# Entanglement of random hypergraph states

You Zhou [1,2,3,*] and Alioscia Hamma [4,5,†]

[1] *Key Laboratory for Information Science of Electromagnetic Waves (Ministry of Education), Fudan University, Shanghai 200433, China*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371*
[4] *Physics Department, University of Massachusetts Boston, Boston, Massachusetts 02125, USA*
[5] *Dipartimento di Fisica Ettore Pancini, Università degli Studi di Napoli Federico II, Via Cinthia, 80126 Napoli NA, Italy*

(Received 29 November 2021; revised 13 March 2022; accepted 7 June 2022; published 7 July 2022)

Random quantum states and operations are of fundamental and practical interests. In this paper, we investigate the entanglement properties of random hypergraph states, which generalize the notion of graph states by applying generalized controlled-phase gates on an initial reference product state. In particular, we study the two ensembles generated by random controlled-Z (CZ) and controlled-controlled-Z (CCZ) gates, respectively. By applying tensor network representation and combinational counting, we analytically show that the average subsystem purity and entanglement entropy for the two ensembles feature the same volume law but greatly differ in typicality, namely, the purity fluctuation is small and universal for the CCZ ensemble while it is large for the CZ ensemble. We discuss the implications of these results for the onset of entanglement complexity and quantum chaos.

DOI: 10.1103/PhysRevA.106.012410

## I. INTRODUCTION

Entanglement [1] is the peculiar characteristic of quantum mechanics in multipartite systems, not only enabling quantum information processing with an advantage on its classical counterpart [2] but also finding fundamental applications in other branches of physics, such as condensed matter [3] and quantum gravity [4]. Quantum hypergraph states [5–7] are an archetypal class of multipartite states generalizing the notion of graph states [8,9] by involving multiqubit controlled-phase gates. Hypergraph states are of wide interest in measurement-based quantum computing [10–12], quantum advantage protocols [13], nonlocality tests [14,15], quantum error correction, and topological phases of matter [11,16–18].

In this paper, we study the entanglement statistics of ensembles of hypergraph states, specifically, ensembles generated by random controlled-Z (CZ) and controlled-controlled-Z (CCZ) gates, respectively. By adopting a tensor network representation, we reduce the calculations to combinational problems. The main results of this paper are (i) the average subsystem purity and entanglement entropy in the two ensembles are essentially the same with Haar random states and, on the other hand, (ii) fluctuations for the subsystem purity are very different: While the CCZ ensemble features $O(d^{-2})$, Haar-like fluctuation, the CZ ensemble has larger $O(d^{-1})$ fluctuations with $d$ the total Hilbert space dimension. Consequently, for subsystems with half numbers of qubits, a volume law $S_2 \simeq N/2 - 1$ for the entanglement entropy is typical for the CCZ ensemble with the variance of entanglement entropy exponentially small, scaling $\exp(-N)$ with qubit number $N$, while the variance of the CZ ensemble is $O(1)$ and makes the expectation value not typical.

These results have a bearing on the different entanglement complexities of the hypergraph states generated by CZ and CCZ gates and can inspire further studies on entanglement cooling algorithms [19–21], quantum (pseudo)randomness [22–24], quantum magic [25,26], and quantum chaotic dynamics [27,28] in many-body physics. In particular, random hypergraph states and generalized controlled-phase gates can provide toy models capturing the essential physics for complex dynamics while being easier to simulate. In addition, these techniques could be useful to study less structured quantum ensembles that are not necessarily an (approximate) $t$ design [29,30].

## II. PRELIMINARIES

### A. Quantum hypergraph state

First, let us recall the basic setup of hypergraph states [6,7]. A hypergraph $G = (V, E)$, is a pair consisting of the vertex set $V = \{1, 2 \cdots, N\}$, and the edge set $E \subset V$. If a hyperedge $e \in E$ contains $1 \leqslant k \leqslant N$ vertices, we say $e$ is a $k$ edge. A hypergraph only containing $k$ edges is said to be $k$ uniform. See Fig. 1 for an illustration. We attach a local Hilbert space $\mathcal{H}_i$ at every vertex $i \in V$ and thus the total Hilbert space is $\mathcal{H} = \otimes_{i\in V}\mathcal{H}_i$. We are concerned with the case of qubits, i.e., $\mathcal{H}_i \simeq \mathbb{C}^2$. The Hilbert space associated to an edge $e$ is $\mathcal{H}_e := \otimes_{i\in e}\mathcal{H}_i$ and of course $\dim \mathcal{H}_e = 2^k$ for a $k$ edge. The total Hilbert space dimension is denoted as $d = 2^N$.

To every hypergraph, we associate a (pure) quantum state in this way. First define the reference state $|\Psi_0\rangle = |+\rangle^{\otimes N}$, with

*you_zhou@fudan.edu.cn
†alioscia.hamma@unina.it

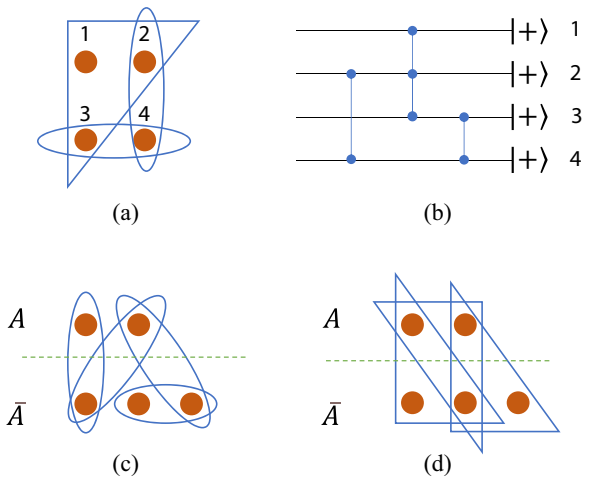



FIG. 1. (a) A hypergraph with four vertices. There are three hyperedges, one of them containing the three vertices 1,2,3. (b) The preparation quantum circuit in Eq. (1), which evolves from *right to left* hereafter. Vertical blue line denotes the $\mathrm{CZ}_e$ gate and the small circles on each qubit line indicate the connection. In a five-qubit system, (c) shows a two-uniform hypergraph state and (d) shows a three-uniform one, respectively.

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ the eigenstate of Pauli $X$ operator. Then, the hypergraph state is obtained from the reference state by operating generalized CZ gates according to the edges $e \in E$:

$$|G\rangle = \left(\prod_{e\in E} \mathrm{CZ}_e\right)|\Psi_0\rangle. \tag{1}$$

Here the quantum gate $\mathrm{CZ}_e = \otimes_{i\in e}\mathbb{I}_i - 2\otimes_{i\in e}|1\rangle_i\langle 1|$ acts nontrivially on $\mathcal{H}_e$, but trivially on the qubits outside. See Fig. 1(b) for the corresponding quantum circuit. For a 1-edge $e = \{i\}$, $\mathrm{CZ}_e$ is just a Pauli Z gate on qubit $i$; for a 2-edge, it becomes the normal CZ gate. Note that the sequence to operate the $\mathrm{CZ}_e$ gate does not matter as they commute with each other, and thus the quantum hypergraph state $|G\rangle$ is uniquely determined by the hypergraph $G$.

Previous works on the entanglement and correlation of hypergraph states mainly deal with specific given states, see, e.g., Refs. [14,15], or results on entanglement witnesses [31], local unitary transformations [32–35], and efficient verification [36,37]. The structure of the states or the number of qubits in the system are usually restricted, since the scaling of the problems makes it quite challenging to extend. In this paper, we instead consider the statistical results of entanglement properties of random hypergraph state ensembles (defined in the next section) and, at the same time, the behavior under large qubit number $N$ can be analyzed. We also remark that Ref. [38] studies random graph states but follows a quite different definition.

### B. Random state ensembles

In this section, we define the random hypergraph state ensembles $\mathcal{E}$ from the corresponding random hypergraph ensembles. In particular, we consider random 2-edge and 3-edge hypergraphs. A random $k$-uniform hypergraph can be determined by the probability $p$ whether there is a $k$ edge among any choice of $k$ sites. In the following, we focus on the case $p = 1/2$.

According to Eq. (1), the corresponding ensembles of hypergraph states are generated by CZ gates and CCZ gates, as shown in Figs. 1(c) and 1(d). Denote the combination number $C_N^k := \binom{N}{k}$ and, formally, the state ensemble is defined as follows.

*Definition 1.* The (k-uniform) random hypergraph state ensemble $\mathcal{E}$ on an $N$-qubit system is generated by

$$\mathcal{E} = \left\{|\Psi\rangle = U|\Psi_0\rangle \,|U = U_{e_{C_N^k}}\cdots U_{e_2}U_{e_1}\right\}. \tag{2}$$

Here each $e_i$ is a distinct $k$ edge of the $N$ vertices, with totally $C_N^k$ such edges, $U_{e_i}$ acts on the Hilbert space $\mathcal{H}_{e_i}$ by taking $\{\mathbb{I}_{e_i}, \mathrm{CZ}_{e_i}\}$ with $1/2$ probability, and $|\Psi_0\rangle = |+\rangle^{\otimes N}$.

Since the $\mathrm{CZ}_e$ gates commute, the order of the gate sequence in Eq. (2) is irrelevant. Of course, there are $2^{C_N^k}$ elements in $\mathcal{E}$ with equal probability, that is, $|\mathcal{E}| = 2^{C_N^k}$. In this paper, we focus on the $k = 2$ and $k = 3$ random hypergraph state ensembles, denoted by $\mathcal{E}_{\mathrm{CZ}}$ and $\mathcal{E}_{\mathrm{CCZ}}$, respectively. Of course, the $k = 1$ case is trivial as this is just a single qubit gate, so the corresponding graph states are just product states. The first nontrivial gate is the $k = 2$, CZ gate. Note that CZ is a Clifford gate but other $\mathrm{CZ}_e$ for $k > 2$ are not [39]. By adding the Hadamard gate to $\mathrm{CZ}_e$, the gate set becomes universal for quantum computing [40] and we conjecture that the results of CCZ hold for other $\mathrm{CZ}_e$ with some constant $k > 3$.

### C. Entanglement entropy and purity

Consider a bipartition of the $N$-qubit system into $\{A, \bar{A}\}$ with $N_A$ and $N_{\bar{A}}$ qubits, respectively, and the total Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$. The bipartite entanglement with respect to $\{A, \bar{A}\}$ of a pure quantum state $|\Psi\rangle$ is quantified by the Rényi-$\alpha$ entanglement entropy defined as

$$S_\alpha(\rho_A) = \frac{1}{1-\alpha}\log_2\left[\mathrm{Tr}\left(\rho_A^\alpha\right)\right], \tag{3}$$

where $S_\alpha$ is the the Rényi-$\alpha$ entropy of the reduced density matrix $\rho_A = \mathrm{Tr}_{\bar{A}}(\Psi)$, with $\Psi = |\Psi\rangle\langle\Psi|$. As $\alpha = 1$, Eq. (3) gives the von Neumann entropy. The Rényi-2 entropy shows

$$S_2(\rho_A) = -\log_2(P_A), \tag{4}$$

with $P_A = \mathrm{Tr}(\rho_A^2)$ the purity functional. The Rényi-2 entropy is a lower bound of the von Neumann entropy. This quantity is particularly useful as the purity $P_A$ can be directly measured in experiment [41,42].

In the next sections, we compute the average subsystem purity and the variance of the purity for the state $\Psi$ from the ensembles $\mathcal{E} = \mathcal{E}_{\mathrm{CZ}}, \mathcal{E}_{\mathrm{CCZ}}$, that is,

$$\langle P_A\rangle_{\mathcal{E}} := \mathbb{E}_{\mathcal{E}}(P_A), \quad \delta^2_{\mathcal{E}}(P_A) := \mathbb{E}_{\mathcal{E}}\left(P_A^2\right) - \left[\mathbb{E}_{\mathcal{E}}\left(P_A\right)\right]^2 \tag{5}$$

Hereafter we also use $\langle\cdot\rangle_{\mathcal{E}}$ to denote the ensemble average.

## III. AVERAGE SUBSYSTEM PURITY

In this section, we study the average purity of a subsystem $A$ for random hypergraph states. By introducing a tensor network representation in Sec. III A to facilitate the calculation, the problem is transformed to some combinational counting

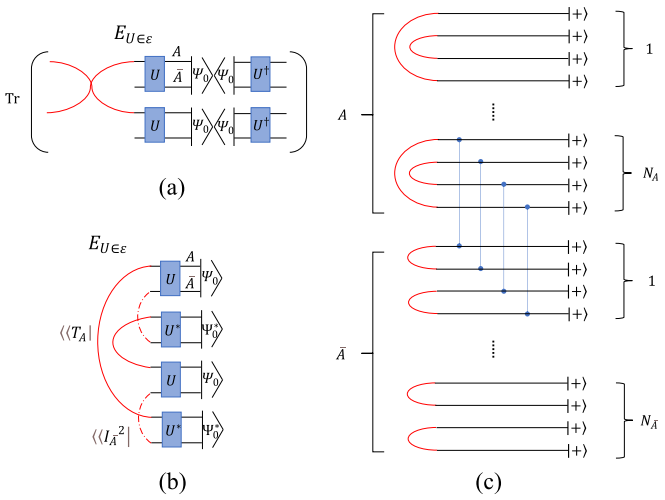



FIG. 2. Tensor network of the purity formula and its vectorization. (a) The purity formula of Eq. (6), with the red cross being the swap operator on subsystem $A$. (b) Rearrangement of the tensors, with swap and identity operators becoming two kinds of vectors on the left. (c) Take the input state as $|\Psi_0\rangle = |+\rangle^{\otimes N}$ and further rearrange the tensor network to put the two-copy of the $i$th qubit Hilbert space $\mathcal{H}_i$ together. As a result, on the right, every qubit corresponds to four lines, each two for one-copy Hilbert space; in the middle, we operate the random $\mathrm{CZ}_e$ gate across $A$ and $\bar{A}$. An example of CZ gate is shown, repeating four times connecting the corresponding lines of the two-qubit; on the left, the original swap and identity in (b) are both decomposed to the qubit level, representing two different connections for qubits in $A$ and $\bar{A}$.

under different constraints induced by the CZ and CCZ operations, respectively. This methodology is also applied to the variance of purity in Sec. IV.

The average purity of the state $\rho_A = \mathrm{Tr}_{\bar{A}}\Psi$ with $\Psi \in \mathcal{E}$ can be expressed by standard technique (e.g., Ref. [43]) as

$$\begin{aligned}\mathbb{E}_\Psi(P_A) &= \mathbb{E}_\Psi \mathrm{Tr}\big(T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ \Psi^{\otimes 2}\big)\\ &= \mathbb{E}_{U\in\mathcal{E}} \mathrm{Tr}\big(T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ U^{\otimes 2}\Psi_0^{\otimes 2}U^{\dagger\otimes 2}\big)\\ &= \mathrm{Tr}\big[T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ \mathbb{E}_{U\in\mathcal{E}}\big(U^{\otimes 2}\Psi_0^{\otimes 2}U^{\dagger\otimes 2}\big)\big]\\ &= \mathrm{Tr}\big[T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ \Phi_{\mathcal{E}}^2\big(\Psi_0^{\otimes 2}\big)\big]. \end{aligned} \tag{6}$$

Above, in the first line the purity is written as an observable on the two-copy Hilbert space $\mathcal{H}^{\otimes 2}$ and $T_A$ is the swap operator on $\mathcal{H}_A^{\otimes 2}$. The random state $\Psi$ is generated by random unitary $U$ on the initial state $\Psi_0$, and we still denote the unitary ensemble with $\mathcal{E}$ without ambiguity. In the third line of Eq. (6), due to the linearity, the order of trace and ensemble average are exchanged, and we denote the resulting two-copy twirling channel as $\Phi_{\mathcal{E}}^2$ in the final line. See Fig. 2(a) for an illustration.

