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

Lecture 17: October 29, 2020

Lecturer: Aram Harrow *Scribe: Annie Wei*

17.1 Entanglement of random states

Recall that last time we studied entanglement in random states. We showed that for $|\psi\rangle \in \mathbb{C}^{d_a} \otimes \mathbb{C}^{d_b}$,

$$\mathbb{E}S(A)_\psi \geq \mathbb{E}S_2(\psi_A) \tag{17.1}$$

$$\geq -\log \mathbb{E}\,\mathrm{tr}\psi_A^2 \tag{17.2}$$

where

$$\mathbb{E}\,\mathrm{tr}\psi_A^2 = \frac{d_A + d_B}{d_A d_B + 1} \tag{17.3}$$

For $d = d_A = d_B$, we get

$$\mathbb{E}S(A)_\psi \geq \log \frac{d^2+1}{2d} \geq \log(d) - 1 \tag{17.4}$$

For $d_A << d_B$, we get

$$\mathbb{E}S(A)_\psi \geq \log(d_A) - \log(1 + \frac{d_A}{d_B}) \approx \log d_A \tag{17.5}$$

That is, a random n-qubit state has k-qubit marginals that look like $I/2^k$ if $k < n/2$.

How accurate is this bound? Suppose that

$$|\psi\rangle = \sum_{ij} G_{ij} |i\rangle \otimes |j\rangle \tag{17.6}$$

with

$$\mathbb{E}|G_{ij}|^2 = \frac{1}{d_A d_B} \tag{17.7}$$

Then this has marginals $\psi_A = GG^\dagger$, corresponding to the complex Wishart distribution.

The histogram of eigenvalues λ of ψ_A follows the Marchenko-Pastor laws and satisfies

$$\lambda_{min} \approx \frac{1}{d_A}\left(1 - \sqrt{\frac{d_A}{d_B}}\right)^2 \tag{17.8}$$

$$\lambda_{max} \approx \frac{1}{d_A}\left(1 + \sqrt{\frac{d_A}{d_B}}\right)^2 \tag{17.9}$$

$$\mu(\lambda) = \frac{\sqrt{(\lambda_{max} - \lambda)(\lambda - \lambda_{min})}}{2\pi(d_A/d_B)\lambda} \tag{17.10}$$

where $\mu(\lambda)$ is the density. A sketch of the proof goes like the following:

$$\mathrm{tr}\psi_A^k = \binom{d_A + k - 1}{k}^{-1} \mathrm{tr}\Pi_{sym}(C_{A_1,\ldots,A_k} \otimes I_{B_1,\ldots,B_k}) \tag{17.11}$$

$$\approx d_A \int \mu(\lambda)\lambda^k d\lambda \tag{17.12}$$

A special case of this is when $d = d_A = d_B$. Then $\lambda_{min} \sim 1/d^2$, $\lambda_{max} \approx 4/d$, and

$$\mu(\lambda) = \frac{\sqrt{4/d - \lambda}}{2\pi\sqrt{\lambda}} \tag{17.13}$$

$$\mu(\sqrt{\lambda}) = \frac{\sqrt{4/d - \lambda}}{\pi} \tag{17.14}$$

This is known as the quarter-circle law (note that there's a Wigner semicircle law for eigenvalues of $G + G^\dagger$, and a circle law for eigenvalues of G).

17.2 Note on Renyi entropies

Suppose we have a state

$$\rho = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| \otimes (I/2)^{\otimes a} \otimes \left|0\right\rangle\left\langle 0\right|^{\otimes(b-a)} + \frac{1}{2}\left|1\right\rangle\left\langle 1\right| \otimes (I/2)^{\otimes b} \tag{17.1}$$

for $a < b$. Then

$$S_0(\rho) = \log(2^a + 2^b) \approx b + 2^{a-b} \tag{17.2}$$

$$S_\infty(\rho) = a + 1 \tag{17.3}$$

$$S(\rho) = 1 + \frac{a+b}{2} \tag{17.4}$$

$$S_\alpha(\rho) = \frac{1}{1-\alpha}\log(2^a(2^{a+1})^{-\alpha} + 2^b(2^{b+1})^{-\alpha}) \tag{17.5}$$

$$= \frac{1}{1-\alpha}[\log((2^{1-\alpha})^a + (2^{1-\alpha})^b) - \alpha] \tag{17.6}$$

For $\alpha > 1$ the first term dominates, while for $\alpha < 1$ the second term dominates. This is why we like taking $\alpha = 1$, where the contributions are the same

17.3 k-designs

Say that μ is a distribution on S_d, the states in $\mathbb{C}^d$. Then μ is a k-design if

$$\mathbb{E}_{|\psi\rangle\sim\mu}\psi^{\otimes k} = \mathbb{E}_{\psi\sim\text{Uniform}}\psi^{\otimes k} = \Pi_{sym}\binom{d+k-1}{k}^{-1} \tag{17.1}$$

Note that we can also define approximate k-designs. 1-designs are pretty easy to come up with, i.e. $\{|000\rangle, ..., |111\rangle\}$ is a 1-design. Stabilizer states are 2-designs (and also 3-designs). (Recall that stabilizer states are those that can be written as $C|0^n\rangle$ for C a Clifford state. Alternatively, we can define them as the simultaneous +1 eigenstate of n commuting operators of the form $\sigma_{i_1} \otimes \sigma_{i_2} \otimes .... \otimes \sigma i_n$.)

