Design of additive quantum codes via the code-word-stabilized framework

Alexey A. Kovalev,[1] Ilya Dumer,[2] and Leonid P. Pryadko[1]
[1]Department of Physics & Astronomy, University of California, Riverside, California 92521, USA
[2]Department of Electrical Engineering, University of California, Riverside, California 92521, USA
(Received 13 September 2011; published 21 December 2011)

We consider design of the quantum stabilizer codes via a two-step, low-complexity approach based on the framework of codeword-stabilized (CWS) codes. In this framework, each quantum CWS code can be specified by a graph and a binary code. For codes that can be obtained from a given graph, we give several upper bounds on the distance of a generic (additive or nonadditive) CWS code, and the lower Gilbert-Varshamov bound for the existence of additive CWS codes. We also consider additive cyclic CWS codes and show that these codes correspond to a previously unexplored class of single-generator cyclic stabilizer codes. We present several families of simple stabilizer codes with relatively good parameters.

DOI: 10.1103/PhysRevA.84.062319 PACS number(s): 03.67.Pp, 03.67.Lx

I. INTRODUCTION

It was the invention of quantum error correcting codes [1–3] (QECCs) that opened quantum computing (QC) as a theoretical possibility. However, high precision required for error correction [4–13] combined with the large number of auxiliary qubits necessary to implement it have so far inhibited any practical realization beyond proof-of-the-principle demonstrations [14–20].

In any QECC, one needs to perform certain many-body quantum measurements in order to decide how to correct the encoded state. The practical difficulty is that a generic code requires measurements that are both complicated and frequent at the same time. It is therefore clear that a quantum computer can only be built via a thorough optimization at every step of the design. In particular, code optimization targets codes that combine good parameters with fairly simple measurements. It is also desirable to parallelize these measurements given a specific on-chip layout of a QC architecture.

To date, the main focus of the QECC-research has been on finding good codes with the traditional code parameters, which are the block length n, code dimension K, and code distance d (or code rate $R \equiv (\log_2 K)/n$ and the relative distance $\delta \equiv d/n$). For stabilizer codes [21,22], we also consider the number of encoded qubits $k = \log_2 K$.

A number of stabilizer codes [23] have been designed that meet or nearly achieve the existing bounds on distance d for the given k and n. Code parameters can be further refined by going beyond the family of stabilizer codes. One example is a recently introduced framework of codeword-stabilized (CWS) quantum codes [24–27]. A qubit CWS code $\mathcal{Q} \equiv (\mathcal{G},\mathcal{C})$ (in standard form) is determined by a graph $\mathcal{G}$ and a classical binary code $\mathcal{C}$. CWS codes include all stabilizer codes as a subclass (the corresponding binary code $\mathcal{C}$ must be linear) but also the codes that have been proven to have parameters superior to those of any stabilizer code [25,28–32]. Unfortunately, typical gains in code dimension K correspond to a fraction of a qubit. Moreover, error-correcting algorithms known for general nonadditive CWS codes have exponential complexity [33,34], as opposed to polynomial complexity of the stabilizer codes.

Even for the relatively simple additive codes, their optimization is a very difficult problem that has exponential complexity. This is one of the main reasons as to why the two relatively simple code families are almost exclusively used among stabilizer codes to estimate the threshold accuracy required for scalable quantum computation: the concatenated codes [4,5,7–12] and the surface codes [6,13], which originated from the toric codes [35]. Both families have very low code rates that scale as inverse powers of code distance.

In this work, we explore how the framework of CWS codes can be used to relegate the design of quantum stabilizer codes to classical binary linear codes in order to simplify the overall design. In particular, we formulate several theorems framing the parameters of an additive CWS code, which can be obtained from a given graph. We also suggest a simple decomposition of the $\mathbb{F}_4$ generator matrix corresponding to the stabilizer in terms of the graph adjacency matrix and the parity check matrix of the binary code. Finally, we design several graph families corresponding to regular lattices, which result in some particularly good codes. These include graphs with circulant adjacency matrix, which can be used to construct single-generator cyclic additive codes, a class of codes overlooked in previous publications. In particular, we prove the existence of single-generator cyclic additive codes with the parameters $[[km,k,m]]$, $k > 10$, and $[[t^2 + (t+1)^2,1,2t+1]]$ (version of toric codes). Note that these code families have distances that are not bounded, unlike any CWS code families constructed previously [25,36].

The paper is organized as follows. In Sec. II, we introduce the notations and briefly review some known results for quantum and classical codes. In Sec. III, we establish several upper bounds on general CWS codes. In Sec. IV, we give a CWS decomposition of the $\mathbb{F}_4$ matrix corresponding to the stabilizer generators. In Sec. V, we formulate the Gilbert-Varshamov (GV) bounds for additive CWS codes, which can be obtained from a given graph. Cyclic additive CWS and more general single-generator additive cyclic codes are considered in Sec. VI, where we discuss their properties and give several examples. We give our conclusions in Sec. VII.

1050-2947/2011/84(6)/062319(11)

II. NOTATIONS AND SOME KNOWN RESULTS

A. Classical and quantum error correcting codes

A *classical* q-ary block error-correcting code $(n,K,d)_q$ is a set of K length-n strings over an alphabet with q symbols. Different strings represent K distinct messages that can be transmitted. The (Hamming) distance between two strings is the number of positions where they differ. Distance d of the code $\mathcal{C}$ is the minimum distance between any two different strings from $\mathcal{C}$.

In the case of *linear* codes, the elements of the alphabet must form a Galois field $\mathbb{F}_q$; all strings form n-dimensional vector space $\mathbb{F}_q^n$. A linear error-correcting code $[n,k,d]_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The distance of a linear code is just the minimum weight of a nonzero vector in the code, where weight $\mathrm{wgt}(\mathbf{c})$ of a vector $\mathbf{c}$ is the number of nonzero elements. A basis of the code is formed by the rows of its *generator matrix* G. All vectors that are orthogonal to the code form the corresponding $(n-k)$-dimensional dual code, its generator matrix is the parity-check matrix H of the original code.

