Local Hamiltonian and Quantum PCP Theorem

Quantum Complexity and Theoretical Physics

Lecturer: Zhengyi Han

Spring 2023

Today we are going to talk about the ground state energy of local Hamiltonians. The "locality" is naturally associated with the spatial geometry of the system, where the most natural interaction between degrees of freedom are those local ones, for instance nearest neighbor interactions. The ground states of these systems exhibit special correlation/entanglement properties. Exploring these properties is the central topic in this lecture.

1 Local Hamiltonian is in QMA

1.1 Some Examples

Definition 1. (k-local Hamiltonians) A k-local Hamiltonian H acts on n qubits, here k is a constant. H can be written as a sum of local Hamiltonian terms, that is,

$$H = \sum_{i=1}^{m} H_i. \tag{1}$$

Each H_i acts nontrivially on k' qubits ($k' \leq k$) and acts trivially on the others.

H can be diagonalized as

$$H = \sum_i \lambda_i |\psi_i\rangle \langle\psi_i| \tag{2}$$

λ_is are different energy levels of the system, and $|\psi_i\rangle$s are the corresponding eigenstates. The Hamiltonian assigns every state ϕ an energy:

$$\langle\phi| H |\phi\rangle = \sum_i \lambda_i |\langle\psi|\phi\rangle|^2 \tag{3}$$

Example 1. (The quantum Ising model) Consider N qubits arranged on a ring. The transverse field Ising model describes a nearest-neighbor magnetic dipole interaction along the Z axis when all spins are subject to a transverse magnetic field along the X axis. The family of such Hamiltonians is given by:

$$H(g) = -\sum_{i=1}^{N} Z_i \otimes Z_{i+1} - g \sum_{i=1}^{N} X_i, \tag{4}$$

where g is a real parameter corresponding to the strength of the transverse field.

Example 2. (The quantum Heisenberg model) It is a generalization of the quantum Ising model. It includes magnetic dipole interactions along X, Y, Z axes. It models the behavior of quantum magnetism in atomic systems. The Hamiltonian can be written as follows:

$$H(J_x, J_y, J_z, g) = J_x \sum_i X_i X_{i+1} + J_y \sum_i Y_i Y_{i+1} + J_z \sum_i Z_i Z_{i+1} + g \sum_i X_i, \tag{5}$$

where J_x, J_y, J_z, g are real parameters. We claim that the ground state is a non-trivial entangled state. Let's consider the local Hamiltonian acting on the i-th and $i+1$-th qubits. The singlet state $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is a eigenstate of those Hamiltonians. And $|\psi_-\rangle$ is maximally entangled. However, we cannot construct such a global state. Because the entanglement is "monogamous". So the ground state cannot satisfy the constraint so perfectly.

1.2 Quantum CSP

For the quantum Ising model, we take $g = 0$. Then it becomes the classical Ising model. We can consider a more complicated case than the ring. Let $G = (V, E)$, a graph with n vertices. We consider such a Hamiltonian:

$$H = \sum_{(u,v)\in E} Z_u \otimes Z_v \tag{6}$$

Solving the ground state of the Hamiltonian can get the Max-Cut of the graph. To see this, we need to do some computation. The operator can be diagonalized:

$$Z_u \otimes Z_v = |00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11| \tag{7}$$

Note that, it has two eigenvalues. $+1$ corresponds with $|00\rangle, |11\rangle$, and -1 corresponds with $|01\rangle, |10\rangle$. We consider $0, 1$ as the label of the two sets. If two points are in the same set, $Z_u \otimes Z_v$ assigns a $+1$ energy penalty.

To develop such an idea, we rewrite our formula:

$$Z_u \otimes Z_v = \sum_{x_u, x_v \in \{0,1\}} \gamma(x_u, x_v) |x_u x_v\rangle\langle x_u x_v| . \tag{8}$$

$\gamma(x_u, x_v) = 1$ if $x_u = x_v$. Otherwise -1. Then we can write H in such format:

$$H = \sum_{(u,v)} \sum_{x_u, x_v \in \{0,1\}} \gamma(x_u, x_v) |\cdots x_u \cdots x_v \cdots\rangle\langle \cdots x_u \cdots x_v \cdots| \tag{9}$$

$$= \sum_{x\in\{0,1\}^n} \left(\sum_{(u,v)\in E} \gamma(x_u, x_v) \right) |x\rangle\langle x| \tag{10}$$

Hence we diagonalize the Hamiltonian. The ground state is the solution to this problem. And we can get the size of the Max-Cut from the ground energy easily.

