadamard transform to the first n qubits, then followed by the unitary operation U_f, we get

$$|0\rangle^{\otimes n}|0\rangle \to \frac{1}{2^{n/2}} \sum_x |x\rangle|0\rangle \to \frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle. \tag{18}$$

From above we can see that quantum parallelism enables all possible values of the function f evaluated simultaneously.

However, this parallelism is not immediately useful. Since under a measurement, the final superposition state $\sum_x |x, f(x)\rangle$ will collapse into a particular state $|x, f(x)\rangle$ and give $f(x)$ for a single x. It requires the ability to extract information about more than one value of $f(x)$ from superposition states, in order to make quantum computation more useful.

The combination of *superposition* and *interference* enables quantum computation to extract some information more efficiently than classical computation. The Deutsch's algorithm has the following steps:

- prepare the initial state $|\psi_0\rangle = |01\rangle$,
- apply the Hadamard transform to both two qubits, $|\psi_1\rangle = H^{\otimes 2}|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$,
- apply the unitary operation U_f, $|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle](|0\rangle - |1\rangle)$
- apply the Hadamard gate to the first qubit,

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \\ \pm|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1) \end{cases} \tag{19}$$

$$= \pm\,|f(0) \oplus f(1)\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{20}$$

- finally, make a measurement of the first qubit, we can determine $f(0) \oplus f(1)$.

The algorithm tells us that the quantum circuit has given us the ability to determine a *global property* of $f(x)$ using only one evalution of $f(x)$.

3.3 The quantum Fourier transform and its application

3.3.1 The quantum Fourier transform

Discrete Fourier transformation has been defined in Appendix B, and the quantum discrete Fourier transformation is defined similarly but for an set of quantum states. The *quantum discrete Fourier transformation* (QDFT) is defined as a *linear operator* with the action on a set of orthonormal basis $\{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$ as,

$$\mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle. \tag{21}$$

For an arbitrary state $|\psi\rangle = \sum_{j=0}^{N-1} x_i |j\rangle$, the quantum Fourier transformation is

$$\mathcal{F}|\psi\rangle = \sum_{j=0}^{N-1} x_i \mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left(\sum_{j=0}^{N-1} x_i e^{\frac{2\pi i}{N} jk} \right) |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k |k\rangle, \tag{22}$$

where y_k's are classical DFT of x_i's.

To implement the QDFT in a quantum computer, we need to construct the unitary quantum circuit for QDFT. First, we consider how to represent the QDFT in the quantum computer with n qubits. Let $N = 2^n$, we can consider the orthonormal basis $\{|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle\}$ is its computational basis. For every integer $1 \leq j \leq 2^n - 1$, we can write its binary representation as

$$j = j_1 j_2 \cdots j_n = j_1 2^{n-1} + \cdots + j_n 2^0, \tag{23}$$

and a binary fraction

$$0.j_l j_{l+1} \cdots j_m = j_l 2^{-1} + j_{l+1} 2^{-2} + \cdots + j_m 2^{-(m-l+1)}. \tag{24}$$

In the binary representation, equation (21) becomes

$$\begin{aligned}
\mathcal{F}|j\rangle =& \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i 2^{-n} jk} |k\rangle \\
=& \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j (\sum_{l=1}^{n} k_l 2^{-l})} |k_1 k_2 \cdots k_n\rangle \\
=& \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
=& \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
=& \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi i k_l (0.j_{n-l+1} \cdots j_n + j_1 j_2 \cdots j_{n-l})} |k_l\rangle \\
=& \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i 0.j_{n-l+1} \cdots j_n} |1\rangle \right)
\end{aligned} \tag{25}$$

where we have used the fact $2^{-l} j = 0.j_{n-l+1} \cdots j_n + j_1 j_2 \cdots j_{n-l}$. Second, we consider constructing the quantum circuits for the QDFT. Since the transformations on every qubit are similar, we can just focus on the first qubit.