For a *binary* code $\mathcal{C}[n,k,d]$, the field is just $\mathbb{F}_2 = \{0,1\}$. For a *quaternary* code C, the field is $\mathbb{F}_4 = \{0,1,\omega,\overline{\omega}\}$, with

$$\omega^2 = \omega + 1, \quad \omega^3 = 1, \quad \text{and} \quad \overline{\omega} \equiv \omega^2. \tag{1}$$

For nonbinary codes, there is also a distinct class of *additive* classical codes, defined as subsets of $\mathbb{F}_q^n$ closed under addition (in the binary case these are just linear codes). A code $\mathcal{C}$ is cyclic if inclusion $(c_0,c_1,\cdots,c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1},c_0,c_1,\ldots,c_{n-2}) \in \mathcal{C}$. Codes that are both linear and cyclic are particularly simple: by mapping vectors to polynomials in the natural way, $\mathbf{c} \to c(x) \equiv c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$, it is possible to show that any such code consists of polynomials that are multiples of a single generator polynomial $g(x)$, which must divide $x^n - 1$ (using the algebra corresponding to the field $\mathbb{F}_q$). The quotient defines the *check polynomial* $h(x)$

$$h(x)g(x) = x^n - 1, \tag{2}$$

which is the generator polynomial of the dual code. The degree of the generator polynomial is $\deg g(x) = n - k$. The corresponding generator matrix G can be chosen as (the first k rows of) the circulant matrix formed by subsequent shifts of the vector that corresponds to $g(x)$.

Qubit quantum error correcting codes are defined in the complex Hilbert space $\mathcal{H}_2^{\otimes n}$, where $\mathcal{H}_2$ is the Hilbert space of a single two-level system. $\mathcal{H}_2$ is formed by all vectors $\alpha|0\rangle + \beta|1\rangle$ with $\alpha,\beta \in \mathbb{C}$, and the inner product such that the two states are orthonormal, $\langle i|j\rangle = \delta_{ij}$, $i,j \in \{0,1\}$. Any operator acting in $\mathcal{H}_2^{\otimes n}$ can be represented as a linear combination of Pauli operators, which form the n-qubit Pauli group $\mathscr{P}_n$ of size 2^{2n+2},

$$\mathscr{P}_n = i^m\{I,X,Y,Z\}^{\otimes n}, \quad m = 0,\ldots,3\,, \tag{3}$$

where X, Y, and Z are the usual Pauli matrices, and I is the identity matrix. The weight $\mathrm{wgt}(E)$ of a Pauli operator E is the number of nonidentity terms in the corresponding tensor product.

All Pauli operators are unitary; they are also Hermitian with eigenvalues ± 1 when the phase factor i^m in Eq. (3) is real-valued, $m = 0,2$. A state $|\psi\rangle$ is stabilized by a Hermitian Pauli operator M if $M|\psi\rangle = |\psi\rangle$. A linear space Q is stabilized by a set of operators $\mathcal{M}$ if each vector in Q is stabilized by every operator in $\mathcal{M}$.

An $((n,K,d))$ *quantum error-correcting code* is a K-dimensional subspace of the Hilbert space $\mathcal{H}_2^{\otimes n}$. Such a subspace can be described by an orthonormal basis $\{|i\rangle\}_{i=1}^K$. Let $\mathcal{E} \subset \mathscr{P}_n$ be some set of Pauli errors. A QECC detects all errors $E \in \mathcal{E}$ if and only if [21,37]

$$\langle j|E|i\rangle = C_E \delta_{ij}\,, \tag{4}$$

where C_E only depends on the error E but is independent of the basis vectors. A QECC has distance d if it can detect all Pauli errors of weight $(d-1)$ but not all errors of weight d. The errors in the set $\mathcal{E}$ can be corrected if and only if all the nontrivial pairwise combinations of errors from $\mathcal{E}$ are detectable [2,3]. Thus, a distance-d code corrects all errors of weight $s \leqslant t \equiv \lfloor (d-1)/2 \rfloor$.

The code $\mathcal{Q}$ is *nondegenerate* if linearly independent errors from $\mathcal{E}$ produce corrupted spaces $E(\mathcal{Q}) \equiv \{E|\psi\rangle : |\psi\rangle \in \mathcal{Q}\}$ that are linearly independent. Otherwise, the code is *degenerate*, implying the existence of at least two *mutually degenerate* linearly independent operators $\{E_1,E_2\} \in \mathcal{E}$ that act identically on $\mathcal{Q}$.

The code is called *pure* if linearly independent errors from $\mathcal{E}$ produce corrupted spaces that are not only linearly independent but also mutually orthogonal. For all codes considered in this work, nondegenerate codes are also pure [22,34].

Two codes are considered equivalent if they differ just by qubit order, and/or discrete rotations leaving each of the single-qubit Pauli groups invariant. The latter are called local Clifford (LC) transformations.

B. Stabilizer quantum error correcting codes

Here we briefly review the well-known family of stabilizer codes [21]. An $[[n,k,d]]$ *stabilizer code* Q is a 2^k-dimensional subspace of the Hilbert space $\mathcal{H}_2^{\otimes n}$ stabilized by an Abelian group $\mathscr{S} \subset \mathscr{P}_n$ with $n-k$ Hermitian Pauli generators, $\mathscr{S} = \langle G_1,\ldots,G_{n-k}\rangle$. Explicitly,

$$Q \equiv \{|\psi\rangle : S|\psi\rangle = |\psi\rangle, \quad \forall\, S \in \mathscr{S}\}\,. \tag{5}$$

Such a code exists only if $-\mathbb{1} \notin \mathscr{S}$. The group $\mathscr{S}$ is called the stabilizer of the code. Changing the sign(s) of one or several of the generators G_i results in replacing Q with one of $2^{n-k}-1$ equivalent codes whose direct sum (together with Q) is the entire space $\mathscr{P}_n$.