17.3.1 Application: ϵ-randomizing maps

We say that $N : D_d \to D_d$ is ϵ-randomizing if $\forall\ \rho$,

$$||N(\rho) - I/d||_\infty \leq \epsilon/d \tag{17.2}$$

We will consider maps of the form

$$N(\rho) = \frac{1}{n}\sum_{i=1}^{n} U_i \rho U_i^\dagger \tag{17.3}$$

How large does n need to be? (Recall that we can do remote state preparation with cost $\log n$.) Note that

$$\text{rank}\, N(|1\rangle\langle 1|) \leq n \tag{17.4}$$

$$\tag{17.5}$$

For a choice of $\epsilon < 1$,

$$||N(|1\rangle\langle 1|) - I/d||_\infty \leq 1/d \tag{17.6}$$

$$\Rightarrow \text{rank}\, N(|1\rangle\langle 1|) = d \tag{17.7}$$

Thus $n \geq d$.

Note that the generalized Paulis work with $n = d^2$, $\epsilon = 0$. In fact, $\epsilon = 0$ allows for teleportation. To see this, note that $\epsilon = 0 \Rightarrow N(\rho) = I/d \Rightarrow N(X) = \text{tr}(X)I/d$ by linearity. Then

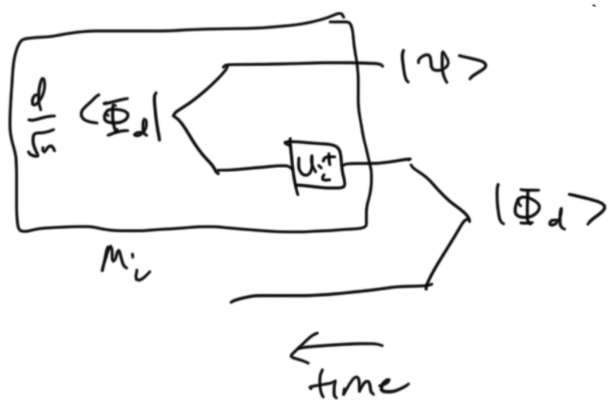
$$(I \otimes N)(\Phi_d) = \frac{1}{d}\sum_{ij} |i\rangle\langle j| \otimes N(|i\rangle\langle j|) \tag{17.8}$$

$$= (I/d) \otimes (I/d) \tag{17.9}$$

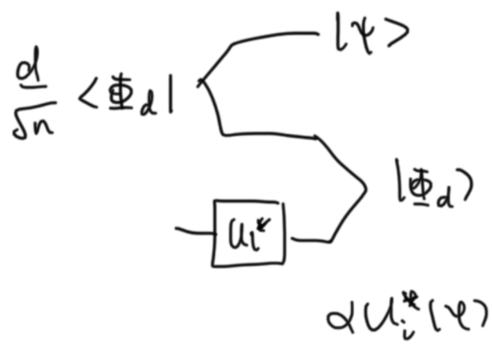
Thus the set of operators

$$M_i = \frac{d^2}{n}(I \otimes U_i)\Phi_d(I \otimes U_i^\dagger) \tag{17.10}$$

is PSD and satisfies $\sum_i M_i = I$, so it forms a POVM. We can draw the following diagram for a teleportation protocol:



Moving the unitary and transposing, this becomes



Note that this also gives us a lower bound $n \geq d^2$ (otherwise we could do teleportation with less than $n < d^2$).

If we let $\epsilon > 0$, it's possible to have $n = O(d/\epsilon^2)$. Let

$$\alpha = \max_\rho ||N(\rho) - I/d||_\infty = \epsilon/d \tag{17.11}$$

$$= \max_{\rho,\sigma} |\mathrm{tr}(N(\rho) - I/d)\sigma| \tag{17.12}$$

$$= \max_{|\rho\rangle,|\varphi\rangle} |\mathrm{tr} N(\psi)\varphi - 1/d| \tag{17.13}$$

$$= \max_{|\rho\rangle,|\varphi\rangle} \left| \frac{1}{n}\sum_{i=1}^n \mathrm{tr}[U_i \psi U_i^\dagger \varphi] - 1/d \right| \tag{17.14}$$

