8.S372/18.S996 Quantum Information Science III **Fall 2020**

Lecture 23: Sep 22, 2020

Lecturer: Aram Harrow *Scribe: Matthew Kearney, Andrew Tan*

23.1 de Finetti Thm for Pure Symmetric States

Let $|\psi\rangle$ be a state in the symmetric subspace of $n+k$ systems in d dimensions.

$$|\psi\rangle \in \mathrm{Sym}^{n+k}\mathbb{C}^d$$

We will show that

$$F(\mathrm{tr}_n(\psi), \int d\mu(\phi)\phi^{\otimes k})^{2k} \geq 1 - \frac{kd}{n}$$

23.1.1 Tomography

We will first take a detour and talk briefly about tomography, which describes which measurements to make to estimate a state. Specifically we can ask the question, given $|\phi\rangle^{\otimes n}$ how well can we estimate $|\phi\rangle$? We will measure with a continuously indexed set of POVM: $\{M_{\hat{\phi}}\}_{\hat{\phi}}$ such that the following holds:

$$\int d\hat{\phi} M_{\hat{\phi}} = \Pi_{\mathrm{sym}}$$

Unlike the usual case where we need the measurements to sum to the identity, since $|\phi\rangle^{\otimes n}$ lies in the symmetric subspace, we only need the measurement operators to sum to the projector onto this subspace. It turns out that the optimal set of measurements is given by

$$M_{\hat{\phi}} = c\hat{\phi}^{\otimes n}$$

Where we can calculate the constant c by calculating

$$\int d\hat{\phi}\hat{\phi}^{\otimes n} = \frac{\Pi_{\mathrm{sym}}}{\mathrm{tr}(\Pi_{\mathrm{sym}})} = \frac{\Pi_{\mathrm{sym}}}{\binom{d+n-1}{n}}$$

This gives us

$$c = \binom{d+n-1}{n}$$

We can now return to the proof of the de Finetti Theorem. Recall that the squared fidelity for pure states is given by

$$F(\phi, \hat{\phi}) = \mathrm{tr}\phi\hat{\phi}$$

Therefore we can calculate the expectation of the squared fidelity as

$$\begin{aligned}
\mathbb{E}F(\phi, \hat{\phi})^2 &= \int d\hat{\phi}\, \mathrm{tr}(\phi\hat{\phi})\, \mathrm{tr}(M_{\hat{\phi}} \phi^{\otimes n}) \\
&= \int d\hat{\phi}\, \mathrm{tr}(\phi\hat{\phi}) \binom{d+n-1}{n} \mathrm{tr}(\phi\hat{\phi})^n \\
&= \binom{d+n-1}{n} \int d\hat{\phi}\, \mathrm{tr}(\phi\hat{\phi})^{n+1} \\
&= \binom{d+n-1}{n} \mathrm{tr}(\phi^{\otimes n+1} \int d\hat{\phi}\, \hat{\phi}^{\otimes n+1}) \\
&= \binom{d+n-1}{n} \mathrm{tr}(\phi^{\otimes n+1} \frac{\Pi_{\text{sym}}}{\binom{d+n}{n+1}}) \\
&= \frac{\binom{d+n-1}{n}}{\binom{d+n}{n+1}} \mathrm{tr}(\phi^{\otimes n+1} \Pi_{\text{sym}}) \\
&= \frac{\binom{d+n-1}{n}}{\binom{d+n}{n+1}} \mathrm{tr}(\phi^{\otimes n+1}) \\
&= \frac{\binom{d+n-1}{n}}{\binom{d+n}{n+1}} \\
&= \frac{n+1}{n+d} \\
&\geq 1 - \frac{d}{n}
\end{aligned}$$

We can also calculate higher moments of the fidelity as well, in which case we find

$$\mathbb{E}F(\phi, \hat{\phi})^{2k} = \frac{\binom{d+n-1}{n}}{\binom{d+n-1+k}{n+k}} = \frac{(n+1)\ldots(n+k)}{(n+d)\ldots(n+d+k-1)} \geq 1 - \frac{dk}{n}$$

23.1.2 de Finetti Theorem Proof

Let $|\psi\rangle$ be given by

$$|\psi\rangle = \int a_\phi \, |\phi\rangle^{\otimes n+k} \, d\phi$$

If we then trace over n of the qudits we get

$$\mathrm{tr}_n(\psi) = \int d\phi (M_\phi \otimes I^{\otimes k})\psi = \int d\phi \, p_\phi \psi_\phi$$

We would like to claim that $\psi_\phi \approx \phi^{\otimes k}$.

