Existence of Pauli-like stabilizers for every quantum error-correcting code

Jhih-Yuan Kao[1,2,*] and Hsi-Sheng Goan[1,2,3,†]

[1] *Department of Physics and Center for Theoretical Physics, National Taiwan University, Taipei 106319, Taiwan*
[2] *Center for Quantum Science and Engineering, National Taiwan University, Taipei 106319, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 106319, Taiwan*

(Received 1 September 2022; accepted 28 July 2023; published 15 September 2023)

The Pauli stabilizer formalism is perhaps the most thoroughly studied means of procuring quantum error-correcting codes, whereby the code is obtained through commutative Pauli operators and "stabilized" by them. In this work we will show that every quantum error-correcting code, including Pauli stabilizer codes and subsystem codes, has a similar structure, in that the code can be stabilized by commutative "Paulian" operators which share many features with Pauli operators and which form a *Paulian stabilizer group*. By facilitating a controlled gate we can measure these Paulian operators to acquire the error syndrome. Examples concerning codeword stabilized codes and bosonic codes will be presented; specifically, one of the examples has been demonstrated experimentally and the observable for detecting the error turns out to be Paulian, thereby showing the potential utility of this approach. This work provides a possible approach to implement error-correcting codes and to find new codes.

DOI: 10.1103/PhysRevA.108.032414

I. INTRODUCTION

Quantum information is stored as quantum states. Due to defects in the devices or executions, and the inevitable interaction of the quantum system with the environment, the state of the quantum system can be changed in a nondeterministic manner, which is an error; consequently, error correction is vital for the information to stay hygienic. Using quantum error-correcting codes, states are prepared in specific subspaces such that if certain errors occur, we can detect and correct them [1–5]. Even though quantum devices without error correction may serve certain purposes such as simulating physical systems [6,7], a universal quantum computer that is scalable still requires error correction [8,9].

Pauli stabilizer codes [1,10,11] are an extremely important class of quantum error-correcting codes. Some of the most promising codes, such as topological codes [12–16], which include surface codes [13,17–26] and quantum low-density parity-check codes [27–30], are based on Pauli stabilizer codes. An advantage of Pauli stabilizer formalism is that it informs us of which measurements to implement to detect the errors, namely, the stabilizer generators.

There are several ways of generalizing the Pauli stabilizer formalism, for example, by generalizing Pauli groups, or nice error bases to nonbinary cases [31–35], or by considering noncommutative groups on binary codes [36]. In this work, instead of defining a certain group and constructing an error-correcting code from it, we will do the opposite: We investigate the structure of any error-correcting code, including subsystem codes [37–43], to show that every code can be stabilized by a "Paulian" stabilizer group (Proposition 1 and Corollary 1), the exact meaning of being Paulian to be explained in Sec. II B. Identifying the Paulian stabilizer group of an error-correcting code may give us a guideline on how to implement such a code: The error syndrome can be obtained by measuring these Paulian operators, which can be conducted via controlled operations (Sec. III D). We will also show how to obtain the Paulian stabilizer group for a concatenated binary code (Sec. IV) [1,2,44], and in Sec. V we will demonstrate some examples. For conciseness, details of some topics can be found in the Appendixes.

II. PRELIMINARIES

$\mathbb{A} \subseteq \mathbb{B}$ means $\mathbb{A}$ is a subset of $\mathbb{B}$, while $\subset$ indicates it is a proper subset. A map $f : \mathbb{X} \to \mathbb{Y}$ to the restriction of $\mathbb{X}' \subseteq \mathbb{X}$, denoted by $f|_{\mathbb{X}'}$, is a map from $\mathbb{X}'$ to $\mathbb{Y}$ with $f|_{\mathbb{X}'}(x) = f(x)\ \forall x \in \mathbb{X}'$ [45–47], for which we will often shrink the codomain to the image $f|_{\mathbb{X}'}(\mathbb{X}') = f(\mathbb{X}')$. The *span* of a set of vectors is the set of all linear combinations thereof, which is a subspace. We will use shorthand to label sets obtained from others in a sensible way, e.g., $\mathcal{H}^{\otimes 3}$ is $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$. The subscript beside an identity operator, denoted by I, or orthogonal projection, denoted by Π, indicates the (sub)space the operator acts on or projects onto; e.g., Π_{C} projects onto $\mathcal{H}_{\mathrm{C}}$.

The code space $\mathcal{H}_{\mathrm{C}}$ of a quantum error-correcting code is a subspace of the entire space $\mathcal{H}$ where the encoded state is stored [1,4,48]; sometimes we simply refer to the code space as the code. With $\mathbb{C}^n$ denoting a generic n-dimensional complex vector space, a code is called an $[[n, k]]$-code if $\mathcal{H} \cong \mathbb{C}^{2^n}$ and $\mathcal{H}_{\mathrm{C}} \cong \mathbb{C}^{2^k}$ for some integers n and k, where $A \cong B$ indicates that A and B are isomorphic; such codes are said to be *binary*. We use the term binary codes in a stricter sense than, e.g., Ref. [49], as we require the code space to be

[*] frankkao@ntu.edu.tw
[†] goan@phys.ntu.edu.tw

binary too. Also, an $((n, k, d))$ code has n qubits, a code space of dimension k and distance d [50]. For a qubit system, $|\pm 1\rangle$ instead of $|0\rangle$ and $|1\rangle$ will denote the ±1-eigenstates.

An operator is said to *stabilize* a subspace $\mathcal{H}'$ if $\mathcal{H}'$ is a subspace of the operator's 1-eigenspace. We will refer to the subspace spanned by all simultaneous eigenvectors with the same simultaneous eigenvalues as a *simultaneous eigenspace*. P^n will denote the Pauli group on $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$, and its members will be called *Pauli operators* [1,31,32]; in this work we will use X_i, Y_i and Z_i to denote Pauli X, Y, Z operators on the ith site. If the code space of a code is the $(1, \ldots, 1)$-simultaneous eigenspace of commutative Pauli operators, the code is called a *Pauli stabilizer code*, and the abelian group generated by these operators is the *stabilizer group* [1,10,11].

A representation of a group G on a space $\mathcal{V}$ is a homomorphism Φ from G to the general linear group of $\mathcal{V}$, and it is said to be faithful if Φ is one-to-one [51]. Abusing the language, we will call the image $\Phi(\mathsf{G})$ "a representation." Two representations G_1 on $\mathcal{H}_1$ and G_2 on $\mathcal{H}_2$ of G are said to be unitarily equivalent if there exits a unitary map $V : \mathcal{H}_1 \to \mathcal{H}_2$ such that $\mathsf{G}_1 = V^{-1}\mathsf{G}_2 V$ [52–54].

A. Involutions

An operator is said to be an involution if it is its own inverse, i.e., if it squares to I [45]; for instance, Pauli X, Y, Z are all involutions. By definition, the spectrum of an involution can only contain ±1, which by the spectral theorem leads to

Lemma 1. An involution on a Hilbert space is normal if and only if it is self-adjoint and if and only if it is unitary.

Self-adjoint involutions are of great physical interest, because they correspond to both physical observables (self-adjoint) and evolution of a system (unitary). A Pauli group is composed of unitary involutions and operators that square to $-I$, which we call counterinvolutions. We can easily see that a counterinvolution is an involution multiplied by i, and vice versa.

If a pair of involutions or counterinvolutions A and B anticommute, for an a-eigenvector $|v\rangle$ of A, $BA|v\rangle = aB|v\rangle = -AB|v\rangle$, and since they are by definition automorphisms, $B|v\rangle \neq 0$ for all nonzero $|v\rangle$; therefore, B maps the a-eigenspace of A to the $-a$-eigenspace, and the $\pm a$-eigenspaces are thus isomorphic.

B. Paulian operators

An operator will be called *Paulian* if

(1) It is either an involution or counterinvolution

(2) It is unitary and

(3) It has two isomorphic eigenspaces unless it has a single eigenspace.

Accordingly, all Pauli operators are Paulian. A Paulian operator is self-adjoint if and only if it is an involution, and it is skew-self-adjoint if and only if it is a counterinvolution.

When the space is finite-dimensional, we could simply require Paulian operators, except for those proportional to I, to be traceless. As the eigenvalues have opposite signs, the two eigenspaces have the same dimension and hence are isomorphic. However, a unitary operator on an infinite-dimensional space is not trace class [54,55] and in general it does not have a well-defined trace, so we simply demand the eigenspaces be isomorphic. Having isomorphic eigenspaces, the unitary map between them will play the role of Pauli Z [cf. (12) and the proof for Proposition 1 (Sec. III A)]; besides, this makes it possible to find anticommuting Paulian operators (cf. the previous subsection).

To appreciate the significance of Paulian operators in physics, we remark

(1) By Lemma 1, a Paulian involution is unitary and self-adjoint at the same time, so it can not only describe the evolution but also be an observable.

(2) Because a Paulian operator (except for those that are proportional to I) is traceless or has two isomorphic eigenspaces, very roughly speaking, if an observable has two possible outcomes, and if both outcomes are equally likely on average with all states considered, then it is Paulian.

Finally, in this work when we refer to an operator as Paulian, it may not necessarily be Paulian on the entire domain, but only Paulian to the restriction of a specific subspace, which subspace has to do with the errors the operator can detect or correct. This will be explained in more detail later.

C. Condition for error correction

The necessary and sufficient condition for a set of errors $\mathbb{E}$ to be correctable is [31,32]

$$\Pi_C E^\dagger F \Pi_C \propto \Pi_C \;\forall E, F \in \mathbb{E}. \tag{1}$$

There are other expressions for this condition, for example, $\Pi_C E^\dagger F \Pi_C = \alpha_{E,F}\Pi_C$ where α is a Hermitian matrix [1,2,4,48], or in terms of inner product and basis [1,2,56]. It is worth mentioning that the common requirement that α is Hermitian is somewhat superfluous: If two operators A and B satisfy

$$\Pi A^\dagger B \Pi = c\Pi$$

for some constant c and orthogonal projection Π, then it must be true that

$$\Pi B^\dagger A \Pi = (\Pi A^\dagger B \Pi)^\dagger = c^*\Pi.$$

Hence the matrix α above is naturally Hermitian. If a code can correct $\mathbb{E}$, it can correct any error in the span of $\mathbb{E}$.

From [4,48], we can find a maximal subset $\mathbb{F}$ of span$\mathbb{E}$ whose elements obey

$$\Pi_C E^\dagger F \Pi_C = \begin{cases} 0, & E \neq F \\ \Pi_C, & E = F \end{cases} \;\forall E, F \in \mathbb{F}, \tag{2}$$

and we call correctable errors in $\mathbb{F}$ *orthonormal*; the set $\mathbb{F}$ is maximal in the sense that

$$\sum_{E\in\mathbb{E}} E\mathcal{H}_C = \bigoplus_{F\in\mathbb{F}} F\mathcal{H}_C, \tag{3}$$

where $\oplus$ denotes an orthogonal direct sum, is satisfied. Note

$$E\mathcal{H}_C \cong \mathcal{H}_C \;\forall E \in \mathbb{E}, \tag{4}$$

so $\bigoplus_{F\in\mathbb{F}} F\mathcal{H}_C$ is an orthogonal direct sum of isomorphic spaces. On the other hand, if we have a set of errors or operators such that the operators in it are "orthogonal" but not necessarily "normalized," i.e., $\Pi_C E^\dagger E \Pi_C = c_E \Pi_C$ for some scalar c_E that is not necessarily 1, then the set is referred to as *orthogonal*.

III. PAULIAN STABILIZER GROUP

Here is the main result of this work, which will be explained in detail soon after; dim below refers to the dimension of a vector space:

Proposition 1. Consider an error-correcting code, with the code space $\mathcal{H}_\mathrm{C}$ belonging in $\mathcal{H}$. There exist operators which stabilize $\mathcal{H}_\mathrm{C}$ and satisfy the following properties:

(1) To the restriction of a $2^m k'$-dimensional subspace $\mathcal{H}'$ for some positive integer m with $\mathcal{H}_\mathrm{C} \subseteq \mathcal{H}' \subseteq \mathcal{H}$ and $k' \geqslant \dim \mathcal{H}_\mathrm{C}$, these operators are mutually commutative Paulian operators, forming an abelian group S called the **Paulian stabilizer group**, which is generated by m operators. If $\mathcal{H}$ is infinite-dimensional, $\mathcal{H}'$ can be as well.

(2) S is an abelian subgroup of a group of Paulian operators P^m_S, which is a faithful representation of P^m.

(3) A subset of all correctable errors can be detected by measuring these operators and corrected by applying proper inverses.

A. The minimal stabilizer group

First, we will prove a "minimal" version of this proposition, which yields a "minimal" Paulian stabilizer group. The reader may skim over the proof and come back later when necessary.

Proof. With $\mathbb{F}$ defined in (2), we choose a subset of $\mathbb{F}' \subseteq \mathbb{F}$ whose cardinality is a positive integral power of 2, m, with $I \in \mathbb{F}'$. As long as the code is nontrivial, such a subset always exists. We want $\mathbb{F}'$ to be as large as possible, so we choose

$$m = \lfloor \log_2 |\mathbb{F}| \rfloor, \tag{5}$$

where $\lfloor \cdot \rfloor$ is the floor function; we thus have $|\mathbb{F}'| = 2^m$.

Let $\mathbb{T}$ be the set of all tuples of ± 1 with length m and (t) be the symbol for elements in $\mathbb{T}$, which we will use for indexing. For each $F \in \mathbb{F}'$, choose a a unique tuple $(t) \in \mathbb{T}$; to put it another way, we define a bijective "syndrome map" $f_\mathrm{sym} : \mathbb{F}' \to \mathbb{T}$ such that $f_\mathrm{sym}(F) \in \mathbb{T}$ is the tuple corresponding to F, which, as we will see, is the syndrome of F. $F_{(t)}$ will denote the error $(t) \in \mathbb{T}$ refers to,

$$F_{(t)} := f^{-1}_\mathrm{sym}((t)), \tag{6}$$

and likewise[1]

$$\mathcal{H}_{(t)} = F_{(t)}\mathcal{H}_\mathrm{C}. \tag{7}$$

Among all such binary tuples (t),

$$(I) := (1, \dots, 1) \tag{8}$$

will serve as a convenient abbreviation; in particular we require

$$F_{(I)} = I, \tag{9}$$

namely, $f_\mathrm{sym}(I)$ is selected to be $(I) = (1, \dots, 1)$. We also define

$$\overline{\mathcal{H}} := \bigoplus_{F \in \mathbb{F}'} F\mathcal{H}_\mathrm{C} = \bigoplus_{(t)\in\mathbb{T}} \mathcal{H}_{(t)} \subseteq \mathcal{H}. \tag{10}$$

Here let $\mathcal{H}'$ of this proposition be $\overline{\mathcal{H}}$. With

$$\dim \overline{\mathcal{H}} = 2^m \dim \mathcal{H}_\mathrm{C}, \tag{11}$$

it means k' is $\dim \mathcal{H}_\mathrm{C}$. We have the following isomorphism:

$$\mathcal{H}_\mathrm{B} := \mathcal{H}_\mathrm{C} \otimes \bigotimes_{i=1}^{m} \mathbb{C}^2_i \cong \overline{\mathcal{H}}, \tag{12}$$

where the subscript i of $\mathbb{C}^2_i$ is for indexing.