That is to say, the ground state of Ising model $H(g = 0)$ is a simple unentangled state (even a bit string). Similarly, when g is very large, the transverse field part of H dominates. The ground state is $|+\rangle^{\otimes N}$. It is also the classical case. While, when $g \neq 0$, since $Z_i \otimes Z_{i+1}$ and $X_i \otimes I_{i+1}$ do not commute, we can not diagonalize the Hamiltonian easily. The ground states of these Hamiltonians will in general exhibit interesting properties.

Max-Cut is in **NP**-completeness. The quantum Ising model can be viewed as quantum Max-Cut. We want to study the quantum analogue of NP. Constraint satisfaction problems (CSP) are in NP. What problem is in quantum NP?

Definition 2. (QMA) A language $L \in$ QMA if there exists a classical polynomial time algorithm A maps inputs $x \in \{0,1\}^*$ to quantum circuits C_x on $n+q = \text{poly}(|x|)$ qubits, such that:

- Completeness: $x \in L \ \Rightarrow \exists \, |\psi\rangle$, such that $\Pr(C_x \text{ accepts } \ |0_n\rangle \otimes |\psi\rangle) \geq 2/3$
- Soundness: $x \in L \ \Rightarrow \forall \, |\psi\rangle \, , \Pr(C_x \text{ accepts } \ |0_n\rangle \otimes |\psi\rangle) \leq 1/3$

Hamiltonian terms are the analogue of classical constraints. The energy are the quantum analogue of solution qualities. For more items, we can refer to the following diagram.

Classical	Quantum
Constraint Satisfaction Problem (CSP)	Hamiltonian
Variables	Qubits
Constraints	Hamiltonian terms
Solution quality	Energy
Optimal solution	Ground state
P	BQP
NP	QMA
Cook-Levin SAT formula	Feynman-Kitaev Hamiltonian

Definition 3. (k-local Hamiltonian problem) Given a $k-$LOCAL-HAM$_{a,b}$ problem, we want to distinguish between:

$$\min_{|\psi\rangle} \langle\psi| H |\psi\rangle \leq a \quad \text{or} \quad \min_{|\psi\rangle} \langle\psi| H |\psi\rangle \geq b,$$

here $a < b$ are real numbers.

Theorem 1. $k-$local Hamiltonian problems are in QMA.

As 3-SAT is complete in NP, LH can be complete in QMA.

Theorem 2. (Quantum Cook-Levin Theorem) $k-$LOCAL-HAM$_{a,b}$ is QMA-complete for $a - b \geq 1/\text{poly}(n)$.

1.3 Why we introduce QMA

Theoretical computer scientists assume that NP $\neq$ QMA, which means that LH do not have an efficient classical proof. In general, the ground state also does not have a useful polynomial-sized description.

It implies that the ground state of a local hamiltonian is likely to be entangled. Otherwise, it can be described easily. Actually, we have known the existence of local Hamiltonians whose ground states are highly entangled. For example, the physical systems being cooled down to near absolute zero exhibit quantum effects like superfluidity, superconductivity or Bose-Einstein condensates.

We give some other examples of QMA-completeness.

Example 3. (Quantum Marginal Problem)
Given a set of local density matrix $\{\rho_j\}$, determine whether there exists an n-particle state ρ, such that $\{\rho_j\}$ are reduced density matrices of ρ. Quantum marginal problems are in QMA-completeness.

Example 4. (N-representability problem) Consider the quantum marginal problem for bosonic or fermionic systems. All the two-particle reduced density matrices (2-RDMs) are the same. We denote it by ρ_2. The corresponding quantum marginal problem is called the N-representability problem. We explain it in the following. (Wen's book Chap4, P95 says the single-particle Hilbert space is no longer a qubit, but in general with a large dimension in order to have non-vanishing fermionic wave function in the first quantization picture. Can you tell me what the RDM matrix is? What is reduced?)

