Lecture 21: November 19

Scribe: Ruohan Shen *Monogamy of Entanglement and de Finetti Theorem*

This lecture explores the concept of quantum entanglement monogamy, emphasizing that, unlike classical correlations, quantum correlations cannot be freely shared among multiple parties. After presenting some intuitive arguments, the de Finetti theorem is introduced to provide a more rigorous foundation for this principle.

21.1 Monogamy of entanglement

If two regions are maximally entangled, their density matrix is represented Φ. Now consider the following question: Does there exist a density matrix ρ_{ABC}, such that the two reduced density matrices $\rho_{AB} = \rho_{AC} = \Phi$ are both maximally entangled? The answer is no. If $\rho_{AB} = \Phi$, then the subsystems AB are in a pure state. For AB to be entangled with C, the reduced density matrix of AB must be a mixed state. Hence, ρ_{ABC} must take the form $\Phi_{AB} \otimes \rho_C$. Consequently, ρ_{AC} cannot be entangled. This demonstrates the fundamental principle that *quantum correlations arising from entanglement cannot be shared simultaneously among multiple parties.*

Then we consider a similar question: can we find a ρ_{ABC} such that $\rho_{AB} = \rho_{AC} = \omega$, where $\omega = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ represents a classical mixture? This time, the answer is YES. The GHZ state $\frac{1}{2}(|000\rangle + |111\rangle)$ satisfies the condition. This demonstrates that *classical correlations, unlike quantum entanglement, can be freely shared among multiple parties.*

Next, we apply this principle to justify a widely used tool in many-body physics: mean-field theory. Consider a local Hamiltonian of the form:

$$H = \sum_{i<j} h_{ij} \tag{21.1}$$

which is a sum of two-body operators, and the Hamiltonian is invariant under permutations of the sites. By "local," we mean that each term in the Hamiltonian acts on a limited number of sites; however, this does not imply geometric locality. Thus, the Hamiltonian H is, in general, fully connected, meaning that interactions can span the entire system. We denote the ground state of this Hamiltonian as $|\varphi_{gs}\rangle$, which corresponds to the eigenstate with the lowest eigenvalue. Without loss of generality, we assume that the ground state's density matrix commutes with any permutation operator:

$$[P_\pi, \varphi_{gs}] = 0, \quad \forall \pi \in S_n \tag{21.2}$$

This assumption implies that the ground state is unique and possesses full permutation symmetry. Equivalently, we assume that there is no additional symmetry or degeneracy in the system that could lead to multiple ground states.

Mean-field theory posits that the reduced density matrix of the ground state on s sites can be approximated as:

$$\varphi_{gs}^s \approx \rho^{\otimes s} \tag{21.3}$$

for some single-site density matrix ρ, provided $|s| \ll n$. This approximation is justified by the principle of entanglement monogamy. Regardless of how connected the Hamiltonian is, the entanglement within any small subsystem is distributed across its interaction with the rest of the system.

For small regions of the state, the total amount of entanglement is bounded by the size of the subsystem itself. Consequently, the entanglement within such a region is effectively "diluted" over its interactions with other parts of the system, resulting in the appearance of weak correlations. As a result, the sites in the subsystem behave approximately as though they are decoupled, leading to the product state approximation $\rho^{\otimes s}$.

Remark 21.1.1. *Consider a symmetry of the Hamiltonian:*

$$UHU^\dagger = H \tag{21.4}$$

If it has a unique ground state $H|\varphi_{gs}\rangle = E_0|\varphi_{gs}\rangle$, then applying U to the ground state reproduce another ground state:

$$HU|\varphi_{gs}\rangle = UH|\varphi_{gs}\rangle = E_0 U|\varphi_{gs}\rangle \tag{21.5}$$

Since we assume that the ground state is unique, we must have $U|\varphi_{gs}\rangle = \lambda|\varphi_{gs}\rangle$. If U represents a permutation operator, it is well-known that its eigenvalues are restricted to ± 1. Therefore, the unique ground state of a permutation-invariant Hamiltonian must be either symmetric or anti-symmetric.

21.2 de Finetti Theorem

In this section, we prove the de Finetti theorem, which makes the 'monogamy of entanglement' more precise.

Theorem 21.2.1 (Quantum de Finetti Theorem)**.** *Given a density matrix $\rho_{A_1\dots A_n} \in D_{d^n}$ that is invariant under permutation:*

$$[\rho_{A_1\dots A_n}, P_\pi] = 0, \quad \forall \pi \in S_n \tag{21.6}$$

Then there exists a measure μ in D_{d^n} such that:

$$\left\| \rho_{A_1\dots A_k} - \int d\mu(\sigma)\sigma^{\otimes k} \right\|_1 \leq \frac{dk}{n} \tag{21.7}$$

The theorem can be interpreted as: in a small subregion, the reduced density matrix looks like a classical mixture of classical product states.