The *normalizer* of $\mathscr{S}$ is a set of Pauli operators generating unitary transformations that leave $\mathscr{S}$ invariant:

$$\mathscr{N} \equiv \{U \in \mathscr{P}_n : U^\dagger S U = S, \forall\, S \in \mathscr{S}\}\,. \tag{6}$$

Elements of the normalizer form a group commuting with $\mathscr{S}$ but not necessarily with each other. It is possible to construct $2k$ logical operators $\overline{X}_j$, $\overline{Z}_j$, $j = 1\cdots k$ belonging to $\mathscr{P}_n$ with the usual commutation relations that generate the normalizer when the generators of $\mathscr{S}$ are included [21,38]. The Abelian subgroup of $\mathscr{N}$, $\mathscr{S}_0 = \langle G_1\cdots G_{n-k},\overline{Z}_1\cdots\overline{Z}_k\rangle$, becomes a maximal Abelian subgroup of $\mathscr{P}_n$ when the generator $i\mathbb{1}$ is also included.

The group $\mathscr{S}_0$ stabilizes a unique *stabilizer* state $|s\rangle \equiv \overline{|0\cdots 0\rangle}$, an $[[n,0,d']]$ stabilizer code, while the operators $\overline{X}_j$ generate the basis of the code, i.e.,

$$\overline{|c_1\cdots c_k\rangle} = \overline{X}_1^{c_1}\cdots \overline{X}_k^{c_k}\,|s\rangle\,. \tag{7}$$

By convention, the stabilizer state is considered nondegenerate, and its distance d' is the minimum weight of a nontrivial member of the group $\mathscr{S}_0$.

For stabilizer codes, phases of (Hermitian) Pauli operators are only needed to choose one of the equivalent codes in Eq. (5), as well as to introduce the commutation relations. It is convenient to drop the phases and map the Pauli operators to two binary strings, $\mathbf{v},\mathbf{u} \in \{0,1\}^n$ [22],

$$U \equiv i^{m'} X^{\mathbf{v}} Z^{\mathbf{u}} \to (\mathbf{v},\mathbf{u}), \tag{8}$$

where $X^{\mathbf{v}} = X_1^{v_1} X_2^{v_2}\cdots X_n^{v_n}$, $Z^{\mathbf{u}} = Z_1^{u_1} Z_2^{u_2}\cdots Z_n^{u_n}$, and $m' = 0\cdots 3$ is generally different from that in Eq. (3). This map preserves the operator algebra, with a product of two Pauli operators U_1 and U_2 corresponding to a sum of the corresponding binary vectors $(\mathbf{v}_1,\mathbf{u}_1)$ and $(\mathbf{v}_2,\mathbf{u}_2)$.

The map of Eq. (8) can be taken one step further [22] to quaternary codes by introducing $\mathbb{F}_4^n$ vectors $\mathbf{e} \equiv \mathbf{u} + \omega\mathbf{v}$ [see Eq. (1); note that this mapping differs slightly from that in Ref. [22]]. We will denote this combined map as a function $\mathbf{e} \equiv \phi(U)$. Note that up to a phase this association also allows us to define $\phi^{-1}(\mathbf{e})$. To be specific, for the Pauli operator $\phi^{-1}(\mathbf{e})$ we will set $m' = \mathbf{v}\cdot\mathbf{u}$ in Eq. (8), which corresponds to $m = 0$ in Eq. (3).

It is easy to check that two Pauli operators commute if and only if the symplectic scalar product $\mathbf{v}_1\cdot\mathbf{u}_2 + \mathbf{u}_1\cdot\mathbf{v}_2$ vanishes (mod 2). In terms of the corresponding $\{\mathbf{e}_1,\mathbf{e}_2\} \subset \mathbb{F}_4$, this corresponds to the vanishing of the *trace inner product*

$$\mathbf{e}_1 * \mathbf{e}_2 \equiv \mathbf{e}_1\cdot\bar{\mathbf{e}}_2 + \bar{\mathbf{e}}_1\cdot\mathbf{e}_2, \tag{9}$$

where $\bar{\mathbf{e}}_i \equiv \mathbf{u}_i + \overline{\omega}\mathbf{v}_i$, $i = 0,1$.

A dual code to an additive $\mathbb{F}_4$ code C (equipped with trace inner product) is defined as [22]

$$C_\perp = \left\{\mathbf{e}' \in \mathbb{F}_4^n : \mathbf{e}' * \mathbf{e} = 0, \text{ for all } \mathbf{e} \in C\right\}. \tag{10}$$

If $C \subseteq C_\perp$, one says C is self-orthogonal. A classical additive code C corresponding to a set of operators $\mathscr{S}_1$ is self-orthogonal if and only if $\mathscr{S}_1$ is an Abelian group. Thus, any quantum stabilizer code can be described as a self-orthogonal classical additive code over $\mathbb{F}_4$. The following theorem is applicable to additive $\mathbb{F}_4$ codes (variant of Theorem 2 from Ref. [22]):

Theorem 1. Suppose C is an additive self-orthogonal code in $\mathbb{F}_4^n$, containing 2^{n-k} vectors, such that there are no vectors of weight $< d$ in $C_\perp \setminus C$. Then $\phi^{-1}(C)$ defines a stabilizer of an additive QECC with parameters $[[n,k,d]]$.

Example 1. The well-known Calderbank-Shor-Steane (CSS) [[7,1,3]] code [39,40] has the stabilizer with the generators [21]

$$\begin{gathered} XXXXIII,\quad XXIIXXI,\quad XIXIXIX,\\ ZZZZIII,\quad ZZIIZZI,\quad ZIZIZIZ, \end{gathered} \tag{11}$$

and the logical operators

$$\overline{X} = ZZZZZZZ,\quad \overline{Z} = XXXXXXX. \tag{12}$$

As any CSS code, this code is linear. Qubit permutations also give an equivalent cyclic linear code with the generator polynomial $g(x) = 1 + x + x^2 + x^4$; $g(x)$ is a factor of $x^7 - 1$. The corresponding check polynomial is $h(x) = 1 + x + x^3$.

