Supplementary Material: A Toy Model of Boundary States with Spurious Topological Entanglement Entropy

Kohtaro Kato[1] and Fernando G.S.L. Brandão[1,2]

[1] *Institute for Quantum Information and Matter*
California Institute of Technology, Pasadena, CA 91125, USA
[2] *Amazon Web Services, AWS Center for Quantum Computing, Pasadena, CA*

I. OPERATOR ALGEBRA QUANTUM ERROR CORRECTION

In this section, we summarize the theory of operator-algebra quantum error correction (OAQEC) [1]. Formally, we say that a set $\mathcal{S} \subset \mathcal{B}(\mathcal{H})$ on a code subspace $\mathcal{H}_C = P_C\mathcal{H}$ ($P_C = I$ in the main text) is correctable for $\mathcal{E}$ if there exists a CPTP-map (also called a channel) $\mathcal{R}$ such that

$$P_C\left(\mathcal{R}\circ\mathcal{E}\right)^\dagger(X)P_C = P_C X P_C\,, \forall X \in \mathcal{S}\,. \tag{S.1}$$

We will call $\mathcal{R}$ *recovery map.* This is equivalent to say we require the information of not the whole code space but particular observables are preserved:

$$\mathrm{Tr}(X\rho) = \mathrm{Tr}\left(X(\mathcal{R}\circ\mathcal{E})(\rho)\right)\ \forall X \in S, \forall \rho \in \mathcal{S}(\mathcal{H}_C)\,. \tag{S.2}$$

This is in contrast to the standard (or subsystem) QEC in which we require that all information (= full density matrix, i.e. the expectation value for all observables) of the logical state is recoverable. A main result of Ref. [1] is the following:

Proposition S.1. *[1] Let $\mathcal{A}$ be a subalgebra of $\mathcal{B}(P_C\mathcal{H})$. Then, $\mathcal{A}$ is correctable for $\mathcal{E}$ on $\mathcal{H}_C$ if, and only if,*

$$[P_C E_a^\dagger E_b P_C, X] = 0\ \forall X \in \mathcal{A}, \forall a, b \tag{S.3}$$

i.e. the algebra $Alg(\{P_C E_a^\dagger E_b P_C\}_{a,b})$ is a subalgebra of $\mathcal{A}'$, where $\mathcal{A}'$ is the commutant of $\mathcal{A}$.

In other words, any subalgebra of $Alg(\{P_C E_a^\dagger E_b P_C\}_{a,b})'$ is correctable. For a given code subspace $\mathcal{H}_C$ and an error $\mathcal{E}$, we define the *correctable algebra* of $\mathcal{E}$ by

$$\mathcal{A}_\mathcal{E} := Alg(\{P_C E_a^\dagger E_b P_C\}_{a,b})' \tag{S.4}$$

$$= \left\{X \in \mathcal{B}(\mathcal{H}_C) \mid [P_C E_a^\dagger E_b P_C, X] = 0\ \forall a, b\right\}\,. \tag{S.5}$$

This is a unital C^*-subalgebra of $\mathcal{B}(\mathcal{H}_C)$.

A. A complementary relation for OAQEC

In the standard QEC, we have a complementary relation implied by the no-cloning theorem: if one can exactly recover a logical state from a noise channel, then one cannot learn any information about the logical state from the output, i.e. the complimentary channel of the noise destroys all information about the logical state. In OAQEC, we can require to recover only partial information from noise. Hence, it might be possible to learn something from the outputs of the complementary channel.

Suppose $\{E_a\}$ are Kraus operators of $\mathcal{E}$. Then, we have a Steinespring isometry $V = \sum_a E_a \otimes |\phi_a\rangle$ for an orthonormal basis $\{|\phi_a\rangle\}$ on $\mathcal{H}_E$. The complementary channel $\mathcal{E}^c$ has a Kraus representation by $\{F_a\}$, defined as

$$F_a = \sum_b |\phi_b\rangle\langle a|E_b\,, \tag{S.6}$$

where $\{|a\rangle\}$ is an orthonormal basis of $\mathcal{H}_B$. The correctable algebra of $\mathcal{E}^c$ is spanned by operators commuting with all

$$P_C F_a^\dagger F_b P_C = P_C\mathcal{E}^\dagger(|a\rangle\langle b|)P_C \tag{S.7}$$

which span $P_C(Im\mathcal{E}^\dagger)P_C$. Hence, $\mathcal{A}_{\mathcal{E}^c} = Alg[(P_C(Im\mathcal{E}^\dagger)P_C)]'$.