To study the random hypergraph state, the initial state is taken as $|\Psi_0\rangle = |+\rangle^{\otimes N}$, with subsystem $A$ containing $N_A \leqslant N/2 \leqslant N_{\bar{A}}$ qubits without loss of generality. The evolution $U$ is sampled from CZ or CCZ ensembles defined in Sec. II B. Actually, one only needs to consider the gate between $A$ and $\bar{A}$, since the gate inside each subsystem commutes with $T_A$ and thus does not affect the purity.

### A. Tensor network representation

Here we introduce a tensor network representation to calculate the average purity. To make the tensor diagram concise, we take the quantum state $\rho$ and observable $O$ as *vectors* and the quantum channel $\Phi$ as a *matrix*. That is, in the form of $\langle\langle O|\Phi|\rho\rangle\rangle$. In our case, $O = T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}$, $\rho = |+\rangle\langle+|^{\otimes 2N}$, and $\Phi$ is the twirling channel $\Phi_{\mathcal{E}}^2$, as shown in the final line of Eq. (6). In particular, one has

$$\mathbb{E}_\Psi(P_A) = \mathbb{E}_{U\in\mathcal{E}}\langle\langle T_A|\ \otimes \big\langle\big\langle \mathbb{I}_{\bar{A}}^2\big|U\otimes U^*\otimes U\otimes U^*\ |\Psi_0\rangle^{\otimes 4}, \tag{7}$$

which is illustrated in Fig. 2(b). There are two different connections on the left, which correspond to the vector form of the operators $\langle\langle T_A|$ and $\langle\langle \mathbb{I}_{\bar{A}}^2|$ in Eq. (7), respectively. For the random hypergraph states here, the random unitary satisfies $U = U^*$ and the initial state $|\Psi_0\rangle$ is the real and product state. In Fig. 2(c), we further rearrange the total Hilbert space $\mathcal{H}^{\otimes 2}$ into $(\mathcal{H}_i^{\otimes 2})^{\otimes N}$, i.e., put the two-copy of the $i$th qubit Hilbert space $\mathcal{H}_i$ together. On the right, every qubit corresponds to four lines, each two for one-copy Hilbert space. In the middle, we operate the random $\mathrm{CZ}_e$ gate across $A$ and $\bar{A}$. Here we show case of a CZ gate, which repeats four times connecting the corresponding lines of the two-qubit in the tensor network. Note that the swap $T_A = \otimes_{i\in A} T_i$ and, of course, the identity operator $\mathbb{I}_{\bar{A}}^{\otimes 2}$ can be written in the product of each qubit operator. As a result, on the left, there are two different connections for each qubit determined by it belonging to $A$ or $\bar{A}$.

To calculate $\mathbb{E}_\Psi(P_A)$, one needs to contract the tensor network in Fig. 2(c) for all possible random $U$ and then average them. Note that in Fig. 2(c), the input vector $(|+\rangle^{\otimes 4})^{\otimes N}$ on the right can take all the possible 0/1 bit values with a normalization constant:

$$\mathcal{N} = \left(\frac{1}{\sqrt{2}}\right)^{4N} = d^{-2}. \tag{8}$$

The unitary in the middle is composed of $\mathrm{CZ}_e$ gates which only introduce $\pm 1$ phase for any computational basis input. By averaging these random unitaries, some bit strings may be canceled out by taking $-1$ and 1 for different unitaries. As a result, to find the final average purity, one only needs to count the number of bit strings which survive on the average effect of all possible gate operations. The following proposition can simplify the counting procedure by observing that the twirling channel in the middle can be decomposed *locally*, since the gate operations on distinct edges are *independent*.

*Proposition 1.* Consider a $t$-fold twirling channel $\Phi_{\mathcal{E}}^t(\cdot) := \mathbb{E}_{U\in\mathcal{E}} U^{\otimes t}(\cdot)U^{\dagger\otimes t}$, with random unitary $U = U_{e_L}\cdots U_{e_2}U_{e_1}$, where each $U_{e_i}$ is sampled independently from the local ensemble on the Hilbert space $\mathcal{H}_{e_i}$. $\Phi_{\mathcal{E}}^t(\cdot)$ can be decomposed into the channel multiplication of the corresponding local twirling channels,

$$\Phi_{\mathcal{E}}^t = \Phi_{\mathcal{E}_{e_L}}^t \circ \Phi_{\mathcal{E}_{e_{L-1}}}^t \cdots \circ \Phi_{\mathcal{E}_{e_2}}^t \circ \Phi_{\mathcal{E}_{e_1}}^t, \tag{9}$$

where $\mathcal{E}_{e_i}$ denotes the random unitary ensemble acting nontrivially on $\mathcal{H}_{e_i}$.

*Proof.* We prove it by using the matrix form of the twirling channel $\tilde{\Phi}_{\mathcal{E}}^t = \mathbb{E}_{U\in\mathcal{E}} U^{\otimes t}\otimes U^{*\otimes t}$, where the tilde denotes the matrix form, which is also called the tensor product expander [44,45]. In this way, the composition of channel can

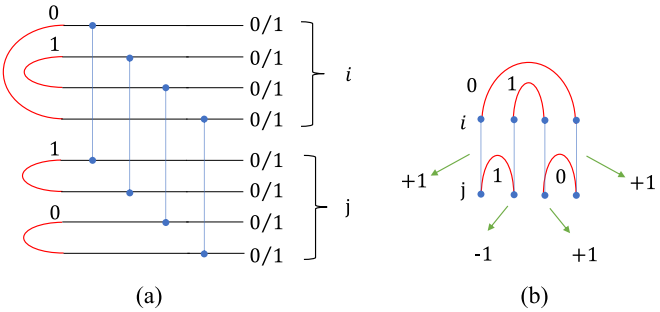



FIG. 3. (a) Tensor network for the two-qubit CZ operation. On the right, there are all possible 0/1 inputs of all black lines. As black lines associated to the same red arc should take the same bit value, one only needs to use the two-bit of the red arcs to denote each qubit, and here we show case for {01, 10}. (b) We rotate (a) 90° for clearness and also omit the nonessential black lines. The qubits $i$ and $j$ are labeled by the the upper and lower two red arcs, with every arc taking 0/1 value. The overall phase is determined by the phase accumulation of all four CZ gates. For the {01, 10} case here, the overall phase is $-1 = (+1) * (-1) * (+1) * (+1)$.

be taken as the multiplication of the matrix,

$$\begin{aligned}\tilde{\Phi}^t_{\mathcal{E}} &= \mathbb{E}_{U=U_{e_L}\cdots U_{e_2}U_{e_1}}\left[U_{e_L}\cdots U_{e_2}U_{e_1}\right]^{\otimes t}\otimes\left[U_{e_L}\cdots U_{e_2}U_{e_1}\right]^{*\otimes t}\\ &= \left[\mathbb{E}_{U_{e_L}\in\mathcal{E}_{e_L}}U_{e_L}^{\otimes t}\otimes U_{e_L}^{*\otimes t}\right]\cdots\left[\mathbb{E}_{U_{e_1}\in\mathcal{E}_{e_1}}U_{e_1}^{\otimes t}\otimes U_{e_1}^{*\otimes t}\right]\\ &= \tilde{\Phi}_{\mathcal{E}^t_{e_L}}\cdots\tilde{\Phi}_{\mathcal{E}^t_{e_2}}\cdot\tilde{\Phi}_{\mathcal{E}^t_{e_1}},\end{aligned} \tag{10}$$

where the second line we use the independence of each unitary ensemble $\mathcal{E}_{e_i}$, then we translate this back to the channel form and get Eq. (9). ■

Proposition 1 is general and suitable for any kind of random unitary ensemble. For our random $\mathrm{CZ}_e$ ensemble in Definition 1, each $e_i$ denotes a specific edge, and $U_{e_i} \in \{\mathbb{I}_{e_i}, \mathrm{CZ}_{e_i}\}$ acting nontrivially on $\mathcal{H}_{e_i}$ with 1/2 probability, which gives the local twirling channel $\Phi^t_{\mathcal{E}_{e_i}}$. Note that the phase gates commute with each other, and thus the order of the decomposition in Eq. (9) does not matter.

### B. Average purity of CZ ensemble

Equipped with the tensor network diagram, we are in the position to calculate the average purity for CZ ensemble. To facilitate the counting procedure, we should first figure out what happens locally, say the twirling channel $\Phi^2_{\mathcal{E}_e}$ on a specific edge $e = \{i, j\}$.

First, for simplicity, let us consider a two-qubit example and then extend to $N$-qubit later. Suppose the qubit $i$ is in $A$ and $j$ is in $\bar{A}$, as shown in Fig. 3(a). Remember that the input state $|+\rangle$ on the right induces no constraint, i.e., every black line can take 0/1 value by ignoring the normalization $\mathcal{N}$, thus every qubit can be denoted by four *classical* bits. Moreover, since the red tensors on the left connect the ends of the black lines, they induce constraints on the bit values. To be specific, any two black lines should take the same bit value if they are connected to the same red arc. Otherwise, it will return zero in the tensor contraction, and thus does not contribute to the summation, no matter what kind of gate operations in the middle. In other words, the bit values of a qubit can be reduced to that of the red arcs and, consequently, one can use the red arcs on the left to label the qubit and only needs to associate a two-bit to each qubit. Figure 3(a) shows the case for {01, 10}. In Fig. 3(b), for the simplicity of the following discussion, we rotate the diagram 90°and omit the nonessential black lines. The CZ gate on the two-qubit can introduce a phase, depending on the value of the classical bits of the red arcs. To be specific, if both red arcs on the two ends of the CZ gate take the value 1, it will give a $-1$ phase, otherwise the phase is 1, and the final phase is determined by multiplication of all phases from the four CZ gates. For the {01, 10} case, the overall phase is $-1$, as shown in Fig. 3(b). We list all possible cases as follows:

$$M_p = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}, \tag{11}$$

and denote it as the *phase* matrix, where the row and column indexes are the two-bits of the two qubits, respectively. The phase matrix is symmetric between the two qubits, also invariant under permutation of the two-bit for the the row or column, and these properties are also reflected in the diagram of Fig. 3(b).

On the other hand, if there is no gate operation, the phase matrix is just the trivial one:

$$J_4 = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}. \tag{12}$$

After taking the average for both cases, the final matrix is the summation of them with 1/2 probability as

$$M_s = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}, \tag{13}$$

denoted as the *summation* matrix.

$M_s$ in some sense can be regarded as a matrix representation of the local twirling channel $\Phi^2_{\mathcal{E}_e}$, and we elaborate this point in Appendix A. In the remainder of the paper, we will adopt this summation matrix formalism to calculate the average purity and its variance.

The matrix $M_s$ in Eq. (13) indicates that only a few bit configurations survive under the effect of the local twirling channel $\Phi^2_{\mathcal{E}_e}$. For instance, the configuration {00, 11} survives but the configuration {01, 10} vanishes. To figure the average purity in this minimal $N = 2$ case, one only needs to count the number of 1s in Eq. (13), i.e., 12, and normalize it with $\mathcal{N} = 1/16$ in Eq. (8) to get 3/4. This is consistent with the direct calculation: there is 1/2 probability to prepare a product state with purity 1 on $A$ and the other 1/2 probability to prepare the Bell state with purity 1/2, which totally returns the average $(1 + 1/2)/2 = 3/4$.

This counting argument can be extended to a general $N$-qubit system by virtue of Proposition 1. We still use two-bit to denote one qubit and our task is to count the total number of bit strings which survive under all possible local twirling channels $\Phi^2_{\mathcal{E}_e}$. Since there is $\Phi^2_{\mathcal{E}_e}$ between any pair of qubits, we just need to move the summation matrix $M_s$ in Eq. (13) on all two-qubits between $A$ and $\bar{A}$. For example, if the two-qubit say $i$, $j$ with $i \in A$ and $j \in \bar{A}$, take the bit configuration such as $\{01, 10\}$, no matter what values of other qubits are, this kind of bit string $\{\cdots 01_{\{i\}}, 10_{\{j\}} \cdots\}$ will vanish and not contribute to the final result.

Note that the matrix elements just depend on the parity information—one can simplify it further by using logical bit $\bar{0} = 00, 11$ and $\bar{1} = 01, 10$ to encode such that

$$M_s = \begin{array}{c} \\ \bar{0} \\ \bar{1} \end{array} \begin{array}{c} \begin{array}{cc} \bar{0} & \bar{1} \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \tag{14}$$

and the phase matrix shows

$$M_p = \begin{array}{c} \\ \bar{0} \\ \bar{1} \end{array} \begin{array}{c} \begin{array}{cc} \bar{0} & \bar{1} \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}. \tag{15}$$

Now every qubit is labeled by *one* classical bit and we utilize $M_s$ to constrain the bit value of any qubit pair in $A$ and $\bar{A}$. From matrix $M_s$, one sees that $\bar{1}$ is not allowed in $A$ and $\bar{A}$ simultaneously. That is, all qubits in $A$ take $\bar{0}$ and those in $\bar{A}$ are arbitrary or vice versa. Consequently, the total number of surviving bit strings for the random CZ scenario is

$$\text{No.}_{\text{CZ}} = (2^{N_A} + 2^{N_{\bar{A}}} - 1)2^N. \tag{16}$$

Here $-1$ accounts for deleting the double counting of the all $\bar{0}$ case; the multiplication $2^N$ is due to the redundancy of the logical encoding. The average purity is obtained by multiplying $\text{No.}_{\text{CZ}}$ with the normalization $\mathcal{N}$ in Eq. (8).

*Theorem 1.* The average purity of the subsystem $A$ with $N_A$ qubits for the random graph states from the CZ ensemble is

$$\langle P_A \rangle_{\text{CZ}} = \frac{d_A + d_{\bar{A}} - 1}{d}, \tag{17}$$

where $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of the subsystem $A(\bar{A})$. For the case of equal partition $d_A = d_{\bar{A}} = \sqrt{d}$, one has $\langle P_A \rangle_{\text{CZ}} = (2\sqrt{d} - 1)/d \sim 2/\sqrt{d}$.

### C. Average purity of CCZ ensemble

Now we move to the scenario of random CCZ hypergraph states. Similar to the CZ scenario in Sec. III B, we still use two classical bits to denote one qubit, and count the number of the surviving bit strings.