Let's construct a unitary map $U : \overline{\mathcal{H}} \to \mathcal{H}_\mathrm{B}$ as follows: Since $\mathcal{H}_{(t)}$'s are isomorphic, there exist unitary maps

$$V_{(t)} : \mathcal{H}_{(t)} \to \mathcal{H}_\mathrm{C} \ \forall (t) \in \mathbb{T}, \tag{13}$$

among which we let $V_{(I)} : \mathcal{H}_\mathrm{C} \to \mathcal{H}_\mathrm{C}$ be I_C. Let's also choose an orthonormal basis $\{|\pm 1\rangle_i\}$ for each $\mathbb{C}^2_i$. For any $(t) = (i_1, \dots, i_m) \in \mathbb{T}$ and any $|v\rangle \in \mathcal{H}_{(t)}$, let

$$U|v\rangle := (V_{(t)}|v\rangle) \otimes |(t)\rangle, \tag{14}$$

where

$$|(t)\rangle := |i_1\rangle_1 \otimes \cdots \otimes |i_m\rangle_m \in \bigotimes_{i=1}^{m} \mathbb{C}^2_i. \tag{15}$$

By definition (10), $\overline{\mathcal{H}}$ is the direct sum of $\mathcal{H}_{(t)}$'s, so U of (14) is defined on the entirety of $\overline{\mathcal{H}}$. U is unitary because $V_{(t)}$'s are unitary and $\{|\pm 1\rangle_i\}$'s are orthonormal bases.

Now, for every $i = 1, \dots, m$ let X_i and Z_i denote the operators on $\mathcal{H}_\mathrm{B}$ that apply Pauli X and Z on $\mathbb{C}^2_i$ and act trivially on the other subsystems including $\mathcal{H}_\mathrm{C}$. Their counterparts on $\overline{\mathcal{H}}$ via U are

$$Z^\mathrm{S}_i := U^{-1}Z_iU, \quad X^\mathrm{S}_i := U^{-1}X_iU; \tag{16}$$

that is, X_i and X^S_i, and Z_i and Z^S_i, are unitarily similar, and in the language of group theory, this is conjugation by U [57]. The group generated by X_i and Z_i is $I_\mathrm{C} \otimes \mathsf{P}^m$, which is a faithful representation of P^m, so the group generated by Z^S_i's and X^S_i's, denoted by P^m_S, is also a faithful representation of P^m: $I_\mathrm{C} \otimes \mathsf{P}^m$ and P^m_S are unitarily equivalent representations, i.e.,

$$\mathsf{P}^m_\mathrm{S} := U^{-1}(I_\mathrm{C} \otimes \mathsf{P}^m)U. \tag{17}$$

With these observations, the proposition is proved:

(1) $I_\mathrm{C} \otimes \mathsf{P}^m$ is a group of Paulian operators, so is P^m_S. Note unless $\mathcal{H}_\mathrm{C}$ is (isomorphic to) $\mathbb{C}^{2^p}$ for some integer p, $I_\mathrm{C} \otimes \mathsf{P}^m$ is not a group of Pauli operators. Besides, Z_i's, m in total, generate a maximal linearly independent and abelian subgroup[2] of $I_\mathrm{C} \otimes \mathsf{P}^m$; by unitary equivalence, Z^S_i's, m in total, also generate a maximal linearly independent and abelian subgroup of P^m_S:

$$\mathsf{S} := \langle Z^\mathrm{S}_1, \dots, Z^\mathrm{S}_m \rangle. \tag{18}$$

[1] Later $\mathcal{H}_{(t)}$ will be defined as the (t)-simultaneous eigenspace of the stabilizers. Hence (7) is not the definition of $\mathcal{H}_{(t)}$, but it is true here.

[2] Please see the discussion near the end of Sec. III C.

(2) Because $\mathcal{H}_C \otimes |(t)\rangle$ are the (t)-simultaneous eigenspaces of Z_i's, $\mathcal{H}_{(t)}$ are the (t)-simultaneous eigenspaces of Z_i^S's. $\mathcal{H}_C = \mathcal{H}_{(I)}$ is hence stabilized by Z_i^S's.

(3) For any $|\psi\rangle \in \mathcal{H}_C$, if $F_{(t)} \in \mathbb{F}'$ occurs, $|\psi\rangle \in \mathcal{H}_C$ becomes $F_{(t)}|\psi\rangle \in \mathcal{H}_{(t)}$, and it is a (t)-simultaneous eigenvector of Z_i^S's; performing the syndrome measurement by measuring Z_i^S's we obtain the simultaneous eigenvalues (t), which are the *error syndrome* [2], and we can correct the error by inverting $F_{(t)}$. Hence, any correctable error E for which

$$E\mathcal{H}_C \subseteq \overline{\mathcal{H}} \tag{19}$$

can be detected and corrected by measuring Z_i^S. ■

In a nutshell, via the isomorphism (12) and U of (14), we borrow the structure from $\mathcal{H}_B$ and apply it to $\mathcal{H}' = \overline{\mathcal{H}} \subseteq \mathcal{H}$: Z_i^S and X_i^S are essentially Pauli Z and X on different subsystems or sites, and such a structure can be established for any quantum error-correcting codes. Treating $\overline{\mathcal{H}}$ and $\mathcal{H}_B$ as identical, $\mathbb{C}_i^2$'s of $\mathcal{H}_B$ are the stabilizer qubits [38]. For Pauli stabilizer codes if we consider $\overline{\mathcal{H}} = \mathcal{H}$ and $\mathcal{H}_B$ as the same space, the unitary map U, which becomes an operator now, is in the Clifford group [2,11,38,58].

We will call members of S *Paulian stabilizers*. Like Pauli stabilizer codes, we can choose any generating set of S for syndrome measurements. From now on, rather than (7), $\mathcal{H}_{(t)}$ will refer to the (t)-simultaneous eigenspace of Z_i^S's, and we will call it a (t)-*syndrome space*. Defining them this way will help us extend the Paulian stabilizers later.

B. A larger stabilizer group

The stabilizers depicted in Sec. III A are the minimal version of Proposition 1 with $\mathcal{H}' = \overline{\mathcal{H}}$, as the procedures laid out above are applicable to every code; however, when $\log_2 |\mathbb{F}|$ is not an integer, $\mathbb{F}' \subset \mathbb{F}$, and there are correctable errors that cannot be detected by Z_i^S's.

Now suppose the code obeys

$$2^{\lceil \log_2 |\mathbb{F}| \rceil} \dim \mathcal{H}_C \leqslant \dim \mathcal{H}, \tag{20}$$

where $\lceil \cdot \rceil$ is the ceiling function. Let

$$m = \lceil \log_2 |\mathbb{F}| \rceil, \tag{21}$$

and we can consider a larger family of orthogonal operators $\mathbb{F}''$ such that $\mathbb{F} \subseteq \mathbb{F}''$, and that in addition to errors in $\mathbb{F}$ obeying (2) we require

$$E\mathcal{H}_C \cong \mathcal{H}_C \quad \text{and} \quad E\mathcal{H}_C \perp F\mathcal{H}_C \; \forall E \neq F \in \mathbb{F}''. \tag{22}$$

Like before, for each element in $\mathbb{F}''$ we will associate with it a unique binary tuple of length m, i.e., a bijection between $\mathbb{F}''$ and $\mathbb{T}$; cf. Sec. III A. In this way, the Paulian stabilizers associated with $\mathbb{F}''$ cover all errors in $\mathbb{F}$. The operators in $\mathbb{F}'' \setminus \mathbb{F}$ may be uncorrectable as they may not satisfy (2), but they are instrumental in constructing a larger Paulian stabilizer group.

In short, we would like the Paulian stabilizers to cover all correctable errors, hence choosing $m = \lceil \log_2 |\mathbb{F}| \rceil$ if possible; if (20) cannot be satisfied, we resort to $m = \lfloor \log_2 |\mathbb{F}| \rfloor$. In particular, given a code with distance d, we have

$$|\mathbb{F}| \leqslant \sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} 3^j, \tag{23}$$

which serves as an upper bound for $|\mathbb{F}|$ and is exact when the code is nondegenerate [1,2]; cf. the quantum Hamming bound [2,48]. Expression (23) combined with (20) is a sufficient condition to judge whether it is possible to find Paulian stabilizers to correct all the errors for this code, explicitly,

$$2^{\left\lceil \log_2 \sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} 3^j \right\rceil} \dim \mathcal{H}_C \leqslant \dim \mathcal{H}, \tag{24}$$

which is necessary and sufficient if the code is nondegenerate.

C. Extending the domain

If $2^m \dim \mathcal{H}_C < \dim \mathcal{H}$, we may extend the domains of Z_i^S's, and they should remain self-adjoint so that they are measurable. The following fact may be utilized [59]:

Theorem 1. For a self-adjoint or unitary operator A with an invariant subspace $\mathcal{H}'$, $A|_{\mathcal{H}'}$ and $A|_{\mathcal{H}'^{\perp}}$ are both self-adjoint or unitary operators.

Hence, to extend a self-adjoint operator, we can define another self-adjoint operator on the space orthogonal to the domain and add them.

In particular, let's extend Z_i^S's as follows: We enlarge all syndrome spaces $\mathcal{H}_{(t)}$'s while keeping them isomorphic and orthogonal to each other, and let their dimension be k', which would be no smaller than $\dim \mathcal{H}_C$. Following how Z_i^S's were originally constructed on $\overline{\mathcal{H}}$ in Sec. III A, we reach the final form of Proposition 1, where $\mathcal{H}'$ is the direct sum of all syndrome spaces and Z_i^S's are commutative Paulian operators to the restriction of $\mathcal{H}'$. Thus, the proof in Sec. III A and the discussion in Sec. III B and this subsection together illustrate the complete picture of Proposition 1.

We remark

(1) $F_{(t)}\mathcal{H}_C$ is a subspace of the corresponding syndrome space $\mathcal{H}_{(t)}$, in particular

$$\mathcal{H}_C \subseteq \mathcal{H}_{(I)}. \tag{25}$$

The code space is stabilized by Z_i^S's, but it is not necessarily the (I)-syndrome space, but a subspace thereof.

(2) If $\mathcal{H}$ is infinite-dimensional, syndrome spaces can be made infinite-dimensional while keeping them isomorphic and mutually orthogonal; an example will be given in Sec. V B.

(3) When $\dim \mathcal{H} / \dim \mathcal{H}_C$ is an integral power of 2, it is always possible to construct a Paulian stabilizer group that uses the space to its full capacity for error correction; specifically, this is true for binary codes.

D. Measuring Paulian operators

Suppose the state is currently in $\mathcal{H}'$. To measure a Z_i^S, we can make use of a generalized-controlled NOT (GCNOT): Consider an ancilla qubit $\mathcal{H}_A \cong \mathbb{C}^2$ initialized at $|1\rangle_A$. To the restriction of $\mathcal{H}' \otimes \mathcal{H}_A$, define

$$\text{GCNOT}|_{\mathcal{H}' \otimes \mathcal{H}_A} := \Pi_- \otimes X_A + \Pi_+ \otimes I_A \tag{26}$$

$$= I_{\mathcal{H}'} \otimes |+\rangle_A\langle +|_A + Z_i^S \otimes |-\rangle_A\langle -|_A, \tag{27}$$

where $\Pi_\pm$ project onto the ±1-eigenspaces of Z_i^S and $|\pm\rangle_A$ are ±1-eigenstates of X_A; in Appendix A it will be explained why (26) and (27) are equal and how unique the GCNOT is. On the entire space $\mathcal{H}\otimes\mathcal{H}_\mathrm{A}$ it is thus

$$\mathrm{GCNOT}=\Pi_-\otimes X_\mathrm{A}+\Pi_+\otimes I_\mathrm{A}+\Pi_{\mathcal{H}'^\perp}\otimes U_\mathrm{A}, \tag{28}$$

where U_A can be any unitary operator; $\Pi_{\mathcal{H}'^\perp}\otimes U_\mathrm{A}$ is there for GCNOT to be unitary; cf. Theorem 1. If the system is in a -1-eigenstate of Z_i^S, the state of the qubit will be mapped to $|-1\rangle_\mathrm{A}$, else it remains at $|1\rangle_\mathrm{A}$, so measuring Z_A on the ancilla afterwards is equivalent to measuring Z_i^S. This operator derives from the generalized CNOT or controlled-X in Refs. [60–63], but we do not require that the system and ancilla have the same dimension. From now on for simplicity we will ignore the restriction.

Quite many implementations of Pauli measurements involve these controlled operations implicitly [3,13,20]: For example, to measure $Z_1\cdots Z_j$, with the (regular) CNOT on the ith (data) qubit with the ancilla as the target denoted by CNOT_i, it can be found

$$\bigotimes_{i=1}^{j}\mathrm{CNOT}_i=\Pi_-\otimes X_\mathrm{A}+\Pi_+\otimes I_\mathrm{A}: \tag{29}$$

$\Pi_\pm$ are the ±1-eigenspaces of $Z_1\cdots Z_j$, so the composition is a generalized CNOT.

Using a nonqubit system as the control may not be as intuitive, so let's instead consider the controlled-Z_i^S:

$$\mathrm{CZ}_i^\mathrm{S}=Z_i^\mathrm{S}\otimes|-1\rangle_\mathrm{A}\langle-1|_\mathrm{A}+I_{\mathcal{H}'}\otimes|1\rangle_\mathrm{A}\langle1|_\mathrm{A}, \tag{30}$$

which is a controlled-U operation with U being the Paulian operator Z_i^S [4]. Compared with (27), we have

$$\mathrm{GCNOT}=(I_{\mathrm{H}'}\otimes H_\mathrm{A})\mathrm{CZ}_i^\mathrm{S}(I_{\mathrm{H}'}\otimes H_\mathrm{A}), \tag{31}$$

where H_A is the Hadamard gate. In other words, if the ancilla is initialized at $|1\rangle_\mathrm{A}$, we can perform an inverse Hadamard gate to map it to $|+\rangle_\mathrm{A}$ and apply the CZ_i^S gate. Measuring X_A on the ancilla, if the result is ±1, then it means the system was in a ±1-eigenstate of Z_i^S, so the overall effect is identical to measuring Z_i^S.