Given a two-particle bosonic or fermionic density matrix ρ_2, determine whether there exists an N-particle bosonic or fermionic state ρ, such that ρ_2 is the two-particle reduced density matrices of ρ.

The N-representability problem is in QMA-complete.

2 Quantum PCP Theorem

2.1 Quantum de Finetti's Theorem and Mean-field Bosonic System

Now we consider a interesting example of many-body bosonic system. It is similar to the N-representability problem. That is, given an integer s, what kind of 2-RDM admits s copy symmetric extension. For example, a biparticle state ρ_{AB}, it can be extended to $\rho_{A,B,B_1,\cdots,B_s}$. There is full symmetry between $B, B_1, \cdots, B_s$. If we take $s \to \infty$, only separable state ρ_{AB} could admit all s-copy symmetry extension. The set of 2-RDMs for this N-boson system contains only states that are very close to separable states when N goes large.

Theorem 3. (Quantum de Finetti's Theorem, simplified version) The k-RDM ρ_k of an N-particle bosonic state can be approximated with an error at most $O(m^2k/N)$ by a mixture of product states of the form $|\alpha\rangle^{\otimes k}$, where α is some single-particle bosonic state.

Theorem 4. (Quantum de Finetti's Theorem, formal version) Let $\rho \in \text{Dens}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right)$ be n-exchangeable. Then there exists a measure μ on $\text{Dens}\left(\mathbb{C}^d\right)$ such that

$$\left\| \text{Tr}_{n-k}(\rho) - \int \sigma^{\otimes k} d\mu(\sigma) \right\|_1 \leq \frac{2k(d+k)}{n+d}, \forall k \leq n$$

For completeness, we list the classical de Finetti's theorem.

Theorem 5. (de Finetti's Theorem) Let P be an n-exchangeable distribution on $[d]^n$ and $\text{Tr}_{n-k}(P)$ be the marginal distribution of P on k elements. Then there exists a measure μ on the set of all distributions on $[d]$ (i.e. the d-simplex) such that $\forall k \leq n$,

$$\left\| Tr_{n-k}(P) - \int Q^{\otimes k} d\mu(Q) \right\| \leq \min\left\{ \frac{2kd}{n}, \frac{k(k-1)}{n} \right\}$$

The quantum de Finetti's theorem provides a explanation for the Hartree's mean-field theory to calculate the ground state energy of a large class of interacting bosonic systems.

Such theory assumes that the ground state is a product state with the form $|\Psi\rangle = |\psi\rangle^{\otimes N}$. So the ground-state energy per particle E_0^h is:

$$E_0^h = \min_{|\Psi_\alpha\rangle} \frac{\langle\Psi_\alpha| H |\Psi_\alpha\rangle}{N} = \frac{1}{2}\min_{|\alpha\rangle} \langle\alpha|^{\otimes 2} H |\alpha\rangle^{\otimes 2}. \tag{11}$$

We want to prove E_0^h is close to the actual ground state energy. Given a arbitary wave function $|\Psi\rangle$, the energy per particle is:

$$\frac{\langle\Psi| H |\Psi\rangle}{N} = \frac{1}{2}\mathrm{Tr}(\rho_2 H_2). \tag{12}$$

When the number of particles goes to infinity, the ground state energy is to minimize the energy from all pure state $|\alpha\rangle$ according to the quantum de Finetti's Theorem

2.2 An Introduction to PCP Theorem

In the QMA setting, we need the gap is portional to $1/\mathrm{poly}(n)$, where n is the number of particles. But maybe the local Hamiltonian terms play an important role in some cases. So can we relax the gap condition while preserve the LH hardness? This is highly related to a conjecture called the "quantum probabilistically checkable proof (quantum PCP)". There is a classical version called "PCP Theorem". To better understand the idea behind such theory, we need to start from the classical version.

Theorem 6. (PCP Theorem, proof checking version)

$\forall \varepsilon > 0$, for all decision problems $L \in$ NP, there exists a randomized polynomial-time verifier V, such that, when given instance x and query access to a proof string y, makes 3 random queries and has the following behavior:

1. Completenesss: If $x \in L_{yes}$, a proof string y such that $V(x, y)$ accepts with probability at least $1 - \varepsilon$.
2. Soundness: If $x \in L_{no}$, then for all proofs y, $V(x, y)$ accepts with probability at most $1/2 + \varepsilon$.