Any $X \in \mathcal{A}_\mathcal{E}$ satisfies $X = P_C\mathcal{E}^\dagger \circ \mathcal{R}^\dagger(X)P_C$, and therefore $\mathcal{A}_\mathcal{E} \subset \mathcal{A}'_{\mathcal{E}^c}$: the correctable algebra of a channel is in the commutant of the correctable algebra of the complementary channel. Information of operators in $\mathcal{A}_\mathcal{E} \cap \mathcal{A}_{\mathcal{E}^c}$ can be extracted from the outputs of both channels and must be in the centers of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_{\mathcal{E}^c}$. For example, if $\mathcal{A}_\mathcal{E} = \mathcal{B}(\mathcal{H}_C)$, then $\mathcal{A}_{\mathcal{E}^c} \subset \mathcal{B}(\mathcal{H}_C)' = \mathbb{C}I$ which corresponds to the complementary relation for the standard QEC.

II. MPS CLASSIFICATION OF $G_1 \times G_2$ SPT PHASES

Here we briefly summarize the MPS classification of 1D SPT phases under on-site $G = G_1 \times G_2$ symmetry [2, 3] to be self-contained. Consider a MPS defined as

$$|\psi_N\rangle = \sum_{\mathbf{i},\mathbf{j}} \mathrm{Tr}\left(A^{i_1j_1}A^{i_2j_2}\dots A^{i_Nj_N}\right)|i_1i_2\dots i_N\rangle_R|j_1j_2\dots j_N\rangle_R\,, \tag{S.8}$$

where $i_k, j_k = 1,\dots,d$, $\forall k$ and A^{ij} is a $D \times D$ matrix. Consider a finite group $G_1 \times G_2$ with a unitary representation $(g_1, g_2) \mapsto U(g_1) \otimes U'(g_2)$ acting on $\mathbb{C}^d \otimes \mathbb{C}^d$. G_1 (G_2) then acts on R (R^c) as an on-site global symmetry $U(g_1)^{\otimes N}$ $\left(U'(g_2)^{\otimes N}\right)$. Suppose $|\psi_N\rangle$ is a symmetric state

$$\left(U(g_1) \otimes U'(g_2)\right)^{\otimes N}|\psi_N\rangle = |\psi_N\rangle\,, \quad \forall (g_1, g_2) \in G_1 \times G_2 \tag{S.9}$$

for all N (up to a global phase). This condition is shown to be equivalent to the following conditions for the single site:

$$\sum_k U(g_1)_{ik}A^{kj} = e^{i\theta(g_1)}V(g_1)A^{ij}V(g_1)^\dagger\,, \quad \sum_k U'(g_2)_{jk}A^{ik} = e^{i\theta(g_2)}V(g_2)A^{ij}V(g_2)^\dagger\,. \tag{S.10}$$

Here, $V(g_1)$ and $V(g_2)$ are unitary consisting a projective representation of $G_1 \times G_2$ in together.

1D SPT phase under symmetry G is classified by the second group cohomology $H^2(G; U(1))$ which is a group of the equivalence class $[\Theta]$ of the phase factor $\Theta : G \times G \to U(1)$. Each factor Θ is defined from the projective representation via

$$V(gh) = e^{i\Theta(g,h)}V(g)V(h) \tag{S.11}$$

up to the equivalence relation

$$\Theta(g,h) \sim \Theta(g,h) + \theta(gh) - \theta(g) - \theta(h) \mod 2\pi\,. \tag{S.12}$$

The symmetric state $|\psi_N\rangle$ is said to be in a non-trivial G SPT phase if the projective representation $V(g)$ is associated to a non-trivial element in the second cohomology class. In particular, in this paper, we employ the following definition used in Ref. [3]:

Definition S.2. *We say symmetric MPS $|\psi_N\rangle$ is in a non-trivial $G_1 \times G_2$ SPT phase if there is $(g_1, g_2) \in G_1 \times G_2$ such that*

$$[V(g_1), V(g_2)] \neq 0\,. \tag{S.13}$$

This only happens for non-trivial projective representation since $[U(g_1), U'(g_2)] = 0$.

III. PROOFS OF THE THEOREMS

A. Proof of Proposition 1

proof. For any CPTP-map $\mathcal{E}$, the corresponding family $\{\rho^{(n)}\}$ satisfies

$$\begin{aligned} I(A_1:C_1|B_1)_{(1)} &= I(A_1:B_1C_1)_{(1)} - I(A_1:B_1)_{(1)} \\ &\geq I(A_1:B_1B_2C_2)_{(2)} - I(A_1:B_1)_{(1)} \\ &= I(A_1:B_1B_2C_2)_{(2)} - I(A_1:B_1)_{(2)} \\ &= I(A_1:C_2|B_1B_2)_{(2)} + I(A_1:B_2|B_1)_{(2)} \\ &\geq I(A_1:C_2|B_1B_2)_{(2)} . \end{aligned}$$

The first inequality follows from the data-processing inequality [4] and Eq. (3), and the second inequality follows from the strong subadditivity [5]. Equality holds when the both inequalities are saturated. The first inequality is saturated if, and only if, [4]:

$$I(A_1:B_1C_1)_{(1)} = I(A_1:B_1B_2C_2)_{(2)} . \tag{S.14}$$

The second inequality saturated if and only if $I(A_1:B_2|B_1)_{(2)} = 0$, i.e.

