

Quantum Information and Quantum Computation

Wang Chao

January 26, 2021

Contents

1	Foundation	5
1.1	Density Matrix	5
1.2	Orthogonal Measurement	6
1.3	Positive Operator-valued Measure	6
1.4	Quantum Channel	6
1.5	Evolution	8
1.6	Markovian Evolution	9
2	Entanglement	11
3	Quantum Information	13
4	Quantum Computation	15
4.1	Quantum Fourier Transformation on \mathbb{Z}_{2^n}	15
4.2	Period Finding	16
4.3	Shor Algorithm	17
5	Quantum Error Correction	19
6	Topological Quantum Computation	21

Chapter 1

Foundation

The whole universe is a large quantum system. Theoretically, any two particles in the universe are correlated. However, we usually care about physical properties of a small part of the universe. We call this part system and the rest environment. Let $|\Psi\rangle$ be a state of the universe. We can construct the state of the system as the reduced density matrix:

$$\rho = \text{tr}_{env}(|\Psi\rangle\langle\Psi|) \quad (1.1)$$

This seems superfluous at first sight. However, in practice we lack the exact information of $|\Psi\rangle$. ρ still provides the enough information we need about the system.

1.1 Density Matrix

Let H be the Hilbert space of a system. From previous discussion we know that if the system is entangled with the environment, the state of the system may be described by a matrix $\rho \in H^2$. However, ρ needs to satisfy a few conditions to make sense:

1. $\text{tr } \rho = 1$.
2. $\rho = \rho^\dagger$.
3. ρ is semi-positive definite.

It's easy to see that density matrices form a convex set in $H \otimes H$, and the interior of this set contains positive definite density matrices.

Definition 1.1.1. We call ρ a pure state if there exists some $|\Psi\rangle \in H$ such that $\rho = |\Psi\rangle\langle\Psi|$. Otherwise we call ρ a mixed state.

Lemma 1.1.2. Only pure states are extremal points(points that are not linear combination of other points).

Proof. Since ρ is semi-positive definite, $\langle a|\rho|a\rangle = 0 \rightarrow \rho|a\rangle = 0$. Let $\rho = |\Psi\rangle\langle\Psi|$ be a pure state. If $\rho = \lambda\rho_1 + (1 - \lambda)\rho_2$ and $\lambda \neq 0, 1$. Then for each $|\Psi^\perp\rangle$ perpendicular to $|\Psi\rangle$, $\langle\Psi^\perp|\rho_1|\Psi^\perp\rangle = \langle\Psi^\perp|\rho_2|\Psi^\perp\rangle = 0$. This leads to that $\rho_1 = \rho_2 = |\Psi\rangle\langle\Psi|$. \square

1.2 Orthogonal Measurement

Let $O = O_{sys} \otimes I_{env}$ be an observable in the universe. We can decompose $O_{sys} = \sum_i o_i P_i$, where

1. P_i is Hermitian
2. $\sum_i P_i = I$
3. $P_i P_j = \delta_{ij} P_i$

P_i is the projective operator into the subspace with eigenvalue o_i . The measurement can also be denoted by (o_i, P_i) . After measurement, the state $|\Psi\rangle$ has the chance $\|P_i \otimes I|\Psi\rangle\|^2$ to collapse into the state $P_i \otimes I|\Psi\rangle / \|P_i \otimes I|\Psi\rangle\|$, with measure value o_i .

If we represent the state of the system by density matrix $\rho = \text{tr}_{env}(|\Psi\rangle\langle\Psi|)$. Then the state has the chance

$$\|P_i \otimes I|\Psi\rangle\|^2 = \langle\Psi|(P_i \otimes I)^2|\Psi\rangle = \text{tr}(P_i^2 \otimes I|\Psi\rangle\langle\Psi|) = \text{tr}_{sys}(P_i^2 \rho) \quad (1.2)$$

to collapse into the state

$$\text{tr}_{env}(P_i \otimes I|\Psi\rangle\langle\Psi|P_i \otimes I) / \text{tr}_{sys}(P_i^2 \rho) = P_i \rho P_i / \text{tr}_{sys}(P_i^2 \rho) \quad (1.3)$$

with measure value o_i .

1.3 Positive Operator-valued Measure

Let's consider a more general measure (o_i, E_i) , where

1. E_i is Hermitian
2. $\sum_i E_i = I$
3. E_i is semi-positive

After measurement, the state ρ has the chance $\text{tr}(E_i \rho)$ to collapse into the state $M_i \rho M_i^\dagger / \text{tr}(E_i \rho)$ where $E_i = M_i^\dagger M_i$.