C. Codeword stabilized codes

CWS codes [25] represent a general class of nonadditive QECCs. A general CWS code is defined in terms of a stabilizer state $|s\rangle$ and a set of K mutually commuting *codeword operators* $\mathcal{W} \equiv \{W_i\}_{i=1}^K \subset \mathscr{P}_n$. Explicitly [cf. Eq. (7)],

$$\mathcal{Q} = \operatorname{span}\left(\{W_i|s\rangle\}_{i=1}^K\right). \tag{13}$$

For nontrivial CWS codes, this construction coincides with union-stabilizer (USt) codes [41], restricted to the zero-dimensional originating code.

Any stabilizer state is LC-equivalent to a *graph state* [42–45], a stabilizer state with the stabilizer group $\mathscr{S}_{\mathcal{G}} \equiv \langle S_1\cdots S_n\rangle$ whose generators S_i are determined by the adjacency matrix $R \in \{0,1\}^{n\times n}$ of a (simple) graph $\mathcal{G}$,

$$S_i = X_i Z^{\mathbf{r}_i}\,, \tag{14}$$

where $\mathbf{r}_i$, $i = 1\cdots n$ denotes the i-th row of R. In fact, such a graph is usually not unique, even after accounting for graph isomorphisms. The full set of LC-equivalent graph states can be generated by a sequence of *local complementations*, operations on a graph where the subgraph corresponding to a neighborhood of a particular vertex is inverted. Such graphs are called *locally equivalent* [46].

Any CWS code $((n,K,d))$ is LC equivalent to a CWS code in *standard form*, defined by an order-n graph $\mathcal{G}$ and a classical binary code $\mathcal{C}$ containing K binary words. The graph defines the graph state, while the vectors of the classical code $\mathbf{c}_i \in \mathcal{C}$ are used to generate the codeword operators, $W_i = Z^{\mathbf{c}_i}$. Thus,

$$\mathcal{Q} = \operatorname{span}\left(\{Z^{\mathbf{c}_i}|s\rangle\}_{i=1}^K\right). \tag{15}$$

It is customary to use notation $Q = (\mathcal{G},\mathcal{C})$ for CWS codes in standard form.

The key simplification of the CWS construction comes from the fact that the basis states $W_i|s\rangle$ are eigenvectors of the graph stabilizer generators,

$$S_i W_i\,|s\rangle = \pm W_i\,|s\rangle\,,\quad S_i \in \mathscr{S}_{\mathcal{G}}. \tag{16}$$

Thus, a Pauli operator in the form of Eq. (8) can be transformed to a Z-only operator $Z^{\mathrm{Cl}_{\mathcal{G}}(U)}$, where the *graph image* of the operator U is the binary vector

$$\mathrm{Cl}_{\mathcal{G}}(U) \equiv \mathbf{u} + \sum_{i=1}^n v_i\mathbf{r}_i \,(\mathrm{mod}\, 2). \tag{17}$$

The error correcting properties of a quantum CWS code $Q = (\mathcal{G},\mathcal{C})$ and the classical code $\mathcal{C}$ are related by the following:

Theorem 2. (after Theorem 3 from Ref. [25]) Consider a CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$. An error E such that $\mathrm{Cl}_{\mathcal{G}}(E) \neq \mathbf{0}$, is detectable in $\mathcal{Q}$ if and only if the binary vector $\mathrm{Cl}_{\mathcal{G}}(E)$ is detectable within the code $\mathcal{C}$. An error E such that $\mathrm{Cl}_{\mathcal{G}}(E) = \mathbf{0}$ is detectable in $\mathcal{Q}$ if and only if $Z^{\mathbf{c}}E = EZ^{\mathbf{c}}$ for all $\mathbf{c} \in \mathcal{C}$.

The case $\mathrm{Cl}_{\mathcal{G}}(E) \neq \mathbf{0}$ corresponds to pure (nondegenerate) errors, while $\mathrm{Cl}_{\mathcal{G}}(E) = \mathbf{0}$ indicates that the error is in the graph stabilizer group $\mathscr{S}_{\mathcal{G}}$; the corresponding detectability condition is a requirement that the error must be degenerate.

While in general CWS codes are nonadditive, they include all stabilizer codes as a subclass. A CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ is additive if $\mathcal{C}$ is a linear code [25]. The stabilizer $\mathscr{S}$ of an additive CWS code in standard form is a subgroup of the graph stabilizer $\mathscr{S}_{\mathcal{G}}$; it can be obtained from the graph-stabilizer generators by a symplectic Gram-Schmidt orthogonalization procedure [34]. Conversely, the representation Eq. (7) of an additive code corresponds to a general CWS code; an LC transformation may be needed to obtain the corresponding standard form, and one can always find a standard form where $\mathcal{C}$ is linear [26]. In the following we will always assume such a representation.

Example 2. The smallest single-error-correcting code is the linear cyclic [[5,1,3]] code [3,47,48] with the generator polynomial $g(x) = 1 + \omega x + \omega x^2 + x^3$, which divides $x^5 - 1$. The corresponding check polynomial is $h(x) = 1 + \omega x + x^2$. This code is unique; its stabilizer generators can be obtained as cyclic permutations of a single operator, $XZZXI$, and the logical operators are

$$\overline{X} = ZZZZZ, \quad \overline{Z} = XXXXX. \tag{18}$$

The corresponding CWS code [25] can be generated from the five-ring graph in Fig. 1 (left), and the binary code has a single generator $\mathbf{c} = (11111)$. Note that both the graph and the binary code preserve the original cyclic symmetry.

Example 3. There exist only two inequivalent single-correcting codes [[6,1,3]]; both are degenerate [39]. One of the codes is obtained from the code in Example 2 by adding a qubit; the graph of the corresponding CWS code can be chosen as a five-ring [Fig. 1, left] and a disconnected vertex $i = 6$; the binary code $\mathcal{C}$ is generated by $\mathbf{c} = (111110)$. The degeneracy group is generated by $S_6 = X_6$. The stabilizer generators for the second code are listed in Ref. [39]. This code corresponds to the graph in Fig. 1 (center), while the binary code is generated by $c_1 = (011100)$. While there are three bits that are not involved with the classical code, they cannot be dropped as they are part of the entangled state. The degeneracy group is generated by $S_1S_2 \equiv X_1X_2$ (the equivalence follows from the fact that the first two vertices of $\mathcal{G}$ share all of their neighbors).