$$S^{(1)}_{A_1} + S^{(1)}_{B_1} - S^{(1)}_{A_1B_1} = S^{(2)}_{A_1} + S^{(2)}_{B_1B_2} - S^{(2)}_{A_1B_1B_2} ,$$

which is equivalent to Eq. (7) by $\rho^{(1)}_{A_1B_1} = \rho^{(2)}_{A_1B_1}$. Since $\rho^{(1)}_{A_1B_1E_1C_1}$ and $\rho^{(2)}_{A_1B_1B_2E_1E_2C_2}$ are pure states, the above equality is equivalent to

$$-S^{(1)}_{A_1} + S^{(1)}_{A_1E_1C_1} - S^{(1)}_{E_1C_1} = -S^{(2)}_{A_1} + S^{(2)}_{A_1E_1E_2C_2} - S^{(2)}_{E_1E_2C_2}$$

after subtracting $2S^{(1)}_{A_1} = 2S^{(2)}_{A_1}$, which is Eq. (8). Therefore, $I(A_1:C_1|B_1)_{(1)} = I(A_1:C_2|B_1B_2)_{(2)}$ if and only if Eqs. (6,8) holds. The same argument applies to $I(A_1:C_1|E_1)_{(1)} = I(A_1:C_2|E_1E_2)_{(2)}$.

We now show Eqs. (6,8) imply

$$\begin{aligned} I(A_1:B_1C_1)_{(1)} &= I(A_1:B_1\dots B_nC_n)_{(n)} , \forall n , \\ I(A_1:E_1C_1)_{(1)} &= I(A_1:E_1\dots E_nC_n)_{(n)} , \forall n . \end{aligned}$$

The converse is clear. Since $\rho^{(2)} = \tilde{\mathcal{E}}_{C_1\to B_2C_2}(\rho^{(1)})$, Eq. (6) implies there exists a *recovery map* $\hat{\mathcal{R}}_{B_1B_2C_2\to C_1}$ such that

$$\begin{aligned} \hat{\mathcal{R}}_{B_1B_2C_2\to C_1}(\rho^{(2)}) &= \hat{\mathcal{R}}_{B_1B_2C_2\to C_1} \circ \tilde{\mathcal{E}}_{C_1\to B_2C_2}(\rho^{(1)}) &\text{(S.15)} \\ &= \rho^{(1)} . &\text{(S.16)} \end{aligned}$$

By definition, we can write $\rho^{(3)}$ as $\tilde{\mathcal{E}}^L_{A_3\to A_1B_1}(\rho^{(2)}_{A_3B_2B_3C_3})$, where $\tilde{\mathcal{E}}^L_{A_3\to A_1B_1}(\cdot) := \mathcal{E}_{A_2A_3\to B_1}(\omega_{A_1A_2}\otimes\cdot)$ is a CPTP-map (here we used the notation $\rho^{(2)}_{A_3B_2B_3C_3}$ for the state after shifting $\rho^{(2)}_{A_1B_1B_2C_2}$). From this expression, Eq. (S.16) implies

$$\begin{aligned} \hat{\mathcal{R}}_{B_2B_3C_3\to C_2}(\rho^{(3)}) &= \hat{\mathcal{R}}_{B_2B_3C_3\to C_2} \circ \tilde{\mathcal{E}}_{C_2\to B_3C_3}(\rho^{(2)}) &\text{(S.17)} \\ &= \tilde{\mathcal{E}}^L \circ \hat{\mathcal{R}}_{B_2B_3C_3\to C_2} \circ \tilde{\mathcal{E}}_{C_2\to B_3C_3}(\rho^{(1)}) &\text{(S.18)} \\ &= \tilde{\mathcal{E}}^L(\rho^{(1)}) &\text{(S.19)} \\ &= \rho^{(2)} . &\text{(S.20)} \end{aligned}$$

This is equivalent to

$$I(A_1:B_1B_2C_2)_{(2)} = I(A_1:B_1B_2B_3C_3)_{(3)} . \tag{S.21}$$

The same argument works for $n > 3$ and under exchanging of $B \leftrightarrow E$. Therefore Eqs. (6,8) are equivalent to Eq. (5), which completes the proof. □

B. Proof of Proposition 2

Proof. By definition, it is clear that $\mathcal{A}_{\tilde{\mathcal{E}}} \supset \mathcal{A}_{\tilde{\mathcal{E}}^{(n)}}$ (information which is recoverable after an additional noise is recoverable without the noise). Suppose that Eq. (5) holds. Then, as shown in the proof of Prop. 1, there exists a recovery map associated with the data-processing inequality such that

$$\hat{\mathcal{R}}_{B_1B_2C_2\to B_1C_1} \circ \tilde{\mathcal{E}}^{(2)}_{C_0\to B_1B_2C_2} = \tilde{\mathcal{E}}^{(1)}_{C_0\to B_1C_1} . \tag{S.22}$$

