Information Scrambling in Chaotic Systems

Jie Ren

Contents

1 Weingarten Calculus

This section discusses the techniques for averaging random unitary operators appearing in various chaotic models.

$$\left\langle U_{i_1j_1}\cdots U_{i_nj_n}U^*_{i'_1j'_1}\cdots U^*_{i'_nj'_n}\right\rangle_{\text{Haar}} \equiv \int_{U_d} dU\; U_{i_1j_1}\cdots U_{i_nj_n}U^*_{i'_1j'_1}\cdots U^*_{i'_nj'_n} \tag{1}$$

We will review a standard formula for the average of matrix elements of the unitary matrix concerning the Haar probability measure.

The central quantity we need is the **Weingarten functions**, which appear when we are evaluating the following integrals:

$$\left\langle U_{i_1j_1}\cdots U_{i_nj_n}U^*_{i'_1j'_1}\cdots U^*_{i'_nj'_n}\right\rangle_{\text{Haar}} = \sum_{\sigma,\tau\in S_k} \delta_{i_1i'_{\sigma(1)}}\cdots\delta_{i_ni'_{\sigma(n)}}\delta_{j_1j'_{\tau(1)}}\cdots\delta_{j_nj'_{\tau(n)}}\,\mathrm{Wg}_d\left(\sigma\tau^{-1}\right), \tag{2}$$

where $\mathrm{Wg}_d(g)$ is the Weingarten function. In practice, we usually encounter cases where $q \le 2$. For the $(n = 1)$ case, the only Weingarten function is

$$\mathrm{Wg}_d([1]) = \frac{1}{d} \quad\Longrightarrow\quad \langle U_{ij}U^*_{i'j'}\rangle = \frac{1}{d}\delta_{ii'}\delta_{jj'}. \tag{3}$$

For the $(n = 2)$ case, the Weingarten functions are

$$\mathrm{Wg}_d([2]) = \frac{-1}{d\,(d^2-1)}, \quad \mathrm{Wg}_d\left([1,1]\right) = \frac{1}{d^2-1}, \tag{4}$$

which leads to the following Haar measure integral:

$$\left\langle U_{i_1 j_1} U_{i_2 j_2} U^*_{i'_1 j'_1} U^*_{i'_2 j'_2} \right\rangle_{\text{Haar}} = \frac{\delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_1}\delta_{j_2 j'_2} + \delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_2}\delta_{j_2 j'_1}}{d^2-1} - \frac{\delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_1}\delta_{j_2 j'_2} + \delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_2}\delta_{j_2 j'_1}}{d(d^2-1)}. \tag{5}$$

1.1 Explicit form

Formally, $\mathrm{Wg}_d(g)$ has the closed form

$$\mathrm{Wg}_d(g) = \frac{1}{n!}\sum_{\lambda} \frac{\chi_\lambda(e)\chi_\lambda(g)}{\prod_{(i,j)\in Y(\lambda)}(d-i+j)}, \tag{6}$$

where

- the sum is over all partitions $\lambda = [\lambda_1, \cdots, \lambda_l]$ of $n = \sum_i \lambda_i$;
- a partition λ specifies a Young diagram $Y(\lambda)$, and also corresponds to an irreducible representation.
- $\chi_\lambda(g)$ is the irreducible character of the symmetric group S_n indexed by the partition λ;
- $(i,j) \in Y(\lambda)$ stands for $1 \le i \le l$, $1 \le j \le \lambda_i$, i.e., the coordinate of the Young diagram.

Note that $\mathrm{Wg}_d(g)$ is related only to the character, so it is a function of classes.

Let us give a few examples. For $(n=1)$, the partition can only be $\lambda = [1]$, which is a trivial representation:

$$\chi_{[1]}(e) = 1 \quad \Longrightarrow \quad \mathrm{Wg}_d([1]) = \frac{1}{d}. \tag{7}$$

For $(n=2)$, the partition can be $\lambda = [2]$ or $\lambda = [1,1]$, corresponding to the character table:

Representation	e	σ
$[2]$	1	1
$[1,1]$	1	-1

Therefore, the explicit calculation leads to

$$\begin{aligned}
\mathrm{Wg}_d(e) &= \frac{1}{2}\left[\frac{1}{d(d+1)} + \frac{1}{d(d-1)}\right] = \frac{1}{d^2-1},\\
\mathrm{Wg}_d(\sigma) &= \frac{1}{2}\left[\frac{1}{d(d+1)} - \frac{1}{d(d-1)}\right] = \frac{-1}{d(d^2-1)}.
\end{aligned}$$

For $(n=3)$, the character table for S_3 is

Representation	e	$(1,2)$	$(1,2,3)$
$[2]$	1	1	1
$[1^3]$	1	-1	1
$[2,1]$	2	0	0

The direct calculation then gives

$$\begin{aligned}
\mathrm{Wg}_d(e) &= \frac{1}{6}\left[\frac{1}{d(d+1)(d+2)}+\frac{1}{d(d-1)(d-2)}+\frac{4}{d(d+1)(d-1)}\right]=\frac{d^2-2}{d(d^2-1)(d^2-4)},\\
\mathrm{Wg}_d((12)) &= \frac{1}{6}\left[\frac{1}{d(d+1)(d+2)}-\frac{1}{d(d-1)(d-2)}\right]=\frac{-1}{(d^2-1)(d^2-4)},\\
\mathrm{Wg}_d((123)) &= \frac{1}{6}\left[\frac{1}{d(d+1)(d+2)}+\frac{1}{d(d-1)(d-2)}-\frac{2}{d(d+1)(d-1)}\right]=\frac{2}{d(d^2-1)(d^2-4)}.
\end{aligned}$$

One useful property of the Weingarten function is the

$$\mathrm{Wg}_d(g)=d^{-n-|g|}\prod_i(-1)^{|C_i|-1}c_{|C_i|-1}+O(d^{-n-|d|-2}),\tag{8}$$

where g is a product of cycles of length C_i, and $c_n=(2n)!/n!(n+1)!$ is the Catalan number, and $|g|$ is the smallest number of transpositions that g is a product of.

1.2 Orthogonal groups

For integral over $O(d)$,

$$\mathbb{E}\left[O_{i_1j_1}\cdots O_{i_{2n}j_{2n}}\right]=\sum_{\sigma,\tau\in M_{2n}}\delta_{i_{\sigma(1)}i_{\sigma(2)}}\cdots\delta_{i_{\sigma(2n-1)}i_{\sigma(2n)}}\delta_{j_{\tau(1)}j_{\tau(2)}}\cdots\delta_{j_{\tau(2n-1)}j_{\tau(2n)}}\mathrm{Wg}_d^O(\sigma^{-1}\tau),\tag{9}$$

where M_{2n} is S_{2n} mod all the switching of $(2n-1,2n)$ pairs, and Wg_d^O is the Weingarten function for orthogonal groups:

$$\mathrm{Wg}_d^O(g)=\frac{1}{(2n)!}\sum_\lambda\frac{\chi_{2\lambda}(e)\sum_{\xi\in H_n}\chi_\lambda(g\xi)}{\prod_{(i,j)\in Y(2\lambda)}(d+2j-i-1)},\tag{10}$$

where H_n is generated by $\{(2i-2,2i),(2i-1,2j-1)(2i,2j)|i,j\le n\}$.