Equation (31) is in the same vein as exchanging the target and control qubits of a (regular) CNOT by composing with Hadamard gates or change of basis [4]: Indeed, (27) can be understood as using the $|\pm\rangle_\mathrm{A}$ states of the ancilla qubit to determine whether to perform Z_i^S, so the ancilla qubit is the control in this sense; with (31) we simply change the "control states" from $|\pm\rangle_\mathrm{A}$ to $|\pm1\rangle_\mathrm{A}$.

Regarding the ancilla qubit as the control as in (27) or (30) also brings the following benefit: Suppose the system is composed of qubits, and that we have a quantum circuit for Z_i^S using fundamental gates, comprising single-qubit gates and CNOT or two-qubits controlled gates; let $Z_i^\mathrm{S}=\prod_i U_i$, and we have

$$\mathrm{CZ}_i^\mathrm{S}=\prod_j\mathrm{CU}_j. \tag{32}$$

If U_i is a single-qubit gate, then we can again decompose CU_j as single-qubit gates and CNOT's; if U_j is a CNOT or a controlled-V_j for some V_j, then CU_j is a Toffoli gate or $C^2(V_j)$, and we can again decompose it as fundamental gates [4,64,65]. Thus, if we are able to carry out Z_i^S as an operation, then we are also able to measure it. Equation (29) can also be better comprehended with the ancilla as the control.

We discussed extending Paulian-ness to a larger space $\mathcal{H}'$ in Sec. III C. From a measurement point of view, how the Paulian stabilizers should be extended depends on whether the corresponding controlled operations are natural, that is, whether we can couple the system with the ancilla via the controlled operations relatively easily.

We can tweak (27) to use an ancilla qudit (which may be composed of several qubits) for the setup to be less error-prone [1,2,58]: Omitting $\Pi_{\mathcal{H}'^\perp}\otimes U_\mathrm{A}$ again, let the system be coupled with the qudit initialized at $|1\rangle_\mathrm{A}$ through this generalized CNOT

$$\sum_{i_+,i_-}(|i_-\rangle\langle i_-|\otimes X_{i_-}+|i_+\rangle\langle i_+|\otimes X_{i_+}), \tag{33}$$

where

(1) $\{|i_\pm\rangle\}$ are orthonormal bases of the ±1-eigenspaces of Z_i^S

(2) Each $X_{i_\pm}$ is an X operator between the states $|1\rangle_\mathrm{A}$ and $|i_\pm\rangle_\mathrm{A}$ of the qudit [60] and

(3) We have an observable Z'_A on the qudit, with $|i_\pm\rangle_\mathrm{A}$ being ±1-eigenstates of Z'_A; $|i_-\rangle_\mathrm{A}$'s may not be orthogonal with or even different from each other, likewise for $|i_+\rangle_\mathrm{A}$'s. $|1\rangle_\mathrm{A}$ is a $+1$-eigenstate of Z'_A, and some of the $|i_+\rangle_\mathrm{A}$'s may be $|1\rangle_\mathrm{A}$.

Afterwards, we measure Z'_A, and all this combined is equivalent to measuring the Paulian operator. Expression (33) is again an adaption of the generalized CNOT from Refs. [60–63].

E. Subsystem codes

Subsystem codes can be considered a generalization of regular error-correcting codes [37–43]: The code space becomes

$$\mathcal{H}_\mathrm{C}=\mathcal{H}_\mathrm{L}\otimes\mathcal{H}_\mathrm{G}\subseteq\mathcal{H}. \tag{34}$$

The information is stored in the logical subsystem $\mathcal{H}_\mathrm{L}$ and the state of the gauge subsystem $\mathcal{H}_\mathrm{G}$ does not matter.

Proposition 1 is also applicable to subsystem codes, explicitly:

Corollary 1. The code space of every subsystem code can be stabilized by operators with properties identical to those listed in Proposition 1. Hence, after obtaining the Paulian stabilizer group S, for any nonzero $A\in\mathcal{L}(\mathcal{H}_\mathrm{G})$, all elements in $(I_\mathrm{L}\otimes A)\mathsf{S}$ leave the encoded state intact.

Let's provide a simple argument as to why this is true: According to Ref. [66], with $\mathbb{E}$ denoting the set of correctable errors, for a subsystem code it is possible to find a set $\mathbb{F}$ of "orthogonal" correctable errors that obeys (3), just like an ordinary error-correcting code. Utilizing $\mathbb{F}$ and the corresponding syndrome spaces, we can obtain Paulian stabilizers by following the steps in Sec. III A.

IV. CONCATENATION OF BINARY CODES

Binary codes with appropriate parameters can be concatenated, and we will illustrate how to acquire the Paulian stabilizer group of the new code, in a similar fashion to Pauli stabilizer codes [48]. A symbol with sub- or superscript in, out, or + (+ for "adding") indicates it belongs to the inner, outer, or concatenated codes, respectively, and the sub- or superscript w means it can be one of those three.

Let them be $[[n_w, k_w]]$-codes, and the inner and outer codes have Paulian stabilizers Z_i^w's. To concatenate them,

$$q := n_{\text{out}}/k_{\text{in}} \tag{35}$$

should be an integer. Let $\mathcal{H}_w$ be the space each code belongs in, and

$$\mathcal{H}_+ = \mathcal{H}_{\text{in}}^{\otimes q}. \tag{36}$$

Define the following operators on $\mathcal{H}_+$:

$$Z_{i,j}^+ := \underbrace{I_{\text{in}} \otimes \cdots \otimes I_{\text{in}}}_{j-1 \text{ subsystems}} \otimes \underbrace{Z_i^{\text{in}}}_{j\text{th } \mathcal{H}_{\text{in}}} \otimes I_{\text{in}} \otimes \cdots \otimes I_{\text{in}}, \tag{37}$$

which are independent and commute with each other, and which stabilize

$$\mathcal{H}_{\text{in,C}}^{\otimes q} \subseteq \mathcal{H}_+, \tag{38}$$

where $\mathcal{H}_{\text{in,C}}$ is the code space of the inner code.

Next, let the logical Pauli operators on the inner code commute with all Z_i^{in}'s, and expand every Z_i^{out} in terms of Pauli operators. Since $\mathcal{H}_{\text{in,C}}$ and $\mathcal{H}_{\text{out}}$ are composed of k_{in} and qk_{in} qubits, respectively, regarding every k_{in} qubits of $\mathcal{H}_{\text{out}}$ as $\mathcal{H}_{\text{in,C}}$ we can replace each Pauli operator in every Z_i^{out} by the corresponding logical Pauli operator on the inner code, and the resultant operator will be denoted by Z_i^+. Z_i^+'s together with $Z_{j,k}^+$'s are mutually commutative and independent Paulian operators, composing the stabilizer generators of the concatenated code.

How to get Z_i^+'s may be a little hard to comprehend, so here's a quick demonstration: Suppose $n_{\text{out}} = 4$ and $k_{\text{in}} = 2$. As $q = 4/2 = 2$,

$$\mathcal{H}_+ = \mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{in}}. \tag{39}$$

If $Z_1^{\text{out}} = (X \otimes X \otimes Z \otimes Y + Z \otimes Z \otimes X \otimes I_2)/2$, then

$$Z_1^+ = (\overline{X}_1\overline{X}_2 \otimes \overline{Z}_1\overline{Y}_2 + \overline{Z}_1\overline{Z}_2 \otimes \overline{X}_1 I_{\text{in}})/2, \tag{40}$$

where $\overline{L}_i$ denotes the logical L operator of the i-th logical qubit. In (40), $\overline{X}_1\overline{X}_2$ and $\overline{Z}_1\overline{Z}_2$ act on the first $\mathcal{H}_{\text{in}}$ of (39), and $\overline{Z}_1\overline{Y}_2$ and $\overline{X}_1 I_{\text{in}}$ on the second one. Notice logical operators acting on different logical qubits commute with one another, so, e.g., $\overline{X}_1\overline{X}_2 = \overline{X}_2\overline{X}_1$. Also a logical identity operator is simply the identity operator on the system, so in (40) instead of $\overline{X}_1\overline{I}_2$ we had $\overline{X}_1 I_{\text{in}} = \overline{X}_1$; we spelled I_{in} out for clarity.

The methods to find the parameters and codewords of concatenated codes are well established [1,44,67,68], on which we will provide a short discussion in Appendix B.

V. EXAMPLES

Here we will show the Paulian stabilizers of some codes, or how to find them.

A. Transformed from Pauli stabilizer codes

Given a Pauli stabilizer code that can correct a set of operators $\mathbb{E}$ with stabilizers Z_i^{S}, we can perform a unitary transformation U on the system, which can be seen as a change of orthonormal basis. The transformed stabilizer generators

$$Z_i^{\text{S}\prime} = UZ_i^{\text{S}}U^{-1} \tag{41}$$

will be Paulian, and they can correct a set of operators $U\mathbb{E}U^{-1}$. If the unitary transformation is local in each (physical) qubit, the distance shall stay the same.

For illustration, consider an n-qubit repetition code with stabilizers [48,69]

$$Z_1Z_2, \ldots, Z_{n-1}Z_n, \tag{42}$$

which can fix an X error on every qubit. We can construct a generalized repetition code for normal operators with

Lemma 2. An operator on $\mathbb{C}^2$ is normal if and only if it can be a linear combination of the identity and a Paulian operator that is not proportional to the identity. Note as the Paulian operator is not proportional to the identity, it has two eigenvalues.

The proof can be found at Appendix E. From the discussion in Secs. II A and II B, the Paulian operator in Lemma 2 can be chosen to be self-adjoint so that it has eigenvalues 1 and −1.

By this lemma, consider any normal operator $E = aI + bV$ on $\mathbb{C}^2$, where $a, b \in \mathbb{C}$ and V is self-adjoint and Paulian. After obtaining V, as X and V have the same spectrum, X and V are unitarily similar via some unitary U; in other words, we can perform local unitary transformations V_i such that $V_i = U_iX_iU_i^{-1}$ for all the (physical) qubits, where the subscript i indicates which qubit the operator act on nontrivially. In this way, we acquire Paulian stabilizers that can correct E on a single qubit:

$$\big(U_iZ_iU_i^{-1}\big)\big(U_{i+1}Z_{i+1}U_{i+1}^{-1}\big), \; i = 1, \ldots, n-1. \tag{43}$$

Hence, we can correct any error that is a normal operator on a single qubit; specifically, the normal operator can be any unitary operator.

B. Bosonic codes

Let's first consider this bosonic binomial code [70–72]:

$$|\overline{1}\rangle := |2\rangle, \; |\overline{-1}\rangle := (|4\rangle + |0\rangle)/\sqrt{2}, \tag{44}$$

which was experimentally demonstrated in Ref. [71] and can correct orthogonal errors I and the annihilation operator a. The space can be partitioned according to parity [70–73]—The code space $\mathcal{H}_{\text{C}} \subset \mathcal{H}_{(1)}$ has even parity while $a\mathcal{H}_{\text{C}} \subset \mathcal{H}_{(-1)}$ has odd parity. With $N := a^\dagger a$, the parity operator

$$Z^{\text{S}} = e^{i\pi N} \tag{45}$$

is actually Paulian (see Sec. II B):

(1) It is clear that (45) is unitary.

(2) Because its eigenvalues are ±1, it is an involution.

(3) Finally, because $\{|2n-2\rangle\}_{n\in\mathbb{N}}$ and $\{|2n-1\rangle\}_{n\in\mathbb{N}}$ are the bases of its ±1-eigenspaces, their orthonormal bases have the same cardinality. Namely we can establish a bijection between $\{|2n-2\rangle\}_{n\in\mathbb{N}}$ and $\{|2n-1\rangle\}_{n\in\mathbb{N}}$. The two eigenspaces are thus isomorphic.

The parity operator is Paulian on the whole space, i.e., $\mathcal{H}' = \mathcal{H}$, which is infinite-dimensional. To measure the syndrome, the controlled phase gate $I \otimes |-1\rangle\langle -1| + e^{i\pi N} \otimes$

$|1\rangle\langle 1|$ [73,74] is the controlled operations (27) and (30) along with appropriate rotation on the ancilla.

The next one is the bosonic code from Ref. [75]:

$$|\bar{1}\rangle := |22\rangle,\ \ |\overline{-1}\rangle := (|40\rangle + |04\rangle)/\sqrt{2}, \tag{46}$$

which protects up to one photon loss, and we have the following orthogonal correctable errors [72,75]:

$$\mathbb{E} = \{I,\, A_{1,1}, A_{1,2}\}, \tag{47}$$

where $A_{i,j}$ is the damping operator for which the jth mode losing i photons (hence I corresponds to $A_{0,1}$ and $A_{0,2}$). We can again choose parity operators as the Paulian stabilizers:

$$Z_1^{\mathrm{S}} = e^{i\pi N_1},\quad Z_2^{\mathrm{S}} = e^{i\pi N_2}. \tag{48}$$

The correctable errors I, $A_{1,1}$ and $A_{1,2}$ will have syndromes $(I) = (1, 1)$, $(-1, 1)$, and $(1, -1)$, respectively. Note in this case, we not only extend the domains to the entire space but also enlarge the Paulian group as $2 = \lceil \log_2 3\rceil > \lfloor \log_2 3\rfloor = 1$; see Secs. III B and III C. Photon loss for the bosonic four-legged cat code can also be detected by parity [72,76–78], so we also have a Paulian stabilizer for such a code.

Finally, in Appendix G we will have a brief discussion about Gottesman-Kitaev-Preskill codes [72,79,80], where we will show a way to construct commutative Paulian stabilizers for these codes and issues with them.

C. Codeword stabilized code

For an n-qubits system, a codeword stabilized code [49,50,81] is obtained in the following way:

(1) We start with a maximally linearly independent and abelian subgroup of a Pauli group (please refer to Appendix D for the exact meaning), called the *word stabilizer*.

(2) We also need a set of Pauli operators $\{W_i\}$, called the *word operators*.

(3) As the word stabilizer is maximally linearly independent and abelian, each of its simultaneous eigenspace is one-dimensional, i.e., it stabilizes a unique quantum state; let it be $|\psi\rangle$.

(4) The codewords are then $W_i|\psi\rangle$'s; i.e., the code space is $\mathrm{span}\{W_i|\psi\rangle\}$.

The following result can be utilized to construct Paulian stabilizers of a codeword stabilized code:

Corollary 2. For a codeword stabilized code:

(1) If P_1 and P_2 are correctable Pauli errors, they are either orthonormal or act identically on the code space bar a multiplication factor.