There also exists another recovery map $\mathcal{R}$ associated with OAQEC, such that

$$(\tilde{\mathcal{E}}^{(1)}_{C_0\to B_1C_1})^\dagger \circ \mathcal{R}^\dagger_{B_1C_1\to C_0}(X_{C_0}) = X_{C_0} \tag{S.23}$$

for any $X_{C_0} \in \mathcal{A}_{\tilde{\mathcal{E}}}$. By combining these two recovery maps together, we obtain that

$$\begin{aligned}(\tilde{\mathcal{E}}^{(1)}_{C_0\to B_1C_1})^\dagger \circ \mathcal{R}^\dagger_{B_1C_1\to C_0}(X_{C_0}) &= (\tilde{\mathcal{E}}^{(2)}_{C_0\to B_1B_2C_2})^\dagger \circ \hat{\mathcal{R}}^\dagger_{B_1B_2C_2\to B_1C_1} \circ \mathcal{R}^\dagger_{B_1C_1\to C_0}(X_{C_0}) \\ &= X_{C_0} .\end{aligned} \tag{S.24}$$

Hence $\mathcal{R}\circ\hat{\mathcal{R}}$ can be regarded as the recovery map (in the sense of OAQEC) against the noise $\tilde{\mathcal{E}}^{(2)}$. Therefore, any $X_{C_0} \in \mathcal{A}_{\tilde{\mathcal{E}}}$ is recoverable after applying $\tilde{\mathcal{E}}^{(2)}$ and thus $X_{C_0} \in \mathcal{A}_{\tilde{\mathcal{E}}^{(2)}}$. By repeating the same argument for all n and the complementary channel, we complete the proof. □

C. Proof of Proposition 4

Proof. It is always true that $\mathcal{A}_{\mathcal{E}^c} = Alg(Im\mathcal{E}^\dagger)'$. If $\mathcal{E}$ satisfies the complementary recovery, $\mathcal{A}_{\mathcal{E}} = \mathcal{A}'_{\mathcal{E}^c} = Alg(Im\mathcal{E}^\dagger)$. Therefore, $Im\mathcal{E}^\dagger \subset Im\mathcal{P}^\dagger_{\mathcal{A}_{\mathcal{E}}}$ and Eq. (15) holds. Conversely, if $Im\mathcal{E}^\dagger \subset Im\mathcal{P}^\dagger_{\mathcal{A}_{\mathcal{E}}}$, then $Alg(Im\mathcal{E}^\dagger) \subset \mathcal{A}_{\mathcal{E}}$ and therefore $\mathcal{A}'_{\mathcal{E}^c} \subset \mathcal{A}_{\mathcal{E}}$. This completes the proof since $\mathcal{A}_{\mathcal{E}} \subset \mathcal{A}'_{\mathcal{E}^c}$ always holds. □

D. Proof of Theorem 6

Proof. Recall that we have shown that $I(A_1 : B_1C_1)_{(1)} = I(A_1 : B_1B_2C_2)_{(2)}$ (and that of E) is sufficient for Eq. (5). $\mathcal{A}_{\tilde{\mathcal{E}}} = \mathcal{A}_{\tilde{\mathcal{E}}^{(2)}}$ (we assume this w.l.o.g.) implies that there exists $\mathcal{R}$ such that $\mathcal{R}\circ\tilde{\mathcal{E}}^{(2)}$ act as the identity map on $\mathcal{A}_{\tilde{\mathcal{E}}}$. It holds that $\tilde{\mathcal{E}}\circ\mathcal{R}\circ\tilde{\mathcal{E}}^{(2)} = \tilde{\mathcal{E}}\circ\mathcal{P}_{\mathcal{A}_{\tilde{\mathcal{E}}}}\circ\mathcal{R}\circ\tilde{\mathcal{E}}^{(2)} = \tilde{\mathcal{E}}$, so we can set $\hat{\mathcal{R}} := \tilde{\mathcal{E}}\circ\mathcal{R}$. This completes the proof by the data-processing inequality.

To calculate CMI, let us show $I(A_1 : B_1C_1)_{(1)} = I(A_1 : A_2)_{\omega_D^{\mathcal{A}}}$. Since $\tilde{\mathcal{E}}\circ\mathcal{P}_{\mathcal{A}} = \tilde{\mathcal{E}}$ by dual complementarity, we have $\tilde{\mathcal{E}}_{A_2\to B_1C_1}(\omega^{\mathcal{A}}_{DA_1A_2}) = \rho^{(1)}_{A_1B_1C_1}$. By the monotonicity of the mutual information under local CPTP-maps, this implies $I(A_1 : B_1C_1)_{(1)} \leq I(A_1 : A_2)_{\omega_D^{\mathcal{A}}}$. By applying the recovery map of OAQEC $\mathcal{R}_{B_1C_1\to A_2}$, we also have $\mathcal{P}_{\mathcal{A}}\circ\mathcal{R}_{B_1C_1\to A_2}(\rho^{(1)}_{A_1B_1C_1}) = \omega^{\mathcal{A}}_D$, therefore $I(A_1 : B_1C_1)_{(1)} \geq I(A_1 : A_2)_{\omega_D^{\mathcal{A}}}$. The same arguments hold for the complementary channel and $\mathcal{B}$, and thus we have