For $(n=1)$ case, the Weingarten function is

$$\mathrm{Wg}_d^O(e)=\frac{1}{d}\quad\Longrightarrow\quad\mathbb{E}\left[O_{i_1j_1}O_{i_2j_2}\right]=\frac{1}{d}\delta_{i_1i_2}\delta_{j_1j_2}.\tag{11}$$

For $(n=2)$ case, the partition $\lambda=[2]/[1,1]$, and $2\lambda=[4]/[2,2]$.

$$H_n=\{e,(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\}\tag{12}$$

The characters we need are listed below:

Representation	e	$(1,2)$	$(1,2,3)$	$(1,2)(3,4)$	$(1,2,3,4)$
$[4]$	1	1	1	1	1
$[2^2]$	2	0	-1	2	0

Then, for the element e:

$$\mathrm{Wg}_d^O(e)=\frac{1}{24}\left[\frac{8}{d(d+2)}+\frac{16}{d(d-1)}\right]=\frac{d+1}{d(d+2)(d-1)}.\tag{13}$$

Note that Wg_d^O is still a function of classes, and is also equal in the same coset S_{2n}/H_n.

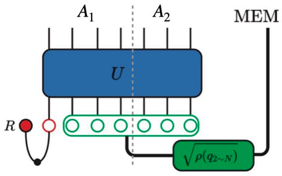
$$\mathrm{Wg}_d^O((23))=\frac{1}{24}\left[\frac{8}{d(d+2)}+\frac{-8}{d(d-1)}\right]=\frac{-1}{d(d+2)(d-1)}.\tag{14}$$

2 Applications for scrambled systems

2.1 Information scrambling by random unitaries

Consider a mixed initial state (we consider an enlarged system as a purification of the mixed state, where the memory is an s-qubit system):

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_R U_A \otimes I_{\mathrm{MEM}}|0,\sqrt{\rho}\rangle + |1\rangle_R U_A \otimes I_{\mathrm{MEM}}|1,\sqrt{\rho}\rangle\right) = \tag{15}$$



,

which contains a reference qubit R maximally entangled with the first qubit of the system A. Applying a random unitary evolution to system A, we ask how much information is shared between R and part of the system A_1.

We can regard the subsystems A_1 and A_2 as two large indices. When calculating $S^{(2)}_{A_1}$, we consider inner-product of the randomized state with boundary $\langle \mathbb{I}_R (12)_{A_1} \mathbb{I}_{A_2 \cup \mathrm{MEM}}|$. Using the Weingarten calculus,

$$\sum_{\sigma,\tau\in S_2} \mathrm{Wg}_2\left(\tau\sigma^{-1}\right)\langle (12)_{A_1}\mathbb{I}_{A_2}|\tau_A\rangle\langle\sigma_A| = \frac{|A|}{|A|^2-1}\left[\left(|A_1| - \frac{1}{|A_1|}\right)\langle (12)_A| + \left(|A_2| - \frac{1}{|A_2|}\right)\langle \mathbb{I}_A|\right], \tag{16}$$

the averaging of the unitary gate effectively alters the boundary to the sum of $\langle \mathbb{I}_R (12)_A \mathbb{I}_{\mathrm{MEM}}|$ and $\langle \mathbb{I}_{A\cup R\cup \mathrm{MEM}}|$. The averaged entropy of A_1 is then[1]

$$2^{-\tilde{S}^{(2)}_{A_1}} = \frac{|A|}{|A|^2-1}\left[\left(|A_1| - \frac{1}{|A_1|}\right)\mathrm{tr}\,\rho_A^2 + \left(|A_2| - \frac{1}{|A_2|}\right)(\mathrm{tr}\,\rho)^2\right]. \tag{17}$$

Similarly, when considering the averaged purity entropy of subsystem $A_1 \cup R$, Eq. (42) changes the boundary from $\langle (12)_R \mathbb{I}_{A_1} (12)_{A_2} \mathbb{I}_{\mathrm{MEM}}|$ to $\langle (12)_{A\cup R} \mathbb{I}_{\mathrm{MEM}}|$ and $\langle (12)_R \mathbb{I}_{A\cup \mathrm{MEM}}|$, i.e.,

$$2^{-\tilde{S}^{(2)}_{A_1\cup R}} = \frac{|A|}{|A|^2-1}\left[\left(|A_1| - \frac{1}{|A_1|}\right)\mathrm{tr}\,\rho^2_{A\cup R} + \left(|A_2| - \frac{1}{|A_2|}\right)\mathrm{tr}\,\rho_R^2\right]. \tag{18}$$

We can quantify the information scrambling by calculating the averaged (purity) mutual information

$$\begin{aligned}\tilde{I}^{(2)}(A_1:R) &\equiv \tilde{S}^{(2)}_{A_1} + \tilde{S}^{(2)}_R - \tilde{S}^{(2)}_{A_1\cup R} = \tilde{S}^{(2)}_{A_1} - \tilde{S}^{(2)}_{A_1\cup R} + 1 \\ &= 1 + \log_2\left[2 - \frac{3}{2}\frac{(2^{\alpha N} - 2^{-\alpha N})}{(2^{\alpha N} - 2^{-\alpha N}) + [2^{(1-\alpha)N} - 2^{-(1-\alpha)N}]2^{-s-1}}\right].\end{aligned} \tag{19}$$

where we assuming A has N qubits and A_2 has αN qubits.

A few remarks are in order. First, when we consider the pure initial state ($s = 0$), the expression is reduced to

$$\tilde{I}^{(2)}(A_1:R) = 1 + \log_2\left[2 - \frac{3(1-4^{-\alpha N})}{2 + 2^{(1-2\alpha)N} - 2^{1-2\alpha N} - 2^N}\right] \simeq \log_2\left[1 + \frac{3}{2 + 2^{(2\alpha-1)N}}\right], \tag{20}$$

where we consider the thermodynamic limit $N \to \infty$. We see that $I_2(A_1 : R)$ behaves like a step function with a critical value at $\alpha = \frac{1}{2}$. It means that recovering Alice's state requires accessing only half of the system for a pure initial state.

[1] Note that what we averaged is $\langle \rho^2_{A_1} \rangle$. We define a purity entropy $\tilde{S}^{(2)}_{A_1} \equiv -\log_2 \langle \rho^2_{A_1}\rangle$. While it is a good approximation of $S^{(2)}_{A_1}$ when the fluctuation is small.

Second, on the other hand, we can consider the maximally mixed ($s = N-1$) initial state. In the thermodynamic limit, we have

$$\tilde{I}^{(2)}(A_1:R) \simeq \log_2\left(1+3\times 4^{-E}\right), \tag{21}$$

where we denote $|A_2| = 2^{-E}$ for the future convenience. This indicates that recovering the initial state requires accessing the entire state. We know that mutual information satisfies $I^{(2)}(A_1:R)+I^{(2)}(A_2\cup\mathrm{MEM}:R)=2$, which leads to $\tilde{I}^{(2)}(A_2\cup\mathrm{MEM}:R)\simeq 2-\log_2(1+3\times 4^{-E})$. Remarkably, Bob can recover the initial information provided that he has access to the full memory, which does not contain any information about the reference, and a few qubits of the system.