- Apply the Hadamard gate, then the first qubit becomes

$$|j_1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right). \tag{26}$$

- Apply j_2-controlled-R_2 gate, where R_2 gate is

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}. \tag{27}$$

  The meaning of j_2-controlled-R_2 gate is that only when $j_2 = 1$ then apply R_2 gate to the first qubit, else applying identity. So the first qubit becomes

$$|j_1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right). \tag{28}$$

- Apply the same j_l-controlled-R_l gate until $l = n$, we get

$$|j_1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right). \tag{29}$$

- Finally, apply the swap operation to transform the first qubit into last one.

The operations for other qubits are similar, and the final step is to swap these qubits into correct order.

The first qubit needs n gates, while the lth qubit needs $n - l + 1$ gates, and the swap operations need at most $3n/2$ gates, so the total number of gates is $n + (n-1) + \cdots + 1 + 3n/2 = \frac{n(n+1)}{2} + 3n/2$. Hence the circuit provides a $\Theta(n^2)$ algorithm for performing the QDFT.

Although the implementing of QDFT is efficient, but there is no way of determining the transformed amplitudes of original states and there is in general on way to efficiently prepare the original to be transformed.

3.3.2 Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$, where the value of φ is unknown. The goal of the *phase estimation algorithm* is to estimate φ.

The phase estimation algorithm consists of three parts: a *black box* (or oracle) to prepare the eigenstate $|u\rangle$ and perform the controlled-U^{2^j} operation for non-negative integer j, the *first register* containing t qubits initially in the state $|0\rangle$ and the *second register* in the state $|u\rangle$. There are four steps for the phase estimation algorithm.

- Apply the Hadamard transformation to the first register.

$$|0\rangle^{\otimes t} \to \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle. \tag{30}$$

- Apply the controlled-U operations on the second register.

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle|u\rangle \to \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle U^k|u\rangle = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle|u\rangle \tag{31}$$

- Apply the inverse Fourier transformation on the first register. If $\varphi = 0.\varphi_1 \cdots \varphi_t$, then

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle|u\rangle \to |\varphi_1 \cdots \varphi_t\rangle|u\rangle \tag{32}$$

- Measure the first register. Then we get the exact value of φ.

In fact, φ can't be exactly expressed in binary representation with t bits. In order to obtain φ accurate to n bits with probability at least $1-\epsilon$, we choose

$$t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil . \tag{33}$$

3.4 Quantum search algorithms

3.4.1 The quantum search algorithm

3.4.2 Quantum search as quantum simulation

3.5 Simulation of quantum systems

3.5.1 Simulation

The goal of simulation is: given an initial state of the system, what is the state at some other time and or position?

Solutions are usually obtained by approximating the state with a digital representation, then discretizing the differential equation in space and time such that an iterative application of a procedure carries the state from the initial to the final conditions.

Just simulating Schrodinger's equation is not the especial difficulty faced in simulating quantum systems. The key challenge in simulating quantum systems is the exponential number of differential equations which must be solved.

4 Open quantum systems

In the real world, there are no perfect closed systems, but only open systems suffering from the unwanted interactions with the environment. These unwanted interaction show up as noise in quantum information processing systems. We need to understand and control such noise processes in order to build quantum information processing systems, so we need the mathematical description of the *open quantum systems*. The open quantum systems are different with closed quantum systems at these points:

- States are not rays in Hilber space.
- Measurements are not orthogonal projections.
- Evolution is not unitary.

To study open quantum system, we will conside the combination of the quantum system and its environment as a closed quantum system and deduce the mathematical description of the quantum system.

4.1 States

The Hilber space of the combination of a quantum system A and its environment B is $\mathcal{H}_{AB} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $\mathcal{H}_{A,B}$ are the Hilbert spaces of A, B with the corresponding orthonormal basis being $\{|i\rangle_A\}$ and $\{|\mu\rangle_B\}$. An arbitrary pure state of $\mathcal{H}_{AB}$ is

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i,\mu} |i\rangle_A \otimes |\mu\rangle_B, \tag{34}$$

then the expectation value of an observable M_A of system A is

$$\begin{aligned}\langle M_A\rangle =&_{AB}\langle\psi|M_A\otimes I_B|\psi\rangle_{AB}\\ =&\sum_{i,j,\mu} a^*_{j\mu}a_{i,\mu}\langle j|M_A|i\rangle\\ =&\mathrm{Tr}(M_A\rho_A)\end{aligned} \tag{35}$$

with ρ_A is the *density matrix* of open quantum system A obtained by taking the partial trace of $|\psi\rangle_{AB}$ over environment B

$$\rho_A=\mathrm{Tr}_B(|\psi\rangle\langle\psi|)=\sum_{i,j,\mu} a^*_{j\mu}a_{i,\mu}|i\rangle\langle j|. \tag{36}$$