(2) Assuming the code has distance d, it is nondegenerate [1,2] if and only if every operator in the word stabilizer except I has distance no smaller than d.

In Appendix F, specifically Sec. F 2, we provide a procedure to construct Paulian stabilizers that is applicable to every codeword stabilized code; here is the essence: We first determine whether there exist Paulian stabilizers that can correct all the relevant errors by (20) or (24); then according to Corollary 2 we can choose linearly independent Pauli errors as orthonormal correctable errors, and to be definite we can check whether the code is nondegenerate again by Corollary 2. We then use the simultaneous eigenspaces of the word stabilizer to build syndrome spaces, which lead to Paulian stabilizers.

An example would be the ((9, 12, 3)) code from Refs. [50,82]: Each element of the word stabilizer except I has at least weight 3, so the code is nondegenerate according to Corollary 2, and we can choose all linearly independent weight-1 Pauli errors, along with I as the orthonormal errors $\mathbb{F}$ of (2). By (23),

$$|\mathbb{F}| = 3\times 9 + 1 = 28,$$

so (20) [or (24)] is satisfied, and we can construct a Paulian stabilizer group to correct all the relevant errors, generated by $\log_2 |\mathbb{F}| = 5$ Paulian operators. Furthermore, we can extend the stabilizers so that each is Paulian on the whole space.

In fact, "Paulian stabilizers" for this code have already been found in Ref. [82], among which some are Pauli.[3] Note, however, that the "Paulian stabilizers" from Ref. [82] possess a different structure from those presented in this work: The Paulian stabilizers of Proposition 1 are elements of a faithful representation of the Pauli group, so they are reminiscent of Pauli stabilizers of a Pauli stabilizer code. On the other hand, those from Ref. [82] are not, so different sequences of measurements are needed for different errors, and more than five observables are needed to detect all the errors, whereas with the Paulian stabilizers of Proposition 1 we require only five commutative observables for measurement. Even though Paulian stabilizers like those in Ref. [82] are interesting and useful *per se*, we will not delve into them. More details about this code can be found in Appendix F 4.

Now let's consider the ((5, 6, 2)) code from Refs. [50,83]. Due to its distance, this code is an error-detecting code. It can be found that, with $\mathbb{P}_1$ denoting the set of all weight-1 Pauli errors, we have

$$\mathcal{H}_{\mathrm{C}}^{\perp} = \sum_{P\in\mathbb{P}_1} P\mathcal{H}_{\mathrm{C}}, \tag{49}$$

which implies for the stabilizers to detect all errors in $\mathbb{P}_1$, we must have

$$\mathcal{H}_{\mathrm{C}} = \mathcal{H}_{(I)}, \tag{50}$$

$$\mathcal{H}_{\mathrm{C}}^{\perp} = \bigoplus_{(t)\in\mathbb{T}\setminus\{(I)\}} \mathcal{H}_{(t)}, \tag{51}$$

where $\mathbb{T}$ is the set of all syndromes; see Sec. III A. For the stabilizers to be Paulian and commutative, each syndrome space must have the same dimension, so (50) and (51) together imply

$$\dim\mathcal{H} = 2^m \dim\mathcal{H}_{\mathrm{C}} \tag{52}$$

for some positive integer m, which is impossible for this system as $\dim\mathcal{H}_{\mathrm{C}} = 6$ and $\dim\mathcal{H} = 2^5 = 32$.

Hence, we cannot find commutative Paulian stabilizers for the ((5, 6, 2)) code to detect all weight-1 errors. This is one of the cases where Paulian stabilizer groups may not be suitable for error correction or detection; cf. the discussion in

[3] That this code can be stabilized by nontrivial Pauli operators can also be verified with Corollary 3 in Appendix F.

Sec. III B. Regardless, because this code has low dimensions, it is easier to demonstrate how to find its Paulian stabilizers as every step can be made explicit without being too clumsy; in addition, we can show how to adapt our approach to error-detecting codes. Details can be found in Appendix F 3.

VI. DISCUSSION AND CONCLUSION

We showed that every quantum error-correcting code, including the subsystem code, can be stabilized by operators which are Paulian and commutative to the restriction of a subspace $\mathcal{H}'$, which may or may not be the entire system $\mathcal{H}$ (Proposition 1 and Corollary 1), with examples given in Sec. V. Also, we showed that the error syndrome can be obtained by measuring the Paulian stabilizers Z_i^{S}'s, which can be achieved by performing controlled operations $\mathrm{C}Z_i^{\mathrm{S}}$'s, so the quantum circuits for conducting Z_i^{S}'s can be transferred to those for measuring them (Sec. III D).

In terms of tensor product structure [84–86], $\mathcal{H}'$ is composed of m stabilizer qubits [38] generated by the Paulian operators, and a subsystem isomorphic to the syndrome spaces, whose dimension k' is no less than $\dim \mathcal{H}_{\mathrm{C}}$, so we can embed $\mathcal{H}_{\mathrm{C}}$ into them. This generalizes the observation made in Refs. [38,86], that for a system composed of qubits, commutative Paulian operators can partition the system into virtual qubits; if the Paulian operators are Pauli it becomes a Pauli stabilizer code.

Paulian stabilizers may be employed to realize codes that are not Pauli stabilizer codes, showcased in Sec. V B. As discussed in Sec. III B, (20) is the condition for Paulian stabilizers to cover all correctable errors. Hence, binary codes may in particular benefit from the existence of Paulian stabilizers, because (20) is always satisfied; the same is true in the case where the code space is finite-dimensional while the entire system is infinite-dimensional, such as the bosonic codes in Sec. V B. Furthermore, as we have demonstrated how to obtain the Paulian stabilizer group of a binary concatenated code in Sec. IV, it may help us obtain a code with higher distance along with the means to realize it.

There are questions still left unanswered that may be worthy of further investigation: There is no unique Paulian stabilizer group for a code, and the ideal Paulian stabilizers are those that are easy to measure or conduct. With a universal set of quantum gates, we can in theory approach them [4,48], but it may need many gates to implement. Hence, for Paulian stabilizers to be useful, how to find the ideal ones is a key issue, which depends on the physical system in question. Also, we showed the existence of Paulian stabilizers for error-correcting codes, but knowing this, can it help us find nontrivial new codes by using Paulian operators that are not Pauli as the stabilizers or correctable errors?

ACKNOWLEDGMENTS

J.-Y.K. would like to thank Prof. Chung-Hsien Chou for introducing him to this area of research, and we thank Dr. Tanmay Singal for very fruitful discussions about various aspects of quantum error correction. H.-S.G. acknowledges support from the National Science and Technology Council, Taiwan, under Grants No. NSTC 112-2119-M-002-014, No. NSTC 111-2119-M-002-006-MY3, No. NSTC 111-2119-M-002-007, No. NSTC 110-2627-M-002-002, No. NSTC 111-2627-M-002-001, and No. NSTC 111-2627-M-002-006, from the U.S. Air Force Office of Scientific Research under Award No. FA9550-23-S-0001, and from the National Taiwan University under Grant No. NTU-CC-112L893404. H.-S.G. is also grateful for the support from the Center for Advanced Computing and Imaging in Biomedicine (NTU-112L900702) through the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE), Taiwan, and the support from the Physics Division, National Center for Theoretical Sciences, Taiwan.

APPENDIX A: GENERALIZED CNOT

Consider any self-adjoint Paulian operator P on $\mathcal{H}$, and an ancilla qubit $\mathcal{H}_{\mathrm{A}} \cong \mathbb{C}^2$. We define the corresponding generalized CNOT as the following unitary operator on $\mathcal{H} \otimes \mathcal{H}_{\mathrm{A}}$:

$$\mathrm{GCNOT} := \Pi_- \otimes X_{\mathrm{A}} + \Pi_+ \otimes I_{\mathrm{A}}, \tag{A1}$$

where $\Pi_\pm$ are the orthogonal projections onto the ± 1-eigenspaces of P and A refers to the ancilla qubit. Here let's have a quick discussion about why GCNOT is equal to

$$I_{\mathcal{H}} \otimes \Pi_+^{\mathrm{A}} + P \otimes \Pi_-^{\mathrm{A}}, \tag{A2}$$

where

$$\Pi_\pm^{\mathrm{A}} := |\pm\rangle_{\mathrm{A}} \langle \pm|_{\mathrm{A}} \tag{A3}$$

are orthogonal projections onto the ± 1-eigenspaces of X_{A}.

If P has only one eigenvalue, then P is either $I_{\mathcal{H}}$ or $-I_{\mathcal{H}}$. For the former, it is fairly easy to see both (A1) and (A2) are $I_{\mathcal{H}} \otimes I_{\mathrm{A}}$, so they are identical. For the latter, (A1) becomes $I_{\mathcal{H}} \otimes X_{\mathrm{A}}$, whereas (A2) becomes

$$\begin{aligned} I_{\mathcal{H}} \otimes \Pi_+^{\mathrm{A}} - I_{\mathcal{H}} \otimes \Pi_-^{\mathrm{A}} &= I_{\mathcal{H}} \otimes (\Pi_+^{\mathrm{A}} - \Pi_-^{\mathrm{A}}) \\ &= I_{\mathcal{H}} \otimes X_{\mathrm{A}}, \end{aligned} \tag{A4}$$

so they are again the same.

If P has two eigenvalues, namely, ± 1, then we have

$$\begin{aligned} \Pi_- \otimes X_{\mathrm{A}} + \Pi_+ \otimes I_{\mathrm{A}} &= \Pi_- \otimes (\Pi_+^{\mathrm{A}} - \Pi_-^{\mathrm{A}}) \\ &\quad + \Pi_+ \otimes (\Pi_+^{\mathrm{A}} + \Pi_-^{\mathrm{A}}) \\ &= (\Pi_+ + \Pi_-) \otimes \Pi_+^{\mathrm{A}} \\ &\quad + (\Pi_+ - \Pi_-) \otimes \Pi_-^{\mathrm{A}} \\ &= I_{\mathcal{H}} \otimes \Pi_+^{\mathrm{A}} + P \otimes \Pi_-^{\mathrm{A}}, \end{aligned} \tag{A5}$$

which is (A2).

In fact, as the relations above do not depend on the dimension of the eigenspaces of X_{A}, we can replace the ancilla qubit with a system with even dimension and X_{A} with another Paulian operator, and identical results will hold.

Second, let's try to answer this question: Given a Paulian operator P, is the generalized CNOT of (A1) the only [besides a global phase factor or a phase difference between the two terms on the right-hand side of (A1)] unitary operator that can achieve what we want of it? Specifically, let $\overline{\mathrm{GCNOT}}$ denote the "most general" GCNOT for P; the property we desire is

$$(I\otimes\Pi_+^{\mathrm{A}})\overline{\text{GCNOT}}(|\psi\rangle\otimes|1\rangle)=e^{i\theta_+}(\Pi_+|\psi\rangle)\otimes|1\rangle,$$
$$(I\otimes\Pi_-^{\mathrm{A}})\overline{\text{GCNOT}}(|\psi\rangle\otimes|1\rangle)=e^{i\theta_-}(\Pi_-|\psi\rangle)\otimes|-1\rangle,\quad\text{(A6)}$$

for every $|\psi\rangle\in\mathcal{H}$, where $\theta_\pm\in[0,2\pi)$. Thus,

$$\begin{aligned}\overline{\text{GCNOT}}(|\psi\rangle\otimes|1\rangle)&=(I\otimes\Pi_+^{\mathrm{A}}+I\otimes\Pi_-^{\mathrm{A}})\overline{\text{GCNOT}}(|\psi\rangle\otimes|1\rangle)\\&=e^{i\theta_+}(\Pi_+|\psi\rangle)\otimes|1\rangle\\&\quad+e^{i\theta_-}(\Pi_-|\psi\rangle)\otimes|-1\rangle.\end{aligned}\quad\text{(A7)}$$

This defines the action of $\overline{\text{GCNOT}}$ on $\mathcal{H}\otimes|1\rangle$,[4] so we can complete it by defining it on the orthogonal complement, namely, $\mathcal{H}\otimes|-1\rangle$. Note

$$\overline{\text{GCNOT}}(\mathcal{H}\otimes|1\rangle)=\mathcal{H}_+\otimes|1\rangle\oplus\mathcal{H}_-\otimes|-1\rangle,\quad\text{(A8)}$$

where $\mathcal{H}_\pm$ are the ±1-eigenspaces of the Paulian operator P. As $\overline{\text{GCNOT}}$ is unitary,

$$\overline{\text{GCNOT}}(\mathcal{H}\otimes|1\rangle)\perp\overline{\text{GCNOT}}(\mathcal{H}\otimes|-1\rangle),\quad\text{(A9)}$$

which suggests

$$\overline{\text{GCNOT}}(\mathcal{H}\otimes|-1\rangle)=\mathcal{H}_-\otimes|1\rangle\oplus\mathcal{H}_+\otimes|-1\rangle.\quad\text{(A10)}$$

$\overline{\text{GCNOT}}|_{\mathcal{H}\otimes|-1\rangle}$ can therefore be any unitary map from $\mathcal{H}\otimes|-1\rangle$ to $\mathcal{H}_-\otimes|1\rangle\oplus\mathcal{H}_+\otimes|-1\rangle$; a simple example is

$$\begin{aligned}\overline{\text{GCNOT}}(|\psi\rangle\otimes|-1\rangle)&:=(U_-\Pi_-|\psi\rangle)\otimes|1\rangle\\&\quad+(U_+\Pi_+|\psi\rangle)\otimes|-1\rangle,\end{aligned}\quad\text{(A11)}$$

where $U_\pm$ are any unitary maps from $\mathcal{H}_\pm$ to themselves (i.e., operators); we may also choose

$$\begin{aligned}\overline{\text{GCNOT}}(|\psi\rangle\otimes|-1\rangle)&:=(U'_+\Pi_+|\psi\rangle)\otimes|1\rangle\\&\quad+(U'_-\Pi_-|\psi\rangle)\otimes|-1\rangle,\end{aligned}\quad\text{(A12)}$$

where $U'_\pm$ are any unitary maps from $\mathcal{H}_\pm$ to $\mathcal{H}_\mp$. (A1) is a special case of (A11) with $U_\pm$ being identities and $\theta_\pm$ of (A6) both being 0.

APPENDIX B: CODE PARAMETERS AND CODEWORDS OF A CONCATENATED BINARY CODE

Because $\mathcal{H}_+$ is $\mathcal{H}_{\text{in}}^{\otimes q}$ and there are $q(n_{\text{in}}-k_{\text{in}})$ of $Z_{i,j}^+$'s and $n_{\text{out}}-k_{\text{out}}$ of Z_i^+'s,

$$n_+=n_{\text{in}}q,\quad\text{(B1)}$$

$$k_+=n_{\text{in}}q-q(n_{\text{in}}-k_{\text{in}})-(n_{\text{out}}-k_{\text{out}})=k_{\text{out}}.\quad\text{(B2)}$$

When $k_{\text{out}}=k_{\text{in}}=1$, $n_+=n_{\text{in}}n_{\text{out}}$ and $k_+=1$, as expected [2,48]. That $k_+=k_{\text{out}}$ is also obvious from the way the codewords are obtained, as will be shown below.