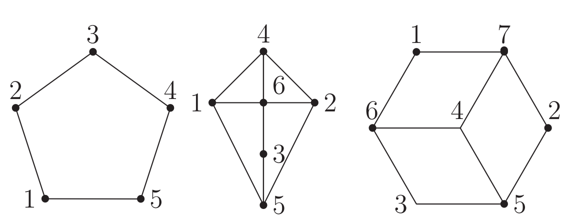

FIG. 1. Left: five-ring graph corresponding to the [[5,1,3]] code in Example 2. Center: "Kite" graph corresponding to the degenerate code [[6,1,3]] from Example 3. Right: The graph corresponding to the cyclic [[7,1,3]] code from Example 4.

TABLE I. Families of the cyclic codes obtained numerically from k copies of the classical repetition code, $p(x) = x^m - 1$, corresponding to $m = 3,5,7$. The expected distance saturation, $d = m$, is reached already at $k \leqslant 4$, even for k and m different from those in Example 12. The operator strings in the last column are representative graph-state generators (the remaining generators are obtained by cyclic shifts).

m	n	k	d	S_1
3	6	2	2	ZXZ
	9	3	3	ZXZ
	12	3	3	ZXZ
5	5	1	3	ZXZ
	10	2	3	ZXZ
	15	3	5	$ZIZIIXIIZIZ$
	20	4	5	$ZIZZXZZIZ$
	25	5	5	$ZIZZXZZIZ$
7	7	1	3	ZXZ
	14	2	5	$ZZIXIZZ$
	21	3	6	$ZIZZXZZIZ$
	28	4	7	$ZIZZIXIZZIZ$

Example 4. The linear cyclic [[7,1,3]] CSS code from the Example 1 is LC equivalent to a CWS code with the graph in Fig. 1 (Right). The corresponding classical code is given by $\mathcal{C} = \{0000000, 1110000\}$. Note that neither the graph nor the binary code is explicitly symmetric with respect to cyclic permutations of the qubits. Note also that an inequivalent CWS cyclic [[7,1,3]] code exists; we constructed such a code among others in Example 12, see Table I.

III. UPPER BOUNDS FOR CWS CODES

In this section we give upper bounds on general CWS codes in terms of the properties of the corresponding graph $\mathcal{G}$ and the binary code $\mathcal{C}$.

Lemma 1. The distance d of the CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ cannot exceed that of $\mathcal{C}$.

Proof. Indeed, any "classical" error in the form $E = i^m Z^{\mathbf{u}}$ is mapped by Eq. (17) to the binary vector $\mathbf{u}$. If E is detectable by $\mathcal{Q}$, $\mathbf{u}$ should be detectable by $\mathcal{C}$. ∎

Lemma 1 concerns with errors which are dealt with by the binary code. On the other hand, a CWS code is an enlargement of the code formed by the graph state. The following observation has been made in Ref. [32,36]:

Lemma 2. The distance d of a nondegenerate CWS code $((n,K,d))$ is limited by the distance $d'(\mathcal{G})$ of the graph stabilizer state, $d \leqslant d'(\mathcal{G})$.

It follows from the fact that any member of the graph stabilizer is either a degenerate error, or it is a nondetectable error. Note, however, as illustrated by the Example 3, in general, the distance of a CWS code can actually be bigger than that of the graph stabilizer state.

For a binary code $\mathcal{C}$, we will say that the j-th bit is *involved* in the code if there are vectors in the code for which the value of j-th bit differ, $c_1^j \neq c_2^j$. Alternatively, if the all-zero vector $\mathbf{0}$ is in the code (which can always be arranged), the condition is that there is a vector $\mathbf{c} \in \mathcal{C}$ where j-th bit is nonzero, $c^j \neq 0$.

Lemma 3. For a CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ with $K > 1$, let us assume that j-th bit is involved in the code $\mathcal{C}$. Then the graph-stabilizer generator S_j violates the error detection condition in Theorem 2.

Proof. Since the generator S_j is in the graph stabilizer, $\mathrm{Cl}_{\mathcal{G}}(S_j) = \mathbf{0}$, one has to check the degenerate condition in Theorem 2. The commutativity of S_j with a given $Z^{\mathbf{c}}$ is determined by the j-th bit of $\mathbf{c}$; conditions of the Lemma ensure that only one of the two vectors commute with S_j. ■

Note that this means that the code distance cannot exceed that of any S_j corresponding to bits involved in the binary code. Since at least d bits must be involved in the binary code, Lemma 3 guarantees the following bound:

Theorem 3. The distance d of a CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ cannot exceed the d-th largest weight of S_i, minimized over all graphs that are locally equivalent to $\mathcal{G}$.

We will also be using the following:

Corollary 3.1. For a graph $\mathcal{G}$ with all vertices of the same degree r, the distance of a CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ cannot exceed $r + 1$.

In particular, for any ring graph $r = 2$, which gives $d \leqslant 3$, for any double-ring graph [26] $d \leqslant 4$, and for a large enough square lattice wrapped into a torus, $d \leqslant 5$.

Obviously, to maximize the distance of a CWS code, one may want to maximize the distance of the binary code $\mathcal{C}$. To this end, it is a good idea to make sure that every bit is involved in $\mathcal{C}$. For such codes, we have

Theorem 4. The distance of a CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$, where the binary code $\mathcal{C}$ involves all bits, cannot exceed the *minimum* weight of S_i, minimized over all graphs that are locally equivalent to $\mathcal{G}$.