So we say that: the state of the open quantum system A is completely described by a density matrix ρ_A. A general density matrix ρ satisfies the following properties:

- ρ is self-adjoint: $\rho=\rho^\dagger$.
- ρ is positive: for any $|\psi\rangle$, $\langle\psi|\rho|\psi\rangle\geq 0$.
- $\mathrm{Tr}(\rho)=1$.

So ρ can be diagonalized in an orthonormal basis with all eigenvalues being real, nonnegative and sum to one, i.e.

$$\rho=\sum_a p_a|a\rangle\langle a| \tag{37}$$

with $0\leq p_a\leq 1$ and $\sum_a p_a=1$. We can interpret ρ as describing an ensemble of pure quantum states, in which each state $|a\rangle$ occurs with probability p_a.

If a state is described by a ray $|\psi\rangle$ in Hilber space, then the stete is *pure* state, its density matrix is $\rho=|\psi\rangle\langle\psi|$. If the state is described by a density matrix with more than one terms, then it's called *mixed* state.

4.2 Quantum measurements

First, we discuss the meaning of measurement. Suppose we want to make a measurement of a system by the set of orthogonal porjective operators $\{E_a, a=1,\cdots,N-1\}$ with

$$E_aE_b=\delta_{ab}E_a,\quad E_a=E_a^\dagger,\quad \sum_a E_a=I. \tag{38}$$

We need to introduce a N-dimensional pointer system with fiducial orthonormal basis $\{|a\rangle, a=1,\cdots,N-1\}$, couple the system to the pointer, and perform the unitary transformation

$$U=\sum_{a,b}E_a\otimes|b+a\rangle\langle b|. \tag{39}$$

If the initial state of the system and the pointer is $|\Psi\rangle=|\psi\rangle\otimes|0\rangle$, then the final state is

$$|\Psi'\rangle=U|\Psi\rangle=\sum_a E_a|\psi\rangle\otimes|a\rangle. \tag{40}$$

If the pointer is measured in the fiducial basis, the probability of obtaining outcome a is

$$P_a=\langle\Psi'|(I\otimes|a\rangle\langle a|)|\Psi'\rangle=\langle\psi|E_a|\psi\rangle=||E_a|\psi\rangle||^2, \tag{41}$$

and the post-measurement state is

$$\frac{E_a|\psi\rangle}{||E_a|\psi\rangle||} \otimes |a\rangle. \tag{42}$$

Finally, if we ignore the point, then we see that the whole process provides us wth a state $\frac{E_a|\psi\rangle}{||E_a|\psi\rangle||}$ with probability $\langle\psi|E_a|\psi\rangle$. So this is the real process of the measurement of a system, and we can say that: the orthogonal measurement of the pointer in the fiducial basis induces the orthogonal measurement on the system.

4.3 Quantum operation

Now we give a mathmatical definition of *quantum operation*. A quantum operation $\mathcal{E}$ is a linear map from a set of density operators of Hilbert space $\mathcal{H}$ to a set of density operators of Hilber space $\mathcal{H}'$ with the following properties:

- $0 \leq \text{Tr}[\mathcal{E}(\rho)] \leq 1$.
- $\mathcal{E}$ is completely positive.

4.4 Classical noise and Markov processes

Let X denote the initial state of a bit with probability p_0 in state 0 and p_1 in state 1, Y is the final state of the bit with q_0 in state 0 and q_1 in state 1, and in the process $X \to Y$ the probability of the bit flipping is p, while $1-p$ for remaining the same. From the formula

$$p(Y=y) = \sum_x p(Y=y|X=x)p(X=x), \tag{43}$$

where the conditional probabilities $p(Y=y|X=x)$ are called *transition probabilities*, we get

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}. \tag{44}$$

Making the assumption that the consecutive noise processes act independently, we can get more complicated stochastic process like $X \to Y \to Z$, which is known as *Markov process*. So noise in classical systems can be described using the theory of stochastic processes, like

$$\vec{q} = E\vec{p} \tag{45}$$

where E is a matrix of transition probabilities called the *evolution matrix*. The evolution matrix must satisfy two conditions

- the *positivity* requirement: all entries of E must be non-negative,
- the *completeness* requirement: all columns of E must sum to one.

