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

Lecture 21: November 12, 2020

Lecturer: Aram Harrow *Scribe: Shankar Balasubramanian*

21.1 Random states as quantum error correcting codes

Random states and QECC states are generically high entangled across cuts, and so one would expect random unitaries/states to serve as potentially good QECCs. Define the stabilizers $S = \langle S_1, S_2, \ldots, S_{n-k} \rangle$ and further define W_ℓ to be a string of Pauli matrices of total weight $\leq \ell$.

If $N(S) \cap W_\ell = \{I\}$ and $|\psi\rangle \in C$ where C is the codespace, then ψ_A is approximately maximally mixed for $|A| \leq \ell$. To this end, suppose $s_1, s_2, \ldots, s_n$ are random commuting Paulis. Then,

$$|W_\ell| \sim \sum_{k=1}^{\ell} \binom{n}{k} 3^k \approx \exp\left[n \left(H_2\left(\frac{\ell}{n}\right) + \frac{\ell}{n} \log 3 \right) \right].$$

We have that $S = N(S)$, so

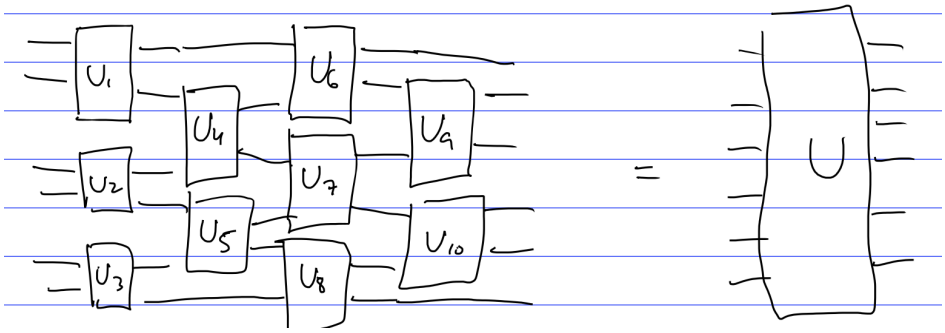
$$\mathbb{E}\,|S \cap W_\ell| = |W_\ell| 2^{-n} \ll 1$$

for $\ell/n < c$. This is known as a Gilbert-Varshamov bound. See quant-ph/0303022 for more details.

21.2 k-designs from random circuits

Let us consider the circuit construction shown below, where all of the unitaries U_1 through U_{10} are chosen from a Haar random distribution over $U(d^2)$ or are a k-design on $U(d^2)$. What kinds of properties can such circuits have?

Let us restrict to the case where $k = 2$ and $d = 2$. We also define $p, q \in \{0, 1, 2, 3\}^2$.



Under the action of the quantum circuit, the local operator $\sigma_p \otimes \sigma_q$ becomes

$$\begin{aligned}\sigma_p \otimes \sigma_q &\to \mathbb{E}_U (U \otimes U)(\sigma_p \otimes \sigma_q)(U \otimes U)^\dagger, \\ &= \begin{cases} 0, & \text{for } p \neq q \\ I, & \text{for } p = q = 00 \\ \frac{1}{15} \sum_{r \neq 00} \sigma_r \otimes \sigma_r, & \text{for } p = q \neq 00 \end{cases}\end{aligned}$$

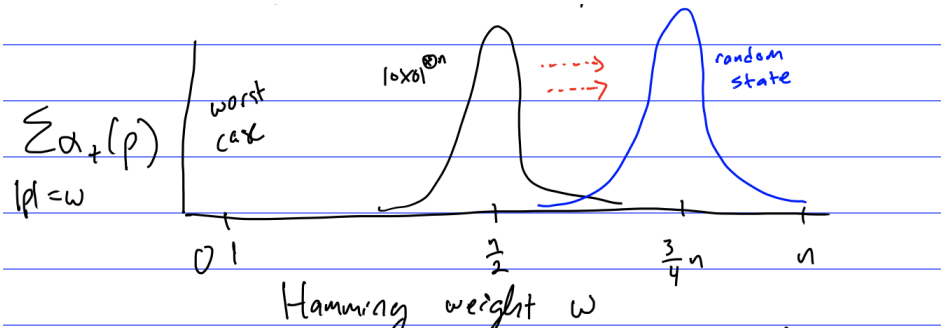
where we have used the fact that $M \to \mathbb{E}(U \otimes U) M (U \otimes U)^\dagger$ is a linear map. Let us start with an initial density matrix $\rho(0) = |0\rangle\langle 0|^{\otimes n}$; then the action of the circuit on this density matrix can be expressed by the relation $\rho(t) = U_t \rho(t-1) U_t^\dagger$ where U_t are random 2-qubit gates on qubits i and j. Because U_t are 2-designs, we want to compute the quantity

$$\mathbb{E}[\rho(t) \otimes \rho(t)] = 2^{-n} \sum_p \alpha_t(p) \sigma_p \otimes \sigma_p + \sum_{p \neq q} \beta_t(p,q) \sigma_p \otimes \sigma_q. \tag{21.1}$$