Theorem 7. (PCP Theorem, hardness of approximation version)

The following decision problem L is NP-complete: given a 3SAT formula ϕ, distinguish between $\omega(\phi) = 1$ and $\omega(\phi) \leq 7/8 + \varepsilon$. Here $\omega(\phi)$ is the maximum fraction of constraints that an assignment can satisfy.

The theorem implies that, unless P=NP, there is no polynomial-time algorithm to approximate the maximum number of satisfiable clauses of a 3SAT formula to within 10%.

And the above two theorems are equivalent.

Now let's put our eyes on the quantum analogue of the PCP Theorem.

Conjecture 1. (Quantum PCP Conjecture, proof checking version) For all $\varepsilon > 0$, for all decision problems $L \in$ QMA, there exsits a quantum polynomial-verifier V that, when given instance x and query access to a quantum proof $|\psi\rangle$, makes measurements on $O(1)$ randomly chosen qubits of $|\psi\rangle$ and has the following behavior:

1. If $x \in L_{yes}$, then there exists a proof $|\psi\rangle$ such that $V(x, |\psi\rangle)$ accepts with probability at least $1 - \varepsilon$.
2. If $x \in L_{no}$, then for all proofs $|\psi\rangle$, $V(x, |\psi\rangle)$ accepts with probability at most $1/2 + \varepsilon$.

It's a natural generalization of classical PCP. But the quantum approximation version is a little different.

Conjecture 2. (Quantum PCP conjecture, hardness of approximation version)

There exists $0 \leq \alpha < \beta \leq 1$ such that the following decision problem L is QMA-complete: given a local Hamiltonian $H = \sum_i^m H_i$ acting on n qubits where each H_i is positive semidefinite and $\|H_i\| \leq 1$, determine whether:

- the ground state of H is at most αm
- the ground state of H is at least βm.

We regard the Hamiltonian terms as clauses. So the theorem says that is QMA-hard to determine, up to precision $\pm(\beta - \alpha)$, the maximum fraction of quantum clauses that can be satisfied.

As classical cases, the above two versions are equivalent. Usually, they are called the Hamiltonian Quantum PCP Conjecture.

2.3 Implication for Physics

From LH in QMA, we know that the states with energy close to $\lambda_{\min}$ will generally be complex to describe, which matches our experimental evidence that really weird quantum stuff can happen at temperatures near absolute zero. We want to ask: can large-scale quantum effects be witnessed at energy scales that correspond to something close to "room temperature"?

This question can be formulated in the language of quantum complexity theory rigorously. We consider the amount of energy as a fraction of the total energy range $\lambda_{\max} - \lambda_{\min}$, is a constant that does not go to zero as the number of particles grows.

For the complexity class QMA, if we modify the proof by a classical description, we get the class QCMA. If the ground state $|\psi\rangle$ with polynomial state complexity (i.e. it have a polynomial-sized classical description). It is not known that whether QMA=QCMA. If we assume QMA $\neq$QCMA, it implies the existence of local Hamiltonians whose ground state exhibit super-polynomial description complexity. If the quantum PCP conjecture holds and QMA $\neq$QCMA, It implies not only

their ground states super-polynomial complex, all states of energy at most βm must have super-polynomial complexity. (Assume a state with energy lower than βm has polynomial description, it will be easy to determine the LH problem.)

Another interesting example connected to "room temperature" is in the following.

Consider a physical system, and its Hamiltonian is H. The system is placed in contact with an infinitely large heat bath at temperature T and left to equilibrate, the state of the system would eventually converge to the Gibbs State:

$$\rho(H,T) = \frac{1}{\mathrm{Tr}(e^{-H/T})} e^{-H/T}$$

The Gibbs state is a density matrix, meaning that it is a probabilistic mixture of pure states. As $T \to 0$, the state approaches a uniform mixture over the ground state of H. If we believe that QMA$\neq$QCMA, we believe that in general, $\rho(H,T)$ for very small T will be a mixture of super-polynomial complex states. On the other hand, if the $T \to \infty$, the state approaches $I/2^n$. There is no entanglement in such a maximally mixed state. It is just like the uniform distribution over all possible classical states. Then we want to ask, for such a system with H, what is the cross-over point in temperature, where the state exhibits high complexity entanglement versus low complexity entanglement? The quantum PCP conjecture posits that there are local Hamiltonian H where you have to crank up T to some quantity that scales with n with n before you start seeing complex entanglement disappear.