This is called positive operator-valued measure (POVM).

POVM can be realized by entangle the system with an auxiliary space $\rho \rightarrow \rho \otimes |0\rangle\langle 0| \in (H_{sys} \otimes H_{aux})^2$. We find a unitary transformation U such that $U|\psi\rangle \otimes |0\rangle = \sum_i (M_i |\psi\rangle) \otimes |i\rangle$. The existence of U is equivalent to that $\sum_i M_i^\dagger M_i = I$. Then POVM can be realized by measuring $H_{sys} \otimes H_{aux}$ by $(o_i, I \otimes |i\rangle\langle i|)$.

1.4 Quantum Channel

A quantum channel is a linear map of density operator

$$\mathcal{E}(\rho) = \sum_a M_a \rho M_a^\dagger \quad (1.4)$$

where $\{M_a\}$ be a set of operators such that $\sum_a M_a^\dagger M_a = I$, called Kraus operators of the channel.

A quantum channel has following easily verified properties:

Definition 1.4.1. A trace-preserving completely positive map \mathcal{E} is a linear map that

1. Preserves positivity completely, that is, $I_k \otimes \mathcal{E}$ preserves Hermiticity and positivity for all positive integer k : $\rho = \rho^\dagger \rightarrow I_k \otimes \mathcal{E}(\rho) = I_k \otimes \mathcal{E}(\rho)^\dagger$ and $\rho \geq 0 \rightarrow I_k \otimes \mathcal{E}(\rho) \geq 0$
2. Preserves trace: $\text{tr}(\mathcal{E}(\rho)) = \text{tr}(\rho)$

Lemma 1.4.2. A quantum channel is a trace-preserving completely positive map

Lemma 1.4.3. A trace-preserving completely positive map is a quantum channel

Proof. Let $\mathcal{E}(\rho)_{kl} = \rho_{ij} C_{ijkl}$. Since C_{ijkl} is completely positive, by Choi's theorem, $C_{ijkl} = C_{jilk}^*$ and C_{ijkl} is semi-positive between ik and jl . The former is obvious and the latter can be seen from the positivity of $I_n \otimes \mathcal{E}$, as illustrated in Fig. 1.1. Thus $C_{ijkl} = \sum_a M_{aki} M_{alj}^*$. Since C_{ijkl} preserves trace, $\sum_a M_a^\dagger M_a = I$. \square

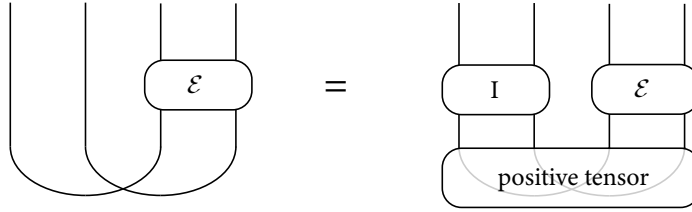


Figure 1.1: Positivity of trace-preserving completely positive map

Definition 1.4.4. A quantum channel \mathcal{E} is called unitary if $\mathcal{E}(\rho) = U\rho U^\dagger$ for a unitary operator U .

Lemma 1.4.5. Let A_{ijkl} and B_{ijkl} be two tensors of index dimension N , such that







1. $A_{ijkl} = A_{klji}^*$ and A_{ijkl} is semi-positive between ij and kl
2. $B_{ijkl} = B_{klji}^*$ and B_{ijkl} is semi-positive between ij and kl
3. $A_{ijkl} B_{jmln} = \delta_{im} \delta_{kn}$

Then $A_{ijkl} = a_{ij}^* a_{kl}$ and $B_{ijkl} = b_{ij}^* b_{kl}$.

The lemma can be expressed in graphical language. Let $\begin{array}{c} \text{---} \\ | \\ \text{A} \\ | \\ \text{---} \end{array}$ and $\begin{array}{c} \text{---} \\ | \\ \text{B} \\ | \\ \text{---} \end{array}$ be Hermitian and semi-positive tensors between their left and right indices, and

$$\text{and } \begin{array}{c} \text{---} \\ | \\ \text{B} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{b}^* \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{b} \\ | \\ \text{---} \end{array} .$$

$$\begin{array}{c} \text{---} \\ | \\ \text{A} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{a}^* \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{a} \\ | \\ \text{---} \end{array} .$$

Clearly  =  and  =  . Since  =  , $D(ij, kl) = 1$ for

RHS. So $D(i, j) = 1$ and $D(ij, kl) = N$, which means

The diagram shows a vertical stack of two nodes, 'b' on top and 'a' on bottom, connected by a vertical line. This is equal to a sum over indices i and j of two separate nodes, i and j , each represented by a circle with a horizontal line through its center. This sum is multiplied by a vertical line with index k at the top and index l at the bottom. To the right of this diagram, the text says "So for $D(i, jkl) =$ ".