2.2 Decoupling inequality

There is a closely related theorem, called the decoupling inequality, which imposes an upper bound on the distance between ρ_{A_2R} and $\rho_{A_2}^{\infty}\otimes\rho_R$, quantified by:

$$\left\langle ||\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R||_1\right\rangle^2 < \frac{|A_2|\cdot|R|}{|A_1|}\operatorname{tr}\rho_{AR}^2. \tag{22}$$

Note that the operator 1-norm is defined as $||O||_1 = \max_j\left\{\sum_i |O_{ij}|\right\}$, and the operator 2-norm is $||O||_2 = \sqrt{\sum_{ij}|O_{ij}|^2}$.

The inequality means that when the qubit number of A_1 is larger than that of A_2, then environment A_2 and reference R quickly become nearly decoupled. Therefore, we expect the mutual information between A_1 and R becomes maximal.

To prove the theorem, we first note[2]

$$\left\langle ||\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R||_1\right\rangle^2 \le |A_2|\cdot|R|\cdot\left\langle\operatorname{tr}\left(\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R\right)^2\right\rangle = |A_2|\cdot|R|\cdot\left\langle\operatorname{tr}\rho_{A_2R}^2\right\rangle - |R|\cdot\operatorname{tr}\rho_R^2. \tag{23}$$

The change of boundary conditions Eq. (16) leads to the following relation

$$\left\langle\operatorname{tr}\rho_{A_2R}^2\right\rangle = \frac{1}{|A_2|}\frac{1-1/|A_1|^2}{1-1/|A|^2}\operatorname{tr}\rho_R^2 + \frac{1}{|A_1|}\frac{1-1/|A_2|^2}{1-1/|A|^2}\operatorname{tr}\rho_{AR}^2 < \frac{1}{|A_2|}\operatorname{tr}\rho_R^2 + \frac{1}{|A_1|}\operatorname{tr}\rho_{AR}^2. \tag{24}$$

We thus prove the theorem.

[2] Cauchy-Schwarz inequality states that

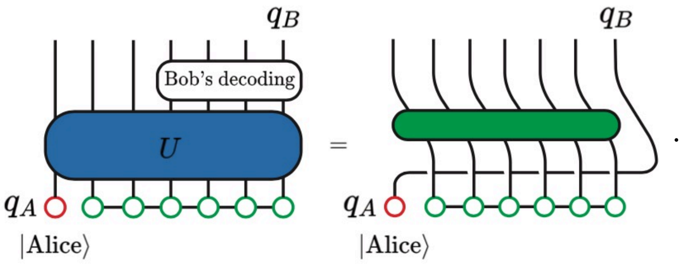
$$\sum_{n=1}^{N}a_n^2\sum_{n=1}^{N}b_n^2 \ge \left(\sum_{n=1}^{N}a_nb_n\right)^2 \implies ||O||_1^2 = \max_j\left(\sum_i|O_{ij}|\right)^2 \le N\max_j\sum_i|O_{ij}|^2 \le N\sum_{i,j}|O_{ij}|^2 = N||O||_2^2.$$

When we take the continuum limit such that $\frac{1}{N}\sum_{n=1}^{N}\to\int dx$, the ineqality becomes $\int f^2(x)dx\int g^2(x)dx \ge \left(\int f(x)g(x)dx\right)^2$. Let $g(x)=1$, and we obtain a continuous version of the inequality:

$$\left[\int dU(\cdots)\right]^2 \le \int dU(\cdots)^2 \implies \left\langle||\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R||_1\right\rangle^2 \le \left\langle\left\|\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R\right\|_1^2\right\rangle \le |A_2|\cdot|R|\cdot\left\langle\left\|\rho_{A_2R}-\rho_{A_2}^{\infty}\otimes\rho_R\right\|_2^2\right\rangle.$$

2.3 Hayden-Preskill protocol

Consider a many-body teleportation described by the following process:



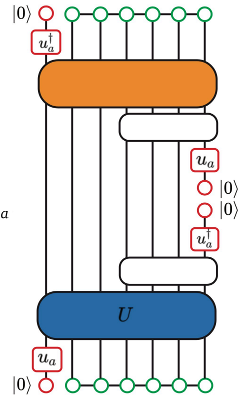
(25)

Denote the quantum state after the decoding $|\Psi_{\text{out}}\rangle$, the fidelity of teleporting the state $|\text{Alice}\rangle$ to the qubit q_B is defined as

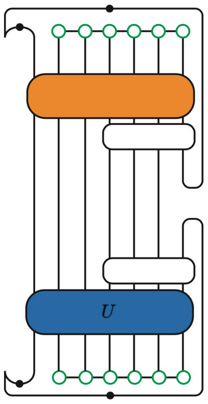
$$F(|\text{Alice}\rangle) = \langle\Psi_{\text{out}}|(|\text{Alice}\rangle\langle\text{Alice}|)_{q_B} \otimes \mathbb{I}|\Psi_{\text{out}}\rangle\,. \tag{26}$$

When the fidelity averaged over Alice's state $\mathbb{E}[F(|\text{Alice}\rangle]$ is 1, it indicates that the system is able to teleport any quantum state with perfect fidelity. The averaged fidelity can be obtained by sampling Alice's state from the action of a random unitary u_a on a basis state $|0\rangle$,

$$\mathbb{E}[F(|\text{Alice}\rangle] = \mathbb{E}_{u_a}$$



$$= \frac{1}{3} + \frac{2}{3}F_{\text{EPR}}, \quad F_{\text{EPR}} \equiv$$



. (27)

Note that the last equation comes from the averaging

$$\int_{U_2} dU\ U_{i_1 0}U^*_{i_1' 0}U_{i_2 0}U^*_{i_2' 0} = \frac{1}{6}(\delta_{i_1 i_1'}\delta_{i_2 i_2'} + \delta_{i_1 i_2'}\delta_{i_2 i_1'}). \tag{28}$$

Also, F_{EPR} can be regarded as the fidelity $F(|\text{EPR}\rangle)$ for a state initially entangled with a reference R before undergoing unitary evolution. A perfect many-body teleportation requires $F_{\text{EPR}} = 1$. So, before decoding, we expect the information shared between R and the subsystem on which the decoder acts maximizes.

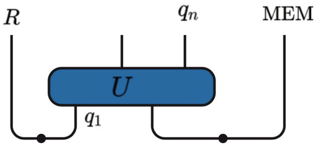
For simplicity, we first consider the case where $A_2 = q_n$ is a single qubit. Now let us look into the mutual information $I(R : \text{MEM} \cup q_n)$ more closely: $I(R : \text{MEM} \cup q_n) = 2 - N + S_{\text{MEM} \cup q_n}$. That is, the mutual information only depends on the entanglement entropy of $\text{MEM} \cup q_n$, satisfying $N - 2 \leq S(\text{MEM} \cup q_n) \leq N$. Since the Von Neumann entropy upper bounds the Renyi entropy, we have,

$$I(R : \text{MEM} \cup q_n) \geq 2 - N + S^{(2)}_{\text{MEM} \cup q_n}. \tag{29}$$

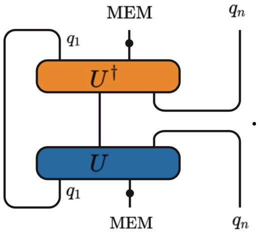
Since in the case we consider here, the qubits $q_{2\sim N}$ are in a fully mixed state, we can choose the simplest purification where the memory contains $(N-1)$ auxiliary qubits that form $(N-1)$