2.4 No-go Result and NLTS Conjecture

Theorem 8. Quantum PCP cannot hold for local Hamiltonians defined on a grid.

Theorem 9. Quantum PCP cannot hold for local Hamiltonians defined on an expander graph. (Using de Finetti's theorem)

The best candidates so far for Hamiltonians that may be useful for any quantum PCP construction are those come from quantum error-correcting codes. Because such codes are defined by a way of making entanglement robust. But the biggest challenge now is to make these Hamiltonians local.

Theorem 10. (NLTS Conjecture/Theorem)(unformal version)

There exists a family of Hamiltonians whose every low-energy state can not be constructed from constant-depth quantum circuits.

3 Further Reading

1. Henry Yuen. Entanglement Complexity, Lecture 1-6. http://www.henryyuen.net/classes/fall2020/
2. Thomas Vidick. Around the Quantum PCP Conjecture, Lecture 5-7, 12-14. http://users.cms.caltech.edu/ vidick/teaching/286_qPCP/index.html

4 Fourier Analysis on Abelian Groups

4.1 Character Theory

In this subsection, we consider **Locally Compact Abelian Group (LCA)**.

Example 5. $\mathbb{R}, \mathbb{Z}, \mathbb{T} := \mathbb{R}/\mathbb{Z} \simeq \{e^{2\pi i\theta}\}$ are all LCA. Furthermore, $\mathbb{Z}$ is discrete, and $\mathbb{T}$ is compact.

There is a **unique** and **canonical** (Harr) measurement on LCA (up to a scalar). So we can do integration on such groups, such as the finite sum.

Definition 4. A character of a LCA G is a continuous function $\gamma : G \to \mathbb{C}^\times$, such that,

1. $|\gamma(g)| = 1$,
2. $\gamma(a+b) = \gamma(a)\gamma(b)$.

We denote all such functions by $\mathrm{Hom}(G, \mathbb{T})$ or $\hat{G}$. Actually, $\mathrm{Hom}(G, \mathbb{T})$ is also LCA. The multiplication of the group is defined by the multiplication point-wise. We call $\hat{G}$ is the dual group of G. That is to say that,

Theorem 11. The dual group of an LCA is also an LCA.

Example 6. $\hat{\mathbb{R}} = \mathbb{R}$, $\hat{\mathbb{Z}} = \mathbb{T}$, $\hat{\mathbb{T}} = \mathbb{Z}$, $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}$

4.2 Fourier Transform of Abelian Groups

4.3 Quantum Fourier Transform on Finite Abelian Groups

Let's focus on the quantum Fourier transform on an arbitrary finite abelian group G.
Actually, G is isomorphic to $\hat{G}$. (By the fundamental structure theorem of finite abelian groups and the duality of $\mathbb{Z}/n\mathbb{Z}$) The quantum Fourier transform is:

$$F_G := \frac{1}{\sqrt{|G|}} \sum_{x\in G} \sum_{y\in \hat{G}} \chi_y(x) \left|y\right\rangle \left\langle x\right| \tag{13}$$

Definition 5. Hidden Subgroup Problem (HSP): Given a finite Abelian group G, a function $f : G \to \mathbb{C}$, such that $f(x) = f(y) \Leftrightarrow x - y \in H$, H is a subgroup of G, find the hidden subgroup H.

Example 7. Factoring and discrete logarithm problem are also HSP. It equals finding the size of a cyclic subgroup.