Corollary 1.4.6. *A quantum channel is invertible iff it's unitary.*

The quantum channel is a model to describe the evolution of the system with entanglement to the environment. We assume that initially there's no entanglement between the system and the environment. The state of the universe is

This may sound absurd since if there's no entanglement between the system and the environment, the system is in pure state. So we may modify our assumption. We assume that the system has no entanglement with its nearby environment. The system may have entanglement with some remote part of the environment. That is, the state of the universe of a local region around the system is

After a short period of time, the local region evolve by a unitary evolution U .

$$\rho'_{local} = U \rho_{local} U^\dagger + \rho_{int} \quad (1.7)$$

where ρ_{ent} described the impact of the interaction between the local region and the rest.

The system would be in state

$$\rho'_{sys} = \text{tr}_{nb \ env}[U \rho_{local} U^\dagger] + \text{tr}_{nb \ env} \rho_{int} \quad (1.8)$$

Here we may omit the influence of interaction between the local region and the rest on the state of the system, since it only has local impact. Then

$$\rho'_{sys} = \text{tr}_{nb \ env}[U \rho_{sys} \otimes \rho_{nb \ env} U^\dagger] \quad (1.9)$$

This is a quantum channel with transformation tensor $C_{ijkl} = \delta_{ik} \delta_{jl} + \mathcal{O}(dt)$. Let

$$C_{ijkl} = \sum_a \lambda_a U_{a,ki} U_{a,lj}^* \quad (1.10)$$

Since $C_{ijkl} C_{jilk} = \sum_i \lambda_i^2 = D^2 + \mathcal{O}(dt)$ and $C_{ijij} = \sum_i \lambda_i = D + \mathcal{O}(dt)$. We have $\lambda_0 = D + \mathcal{O}(dt)$ and $\lambda_i = \mathcal{O}(dt)$ when $i > 0$.

Then

$$\lambda_0 U_{0,ki} U_{0,lj}^* = \delta_{ik} \delta_{jl} + \mathcal{O}(dt) \quad (1.11)$$

By contraction with δ_{ik} on both sides, we see that $U_{0,ij} = e^{i\theta} \frac{1}{\sqrt{D}} \delta_{ij} + \mathcal{O}(dt)$.

Then we conclude

$$C_{ijkl} = \sum_a M_{aki} M_{alj}^* \quad (1.12)$$

where

$$M_{0ij} = \delta_{ij} - idt H_{ij} + dt K_{ij} \quad (1.13)$$

$$M_{aij} = \sqrt{dt} L_{aij} \quad (a > 0) \quad (1.14)$$

Here, H and K are Hermitian. H , K and L_a are $\mathcal{O}(1)$.

Since $\sum_a M_a^\dagger M_a = I$, we have $2K = -\sum_{a>0} L_a^\dagger L_a$.

Let \mathcal{E} and \mathcal{E}' be two infinitesimal quantum channels with Hamiltonian H and H' and Lindblad operators $\{L_a\}$ and $\{L'_a\}$. Then $\mathcal{E} \circ \mathcal{E}' = \mathcal{E}' \circ \mathcal{E}$ is the quantum channels with Hamiltonian $H + H'$ and Lindblad operators $\{L_a, L'_a\}$.

1.6 Markovian Evolution

Let's consider an evolution process from t_0 to t_2 . As before, we assume the state at t_0 has no entanglement with its nearby environment. However, at each $t_1 \in (t_0, t_2)$, the system has entanglement with its nearby environment. So the quantum channel from t_0 to t_2 is not the composition of one from t_0 to t_1 and one from t_1 to t_2 . In other words, the evolution from t_1 to t_2 requires information of the environment that has been transferred from the system during the time period from t_0 to t_1 . The evolution is non-Markovian.