IV. ADDITIVE CWS CODES AND QUATERNARY CODES

The stabilizer of an additive CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ is a subgroup of the Abelian graph stabilizer $\mathscr{S}_{\mathcal{G}}$, and its generators $G_i \in \mathscr{S}$ can be expressed as products of graph stabilizer generators S_i [25,34]. Explicitly,

$$G_i = \prod_{j=1}^{n} S_j^{P_{ij}}, \tag{19}$$

where $P \in \{0,1\}^{n-k\times n}$ is the corresponding matrix of binary coefficients. With the help of Eq. (14), we obtain the following decomposition for the generator matrix G of the associated additive $\mathbb{F}_4$ code C,

$$G = P\,(\omega\mathbb{1} + R)\,, \tag{20}$$

where $R \in \{0,1\}^{n\times n}$ is the symmetric graph adjacency matrix with zeros along the diagonal, and $\mathbb{1}$ is the $n \times n$ identity matrix. The relation between the binary code $\mathcal{C}$ and the quaternary code C is explicitly given by the following:

Lemma 4. The additive $\mathbb{F}_4$ code C with the generator matrix Eq. (20) is the map $\phi(\mathscr{S})$ of the stabilizer $\mathscr{S}$ of the additive CWS code $\mathcal{Q} = (\mathcal{G},\mathcal{C})$ generated by the graph with the adjacency matrix R and the linear binary code $\mathcal{C}$, if and only if P is the parity check matrix of $\mathcal{C}$.

Proof. Use the basis vectors in Eq. (15) and the commuting operators in Eq. (19) corresponding to the rows of the matrix G [Eq. (20)]. Direct calculation gives

$$G_i\, Z^{\mathbf{c}}|s\rangle = \prod_{j=1}^{n} S_j^{P_{ij}}\, Z^{\mathbf{c}}|s\rangle = (-1)^{P_{ij}c^j}\, Z^{\mathbf{c}}\,|s\rangle, \tag{21}$$

where summation over repeated indices is assumed. The statement of the Lemma (both ways) follows from the definition of the parity check matrix. ■

We can now easily relate the error detection conditions for additive codes in Theorems 1 (codes over $\mathbb{F}_4$) and 2 (CWS codes). The code C in Theorem 1 is given by additive combinations of the $n - k$ rows of the generator matrix Eq. (20). Evaluating the outer trace product of the generator matrix Eq. (20) with a vector $\mathbf{e} = \mathbf{u} + \omega\mathbf{v}$, we obtain the condition for the vector to be in $C_\perp$

$$0 = G * \mathbf{e} = P(\mathbf{u} + R\mathbf{v}). \tag{22}$$

This uniform linear system of $n - k$ equations with $2n$ variables has $n + k$ linearly independent solutions. The corresponding basis can be chosen as a set of k linearly independent "classical" vectors $\mathbf{e}_i = \mathbf{u}_i$, where $P\mathbf{u}_i = 0$ and the corresponding $v_i = 0$, $i = 1\cdots k$, plus n linearly independent vectors such that $u_j = Rv_j$, $j = k + 1\cdots k + n$. Some linear combinations of the latter vectors are actually in C. These can be found using the identity $(C_\perp)_\perp = C$: the corresponding $\mathbf{v}_j$ have to satisfy $\mathbf{u}_i \cdot \mathbf{v}_j = 0$, which precisely corresponds to the degenerate case, $\mathrm{Cl}_{\mathcal{G}}(E) = 0$, in Theorem 2.

General theory of CWS codes guarantees that generator matrix of a quantum code equivalent to any additive self-orthogonal code over $\mathbb{F}_4$ can be decomposed in the form of Eq. (20). Conversely, any matrix in the form of Eq. (20) with binary matrices P and R generates a self-orthogonal code over $\mathbb{F}_4$ as long as the matrix R is symmetric. We use it in the following section to prove the lower Gilbert-Varshamov (GV) bound for the parameters of an additive CWS code, which can be obtained from a given graph.

V. GV BOUND FOR THE ADDITIVE CWS CODES WITH A GIVEN GRAPH

The GV bound is a counting argument which nonconstructively proves the existence of codes with parameters exceeding a certain threshold. The argument is based on the fact that the set of possible codes (vector spaces) vastly outnumbers the set of vectors. Then, if we count all codes of a given length n, and then subtract the number of codes that contain any vector of weight $d - 1$ or less, the remaining codes (if any) will all have distance d or more. This "greedy" argument ignores any possible double counting of codes that contain several small-weight vectors. Note that the GV bound necessarily gives asymptotically *good* codes with relative distance $\delta \equiv d/n$ and code rate $R \equiv k/n$ bounded away from 0 as $n \to \infty$.

For the entire class of pure stabilizer codes, the asymptotic GV bound [49] states that there exist codes of length $n \to \infty$ such that

$$\delta \log_2 3 + H_2(\delta) \geqslant 1 - R, \tag{23}$$

where $H_2(\delta) \equiv -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$ is the binary entropy function. We are going to prove that the same bound also holds for pure CWS codes corresponding to a given graph $\mathcal{G}$, as long as $d \leqslant d'(\mathcal{G})$ [see Lemma 2]. We are using Eq. (20) to parametrize the stabilizer matrices; the resulting $\mathbb{F}_4$ codes are automatically self-orthogonal. Let $N^{\mathcal{G}}_{n,k}$ be the number of CWS codes that have length n, dimension at least k, and correspond to a given graph $\mathcal{G}$. Let also $N^{\mathcal{G}}_{\mathbf{e},n,k}$ be the number of such codes that contain a given vector $\mathbf{e} = \mathbf{u} + \omega \mathbf{v}$, $\operatorname{wgt} \mathbf{e} < d'(\mathcal{G})$, in $C_\perp$ [see Eq. (20)]. The corresponding condition Eq. (10) is given by the trace inner product [Eq. (22)]. For $\operatorname{wgt} \mathbf{e} < d'(\mathcal{G})$, the binary vector $\mathbf{c} \equiv \mathbf{u} + R\mathbf{v}$ is always nonzero (which also guarantees that $\mathbf{e} \notin C$). As a result, $N^{\mathcal{G}}_{\mathbf{e},n,k}$ and $N^{\mathcal{G}}_{n,k}$ represent the corresponding numbers for the *binary* codes.