In summary, classical noise processes are described by the Markov process, provided that the noise is caused independently by environment in each stage, and the final probabilities is generated by linear transformation of initial probabilities, described by evolution matrix.

4.5 Quantum operations

As the sate of a classical system is described by a vector of probabilities, a quantum system is describe by the density operator ρ. And similar to the evolution of a classical system as in 45, the quantum system transform as

$$\rho \to \rho' = \mathcal{E}(\rho) \tag{46}$$

where the map $\mathcal{E}$ is called *quantum operation*. Quantum operation includes the examples of unitary evolutions and measurements.

4.5.1 Environments and quantum operations

The way to describe the dynamics of an open quantum system is to regard the system and its environment as a closed quantum system. Suppose the system is in the state ρ_{s} and the environment in ρ_{e}, then the initial state is $\rho_{\mathrm{s}} \otimes \rho_{\mathrm{e}}$. After a unitary transformation U, we perform a partial trace over the environment, then the quantum operation is defined as:

$$\mathcal{E}(\rho_{\mathrm{s}}) = \mathrm{tr}_{\mathrm{e}}[U(\rho_{\mathrm{s}} \otimes \rho_{\mathrm{e}})U^\dagger]. \tag{47}$$

There are two points.

- We assume that the system and the environment start in a product state.
- If the system has a Hilbert space of d dimensions, it suffices to model the environment with a Hilber space of no more than d^2 dimensions.

The quantum operation can also be generalized as mapping the density operators of system A to the density operators of system B,

$$\mathcal{E}(\rho_A) = \rho'_B = \mathrm{tr}_A[U(\rho_A \otimes \rho_B)U^\dagger]. \tag{48}$$

4.5.2 Operator-sum representation

From the definition of quantum operation (47), we can get the operator-sum representation. Suppose the system is in a state ρ, while the environment is in a pure state $|e_0\rangle\langle e_0|$ and $\{\langle e_k|\}$ is an orthonormal basis of the Hilbert space of the environment. Then (47) gives

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U\left(\rho \otimes |e_0\rangle\langle e_0|\right)U^\dagger|e_k\rangle = \sum_k E_k \rho E_k^\dagger \tag{49}$$

where $E_k = \langle e_k|U|e_0\rangle$ is an operator on the state space of the system. The second equation of (49) is known as the *operator-sum representation* of $\mathcal{E}$, and the operators $\{E_k\}$ are the *operation elements* of $\mathcal{E}$.

- There is another interpretation. After the unitary transformation U, we apply a measurement $|e_k\rangle\langle e_k|$ of the environment and get a state of the composite system as

  $$\rho_k^{\mathrm{SE}} = \frac{|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|}{\mathrm{tr}(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|)} = \frac{|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|}{\mathrm{tr}_{\mathrm{S}}(E_k\rho E_k^\dagger)} \tag{50}$$

  with a probability

  $$p(k) = \mathrm{tr}(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|) = \mathrm{tr}_{\mathrm{S}}(E_k\rho E_k^\dagger). \tag{51}$$

  After partial tracing the environment, we get the state of the system as

  $$\rho_k^{\mathrm{S}} = \mathrm{tr}_{\mathrm{E}}(\rho_k^{\mathrm{SE}}) = \frac{\mathrm{tr}_{\mathrm{E}}(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|)}{\mathrm{tr}_{\mathrm{S}}(E_k\rho E_k^\dagger)} = \frac{E_k\rho E_k^\dagger}{\mathrm{tr}_{\mathrm{S}}(E_k\rho E_k^\dagger)}, \tag{52}$$

  and the corresponding probability remains the same as $p(k)$. Summing up the results of all possible measurements of the environment, we get the final state of the system

  $$\mathcal{E}(\rho) = \sum_k p(k)\rho_k^{\mathrm{S}} = \sum_k E_k\rho E_k^\dagger. \tag{53}$$