First, we should figure out what happens locally, say the corresponding summation matrix $M_s$ caused by the local twirling channel $\Phi^2_{\mathcal{E}_e}$. The only difference compared with the CZ scenario is that CCZ involves three qubits $i$, $j$, $k$, and thus the corresponding phase matrix $M_p$ is actually a *three-index tensor* $M^p_{ijk}$, and we denote the trivial all-one tensor without gate operation as $J_{ijk}$, as shown in Figs. 4(a) and 4(b). The summation tensor is their average:

$$M^s_{ijk} = \tfrac{1}{2}\left(M^p_{ijk} + J_{ijk}\right). \tag{18}$$

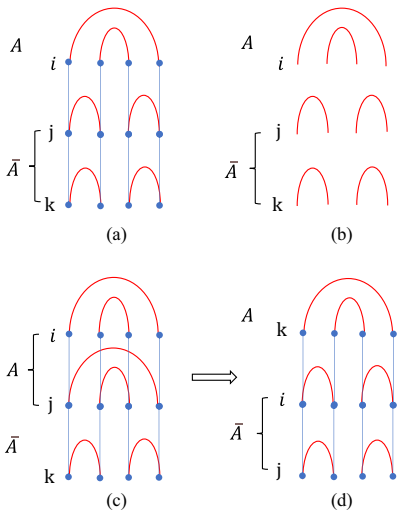



FIG. 4. Phase matrix (three-index tensor) for the CCZ scenario. For (a) and (b), qubit $i$ is in $A$, the other two qubits $j, k$ are in $\bar{A}$. (a) is the phase tensor $M^p_{ijk}$ when operating the CCZ gate and (b) is the trivial all-one tensor $J_{ijk}$ without gate operation. The summation tensor $M^s_{ijk}$ is the average of both. (c) is the phase tensor $\tilde{M}^p_{ijk}$ for the case of $i, j \in A, k \in \bar{A}$, which is different from $M^p_{ijk}$ due to the shape of the red tensors. But it can be deformed to $M^p_{kij}$ in (d) without changing the topology.

Suppose qubit $i \in A$, and the other two qubits $j, k \in \bar{A}$ for the case in Fig. 4(a), we can write $M^p_{ijk}$ by fixing the bit value of $i$. If qubit $i$ takes the logical $\bar{0}$, denoted by $\mathbf{i} = \bar{0}$ with the bold font, the matrix between $j$ and $k$ is the trivial 4×4 all-one matrix $J_4 = J_2^{\otimes 2}$ in Figs. 5(a) and 5(b). In this case, the

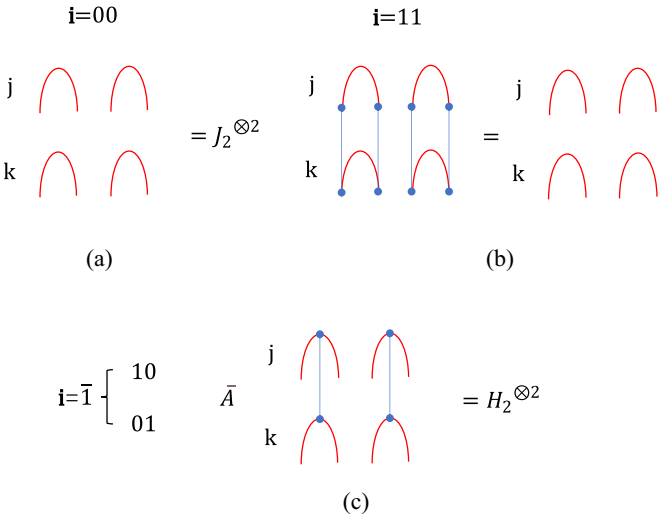
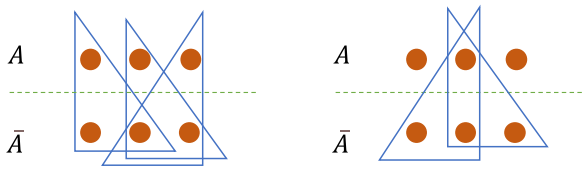



FIG. 5. Phase tensor $M^p_{ijk}$ in Fig. 4(a) for different classical bit values of qubit $i$. (a) For $\mathbf{i} = 00$, the blue CCZ gate can not introduce phase on the $j, k$ qubits, and thus the matrix between $j, k$ is $J_2^{\otimes 2}$. (b) For $\mathbf{i} = 11$, the CCZ gates reduce to CZ gates on $j, k$. However, the nearby two CZ gates cancel with each other and lead also to $J_2^{\otimes 2}$. (c) For $\mathbf{i} = 01, 10$, there is only one CZ gate on a pair of red arcs, and the corresponding matrix form is $H_2^{\otimes 2}$.




(a) (b)

FIG. 6. An illustration for the *half* CCZ ensemble. In an $N = 6$-qubit system, subsystem $A$ and $\bar{A}$ both contain $N_A = N_{\bar{A}} = 3$ qubits. For every three-qubit $i \in A$, $j, k \in \bar{A}$, we could operate a CCZ on them or not with $1/2$ probability. In this way, there are $N_A * C^2_{N_{\bar{A}}}$ possible gate patterns with equal probability. In (a) and (b), we show two examples for the gate pattern.

summation tensor is

$$M^s_{ijk} = |\mathbf{i}\rangle\langle\mathbf{i}| \otimes \tfrac{1}{2}(J_4 + J_4) = |\mathbf{i}\rangle\langle\mathbf{i}| \otimes J_4. \tag{19}$$

with $\mathbf{i} = 00, 11$ and Dirac notation is adopted to write the tensor.

If qubit $\mathbf{i} = \bar{1}$, the matrix between $j, k$ is $H_2^{\otimes 2}$ in Fig. 4(c), with $H_2$ being the $2\times2$ Hadamard matrix *without* normalization constant $1/\sqrt{2}$ hereafter. And the resulting summation tensor is

$$\begin{aligned} M^s_{ijk} &= |\mathbf{i}\rangle\langle\mathbf{i}| \otimes 1/2\left(H_2^{\otimes 2} + J_2^{\otimes 2}\right), \\ &= |\mathbf{i}\rangle\langle\mathbf{i}| \otimes \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}, \\ &:= |\mathbf{i}\rangle\langle\mathbf{i}| \otimes M^s_i \end{aligned} \tag{20}$$

for $\mathbf{i} = 01, 10$, and we denote the matrix between $j, k$ with a fixed $\mathbf{i}$ as $M^s_i$.

For simplicity of discussion, in the following we first consider a subensemble with random CCZ gates defined as follows. For every three-qubit $i \in A$, $j, k \in \bar{A}$, we operate a CCZ on them or not with probability $1/2$, and the whole ensemble is composed of these local ones, similar to Definition 1. This ensemble is different from the original random CCZ ensemble, where $\mathrm{CCZ}_{ijk}$ with $i, j \in A, k \in \bar{A}$ is also allowed, and thus we call it a *half* CCZ ensemble. See Fig. 6 for an illustration.

Similar to the CZ scenario, we will count the number of survival bit strings of this half ensemble to calculate the average purity, with constraints from Eqs. (19) and (20). By Eq. (19), it is not hard to see that as $\mathbf{i} = \bar{0}$, actually there is no constraint on $j, k$; by Eqs. (20), as $\mathbf{i} = \bar{1}$, some values of $j, k$ would vanish, shown as the zero elements in the matrix $M^s_i$.

First, if $\forall i \in A, \mathbf{i} = \bar{0}$, $j \in \bar{A}$ can take any value, totally $1 * 4^{N_{\bar{A}}} * 2^{N_A}$, where $2^{N_A}$ is the logical encoding abundance. Second, if there exists $\mathbf{i} = \bar{1} \in A$, there are three possibilities for $j \in \bar{A}$.

(1) $j$ only takes 00 or 11, totally $2^{N_{\bar{A}}}$.

(2) There exists one $\mathbf{j} = 01$ or 10 and the remaining $k \in \bar{A}$ can just be 00, totally $2C^1_{N_{\bar{A}}} = 2N_{\bar{A}}$.

(3) There exists one $\mathbf{j} = 01$ and one $\mathbf{k} = 10$, and the remaining qubits can just be 00, totally $2C^2_{N_{\bar{A}}} = N_{\bar{A}}(N_{\bar{A}} - 1)$.

As a result, the average purity of this half ensemble is obtained by summing the number of survival bit strings in all the above cases and multiplying the normalization in Eq. (8),

$$\begin{aligned} \langle P_A\rangle_{\mathrm{CCZ},h} &= 2^{N_A}\frac{4^{N_{\bar{A}}} + (2^{N_A} - 1)[2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}} + 1)]}{4^N} \\ &= \frac{d_A + d_{\bar{A}} - 1}{d} + \frac{d_A(d_A - 1)N_{\bar{A}}(N_{\bar{A}} + 1)}{d^2}, \end{aligned} \tag{21}$$

where the front $2^{N_A}$ is for the logical encoding abundance of the qubit in $A$. In the case of equal partition $N_A = N_{\bar{A}} = N/2$, it shows $\langle P_A\rangle_{\mathrm{CCZ},h} \sim 2/\sqrt{d} + O(N^2/d)$.

Finally, we look into the original full CCZ ensemble. Like before, we should additionally figure out the phase tensor for the case $i, j \in A$, and $k \in \bar{A}$. By the symmetry, the new tensor is almost the same to the original one. One has the relation of the phase tensor $\tilde{M}^p_{ijk} = M^p_{kij}$ by deforming the tensor in Fig. 4(c) to the one in Fig. 4(d), so does the summation tensor. As a result, the additional gate will induce more constraints on the bit string, which leads to the *decrease* of the average purity.

Actually, only the last two cases 2 and 3 listed before change. When there is $k \in \bar{A}$ taking 01 or 10, that is, $\mathbf{k} = \bar{1}$, we can use the summation tensor $\tilde{M}^s_{ijk} = M^s_{kij}$ in Eqs. (20) to constraint the bit value of qubits back in $A$. Since the case of $\forall i \in A, \mathbf{i} = \bar{0}$ has already been counted, one needs to figure out the case that $\exists i \in A, \mathbf{i} = \bar{1}$. Following the same counting procedure in cases 2 and 3, one can find that there are $N_A(N_A + 1)$ choices for $A$. By summing the numbers of all these possibilities, one has the result of average purity as follows.

*Theorem 2.* The average purity of subsystem $A$ with $N_A$ qubits for the random hypergraph states from the CCZ ensemble is

$$\langle P_A\rangle_{\mathrm{CCZ}} = \frac{d_A + d_{\bar{A}} - 1}{d} + \frac{N_A(N_A + 1)N_{\bar{A}}(N_{\bar{A}} + 1)}{d^2}, \tag{22}$$

where $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of subsystem $A(\bar{A})$. For the case of equal partition $d_A = d_{\bar{A}} = \sqrt{d}$, one has $\langle P_A\rangle_{\mathrm{CCZ}} = 2/\sqrt{d} - 1/d + O(N^4/d^2)$.

At the end of this section, we remark that the average purity results of CZ and CCZ ensembles obtained here are almost equal to that of Haar random states [46,47], i.e.,

$$\langle P_A\rangle_{\mathrm{Haar}} = \frac{d_A + d_{\bar{A}}}{d + 1}, \tag{23}$$

and any state ensemble satisfies projective two-design, such as the orbit of Clifford group [22,48]. Actually, the CZ and CCZ ensemble are *not* projective two-design, even approximately [49,50].

## IV. FLUCTUATIONS OF THE PURITY

In Sec. III, one sees that the average subsystem purities of random CZ and CCZ ensembles share the same leading term. In this section, we find that the variances of the purity of the two ensembles are quite different:

$$\delta^2(P_A) = \mathbb{E}_\Psi\left(P_A^2\right) - [\mathbb{E}_\Psi(P_A)]^2.$$

The essential quantity one needs to figure out is the first term $\mathbb{E}_\Psi(P_A^2)$. Similar to Eq. (6) for the average purity, it can be written on the four-copy Hilbert space $\mathcal{H}^{\otimes 4}$ as

$$\begin{aligned}\mathbb{E}_\Psi\left(P_A^2\right) &= \mathbb{E}_\Psi\left[\mathrm{Tr}\left(T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ \Psi^{\otimes 2}\right)\right]^2 \\ &= \mathbb{E}_{U\in\mathcal{E}}\ \mathrm{Tr}\left[T_A^{(1,2)} \otimes T_A^{(3,4)} \otimes \mathbb{I}_{\bar{A}}^{\otimes 4}\ U^{\otimes 4}\Psi_0^{\otimes 4}U^{\dagger\otimes 4}\right] \\ &= \mathrm{Tr}\left[T_A^{(1,2)} \otimes T_A^{(3,4)} \otimes \mathbb{I}_{\bar{A}}^{\otimes 4}\ \Phi_{\mathcal{E}}^4\left(\Psi_0^{\otimes 2}\right)\right]. \end{aligned} \tag{24}$$

Here we can still vectorize Eq. (24) in the form of $\langle\langle O|\tilde{\Phi}|\rho\rangle\rangle$ as in Eq. (7). $O = T_A^{(1,2)} \otimes T_A^{(3,4)} \otimes \mathbb{I}_{\bar{A}}^{\otimes 4}$, $\rho = |+\rangle\langle+|^{\otimes 4N}$, and $\Phi$ is the four-copy twirling channel $\Phi_{\mathcal{E}}^4$, whose matrix form shows

$$\tilde{\Phi}_{\mathcal{E}}^4 = (U \otimes U^*)^{\otimes 4} = U^{\otimes 8}, \tag{25}$$

with the fact that $U = U^*$ for phase gates. One can draw the corresponding diagram by *doubling* Fig. 2(b).

Similar to the average purity in Fig. 2(c), we still apply the tensor network representation to calculate the expectation value here. We arrange the total Hilbert space $\mathcal{H}^{\otimes 4}$ as $(\mathcal{H}_i^{\otimes 4})^{\otimes N}$, i.e., put the two-copy of the $i$th qubit Hilbert space $\mathcal{H}_i$ together in Fig. 7(a). On the right, every qubit corresponds to eight lines, each two for one-copy Hilbert space. In the middle, we operate the random $\mathrm{CZ}_e$ gate across $A$ and $\bar{A}$. Here we show the case of a CZ gate, which repeats eight times by Eq. (25), connecting the corresponding lines of the two-qubit in the tensor network. On the left, by decomposing the swap $T_A^{(1,2)} \otimes T_A^{(3,4)}$ and the identity $\mathbb{I}_{\bar{A}}^{\otimes 4}$ to the qubit level, there are two different connections for each qubit determined by it belonging to $A$ or $\bar{A}$.

To calculate $\mathbb{E}_\Psi(P_A^2)$, one needs to contract the tensor network in Fig. 7(a) under the average effect of the random $U$. Note that the input vector $(|+\rangle^{\otimes 8})^{\otimes N}$ on the right of Fig. 7(a) can take all the possible 0/1 bit values with a normalization constant:

$$\mathcal{N}_v = \left(\frac{1}{\sqrt{2}}\right)^{8N} = d^{-4}. \tag{26}$$

Similar to the average purity scenario, one needs to count the number of bit strings which survive under the twirling channel $\Phi_{\mathcal{E}}^4$, which can also be decomposed locally by Proposition 1. In fact, like Fig. 3(a), one can associate four classical bits to one qubit due to the connections on the left in Fig. 7(a), and we still apply the phase and summation matrix (tensor) to describe the local twirling channel $\Phi_{\mathcal{E}_e}^4$ on edge $e$.