For the second term, we know that the expectation value will render it zero (or vanishingly small) once all of the qubits have been touched a sufficient number of times. Therefore, this quantity can be modelled by the dynamics of $\alpha_t(p)$ by the relation $\alpha_t = M \alpha_{t-1}$ for M a stochastic matrix. In particular, the stochastic update rule is to map $00 \to 00$ and $r \neq 00 \to r' \sim U[\{01, \ldots, 33\}]$ where $U[S]$ indicates a uniform distribution over elements in set S. Since M has largest eigenvalue equal to 1, we can compute the steady state vector:

$$\alpha_t = \lim_{t \to \infty} M^t \alpha_0 = \begin{bmatrix} 2^{-n} \\ 4^{-n}/(1+2^n) \\ \vdots \\ 4^{-n}/(1+2^n) \end{bmatrix}.$$

Now we ask what the mixing time of this Markov chain is. The worst starting point is the string $1000\ldots0$, because the only transition can occur when qubits 0 and 1 are touched, which only locally updates the string. Therefore, it takes a long time to reach



all bits. In general, the convergence time depends on the geometry. For 1D circuits, $O(n^2)$ gates are required. For a fully connected architecture, the convergence time is $n + n/2 + n/3 + \ldots \sim n \log n$ gates are required.

Consider the state $|0\rangle\langle 0|^{\otimes n} = \left(\frac{I+\sigma_3}{2}\right)^{\otimes n}$. This can be thought of as a mixture of $\{00\ldots00, 00\ldots03, 00\ldots30, \cdots, 33\ldots33\}$. The time requires for the circuit to be maximally entangled from this starting state is $\Omega(n^2)$ for 1D circuits and $\Omega(n \log n)$ for fully connected circuits. Thus, even for this simplified case, we get the same bounds. We can plot the distribution of outcomes, shown above.

Let us explore the structure of the Markov chain more. Denote $* = \{1, 2, 3\}$ which collapses the state space to 00, 0∗, ∗0, and ∗∗. The transition probabilities (written above the arrows) are

$$p_i p_j(t) = \{00\} \xrightarrow{1} p_i p_j(t+1) = \{00\}$$
$$p_i p_j(t) = \{0*, *0, **\} \xrightarrow{\frac{6}{15}} p_i p_j(t+1) = \{0*, *0\}$$
$$p_i p_j(t) = \{0*, *0, **\} \xrightarrow{\frac{9}{15}} p_i p_j(t+1) = \{**\}$$

Therefore, the Hamming weight w follows a random walk with a drift towards $w = \frac{3}{4}n$. This also goes under the name Ornstein-Uhlenbeck process. It can be shown that

$$\left| w - \frac{3}{4}n \right| \sim e^{-ct/n}$$

for $w > 0.1n$. The random walk is mixed when $\left|w - \frac{3}{4}n\right| \leq \sqrt{n}$ or when $t = O(n \log n)$.

It is important to beware that the convergence time depends on the metric used. For example, define the anticoncentration

$$\Lambda = \sum_{z \in \{0,1\}^n} |\langle z|U|0^n\rangle|^4 = \sum_z p(z)^2.$$

It can be computed that $\Lambda = 1$ for $U = I$ and that $\Lambda = 2^{-n}$ for Haar random U. The

computation goes like

$$\begin{aligned}\mathbb{E}\Lambda &= \mathrm{Tr}\left(\sum_z |z\rangle\langle z| \otimes |z\rangle\langle z|\right) \frac{I+F}{2^n(2^n+1)} \\ &= \frac{2}{2^n+1}.\end{aligned}$$

Anticoncentration is a property that appears in the goal of quantum supremacy. In general, the hardness of simulating quantum circuit families uses anticoncentration to extend worst-case hardness to average-case hardness.