EPR pairs with the $(N-1)$ spins in the system. The time-evolved purified state is

$$|\Psi\rangle =$$



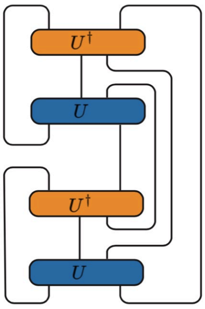
$$, \quad \rho(\mathrm{MEM}\cup q_n) = \frac{1}{2}$$



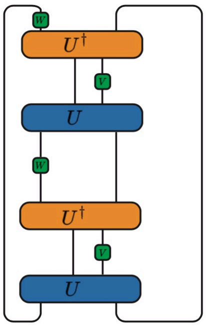
$$. \qquad (30)$$

From the density matrix, we can obtain the purity $\operatorname{tr}\rho^2(\mathrm{MEM}\cup q_n)$ as

$$\operatorname{tr}\rho^2(\mathrm{MEM}\cup q_n) = \frac{1}{4^N}$$



$$= \frac{1}{4^{N+1}}\sum_{W,V}$$



$$, \qquad (31)$$

where W and V are summed over local Pauli matrices on q_1 and q_n. In the last equation, we used the completeness relation of Pauli operators. When either V_1 or W_n equals the identity, the trace contributes 1 to the sum. Separating these terms from the others, we get,

$$\operatorname{tr}\rho^2(\mathrm{MEM}\cup q_n) = \frac{1}{2^{N+2}}\left[7 + \sum_{W_1,V_n\neq I}\frac{1}{2^N}\operatorname{tr}\left(W_1(-t)V_nW_1(-t)V_n\right)\right] \qquad (32)$$

The purity becomes a sum of local correlators between Pauli operators. The Renyi entropy is just $-\log_2\operatorname{tr}\left(\rho^2\right)$. The mutual information is then upper-bounded by the correlator

$$I\left(R:\mathrm{MEM}\cup q_n\right) \geq 4 - \log_2\left[7 + \sum_{W_1,V_n\neq I}\frac{1}{2^N}\operatorname{tr}\left(W_1(-t)V_nW_1(-t)V_n\right)\right]. \qquad (33)$$

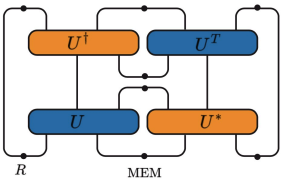
We emphasize that this inequality applies to any unitary U. Each term in the summation has the maximum value of 1, in which case the right-hand side takes the minimal value of 0. This happens when the Heisenberg operator $V_1(-t)$ commutes with the operator W_n for all V and W. When $V_1(-t)$ and W_n start to overlap, the correlator decreases from 1. As a result, $I\left(R:\mathrm{MEM}\cup q_n\right)$ is nonzero, indicating that the information has reached q_n. At the late time, all the terms decay to 0, and the right-hand side becomes $4-\log_2 7$.

Now we discuss the decoding protocol for the Hayden-Preskill setup. The probabilistic decoding protocol goes as follows:

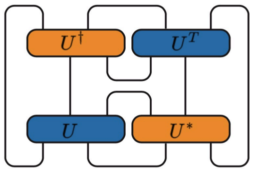
1. Bob takes another two qubits, q_1' and R', and prepares them in an EPR state.
2. Bob applies the unitary operator U^* to $\mathrm{MEM}\cup q_1'$.
3. Bob performs Bell's measurement on each qubit in E and its partner in MEM, with which it forms an EPR initially.
4. The entire protocol is repeated including preparing the state until the outcome of all the Bell measurements are the EPR states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

After these steps, the reference R and R', one of Bob's new qubits, would have high fidelity to form an EPR. This protocol is probabilistic because in step 3 Bob needs to post-select the EPR pairs from the Bell measurements. To understand this decoder, let us calculate the probability of successful postselection and the fidelity $F_{\text{EPR}}\left(R,R'\right)$ given successful postselection. The probability of successful postselection is

$$\Delta =$$



$$= \frac{1}{2^{N+1+E}}$$



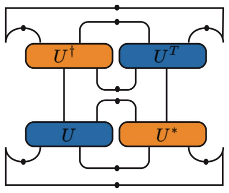
$$. \tag{34}$$

Notice that the diagram is the same as that in Eq. (31) for calculating $\rho^2(\text{MEM}\cup A_2)$. Therefore,

$$\Delta = 2^{N-1-E}\,\text{tr}^2\left(\rho_{\text{MEM}\cup A_2}\right) = 2^{-I^{(2)}(R:\text{MEM}\cup E)}. \tag{35}$$

The probability of the postselection is directly related to the Renyi mutual information between R and Bob's qubit before the decoding. Given the successful postselection, the fidelity that R and R' form an EPR is

$$F_{\text{EPR}} =$$



$$/\Delta = 2^{I^{(2)}(R:\text{MEM}\cup A_2)-2} = \frac{1}{1+3\times 4^{-E}}. \tag{36}$$

That is, F_{EPR} approach 1 exponentially fast as E increases, indicating perfect teleportation fidelity given successful postselection for fully scrambling unitary time evolution. In general, since $\text{tr}^2\,\rho^2(\text{MEM}\cup E)$ can be written as the sum of OTOCs as shown in Eq. (31), the fidelity F_{EPR} is also directly related to OTOCs as

$$F_{\text{EPR}} = \left[\frac{1}{4^E}\frac{1}{2^N}\sum_{W_1,V_{A_2}}\text{tr}\left(W_1(-t)V_{A_2}W_1(-t)V_{A_2}\right)\right]^{-1}, \tag{37}$$

where V_1 and W_{A_2} are summed over all local operators, including the identity, in the first qubit and E, respectively. In the fully scrambled regime, the OTOC is 1 if either V_1 or W_E is the identity and 0 otherwise, and we get Eq. (36) back. We see that OTOC provides a tool to detect information propagation and is directly related to the fidelity of information recovery.

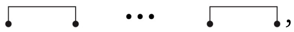
3 Random Quantum Circuit

The Haar-measure integral naturally appears in the calculation of many entanglement-related properties. For example, when we apply a random unitary operator U on (part of) the state $|\psi\rangle$, the resulting state is $|\psi'\rangle = U|\psi\rangle$. The average of the exponential of n-th order renyi entropy on part B,

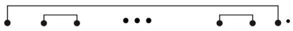
$$Z_n \equiv \left\langle q^{-(n-1)S_B^{(n)}}\right\rangle_{\text{Haar}} = \left\langle \text{tr}\,\rho_B^n\right\rangle_{\text{Haar}} = \left\langle \text{tr}_B\left(\text{tr}_A\, U|\psi\rangle\langle\psi|U^\dagger\right)^n\right\rangle_{\text{Haar}}, \tag{38}$$

formally takes the form of a partition function. We can map Eq. (38) to an enlarged system initially at $|\Psi\rangle \equiv |\psi\rangle^{\otimes n}|\psi^*\rangle^{\otimes n}$, and the action of the unitary operator takes the form $\mathcal{U} =$

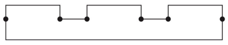
$U^{\otimes n}U^{*\otimes n}$. We regard the $2n$-fold replica indices as a new internal degree of freedom, and then the system is again a quantum chain. The tricky part is the traces. For a single site i in part A, the trace is within each replica, therefore it is straightforward to check that the trace part can be equivalently expressed as the inner product with the bra:

$$\langle e|_i = \delta_{i_i\bar{i}_1}\cdots\delta_{i_n\bar{i}_n} \equiv$$  $, \qquad (39)$

where we have introduced a graphic notation to represent the states. For a site i in part B, the