Then, the standard counting arguments [50] show that

$$(2^n - 1)N^{\mathcal{G}}_{\mathbf{e},n,k} = (2^k - 1)N^{\mathcal{G}}_{n,k}. \tag{24}$$

Here, we use the fact that each of $2^n - 1$ vectors $\mathbf{c}$ belongs to the same number $N^{\mathcal{G}}_{\mathbf{e},n,k}$ of binary codes; also each of $N^{\mathcal{G}}_{n,k}$ binary codes contains $2^k - 1$ nonzero vectors $\mathbf{c}$. The number of quaternary vectors of weight s is $3^s\binom{n}{s}$. Thus, for any graph $\mathcal{G}$, there exists a distance-d CWS code, as long as

$$N^{\mathcal{G}}_{\mathbf{e},n,k} \sum_{s=1}^{d-1} 3^s \binom{n}{s} < N^{\mathcal{G}}_{n,k}. \tag{25}$$

Now we see that there exist $[[n,k,d]]$ CWS codes for the graph $\mathcal{G}$ with distance

$$d = \min\{d_{GV}, d_{\max}\}, \tag{26}$$

where $d_{\max}$ is the distance of the graph state $d'(\mathcal{G})$ and

$$d_{GV} = \max d : \sum_{s=1}^{d-1} 3^s \binom{n}{s} < \frac{2^n - 1}{2^k - 1}. \tag{27}$$

Note that thus obtained quantum codes are always pure, since the summation in the l.h.s. can only be extended up to $d_{\max} - 1$. Apart from this latter condition, Eq. (27) is identical to the quantum Gilbert-Varshamov bound [49] for pure stabilizer codes, and takes the asymptotic form of Eq. (23) as $n \to \infty$.

The exact GV bound $d \geqslant d_{GV}$ for pure stabilizer codes (without the restriction on the distance) is recovered if we go over different graphs. Indeed, the GV bound Eq. (23) also applies for the special case of $k = 0$, corresponding to stabilizer states or self-dual codes [51]. The GV bound on the relative distance is monotonous in k and reaches its maximum at

$$\delta_{k=0} \approx 0.189. \tag{28}$$

Then, for given n and $\delta < \delta_{k=0}$, one can always find a suitable graph such that the GV bound $d \leqslant d_{GV}$ becomes more restrictive than the condition $d \leqslant d_{\max}$.

In practice, graphs with large distance $d'(\mathcal{G})$ are complicated (have too many edges). It is much easier to come up with graph families corresponding to a fixed graph-state distance $d'(\mathcal{G})$. For $n \to \infty$, the corresponding code families approach the maximum rate $R = 1$ and have asymptotic redundancy $r \equiv n - k$ defined by Eq. (27):

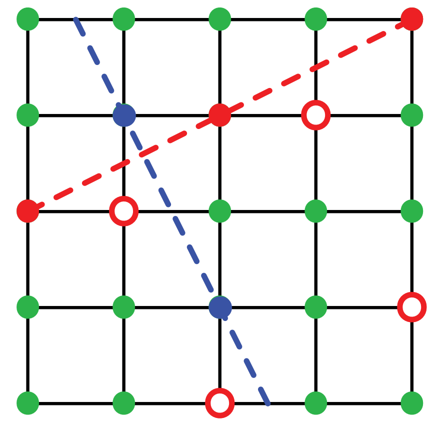

FIG. 2. (Color online) Square-lattice additive CWS code [[25,4,4]]. Circles represent the qubits. All $k = 4$ translations of the empty-circle pattern form the classical codewords $\mathbf{c}_i$. The generators of the stabilizer are formed as the products of the graph-state stabilizer generators along the directions parallel to the dashed lines.

$$r \leqslant d \log_2 3 + n H_2(d/n). \tag{29}$$

It is readily verified that the r.h.s of Eq. (29) has the order of $d \log_2(3n/d)$ if $d = \text{const}$ and $n \to \infty$.

Example 5. Graphs in the form of sufficiently large finite square lattice fragments [Fig. 2] have maximum distance $d_{\max} = 5$, but this requires that the bits in the corners and around the perimeter not be involved in the classical code. Somewhat better redundancy can be achieved by avoiding only the bits in the corners, which gives $d_{\max} = 4$. Consider the family of classical codes, where the codewords are obtained by taking all translations of the pattern shown in Fig. 2 with open symbols. The weight of any linear combination of such codewords is at least 4. The lattice shown corresponds to the code [[25,4,4]], while general $m_x \times m_y$ lattice gives the code with the parameters $[[m_x m_y, (m_x - 3)(m_y - 3), 4]]$. Asymptotically, the redundancy for $m_x = m_y$ is $n - k \approx 6n^{1/2}$, $n \to \infty$, which is bigger than the logarithm in Eq. (29). However, the fraction of auxiliary qubits vanishes as $\propto 1/n^{1/2}$ for large n. The code distance can be increased with higher-dimensional generalizations, e.g., we can generalize this construction to D-dimensional hypercubic lattice with $2D$ nearest neighbors so that the distance is $d = 2D$ in full analogy with the two-dimensional case. The corresponding redundancy will scale with the area of the boundary.

While the code in Fig. 2 serves as a good illustration of the concept of lattice codes with simple stabilizer structure, it is still far from optimal. On the 5×5 square lattice we have constructed numerically a code [[25,9,5]] with weight-7 codewords, which can be mapped into each other by translations and rotations. This design is only one logical qubit short of the best-known generic code [[25,10,5]].

Example 6. Consider graphs in the form of $L \times L$ square lattices wrapped into tori due to periodic boundary conditions. For $L \geqslant 5$, these graphs have the distance $d'(\mathcal{G}) = 5$. GV bound Eq. (25) shows that the CWS codes with the following parameters can be obtained for these graphs: [[25,4,5]], [[36,13,5]], [[49,24,5]], [[64,38,5]], [[81,53,5]], ...

Example 7. Consider graphs in the form of $L \times L$ triangular lattices wrapped into tori due to periodic boundary conditions. These graphs have the distance $d'(\mathcal{G}) = \min(L,7)$. GV bound Eq. (25) shows that the CWS codes with the following parameters can be obtained for these graphs: [[36,9,6]], [[49,15,7]], [[64,28,7]], [[81,43,7]], ...