### A. Variance of purity for CZ ensemble

Similar to the average purity scenario in Sec. III B, we should first figure out what happens locally, say the summation matrix for the twirling channel $\Phi_{\mathcal{E}_e}^4$. Considering $e = \{i, j\}$ with $i \in A$, $j \in \bar{A}$, each qubit is labeled by the four-bit shown in Fig. 7(b), where one can directly see that the phase matrix is just the tensor product of the one in Fig. 3(b). By applying the logical encoding as in Eq. (15), each qubit can be labeled by a two-bit, and the phase matrix here

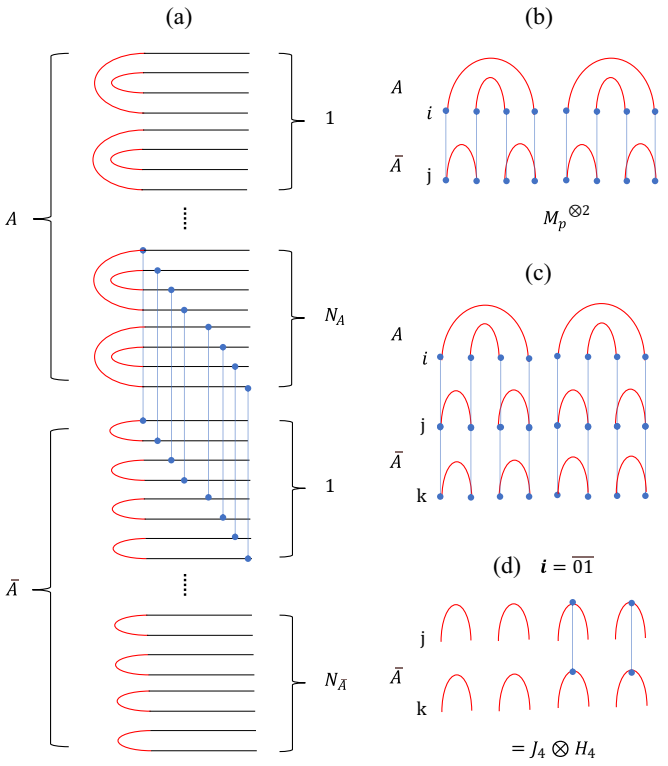



FIG. 7. Tensor network for the purity variance formula and the phase tensors. (a) We rearrange Eq. (24) in the current tensor network form. On the right, every qubit corresponds to eight lines, each two for one-copy Hilbert space. Every line can take one bit 0/1 value. In the middle, we can operate CZ or CCZ across $A$ and $\bar{A}$ in this double Hibert space. Here we show explicitly the CZ between the last qubit in $A$ and the first qubit in $\bar{A}$. On the left, there are two kinds of boundary operators corresponding to swap and identity on the qubit Hilbert space $\mathcal{H}_i^{\otimes 4}$, depending on whether qubit $i$ is in $A$ or $\bar{A}$. (b) The phase matrix for the CZ gate, which is the two-copy tensor product of the one in Fig. 3(b) for the average purity scenario. (c) The phase tensor for the CCZ gate with qubit $i$ in A and $j,k$ in $\bar{A}$, which is the tensor product of the one in Fig. 4(a). (d) The effective matrix on $j, k$ depends on the value of $i$. For example, if $i$ takes $\bar{0}\bar{1}$, the matrix on $j,k$ is $J_4 \otimes H_4$ shown in Eq. (33).

shows

$$M_p' = M_p^{\otimes 2} = \begin{array}{c} \\ \bar{0}\bar{0} \\ \bar{0}\bar{1} \\ \bar{1}\bar{0} \\ \bar{1}\bar{1} \end{array} \begin{array}{c} \begin{array}{cccc} \bar{0}\bar{0} & \bar{0}\bar{1} & \bar{1}\bar{0} & \bar{1}\bar{1} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array}. \tag{27}$$

The summation matrix is obtained by average $M_p'$ with the all-one matrix

$$M_s' = \begin{array}{c} \\ \bar{0}\bar{0} \\ \bar{0}\bar{1} \\ \bar{1}\bar{0} \\ \bar{1}\bar{1} \end{array} \begin{array}{c} \begin{array}{cccc} \bar{0}\bar{0} & \bar{0}\bar{1} & \bar{1}\bar{0} & \bar{1}\bar{1} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}. \tag{28}$$

$M'_s$ shows the constraint on the classical bit configurations of the qubits in $A$ and $\bar{A}$. Like Sec. III B, we list all the surviving possibilities on the logical encoding level as follows.

(1) $A$ only contains $\bar{0}\bar{0}$, and there is no constraint on the bit value of qubits in $\bar{A}$, and vice versa, totally $4^{N_A} + 4^{N_{\bar{A}}} - 1$.

(2) only $\bar{0}\bar{0}$ and $\bar{1}\bar{1}$ appear in both $A$ and $\bar{A}$, totally $(2^{N_A} - 1)(2^{N_{\bar{A}}} - 1)$.

(3) $A$ contains $\bar{0}\bar{1}$ and $\bar{0}\bar{0}$, and $\bar{A}$ contains $\bar{1}\bar{0}$ and $\bar{0}\bar{0}$, and vice versa, totally $2(2^{N_A} - 1)(2^{N_{\bar{A}}} - 1)$.

As a result, by summing the number of the possible bit strings and normalizing the constant in Eq. (26), one has

$$\langle P_A^2 \rangle_{\mathrm{CZ}} = \frac{4^N[4^{N_A} + 4^{N_{\bar{A}}} - 1 + 3(2^{N_A} - 1)(2^{N_{\bar{A}}} - 1)]}{4^{2N}} = \frac{d_A^2 + d_{\bar{A}}^2 - 1 + 3(d_A - 1)(d_{\bar{A}} - 1)}{d^2}. \tag{29}$$

Here $4^N$ multiplication is due to the logical encoding redundancy. For example, $\bar{0}\bar{0}$ encoding for a qubit can correspond to four possibilities. As a result, by combing the average purity result in Eq. (17), the variance shows as follows.

*Theorem 3.* For a subsystem $A$ with $N_A$ qubits, the variance of the purity $P_A$ defined in Eqs. (5) for the random graph states from the CZ ensemble is

$$\delta^2_{\mathrm{CZ}}(P_A) = \frac{(d_A - 1)(d_{\bar{A}} - 1)}{d^2}, \tag{30}$$

where $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of the subsystem $A(\bar{A})$. For the case of equal partition $d_A = d_{\bar{A}} = \sqrt{d}$, one has $\delta^2_{\mathrm{CZ}}(P_A) = d^{-1} - 2d^{-\frac{3}{2}} + d^{-2}$.

We remark that the variance of the subsystem purity of the CZ ensemble is similar to that of random stabilizer states [51], which scales as $d^{-1}$ for the equal partition.

To get the above variance, one subtracts $[\mathbb{E}_\Psi(P_A)]^2$ from $\mathbb{E}_\Psi(P_A^2)$ in Eq. (29). Actually one is only left with the bit strings in case 2, and the bit strings in cases 1 and 3 also survive in the formula of $[\mathbb{E}_\Psi(P_A)]^2$. The reason is as follows. For qubit $i$, it can be denoted by two logical bits $\mathbf{i_1 i_2}$, and the constraint from $M'_p$ in Eq. (27) on any qubit-pair $i$ and $j$ reads

$$\langle \mathbf{i_1}| M_p |\mathbf{j_1}\rangle * \langle \mathbf{i_2}| M_p |\mathbf{j_2}\rangle = 1. \tag{31}$$

On the other hand, the constraint of $[\mathbb{E}_\Psi(P_A)]^2$ for the two logical bits are independent, say $\langle \mathbf{i_1}| M_p |\mathbf{j_1}\rangle = 1$ *and* $\langle \mathbf{i_2}| M_p |\mathbf{j_2}\rangle = 1$. As a result, the difference is the case where there exist two qubits $i, j$ such that the two terms both take $-1$, which is just case 2. This phenomena is general and also applicable to the CCZ scenario, and we illustrate it in detail in Appendix B.

### B. Variance of purity for CCZ ensemble

Similar to the average purity scenario in Sec. III C, we first figure out the local phase and summation tensors. Considering three qubits $i \in A$ and $j, k \in \bar{A}$, as shown in Fig. 7(c), each qubit is labeled by four-bit. It is clear that the phase tensor is the tensor-product of the one in the average purity scenario in Fig. 4(a),

$$M'^p_{ijk} = M^p_{i_1 j_1 k_1} \otimes M^p_{i_2 j_2 k_2}, \tag{32}$$

with $i = \{i_1 i_2\}$ and $i_1, i_2$ both taking two-bit values, same for $k$ and $j$.

By using the logical encoding as in Sec. III C, $i_1$ and $i_2$ of qubit $i$ can be both labeled by one logical bit of $\bar{0}, \bar{1}$. Depending on the status of $i$, the matrix between $j$ and $k$ shows

$$\mathbf{i} = \bar{0}\bar{0}, \quad J_4 \otimes J_4 = J_{16}, \quad \mathbf{i} = \bar{0}\bar{1}, \quad J_4 \otimes H_4,$$
$$\mathbf{i} = \bar{1}\bar{0}, \quad H_4 \otimes J_4, \quad \mathbf{i} = \bar{1}\bar{1}, \quad H_4 \otimes H_4 = H_{16}, \tag{33}$$

where $J_4$ denotes the trivial all-ones $4\times4$ matrix, and $H_4 = H_2^{\otimes 2}$. See Fig. 7(d) for the illustration of the second case $\mathbf{i} = \bar{0}\bar{1}$.

The summation tensor is obtained by averaging $M'^p_{ijk}$ with the trivial all-one tensor $J_{ijk}$. For a fixed $\mathbf{i}$, say $\mathbf{i} = \bar{0}\bar{1}$, the matrix between $j, k$ shows

$$M'^s_i = \tfrac{1}{2}(J_4 \otimes H_4 + J_{16}) = J_4 \otimes \tfrac{1}{2}(H_4 + J_4) = J_4 \otimes M^s_i, \tag{34}$$

where the explicit form of $M^s_i$ is given in Eqs. (20). Similarly, $M'^s_i$ for different $\mathbf{i}$ is obtained by averaging every matrix in Eqs. (33) with $J_{16}$, and they show, respectively,

$$\mathbf{i} = \bar{0}\bar{0}, \quad M'^s_i = J_{16}, \tag{35}$$

$$\mathbf{i} = \bar{0}\bar{1}, \quad M'^s_i = J_4 \otimes M^s_i, \tag{36}$$

$$\mathbf{i} = \bar{1}\bar{0}, \quad M'^s_i = M^s_i \otimes J_4, \tag{37}$$

$$\mathbf{i} = \bar{1}\bar{1}, \quad M'^s_i = \tfrac{1}{2}(H_{16} + J_{16}). \tag{38}$$

In the following, as in the average purity scenario in Sec. III C, we first count the survival bit string for the half ensemble of CCZ gates, say any $\mathrm{CCZ}_{\{ijk\}}$ gate with $i \in A$, $j, k \in \bar{A}$, with the help of the summation tensor in Eqs. (35) to (38), and extend to the full ensemble later. There are several possible cases listed as follows.

(1) $A$ only contains $\bar{0}\bar{0}$, $\bar{A}$ can be arbitrary by Eq. (35), totally $16^{N_{\bar{A}}}$.

(2) $A$ only contains $\bar{0}\bar{0}$ and $\bar{0}\bar{1}$. Due to Eq. (36), the first two-bit of qubit in $\bar{A}$ can be arbitrary, and the last two should be restricted by $M^s_i$ in Eqs. (20). Totally,

$$(2^{N_A} - 1)4^{N_{\bar{A}}}[2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}} + 1)].$$

Here $(2^{N_A} - 1)$ counts the possibility for $A$. $4^{N_{\bar{A}}}$ counts the possibility for the first two-bit of the qubit in $\bar{A}$. $[2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}} + 1)]$ accounts for the possibility for the last two-bit of qubits in $\bar{A}$, which follows similarly by summing cases 1 to 3 in Sec. III C. Same result holds for $A$ only containing $\bar{0}\bar{0}$ and $\bar{1}\bar{0}$.

(3) $A$ contains at least two types from $\{\bar{0}\bar{1}, \bar{1}\bar{0}, \bar{1}\bar{1}\}$. For the qubit in $\bar{A}$, both the first two-bit and last two-bit are restricted. For example, suppose $A$ has $\bar{0}\bar{1}$ and $\bar{1}\bar{1}$, the constraint follows Eqs. (36) and (38). Consider two qubits $j, k \in \bar{A}$, the constraint on the classical four-bit values is actually

$$\langle \mathbf{j_1}| H_4 |\mathbf{k_1}\rangle = 1, \quad \langle \mathbf{j_2}| H_4 |\mathbf{k_2}\rangle = 1, \tag{39}$$

with $\mathbf{j_1}, \mathbf{j_2}$ denoting the first and last two-bits of qubit $j$, similar for $k$. Note that the constraints are *independent* on $\mathbf{j_1}$ and $\mathbf{j_2}$. Totally,

$$[4^{N_A} - 3(2^{N_A} - 1) - 1][2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}} + 1)]^2$$

where the first braket counts the possibility for $A$, and the second for $\bar{A}$ follows a similar argument as in case 2. We count the possibility for the first and lat two-bit independently and thus there is a square.

(4) $A$ contains $\bar{0}0$ and $\bar{1}1$. For the qubit in $\bar{A}$, both the first and last two-bit are restricted. Now the bit values of qubits $j, k \in \bar{A}$ is constrained *jointly* by Eq. (38). That is,

$$\langle \mathbf{j_1}| H_4 |\mathbf{k_1}\rangle * \langle \mathbf{j_2}| H_4 |\mathbf{k_2}\rangle = 1, \tag{40}$$

compared with Eqs. (39) in case 3. We count this case explicitly as follows in Lemma 1.

Denote the four-bit of the two-qubit $j, k$ as $\{a_t\}$ and $\{b_t\}$ with $t = 1, 2, 3, 4$. The constraint in Eq. (40) is actually

$$\prod_t \langle a_t| H_2 |b_t\rangle = \prod_t (-1)^{a_t b_t} = (-1)^{\sum_t a_t b_t} = 1 \tag{41}$$

or, equivalently, the binary vectors $\vec{a}$ and $\vec{b}$ are orthogonal on the binary filed. If we denote the number of bit configurations satisfy this condition as No. 4, one has the following result of it, with the proof in Appendix C.

*Lemma 1.* Suppose there are $m$ distinct positions, one assigns four-bit vector $\vec{v}_i \in \mathbb{F}_2^4$ to each of them $1 \leqslant i \leqslant m$, with the constraint

$$\vec{v}_i \cdot \vec{v}_j = 0 \text{ Mod}(2), \forall i \neq j.$$

The number of all possible assignments is

$$\text{No.}_4 = 3 * 4^{\text{m}} + \Theta(\text{m}^2)2^{\text{m}} + \Theta(\text{m}^4) \tag{42}$$

for large $m$.

As a result, by summing all the possibilities and normalizing the constant in Eq. (26), one has

$$\begin{aligned}\left\langle P_A^2\right\rangle_{\text{CCZ},h} &= 4^{N_A} \frac{16^{N_{\bar{A}}} + 2(2^{N_A}-1)4^{N_{\bar{A}}}[2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}}+1)] + [4^{N_A} - 3(2^{N_A}-1) - 1][2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2 + (2^{N_A}-1)\text{No.}_4}{4^{2N}} \\ &= \frac{\{d(d_A + d_{\bar{A}} - 1) + d_A(d_A-1)N_{\bar{A}}(N_{\bar{A}}+1)\}^2 + d_A^2(d_A-1)\{\text{No.}_4 - [d_{\bar{A}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2\}}{d^4},\end{aligned} \tag{43}$$

with $4^{N_A}$ multiplication due to the logical encoding redundancy for qubit in $A$. As a result, by combing the average purity result in Eq. (21), the variance of the half CCZ ensemble shows as follows.