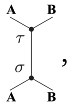
$$\langle(12\cdots n)|_i = \delta_{i_1\bar{i}_2}\delta_{i_2\bar{i}_3}\cdots\delta_{i_{n-1}\bar{i}_n}\delta_{i_n,\bar{i}_1} \equiv$$  $. \qquad (40)$

The graphic notation makes the evaluation of the inner product intuitive. For example, we have

$$\langle e|(123)\rangle =$$  $= q. \qquad (41)$

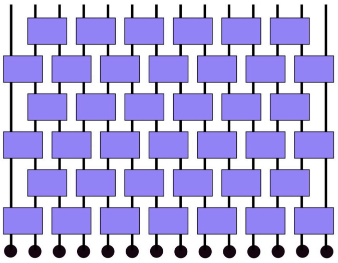
That is, the inner product only depends on the number of cycles in permutation element $\sigma^{-1}\tau$, i.e., $\langle\sigma|\tau\rangle = q^{\#(\sigma^{-1}\tau)}$.

Assuming the unitary operator acts on sites both in A and B, with local Hilbert space dimension q_A and q_B respectively. Taking the Haar-measure average, the random unitary operator is mapped to a tensor node:

$$\left\langle U^{\otimes n}U^{*\otimes n}\right\rangle_{\text{Haar}} = \sum_{\sigma,\tau\in S_n} \text{Wg}_d\left(\tau\sigma^{-1}\right)|\tau_A\tau_B\rangle\langle\sigma_A\sigma_B| \equiv \sum_{\sigma,\tau\in S_n} \text{Wg}_d\left(\tau\sigma^{-1}\right)$$  $, \qquad (42)$

where $d = q_A q_B$.

Now consider the unitary dynamics described by the random circuits:

$$|\psi(t)\rangle = U_{\text{circuit}}(t)|\psi_0\rangle =$$  $. \qquad (43)$

As the first remark, we will show that in the $q \to \infty$ limit, a single action of a random unitary gate U_x on sites x and $(x+1)$ will increase the zeroth-, first-, and second-order Renyi entropy maximally (we denote as $S_x^{(n)}$ the entropy of the first x sites):

$$S_x^{(n)}(t+1) = \min\left\{S_{x+1}^{(n)}(t+1), S_{x-1}^{(n)}(t+1)\right\} + 1,\ n = 0,1,2. \qquad (44)$$

This can be proved by showing $S^{(2)}$ approaches $S^{(0)}$ in this limit. We thus first define their difference as $\Delta(x,t) = S_x^{(0)}(t) - S_x^{(2)}(t) \geq 0$. Using Eq. (16), which gives

$$\left\langle \operatorname{tr}\rho_x(t+1)^2\right\rangle = \frac{q}{q^2+1}\left\langle \operatorname{tr}\rho_{x+1}^2 + \operatorname{tr}\rho_{x-1}^2\right\rangle = \frac{q^2}{q^2+1}\left\langle q^{-S_{x+1}^{(2)}(t)-1}\right\rangle + \frac{q^2}{q^2+1}\left\langle q^{-S_{x-1}^{(2)}(t)-1}\right\rangle. \qquad (45)$$

Note that $S^{(0)}$ satisfies the maximal growth rate, which implies:

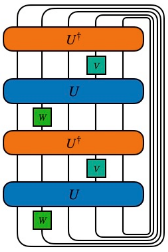
$$\left\langle q^{\Delta(x,t+1)}\right\rangle < \left\langle q^{\Delta(x-1,t)}\right\rangle + \left\langle q^{\Delta(x+1,t)}\right\rangle \implies \left\langle q^{\Delta_{\max}(t+1)}\right\rangle < 2\left\langle q^{\Delta_{\max}(t)}\right\rangle, \qquad (46)$$

where $\Delta_{\max}(t) \equiv \max_x\{\Delta(x,t)\}$. We may iterate the time step successively: $\left\langle 2^{(\log_2 q)\Delta_{\max}(t)}\right\rangle < 2^t$. At fixed time t, as $q \to \infty$, the probability distribution for Δ concentrates around $\Delta = 0$, so $S^{(2)}$ and $S^{(0)}$ agree.

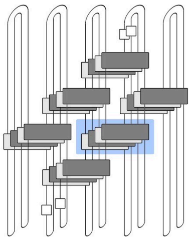
3.1 Scrambling in random circuit

We will consider the information scrambling in the random circuit model. The quantity we consider here is the averaged out-of-time-ordered correlator of two Pauli operators W and V on the sites 0 and x respectively. This can be mapped to a tensor network by folding the evolution circuits and taking the Haar average:

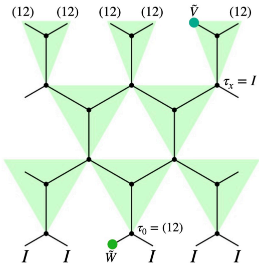
$$F(x,t) = \frac{1}{q^N}$$



$$\xrightarrow{\text{fold}} \frac{1}{q^N}$$

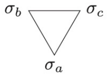


$$\xrightarrow{\text{average}} \frac{1}{q^N}$$



$$, \quad (47)$$

The model can be further simplified by tracing out the middle “spin" in the green triangle. We can then denote the weight for the resulting triangle as:



$$= \sum_{\tau=e,(12)} \mathrm{Wg}_d(\sigma_a\tau^{-1})q^{\#(\sigma_b^{-1}\tau)+\#(\sigma_c^{-1}\tau)} = \begin{cases} \delta_{\sigma_a\sigma_b} & \sigma_b = \sigma_c \\ \frac{q}{q^2+1} & \sigma_b \neq \sigma_c \end{cases}. \tag{48}$$

This weight function makes the model behave like an Ising magnet

$$h_3 = \alpha s_a s_b + \alpha s_a s_c + \beta s_b s_c + \gamma,$$

with local sites taking values $|e\rangle \sim (s=1)$ or $|(12)\rangle \sim (s=-1)$. The 3 parameters can be determined as

$$a = \frac{1}{4}, \quad b = \frac{1}{4} - \frac{q}{2(q^2+1)}, \quad c = \frac{1}{4} + \frac{q}{2(q^2+1)}.$$

In the domain wall picture, this Ising magnet has the property that the domain wall shall not be horizontal.

For the spin τ_0. When $\tau_0 = (12)$, since we assume W to be Pauli (therefore $W^2 = \mathbb{I}$), we could replace W with $\mathbb{I}$ for this τ_0. While in doing so, τ_0 can also be e, which is a fictitious contribution. Taking in this part, the total result is 1. Therefore, the OTOC can be expressed as

$$F = 1 - \sum_{\tau} W(\tau)|_{\tau_0 \to e, W \to \mathbb{I}}. \tag{49}$$

We denote $C(x,t) = 1 - F(x,t)$ and calculate this instead in the following. When considering the statistical model corresponding to $C(x,t)$, there will be two downward domain walls starting from x, the total weight is nonzero only when τ_0 is in the e domain.