However, if we make the assumption has the the information transferred from the system to the environment dissipate really fast. Then at each time, the system has no entanglement with its nearby environment. Then the global quantum channel is the composition of infinitesimal quantum channels:

$$\mathcal{E}_{t \rightarrow t'} = \mathcal{E}_{t' - \Delta t \rightarrow t'} \circ \cdots \circ \mathcal{E}_{t \rightarrow t + \Delta t} \quad (1.15)$$

The evolution of the system can be described by a differential equation

$$\rho(t + \Delta t) = \sum_a M_a \rho(t) M_a^\dagger \quad (1.16)$$

$$= (I - i dt H + dt K) \rho(t) (I + i dt H + dt K) + \sum_{a>0} L_a \rho L_a^\dagger \quad (1.17)$$

$$\dot{\rho} = -i[H, \rho] + \sum_{a>0} (L_a \rho L_a^\dagger - \frac{1}{2} \rho L_a^\dagger L_a - \frac{1}{2} L_a^\dagger L_a \rho) \quad (1.18)$$

Chapter 2

Entanglement

Chapter 3

Quantum Information

Chapter 4

Quantum Computation

4.1 Quantum Fourier Transformation on \mathbb{Z}_{2^n}

The Fourier transformation is the unitary operator F_N such that

$$F_N \sum_x f(x)|x\rangle = \frac{1}{\sqrt{N}} \sum_y \sum_x f(x) e^{2\pi i xy/N} |y\rangle \quad (4.1)$$

For each basis vector $|x\rangle$,

$$F_N |x\rangle = \frac{1}{\sqrt{N}} \sum_y e^{2\pi i xy/N} |y\rangle \quad (4.2)$$

Let $N = 2^n$, and

$$x = \sum_i x_i 2^i \quad (4.3)$$

$$y = \sum_i y_i 2^i \quad (4.4)$$

Then

$$xy = \sum_i y_i 2^i \sum_j x_j 2^j \equiv \sum_i y_i \sum_{i+j < n} x_j 2^{i+j} \pmod{N} \quad (4.5)$$

The Fourier transformation on a basis becomes

$$F_N |x\rangle = \frac{1}{\sqrt{N}} \sum_y e^{2\pi i \sum_i y_i \sum_{i+j < n} x_j 2^{i+j}/N} |y\rangle \quad (4.6)$$

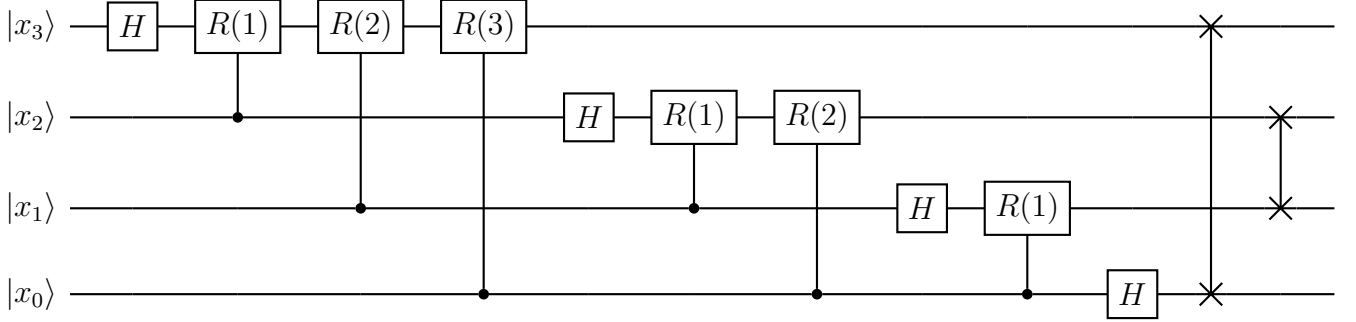
$$= \frac{1}{\sqrt{N}} \bigotimes_{i=0}^{n-1} \sum_{y_i} e^{2\pi i y_i \sum_{i+j < n} x_j 2^{i+j}/N} |y_i\rangle \quad (4.7)$$

$$= \bigotimes_{i=0}^{n-1} \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i \sum_{i+j < n} x_j 2^{i+j-n}} |1\rangle) \quad (4.8)$$

$$= \text{Inv} \bigotimes_{i=0}^{n-1} \frac{1}{\sqrt{2}} (|0\rangle + e^{\pi i \sum_{j \leq i} x_j 2^{j-i}} |1\rangle) \quad (4.9)$$

$$= \text{Inv} \prod_{i=n-1}^0 \prod_{j=i-1}^0 R_{ji}(i-j) H_i |x\rangle \quad (4.10)$$

where H_i is Hadamard gate on qubit i , Inv is the operator $|x_0 \dots x_{n-1}\rangle \mapsto |x_{n-1} \dots x_0\rangle$, and $R_{ji}(d)$ is operator $\text{diag}(1, e^{i\pi/2^d})$ on qubit i controlled by qubit j .



This method can be generalized into quantum Fourier transformation on a ring $\prod_i \mathbb{Z}_{N_i}$.