And it's natural that the total probability equals one, i.e.,

$$1 = \sum_k p(k) = \mathrm{tr}_\mathrm{S}(\sum_k E_k^\dagger E_k \rho). \tag{54}$$

Since ρ is arbitrary, we get the so-called *completeness relation*,

$$\sum_k E_k^\dagger E_k = 1. \tag{55}$$

- The above quantum process is analogous to the classical noise process. Classical initial and final states are described by vectors of probabilities, while the quantum state of the system is described by the density operator ρ or $\mathcal{E}(\rho)$. The classical state is transformed by the evolution matrix as (45), while the quantum state is transformed by the quantum operation as (49). The classical evolution matrix satisfies the completeness relation, while the quantum operation elements also satisfy the completeness relation (55). The set of quantum operation operators is called *trace-preserving*, if it satisfy the completeness relation.

Quantum operation can also be used to describe the process of a measurement of the system. Suppose the system is in the state ρ^S, and the joint state of the system and the environment is $\rho^\mathrm{SE} = \rho^\mathrm{S} \otimes |e_0\rangle\langle e_0|$. Then the composite system evolves by the unitary transformation U, after that a projective measurement P_m is performed on the composite system. The final state is

$$\frac{P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m}{\mathrm{tr}(P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m)}, \tag{56}$$

partial tracing out the environment, we get

$$\frac{\mathrm{tr}_\mathrm{E}(P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m)}{\mathrm{tr}(P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m)}. \tag{57}$$

So we define the quantum operation as

$$\mathcal{E}_m(\rho) = \mathrm{tr}_\mathrm{E}(P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m), \tag{58}$$

and it's operator-sum representation is

$$\begin{aligned} \mathcal{E}_m(\rho) &= \sum_{kj} \mathrm{tr}_\mathrm{E}(|e_k\rangle\langle e_k| P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m |e_j\rangle\langle e_j|) \\ &= \sum_k \langle e_k| P_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P_m |e_k\rangle \\ &= \sum_k E_k \rho E_k^\dagger \end{aligned} \tag{59}$$

with $E_k = \langle e_k|P_m U|e_0\rangle$.

5 Quantum error-correction

This chapter covers three topics: quantum error-correcting codes, fault-tolerant quantum computation, and the threshold theorem.

5.1 Quantum error-correction code

The key idea of error-correction codes is that we should *encode* the message by adding some redundant information to the message, so even if some of the information in the encoded message is corrupted by noise, there will be enough redundancy in the encoded message to recover or *decode* the message.

Consider a simple classical example, a bit is transmitted through a noisy channel, with the probability of flipping being p. To protect the bit, we can simply replace it by three copies of itself as

$$0 \to 000, \quad 1 \to 111. \tag{60}$$

We can decode the output from the channel by assuming that the output value is whatever value appears more times in the output. The probability that two or more of the bits are flipped is $p_e = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$. Then if $p < 1/2$, the code is more reliable for $p < p_e$.

5.2 Theory of quantum error-correction

After encoding the original quantum state into a quantum error-correcting code, the code experiences a *noisy process*, and then the *error syndrome* and a *recovery* operation are performed. We assume the noise is described by a quantum operation $\mathcal{E}$ and the complete error-correction procedure is described by quantum operation $\mathcal{R}$.

6 Quantum computer

6.1 Conditions for quantum computer

A quantum computer has to be *well isolated* in order to retain its quantum properties, but at the same time its qubits have to be *accessible* so that they can be manipulated to perform a computation and to read out the result.

Any physical systems suffer unwanted interactions with the outside world, called *quantum noise* or *decoherence*, and other different noises. A simple index can characterize these, the length of the longest possible quantum computation, which is roughly given by the ratio of τ_Q to τ_{op}. τ_Q is the time for which a system remains quantum mechanically coherent, and τ_{op} is the time to perform a elementary unitary transformation.

There are four basic requirements for quantum computation.