$$\begin{aligned}I(A_1 : C_1|B_1)_{(1)} &= I(A_1 : B_1C_1)_{(1)} - I(A_1 : B_1)_{(1)} &\text{(S.25)}\\ &= I(A_1 : B_1C_1)_{(1)} + I(A_1 : E_1C_1)_{(1)} - 2S(A_1) &\text{(S.26)}\\ &= I(A_1 : A_2)_{\omega_D^{\mathcal{A}}} + I(A_1 : A_2)_{\omega_D^{\mathcal{B}}} - 2S(A_1) &\text{(S.27)}\\ &= I_c(A_1\rangle A_2)_{\omega_D^{\mathcal{A}}} + I_c(A_1\rangle A_2)_{\omega_D^{\mathcal{B}}} , &\text{(S.28)}\end{aligned}$$

where $\omega_D^{\mathcal{A}} := (\mathrm{id}\otimes\mathcal{P}_{\mathcal{A}})(|\omega_D\rangle\langle\omega_D|)$ and $\omega_D^{\mathcal{B}} := (\mathrm{id}\otimes\mathcal{P}_{\mathcal{B}})(|\omega_D\rangle\langle\omega_D|)$. Here $I_c(A\rangle B) := S(B) - S(AB)$ is the coherent information [6].

The correctable algebras have decompositions

$$\mathcal{A} \cong \bigoplus_k M_{n_k}(\mathbb{C})\otimes I_{n'_k} , \quad \mathcal{B} \cong \bigoplus_l M_{m_l}(\mathbb{C})\otimes I_{m'_l}, \tag{S.29}$$

where $\sum_k n_k n'_k = \sum_l m_l m'_l = D$. From these representations, it turns out that [7]

$$\omega_D^{\mathcal{A}} = \bigoplus_k p_k \frac{1}{n'_k} (I_{n_k})_{A_1} \otimes (\omega_{n_k})_{A_1 A_2} \otimes (\rho_{n'_k})_{A_2} \tag{S.30}$$

with $p_k = \frac{n_k n'_k}{D}$ and some fixed states $\{\rho_{n_k}\}$. By simple calculations we have

$$I_c(A_1 \rangle A_2)_{\omega_D^{\mathcal{A}}} = S(A_2)_{\omega_D^{\mathcal{A}}} - S(A_1 A_2)_{\omega_D^{\mathcal{A}}} \tag{S.31}$$

$$= \sum_k p_k \log n_k - \sum_k p_k \log n'_k \tag{S.32}$$

$$= \sum_k p_k \log \frac{n_k}{n'_k} . \tag{S.33}$$

Therefore, by applying the same argument for $\mathcal{B}$,

$$I(A_1 : C_1 | B_1)_{(1)} = \sum_k p_k \log \frac{n_k}{n'_k} + \sum_l q_l \log \frac{m_l}{m'_l} \tag{S.34}$$

holds with $q_l = \frac{m_l m'_l}{D}$. One may obtain more detailed formula by employing $\mathcal{B}' \subset \mathcal{A}$. The algebras satisfy $\mathcal{A} = \mathcal{B}'$ if and only if $|\{k\}| = |\{l\}|$, $p_k = q_k$, $m_k = n'_k$ and $m'_k = n_k$. This leads $I(A_1 : C_1 | B_1)_{(1)} = 0$.

E. Proof of Theorem 7

In this section, we prove Theorem 7. We start from deriving the group structure of tensor product logical unitaries. We then reveal a sufficient condition to imply the existence of SPT phase from the non-zero value of CMI. We finally show that all stabilizer states satisfy the sufficient condition.

Recall that it is necessary to have a tensor product logical operator for $\phi^{(n)}$ to be in a SPT phase (under on-site symmetry). Let $\mathcal{G}_{\mathcal{A}} := \mathcal{U}(\mathcal{L}_{\mathcal{A}}) \cap (\mathcal{B}(\mathcal{H}_B) \otimes \mathcal{B}(\mathcal{H}_C))$ be the set of all tensor product logical operators. Since $\mathcal{L}_{\mathcal{A}}$ is the pre-image of $*$-homomorphism, it is a finite-dimensional C^*-algebra and therefore $\mathcal{U}(\mathcal{L}_{\mathcal{A}})$ is a compact and connected Lie group. $\mathcal{G}_{\mathcal{A}}$ is then a Lie subgroup of $\mathcal{U}(\mathcal{L}_{\mathcal{A}})$.

Proposition S.3. *Define $\mathcal{C}_{\mathcal{A}}$ as the subgroup of logical operators*

$$\mathcal{C}_{\mathcal{A}} = \{U_B \otimes I_C, U_B \in \mathcal{L}_{\mathcal{A}}\} . \tag{S.35}$$

$\mathcal{C}_{\mathcal{A}}$ is the identity component of $\mathcal{G}_{\mathcal{A}}$.