Calculating the fidelity we get

$$\begin{aligned}
F(\mathrm{tr}_n(\psi), \int d\phi \, p_\phi \phi^{\otimes k})^2 &\geq \int d\phi \, p_\phi F(\psi_\phi, \phi^{\otimes k})^2 \\
&= \int d\phi \, \mathrm{tr}(p_\phi \psi_\phi \phi^{\otimes k}) \\
&= \int d\phi \, \mathrm{tr}((M_\phi \otimes \phi^k)\psi) \\
&= \mathrm{tr}(\int d\phi \binom{d+n-1}{n} \phi^{\otimes n+k} \psi) \\
&= \frac{\binom{d+n-1}{n}}{\binom{d+n-1+k}{n+k}} \\
&= \frac{(n+1)\ldots(n+k)}{(n+d)\ldots(n+d+k-1)} \\
&\geq 1 - \frac{dk}{n}
\end{aligned}$$

As a corollary to this we have that for non pure states: If $\rho \in D_{d^{n+k}}$ and $[\rho, p_d(\pi)] = 0 \forall \pi$ then

$$F(\mathrm{tr}_n(\rho), \int d\mu(\sigma) \, \sigma^{\otimes k})^2 \geq 1 - \frac{d^2 k}{n}$$

23.1.3 Examples of de Finetti Theorem

Below are some examples to illustrate the theorem.

23.1.3.1 Example 1

Let $|\psi\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$. Then we have that for $k \geq 1$

$$\mathrm{tr}_{n-k}\psi = \frac{|0\rangle\langle 0|^{\otimes k} + |1\rangle\langle 1|^{\otimes k}}{2}$$

So we can start with a state that looks nothing like a product state and after just tracing out one system we end with a state that is exactly the state described by the de Finetti theorem.

23.1.3.2 Example 2

Let $\rho = \binom{n}{n/2}^{-1} \sum\limits_{x\in\{0,1\}^n, |x|=n/2} |x\rangle\langle x| := W^n_{n/2}$, which is far from any $\sigma^{\otimes n}$. Then we have that

$$\mathrm{tr}_{n-k}\rho = \sum_{j=0}^{k} \frac{\binom{n/2}{j}\binom{n/2}{k-j}}{\binom{n}{n/2}} W^k_j \approx 2^{-k}\binom{k}{j} W^k_j$$

23.1.3.3 Example 3

This example shows why it is important that n must be bigger than d. We have that $|\phi\rangle = n \sum\limits_{\pi\in S_n} \mathrm{sgn}(\pi)\,|\pi(1),\dots,\pi(n)\rangle \in \mathbb{C}^{\ltimes\otimes n}$.

$$\mathrm{tr}_{n-2}\phi = \binom{n}{2}\Pi_{\mathrm{anti}}$$

This state is very far from separable states even though $k = 2$.

23.2 Applications

23.2.1 Mean-Field Theory

Let the Hamiltonian acting on our set of qudits be given by

$$H = \binom{n}{k} \sum_{i_1<i_2<\cdots<i_k} h_{i_1,\dots,i_k}$$

If we then look at the trace of the Hamiltonian applied to the ground state we get

$$\begin{aligned}\operatorname{tr}(H\psi_{gs}) &= \operatorname{tr}(H\rho)\\ &= \operatorname{tr}(h\otimes I^{\otimes n-k})\rho\\ &\geq \operatorname{tr}(h\int d\mu(\sigma)\sigma^{\otimes k}) - \|h\|_\infty \frac{d^2k}{n-k}\\ &\geq \min_\sigma \operatorname{tr}(h\sigma^{\otimes k}) - \|h\|_\infty \frac{d^2k}{n-k}\end{aligned}$$

At the same time we have that because ψ_{gs} is the ground state we know

$$\operatorname{tr}(H\psi_{gs}) \leq \min_\sigma \operatorname{tr}(h\sigma^{\otimes k}) = \min_\sigma \operatorname{tr}(H\sigma^{\otimes n})$$

23.2.2 Security of QKD

In QKD, Alice sends $H^{a_1}|r_1\rangle \otimes H^{a_2}|r_2\rangle \otimes \cdots \otimes H^{a_n}|r_n\rangle$ for $a, r \in \{0,1\}^n$ uniformly random binary strings. Bob then applies $H^{b_1} \otimes H^{b_2} \otimes \cdots \otimes H^{b_n}$ for $b \in \{0,1\}^n$ also a random binary string. Against i.i.d. attacks (attacks where Eve does the same thing to every qubit), this protocol can tolerate a bit error rate $< p_c \approx 0.14$.