Let's see the standard procedure of HSP:

$$\left|G\right\rangle := \frac{1}{\sqrt{G}} \sum_{x\in G} \left|x\right\rangle \left|0\right\rangle \tag{14}$$

Apply the black-box f oracle:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle \tag{15}$$

We now define the coset state:

$$|x + H\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle \tag{16}$$

Then we measure the second register and discard it, we get a random pure state: $|x + H\rangle$. The distribution is uniform on all cosets. Or equivalently, the state can be described as a mixed state:

$$\rho_H := \frac{1}{|H|} \sum_{x \in G} |x + H\rangle \langle x + H| \tag{17}$$

Let's say what happened after applying QFT:

$$|x \hat{+} H\rangle := F_G |x + H\rangle \tag{18}$$

After some calculation:

$$|x \hat{+} H\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in \hat{G}} \chi_y(x) \chi_y(H) |y\rangle \tag{19}$$

here, $\chi(H) = \frac{1}{|H|} \sum_{h \in H} \chi(h)$. We want to argue that, characters only trivial on the subgroup H will count. By the orthogonality of characters:

$$\langle \chi_y, \chi_{y^*} \rangle = \delta_{y,y^*} \tag{20}$$

Let's take χ_{y^*} as a trivial character on H. Then:

$$|x \hat{+} H\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in \hat{G}} \chi_y(x) \sum_{h \in H} \chi_y(h) \chi_{y^*}(h) |y\rangle \tag{21}$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{y : \chi_y(H) = 1} \chi_y(x) |y\rangle \tag{22}$$

Considering the mixed state ρ_H before applying the Fourier transform, we denote it as $\hat{\rho_H}$ then. After some calculation, we can find that

$$\hat{\rho}_H = \frac{|H|}{|G|} \sum_{y : \chi_y(H) = 1} |y\rangle \langle y| \tag{23}$$

That is to say, $\hat{\rho}_H := F_G \rho_H F_G^\dagger$ is diagonal. (Circulant matrix can be diagonalized by Fourier transform.) So we can measure the state under the computational basis without losing any information.

Once we get the result χ_y after measuring, we can calculate its kernal $\ker(\chi_y)$. It's clearly that $H < \cap \ker(\chi_y)$. So the problem is how many times should we measure to get the hidden subgroup H? Suppose after some measuring, we get $K := \cap \ker(\chi_y)$. If $K \not< \ker(\chi_y)$, $|K \cap \ker(\chi_y)| \leq |K|/2$. So the size decreased to its half. What's probability that we get such χ_y? It's greater than $1/2$ by Lagarange's theorem.

5 Fourier Analysis on Finite Non-Abelian Groups

5.1 Representation Theory

We need to list some basic results of representation of finite groups. A representation is a homomorphism $\sigma : G \to GL(V),\ d_\sigma := \dim(V)$. The chatacter of a representation is a function:$\chi_\sigma(g) := \mathrm{Tr}(\sigma(g))$.

1. χ is a conjugate class function.
2. Given two representations, they are isomorphic if they have the same character.
3. For characters of irreducible representations, $\langle \chi, \chi \rangle = 1$, $\langle \chi, \chi' \rangle = 0$ if they are not isomorphic.
4. Given two irreducible representations ϕ, ψ,
   - $\langle \phi_{ij}, \psi_{kl} \rangle = 0$
   - $\langle \phi_{ij}, \psi_{kl} \rangle = 1/n$ if $i = k, j = l$. Otherwise 0.
5. For all irreducible representations $\sigma_1, \cdots, \sigma_m$ of G, $\sum \sigma_i^2 = |G|$.
6. $L \simeq \bigoplus(\sigma \otimes I_{d_\sigma}),\ R \simeq \bigoplus(I_{d_\sigma}) \otimes \sigma^*$

5.2 Fourier Transform on Finite Non-Abelian Groups

The Fourier transform on finite Abelian groups is a ring isomorphism $F : (L(G), +, *) \to (L(\hat{G}), +, \cdot)$ (Convolution Theorem). In Non-Abelian cases, we need to transform the function to matrixes.

By Schur's Orthogonality, $L(G) \simeq \mathbb{C}^{|G|}$. Let $\phi^{(1)}, \cdots, \phi^{(m)}$ be all irreducible representations, $\sqrt{d_k}\phi_{ij}^{(k)}$ form an orthonormal basis for $L(G)$. So we can define the Fourier transform.

Definition 6. We define the Fourier transform $F : L(G) \to M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ by $F(f) = (\hat{f}(\phi^{(1)}), \cdots, \hat{f}(\phi^{(m)}))$, where

$$\hat{f}(\phi^{(k)})_{ij} = |G| \langle f, \phi_{ij}^{(k)} \rangle = \sum f(g)\overline{\phi_{ij}^{(k)}}(g)$$

Such transform is an isomorphism of vector space. Furthermore, it's a ring isomorphism.