Proof. Suppose $U = e^{itO} \in \mathcal{U}(\mathcal{L}_{\mathcal{A}})$. Then $\tilde{\mathcal{E}}^\dagger(e^{itO}) = e^{it\tilde{\mathcal{E}}^\dagger(O)} \in \mathcal{U}(\mathcal{A})$ ($\tilde{\mathcal{E}}^\dagger$ is a $*-$homomorphism) and therefore $\tilde{\mathcal{E}}^\dagger(O) \in \mathcal{A}$, i.e. $O \in \mathcal{L}_{\mathcal{A}}$. The Lie algebra of $\mathcal{U}(\mathcal{L}_{\mathcal{A}})$, which we denote by $\mathfrak{u}(\mathcal{L}_{\mathcal{A}})$, is therefore Hermitian logical operator on BC. Furthermore, $\mathfrak{u}(\mathcal{L}_{\mathcal{A}})$ should not contain operators like $I_B \otimes O_C$ for $O_C \neq I_C$, since the input of $\tilde{\mathcal{E}}$ and C is uncorrelated. Therefore,

$$\mathfrak{u}(\mathcal{L}_{\mathcal{A}}) = \left\{ L_B \otimes I_C \, , \, L_{BC} \in \mathcal{L}_{\mathcal{A}} \middle| L_B = L_B^\dagger \, , \, L_{BC} = L_{BC}^\dagger \right\} , \tag{S.36}$$

where $\mathrm{Tr}_B L_{BC} = \mathrm{Tr}_C L_{BC} = 0$. The Lie algebra of $\mathcal{G}_{\mathcal{A}}$ is a subalgebra of $\mathfrak{u}(\mathcal{L}_{\mathcal{A}})$. For any non-local term L_{BC}, $e^{itL_{BC}}$ cannot be a tensor product for all $t \in \mathbb{R}$. Therefore, the identity component is given by $\{e^{itL_B \otimes I_C}\}$, which is Eq. (53). □

A well-known result on Lie group implies that the identity component is a closed normal subgroup and the quotient group $\mathcal{G}_{\mathcal{A}}/\mathcal{C}_{\mathcal{A}}$ is a discrete group (see e.g. Ref. [8] and references therein for more details). Since $\mathcal{G}_{\mathcal{A}}$ is compact, we obtain the following.

Corollary S.4. *$\mathcal{G}_{\mathcal{A}}/\mathcal{C}_{\mathcal{A}}$ is a finite group.*

The exactly same arguments holds for $\mathcal{G}_{\mathcal{B}}$ and $\mathcal{C}_{\mathcal{B}}$. We denote an abstract group isomorphic to $\mathcal{G}_{\mathcal{A}}/\mathcal{C}_{\mathcal{A}}$ by G_1 and similarly use G_2 for $\mathcal{G}_{\mathcal{B}}/\mathcal{C}_{\mathcal{B}}$. Under dual complementarity, we have $\mathcal{C}_{\mathcal{A}} = \mathcal{U}(\mathcal{L}_{\mathcal{B}'})$. Let $\hat{\mathcal{G}}_{\mathcal{A}} \leqslant \mathcal{U}(\mathcal{A})$ be a subgroup of unitaries that have logical operators in $\mathcal{G}_{\mathcal{A}}$. It is easy to check $\mathcal{U}(\mathcal{B}') \lhd \hat{\mathcal{G}}_{\mathcal{A}}$ and we obtain $\hat{\mathcal{G}}_{\mathcal{A}}/\mathcal{U}(\mathcal{B}') \cong G_1$ as well. For any $g \in G_1$ there exists $V(g) \neq I \in \hat{\mathcal{G}}_{\mathcal{A}}$ such that the corresponding logical operator is in the form $U_B \otimes U_C(g)$ with unitaries $U_B, U_C(g) \neq I_B, I_C$. $U_C(g)$ is independent of particular choice of element from the equivalence class $[V(g)]$, which has one-to-one correspondence with g by definition.

If G_1 represents the physical symmetry of the state, then $U_C(g) \in [V(g)]$ for any $g \in G_1$ by $C \cong A$. This guarantees that we obtain tensor product logical operators for arbitrary length n. However, in general there is no guarantee that $U_C(g)$ again has a tensor product logical operator. Actually, the non-trivial example shown in the main text violates this condition. We denote by H_1 the subgroup of G_1 such that $U_C(h) \in [V(h)]$ for any $h \in H_1$.