To find the distance, in the simple case of $k_{\text{in}}=1$, to change the logical state of the concatenated code an operator has to act nontrivially on at least d_{out} inner logical qubits; for the logical state of the inner code to change, the operator needs to act nontrivially on at least d_{in} physical qubits of $\mathcal{H}_{\text{in}}$, so the distance is at least $d_{\text{out}}d_{\text{in}}$ [1,2,67].

More generally:

(i) To change the logical state of the concatenated code at least d_{out} inner logical qubits should be acted upon nontrivially.

(ii) Each $\mathcal{H}_{\text{in}}$ subsystem contains k_{in} inner logical qubits.

(iii) To change the logical state of an $\mathcal{H}_{\text{in}}$ system, i.e., the state of its logical qubits, at least d_{in} physical qubits need to be acted on nontrivially.

Therefore, the distance of the concatenated code satisfies [1,2,67]

$$d_+\geqslant\lceil d_{\text{out}}/k_{\text{in}}\rceil d_{\text{in}}.\quad\text{(B3)}$$

We can obtain the codewords given those of the outer and inner codes. For example, say that $(|1,-1,-1,1\rangle+|-1,-1,-1,-1\rangle)/\sqrt{2}$ is a codeword of the outer code, and the inner code has two logical qubits. This codeword will become

$$(\overline{|1,-1\rangle}\otimes\overline{|-1,1\rangle}+\overline{|-1,-1\rangle}\otimes\overline{|-1,-1\rangle})/\sqrt{2},$$

where $\overline{|i,j\rangle}\in\mathcal{H}_{\text{in,C}}$ are logical states of the inner code, i for the first logical qubit and j for the second one.

So far we have taken the outer code as composed of n_{out} qubits, but we can treat it as composed of q subsystems each with dimension $\dim\mathcal{H}_{\text{in,C}}$ instead. We can then follow the standard procedure for finding the codewords and parameters of a concatenated code as in, e.g., Refs. [1,44,67,68]: Replacing each $\dim\mathcal{H}_{\text{in,C}}$-dimensional subsystem of the outer code by $\mathcal{H}_{\text{in}}$, the concatenated code hence has $\dim\mathcal{H}_+=(2^{n_{\text{in}}})^q$ and $\dim\mathcal{H}_{+,\text{C}}=2^{k_{\text{out}}}$. The distance is no smaller than the product of that of the outer code and that of the inner one; note as compared to when it is regarded as composed of qubits, the distance of the outer code now should be reduced by a factor of k_{in} because each of its q subsystems is composed of k_{in} qubits.

APPENDIX C: PHASELESS GROUP

For a group of operators G containing $\{I,-I,iI,-iI\}$ as a subgroup, we define

$$\hat{\mathsf{G}}:=\mathsf{G}/\{I,-I,iI,-iI\}.\quad\text{(C1)}$$

As $\{I,-I,iI,-iI\}$ is clearly normal, $\hat{\mathsf{G}}$ is a quotient group [87]. Specifically, for the Pauli group $\hat{\mathsf{P}}^n$ can be regarded as a "phaseless" version of the Pauli group: Abusing the language, we will regard the coset representatives as elements of $\hat{\mathsf{P}}^n$; consequently, we will also call $\hat{\mathsf{P}}^n$ a Pauli group and its elements *Pauli operators*. By removing the phases, $\hat{\mathsf{P}}^n$ becomes linearly independent; in particular, $\hat{\mathsf{P}}^n$ is a basis of $\mathcal{L}(\mathbb{C}^{2^n})$ [1,31,32]. The phaseless Pauli group $\hat{\mathsf{P}}^1$ is isomorphic to the Klein four-group and $\hat{\mathsf{P}}^n$ is isomorphic to the direct product of n copies of the Klein four-group [88].

For the same reason as why we introduced the phaseless Pauli group, given a subgroup of a Pauli/Paulian group, it is convenient to consider the phaseless version of it. As $\{I,-I,iI,-iI\}$ may not always be in such a subgroup, we define the following:

(1) If G has $\{I,-I,iI,-iI\}$ as a subgroup, then its phaseless counterpart is defined like before, i.e., (C1).

(2) If $iI\notin\mathsf{G}$ but $-I\in\mathsf{G}$, then

$$\hat{\mathsf{G}}:=\mathsf{G}/\{I,-I\}.\quad\text{(C2)}$$

[4] $\mathcal{H}\otimes|1\rangle$ and $\mathcal{H}\otimes\text{span}(|1\rangle)$ are identical, so the former is a space as well.

(3) Finally, if $-I \notin \mathsf{G}$,

$$\hat{\mathsf{G}} := \mathsf{G}. \tag{C3}$$

Like before, we take the coset representatives as elements of such a quotient group, which is the reason why we "defined" $\hat{\mathsf{G}}$ as G in (C3). Correspondingly there is arbitrariness in the choice of its elements: Indeed, saying $P \in \hat{\mathsf{G}}$ is no different from saying $P \in \mathsf{G}$. It is only when we compare sets does it make a difference: For example, if we say a set $\mathbb{S}$ is equal to $\hat{\mathsf{G}}$, then there should exist no two elements in $\mathbb{S}$ that differ by a nontrivial multiplication factor; cf. (C3) and later (D1).

APPENDIX D: COMMUTATIVITY OF PAULI SUBGROUPS

Here is a property concerning subgroups of Pauli groups:

Lemma 3. For any subgroup G of a Pauli group, $-I \notin \mathsf{G}$ if and only if G is linearly independent, and only if G is composed wholly of involutions and is abelian.

Proof. Suppose $-I \in \mathsf{G}$. Being a subgroup of the Pauli group, every element of G is either an involution or a counterinvolution. If $A \in \mathsf{G}$ were a counterinvolution, then $A^2 = -I$ would also be in G, a contradiction, so every element is involutory. Next, a pair of Pauli operators either commute or anticommute. If $A, B \in \mathsf{G}$ anticommuted, $ABA^{-1} = -B = (-I)B \in \mathsf{G}$, so $ABA^{-1}B^{-1} = -I \in \mathsf{G}$, a contradiction. Hence every element in G commutes with one another, meaning G is abelian. Note that because $-I$ is an involution and commutes with all operators, G being abelian and comprising purely involutions does not imply $-I \in \mathsf{G}$

Because $\{I, -I\}$ is linearly dependent, clearly a linearly independent subgroup should not contain $-I$. The other way around, assume $-I \notin \mathsf{G}$. Since the phaseless Paulian group (or the collection of its coset representatives) is a basis [1,31,32], any subset of it is also linearly independent. In other words, any subset of a Pauli group, if no element differs from another by a multiplication factor, is linearly independent. As $(iI)^2 = -I$, $-I \notin \mathsf{G}$ implies that iI and $-iI$ are not in G either; if $A \in \mathsf{G}$ and $aA \in \mathsf{G}$ for some nontrivial multiplication factor a (namely, a is -1 or i or $-i$), then $aI \in \mathsf{G}$ because $A^{-1}(aA) = aI$, a contradiction. Hence G is linearly independent. ■

As $-I$ and $\pm iI$ commute with all operators, an abelian subgroup of P^n can contain the subgroup $\{I, -I\}$ or $\{I, -I, iI, -iI\}$, in which case the abelian subgroup is linearly dependent. To get rid of these extra factors, we can take the phaseless group of it, as we did in (C1). When we refer to a subgroup S of a Pauli, or Paulian, group as *maximally linearly independent and abelian*, it means that we cannot add any more Pauli or Paulian operators to it while keeping the subgroup both linearly independent and abelian; to put it another way, S is abelian and

$$\hat{\mathsf{S}} = \mathsf{S}. \tag{D1}$$

Some properties of such a group are revealed by Lemma 3; in particular this lemma shows that for a Pauli or Paulian[5] subgroup to be linearly independent, it must be abelian, so calling it abelian is actually redundant, but it helps show off this important attribute.

APPENDIX E: PROOF FOR LEMMA 2

If: Let $A = aI + bU$ be an operator for which a and b are scalars and U is a unitary operator. Since I and U commute, apparently $A^\dagger A = AA^\dagger$. Note this holds true whether A is on $\mathbb{C}^2$ and whether U is Paulian.

Only if: Let A be a normal operator on $\mathbb{C}^2$. Because it is normal, it is unitarily diagonalizable and the eigenspaces are orthogonal. If there is only one eigenvalue, then A is proportional to I; if it has two different eigenvalues c_1 and c_2, we can solve the equations $c_1 = a + b$ and $c_2 = a - b$. Suppose A becomes diagonal under a unitary V, which in terms of a matrix means

$$VAV^{-1} = \begin{pmatrix} a+b & 0 \\ 0 & a-b \end{pmatrix}. \tag{E1}$$

Consider the matrix of Pauli Z:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \tag{E2}$$

we have $VAV^{-1} = aI + bZ$, so $A = aI + bV^{-1}ZV$. Because $V^{-1}ZV$ is unitarily similar to Z, it has the same spectrum $\{1, -1\}$ and is Paulian.

APPENDIX F: CODEWORD STABILIZED CODES

First, we will establish some properties of codeword stabilized codes that are essential in constructing Paulian stabilizers in Sec. F 1, and then we will provide the steps to do so, and details of the two codes from Sec. V C. In the following discussion we will assume the system is composed of n qubits; please refer to Sec. V C for the relevant terminologies and how codeword stabilized codes are constructed.

In this section we will express Pauli operators in the following way, e.g.,

$$XIZ = X \otimes I \otimes Z, \tag{F1}$$

and suppose the system is composed of three qubits:

$$X_2 = I \otimes X \otimes I = IXI. \tag{F2}$$

In addition, I in this subsection will refer to the identity operator on a single qubit. To distinguish the identity operator on the whole system from those on individual qubits, we will label the former as I_n, assuming the whole system is composed of n qubits, so, e.g.,

$$I_3 = III. \tag{F3}$$

1. Preliminaries

Let S_w denote the word stabilizer. In general we will consider a particular generating set g of S_w, which will be taken as a tuple of generators, so we can associate each simultaneous eigenspace of S_w with a unique n-tuple of ± 1 that is the simultaneous eigenvalues with respect to g, just like the error syndromes in relation to Paulian stabilizers. Such a tuple of simultaneous eigenvalues will be denoted by $\hat{t}$, and the set of all these tuples by $\mathbb{W}$. Like the tuples of syndromes (t),

[5] In this work a Paulian group is unitarily similar to a "Pauli" group (see Sec. III A), so Lemma 3 also holds for Paulian subgroups.

we will use $\hat{t}$ to label spaces and the like, e.g., $\mathcal{H}_{\hat{t}}$ is the $\hat{t}$-simultaneous eigenspace of g, which, to put another way, is a bijective map from $\mathbb{W}$ to the collection of all simultaneous eigenspaces of S_w or g:

$$\mathbb{W} \ni \hat{t} \mapsto \mathcal{H}_{\hat{t}}; \tag{F4}$$

cf. the syndrome map in Sec. III A.

Let the state stabilized by the word stabilizer be $|s\rangle$, and W be any Pauli operator in P^n. Due to commutativity and anticommutativity, for any simultaneous eigenvector of a set or group of commutative Pauli operators, after acted upon by a Pauli operator it is still a simultaneous eigenvector of the same set or group of Pauli operators, so $W|s\rangle$ is also a simultaneous eigenvector of S_w, which implies the following:

Lemma 4. Given a codeword stabilized code, for two Pauli operators $P_1, P_2 \in \mathsf{P}^n$, either $P_1|s\rangle \propto P_2|s\rangle$ or $P_1|s\rangle \perp P_2|s\rangle$. Hence, either $P_1\mathcal{H}_\mathrm{C} \perp P_2\mathcal{H}_\mathrm{C}$ or $P_1\mathcal{H}_\mathrm{C} \cap P_2\mathcal{H}_\mathrm{C} \neq \{0\}$, i.e., $P_1\mathcal{H}_\mathrm{C} \perp P_2\mathcal{H}_\mathrm{C}$ if and only if $P_1\mathcal{H}_\mathrm{C} \cap P_2\mathcal{H}_\mathrm{C} = \{0\}$.

Proof. Since $P_1|s\rangle$ and $P_2|s\rangle$ are both simultaneous eigenvectors of S_w, and because each simultaneous eigenspace is one-dimensional, they are either in the same eigenspace, i.e., proportional or orthogonal. Likewise, as $\mathcal{H}_\mathrm{C}$ is an orthogonal direct sum of simultaneous eigenspaces of S_w, so are $P_1\mathcal{H}_\mathrm{C}$ and $P_2\mathcal{H}_\mathrm{C}$. Again, because the simultaneous eigenspaces of S_w are one-dimensional, either $P_1\mathcal{H}_\mathrm{C} \perp P_2\mathcal{H}_\mathrm{C}$ or $P_1\mathcal{H}_\mathrm{C} \cap P_2\mathcal{H}_\mathrm{C} \neq \{0\}$. ■

This lemma leads to

Corollary 3. For a codeword stabilized code, a Pauli operator P obeys $P|_\mathrm{C} \propto I_\mathrm{C}$ if and only if $P \in \mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$ and P commutes, or anticommutes, with all the word operators at the same time. In other words, a Pauli operator P stabilizes the code if and only if

(1) Either $P \in \mathsf{S}_w$ and P commutes with all the word operators

(2) Or $P \in -\mathsf{S}_w$ and P anticommutes with all the word operators.

Clearly, if I_n is a word operator, the only possibility is P commuting with all the word operators.

As we discussed in Sec. D, because S_w is a maximal linearly independent and abelian subgroup of P^n, $\mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$ is a maximal abelian subgroup. A Pauli stabilizer for a codeword stabilizer code that is guaranteed to exist is I. As shown in Ref. [50], Pauli stabilizer codes are a special case of codeword stabilizer codes, which of course have nontrivial Pauli stabilizers.