We consider the quantum case. $|x\rangle$ is a basis of $L(G)$, it is mapped to the vector space $\bigoplus(\mathbb{C}^{d_\sigma} \times \mathbb{C}^{d_\sigma})$

$$|\hat{x}\rangle := \sum_\sigma \frac{d_\sigma}{\sqrt{|G|}} |\sigma, \sigma(x)\rangle \tag{24}$$

where,

$$|\sigma(x)\rangle := \sum_{j,k} \frac{\sigma(x)_{jk}}{\sqrt{d_\sigma}} |j, k\rangle \tag{25}$$

So we can write the quantum Fourier transform explicitly:

$$F_G := \sum |\hat{x}\rangle \langle x| = \sum_x \sum_\sigma \sqrt{\frac{d_\sigma}{|G|}} \sum_{j,k} \sigma(x)_{j,k} |\sigma, j, k\rangle \langle x| \tag{26}$$

Since the irreducible decompose is not unique, the Fourier transform is also not defined uniquely.

Using the orthogonality, we can verify that F_G is unitary.

In Abelian case, the regular representation $U(x)$ commutes with the density matrix ρ_H, ρ_H can be diaganolized by Fourier transform. So $U(x)$ can also be diaganolized by Fourier transform. While in the non-Abelian case, the left (right) regular representations is blocked diagnoalized.

$$\hat{L}(x) := F_G L(x) F_G^\dagger = \sum |\hat{xy}\rangle \langle \hat{y}| \tag{27}$$

$$= \sum_\sigma \sum_{j,k,l} \sigma(x)_{j,l} |\sigma, j, k\rangle \langle \sigma, l, k| \tag{28}$$

$$= \bigoplus (\sigma(x) \otimes I_{d_\sigma}) \tag{29}$$

5.3 Fourier Sampling

Let's consider HSP in non-Abelian case. The coset state $|gH\rangle := \frac{1}{\sqrt{|H|}} \sum |gh\rangle$. Since cosets are uniform, the mixed state can be described as $\rho_H := \frac{1}{|G|} \sum |gH\rangle \langle gH|$. The regular representations play an important role in the analysis of such functions. This is because:

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum R(h) |g\rangle . \tag{30}$$

Hence we can rewrite the mixed state using the right regular representation.

$$\rho_H = \frac{1}{|G|} \sum R(h) \tag{31}$$

So according to the above study of regular representation, we kown that the density matrix ρ_H is block-diagonalized by Fourier transform.

$$\hat{\rho}_H = F_G \rho_H F_G^\dagger = \frac{1}{|G|} \bigoplus (I_{d_\sigma} \otimes \sigma(H)^*) \tag{32}$$

, where $\sigma(H) := \sum \sigma(h)$.

The probability that result is σ is:

$$\Pr(\sigma) = \frac{1}{|G|} \mathrm{Tr}(I_{d_\sigma} \otimes \sigma(H)^*) = \frac{d_\sigma}{|G|} \sum \chi_\sigma(h)^* \tag{33}$$

So how many times do we need to recover the information of H?

If H is a normal subgroup. This is similar to Abelian case. Since $gHg^{-1} = H$

$$\sigma(H) = \frac{1}{|G|} \sum \sigma(ghg^{-1}) \tag{34}$$

It commutes with $\sigma(g)$ for all $g \in G$. By Schur's Lemma, σ is proportional to identity. Hence $\hat{\rho}_H$'s blocks are all a multiple of identity. We can measure the state in the computational basis.

$$\Pr(\sigma) = d_\sigma^2 |H|/|G|(H \leq \ker\sigma). \tag{35}$$

It is similar to the Abelian case, which can be done in polynomial time. Measuring a diagonal density matrix under computational basis will reveal all information. But for non-normal cases, we can not get all information just by measuring the name register of representations.

What does this mean? Certainly, we can get the result of σ, but the probability can not be polynomially small. In normal case, its like abelian case, the probability is proportional to the ratio of the size of H and G, which might not hold for the nonabelian cases.

To get more information of the state, we need to measure more elements. Strong Fourier sampling not only measures the name of the representations, but also measure the row and column element of the matrix.