A simple situation is that $H_1 = G_1$. However, the group G_1 can still be small compare to $\mathcal{A}$. To avoid this problem, we further assume $\hat{\mathcal{G}}_{\mathcal{A}}$ spans the whole correctable algebra. We show these two conditions are strong enough to obtain a non-trivial SPT phase from the value of CMI:

Proposition S.5. *Let V be an isometry satisfying all of the following properties:*

- *dual complementarity*
- $H_1 = G_1$, $H_2 = G_2$
- $Alg(\hat{\mathcal{G}}_{\mathcal{A}}) = \mathcal{A}$, $Alg(\hat{\mathcal{G}}_{\mathcal{B}}) = \mathcal{B}$

Then the MPS generated by V is in a non-trivial $G_1 \times G_2$ SPT phase after corse-graining a constant number of sites if, and only if,

$$I(A_1 : C_n|B_n)_{(n)} > 0, \ \forall n.$$

Proof. Since $H_1 = G_1$, any $V(g)$ has a logical operator in the form $U_B \otimes U_C(g)$ with $U_C(g) \in \hat{\mathcal{G}}_{\mathcal{A}}$. The equivalence class of unitaries $U_C(g)$ again consists a group isomorphic to G_1. It is clear that $f : g \mapsto [U_C(g)]$ is surjective from its definition. To show it is also injective, suppose that $U_C(g) = U_C(g')$ for $g, g' \in G_1$. Then we can find logical operators of $V(g)V(g')^\dagger$ in the form $U_B \otimes I_C$, and thus $V(g)V(g')^\dagger \in \mathcal{U}(\mathcal{B}')$. This implies $[V(g)] = [V(g')] \Leftrightarrow g = g'$. Moreover, if $U_C(g) = VU_C(g')$ for $V \in \mathcal{U}(\mathcal{B}')$, then $g = g'$. This is because we can apply $\mathcal{V}_{C\to E'B'C'}$ and then logical operators of $U_C(g)$ and $VU_C(g')$ has the same unitary on C', so the injectivity discussed before applies to this case as well. Therefore $f : g \mapsto [U_C(g)]$ is a well-defined group isomomorphism.

Both $[V(g)]$ and $[U_C(g)]$ form $\hat{\mathcal{G}}_{\mathcal{A}}/\mathcal{U}(\mathcal{B}')$, but the labeling could be different, i.e. it might be true that $[V(g)] = [U_C(g')]$. The correspondence between $[V(g)]$ and $[U(g)]$ is a permutation (or automorphism) $Per : g' \mapsto g$ on G_1. Therefore, there exists a constant $m \in \mathbb{N}$ such that $(Per)^m = id_{G_1}$. By coarse-graining m channels, we obtain the desired relation

$$\mathcal{V}_{A_2\to B_m E_m C}(V(g)|\psi\rangle_{A_2}) = (U_{B_m}(g) \otimes V(g))\mathcal{V}_{A_2\to B_m E_m C}(|\psi\rangle_{A_2}) \ \forall g \in G_1 \tag{S.37}$$

with a unitary $U_{B_m}(g)$, where B_m and E_m are the coarse-grained systems. These arguments are also applicable for G_2, with possibly different coarse-graining scale m'. If $m \neq m'$, we coarse-grain $\tilde{m} := \mathrm{lcm}(m, m')$ sites. The unitaries $U_{B_{\tilde{m}}}(g_1) \otimes U_{E_{\tilde{m}}}(g_2)$ for $(g_1, g_2) \in G_1 \times G_2$, constracted in this way, form a unitary representation of $G_1 \times G_2$.

The states generated by V satisfy $I(A_1 : C_n|B_n)_{(n)} > 0$ if and only if $\mathcal{B} \subsetneq \mathcal{A}'$ (Theorem 6) due to dual complementarity. Moreover, $V(g_1)$ and $V(g_2)$ form a non-trivial projective representation. By assumption, $\hat{\mathcal{G}}_{\mathcal{A}}$ and $\hat{\mathcal{G}}_{\mathcal{A}}$ contain the basis of $\mathcal{A}$ and $\mathcal{B}$. Moreover, for every g_1, g_2 $V(g_2) \in \hat{\mathcal{G}}_{\mathcal{B}} \subset \mathcal{B}'$ and $V(g_1) \in \hat{\mathcal{G}}_{\mathcal{A}} \backslash \mathcal{U}(\mathcal{B}')$ and therefore there exists a pair (g_1, g_2) such that $[V(g_1), V(g_2)] \neq 0$ (note that the corresponding symmetery actions $U_{B_{\tilde{m}}}(g_1) \otimes I_{E_{\tilde{m}}}$ and $I_{B_{\tilde{m}}} \otimes U_{E_{\tilde{m}}}(g_2)$ commute each other). This completes the proof. □