Proof. Given a Pauli operator $W \in \mathsf{P}^n$, for $W|s\rangle$ to be an eigenvector of another Pauli operator P, P must commute with all elements in S_w as $W|s\rangle$ is a simultaneous eigenvector of S_w; because S_w is a maximal linearly independent and abelian subgroup of P^n, it implies $P \in \mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$. Furthermore, if $PW = \pm WP$, $PW|s\rangle = \pm WP|s\rangle$, which leads to the requirement on commutation relations between P and the word operators. The other direction is pretty obvious and hence omitted. ■

An error E is detectable if and only if E satisfies [48,50]

$$\Pi_\mathrm{C} E \Pi_\mathrm{C} \propto \Pi_\mathrm{C}. \tag{F5}$$

The following lemma considers a property of detectable errors:

Lemma 5. Let E be a unitary operator which obeys $\Pi_\mathrm{C} E \Pi_\mathrm{C} = a\Pi_\mathrm{C}$ for some scalar a; note $|a| \leqslant 1$ by unitarity of E. For such an operator we can find the following:

(i) $|a| = 0$ if and only if $E\mathcal{H}_\mathrm{C} \perp \mathcal{H}_\mathrm{C}$, in which case $E\mathcal{H}_\mathrm{C} \cap \mathcal{H}_\mathrm{C} = \{0\}$.

(ii) $|a| = 1$ if and only if $E|_\mathrm{C} = e^{i\theta}I_\mathrm{C}$ for some real θ, in which case $E\mathcal{H}_\mathrm{C} = \mathcal{H}_\mathrm{C}$.

(iii) $|a| \in (0, 1)$ if and only if $E\mathcal{H}_\mathrm{C}$ and $\mathcal{H}_\mathrm{C}$ are not orthogonal and $E\mathcal{H}_\mathrm{C} \cap \mathcal{H}_\mathrm{C} = \{0\}$.

Correspondingly, the following conditions are equivalent:

(I) $|a| = 1$.

(II) $E|_\mathrm{C} = e^{i\theta}I_\mathrm{C}$ for some real θ.

(III) $E\mathcal{H}_\mathrm{C} = \mathcal{H}_\mathrm{C}$.

(IV) $E\mathcal{H}_\mathrm{C} \cap \mathcal{H}_\mathrm{C} \neq \{0\}$.

Proof. (i) is obvious.

(ii) It is apparent that $E|_\mathrm{C} = e^{i\theta}I_\mathrm{C}$ implies $a = e^{i\theta}$ and thus $|a| = 1$. To show the converse, we first note

$$||\Pi_\mathrm{C}|w\rangle|| \leqslant |||w\rangle|| \tag{F6}$$

which becomes an equality if and only if $|w\rangle \in \mathcal{H}_\mathrm{C}$. Now, consider any $|v\rangle \in \mathcal{H}_\mathrm{C}$ and let $a = e^{i\theta}$ we have

$$\begin{aligned} |||v\rangle|| &= ||\Pi_\mathrm{C} E \Pi_\mathrm{C}|v\rangle|| \\ &\leqslant ||E|v\rangle|| = |||v\rangle||, \end{aligned} \tag{F7}$$

implying $E|v\rangle \in \mathcal{H}_\mathrm{C}$. As this is true for all $|v\rangle \in \mathcal{H}_\mathrm{C}$ and E is unitary, we have $E\mathcal{H}_\mathrm{C} = \mathcal{H}_\mathrm{C}$. Next, since $e^{i\theta}|v\rangle = \Pi_\mathrm{C} E|v\rangle = E|v\rangle$ for all $|v\rangle \in \mathcal{H}_\mathrm{C}$, we obtain $E|_\mathrm{C} = e^{i\theta}I_\mathrm{C}$.

(iii) If $E\mathcal{H}_\mathrm{C} \cap \mathcal{H}_\mathrm{C} = \{0\}$, for any nonzero $|v\rangle \in \mathcal{H}_\mathrm{C}$, because $E\Pi_\mathrm{C}|v\rangle = E|v\rangle \notin \mathcal{H}_\mathrm{C}$,

$$\begin{aligned} |a|\,|||v\rangle|| &= ||\Pi_\mathrm{C} E \Pi_\mathrm{C}|v\rangle|| \\ &< ||E|v\rangle|| \\ &= |||v\rangle||, \end{aligned} \tag{F8}$$

implying $|a| < 1$, and because $E\mathcal{H}_\mathrm{C}$ and $\mathcal{H}_\mathrm{C}$ are not orthogonal, $|a| > 0$. On the contrary, when $|a| \in (0, 1)$, since $a \neq 0$, $E\mathcal{H}_\mathrm{C}$ must not be orthogonal to $\mathcal{H}_\mathrm{C}$. Should $E\mathcal{H}_\mathrm{C}$ and $\mathcal{H}_\mathrm{C}$ have nontrivial intersection, there exist nonzero $|v\rangle \in \mathcal{H}_\mathrm{C}$ such that $E|v\rangle \in \mathcal{H}_\mathrm{C}$, and for such $|v\rangle$, we have $||E\Pi_\mathrm{C}|v\rangle|| = ||E|v\rangle|| = |||v\rangle||$, so

$$|a|\,|||v\rangle|| = ||\Pi_\mathrm{C} E \Pi_\mathrm{C}|v\rangle|| = |||v\rangle||, \tag{F9}$$

a contradiction; therefore $E\mathcal{H}_\mathrm{C} \cap \mathcal{H}_\mathrm{C} = \{0\}$.

Let's go on to show why conditions (I) to (IV) are equivalent:

(1) By (ii), (I) → (II), and (II) → (III).

(2) Clearly (III) → (IV).

(3) Because only when $|a| = 1$ do $E\mathcal{H}_\mathrm{C}$ and $\mathcal{H}_\mathrm{C}$ intersect nontrivially, (IV) implies (I).

This completes the proof. ■

Corollary 4. For a codeword stabilized code:

(a) Every detectable Pauli error P obeys either $P\mathcal{H}_\mathrm{C} \perp \mathcal{H}_\mathrm{C}$ or $P \in \mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$; in the latter case $P|_\mathrm{C} \propto I_\mathrm{C}$ and it is hence also correctable.

(b) For every pair of correctable Pauli errors P_1 and P_2, either P_1 and P_2 are orthonormal or there exists $S \in \mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$ such that $P_2 = P_1S$; in the latter case $S|_\mathrm{C} \propto I_\mathrm{C}$ so $P_2|_\mathrm{C} \propto P_1|_\mathrm{C}$.

Note that a correctable unitary operator is "normalized" according to our definition, so a correctable Pauli error is normalized.

Proof. (a): As the Pauli error P is detectable, we will make use of Lemma 5: If $P\mathcal{H}_\mathrm{C} = \mathcal{H}_\mathrm{C}$, it obeys condition (ii) of Lemma 5, and according to Corollary 3 it must be in $\mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$; if not, it satisfies either (i) or (iii) of Lemma 5. As Lemma 4 shows, (iii) cannot occur, so only (i) and (ii) are possible, completing the proof for (a).

(b): For correctable Pauli operators P_1 and P_2, they satisfy $\Pi_\mathrm{C} P_1^\dagger P_2 \Pi_\mathrm{C} \propto \Pi_\mathrm{C}$. By Lemma 4, either $P_1\mathcal{H}_\mathrm{C} \perp P_2\mathcal{H}_\mathrm{C}$ or $P_1\mathcal{H}_\mathrm{C} \cap P_2\mathcal{H}_\mathrm{C} \neq \{0\}$. If it is the former, $\Pi_\mathrm{C} P_1^\dagger P_2 \Pi_\mathrm{C} = 0$, i.e., they are orthonormal. If the latter, $\Pi_\mathrm{C} P_1^\dagger P_2 \Pi_\mathrm{C} \neq 0$, in which case we must have $P_1\mathcal{H}_\mathrm{C} = P_2\mathcal{H}_\mathrm{C}$ and they must act identically except for a multiplication factor on $\mathcal{H}_\mathrm{C}$, else one could not invert the action of the other on $\mathcal{H}_\mathrm{C}$. As $S := P_1^{-1}P_2$ is also a Pauli operator and $S|_\mathrm{C} \propto I_\mathrm{C}$, $S \in \mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$ by Corollary 3. ■

Corollary 2 is (iv) of the following corollary combined with (a) of Corollary 4; below "wt" refers to the weight of an operator:

Corollary 5. Consider an n-qubit codeword stabilized code with distance d, for which $\mathrm{wt}S \geqslant d$ for all $S \in \mathsf{S}_w \setminus \{I_n\}$.

(i) If $P \in \mathsf{P}^n$ has $\mathrm{wt}P < d$ and is not proportional to I_n, then I_n and P are orthogonal.

(ii) For $P_1, P_2, P_1P_2 \in \mathsf{P}^n$, suppose that their weights are all less than d and that they are linearly independent; then elements in $\{I_n, P_1, P_2, P_1P_2\}$ are mutually orthogonal.

(iii) For a pair of operators in P^n, if their weights are both no higher than $\lfloor (d-1)/2 \rfloor$ and if they are not proportional to each other, they are orthonormal.

(iv) The code is nondegenerate [1,2]: Indeed, for a codeword stabilized code with distance d, it is nondegenerate if and only if $\mathrm{wt}S \geqslant d$ for all $S \in \mathsf{S}_w \setminus \{I_n\}$.

Note this corollary does not imply that a codeword stabilized code whose word stabilizers obey the condition on weights above will have distance d. The code having distance d is part of the assumption. Also, it may seem weird at first sight that word operators did not show up, even though they are essential in formulating a codeword stabilizer code. Their roles here are implicit: As we have assumed the code has distance d, Pauli errors of certain weights must obey specific conditions with the word stabilizer and word operators as listed in Ref. [50].

Proof. (i) Because P is not in $\mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$ (due to its weight) and is detectable, Corollary 4 implies P and I_n are orthogonal.

(ii) First, due to their weights and linear independence,[6] P_1, P_2, P_1P_2 are not in $\mathsf{S}_w\{I_n, -I_n, iI_n, -iI_n\}$. Let G be the group generated by P_1, P_2, and their adjoints. By linear independence and the fact that the adjoint of a Pauli operator differs at most by a multiplication factor, we have

$$\hat{\mathsf{G}} = \{I_n, P_1, P_2, P_1P_2\}. \tag{F10}$$

By Corollary 4 or (i) of this corollary, for all $O \in \hat{\mathsf{G}}$ except I_n, $\Pi_\mathrm{C} O \Pi_\mathrm{C} = 0$, so for all $O_1, O_2 \in \hat{\mathsf{G}}$ with $O_1 \neq O_2$

$$\Pi_\mathrm{C} O_1^\dagger O_2 \Pi_\mathrm{C} = 0, \tag{F11}$$

because $O_1^\dagger O_2$ is also in G and is not proportional to I_n; O_1 and O_2 are therefore orthogonal.

(iii) Suppose we have $P_1, P_2 \in \mathsf{P}^n$ that are not proportional to each other and whose weights are no higher than $\lfloor (d-1)/2 \rfloor$. If one of them is proportional to I_n, then they are orthonormal by (i); else P_1P_2 will not be proportional to I_n and $\mathrm{wt}P_1P_2 < d$, so by (ii) P_1 and P_2 are orthonormal.

(iv) By (iii), the condition on weights is a sufficient condition for nondegeneracy. To show it is a necessary condition, suppose there exists $S \in \mathsf{S}_w \setminus \{I_n\}$ whose weight is less than d. From its weight, S is detectable, and because it is in S_w, it must act like an identity on the code space (according to Corollary 4). Then there would exist nontrivial Pauli operators $P_1 \neq P_2$ for which $\mathrm{wt}P_i \leqslant \lfloor (d-1)/2 \rfloor$, $i = 1, 2$ such that $P_1 = P_2 S$, so P_1 and P_2 act the same on the code space, implying the code is degenerate. ■

2. Constructing Paulian stabilizers

In this part we will discuss how to construct Paulian stabilizers for codeword stabilized codes, where we will make heavy use of $\mathcal{H}_{\hat{t}}$'s, i.e., the simultaneous eigenspaces of S_w. Unlike the proof for Proposition 1, we will not attempt to build the minimal group first and expand upon it. A quick reminder: g denotes a tuple of generators of S_w and $\mathbb{W}$ is the collection of all the tuples of simultaneous eigenvalues with respect to g; please refer back to the start of Sec. F 1. Let's lay out the procedure:

(A.1) First, check if (20) is satisfied to see whether it is possible to correct all errors with Paulian stabilizers. Here we will assume this is true; we then choose a set $\mathbb{F}$ of orthonormal correctable Pauli errors. For a code with a given distance, we can use (24), and select linearly independent Pauli errors with weight no higher than $\lfloor (d-1)/2 \rfloor$ as orthonormal correctable errors; specifically, if the code is nondegenerate, which can be easily checked via Corollary 5, we can choose all of them.

(A.2) As discussed in the proof for Lemma 4, $P\mathcal{H}_\mathrm{C}$ is a direct sum of simultaneous eigenspaces of $\mathbb{S}_w$ for any Pauli operator P; hence for $F \in \mathbb{F}$, let $\mathbb{W}_F$ denote the subset of $\mathbb{W}$ such that

$$F\mathcal{H}_\mathrm{C} = \bigoplus_{\hat{t} \in \mathbb{W}_F} \mathcal{H}_{\hat{t}}. \tag{F12}$$

$\mathbb{W}_F$ can be found out by making use of the commutation relations between the word operators and g, and those between the word operators and F.

(A.3) Since

$$\bigoplus_{F \in \mathbb{F}} F\mathcal{H}_\mathrm{C} = \bigoplus_{F \in \mathbb{F}} \bigoplus_{\hat{t} \in \mathbb{W}_F} \mathcal{H}_{\hat{t}}, \tag{F13}$$

and since for all $F_1, F_2 \in \mathbb{F}$

$$\mathbb{W}_{F_1} \cap \mathbb{W}_{F_2} = \varnothing \text{ if } F_1 \neq F_2, \tag{F14}$$

[6] By linear independence none of them can be proportional to I_n.

where $\varnothing$ refers to the empty set, with

$$\mathbb{W}_\perp := \mathbb{W} \setminus \bigcup_{F\in\mathbb{F}} \mathbb{W}_F, \tag{F15}$$

we have

$$\left(\bigoplus_{F\in\mathbb{F}} F\mathcal{H}_{\mathrm{C}}\right)^{\perp} = \bigoplus_{\hat{t}\in\mathbb{W}_\perp} \mathcal{H}_{\hat{t}}. \tag{F16}$$

The set $\mathbb{W}_\perp$ and the associated simultaneous eigenspaces will be used as "spares."