*Theorem 4.* For a subsystem $A$ with $N_A$ qubits, the variance of the purity $P_A$ defined in Eqs. (5) for the random hypergraph states from the half CCZ ensemble is

$$\begin{aligned}\delta^2_{\text{CCZ,h}}(P_A) &= \frac{d_A^2(d_A-1)\{\text{No.}_4 - [d_{\bar{A}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2\}}{d^4} \\ &\leqslant \frac{9d_A}{d^2} \leqslant 9d^{-\frac{3}{2}},\end{aligned} \tag{44}$$

where No. 4 is in Lemma 1 by taking $m = N_{\bar{A}}$, and $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of the subsystem $A(\bar{A})$.

Similar to the discussion at the end of Sec. IV B, from Eq. (44), it is not hard to see that only case 4 contributes to the final variance. Actually, the bit strings in cases 1–3 have already been counted for $[\mathbb{E}_\Psi(P_A)]^2$ of Eq. (21) in Sec. III C. In particular, the $[d_{\bar{A}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2$ in Eq. (44) indicates that one should further substrate the solution of Eq. (40) with $\langle \mathbf{j_1}| H_4 |\mathbf{k_1}\rangle = \langle \mathbf{j_2}| H_4 |\mathbf{k_2}\rangle = 1$ for all $j, k$ pairs.

Before moving to the full CCZ ensemble, we would like to remark that as one extends the random CCZ gates from the half ensemble to the full ensemble, the average value should decrease,

$$\left\langle P_A^2\right\rangle_{\text{CCZ}} \leqslant \left\langle P_A^2\right\rangle_{\text{CCZ},h}, \tag{45}$$

since the full ensemble will induce more constraints on the bit configuration and less of them can survive. As a result, by inserting the average purity in Eq. (22), one has the result for the full ensemble, with the proof left to Appendix D.

*Corollary 1.* For a subsystem $A$ with $N_A$ qubits, the variance of the purity $P_A$ defined in Eqs. (5) for the random hypergraph states from the CCZ ensemble is upper bounded by

$$\delta^2_{\text{CCZ}}(P_A) < \left\langle P_A^2\right\rangle_{\text{CCZ,h}} - \langle P_A\rangle^2_{\text{CCZ}} < 3N^2 d^{-\frac{3}{2}} \tag{46}$$

for sufficient large $N$ and $d = 2^N$ is the total Hilbert space dimension.

Furthermore, one can enhance the bound by more delicate counting as in the average purity scenario in Sec. III C, and show that the variance of the full ensemble scales as $d^{-2}$, compared to $d^{-1.5}$ in Corollary 1.

*Theorem 5.* For a subsystem $A$ with $N_A$ qubits, the variance of the purity $P_A$ defined in Eqs. (5) for the random hypergraph states from the CCZ ensemble is

$$\delta^2_{\text{CCZ}}(P_A) = 4d^{-2} - 2(d_A + d_{\bar{A}})d^{-3} + O(N^4)d^{-3}, \tag{47}$$

where $d = 2^N$ is the total Hilbert space dimension.

The proof is Appendix E. Note that the variance of the subsystem purity of CCZ ensemble is similar to that of Haar random states [51,52], which scales as $d^{-2}$ for the equal partition.

At the end of this subsection, we give some remarks on the generalization of our method beyond the uniform ensemble of the $\text{CZ}_e$ gate in Definition 1. First, suppose the hypergraph state ensemble is not uniform, say the probability $p \neq 1/2$, one can still apply the phase and/or summation matrix formalism, and now $M_s$, say in Eq. (13), become $M_s = pM_p + (1-p)J$, which could make the calculation more involved. But we conjecture that any constant deviation of $p$ from $1/2$ will not essentially change the previous results on the purity and its variance. Generally, the $M_s$ matrix could be a summation or integral like

$$M_s = \sum_i p_i M_p^{(i)}, \tag{48}$$

where $M_p^{(i)}$ is the phase matrix for some phase gate with applying probability $p_i$. In our original uniform ensemble, the

gates are $\{\mathbb{I}_e, \mathrm{CZ}_e\}$, both with $1/2$ probability. Moreover, our formalism could also be suitable for diagonal gates, since they keep the transformation on the computational basis.

## V. IMPLICATIONS FOR THE ENTANGLEMENT ENTROPY

In this section, we utilize the results of the average subsystem purity and its variance obtained in Secs. III and IV to show some statistical behaviors of the entanglement entropy.

Recall that the von Neumann entropy can be bounded by the Rényi-2 entropy

$$\mathbb{E}_\Psi S_1(\rho_A) \geqslant \mathbb{E}_\Psi S_2(\rho_A) = \mathbb{E}_\Psi - \log_2(P_A) \geqslant -\log_2(\mathbb{E}_\Psi P_A), \tag{49}$$

where the last line is due to the convexity. Consequently, by Theorems 1 and 2, one has the following result.

*Corollary 2.* For subsystem $A$ with $N_A$ qubits, the average Rényi-2 entanglement entropy of the random hypergraph states from both CZ and CCZ ensembles is lower bounded by

$$\langle S_2(\rho_A)\rangle \geqslant -\log_2\left(\frac{d_A + d_{\bar{A}}}{d}\right), \tag{50}$$

where $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of the subsystem $A(\bar{A})$, and so does the average von Neumann entropy $\langle S_1(\rho_A)\rangle$ by Eq. (49).

Some remarks are as follows. In the regime $N_{\bar{A}} - N_A \gg 1$, it is clear that the average entanglement entropy for both ensembles equals the qubit number in subsystem $A$, $\langle S_2(\rho_A)\rangle \sim -\log_2(d_A^{-1}) = N_A$, which is the largest possible value. In the regime $N_A = N_{\bar{A}} = N/2$, the lower bound of average entropy reads $-\log_2(2d^{-1/2}) = N/2 - 1$, which shows a constant departure to the maximal possible value. This subtlety is also observed for random stabilizer states [53], and Haar random states [54].

Moreover, we can apply the variance of the purity function $P_A$ to show the typical behavior. By Chebyshev inequality,

$$\Pr\{|P_A - \langle P_A\rangle| > \varepsilon\} \leqslant \frac{\delta^2(P_A)}{\varepsilon^2}, \tag{51}$$

and one can further obtain the following result on entanglement entropy.

*Proposition 2.* For a subsystem $A$ with $N_A$ qubits, the probability of the entanglement entropy deviation is upper bounded by

$$\Pr\left\{S_2(\rho_A) \leqslant -\log_2\left(\frac{d_A + d_{\bar{A}}}{d}\right) - 1.5\varepsilon d_A\right\} \leqslant \frac{\delta^2(P_A)}{\varepsilon^2}, \tag{52}$$

where $d_{A(\bar{A})} = 2^{N_{A(\bar{A})}}$ is the Hilbert space dimension of the subsystem $A(\bar{A})$, and $\delta^2(P_A)$ is the variance of the subsystem purity $P_A$ of CZ or CCZ ensembles.

By Theorems 3 and 5, the variances $\delta^2_{\mathrm{CZ}}(P_A) = \Theta(d^{-1})$ and $\delta^2_{\mathrm{CCZ}}(P_A) = \Theta(d^{-2})$, no matter the relative size between $N_A$ and $N_{\bar{A}}$. In the regime $d_A \ll d_{\bar{A}}$, one can choose $\delta(P_A) \ll \varepsilon \ll d_A^{-1}$ for both ensembles such that the amount of the deviation, i.e., $1.5\varepsilon d_A$, from the maximal entropy is negligible, and also the probability of this deviation i.e., $\delta^2(P_A)/\varepsilon^2$, is exponentially small with respect to the qubit number $N$. As a result, one can further show exponentially small variance of the entanglement entropy. We leave the proof of Proposition 2 and the detailed discussion to Appendix F 1.

In the regime $d_A \simeq d_{\bar{A}}$ i.e., the subsystem size is comparable $N_{\bar{A}} - N_A = O(\log_2(N))$, $d_A \sim d^{-\frac{1}{2}}$ now. The previous argument can still apply for the CCZ ensemble, for example, by choosing $d^{-1} \ll \varepsilon \sim d^{-\frac{3}{4}} \ll d^{-\frac{1}{2}}$ to make the deviation and the corresponding probability both exponentially small. We summarize the result for the equal partition for conciseness as follows.

*Theorem 6.* Given a system of $N$-qubit with $N$ sufficient large, and the equal subsystem size $N_A = N_{\bar{A}}$, for the random hypergraph states from the CCZ ensemble, the probability of the entanglement entropy deviation is upper bounded by

$$\Pr\left\{\left|S_2(\rho_A) - \left(\frac{N}{2} - 1\right)\right| \geqslant 1.6\varepsilon d^{\frac{1}{2}}\right\} \leqslant \frac{4d^{-2}}{\varepsilon^2}, \tag{53}$$

where $d = 2^N$ is the total Hilbert space dimension and $d^{-1} \ll \varepsilon \ll d^{-\frac{1}{2}}$. Consequently, by taking $\varepsilon \sim d^{-\frac{3}{4}}$, the variance of the entanglement entropy with respect to the CCZ ensemble is bounded by

$$\mathrm{Var}_{\mathrm{CCZ}}[S_2(\rho_A)] < 1.6Nd^{-\frac{1}{2}}. \tag{54}$$

The proof of Theorem 6 is left in Appendix F 2. It is not hard to see that such exponentially small variance of entanglement entropy also holds for the half CCZ ensemble, as the standard variance of purity is about $\delta_{\mathrm{CCZ},h}(P_A) \sim d^{-3/4} \ll d^{-1/2}$ in Theorem 4. We remark that similar concentration of measure bound on entanglement entropy of Haar random states is also shown in Ref. [54].

However, it is not applicable to the CZ ensemble now, since $\delta_{\mathrm{CZ}}(P_A) = \Theta(d^{-1/2})$ and $d_A \sim d^{1/2}$, i.e., the standard variance is comparable to the expectation value of purity $\langle P_A\rangle \sim d^{-1/2}$ by Theorem 1. There is no room to choose an appropriate $\varepsilon$ such that the deviation and the corresponding probability in Eq. (52) both keep exponentially small. Especially in the equal partition case, one thus expects a *constant* variance of the entanglement entropy, which is proved in the following theorem.

*Theorem 7.* Given a system of $N$ qubits with the equal subsystem size $N_A = N_{\bar{A}}$, for the random graph states generated by random CZ gates, the variance of the entanglement entropy

$$\mathrm{Var}_{\mathrm{CZ}}[S_2(\rho_A)] > 0.128, \tag{55}$$

for sufficient large $N$.

The proof is based on the statistical result of the rank distribution for the random binary matrix [55], and we leave it to Appendix F 3.

## VI. CONCLUDING REMARKS

In this paper, we study the entanglement properties of random hypergraph states generated by CZ and CCZ gates, respectively. We find that, though the average subsystem purity and entanglement both feature the same volume law, fluctuations of entanglement in the CZ ensemble are large, while the CCZ ensemble shows typical values of entanglement with vanishing fluctuations. These results show that, in spite of CCZ gates not being universal, they feature universal entanglement behavior [51].

In perspective, there are several directions to explore starting from the results presented here. First, one could study general hypergraph states with $k > 3$ edges using the phase matrix method here. The extension to more general diagonal gates [5,50,56], qudit cases [57,58], and mixed states [47,59] are also possible. Second, in this paper we focus on the bipartite entanglement and it is interesting to study the tripartite and even complex entanglement structure [60,61] and entanglement distillation yield [47] of the random hypergraph state, which would supply useful tools to quantum networks. Third, the main difference between CCZ and CZ gates is that CCZ gates are non-Clifford, and as such they can produce magic. The relationship between fluctuations of the purity and magic has been shown in Refs. [51,62]. On the other hand, non-Clifford gates are involved in the onset of entanglement complexity and emergent irreversibility in unitary evolution [19]. In this context, it would be interesting to show the transition to quantum chaos behavior by doping a CZ circuit with CCZ gates [51,63,64]. Moreover, it would thus be very important to show that the fluctuations of the purity are directly responsible for the onset of entanglement complexity and the impossibility of undoing entanglement by Metropolis-like algorithms [19,20]. For the same reason, it would be interesting to study the behavior of (higher order) out-of-time-order correlation functions [17,65] under CZ and CCZ circuits, with and without doping. Finally, it would be intriguing to see whether our techniques here can be useful to study many-qubit magic states [62,66].

## ACKNOWLEDGMENTS

We thank Mile Gu, Xun Gao, Arthur Jaffe, and Zhengwei Liu for useful discussions. Y.Z. is supported by the startup funding of Fudan Univ., the Quantum Engineering Program No. QEP-SF3, National Research Foundation of Singapore under its NRF-ANR joint program (No. NRF2017-NRF-ANR004 VanQuTe), the Singapore Ministry of Education Tier 1 Grant No. RG162/19, FQXi-RFP-IPW-1903 from the foundational Questions Institute and Fetzer Franklin Fund, a donor-advised fund of the Silicon Valley Community Foundation. A.H. acknowledges support from NSF Award No. 2014000. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the National Research Foundation, Singapore.

## APPENDIX A: THE RELATION BETWEEN $M_s$ AND $\Phi^k_{\mathcal{E}_e}$

In the main text, we used the summation matrix (tensor) $M_s$ to account for the effect of the local twirling channel $\Phi^k_{\mathcal{E}_e}$, with $k = 2$ and 4 for the average purity and the variance respectively. Here we clarify the relation between $M_s$ and $\Phi^k_{\mathcal{E}_e}$ in detail by considering the example for $k = 2$ and the random CZ gate. The argument applies to other cases.

Recall in Fig. 2(c) in the main text the formula of average purity has been vectorized. The input state is $|+\rangle^{\otimes 2N}$, which can exhaust all the computational basis input. The matrix representation of the twirling channel $\tilde{\Phi}^2_{\mathcal{E}}$ is diagonal in the computational basis. And it can be decomposed to local twirling channels $\tilde{\Phi}^2_{\mathcal{E}_e}$, with $e$ for a specific edge $e = \{i, j\}$, by

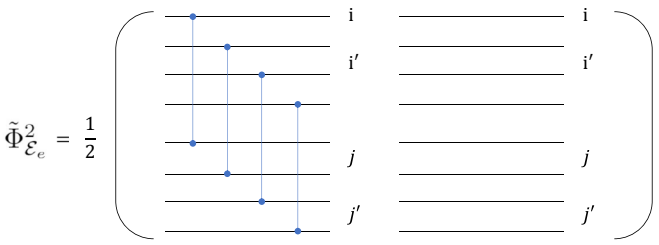



FIG. 8. Tensor network for the matrix form of the local twirling channel $\tilde{\Phi}^2_{\mathcal{E}_e}$.

Proposition 1. The tensor diagram is shown in Fig. 8, which is the average of the two possibilities $\mathrm{CZ}_e$ and $\mathbb{I}_e$. Every line can take take 0/1, and thus $\tilde{\Phi}^2_{\mathcal{E}_e}$ is $8\times 8$ diagonal matrix. To get $\tilde{\Phi}^2_{\mathcal{E}_e}$, one just needs to figure out eght diagonal elements there. Actually, for the average purity we consider, one needs not to figure out all of them. The vectorized swap and identity operators on the left in Fig. 2(c) further restrict the possible computational basis input. As illustrated in Fig. 3(a), the four bits on the line of $i$ and $i'$ which correspond to qubit $i$ will be reduced to two bits, similar to qubit $j$.