1. Proof of Theorem 7

Proof. We show the theorem by proving that all the conditions in Proposition S.5 are satisfied when V is Clifford. Since V is Clifford, $\mathcal{V}_{A_2\to BEC}$ is an encoding map of a stabilizer code. In stabilizer codes, all the logical operators are spanned by logical Pauli operators [10]. The pre-image of $\tilde{\mathcal{E}}^\dagger$ is thus spanned by Pauli operators and it follows that $\mathcal{A} = Alg\{P_i | \exists \tilde{P}_B \otimes \tilde{P}_C \in \mathcal{L}(P_i)\}$, where $\tilde{P}_B$ and $\tilde{P}_C$ are Pauli operators. Let $D = 2^K$ without loss of generality. A is regarded as a K-qubit system and Pauli operators on A are generated by Z_i, X_i operators acting on ith qubit. Then, the generators of $\mathcal{A}$ (up to a local Clifford) are summarized as a table:

$$\mathcal{A} \cong Alg \begin{pmatrix} 1 & \cdots & l & l+1 & \cdots & m & m+1 & \cdots & K \\ Z & \cdots & Z & Z & \cdots & Z & I & \cdots & I \\ I & \cdots & I & X & \cdots & X & I & \cdots & I \end{pmatrix}. \tag{S.38}$$

Here, the first column means $\mathcal{A}$ contains Z_1, but not contains X_1. In the same way, $m+1$th column means $\mathcal{A}$ does not contain both Z_{m+1} and X_{m+1}. The commutant of $\mathcal{A}$ is immediately given as

$$\mathcal{A}' \cong Alg\begin{pmatrix} 1 & \cdots & l & l+1 & \cdots & m & m+1 & \cdots & K \\ Z & \cdots & Z & I & \cdots & I & Z & \cdots & Z \\ I & \cdots & I & I & \cdots & I & X & \cdots & X \end{pmatrix}. \tag{S.39}$$

From these expressions it is clear that $\mathcal{A} = Alg(\hat{\mathcal{G}}_{\mathcal{A}})$. Let $g_{BC}(g_E)$ is the number of independent logical Pauli operators supported on BC (E). For stabilizer codes, it is known that they satisfy the formula $g_{BC} + g_E = 2K$ [9]. It is then clear that the number of logical operators found on E is $l+2(K-m)$, which is the number of independent generators of $\mathcal{A}'$. Since the correctable algebra corresponding to output on E should be a subalgebra of $\mathcal{A}'$, they must be equivalent. Therefore dual complementarity is satisfied.

$H_1 = G_1$ follows from $\mathcal{A} = \mathcal{A}_{\tilde{\mathcal{E}}} = \mathcal{A}_{\tilde{\mathcal{E}}^{(2)}}$. Let us consider $P_i \in \mathcal{A}\backslash\mathcal{B}'$. For $n = 1$, P_i have a logical operator $\tilde{P}_{B_1} \otimes \tilde{P}_{C_1} \in \mathcal{L}(P_i)$ such that $\tilde{P}_C \neq I_C$. Since $\tilde{P}_C$ is also a Pauli operator, it has a logical Pauli operator on $B_2E_2C_2$. Suppose every such $\tilde{P}_C$ has no logical operator on B_2C_2. Then $\tilde{P}_C \in \mathcal{A}_{\tilde{\mathcal{E}}}\backslash\mathcal{A}'_{\tilde{\mathcal{F}}}$ but $\tilde{P}_C \notin \mathcal{A}_{\tilde{\mathcal{E}}^{(2)}}\backslash\mathcal{A}'_{\tilde{\mathcal{F}}^{(2)}}$, which conflicts to $\mathcal{A} = \mathcal{A}_{\tilde{\mathcal{E}}} = \mathcal{A}_{\tilde{\mathcal{E}}^{(2)}}$ and $\mathcal{B} = \mathcal{A}_{\tilde{\mathcal{F}}} = \mathcal{A}_{\tilde{\mathcal{F}}^{(2)}}$. Therefore $\mathcal{L}(\tilde{P}_C)$ contains operator on B_2C_2, which is also a Pauli operator and thus has a tensor product form. This proves $H_1 = G_1$. The same arguments hold for H_2. □

---

[1] C. Beny, A. Kempf, and D. W. Kribs, Quantum error correction of observables *Physical Review A*, 76, 042303 (2007).

[2] N. Schuch, D. Pérez-García, and J. I. Cirac, Classifying quantum phases using matrix product states and projected entangled pair states. *Phys. Rev. B*, 84, 165139 (2011).

[3] L. Zou and J. Haah, Spurious long-range entanglement and replica correlation length. *Phys. Rev. B*, 94:075151, (2016).

[4] Michael A Nielsen and I Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, (2000).

[5] E. H. Lieb and M. B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy. *J. Math. Phys.* 14, 1938 (1973).

[6] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction. *Phys. Rev. A* 54, 2629 (1996).

[7] M. Takesaki, Theory of Operator Algebras I. NewYork–Heidelberg–Berlin: Springer–Verlag, (1979).

[8] B. Eastin and E. Knill, Restrictions on Transversal Encoded Quantum Gate Sets. *Phys. Rev. Lett.*, 102, 110502 (2009).

[9] B. Yoshida and I. L. Chuang, Framework for classifying logical operators in stabilizer codes. *Phys. Rev. A*, 81, 052302 (2010).

[10] A necessary and sufficient condition for an operator O to be logical is $[O, S_i] = 0$ for all stabilizer generators S_i. O can be expanded in the product Pauli basis and it turns out that each non-zero part should commute with S_i to satisfy the condition.