Alternatively, we may also write

$$\sum_z |z\rangle\langle z| \otimes |z\rangle\langle z| = 2^{-n} \sum_{p\in\{0,3\}^n} \sigma_p \otimes \sigma_p$$

and this imples

$$\Lambda = \sum_{p\in\{0,3\}^n} \alpha_t(p).$$

In 1D, Λ converges in $O(n \log n)$ steps, or in $O(\log n)$ depth. The details can be found in (2005.02421)

21.3 Techniques for bounding convergence time

The first method is the spectral method, where one computes the value of the second largest eigenvalue, so that the error as a function of iteration t vanishes as $\sim (\lambda_2(M))^t$. For $k > 2$, M is no longer stochastic. Let us restrict to 1D and compute

$$G^k_{\text{circuit}} = \mathbb{E}_{1\le i\le n-1}\mathbb{E}_{U\sim U(4)} \left(\left(I^{\otimes i-1} \otimes U \otimes I^{\otimes n-i-1}\right) \otimes \left(I^{\otimes i-1} \otimes U^* \otimes I^{\otimes n-i-1}\right)\right)^{\otimes k}.$$

Then, under many iterations

$$(G^k_{\text{circuit}})^t \to G^k_{\text{Haar}} = \text{proj}\{|\psi\rangle : \left(U^{\otimes k} \otimes U^{*\otimes k}\right)|\psi\rangle = |\psi\rangle\}$$

and we find

$$G^k_{\text{ciruit}} = \frac{1}{n-1}\sum_{i=1}^{n-1} P_{i,i+1},$$

which has eigenvalues in the interval $[0, 1]$. We may write G^k_{ciruit} in the block diagonal structure

$$G^k_{\text{ciruit}} = \left[\begin{array}{c|c} G^k_{\text{Haar}} & \\ \hline & A \end{array}\right]$$

with $\| A \|_\infty < 1$. There are several bounds and conjectures for the maximum singular value of A. Currently, in (1208.0692), it is rigorously shown that

$$\| A \|_\infty \leq 1 - \frac{1}{nk^{O(1)}},$$

while (1905.12053) argues that it is possible for the upper bound to be independent of k.

Another method that exists is a method of mapping quantum circuits to statistical mechanical models, some of which possess exact solutions. We first start by computing the expectation value of the quantity

$$\mathbb{E}[(U \otimes U^*)^{\otimes k}],$$

where U is Haar random. It can be verified that

$$\begin{aligned}\mathbb{E}[(U \otimes U^*)^{\otimes k}] &= \text{proj span}\left\{|\Phi_\pi\rangle = (I^{\otimes k} \otimes P_d(\pi))|\Phi\rangle^{\otimes k}\right\} \\ &= \sum_{\sigma,\tau} |\Phi_\sigma\rangle\langle\Phi_\tau| \text{Wg}(\sigma,\tau).\end{aligned}$$

In general, what is proj span $\{|v_1\rangle, |v_2\rangle, \ldots, |v_m\rangle\} = \Pi$? Define

$$K = \sum_{i=1}^{m} |v_i\rangle\langle i|.$$

Then, it follows that

$$\Pi = K(K^\dagger K)^{-1} K^\dagger.$$

This can be seen since $\Pi|v_i\rangle = \Pi K|i\rangle = K|i\rangle = |v_i\rangle$, as desired. In the current case,

$$K = \sum_{\pi} |\Phi_\pi\rangle\langle\pi|,$$

and

$$K^\dagger K = \sum_{\sigma,\tau} \langle\Phi_\sigma|\Phi_\tau\rangle|\tau\rangle\langle\sigma|.$$

Let us carefully compute

$$\begin{aligned}G_{\sigma,\tau} = \langle\Phi_\sigma|\Phi_\tau\rangle &= \langle\Phi|^{\otimes n} I^{\otimes n} \otimes P_d(\sigma^{-1}\tau)|\Phi\rangle^{\otimes n} \\ &= \frac{\text{Tr} P_d(\sigma^{-1}\tau)}{d^n} = d^{\#\text{ cycles}(\sigma^{-1}\tau)-n} = d^{-\text{dist}(\sigma,\tau)}.\end{aligned}$$

We define the Weingarten function $\text{Wg} = G^{-1}$ and it is close to the identity if $d \gg n^2$. Schematically, we may express the relation between the original expectation value and the Weingarten function by the diagram below (see 1905.12053 for more details):

$$\mathbb{E}[(U \otimes U^*)^{\otimes k}] = \sum_{\sigma,\tau}$$