By further taking $i, i'$ as the row index and $j, j'$ as the column index, we reach the phase matrix in Fig. 3(b) and also the summation matrix $M_s$ in Eq. (13).

## APPENDIX B: THE DIFFERENCE BETWEEN $\mathbb{E}_\Psi(P_A^2)$ AND $[\mathbb{E}_\Psi(P_A)]^2$ IN THE VIEW OF PHASE MATRIX

The difference of $\mathbb{E}_\Psi(P_A^2)$ and $[\mathbb{E}_\Psi(P_A)]^2$ is the variance in Eqs. (5). Here we illustrate the difference with phase matrix formalism in detail, which can simplify the counting procedure of the surviving bit strings when calculating the variance.

By doubling Eq. (6), let us write $[\mathbb{E}_\Psi(P_A)]^2$ explicitly on four-copy Hilbert space $\mathcal{H}^{\otimes 4}$ as

$$\begin{aligned}[\mathbb{E}_\Psi(P_A)]^2 &= \mathrm{Tr}\big[T_A \otimes \mathbb{I}_{\bar{A}}^{\otimes 2}\ \Phi^2_{\mathcal{E}}\big(\Psi_0^{\otimes 2}\big)\big]^2 \\ &= \mathrm{Tr}\big[T_A^{(1,2)} \otimes T_A^{(3,4)} \otimes \mathbb{I}_{\bar{A}}^{\otimes 4} \quad \Phi^2_{\mathcal{E}} \otimes \Phi^2_{\mathcal{E}}\big(\Psi_0^{\otimes 4}\big)\big].\end{aligned} \tag{B1}$$

Compared with $\mathbb{E}_\Psi(P_A^2)$ in Eq. (24), the input state $\Psi_0^{\otimes 4}$ and the swap (identity) operators are the same, and the only difference is the twirling channel in the middle. In particular, one is $\Phi^2_{\mathcal{E}} \otimes \Phi^2_{\mathcal{E}}$, where the first two-copy and the last two-copy are independently twirled and the other is $\Phi^4_{\mathcal{E}}$, with four-copy twirled together. Similar to the proof for Proposition 1, $\Phi^2_{\mathcal{E}} \otimes \Phi^2_{\mathcal{E}}$ can also be decomposed to the local twirling channel on a specific edge $\Phi^2_{\mathcal{E}_e} \otimes \Phi^2_{\mathcal{E}_e}$.

In the following, we use CZ ensemble to illustrate the difference of these two twirling channels in terms of the phase matrix. The result on CCZ ensemble follows similarly. Similar to Fig. 7(a) of $\mathbb{E}_\Psi(P_A^2)$, we can draw the tensor network diagram of $[\mathbb{E}_\Psi(P_A)]^2$ of Eq. (B1) in Fig. 9(a). On the right, every qubit corresponds to eight lines, each two for one-copy Hilbert space. Every line can take can take one bit 0/1 value with a normalization constant in Eq. (26). On the left, there are two different connections for each qubit by decomposing the swap $T_A^{(1,2)} \otimes T_A^{(3,4)}$ and the identity $\mathbb{I}_{\bar{A}}^{\otimes 4}$ to the qubit level. The difference is in the middle, where we operate the random

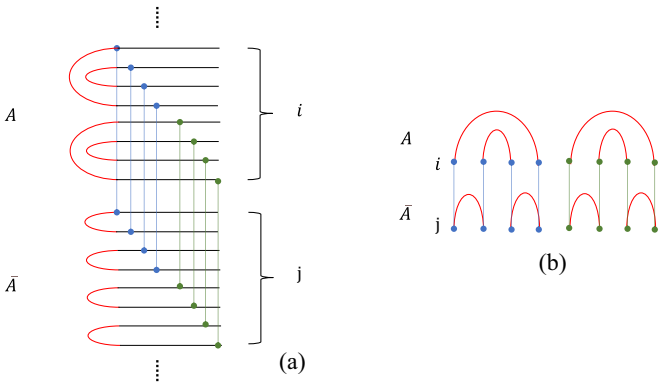



FIG. 9. Tensor network for $[\mathbb{E}_\Psi(P_A)]^2$ and the phase matrix.

$CZ_e$ gate across $A$ and $\bar{A}$, and we show the case of the gates between $i$ and $j$. Note that two different colors (blue and green) are used to denote the independence of the CZ gates on the first two-copy and the last two-copy.

In Fig. 9(b), we rotate the diagram to compare it with the previous phase matrix in Fig. 7(b), where the CZ gate repeats eight times. Similar to the discussion Sec. IV A, every qubit $i$ is denoted by a four-bit and further by two-bit $i_1 i_2$ with logical encoding. Now the constraints between any qubit pair $i, j$ across $A, \bar{A}$ becomes

$$\langle \mathbf{i_1}| \langle \mathbf{i_2}| M_s \otimes M_s |\mathbf{j_1}\rangle |\mathbf{j_2}\rangle = \langle \mathbf{i_1}| \langle \mathbf{i_2}| \frac{M_p + J_2}{2} \otimes \frac{M_p + J_2}{2} |\mathbf{j_1}\rangle |\mathbf{j_2}\rangle , \tag{B2}$$

with $M_s$ and $M_p$ defined in Eqs. (14) and (15). That is,

$$\langle \mathbf{i_1}| M_p |\mathbf{j_1}\rangle = 1, \quad \langle \mathbf{i_2}| M_p |\mathbf{j_2}\rangle = 1. \tag{B3}$$

On the other hand, the phase matrix of Eq. (27) in Fig. 7(b) induces a constraint as

$$\langle \mathbf{i_1}| \langle \mathbf{i_2}| \frac{M_p^{\otimes 2} + J_4}{2} |\mathbf{j_1}\rangle |\mathbf{j_2}\rangle , \tag{B4}$$

i.e.,

$$\langle \mathbf{i_1}| M_p |\mathbf{j_1}\rangle * \langle \mathbf{i_2}| M_p |\mathbf{j_2}\rangle = 1. \tag{B5}$$

Compared with Eq. (B3), this constraint is loose. That is, any bit-string configuration that satisfies Eq. (B3) also survives here, which leads to $\delta^2 = \mathbb{E}_\Psi(P_A^2) - [\mathbb{E}_\Psi(P_A)]^2 \geqslant 0$, a non-negative variance. As a result, to calculate $\delta^2$, one only needs to count the net number of bit strings which satisfy Eq. (B5), but not Eq. (B3). That is, for a bit-string configuration, there exists qubit-pair $i, j$, such that $\langle \mathbf{i_1}| M_p |\mathbf{j_1}\rangle = -1$ and $\langle \mathbf{i_2}| M_p |\mathbf{j_2}\rangle = -1$.

## APPENDIX C: PROOF OF LEMMA 1

*Proof.* To satisfy the inner product on the binary field, generally one cannot assign the same binary vector $\vec{v}$ with an odd hamming weight (the number of 1s), denoted by $w_2(\vec{v}) = 1$, to more than one position, since the inner product $\vec{v} \cdot \vec{v} = 1$ in this case.

First, we give explicit assignments, with $\vec{v}$ only owning an even Hamming weight $w_2(\vec{v}) = 0$. There are totally eight ones, and they can be divided into three sets, each with four elements, i.e.,

$$\{0000, 0011, 1100, 1111\}, \{0000, 0101, 1010, 1111\}, \times \{0000, 0110, 1001, 1111\}. \tag{C1}$$

It is easy to check that the inner product between the elements (also with itself) inside each set is 0. As a result, one can randomly assign a bit string from any of three sets to the $m$ positions which satisfies the inner product constraint. This gives $3 * 4^m - 2 * 2^m$, where $2^m$ accounts for the redundant counting of the case by only assigning a bit string from the set $\{0000, 1111\}$.

Furthermore, we consider adding $\vec{v}$ with $w_2(\vec{v}) = 1$ to the previous assignments. For a given $\vec{v}$, as mentioned before, it can only appear in the $m$ position once. At the same time, the subsequent assignment of $\vec{v}'$ with $w_2(\vec{v}') = 0$ is restricted. In particular, besides $\vec{v}' = 0000$, one can only choose one element in each set in Eq. (C1) due to the inner product constraint. For example, suppose $\vec{v} = 1000$, we can only choose $\vec{v}_1' = 0011$, $\vec{v}_2' = 0101$ and $\vec{v}_3' = 0110$ besides 0000. Note that one cannot choose any two of them $\vec{v}_1', \vec{v}_2', \vec{v}_3'$ at the same time since the inner product between them is 1. Consequently, the number of all possible assignments containing exactly one element $\vec{v}$ with $w_2(\vec{v}) = 1$ is

$$C_8^1 A_m^1 * 3 * 2^{m-1} = 12m2^m,$$

where $C_8^1 A_m^1$ represents choosing one $\vec{v}$ from total eight odd-weight bit strings and putting it in one of $m$ positions; $3 * 2^{m-1}$ represents assigning a bit string to other $m - 1$ positions from $\{0000, \vec{v}_i'\}$ for $i = 1, 2, 3$.

We can continue this process by considering more than one odd-weight bit string in $m$ positions. In fact, this process can at most go to four odd-weight bit strings. To be specific, suppose one choosees four distinct odd-weight strings, $\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4$, which are orthogonal to each other; they already form a complete basis of $\mathbb{F}_2^4$. Consequently, there is no bit string $v_5$ besides the trivial 0000 such that the inner products of $v_5$ with $v_i$, $1 \leqslant i \leqslant 4$ are all zero. For this case of four odd-weight strings, one can only assign 0000 to other $m - 4$ positions, totally, $56A_m^4$.

A similar argument also holds for the case of three odd-weight strings, for example, $\vec{v}_1 = 1000$, $\vec{v}_2 = 0100$, $\vec{v}_3 = 0010$. One cannot find an even-weight string $\vec{v}'$ orthogonal to all of them. Totally $8A_m^3$. For the case of two odd-weight strings, it depends on the specific choice. For example, if one selects $\vec{v}_1 = 1000$, $\vec{v}_2 = 0111$, there are three legal even-weight strings besides 0000, the same as the one odd-weight string case; if $\vec{v}_1 = 1000$, $\vec{v}_2 = 0100$, there is only one nontrivial string $\vec{v}' = 0011$. As a result, totally $(C_4^1 * 3 + C_4^2 * 2)A_m^2 2^{m-2}$.

In summary, the number of all possible assignments is obtained by summing these numbers of all possible assignments,

$$\begin{aligned} \text{No.}_4 &= 3 * 4^m - 2 * 2^m + 12m2^m + 24A_m^2 2^{m-2} + 8A_m^3 + 56A_m^4 \\ &= 3 * 4^m + (6m^2 + 6m - 2)2^m + 4A_m^2 + 8A_m^3 + 56A_m^4 \\ &= 3 * 4^m + \Theta(m^2)2^m + \Theta(m^4), \end{aligned} \tag{C2}$$

and we finish the proof. ■

## APPENDIX D: PROOF OF COROLLARY 1 FOR $N_A$ QUBITS IN SUBSYSTEM $A$

Here we prove Corollary 1 for the general qubit number in $A$. As mentioned in the main text, the variance of the purity for the full CCZ ensemble can be upper bounded by

$$\begin{aligned}\delta^2_{\mathrm{CCZ}} &< \langle P_A^2\rangle_{\mathrm{CCZ},h} - \langle P_A\rangle^2_{\mathrm{CCZ}} \\ &= \langle P_A^2\rangle_{\mathrm{CCZ},h} - \langle P_A\rangle^2_{\mathrm{CCZ},h} + \langle P_A\rangle^2_{\mathrm{CCZ},h} - \langle P_A\rangle^2_{\mathrm{CCZ}} \\ &= \delta^2_{\mathrm{CCZ},h} + \langle P_A\rangle^2_{\mathrm{CCZ},h} - \langle P_A\rangle^2_{\mathrm{CCZ}}. \end{aligned} \tag{D1}$$

By inserting the results in Eqs. (21), (22), and (44), one has

$$\begin{aligned}\delta^2_{\mathrm{CCZ}} &< \frac{9d_A}{d^2} + 3\frac{d_A + d_{\bar{A}} - 1}{d} * \frac{d_A(d_A-1)N_{\bar{A}}(N_{\bar{A}}+1)}{d^2} \\ &< \frac{9d_A}{d^2} + \frac{6d_{\bar{A}}}{d} * \frac{d_A^2 N_{\bar{A}}(N_{\bar{A}}+1)}{d^2} \\ &= \frac{d_A}{d^2}[9 + 6N_{\bar{A}}(N_{\bar{A}}+1)] < 3N^2 d^{-1.5} \end{aligned} \tag{D2}$$

by using the fact that $N_A \leqslant N_{\bar{A}}$ and $d_A \leqslant d_{\bar{A}}$.

## APPENDIX E: PROOF OF THEOREM 5

Here we prove a tighter result for the variance of the purity of the full CCZ ensemble by counting the total surviving bit strings. Similar to the average purity scenario in Sec. III C, the further introduction of the random gates $\mathrm{CCZ}_{ijk}$ with $i, j \in A$, $k \in \bar{A}$ will induce more constraints on the bit configuration back from $\bar{A}$ to $A$. In particular, similar to Eq. (32) in Fig. 7(c), the phase tensor follows directly by the tensor product of the one in Fig. 4(c), $\tilde{M}^p_{ijk} = \tilde{M}^p_{i_1 j_1 k_1} \otimes \tilde{M}^p_{i_2 j_2 k_2}$, and it equals $M^p_{kij}$ by Fig. 4(d).

In the following, we follows cases 1–4 of the half CCZ ensemble in Sec. IV B and use the phase tensor to apply additional constraints from $\bar{A}$ to $A$. Remembering the discussion on the half CCZ ensemble in Sec. IV B, only case 4 can contain bit strings surviving in the formula of $\mathbb{E}_\Psi(P_A^2)$ but not in the one of $[\mathbb{E}_\Psi(P_A)]^2$, which accounts for the final variance (see also the illustration in Appendix B). For completeness, here we list all the possible bit stings, but finally we will only count the one that contributes to the net variance.

(1) $A$ only contains $\bar{0}\bar{0}$, $\bar{A}$ can be arbitrary, and vice versa. Totally, $(4^{N_A} + 4^{N_{\bar{A}}} - 1)4^N$ with $4^N$ for the logical encoding.

(2) $A$ only contains $\bar{0}\bar{0}$ and $\bar{0}\bar{1}$. The first two-bit of the qubit in $\bar{A}$ can be arbitrary and the last two should be restricted. We consider several possibilities for the last two-bit.

(a) If they all take $\bar{0}$, it will not induce any constraint backward on $A$, thus $(2^{N_A} - 1) * (2^{N_{\bar{A}}} - 1)4^N$.

(b) For the case there is one 01(10) or two of 01,10, it means logical $\bar{1}$ on the last two-bit. As a result, it further induces constraint on the last two-bit of the qubits in $A$, i.e., the logical $\bar{0}\bar{1}$ there. Similar to case 2 in Sec. IV B, one has totally $2^{N_A}N_A(N_A+1) * 4^{N_{\bar{A}}}N_{\bar{A}}(N_{\bar{A}}+1)$.

The same result holds for $A$ only containing $\bar{0}\bar{0}$ and $\bar{1}\bar{0}$ by symmetry.