In the bottom region, each Ising variable $\tau = (12)$ contributes a factor q^2, which will be renormalized out, while each $\tau = e$ contributes a factor of q^4, which contributes an additional q^2 factor (factor q per site). Since the number of Ising variables is half of the original spin, the size of the bottom domain contributes additional weight to the partition function. Now the evaluation of the partition function is mapped to a random walk problem. We introduce the null coordinate

$$\underline{u} \equiv \frac{1}{2}(\underline{t} + \underline{x}), \quad \underline{v} \equiv \frac{1}{2}(\underline{t} - \underline{x}), \tag{50}$$

and denote the endpoint in this coordinate as (l_u, l_v). Note that $l_u + l_v = t$. For each step, the trajectory increases one unit in either $\underline{u}$ or $\underline{v}$ direction. We denote the endpoint (light-cone coordinate) of the left/right random walk as:

$$X_L = (l_u - u, l_v - t + u), \quad X_R = (l_u - t + v, l_v - v). \tag{51}$$

The length of the bottom domain is

$$(X_L^u - X_L^v) - (X_R^u - X_R^v) = 2t - 2u - 2v. \tag{52}$$

Also, two domain walls contribute a constant factor of $\left[q/(q^2+1)\right]^{2t}$. Therefore, the asymptotic behavior of the weight function is:

$$C(x,t) \propto \left(\frac{q}{q^2+1}\right)^{2t} \sum_{u=0}^{l_u} \sum_{v=0}^{l_v} q^{2t-2u-2v} \binom{t}{u}\binom{t}{v} = \left[\sum_{u=0}^{l_u} \binom{t}{u} \frac{q^{2(t-u)}}{(q^2+1)^t}\right] \left[\sum_{v=0}^{l_v} \binom{t}{v} \frac{q^{2(t-v)}}{(q^2+1)^t}\right].$$

Note that in the last expression, the summation corresponds to the distribution of random walk with a biased probability $p = 1/(q^2+1)$. We remark here that we completely neglect the cases where two paths cross since it's negligible in the long-time limit, while in the early time, it's just a constant factor.

Theorem 1. *The binomial expression gives a Gaussian distribution:*

$$f(u,t) = \binom{t}{u}(1-p)^{t-u}p^u \xrightarrow{x=2u-t} \exp\left[-\frac{1}{2}\left(\frac{x - v_B t}{\sigma(t)}\right)^2\right],$$

where the butterfly velocity v_B and the broadening factor $\sigma(t)$ are

$$v_B = 1 - 2p = \frac{q^2-1}{q^2+1}, \quad \sigma(t) = 2\sqrt{p(1-p)t} = \frac{2q\sqrt{t}}{q^2+1}.$$

Proof. Sterling's approximation:

$$n! \sim \sqrt{2n\pi}\left(\frac{n}{e}\right)^n. \tag{53}$$

Using this approximation, and think of t and u as both large,

$$f(u,t) = \sqrt{\frac{t}{2\pi t(t-u)}}(1-p)^{t-u}p^u\left(\frac{u}{t}\right)^{-u}\left(1-\frac{u}{t}\right)^{-t+u}.$$

Assuming $u = pt + \delta$,

$$\begin{aligned} f(u,t) &= \sqrt{\frac{t}{2\pi u(t-u)}}(1-p)^{t-u}p^u\left(p+\frac{\delta}{t}\right)^{-u}\left(1-p-\frac{\delta}{t}\right)^{-t+u} \\ &= \sqrt{\frac{t}{2\pi u(t-u)}}\left(1+\frac{\delta}{pt}\right)^{-pt+\delta}\left(1-\frac{\delta}{(1-p)t}\right)^{-(1-p)t+\delta} \end{aligned}$$

Taking the logarithm,

$$\begin{aligned} \ln\left[\sqrt{\frac{2\pi u(t-u)}{t}}f\right] &= (\delta - pt)\ln\left(1+\frac{\delta}{pt}\right) - [\delta + (1-p)t]\ln\left(1-\frac{\delta}{(1-p)t}\right) \\ &= (\delta - pt)\left(\frac{\delta}{pt} - \frac{1}{2}\frac{\delta^2}{p^2t^2}\right) - [\delta - (1-p)t]\left[\frac{\delta}{(1-p)t} + \frac{1}{2}\frac{\delta^2}{(1-p)^2t^2}\right] \\ &= -\frac{\delta^2}{2p(1-p)t} + O(\delta^3). \end{aligned}$$

Note that $x = 2u - t = (2p-1)t + 2\delta$, therefore,

$$\delta = \frac{x + (1-2p)t}{2} \equiv \frac{x + v_B t}{2}.$$

We then get the following distribution

$$f(x,t) \simeq \frac{1}{\sqrt{2\pi}\sqrt{p(1-p)t}} \exp\left[-\frac{(x+v_B t)^2}{8p(1-p)t}\right].$$

The variance is

$$\sigma(t) = 2\sqrt{p(1-p)t}.$$

Note that

$$f(x,t) = \begin{cases} \frac{2}{\sqrt{2\pi}\sigma(t)} \exp\left[-\frac{1}{2}\left(\frac{x+v_B t}{\sigma(t)}\right)^2\right] & x = t \mod 2 \\ 0 & x \neq t \mod 2 \end{cases}.$$

In the continuum limit, we can smooth the function and therefore get rid of the factor 2. Therefore we reach the desired expression. □

With proper normalization, we obtain the asymptotic expression for the OTOC:

$$C(x,t) = \operatorname{erf}\left(\frac{x+v_B t}{\sigma(t)}\right)\operatorname{erf}\left(\frac{x-v_B t}{\sigma(t)}\right), \quad \operatorname{erf}(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{x^2}{2}}dx. \tag{54}$$

Thus, we have shown via an exact calculation that operator spreading in (1 + 1)D can be understood in terms of diffusion and drift. The front of the operator propagates at a finite velocity $v_B < 1$. However, the front also broadens diffusively, so its width is proportional to $\sqrt{t}$. We conjecture that this physics also occurs in generic (nonintegrable) 1D systems undergoing deterministic Hamiltonian dynamics.

3.2 Entanglement entropy and replica trick

The above mapping can be generalized to entanglement entropy. In particular, the averaged purity entropy, defined as $\tilde{S}_x^{(2)}(t) \equiv -\log_q\langle \operatorname{tr}\rho_x^2(t)\rangle$, can be mapped to a statistical model described by a statistical model with the same bulk as Eq. (47), but with a free boundary condition on the bottom and a fixed boundary $\left\langle e^{\otimes x}, (1,2)^{\otimes(N-x)}\right|$ on the top. In the domain-wall language, all random paths contribute equally to the partition function Z, i.e.,

$$Z \simeq \left(\frac{2q}{q^2+1}\right)^t \quad \Longrightarrow \quad \tilde{S}_x^{(2)}(t) \simeq \tilde{v}_2 t, \quad \tilde{v}_2 = \log_q\left(\frac{q^2+1}{2q}\right). \tag{55}$$

We can generalize the purity entropy to higher orders, and define $\tilde{S}_x^{(n)} \equiv -\frac{1}{n-1}\log_q\langle \operatorname{tr}\rho_x^n\rangle$. We expect all entanglement entropies to grow linearly in time, i.e., $\tilde{S}^{(n)}(t) \simeq \tilde{v}_n t$, $S^{(n)}(t) \equiv v_n t$. In particular, $v_1 = v_E$ is called the entanglement speed. Note that since the exponential function is convex,

$$\left\langle q^{-(n-1)S^{(n)}(t)}\right\rangle \geq q^{-(n-1)\langle S^{(n)}(t)\rangle} \quad \Longrightarrow \quad \tilde{S}^{(n)}(t) \leq S^{(n)}(t) \quad \Longrightarrow \quad \tilde{v}_n \leq v_n \leq v_E. \tag{56}$$

Note that this expression bounds the growth rate of $S^{(n)}(t)$ but does not fix it, since the averaging of exponentials will be affected by anomalously small values of $S^{(n)}$, making it very different from $\tilde{S}^{(n)}$.