What to do about general attacks though? Alice and Bob can use a symmetric protocol therefore discarding $n-k$ quibits and leaving the remaining qubits in a state approximately equal to $\int d\mu(\sigma)\,\sigma^{\otimes k}$ with error k/n. In other words we can sacrifice $O(1/\epsilon^2)$ qubits to learn σ to error ϵ. Normally in cryptography we expect that security should be exponentially good in the amount of effort made, but here we can only keep $O(\sqrt{n})$ qubits and the error decreases as O(1/n).

23.2.3 Exponential de Finetti Theorem

Sometimes other theorems help us to get better bounds. The exponential de Finetti theorem states that if $\rho_{n+k} \in D_{d^{n+k}}$ symmetric, then

$$\rho_k = \operatorname{tr}_n(\rho_{n+k}) \approx \int d\mu(\sigma)\,\sigma^{k-r} \otimes \phi_r$$

Where ϕ_r is just an arbitrary density matrix on r systems. In this case we find that the error is approximately less than or equal to $k^{O(d)} \exp \frac{-kr}{n+k}$.

23.2.4 de Finetti Reductions

If $\rho_n \in D_{d^n} \in \mathrm{Sym}$

$$\rho_k \leq (n+1)^{d^2} \int\limits_{\sigma \in D_d} \sigma^{\otimes n} \, d\sigma$$

Then we get that for some bad event B,

$$\mathbb{P}(B) = \mathrm{tr}(M\rho_n) \leq (n+1)^{O(d^2)} \int d\sigma \, \mathrm{tr}(M\sigma^{\otimes n})$$

If our probability is exponentially small, paying a polynomial pre-factor won't matter, so this can be useful for upper bounds.

23.2.5 Applications to Classical Optimization Algorithms

The goal of the optimization algorithms is to find

$$h_s(y) = \max_{x \in S} \langle x, y \rangle$$

For density matrices D_d and measurement M we have

$$h_{D_d}(M) = \|M\|_\infty$$

Solving the following is much harder however

$$h_{\mathrm{sep}}(M) = \max_{\alpha, \beta \in D_d} \mathrm{tr}(M(\alpha \otimes \beta))$$

It is NP hard to get error O(1/d). Define the following set

$$\mathrm{SepSym}(d,k) = \mathrm{conv}\{\sigma^{\otimes k} : \sigma \in D_d\}$$

We have that

$$\mathrm{SepSym}(d,k) \subseteq \mathrm{SymExt}(d,k,n) = \{\rho_k \in D_{d^k} : \exists \rho_n \in D_{d^n}, \text{ symmetric}\}$$

We have that

$$h_{\text{SepSym}}(M) \leq h_{\text{SymExt}} \leq h_{\text{SepSym}}(M) + O(\frac{d^2k}{n})$$

23.2.6 Monogamy Using Information Theory

Let system A be entangled with systems $B_1, \ldots, B_n$ such that B_i is conditionally independent of B_j given A for $i \neq j$. There is a trade off between entanglement of $\rho_{AB_1}, \cdots, \rho_{AB_n}$ without requiring symmetry assumptions and $n \approx \log d$ instead of poly(d).

We have that

$$\begin{aligned} 2\log d_A &\geq I(A:B_1,\ldots,B_n) \\ &= I(A:B_1) + I(A:B_2|B_1) + \cdots + I(A:B_n|B_1\ldots B_{n-1} \end{aligned}$$

$$\mathbb{E}_{j\in[n]} I(A:B_j|B_1^{j-1}) = 2\log(d_A)/n \leq \epsilon^2 \quad \text{if } n \geq \frac{2\log(d_A)}{\epsilon^2}$$

Why is this helpful? squashed entanglement:

$$E_{sq}(\rho^{AB}) - \inf\{\frac{1}{2}I(A:B|E) : \rho^{ABE} \text{ an extension of } \rho^{AB}\}$$

Then we have that $\mathbb{E}_i E_{sq}(\rho^{AB_i}) \leq \frac{\log(d_A)}{n}$.

ρ_{AB} is n-extendable if $\exists \tilde{\rho}^{AB_1\ldots B_n}$ s.t. $\rho^{AB} = \tilde{\rho}^{AB_i} \forall i$. Then we have $E_{sq}(\rho) \leq \log(d_A)/n$.

We have that

$$E_D \leq E_{sq} \leq E_F$$

But if $E_{sq}(\rho) \leq \epsilon^2$, is ρ close to Sep? On PSET 9 we will show that if ρ is $\frac{\log(d_A)}{\epsilon^2}$-extendable then we have that

$$\max_{M\in\text{1-LOCC}} \min_{\sigma\in\text{Sep}} |\text{tr}(M(\rho-\sigma))| \leq \epsilon$$

This gives us non-trivial approximation bounds for runtime $d^{O(\log d)}$.