(A.4) Let $m = \lceil \log_2 |\mathbb{F}| \rceil$, and $\mathbb{T}$, as before, be the collection of all m-tuples of ± 1, i.e., syndromes. Choose a unique syndrome for each error in $\mathbb{F}$, namely, a one-to-one map $f_{\mathrm{sym}} : \mathbb{F} \to \mathbb{T}$, the "syndrome map,"[7] and we require $f_{\mathrm{sym}}(I_n) = (I)$, where (I) is the tuple whose components are all 1. If $m > \log_2 |\mathbb{F}|$, there will be "excess" syndromes that do not correspond to correctable errors; i.e., they are members of

$$\mathbb{T} \setminus f_{\mathrm{sym}}(\mathbb{F}). \tag{F17}$$

The total number of excess syndromes is

$$|\mathbb{T} \setminus f_{\mathrm{sym}}(\mathbb{F})| = |\mathbb{T}| - |f_{\mathrm{sym}}(\mathbb{F})| = 2^m - |\mathbb{F}|. \tag{F18}$$

If $m = \log_2 |\mathbb{F}|$, then this already gives us the "minimal" Paulian stabilizers; see Sec. III A and A.6 on how to define Paulian stabilizers given the syndrome spaces.

(A.5) Now let's designate all the syndrome spaces. The properties we desire of them are (cf. Sec. III C):

(a) The syndrome space associated with each error $F \in \mathbb{F}$ should contain $F\mathcal{H}_{\mathrm{C}}$:

$$F\mathcal{H}_{\mathrm{C}} \subseteq \mathcal{H}_{f_{\mathrm{sym}}(F)} \ \forall F \in \mathbb{F}. \tag{F19}$$

(b) The syndrome spaces are orthogonal: For any two distinct syndromes (s) and (t),

$$\mathcal{H}_{(s)} \perp \mathcal{H}_{(t)}. \tag{F20}$$

(c) All syndrome spaces are isomorphic:

$$\mathcal{H}_{(s)} \cong \mathcal{H}_{(t)} \ \forall (s), (t) \in \mathbb{T}. \tag{F21}$$

To achieve them, for every $(t) \in \mathbb{T}$ we choose a subset $\mathbb{W}_{(t)}$ of $\mathbb{W}$ and demand the syndrome spaces be

$$\mathcal{H}_{(t)} := \bigoplus_{\hat{s}\in\mathbb{W}_{(t)}} \mathcal{H}_{\hat{s}}; \tag{F22}$$

$\mathbb{W}_{(t)}$'s shall satisfy the following conditions:

(a) To comply with (F19), for all $(t) \in f_{\mathrm{sym}}(\mathbb{F})$ we require

$$\mathbb{W}_{F_{(t)}} \subseteq \mathbb{W}_{(t)}; \tag{F23}$$

see the definition of $\mathbb{W}_F$ for all $F \in \mathbb{F}$ in (F12).

(b) To satisfy (F20),

$$\mathbb{W}_{(s)} \cap \mathbb{W}_{(t)} = \varnothing \ \forall (s) \neq (t). \tag{F24}$$

(c) To obey (F21),

$$|\mathbb{W}_{(s)}| = |\mathbb{W}_{(t)}| \ \forall (s), (t) \in \mathbb{T}. \tag{F25}$$

Since $\dim \mathcal{H}_{\hat{t}} = 1$, $|\mathbb{W}_{(t)}|$ is the dimension of each syndrome space, and $|\mathbb{W}_{(t)}| - \dim \mathcal{H}_{\mathrm{C}}$ can show how much we extend the domain of the Paulian stabilizers.

Note

$$\mathbb{W}_{(t)} \setminus \mathbb{W}_{F_{(t)}} \subseteq \mathbb{W}_\perp \ \forall (t) \in f_{\mathrm{sym}}(\mathbb{F}), \tag{F26}$$

$$\mathbb{W}_{(t)} \subseteq \mathbb{W}_\perp \ \forall (t) \in \mathbb{T} \setminus f_{\mathrm{sym}}(\mathbb{F}), \tag{F27}$$

so the spares—$\mathbb{W}_\perp$ of (F15) and the associated eigenspaces—are used to fill in each syndrome space. Finally, if the stabilizers are to be Paulian on the entire space $\mathcal{H}$, the dimension of each syndrome space is

$$\dim \mathcal{H}_{(t)} = 2^n/2^m = 2^{n-m}, \tag{F28}$$

i.e., each is composed of $n - m$ qubits.

(A.6) With the syndrome spaces specified, we have the corresponding Paulian stabilizers: For all $i = 1, \ldots, m$,

$$Z_i^{\mathrm{S}} := \Pi_{\bigoplus_{(t)_i=1,(t)\in\mathbb{T},}\mathcal{H}_{(t)}} - \Pi_{\bigoplus_{(t)_i=-1,(t)\in\mathbb{T}}\mathcal{H}_{(t)}}, \tag{F29}$$

where $(t)_i$ is the ith component of (t). The domain of the Paulian stabilizers, $\mathcal{H}'$ of Proposition 1, is thus

$$\mathcal{H}' = \bigoplus_{(t)\in\mathbb{T}} \mathcal{H}_{(t)}. \tag{F30}$$

Defined this way, each Z_i^{S} is clearly Paulian to the restriction of $\mathcal{H}'$. They commute, with (t)-simultaneous eigenspaces $\mathcal{H}_{(t)}$; i.e., (t)'s are the error syndromes and $\mathcal{H}_{(t)}$'s are the corresponding syndrome spaces. Because we have demanded I_n have syndrome (I), Z_i^{S}'s are stabilizers.

In the examples to come, we will demonstrate how to put them into practice.

3. ((5, 6, 2)) code

Let's start off with the ((5, 6, 2)) code from Refs. [50,83]. As discussed in Sec. V C, it is impossible to find a Paulian stabilizer group that can detect all the weight-1 errors for this code, but due to its low dimensions, it is easier to demonstrate the procedure shown in Sec. F 2 with this code, and we can also show how to adapt the methods for error-detecting codes.

The word stabilizer of this code is generated by $ZXZII$ and all its cyclic shifts, i.e.,

$$g = (ZXZII, XZIIZ, ZIIZX, IIZXZ, IZXZI), \tag{F31}$$

and the word operators are

$$IIIII, ZZIZI, IZZIZ, ZIZZI, IZIZZ, ZIZIZ. \tag{F32}$$

Now let's follow the steps listed in Sec. F 2:

A.1: As this code is an error-detecting code, how do we choose orthonormal Pauli errors? In fact, because the code has distance 2, we infer from (ii) of Corollary 5 that $\mathbb{F} = \{X_i, Y_i, Z_i, I_5\}$ is orthonormal for a fixed $i = 1, \ldots, 5$, and we will use them as the orthonormal "correctable" errors.

A.2: We should find $\mathbb{W}_F$ for each $F \in \mathbb{F}$. As a demonstration, we will show how to find $\mathbb{W}_{X_1}$. First, consider the word

[7] The syndrome map in Sec. III A was defined on $\mathbb{F}'$ instead of $\mathbb{F}$, so it was bijective besides injective.

operator $ZZIZI$. Its commutation relation with g of (F31), if expressed as a tuple of ±1 with +1 for commuting and −1 for anticommuting, is

$$(-1, -1, 1, -1, 1), \tag{F33}$$

which is exactly the simultaneous eigenvalues of the vector $ZZIZI|s\rangle$ with respect to g. Repeating for all the word operators, we obtain $\mathcal{H}_C$ as the direct sum of simultaneous eigenspaces of g or S_w. To obtain $\mathbb{W}_{X_1}$, we check how X_1 commutes with g: The commutation relation is

$$(-1, 1, -1, 1, 1), \tag{F34}$$

which means $X_1(ZZIZI|s\rangle)$ has simultaneous eigenvalues

$$\begin{aligned}&(-1\times(-1), -1\times 1, 1\times(-1), -1\times 1, 1\times 1)\\ &\quad= (1, -1, -1, -1, 1),\end{aligned} \tag{F35}$$

namely, multiplications component by component between (F33) and (F34); $(1, -1, -1, -1, 1)$ from (F35) is therefore an element of $\mathbb{W}_{X_1}$. Doing this all over again for all the word operators gives us $\mathbb{W}_{X_1}$.

A.3: After obtaining each $\mathbb{W}_F$, $\mathbb{W}_\perp$ should have $2^5 - \dim \mathcal{H}_C \times 4 = 8$ elements. When $i = 1$, they are

$$\begin{aligned}\hat{a} &:= (-1, -1, -1, 1, -1),\\ \hat{b} &:= (-1, -1, -1, 1, 1),\\ \hat{c} &:= (-1, 1, 1, 1, -1),\\ \hat{d} &:= (1, -1, -1, -1, -1),\\ \hat{e} &:= (-1, 1, 1, 1, 1),\\ \hat{f} &:= (1, -1, -1, -1, 1),\\ \hat{g} &:= (1, 1, 1, -1, -1),\\ \hat{h} &:= (1, 1, 1, -1, 1).\end{aligned} \tag{F36}$$

A.4: Since $\log_2 |\mathbb{F}| = 2$ is an integer, in this case we do not have any excess syndromes. Let's choose the syndrome for each element of $\mathbb{F}$, e.g.

$$\begin{aligned}F_{(1,1)} &= I_5,\ F_{(1,-1)} = X_i,\\ F_{(-1,1)} &= Y_i,\ F_{(-1,-1)} = Z_i;\end{aligned} \tag{F37}$$

a quick reminder: $(I) = (1, 1)$ in this case. They give us the minimal Paulian stabilizers:

$$\begin{aligned}Z_1^S|_{\overline{\mathcal{H}}} &= \Pi_{\mathcal{H}_C\oplus X_i\mathcal{H}_C} - \Pi_{Y_i\mathcal{H}_C\oplus Z_i\mathcal{H}_C},\\ Z_2^S|_{\overline{\mathcal{H}}} &= \Pi_{\mathcal{H}_C\oplus Y_i\mathcal{H}_C} - \Pi_{X_i\mathcal{H}_C\oplus Z_i\mathcal{H}_C}.\end{aligned} \tag{F38}$$

A.5: As addressed in the previous point, we have already had the minimal Paulian stabilizers, and we would like to extend their domain to the whole space while keeping them Paulian. We can choose

$$\begin{aligned}\mathbb{W}_{(1,1)} \setminus \mathbb{W}_{F_{(1,1)}} &= \{\hat{a}, \hat{b}\},\\ \mathbb{W}_{(1,-1)} \setminus \mathbb{W}_{F_{(1,-1)}} &= \{\hat{c}, \hat{d}\},\\ \mathbb{W}_{(-1,1)} \setminus \mathbb{W}_{F_{(-1,1)}} &= \{\hat{e}, \hat{f}\},\\ \mathbb{W}_{(-1,-1)} \setminus \mathbb{W}_{F_{(-1,-1)}} &= \{\hat{g}, \hat{h}\},\end{aligned} \tag{F39}$$

so

$$\begin{aligned}\mathcal{H}_{(1,1)} &= \mathcal{H}_C \oplus \mathcal{H}_{\hat{a}} \oplus \mathcal{H}_{\hat{b}},\\ \mathcal{H}_{(1,-1)} &= X_i\mathcal{H}_C \oplus \mathcal{H}_{\hat{c}} \oplus \mathcal{H}_{\hat{d}},\\ \mathcal{H}_{(-1,1)} &= Y_i\mathcal{H}_C \oplus \mathcal{H}_{\hat{e}} \oplus \mathcal{H}_{\hat{f}},\\ \mathcal{H}_{(-1,-1)} &= Z_i\mathcal{H}_C \oplus \mathcal{H}_{\hat{g}} \oplus \mathcal{H}_{\hat{h}}.\end{aligned} \tag{F40}$$

A.6: Now we have commutative stabilizers that are Paulian on the whole space:

$$\begin{aligned}Z_1^S &= \Pi_{\mathcal{H}_{(1,1)}\oplus\mathcal{H}_{(1,-1)}} - \Pi_{\mathcal{H}_{(-1,1)}\oplus\mathcal{H}_{(-1,-1)}}\\ Z_2^S &= \Pi_{\mathcal{H}_{(1,1)}\oplus\mathcal{H}_{(-1,1)}} - \Pi_{\mathcal{H}_{(1,-1)}\oplus\mathcal{H}_{(-1,-1)}}.\end{aligned} \tag{F41}$$

With X_i, Y_i, Z_i, and I_5 chosen as the orthonormal correctable errors, they have distinct syndromes with respect to the Paulian stabilizers, and we can correct their linear combinations, i.e., all errors occurring on the ith qubit. As discussed earlier, the Paulian stabilizers for this code cannot detect all weight-1 errors; however, it can be found that with our choice of the syndrome spaces all single X errors can be detected: Each single X error maps $\mathcal{H}_C$ to a subspace of $\mathcal{H}_{(I)}^\perp$, so the syndrome is different from (I) and is detectable.

4. ((9, 12, 3)) code

Now let's consider the ((9, 12, 3)) code from Refs. [50,82], which, unlike the previous example, is a legitimate error-correcting code. Since we have by and large demonstrated the methods in our previous example, we will only focus on the key points, and since the dimension is too large we will not give explicit forms of the Paulian stabilizers.

(1) A.1: The word stabilizer is generated by $ZXZIIIIII$ and all its cyclic shifts, so it is apparent that

$$\mathrm{wt} S \geqslant d = 3\ \forall S \in \mathsf{S}_W \setminus \{I\}. \tag{F42}$$

By Corollary 5 the code is nondegenerate, so we choose all linearly independent Pauli errors with weight no larger than 2, which means by (23) we have

$$|\mathbb{F}| = 1 + 9 \times 3 = 28.$$

Because

$$2^{\lceil \log_2 |\mathbb{F}| \rceil} \dim \mathcal{H}_C = 2^5 \times 12 < 2^5 \times 2^4 = \dim \mathcal{H} = 2^9,$$

it is possible for this code to have Paulian stabilizers that correct all the relevant errors.

(2) A.2 and A.3 are routine.

(3) A.4: As $m = \lceil \log_2 |\mathbb{F}| \rceil = 5 > \log_2 |\mathbb{F}|$, we will have excess syndromes in this case, and they are $2^m - |\mathbb{F}| = 4$ in total.

(4) A.5: If we want the stabilizers to be Paulian on the whole space, then each syndrome space is composed of $n - m = 4$ qubits. For each syndrome (t) that points to an error $F_{(t)}$ in $\mathbb{F}$, $\dim \mathcal{H}_{(t)} - \dim F_{(t)}\mathcal{H}_C = \dim \mathcal{H}_{(t)} - \dim \mathcal{H}_C = 4$, so we need four elements of $\mathbb{W}_\perp$ to construct the associated syndrome space $\mathcal{H}_{(t)}$, while for each excess syndrome we need $2^4 = 16$ elements of $\mathbb{W}_\perp$.

(5) We can define the Paulian stabilizers following A.6. As there are four excess syndromes, there are four syndrome spaces no correctable errors will map the code space into. They exist to make the stabilizers Paulian.