There's also a classical version of this theorem.

Theorem 21.2.2 (Classical de Finetti Theorem)**.** *If a n-variable probability distribution satisfies:*

$$p(z_1, \dots, z_n) = p(z_{\pi(1)}, \dots, z_{\pi(n)}), \quad \forall \pi \in S_n \tag{21.8}$$

Then there exists a measure μ in the space of distributions such that:

$$p(z_1, \dots, z_k) = \int d\mu(q) q(z_1) \dots q(z_k) \tag{21.9}$$

Philosophically, the classical version justifies the use of i.i.d. distribution. It says that if the distribution is permutation-invariant, than it must look like something i.i.d.

The proof of the quantum de Finetti theorem proceeds in two steps: first, we establish the pure-state de Finetti theorem; then, we demonstrate how the general quantum de Finetti theorem can be reduced to the pure-state case.

Theorem 21.2.3 (Pure state de Finetti theorem)**.** *For a pure state $|\psi\rangle \in \mathrm{Sym}^{n+k}\mathbb{C}^d$, there exists a measure μ on the space of pure states such that*

$$F\left(\mathrm{Tr}_n \psi, \int d\mu(\phi)\phi^{\otimes k}\right)^2 \geq 1 - \frac{dk}{n} \tag{21.10}$$

Proof. Recall the identity

$$\mathbb{E}_{\phi\sim\mathrm{Haar}}\phi^n = \frac{\Pi_{sym}^{(n)}}{d[n]} \tag{21.11}$$

where $d[n] = \binom{d+n-1}{n}$. This identity can be interpreted as stating that ϕ forms an (over)complete basis in the symmetric subspace (up to a normalization factor). This is analogous to the coherent states, where $\int \frac{d\alpha}{2\pi} |\alpha\rangle\langle\alpha| = I$. Using this idea, we can attempt to decompose the reduced density matrix $\mathrm{Tr}_n \psi$ using ϕ as a basis. Define the POVM $M_\phi = \phi^n d[n]$ that satisfies $\int d\phi M_\phi = I$. Then, we can express

$$\mathrm{Tr}_n \psi = \int d\phi \ \mathrm{Tr}_n \left[(M_\phi \otimes I)\,\psi\right] \tag{21.12}$$

$$= \int d\phi\, p(\phi)\psi_\phi \tag{21.13}$$

where ψ_ϕ is the normalized density matrix after measuring ϕ. We expect $\psi_\phi \approx \phi^{\otimes k}$, and this decomposition naturally provides a representation of $\mathrm{Tr}_n \psi$ as a "classical mixture of product states." To make this intuition rigorous, we calculate the fidelity, allowing us to precisely quantify how well ψ_ϕ approximates $\phi^{\otimes k}$.

$$F\left(\mathrm{Tr}_n \psi, \int d\phi\, p(\phi)\phi^{\otimes k}\right)^2 = F\left(\int d\phi\, p(\phi)\psi_\phi, \int d\phi\, p(\phi)\phi^{\otimes k}\right)^2 \tag{21.14}$$

$$\geq \int d\phi\, p(\phi) F\left(\psi_\phi, \phi^{\otimes k}\right)^2 \tag{21.15}$$

$$= \int d\phi \ \mathrm{Tr}_k\left(\left[\mathrm{Tr}_n\left(d[n]\phi^{\otimes n}\otimes I_k\right)\psi\right]\phi^{\otimes k}\right) \tag{21.16}$$

$$= \int d\phi \ \mathrm{Tr}\left[\phi^{\otimes n+k}\psi\right] d[n] \tag{21.17}$$

$$= \frac{\mathrm{Tr}\left[\Pi_{sym}^{(n+k)}\psi\right]}{d[n+k]} d[n] \tag{21.18}$$

$$= \frac{d[n]}{d[n+k]} \geq 1 - \frac{dk}{n} \tag{21.19}$$

This concludes the proof. □

Then we start to prove the quantum de Finetti theorem:

Proof. For any symmetric density matrix $\rho_{A_1\ldots A_n}$ that satisfies (21.6), we can find a symmetric purification:

$$|\psi\rangle_{A_1B_1\ldots A_nB_n} \in \mathrm{Sym}^n(A\otimes B) \tag{21.20}$$

Here, the symmetric subspace is defined for the representation $\pi \to P_{\pi_A}\otimes P_{\pi_B}$, and each local site now has dimension $d^2 = d_{A_i}d_{B_i}$ correspondingly. Clearly, the canonical purification