(3) $A$ contains at least two types from $\{\bar{0}\bar{1}, \bar{1}\bar{0}, \bar{1}\bar{1}\}$. For the qubit in $\bar{A}$, both the first two and last two-bits are constrained independently. Previously there are totally $4^{N_A}[4^{N_A} - 3(2^{N_A} - 1) - 1][2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2$ bit strings. The first term is for possibilities of $A$ and the second one is for $\bar{A}$. Since now different bit configurations induce different constraints backward on $A$, we discuss the terms in $[2^{N_{\bar{A}}} + N_{\bar{A}}(N_{\bar{A}}+1)]^2$ separately.

(a) $2^{N_{\bar{A}}} * 2^{N_{\bar{A}}}$. This term corresponds to all bit strings taking $\bar{0}\bar{0}$ in $\bar{A}$, which has already been counted in case 1.

(b) $2 * 2^{N_{\bar{A}}}N_{\bar{A}}(N_{\bar{A}}+1)$. This term corresponds to the first two-bits of all qubits in $\bar{A}$ taking $\bar{0}$, and the last two-bits taking one 01(10) or two of 01,10, or vice versa. For the first case, there is logical $\bar{1}$ on the last two-bit and thus it induces constraint on the logical $\bar{0}\bar{1}$ and $\bar{1}\bar{1}$ in $A$. The number of the possibilities in $A$ reduces from $4^{N_A}[4^{N_A} - 3(2^{N_A} - 1) - 1]$ to $[4(2^{N_A-1} - 1)C^1_{N_A} + 4(2^{N_A-2} - 1)C^2_{N_A} + 4(2^{N_A-2})C^2_{N_A}] * 2^{N_A} \sim \Theta(N_A^2)4^{N_A}$.

(c) $N_{\bar{A}}^2(N_{\bar{A}}+1)^2$. This term corresponds to the case that both the first two-bits and the last two-bits of the qubits in $\bar{A}$ can take logical $\bar{1}$. There are a few different induced constraints on $A$ based on the specific bit configurations, and we will figure out the updated number of surviving bit strings, denoted by $n_{3c}$, later.

(4) $A$ only contains $\bar{0}\bar{0}$ and $\bar{1}\bar{1}$. For the qubit in $\bar{A}$, both the first and last two-bit are restricted jointly. The summation tensor is given in Eq. (38), and previously there were $4^{N_A}(2^{N_A} - 1) * \mathrm{No.}_4(m = N_{\bar{A}})$ surviving bit strings with No. 4 in Eq. (42) by taking $m = N_{\bar{A}}$. Different choices of bit strings from No. 4, which is detailed in Appendix C, will induce different constraints backward on $A$. We denote the updated number of surviving bit strings as $n_4$ and figure it out later.

To calculate the variance, one should in principle get $\mathbb{E}_\Psi(P_A^2)$ by summing all the numbers of the above possibilities in cases 1–4, and normalizing it with the constant in Eq. (26). As discussed before, there are actually only a few bit strings contributing to the final variance, since many of them in the above cases also survive in the formula of $[\mathbb{E}_\Psi(P_A)]^2$. In particular, it is not hard to check that only the above case 3(c) and case 4 can contain this kind of genuine bit string. As a result, one has the upper bound on the variance:

$$\delta^2_{\mathrm{CCZ}} < (n_{3c} + n_4)d^{-4}. \tag{E1}$$

Let us first figure out $n_4$ in case 4, by checking all the possible bit strings in $\bar{A}$, described by No. 4 shown explicitly in Appendix C. First, we are interested in the leading order in No. 4, that is, the configuration from the three even-hamming-weight sets shown in Eq. (C1). Note that the first set corresponds to all $\bar{0}\bar{0}$ cases, which has been already counted in case 1. The last two sets both correspond to $\bar{0}\bar{0}$, $\bar{1}\bar{1}$, and thus induce constraint backward on $A$, which is described by the summation tensor in Eq. (38), or more explicitly by Eq. (40) with $j, k \in A$ now. Just as the previous constraint from $A$ to $\bar{A}$, the number of legal bit configuration in $A$ is $2 * 4^{N_A} - 2^{N_A}$, where we can only choose the last two sets in Eq. (C1) now for $A$. Second, for the bit configuration with a few odd-hamming-weight bit strings, there is $\bar{0}\bar{1}$ or $\bar{1}\bar{0}$ appearing in $\bar{A}$. For example, if there is $\bar{1}\bar{0}$ in $\bar{A}$, the first two-bit on the logical $\bar{0}\bar{0}$ and $\bar{1}\bar{1}$ in $A$ will be restricted, and there are $2^{N_A}N_A(N_A+1)$ possibilities, and this number can further decrease to $\Theta(N_A^2)$ if there is also constraint on the last two-bit.

As a result, the number in case 4 is bounded by

$$\begin{aligned} n_4 &< (2*4^{N_A}-2^{N_A})(2*4^{N_{\bar{A}}}-2^{N_{\bar{A}}}) \\ &\quad + 2^{N_A}N_A(N_A+1)*\Theta\big(N_{\bar{A}}^2\big)2^{N_{\bar{A}}} \\ &= 4d^2 - 2(d_A+d_{\bar{A}})d + \Theta\big(N_A^2N_{\bar{A}}^2\big)d. \end{aligned} \tag{E2}$$

Similarly, one can consider the bit strings in case 3(c). For the previous total $N_{\bar{A}}^2(N_{\bar{A}}+1)^2$ bit configurations, $2N_{\bar{A}}(N_{\bar{A}}+1)$ of them correspond to $\bar{A}$ only containing $\bar{0}\bar{0}$, $\bar{1}\bar{1}$. In this case, by following case 4, the number of possibilities on $A$ is upper bounded by the odd-hamming weight cases in No. 4($m = N_A$), since the precondition is that $A$ has two types from $\{\bar{0}\bar{1}, \bar{1}\bar{0}, \bar{1}\bar{1}\}$. For the other cases, $\bar{A}$ contains two types from $\{\bar{0}\bar{1}, \bar{1}\bar{0}, \bar{1}\bar{1}\}$. One can directly follow case 3(c) and the possibilities in $A$ are thus bounded by $N_A^2(N_A+1)^2$. As a result, one has

$$n_{3c} = \Theta\big(N_A^2\big)2^{N_A}\Theta\big(N_{\bar{A}}^2\big) + \Theta\big(N_A^4\big)\Theta\big(N_{\bar{A}}^4\big) = \Theta\big(N_A^2N_{\bar{A}}^2\big)d_A. \tag{E3}$$

Inserting Eqs. (E2) and (E3) into Eq. (E1), one has

$$\delta_{\mathrm{CCZ}}^2 < 4d^{-2} - 2(d_A+d_{\bar{A}})d^{-3} + \Theta\big(N_A^2N_{\bar{A}}^2\big)d^{-3}. \tag{E4}$$

In addition, by observing that the configurations in the first term of Eq. (E2), that is, $(2*4^{N_A}-2^{N_A})(2*4^{N_{\bar{A}}}-2^{N_{\bar{A}}}) + 2^{N_A}N_A(N_A+1)$ are all genuine ones. Consequently, one also has

$$\delta_{\mathrm{CCZ}}^2 > 4d^{-2} - 2(d_A+d_{\bar{A}})d^{-3} \tag{E5}$$

and we finish the proof. We remark that the more exact value of the variance is

$$\delta_{\mathrm{CCZ}}^2 = 4d^{-2} - 2(d_A+d_{\bar{A}})d^{-3} + \Theta\big(N_A^2N_{\bar{A}}^2\big)(d_A+d_{\bar{A}})d^{-4} \tag{E6}$$

by counting the genuine configurations in $n_{3c}$ and $n_4$ more carefully. Since it shares the leading and subleading terms with Eq. (47), we do not elaborate it here.

## APPENDIX F: ON THE FLUCTUATION OF THE ENTANGLEMENT ENTROPY

### 1. Proof of proposition 2 and discussion on the variance

Here we first prove the deviation probability of Proposition 2 in main text, and discuss the implication on the variance of the entanglement entropy. Hereafter, for simplicity, the $\log_2$ function is base 2 without clarification.

*Proof.* The probability of the entanglement entropy deviation can be bounded by the Chebyshev inequality:

$$\begin{aligned} \Pr\{-\log_2(P_A) \leqslant -\log_2(\langle P_A\rangle + \varepsilon)\} &= \Pr\{P_A - \langle P_A\rangle \geqslant \varepsilon\} \\ &\leqslant \Pr\{|P_A - \langle P_A\rangle| \geqslant \varepsilon\} \leqslant \frac{\delta^2(P_A)}{\varepsilon^2}. \end{aligned} \tag{F1}$$

The average purity $\langle P_A\rangle \leqslant \frac{d_A+d_{\bar{A}}}{d}$ for both ensembles by Theorems 1 and 2, and one has

$$\begin{aligned} -\log_2(\langle P_A\rangle + \varepsilon) &\geqslant -\log_2\left(\frac{d_A+d_{\bar{A}}}{d} + \varepsilon\right) \\ &= -\log_2\left(\frac{d_A+d_{\bar{A}}}{d}\right) - \log_2\left(1 + \frac{\varepsilon d}{d_A+d_{\bar{A}}}\right) \\ &\geqslant -\log_2\left(\frac{d_A+d_{\bar{A}}}{d}\right) - \frac{\log_2(e)\varepsilon d}{d_A+d_{\bar{A}}} \\ &\geqslant -\log_2\left(\frac{d_A+d_{\bar{A}}}{d}\right) - 1.5\varepsilon d_A, \end{aligned} \tag{F2}$$

where in the last-but-one inequality we use $\log_2(1+x) \leqslant \log_2(e)x$. Substituting $-\log_2(\langle P_A\rangle + \varepsilon)$ in Eq. (F1) with the lower bound in Eq. (F2), we finish the proof. ■

As mentioned in main text, we can use the deviation probability in Proposition 2 to bound the variance of the entanglement entropy. Denote $\Delta = \frac{d_A+d_{\bar{A}}}{d}$, one bounds the variance by the expectation for the square of the difference to the maximal possible entropy $\log_2(d_A) = N_A$.

$$\begin{aligned} \mathrm{Var}[S_2(\rho_A)] = \mathbb{E}_\Psi[S_2(\rho_A) - \langle S_2(\rho_A)\rangle]^2 &\leqslant \mathbb{E}_\Psi[\log_2(d_A) - S_2(\rho_A)]^2 = \mathbb{E}_{\{\Psi|S_2(\rho_A)\leqslant -\log_2(\Delta)-\log_2(e)\varepsilon d_A\}}[\log_2(d_A) - S_2(\rho_A)]^2 \\ &\quad + \mathbb{E}_{\{\Psi|S_2(\rho_A)>-\log_2(\Delta)-\log_2(e)\varepsilon d_A\}}[\log_2(d_A) - S_2(\rho_A)]^2 \\ &\leqslant N_A^2\Pr\{S_2(\rho_A) \leqslant -\log_2(\Delta) - \log_2(e)\varepsilon d_A\} + [\log_2(d_A) + \log_2(\Delta) + \log_2(e)\varepsilon d_A]^2 \\ &\leqslant N^2\frac{\delta^2(P_A)}{\varepsilon^2} + \log_2^2(e)(d_A/d_{\bar{A}} + \varepsilon d_A)^2. \end{aligned} \tag{F3}$$

In the last-but-one line, for the first term we note that $[\log_2(d_A) - S_2(\rho_A)]^2 \leqslant N_A^2$, and later use Proposition 2 to bound the probability for the small entropy cases; for the second term corresponding to the cases with entropy near $\log_2(d_A)$, we directly take the maximal deviation and the probability can be bounded trivially by 1.

In the regime $d_A \ll d_{\bar{A}}$, one can choose an appropriate $\delta(P_A) \ll \varepsilon \ll d_A^{-1}$ to control the variance exponentially small for both ensembles. To balance the two terms in Eq. (F3), one can choose $\varepsilon = \sqrt{\delta(P_A)d_A^{-1}}$. In this way, the entropy variance is in the order,

$$\mathrm{Var}[S_2(\rho_A)] \sim \delta(P_A)d_A, \tag{F4}$$

by omitting the insignificant coefficient of $N$. Remembering that the purity variances $\delta_{\mathrm{CZ}}^2(P_A) = \Theta(d^{-1})$ and $\delta_{\mathrm{CCZ}}^2(P_A) = \Theta(d^{-2})$ by Theorems 3 and 5, consequently the entropy variances for both ensembles can be quite small in the regime $d_A \ll d_{\bar{A}}$. It is not hard to see that this is also true for $S_1(\rho_A)$.

### 2. Proof of theorem 6

Furthermore, in the regime that $d_A \sim d_{\bar{A}} \sim d^{1/2}$, the argument in Sec. F 1 can still apply for the CCZ ensemble. We prove Theorem 6 as follows.

*Proof.* Similar to Eq. (F1), we can bound the probability for entropy deviation by Chebyshev inequality. Different from

Eq. (F1), we now consider deviation on both sides:

$$\Pr\{-\log_2(P_A) \geqslant -\log_2(\langle P_A\rangle - \varepsilon)\} \bigcup \Pr\{-\log_2(P_A) \leqslant -\log_2(\langle P_A\rangle + \varepsilon)\} \leqslant \frac{\delta^2}{\varepsilon^2}. \tag{F5}$$

By Theorem 2 for the case of $d_A = d_{\bar{A}} = d^{1/2}$,

$$\begin{aligned} -\log_2(\langle P_A\rangle - \varepsilon) &< -\log_2(2d^{-1/2} - d^{-1} - \varepsilon) \\ &= -\log_2(2d^{-1/2}) - \log_2\left[1 - \tfrac{1}{2}(d^{-1} + \varepsilon)d^{1/2}\right] \\ &< (N/2-1) + \tfrac{1.1}{2}\log_2(e)(d^{-1} + \varepsilon)d^{1/2} \\ &< (N/2-1) + 0.8(d^{-1} + \varepsilon)d^{1/2}. \end{aligned} \tag{F6}$$

In the last-but-one line, we use the relation $-\log_2(1-x) = \log_2(e)(x + x^2/2 + x^3/3\cdots) < 1.1\log_2(e)x < 0.8x$ for sufficient small $x = \frac{1}{2}(d^{-1} + \varepsilon)d^{1/2}$ here. By Eq. (F2), one also has $-\log_2(\langle P_A\rangle + \varepsilon) \geqslant (N/2-1) - 1.5\varepsilon d^{1/2}$. Since we take $d^{-1} \ll \varepsilon \ll d^{-\frac{1}{2}}$, one has $0.8(d^{-1} + \varepsilon)d^{1/2} < 1.6\varepsilon d^{1/2}$. By inserting these bounds in Eq. (F5) and noting that $\delta^2_{\mathrm{CCZ}}(P_A) < 4d^{-2}$ in Theorem 5, one has

$$\Pr\left\{\left|S_2(\rho_A) - \left(\frac{N}{2} - 1\right)\right| \geqslant 1.6\varepsilon d^{1/2}\right\} \leqslant \frac{4d^{-2}}{\varepsilon^2}. \tag{F7}$$

The variance of the entanglement entropy can be proved in the same way as in Eq. (F3), but consider the difference from $N/2-1$ here.

$$\begin{aligned} \mathrm{Var}[S_2(\rho_A)] &= \mathbb{E}_\Psi[S_2(\rho_A) - \langle S_2(\rho_A)\rangle]^2 \\ &\leqslant \mathbb{E}_\Psi[S_2(\rho_A) - (N/2-1)]^2 \\ &= \mathbb{E}_{\{\Psi||S_2(\rho_A)-(N/2-1)|\geqslant 1.6\varepsilon d^{1/2}\}}[S_2(\rho_A) - (N/2-1)]^2 \\ &\quad + \mathbb{E}_{\{\Psi||S_2(\rho_A)-(\frac{N}{2}-1)|< 1.6\varepsilon d^{1/2}\}}[(N/2-1) - S_2(\rho_A)]^2 \\ &\leqslant (N/2)^2 \Pr\left\{\left|S_2(\rho_A) - \left(\frac{N}{2} - 1\right)\right| \geqslant 1.6\varepsilon d^{1/2}\right\} + (1.6\varepsilon d^{1/2})^2 \\ &\leqslant N^2\frac{d^{-2}}{\varepsilon^2} + 1.6^2\varepsilon^2 d. \end{aligned} \tag{F8}$$

By taking $\varepsilon = \sqrt{N/1.6}d^{-\frac{3}{4}}$, one has $\mathrm{Var}[S_2(\rho_A)] \leqslant 1.6Nd^{-\frac{1}{2}}$. ■

### 3. Proof of theorem 7

For the CZ ensemble, as mentioned in main text, since the variance of the purity $\delta_{\mathrm{CZ}}(P_A) = \Theta(d^{-1/2})$ is comparable to the expectation value of the purity $\langle P_A\rangle \sim d^{-1/2}$ in the regime $d_A \sim d_{\bar{A}}$, one expects a constant variance of entanglement entropy, and we prove Theorem 7 here.