- Robustly represent quantum information. A qubit is a two-dimensional Hilbert space, then it's desirable to make the physical realization of a qubit to be a two-level quantum system, at least a *finite-level* quantum system. For a finite-level quantum system, it's still possible to appear decoherence for the qubit, i.e., the transitions from the superposition state of two chosen states to other unwanted states. For single qubits, the figure of merit is the *minimum lifetime of arbitrary superposition states.* T_1, the longitudinal relaxation time of the higher energy $|1\rangle$ state, is just a classical state lifetime, while T_2, the transverse relaxation time of states such as $|0\rangle + |1\rangle/\sqrt{2}$ is a good measure.

- Prepare a fiducial initial state. One of the most important requirements for being able to perform a useful computation is to be able to prepare the desired input. For quantum computation, it is only necessary to be able to *repeatedly* produce *one specific* quantum state with *high fidelity*, since a unitary transformation can turn it into any other desired input state. So input state preparation is a significant problem for most physical systems. Two figures of merit are relevant to input state preparation: the *minimum fidelity* with which the initial state can be prepared in a given state ρ_{in}, and the *entropy* of ρ_{in}.

- Performance of unitary transformation. We need to control the Hamilonian of a quantum system to realize the universal qubit gates, and we also need to require the ability to address individual qubits and to apply unitary gates to selected qubits. There are also many sources of decoherence, for example, unrecorded imperfections in unitary transformations, the cumulative effect of systematic errors, the back-action of the control system. Two figures of merit for unitary transforms are: the minimum achievable fidelity F and the maximum time t_{op} required to perform elementary operations.

- Measurement of output result. The output from a good quantum algorithm is a superposition state which gives a useful answer with high probability when measured. There are still many difficulties. A good figure is the signal to noise ratio.

A Complex roots of unity

A complex nth root of unity is a complex number ω such that $\omega^n = 1$. There are exactly n complex nth roots of unity:

$$e^{\frac{2\pi i}{n}k} \quad \text{for} \quad k = 0, 1, \cdots, n-1. \tag{61}$$

The value $\omega_n = e^{\frac{2\pi i}{n}}$ is called the principal nth root of unity, then the n complex roots are

$$\{\omega_n^0, \omega_n^1, \cdots, \omega_n^{n-1}\}. \tag{62}$$

The n complex roots of unity are equally spaced around the circle of unit radius centered at the origin of the complex plane. There are some properties we need to note:

- Cancellation lemma. For any integers $n \geq 0$, $k \geq 0$, and $d > 0$,

$$\omega_{dn}^{dk} = \omega_n^k. \tag{63}$$

- Halving lemma. If $n > 0$ is even, then the squares of the n complex nth roots of unity are the $n/2$ complex $\frac{n}{2}$th roots of unity.

- Summation lemma. For any integer $n \geq 1$ and nonzero integer k not divisible by n,

$$\sum_{j=0}^{n-1} (\omega_n^k)^j = 0. \tag{64}$$

B Discrete Fourier Transform

The discrete Fourier transform is an invertible, linear transformation $\mathcal{F} : \mathbb{C}^N \to \mathbb{C}^N$. For a sequence of N complex numbers, $\mathcal{F} : \{x_0, x_1, \cdots, x_{N-1}\} \to \{y_0, y_1, \cdots, y_{N-1}\}$ is defined by

$$y_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N}kn}. \tag{65}$$

Its inverse transformation is given by

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} y_k e^{\frac{2\pi i}{N}kn}. \tag{66}$$

There are some special properties we need to note:

- Orthogonality. Let u_k be a vector $(1, e^{\frac{2\pi i}{N}k}, e^{\frac{2\pi i}{N}2k}, \cdots, e^{\frac{2\pi i}{N}(N-1)k})^T$, then

$$u_k^T u_l^* = \sum_{n=0}^{N-1} e^{\frac{2\pi i}{N}nk} e^{-\frac{2\pi i}{N}nl} = N\delta_{kl}. \tag{67}$$

- Parseval's theorem. Let $\{y_k\}$ and $\{w_k\}$ are the DFTs of $\{x_n\}$ and $\{z_n\}$, then

$$\sum_{n=0}^{N-1} x_n z_n^* = \frac{1}{N} \sum_{k=0}^{N-1} y_k w_k^*. \tag{68}$$