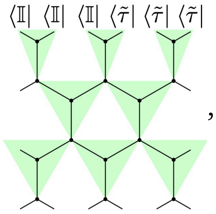
We can use the replica trick to access the average of Renyi entropies. That is, we first calculate the average of k-th power of $Z_n \equiv \operatorname{tr}\rho_x^n(t)$ for an arbitrary integer number k. Using the facts

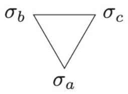
$$\langle Z_n^k\rangle = 1 + k\langle \ln Z_n\rangle + \frac{k^2}{2}\langle \ln^2 Z_n\rangle + O(k^3), \quad \log_q(1+x) = \frac{1}{\ln q}\left(x - \frac{1}{2}x^2\right) + O(x^3), \tag{57}$$

we obtain a formal series expansion for the replicated system:

$$\begin{aligned}\log_q\langle Z_n^k\rangle &= k\frac{\langle \ln Z_n\rangle}{\ln q}+\frac{k^2}{2}\left[\frac{\langle \ln^2 Z_n\rangle}{\ln q}-\frac{\langle \ln Z_n\rangle^2}{\ln q}\right]+O(k^3)\\ &= -k(n-1)\left\langle S^{(n)}(t)\right\rangle+\frac{k^2(n-1)^2\ln q}{2}\left\langle\left[S^{(n)}(t)-\left\langle S^{(n)}(t)\right\rangle\right]^2\right\rangle+O(k^3).\end{aligned} \tag{58}$$

That is, if we obtain the analytic form of $\left\langle Z_n^k\right\rangle$ for $k\to 0$, we not only know the averaged n-th order Renyi entropy, but also the variance thereof. The full expression for $\left\langle Z_n^k\right\rangle$ is obtained by contracting the tensors (blocks) in accordance with the spatiotemporal structure of the circuit. Graphically, $\left\langle[\operatorname{tr}\rho_x^n]^k\right\rangle$ can be represented as a lattice magnet with a specific boundary condition, which can be graphically represented as:

$\langle Z_n^k\rangle =$ 

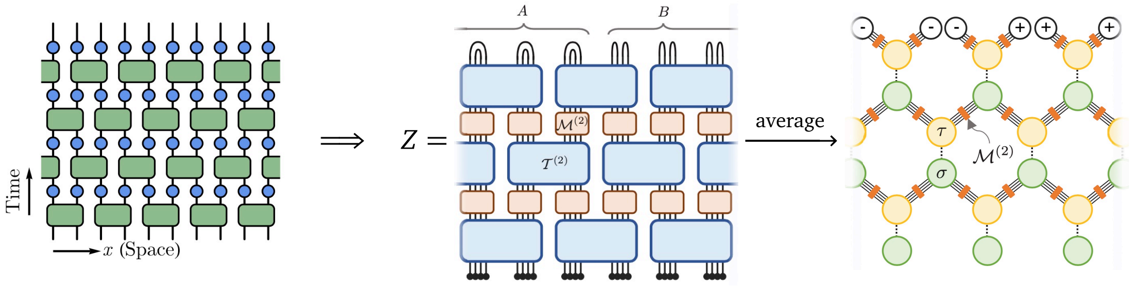
, 

$= \sum_{\tau\in S_{nk}} \mathrm{Wg}_d(\sigma_a\tau^{-1})q^{\#(\sigma_b^{-1}\tau)+\#(\sigma_c^{-1}\tau)}$, (59)

where on the upper boundary $|\tilde{\tau}\rangle = \left|(12\cdots n)^{\otimes k}\right\rangle$, and there is a free boundary condition on the bottom.

3.3 Monitored random circuits

Consider a random unitary circuit interspersed by local projective measurements:



Each blue circle is a random measurement described by the Krause operator

$$\{\mathcal{M}\} = \left\{\sqrt{1-p}\,\mathbb{I},\sqrt{p}|0\rangle\langle 0|,\cdots,\sqrt{p}|q\rangle\langle q|\right\}. \tag{60}$$

We will consider the averaged purity entropy of this monitored evolution, which can also be mapped to a statistical model. The unitary gate can be averaged similarly. The only difference is the insertion of a quantum channel $\{\mathcal{M}\}$ represented by small orange bricks. The statistical weight on the monitored bond is:

$$W_p(\sigma,\tau) = \sum_{i=0}^{q}\langle\sigma|\mathcal{M}_i^{\otimes 4}|\tau\rangle = \begin{cases}(1-p)q^2+pq & \sigma=\tau\\ q & \sigma\neq\tau\end{cases} = (1-p)q^{\#(\sigma^{-1}\tau)}+pq\equiv W_p(\sigma^{-1}\tau). \tag{61}$$

The statistical model is now a classical Ising model (with $\mathbb{Z}_2$ spin-flip symmetry). We can use the Ising variables $(+)\equiv e$, $(-)\equiv(12)$ to simplify the notation. By integrating out the middle spin degrees of freedom, we can obtain a triangle Ising model:

$$J\left(\sigma_b,\sigma_c;\sigma_a\right) = \sum_{\tau=\pm}\mathrm{Wg}_d\left(\sigma_a\tau\right)W_p(\tau\sigma_b)W_p(\tau\sigma_c)\equiv\exp\left(-J_h\sigma_b\sigma_c-J_d\sigma_a\sigma_b-J_d\sigma_a\sigma_c\right), \tag{62}$$

where the pairwise interacting strength in the horizontal/diagonal directions is J_h/J_d:

$$\begin{aligned} J(+,+;+) &= \mathrm{Wg}(+)W_p^2(+) + \mathrm{Wg}(-)W_p^2(-) = C\ e^{-J_h-2J_d}, \\ J(-,-;+) &= \mathrm{Wg}(+)W_p^2(-) + \mathrm{Wg}(-)W_p^2(+) = C\ e^{-J_h+2J_d}, \\ J(+,-,+) &= [\mathrm{Wg}(+)+\mathrm{Wg}(-)]\,W_p(+)W_p(-) = C\ e^{+J_h}. \end{aligned} \tag{63}$$

This classical model is exactly solvable. The critical point is at

$$2e^{2J_h} = e^{-2J_d} - e^{2J_d} \quad\Longleftrightarrow\quad 2J(+,-;+) = J(+,+;+) - J(-,-;+), \tag{64}$$

which leads to the exact transition frequency p_c for averaged purity:

$$2\frac{\mathrm{Wg}(+)/\mathrm{Wg}(-)+1}{\mathrm{Wg}(+)/\mathrm{Wg}(-)-1} = \frac{W_p(+)}{W_p(-)} - \frac{W_p(-)}{W_p(+)} \implies p_c = \frac{q^3-q^2-\sqrt{2(q^4+1)}+q+1}{(q-1)(q^2+1)}. \tag{65}$$

For the qubit case ($q=2$), $p_c = (7-\sqrt{34})/5 = 0.2338\cdots$. This transition point is smaller than the numerical result ($P_c \approx 0.26$). We also note that in the $q \to \infty$ limit, $p_c \to 1$ apparently deviates from the percolation transition point (where $p_c = 1/2$).