If we want to use the three Pauli stabilizers from Ref. [82], since they are also part of the word stabilizer (Corollary 3), it is better to let them be in the tuple of generators g, and steps A.4 and A.5 should be done accordingly; e.g., in A.4 the syndrome for each orthonormal Pauli error should be chosen by how the error commutes with the Pauli stabilizers—so that these Pauli stabilizers will be among the Paulian stabilizers built in step A.6.

APPENDIX G: GOTTESMAN-KITAEV-PRESKILL CODES

Let $q = (a^\dagger + a)/\sqrt{2}$ and $p = i(a^\dagger - a)/\sqrt{2}$ be conjugate quadrature operators. A Gottesman-Kitaev-Preskill (GKP) code for a single oscillator has two stabilizers, which are $e^{2i\pi q/\alpha}$ and $e^{-in\alpha p}$ for some real α, where n is the dimension of the code space [79,89]; clearly the stabilizers are not Paulian. Such codes can correct small shifts in both q and p; specifically, they can correct displacements with $|\Delta q| < \alpha/2$ and $|\Delta p| < \pi/(n\alpha)$ [79]. The eigenstates of these stabilizers are not physical in that they are infinitely squeezed, so in practice finitely squeezed states are used; the error probability can be acceptably low if the state is squeezed sufficiently [79,80]. If the anticipated errors in q and p are comparable in magnitude, "square" GKP codes can be used, by choosing $\alpha = \sqrt{2\pi/n}$. When $n = \dim \mathcal{H}_C = 2$, the stabilizers are $e^{2i\sqrt{\pi}q}$ and $e^{-2i\sqrt{\pi}p}$ [72,79,80].

To measure the syndrome, one way is by preparing the ancilla in a GKP state, and utilizing the Steane circuit to ascertain the amount of shifts by measuring the ancilla [72,79,90,91]. The outcomes are analog (or connected) rather than binary [72], and the corresponding measurement on the system is therefore not Paulian. Another avenue is phase estimation [72,89]: Given a unitary operator U on a system, if the system is in an $e^{i\theta}$-eigenstate, the procedure to estimate the phase, i.e., θ is called phase estimation. Because the stabilizers of GKP codes are unitary, we can obtain the syndrome this way; furthermore, as the simultaneous eigenspaces of $e^{2i\pi q/\alpha}$ and $e^{-in\alpha p}$ are translations of the code space in p and q, they are orthogonal and isomorphic [79].

Phase estimation can be achieved by coupling the system and ancilla qubits via controlled-U^k gates, and after performing suitable operations and measurements on the ancilla qubits we are able to approximate the phase θ [4,92–95]. It may seem that each measurement of an ancilla qubit is equivalent to measuring a Paulian operator on the system, as we have two measurement outcomes and they are equally likely (cf. Sec. II B); however, it can be easily checked that such measurements in general are not orthogonal measurements, which is also evident from the coupling between the system and the ancilla being controlled-U^k (cf. Sec. III D). Hence, we cannot describe each measurement with a single self-adjoint operator, let alone a Paulian operator.

Theoretically, we can construct commutative "Paulian" operators Z^{S}_j's for phase estimation: For convenience, let's rescale θ, so that the eigenvalues of U are $e^{2i\pi\theta}$ with $\theta \in [0, 1)$ [4]. Each Z^{S}_j is to measure the 2^{-j} digit of θ in binary representation, and $\theta = 0$ would correspond to the $(1, 1, \cdots)$-simultaneous eigenvalues of Z^{S}_j's. Hence, with $\mathcal{H}_\theta$ denoting the $e^{2i\pi\theta}$-eigenspace of U, we let the 1 and -1-eigenspaces of Z^{S}_j be the direct sums of $\mathcal{H}_\theta$ over all θ whose 2^{-j} digit in binary representation are 0 and 1, respectively. Under this construction, Z^{S}_j's shall be commutative and stabilize 1-eigenvectors of U (i.e., $\theta = 0$), and we can measure Z^{S}_j's to estimate the phase: For example, for an eigenvector of U with $\theta = 0.1010$ in binary representation, it is a (0,1,0)-simultaneous eigenvector of Z^{S}_j's for $j = 1, 2, 3$. However, whether they are truly Paulian or not (as defined in Sec. II B) depends on the spectral structure of U. The ±1-eigenspaces may fail to be isomorphic.

For GKP codes, we can construct phase estimation operators for $e^{2i\pi q/\alpha}$ and $e^{-in\alpha p}$ respectively according to the previous paragraph, and these phase estimation operators are truly Paulian. The issue is that, even though they exist, to carry them out we need to couple very specific intervals of θ with the ancilla; see the ±1-eigenspaces of each Z^{S}_j above and Sec. III D. Hence, existing schemes for error correction, such as those in Refs. [72,80,89,91,96], are more practical.

A closing remark: As discussed in Sec. VI, commutative Paulian stabilizers are not unique, nor are the ones shown above. However, to construct practical Paulian stabilizers, appropriate syndrome spaces should be chosen, and this poses a great challenge, especially given the "continuous" nature of the errors for GKP codes. That being said, in practice states that approximate the true GKP codewords are used, and if confined to these physical states, we might be able to find suitable syndrome spaces to build practical Paulian stabilizers. This is, however, beyond the scope of this work.

[1] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997, arXiv:quant-ph/9705052.

[2] D. Gottesman, in *Quantum Information Science and its Contributions to Mathematics*, edited by S. J. Lomonaco, Jr., Vol. 68 of Proceedings of Symposia in Applied Mathematics (American Mathematical Society, Washington, DC, 2010), pp. 13–58; D. Gottesman, arXiv:0904.2557 [quant-ph].

[3] B. M. Terhal, Rev. Mod. Phys. **87**, 307 (2015).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2011).

[5] J. Roffe, Contemp. Phys. **60**, 226 (2019).

[6] I. Buluta and F. Nori, Science **326**, 108 (2009).

[7] I. M. Georgescu, S. Ashhab, and F. Nori, Rev. Mod. Phys. **86**, 153 (2014).

[8] J. Preskill, Quantum **2**, 79 (2018).

[9] J. I. Cirac, Nanophotonics **10**, 453 (2021).

[10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[11] A. Calderbank, E. Rains, P. Shor, and N. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).

[12] A. Kitaev, Ann. Phys. **303**, 2 (2003).

[13] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[14] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).

[15] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[16] A. G. Fowler, A. C. Whiteside, A. L. McInnes, and A. Rabbani, Phys. Rev. X **2**, 041003 (2012).

[17] S. B. Bravyi and A. Y. Kitaev, arXiv:quant-ph/9811052.

[18] M. Freedman and D. Meyer, Found. Comput. Math. **1**, 325 (2001).

[19] D. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter, New J. Phys. **14**, 123011 (2012).

[20] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Phys. Rev. A **86**, 032324 (2012).

[21] C. D. Hill, E. Peretz, S. J. Hile, M. G. House, M. Fuechsle, S. Rogge, M. Y. Simmons, and L. C. L. Hollenberg, Sci. Adv. **1**, e1500707 (2015).

[22] R. Versluis, S. Poletto, N. Khammassi, B. Tarasinski, N. Haider, D. J. Michalak, A. Bruno, K. Bertels, and L. DiCarlo, Phys. Rev. Appl. **8**, 034021 (2017).

[23] L. A. Landau, S. Plugge, E. Sela, A. Altland, S. M. Albrecht, and R. Egger, Phys. Rev. Lett. **116**, 050501 (2016).

[24] M. Takita, A. D. Córcoles, E. Magesan, B. Abdo, M. Brink, A. Cross, J. M. Chow, and J. M. Gambetta, Phys. Rev. Lett. **117**, 210505 (2016).

[25] T. J. Yoder and I. H. Kim, Quantum **1**, 2 (2017).

[26] J. P. B. Ataides, D. K. Tuckett, S. D. Bartlett, S. T. Flammia, and B. J. Brown, Nat. Commun. **12**, 2172 (2021).

[27] T. Camara, H. Ollivier, and J.-P. Tillich, in *2007 IEEE International Symposium on Information Theory, Nice, France* (IEEE, Piscataway, NJ, 2007), pp. 811–815.

[28] D. Gottesman, arXiv:1310.2984 [quant-ph].

[29] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, IEEE Access **3**, 2492 (2015).

[30] N. P. Breuckmann and J. N. Eberhardt, PRX Quantum **2**, 040101 (2021).

[31] E. Knill, arXiv:quant-ph/9608048.

[32] E. Knill, arXiv:quant-ph/9608049.

[33] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).

[34] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inf. Theory **52**, 4892 (2006).

[35] P. Nadkarni and S. Garani, Quantum Inf. Process. **20**, 256 (2021).

[36] X. Ni, O. Buerschaper, and M. Van den Nest, J. Math. Phys. **56**, 052201 (2015).

[37] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

[38] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).

[39] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quant. Inf. & Comput. **6**, 383 (2006).

[40] D. Bacon, Phys. Rev. A **73**, 012340 (2006).

[41] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, in *44th Annual Allerton Conference on Communication, Control, and Computing* (University of Illinois Urbana-Champaign, Monticello, Illinois, 2006); arXiv:quant-ph/0610153.

[42] P. Aliferis and A. W. Cross, Phys. Rev. Lett. **98**, 220502 (2007).

[43] O. Higgott and N. P. Breuckmann, Phys. Rev. X **11**, 031039 (2021).

[44] E. Knill and R. Laflamme, arXiv:quant-ph/9608012.

[45] S. Roman, *Advanced Linear Algebra*, 3rd ed. (Springer, New York, 2008).

[46] L. H. Loomis and S. Sternberg, *Advanced Calculus*, rev. ed. (Jones and Bartlett, Boston, 1990).

[47] J.-Y. Kao, Ph.D. thesis, National Cheng Kung University, 2020; arXiv:2008.03893 [quant-ph].

[48] J. Preskill (unpublished).

[49] X. Chen, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 062315 (2008).

[50] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, IEEE Trans. Inf. Theory **55**, 433 (2009).

[51] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, 2nd ed. (Springer, Cham, 2015).

[52] N. Landsman, arXiv:math-ph/9807030.

[53] I. F. Putnam, Lecture notes on C*-algebras (2019), https://www.math.uvic.ca/faculty/putnam/ln/C∗-algebras.pdf.

[54] B. Blackadar, *Operator Algebras: Theory of C^*-Algebras and von Neumann Algebras* (Springer-Verlag, Berlin, 2006).

[55] B. C. Hall, *Quantum Theory for Mathematician* (Springer, New York, 2013).

[56] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[57] S. Roman, *Fundamentals of Group Theory: An Advanced Approach* (Birkhäuser, Boston, 2010).

[58] D. Gottesman, Phys. Rev. A **57**, 127 (1998).

[59] S. Axler, *Linear Algebra Done Right*, 3rd ed. (Springer, Cham, 2015).

[60] Y.-M. Di and H.-R. Wei, Phys. Rev. A **87**, 012325 (2013).

[61] Y.-M. Di and H.-R. Wei, Phys. Rev. A **92**, 062317 (2015).

[62] A. Pavlidis and E. Floratos, Phys. Rev. A **103**, 032417 (2021).

[63] A. Saha, R. Majumdar, D. Saha, A. Chakrabarti, and S. Sur-Kolay, Phys. Rev. A **105**, 062453 (2022).

[64] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[65] Y. Liu, G. L. Long, and Y. Sun, Int. J. Quantum Inform. **06**, 447 (2008).

[66] D. W. Kribs and R. W. Spekkens, Phys. Rev. A **74**, 042329 (2006).

[67] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, Phys. Rev. A **79**, 050306(R) (2009).

[68] Y.-J. Wang, B. Zeng, M. Grassl, and B. C. Sanders, in *2013 IEEE International Symposium on Information Theory, Istanbul, Türkiye* (IEEE, Piscataway, 2013), pp. 529–533.

[69] J. M. Günther, F. Tacchino, J. R. Wootton, I. Tavernelli, and P. K. Barkoutsos, Quantum Sci. Technol. **7**, 015009 (2022.

[70] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, Phys. Rev. X **6**, 031006 (2016).

[71] L. Hu, Y. Ma, W. Cai, X. Mu, Y. Xu, W. Wang, Y. Wu, H. Wang, Y. Song, C.-L. Zou *et al.*, Nat. Phys. **15**, 503 (2019).

[72] B. M. Terhal, J. Conrad, and C. Vuillot, Quantum Sci. Technol. **5**, 043001 (2020).

[73] L. Sun, A. Petrenko, Z. Leghtas, B. Vlastakis, G. Kirchmair, K. Sliwa, A. Narla, M. Hatridge, S. Shankar, J. Blumoff *et al.*, Nature (London) **511**, 444 (2014).

[74] B. Vlastakis, G. Kirchmair, Z. Leghtas, S. E. Nigg, L. Frunzio, S. M. Girvin, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Science **342**, 607 (2013).

[75] I. L. Chuang, D. W. Leung, and Y. Yamamoto, Phys. Rev. A **56**, 1114 (1997).

[76] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, Phys. Rev. Lett. **111**, 120501 (2013).

[77] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, New J. Phys. **16**, 045014 (2014).

[78] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. Girvin, L. Jiang *et al.*, Nature (London) **536**, 441 (2016).

[79] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).

[80] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf *et al.*, Nature (London) **584**, 368 (2020).

[81] I. Chuang, A. Cross, G. Smith, J. Smolin, and B. Zeng, J. Math. Phys. **50**, 042109 (2009).

[82] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Phys. Rev. Lett. **101**, 090501 (2008).

[83] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).

[84] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[85] P. Zanardi, Phys. Rev. Lett. **87**, 077901 (2001).

[86] P. Zanardi, D. A. Lidar, and S. Lloyd, Phys. Rev. Lett. **92**, 060402 (2004).

[87] S. Lang, *Algebra*, rev. 3rd ed. (Springer, New York, 2002).

[88] J. Levick, T. Jochym-O'Connor, D. W. Kribs, R. Laflamme, and R. Pereira, J. Phys. A **49**, 125302 (2016).

[89] B. M. Terhal and D. Weigand, Phys. Rev. A **93**, 012315 (2016).

[90] A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).

[91] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal, Phys. Rev. A **99**, 032344 (2019).

[92] A. Y. Kitaev, arXiv:quant-ph/9511026.

[93] R. B. Griffiths and C.-S. Niu, Phys. Rev. Lett. **76**, 3228 (1996).

[94] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde, Nature (London) **450**, 393 (2007).

[95] K. M. Svore, M. B. Hastings, and M. Freedman, Quant. Inf. & Comput. **14**, 306 (2013).

[96] J. Hastrup, K. Park, J. B. Brask, R. Filip, and U. L. Andersen, npj Quantum Inf. **7**, 17 (2021).