We will later use the fact that

$$\left|\frac{1}{n}\sum_{i=1}^{n}\mathrm{tr}[U_iAU_i^\dagger B]-1/d\right|\leq ||A||_1||B||_1\left(\frac{1}{d}+\alpha\right) \tag{17.15}$$

for A, B Hermitian. Now fix ψ, φ, i, and let

$$\mathrm{tr}U_i\psi U_i^\dagger\varphi = |\gamma_1|^2 \tag{17.16}$$

where $U_i\left|\psi\right\rangle = \left|\gamma\right\rangle$, $\left|\varphi\right\rangle = \left|1\right\rangle$. Also let $\left|g\right\rangle = r\left|\gamma\right\rangle$ so that

$$\mathbb{E}\exp(\lambda|\gamma_1|^2) \leq \mathbb{E}e^{\lambda r^2}\mathbb{E}\exp(\lambda|\gamma_1|^2) \tag{17.17}$$

$$= \mathbb{E}e^{-\lambda|g_1|^2} \tag{17.18}$$

$$= \frac{1}{1-\lambda/d} \tag{17.19}$$

$$\mathbb{E}\exp(\lambda\frac{1}{n}\sum_i\mathrm{tr}[U_i\psi U_i^\dagger\varphi]) \leq \left(1-\frac{\lambda}{nd}\right)^{-n} \tag{17.20}$$

after some algebra (see quant-ph/0307100 for more details).

Now, for fixed ψ, φ, we have that

$$\Pr\left[\left|\frac{1}{n}\sum_i\mathrm{tr}[U_i\psi U_i^\dagger\varphi]-\frac{1}{d}\right|\geq\epsilon/d\right]\leq\exp(-cn\epsilon^2) \tag{17.21}$$

We want to be able to make a statement about

$$\Pr\left[\exists\psi,\varphi\left|\frac{1}{n}\sum_i\mathrm{tr}[U_i\psi U_i^\dagger\varphi]-\frac{1}{d}\right|\geq\epsilon/d\right] \tag{17.22}$$

Normally we would use a union bound, but in this case we need to use a δ-net. Specifically, we say that M is a δ-net if $\forall\left|x\right\rangle\in S_d$, $\exists\left|\beta\right\rangle\in M$ such that $||\left|\alpha\right\rangle-\left|\beta\right\rangle||_2\leq\delta$.

We claim that there exists a M of size $|M|\leq(1+(2/\delta))^{2d}$. To prove this, we add $\left|\beta_1\right\rangle, \left|\beta_2\right\rangle, ...$ to M until $||\left|\beta_i\right\rangle-\left|\beta_j\right\rangle||_2>\delta$ no longer holds. Note that the $B(\left|\beta_i\right\rangle,\delta/2)$ are all disjoint and are contained in $B(0,1+\delta/2)$. Letting $\mathrm{Vol}(B(0,r))=C_dr^{2d}$, $|M|C_d(\delta/2)^{2d}\leq C_d(1+\delta/2)^{2d}\Rightarrow|M|\leq(1+2/\delta)^{2d}$.

Now converting this to the trace norm,

$$||\left|\psi\right\rangle-\left|\varphi\right\rangle||_{\ell_2}\geq\frac{1}{2}||\psi-\varphi||_{S_1} \tag{17.23}$$

Thus M is a δ-net with $|M|\leq(3/\delta)^{2d}$.

Now let

$$\beta = \max_{|\psi_0\rangle, |\varphi_0\rangle \in M} \left| \frac{1}{n} \sum_{i=1}^{n} \mathrm{tr} U_i \psi_0 U_i^\dagger \varphi_0 - \frac{1}{d} \right| \tag{17.24}$$

Note that

$$\Pr[\beta \geq \epsilon/d] \leq (3/\delta)^{4d} e^{-cn\epsilon^2} < 1 \tag{17.25}$$

if we choose $\delta = O(1)$, $n = O(d/\epsilon^2)$. Now we just need to extend to points not in the net. Letting

$$||\psi - \psi_0||_1 \leq 2\delta \tag{17.26}$$

$$||\varphi - \varphi_0||_1 \leq 2\delta \tag{17.27}$$

for some ψ, φ,

$$\alpha = \left| \frac{1}{n} \sum_{i=1}^{n} \mathrm{tr} U_i \psi U_i^\dagger \varphi - \frac{1}{d} \right| \tag{17.28}$$

$$\leq \left| \frac{1}{n} \sum_{i=1}^{n} \mathrm{tr} U_i \psi_0 U_i^\dagger \varphi_0 - \frac{1}{d} \right| + \left| \frac{1}{n} \sum_{i=1}^{n} \mathrm{tr} U_i (\psi - \psi_0) U_i^\dagger \varphi_0 \right| + \left| \frac{1}{n} \sum_{i=1}^{n} \mathrm{tr} U_i \psi_0 U_i^\dagger (\varphi - \varphi_0) \right| \tag{17.29}$$

$$\leq \beta + 2 \cdot 2\delta \left(\frac{1}{d} + \alpha \right) \tag{17.30}$$

$$\Rightarrow \alpha \leq \frac{1}{1 - 4\delta} (\beta + \frac{4\delta}{d}) = O(\epsilon/\delta) \tag{17.31}$$

Note that $(I \otimes N)\Phi_d$ has rank d/ϵ^2 but is LOCC-indistinguishable from $I/d \otimes I/d$ with rank d^2. Thus it accomplishes data hiding.