$\left(\sqrt{\rho}_A \otimes I_B\right) \sqrt{d^n} \left|\Phi\right\rangle_{AB}$ satisfies this condition. Then, we apply the pure state de Finetti theorem to the state $\left|\psi\right\rangle_{AB}$ and get

$$F\left(\mathrm{Tr}_{n-k}\,\psi_{AB}, \int d\mu(\phi)\,\phi^{\otimes k}\right)^2 \geq 1 - \frac{d^2 k}{n-k} \tag{21.21}$$

By tracing out system B, we get

$$F\left(\mathrm{Tr}_{n-k}\,\psi_A, \int d\mu(\phi)\ \left(\mathrm{Tr}_{B_i}\,\phi\right)^{\otimes k}\right)^2 \geq F\left(\mathrm{Tr}_{n-k}\,\psi_{AB}, \int d\mu(\phi)\,\phi^{\otimes k}\right)^2 \tag{21.22}$$

And because $T \leq \sqrt{1-F^2}$, we put everything together, we get

$$\left\|\rho_{A_1\ldots A_k} - \int d\mu(\phi)\,\phi_A^{\otimes k}\right\|_1 \leq \left\|\rho_{A_1 B_1 \ldots A_k B_k} - \int d\mu(\phi)\,\phi^{\otimes k}\right\|_1 \tag{21.23}$$

$$\leq 2\sqrt{1 - F\left(\rho_{A_1 B_1 \ldots A_k B_k}, \int d\mu(\phi)\,\phi^{\otimes k}\right)^2} \tag{21.24}$$

$$\leq 2\sqrt{\frac{d^2 k}{n-k}} \tag{21.25}$$

□

Note that this bound is weaker than Theorem 21.2.1. However, it represents the best achievable result using this method. Establishing Theorem 21.2.1 needs a more sophisticated and intricate approach. Interested readers are encouraged to consult Corollary 1 of arXiv:1010.1875 or Watrous's notes for further details.

21.3 Application

21.3.1 QKD

Conventional QKD protocols typically prove security under the assumption of independent and identically distributed (i.i.d.) noise, leaving their security unproven for correlated noise. However, since these protocols treat bits symmetrically, the de Finetti theorem can be employed to reduce Eve's general attack to a mixture of i.i.d. attacks, thereby providing a way to bound the error rate even in the presence of correlations.

To elaborate, we present the de Finetti reduction. Assume the density matrix $[\rho_{A_1\ldots A_n}, P_\pi] = 0$ is symmetric under any permutation $\pi \in S_n$. Then there exists a measure μ such that

$$\rho_{A_1\ldots A_n} \leq n^{O(d^2)} \int d\mu(\sigma)\,\sigma^{\otimes n} \tag{21.26}$$

The proof is straightforward. Consider a purification $\left|\psi\right\rangle \in \mathrm{Sym}^n(A \otimes B)$. We observe that:

$$\psi \leq \Pi_{sym}^{d^2,n} = d^2[n] \int d\phi\,\phi^{\otimes n} \tag{21.27}$$

Since $d^2[n] \leq n^{O(d^2)}$, we conclude the proof. This has practical significance: if $\mathrm{Tr}\,M\sigma \leq \epsilon$, then $\mathrm{Tr}\,M\rho \leq n^{O(d^2)}\epsilon$.

21.3.2 Optimization

Define the set of separable states as:

$$\text{Sep} = \text{Sep}(d_A, d_B) = \text{conv}\{\alpha \otimes \beta : \alpha \in D_{d_A}, \beta \in D_{d_B}\} \tag{21.28}$$

For simplicity, we will take $d_A = d_B$ in the following.

We further define the support function as follows:

$$h_{\text{Sep}}(M) = \max_{\sigma \in \text{Sep}} \text{Tr}\left[M\sigma\right] \tag{21.29}$$

which can be interpreted as the maximum overlap of the observable M with any separable state σ . Equivalently, this represents the highest probability of obtaining an outcome consistent with separable states when performing a measurement described by M .

The problem can be made easier if we restrict the search space to only the symmetric separable states:

$$h_{\text{SepSym}}(M) = \max_{\alpha} \text{Tr}\left[M\left(\alpha \otimes \alpha\right)\right] \tag{21.30}$$

Next, we introduce the concept of k -extendable states. A bipartite density matrix ρ_{AB} is called k -extendable if there exists a symmetric extension $\rho_{AB_1 \ldots B_k}$such that:

$$\tilde{\rho}_{AB_i} = \rho_{AB} \tag{21.31}$$

The set of k-extendable states is nearly equivalent to the set of separable states, and when k is larger, the difference is smaller. k-extenable states are much easier to calculate.