Compared to studying the the variance $\mathrm{Var}[S_2(\rho_A)]$ with $\delta_{\mathrm{CZ}}(P_A)$ in the previous subsections, here we directly evaluate $S(\rho_A)$ and then $\mathrm{Var}[S_2(\rho_A)]$ by the property of the graph state.

First, we briefly review the formula of the entanglement entropy of graph state [67]. Any simple graph, $G$ can be uniquely determined by its adjacency matrix denoted as $\Gamma$, with $\Gamma_{i,j} = 1$ iff $(i, j) \in E$. Suppose the vertex set $V = \{N\}$ is partitioned into two complementary subsets $A$ and $\bar{A}$, the adjacency matrix $\Gamma$ can be arranged in the following form:

$$\Gamma_G = \begin{pmatrix} \Gamma_A & \Gamma_{A\bar{A}} \\ \Gamma^T_{A\bar{A}} & \Gamma_{\bar{A}} \end{pmatrix}, \tag{F9}$$

where $\Gamma_A, \Gamma_{\bar{A}}$ describe the connections inside each subsystem, and the off-diagonal $N_A \times N_{\bar{A}}$ submatrix $\Gamma_{A\bar{A}}$ is for the ones between them.

Given a graph state $|G\rangle$ with its associated graph $G$, the reduced density matrix of a subsystem $A$ is $\rho_A = \mathrm{Tr}_{\bar{A}}(|G\rangle\langle G|)$, where the partial trace is on $\bar{A}$. The explicit formula of the entanglement entropy is

$$S_2(\rho_A) = \mathrm{rank}(\Gamma_{A\bar{A}}), \tag{F10}$$

where the rank is on the binary field $\mathbb{F}_2$. Note that Renyi-$\alpha$ entropy $S_\alpha(\rho_A)$ of any order is also suitable here, since the spectrum of $\rho_A$ is flat for graph states [67].

The random graph state generated by random CZ gates just corresponds to randomly assigning $0/1$ with equal probability in the adjacency matrix $\Gamma$. If only considering the entanglement entropy, one only needs to study the statistical property of $\mathrm{rank}(\Gamma_{A\bar{A}})$ for random $\Gamma_{A\bar{A}}$. The following lemma considering the rank distribution of the random binary matrix [55].

*Lemma 2 (Theore, 3.2.1* [55]). For the random $n\times n$ binary matrix $\Gamma$, with each element $\Gamma_{ij}$ distributing independently, and equally taking value $0/1$, the probability for the rank of $\Gamma$ on the binary field shows

$$\begin{aligned} Q_s &:= \Pr\{\mathrm{rank}(\Gamma) = n - s\} \\ &= 2^{-s^2}\prod_{i\geqslant s+1}^{\infty}(1-2^{-i})\prod_{1\leqslant i\leqslant s}(1-2^{-i})^{-1} \end{aligned} \tag{F11}$$

as $n \to \infty$. In particular, $Q_1 = 2Q_0$, $Q_2 = \frac{4}{9}Q_0$, and numerically $Q_0 \approx 0.288\cdots$.

Based on this prior knowledge, we can prove Theorem 7 by considering the square matrix $\Gamma_{A\bar{A}}$ with $N_A = N_{\bar{A}} = N/2$ with $N \to \infty$.

*Proof.* From Corollary 2, one knows that $\langle S_2(\rho_A)\rangle \geqslant -\log_2(\frac{2\sqrt{d}}{d}) = N/2 - 1$. By using Lemma 2, one has

$$\begin{aligned}\mathrm{Var}[S_2(\rho_A)] &= \sum_{s=0}^{N/2} Q_s[(N/2-s) - \langle S_2(\rho_A)\rangle]^2 > Q_2[(N/2-2) - \langle S_2(\rho_A)\rangle]^2 > Q_2[(N/2-2) - (N/2-1)]^2 \\ &= \frac{4}{9}Q_0 \approx 0.128. \end{aligned} \tag{F12}$$

■


[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, New York, 2011)

[3] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, Entanglement in many-body systems, Rev. Mod. Phys. **80**, 517 (2008).

[4] X.-L. Qi, Does gravity come from quantum information? Nat. Phys. **14**, 984 (2018).

[5] C. Kruszynska and B. Kraus, Local entanglability and multipartite entanglement, Phys. Rev. A **79**, 052304 (2009).

[6] M. Rossi, M. Huber, D. BruB, and C. Macchiavello, Quantum hypergraph states, New J. Phys. **15**, 113022 (2013).

[7] R. Qu, J. Wang, Z.-S. Li, and Y.-R. Bao, Encoding hypergraphs into quantum states, Phys. Rev. A **87**, 022311 (2013).

[8] H. J. Briegel and R. Raussendorf, Persistent Entanglement in Arrays of Interacting Particles, Phys. Rev. Lett. **86**, 910 (2001).

[9] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, Entanglement in graph states and its applications, in *Proceedings of the International School of Physics "Enrico Fermi" Volume 162: Quantum Computers, Algorithms and Chaos* (IOS Press, Amsterdam, 2006), pp. 115–218.

[10] J. Miller and A. Miyake, Hierarchy of universal entanglement in 2D measurement-based quantum computation, npj Quantum Inf. **2**, 16036 (2016).

[11] J. Miller and A. Miyake, Latent Computational Complexity of Symmetry-Protected Topological Order with Fractional Symmetry, Phys. Rev. Lett. **120**, 170503 (2018).

[12] Y. Takeuchi, T. Morimae, and M. Hayashi, Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements, Sci. Rep. **9**, 13585 (2019).

[13] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations, Phys. Rev. Lett. **117**, 080501 (2016).

[14] O. Gühne, M. Cuquet, F. E. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, and C. Macchiavello, Entanglement and nonclassical properties of hypergraph states, J. Phys. A: Math. Theor. **47**, 335303 (2014).

[15] M. Gachechiladze, C. Budroni, and O. Gühne, Extreme Violation of Local Realism in Quantum Hypergraph States, Phys. Rev. Lett. **116**, 070401 (2016).

[16] M. Levin and Z.-C. Gu, Braiding statistics approach to symmetry-protected topological phases, Phys. Rev. B **86**, 115109 (2012).

[17] B. Yoshida, Topological phases with generalized global symmetries, Phys. Rev. B **93**, 155131 (2016).

[18] A. Hamma, R. Ionicioiu, and P. Zanardi, Bipartite entanglement and entropic boundary law in lattice spin systems, Phys. Rev. A **71**, 022315 (2005).

[19] C. Chamon, A. Hamma, and E. R. Mucciolo, Emergent Irreversibility and Entanglement Spectrum Statistics, Phys. Rev. Lett. **112**, 240501 (2014).

[20] D. Shaffer, C. Chamon, A. Hamma, and E. R. Mucciolo, Irreversibility and entanglement spectrum statistics in quantum circuits, J. Stat. Mech. (2014) P12007.

[21] Z.-C. Yang, A. Hamma, S. M. Giampaolo, E. R. Mucciolo, and C. Chamon, Entanglement complexity in quantum many-body dynamics, thermalization, and localization, Phys. Rev. B **96**, 020408(R) (2017).

[22] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).

[23] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, Phys. Rev. A **80**, 012304 (2009).

[24] B. Collins and I. Nechita, Random matrix techniques in quantum information theory, J. Math. Phys. **57**, 015215 (2016).

[25] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys. **14**, 113011 (2012).

[26] V. Veitch, S. H. Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New J. Phys. **16**, 013009 (2014).

[27] P. Hayden and J. Preskill, Black holes as mirrors: Quantum information in random subsystems, J. High Energy Phys. 09 (2007) 120.

[28] D. A. Roberts and B. Yoshida, Chaos and complexity by design, J. High Energy Phys. 4 (2017) 121.

[29] A. Ambainis and J. Emerson, Quantum t-designs: t-wise independence in the quantum world, in *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (IEEE, Piscataway, NJ, 2007), pp. 129–140.

[30] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. **48**, 052104 (2007).

[31] M. Ghio, D. Malpetti, M. Rossi, D. Bruß, and C. Macchiavello, Multipartite entanglement detection for hypergraph states, J. Phys. A: Math. Theor. **51**, 045302 (2018).

[32] X.-Y. Chen and L. Wang, Locally inequivalent four-qubit hypergraph states, J. Phys. A: Math. Theor. **47**, 415304 (2014).

[33] M. Gachechiladze, N. Tsimakuridze, and O. Gühne, Graphical description of unitary transformations on hypergraph states, J. Phys. A: Math. Theor. **50**, 19LT01 (2017).

[34] N. Tsimakuridze and O. Gühne, Graph states and local unitary transformations beyond local Clifford operations, J. Phys. A: Math. Theor. **50**, 195302 (2017).
[35] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, Local unitary symmetries of hypergraph states, J. Phys. A: Math. Theor. **48**, 095301 (2015).
[36] T. Morimae, Y. Takeuchi, and M. Hayashi, Verification of hypergraph states, Phys. Rev. A **96**, 062321 (2017).
[37] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, Phys. Rev. Applied **12**, 054047 (2019).
[38] B. Collins, I. Nechita, and K. Życzkowski, Random graph states, maximal flow and Fuss–Catalan distributions, J. Phys. A: Math. Theor. **43**, 275303 (2010).
[39] D. Gottesman, The Heisenberg representation of quantum computers, arXiv:quant-ph/9807006.
[40] Y. Shi, Both Toffoli and controlled-not need little help to do universal quantum computation, arXiv:quant-ph/0205115.
[41] R. Islam, R. Ma, P. M. Preiss, M. Eric Tai, A. Lukin, M. Rispoli, and M. Greiner, Measuring entanglement entropy in a quantum many-body system, Nature (London) **528**, 77 (2015).
[42] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, Probing Rényi entanglement entropy via randomized measurements, Science **364**, 260 (2019).
[43] A. Hamma, S. Santra, and P. Zanardi, Quantum Entanglement in Random Physical States, Phys. Rev. Lett. **109**, 040502 (2012).
[44] R. A. Low, Pseudo-randomness and learning in quantum computation, Ph.D. thesis, University of Bristol, UK, 2010.
[45] G. Tóth and J. J. García-Ripoll, Efficient algorithm for multiqudit twirling for ensemble quantum computation, Phys. Rev. A **75**, 042311 (2007).
[46] K. Zyczkowski and H.-J. Sommers, Induced measures in the space of mixed quantum states, J. Phys. A: Math. Gen. **34**, 7111 (2001).
[47] G. Smith and D. Leung, Typical entanglement of stabilizer states, Phys. Rev. A **74**, 062314 (2006).
[48] H. Zhu, R. Kueng, M. Grassl, and D. Gross, The Clifford group fails gracefully to be a unitary 4-design, arXiv:1609.08172.
[49] Y. Nakata, M. Koashi, and M. Murao, Generating a state t-design by diagonal quantum circuits, New J. Phys. **16**, 053043 (2014).
[50] Y. Nakata and M. Murao, Diagonal quantum circuits: Their computational power and applications, Eur. Phys. J. **129**, 152 (2014).
[51] L. Leone, S. F. E. Oliviero, Y. Zhou, and A. Hamma, Quantum chaos is quantum, Quantum **5**, 453 (2021).
[52] A. Hamma, S. Santra, and P. Zanardi, Ensembles of physical states and random quantum circuits on graphs, Phys. Rev. A **86**, 052324 (2012).
[53] O. Dahlsten and M. B. Plenio, Exact entanglement probability distribution of bi-partite randomised stabilizer states, Quantum Inf. Comput. **6**, 527 (2006).
[54] P. Hayden, D. W. Leung, and A. Winter, Aspects of generic entanglement, Commun. Math. Phys. **265**, 95 (2006).
[55] V. F. Kolchin, *Random Graphs*, Encyclopedia of Mathematics and its Applications (Cambridge University Press, Cambridge, 1998).
[56] J. Iaconis, Quantum state complexity in computationally tractable quantum circuits, PRX Quantum **2**, 010329 (2021).
[57] F. E. S. Steinhoff, C. Ritz, N. I. Miklin, and O. Gühne, Qudit hypergraph states, Phys. Rev. A **95**, 052340 (2017).
[58] F.-L. Xiong, Y.-Z. Zhen, W.-F. Cao, K. Chen, and Z.-B. Chen, Qudit hypergraph states and their properties, Phys. Rev. A **97**, 012323 (2018).
[59] J.-Y. Wu, M. Rossi, H. Kampermann, S. Severini, L. C. Kwek, C. Macchiavello, and D. Bruß, Randomized graph states and their entanglement properties, Phys. Rev. A **89**, 052335 (2014).
[60] Otfried Gühne, G. Toth, and H. J. Briegel, Multipartite entanglement in spin chains, New J. Phys. **7**, 229 (2005).
[61] Y. Zhou, Q. Zhao, X. Yuan, and X. Ma, Detecting multipartite entanglement structure with minimal resources, npj Quantum Inf. **5**, 83 (2019).
[62] L. Leone, S. F. Oliviero, and A. Hamma, Rényi Entropy of Magic, Phys. Rev. Lett. **128**, 050402 (2022).
[63] S. Zhou, Z. Yang, A. Hamma, and C. Chamon, Single T gate in a Clifford circuit drives transition to universal entanglement spectrum statistics, SciPost Phys. **9**, 087 (2020).
[64] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates, arXiv:2002.09524.
[65] S. H. Shenker and D. Stanford, Multiple shocks, J. High Energy Phys. 12 (2014) 046.
[66] Z.-W. Liu and A. Winter, Many-body quantum magic, PRX Quantum **3**, 020333 (2022).
[67] M. Hein, J. Eisert, and H. J. Briegel, Multiparty entanglement in graph states, Phys. Rev. A **69**, 062311 (2004).