In the following, we will consider general $\tilde{S}^{(n)}$ in the $q \to \infty$ limit. The weights $\mathrm{Wg}_d(\sigma)$ and $W_p(\sigma)$ in the large q limit simplified to

$$\mathrm{Wg}_d(\sigma) \simeq q^{-2n}\delta_{\sigma,\mathbb{I}}, \quad W_p(\sigma) \simeq (1-p)q^n\delta_{\sigma,\mathbb{I}}+pq \quad\implies\quad J(\sigma_b,\sigma_c;\sigma_a) \simeq e^{-K(p)(\delta_{\sigma_a,\sigma_b}+\delta_{\sigma_a,\sigma_c})}, \tag{66}$$

where $K(p) = -\ln\left[1+\frac{1-p}{p}q^{n-1}\right] < 0$. This is a $(nk)!$-state Potts model, whose transition point is $K_c = -\ln(1+\sqrt{n!})$. Therefore

$$p_c = \frac{q^{n-1}}{q^{n-1}+\sqrt{n!}} = \begin{cases} 0.5 & n=1 \\ 1 & n>1 \end{cases}. \tag{67}$$

We recover the percolation result for $S^{(1)}$.

4 Classical Shadows

For an unknown quantum state ρ, a **classical shadow** is obtained by

1. Apply random unitary U_i to ρ;
2. Perform projective measurement on every site, which produces a vector $|b_i\rangle$;
3. Repeat the procedure for multiple times, obtaining an ensemble $\{(U_i, |b_i\rangle)|i=1,2,\ldots,N\}$.

The expectation of $U_i^\dagger|b_i\rangle$ is a linear map of the density matrix:

$$\mathcal{M}(\rho) = \mathbb{E}\left[U^\dagger|b\rangle\langle b|U\right] = \sum_b \int_{U(d)} \langle b|U\rho U^\dagger|b\rangle \cdot U^\dagger|b\rangle\langle b|U. \tag{68}$$

In the following, we will consider different choice twirling $\{U_i\}$.

4.1 Global twirling

If $U \in U(2^n)$, the Weingarten calculus returns:

$$\int_U U_{ij_1} U_{ij_2} U^*_{ij'_1} U^*_{ij'_2} = \frac{\delta_{j_1 j'_1}\delta_{j_2 j'_2} + \delta_{j_1 j'_2}\delta_{j_2 j'_1}}{2^n(2^n+1)}. \tag{69}$$

Therefore, the linear map is

$$\mathcal{M}(\rho) = \sum_{i,\{j\}} \int_U U_{ij_1} U^*_{ij_2} U_{ij_3} U^*_{ij_4} \rho_{j_1 j_2} |j_4\rangle\langle j_3| = \frac{\operatorname{tr}\rho\mathbb{I} + \rho}{2^n+1}. \tag{70}$$

The inverse is $\mathcal{M}^{-1}(\rho) = (2^n+1)\rho - \operatorname{tr}(\rho)\mathbb{I}$. For an observable o,

$$\operatorname{tr}(\rho o) = \operatorname{tr}[\mathcal{M}(\rho)\mathcal{M}^{-1}(o)] = (2^n+1)\mathbb{E}\left[\langle b|UoU^\dagger|b\rangle\right] - \operatorname{tr} o. \tag{71}$$

Note that we used the fact that $\mathcal{M}$ is self-adjoint since

$$\operatorname{tr}[\mathcal{M}(A)\cdot B] = \frac{1}{d+1}[\operatorname{tr}A\operatorname{tr}B + \operatorname{tr}(AB)] = \operatorname{tr}[A\cdot\mathcal{M}(B)].$$

The classical shadow gives the sample $\hat{o} = \langle b|U\mathcal{M}^{-1}(o)U^\dagger|b\rangle$. The variance is

$$\operatorname{Var}[\hat{o}] = \sum_b \int_U \langle b|U\rho U^\dagger|b\rangle\langle b|U\mathcal{M}^{-1}(o)U^\dagger|b\rangle^2 - [\mathbb{E}(o)]^2 \le \left\| o - \frac{\operatorname{tr} o}{2^n}\mathbb{I}\right\|_{\text{shadow}}, \tag{72}$$

where the shadow norm is defined as

$$\|o\|^2_{\text{shadow}} = \max_\sigma \sum_b \int_U \langle b|U\sigma U^\dagger|b\rangle\langle b|U\mathcal{M}^{-1}(o)U^\dagger|b\rangle^2. \tag{73}$$

We will consider the bound for the shadow norm, using the Weingarten calculus result

$$\int_{U(d)} U_{ij_1}U_{ij_2}U_{ij_3}U^*_{ij'_1}U^*_{ij'_2}U^*_{ij'_3} = \frac{\delta^{j_1,j_2,j_3}_{j'_1,j'_2,j'_3} + \delta^{j_1,j_2,j_3}_{j'_2,j'_1,j'_3} + \delta^{j_1,j_2,j_3}_{j'_1,j'_3,j'_2} + \delta^{j_1,j_2,j_3}_{j'_3,j'_2,j'_1} + \delta^{j_1,j_2,j_3}_{j'_2,j'_3,j'_1} + \delta^{j_1,j_2,j_3}_{j'_3,j'_1,j'_2}}{2^n(2^n+1)(2^n+2)}. \tag{74}$$

For traceless operator o, the result is

$$\|o\|^2_{\text{shadow}} = \frac{2^n+1}{2^n+2}\max_\sigma\left[\operatorname{tr}(o^2) + 2\operatorname{tr}(\sigma o^2)\right] < 3\operatorname{tr}(o^2). \tag{75}$$

In this way, if o is a projector to a certain state, the shadow norm is bounded by a constant.

4.2 Local twirling

If $U \in U(2)^{\otimes n}$, the linear map shall be described by the tensor product

$$\mathcal{M}(o_1\otimes\cdots\otimes o_N) = \bigotimes_{i=1}^N \frac{\operatorname{tr} o_i\mathbb{I} + o_i}{3}, \quad \mathcal{M}^{-1}(o_1\otimes\cdots\otimes o_N) = \bigotimes_{i=1}^N (3o_i - \operatorname{tr} o_i\mathbb{I}). \tag{76}$$

This map has a simple form only if the operator it acts on is a tensor product. It is suitable to predict a k-local Pauli operator $o = P_{i_1}\otimes\cdots\otimes P_{i_k}$:

$$\operatorname{tr}(\rho o) = \operatorname{tr}[\mathcal{M}(\rho)\mathcal{M}^{-1}(o)] = \prod_{j=1}^k \left\{3\mathbb{E}\left[\langle b|UP_{i_j}U^\dagger|b\rangle\right] - \operatorname{tr}P_{i_j}\right\}. \tag{77}$$

Similarly, the shadow norm is

$$\|o\|^2_{\text{shadow}} = \max_\sigma \operatorname{tr}\left[\sigma\bigotimes_{j=1}^k \frac{3}{4}\left(\operatorname{tr}P^2_{i_j}\mathbb{I} + 2P^2_{i_j}\right)\right] = 3^k. \tag{78}$$