4.2 Period Finding

Let $f(x)$ be a periodic function on \mathbb{Z}_N with period r . Let's suppose there's a unitary transformation $U : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$. Choose $N > r^2$. Then

$$U \sum_{x=1, \dots, N} |x\rangle|0\rangle = \sum_{x=1, \dots, N} |x\rangle|f(x)\rangle \quad (4.11)$$

Then let's measure the second register and get result a . The state in first register becomes

$$\sum_{x=1, \dots, N, f(x)=a} |x\rangle = \sum_{n=1, \dots, M} |x_0 + nr\rangle \quad (4.12)$$

where x_0 is the smallest integer such that $f(x_0) = a$, and $x_0 + Mr$ is the largest integer.

After quantum Fourier transformation, the state becomes

$$\frac{1}{\sqrt{N}} \sum_{q=1, \dots, N} \left(\sum_{n=1, \dots, M} e^{2\pi i (x_0 + nr)q/N} \right) |q\rangle \quad (4.13)$$

The peaks of this distribution is at $\frac{q}{N} = \frac{j}{r}$. By Preskill, the probability of measured value of $\frac{q}{N}$ to fall in $[\frac{j}{r} - \frac{1}{2N}, \frac{j}{r} + \frac{1}{2N}]$ for some j is $> \frac{4}{\pi^2}$. If we measure $\frac{q}{N}$ and approximated the result, which is close to $\frac{j}{r}$, by a rational $\frac{a}{b}$ such that $b < \sqrt{N}$, clearly $a/b = j/r$. Thus we can obtain $\frac{j}{r}$ by applying continued fraction algorithm to the measure value of $\frac{q}{N}$. Chances are that j and r are coprime, and we obtain r .

This method can be generalized into functions over a ring $\prod_i \mathbb{Z}_{N_i}$, such Simon's method on $\mathbb{Z}_2^{\otimes n}$.

4.3 Shor Algorithm

The algorithm to factor a number N is

1. Randomly choose a number $a < N$ coprime to N
2. Use quantum algorithm to find smallest r such that $a^r \equiv 1 \pmod{N}$.
3. If r is odd, change a and restart. If r is even, we have $(a^{r/2} + 1)(a^{r/2} - 1) \equiv 0 \pmod{N}$
4. Clearly $(a^{r/2} - 1) \not\equiv 0 \pmod{N}$. If $(a^{r/2} + 1) \equiv 0 \pmod{N}$, change a and restart. Otherwise, $\gcd(a^{r/2} + 1, N)$ is a nontrivial divisor of N .

r can be obtained by finding the period of the function

$$f_{a,N}(x) = a^x \pmod{N} \quad (4.14)$$

using the previous algorithm.

Here we provide the quantum circuit to perform $U|x\rangle|1\rangle = |x\rangle|f_{a,N}(x)\rangle$. Let's express x as a binary expansion

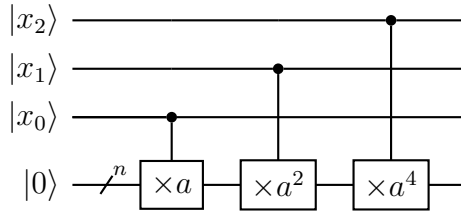
$$x = \sum_i x_i \cdot 2^i \quad (4.15)$$

Then

$$a^x \pmod{N} = a^{\sum_i x_i \cdot 2^i} \pmod{N} = \prod (a^{2^i})^{x_i} \pmod{N} = \prod (a_i)^{x_i} \pmod{N} \quad (4.16)$$

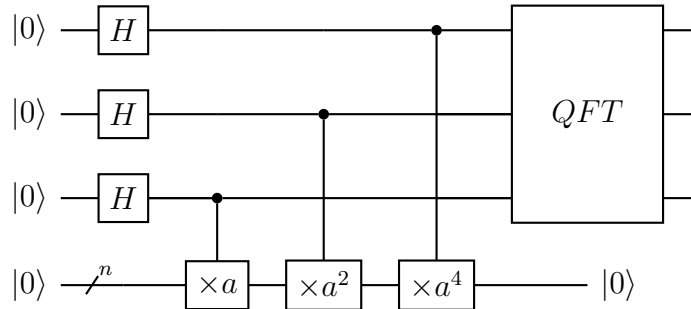
where $a_i = (a^{2^i}) \pmod{N}$ and can be calculated by $a_i = (a_{i-1})^2 \pmod{N}$.

The quantum circuit to perform $U|x\rangle|1\rangle = |x\rangle|f_{a,N}(x)\rangle$ is



where $|1\rangle$ is encoded by $|0\rangle^{\otimes n}$.

The whole circuit of Shor's algorithm is



Chapter 5

Quantum Error Correction

Chapter 6

Topological Quantum Computation