VI. SINGLE-GENERATOR ADDITIVE CYCLIC CODES

Example 4 shows that a cyclic additive code does not necessarily preserve its symmetry when converted to CWS standard form. By a *cyclic* additive CWS code we just mean a code that is cyclic in standard form, with a circulant graph. For such a code, Eq. (20) can be rewritten as the generator polynomial,

$$g(x) = p(x)[\omega + r(x)], \tag{30}$$

where the polynomials $p(x)$ and $r(x)$ are binary, $p(x)$ is the parity-check polynomial of a binary cyclic code (and therefore must divide $x^n - 1$), while $r(x)$ corresponds to a symmetric circulant matrix,

$$r(x^{n-1}) = r(x) \,(\mathrm{mod}\, x^n - 1). \tag{31}$$

Any such *symmetric* polynomial $r(x)$ leads to a valid self-orthogonal additive code. The dimension of the quantum code corresponding to the generator polynomial [Eq. (30)] is $k = \deg p(x)$.

Previously, the additive cyclic QECCs were introduced in Theorem 14 of Ref. [22], stating that any such code has two generators. A *single*-generator additive code described by Eq. (30) represents a new setting, in which the second generator is equal to zero. This condition gives a self-orthogonal additive code C [see Sec. II B] with no binary codewords (any $\mathbf{e} \in C$, $\mathbf{e} \equiv \mathbf{u} + \omega\mathbf{v}$, has $\mathbf{v} \neq 0$).

A somewhat wider class of *single-generator* cyclic additive codes can be also defined via Eq. (30), without requiring the symmetry [Eq. (31)] of $r(x)$. Then, two codes, $\mathcal{Q}$ and $\mathcal{Q}'$, which have a generator polynomial in the form of Eq. (30) with the same $p(x) = p'(x)$, are equivalent, if and only if

$$r(x) = r'(x) \,\mathrm{mod}\, q(x), \tag{32}$$

where $q(x) = (x^n - 1)/p(x)$ is the generator polynomial of the binary code [22]. Such a polynomial [Eq. (30)] generates a self-orthogonal $\mathbb{F}_4$ code, if and only if [22]

$$p(x)p(x^{n-1})r(x^{n-1}) = p(x)p(x^{n-1})r(x) \,(\mathrm{mod}\, x^n - 1). \tag{33}$$

This guarantees self-orthogonality for any $r(x)$, as long as

$$p(x)p(x^{n-1}) = 0 \;\mathrm{mod}\, x^n - 1. \tag{34}$$

An alternative formulation of this sufficient condition is that the corresponding generator polynomial $q(x)$ must contain no more than one root from each pair (α,α^{-1}) of mutually conjugate n-th roots of unity, $\alpha^n = 1$. In particular, a self-reciprocal (*palindromic*) polynomial,[1]

$$x^{\deg q(x)} q(1/x) = q(x), \tag{35}$$

always contains roots in pairs α and α^{-1}. For such polynomials, Eq. (34) always fails [including the special case of $q(x) = 1 + x$, which has only one root $\alpha = \alpha^{-1} = 1$].

A. Single-generator cyclic codes from a binary code

The algebraic condition Eq. (2) on check polynomials for linear cyclic codes makes them simpler to implement but also dramatically restricts their number. In particular, the general counting approach to finding CWS codes [see Sec. V], where one first chooses a graph and then searches for a suitable binary code, can hardly be applied to cyclic CWS codes. Even for classical binary cyclic codes, there are no counting arguments known to date that yield asymptotically good codes, let alone the stronger GV bound (see Research Problem 9.2 in Ref. [50]). Also, long BCH codes—one of the major subclasses of cyclic codes—are asymptotically bad and have a slowly declining relative distance $\delta \sim (2 \ln R^{-1})/\log_2 n$ for any code rate R. On the other hand, binary cyclic codes often achieve the best-known parameters (exceeding the GV bound) on short lengths $n \leqslant 256$. Thus, using simple cyclic codes in quantum design can yield both good parameters and feasible implementation on the short blocks.

To better evaluate code distance of single-generator quantum cyclic codes [Eq. (30)], we will modify our counting approach of Sec. V and begin with a binary cyclic code. Namely, we will fix some parity-check polynomial $p(x)$ with a desired degree k among the binary factors of $x^n - 1$. Then we will search for a polynomial $r(x)$, either corresponding to a circulant graph [see Eq. (31)] or satisfying the more general orthogonality condition Eq. (33). However, this transition will show that the parameters of quantum codes generated this way strongly depend on the chosen binary code. We will concentrate exclusively on the binary codes with irreducible generator polynomial $q(x)$. We will show that the distance of such a cyclic CWS code is limited from below by the GV bound (or the variants thereof) and from above by the distance of the classical cyclic code. Since GV bound always produces asymptotically good codes, the parameters of our quantum codes will be mostly limited (at least, for long blocks) by their binary counterparts.

We begin with analyzing the condition Eq. (22) for a cyclic CWS code. For a vector $\mathbf{e} \in \mathbb{F}_4^n$ to be in $C_\perp$, this condition can be rewritten in terms of the corresponding polynomials,

$$p(x)\,[u(x) + r(x)v(x)] = 0 \;\mathrm{mod}\, x^n - 1\,, \tag{36}$$

where the coefficients of the (reversed for notational convenience) polynomial $e(x^{n-1}) \equiv u(x) + \omega v(x)$ are given by the

[1] In the literature, such polynomials have also been called "symmetric." We prefer to reserve this term for the polynomials [Eq. (31)] that correspond to symmetric circulant matrices. Palindromic polynomials have reflection symmetry with respect to their "centers," while Eq. (31) corresponds to a symmetry with respect to the free term, with an implicit circulant symmetry.

components of the vector $\mathbf{e} \in \mathbb{F}_4^n$. Since binary $p(x)$ divides $x^n - 1$, we can rewrite this in terms of the corresponding generator polynomial $q(x) = (x^n - 1)/p(x)$ for the binary code $\mathcal{C}$,

$$u(x) + r(x)v(x) = 0 \mod q(x). \tag{37}$$

Now, if $v(x)$ is mutually prime with $q(x)$, Eq. (37) can be solved for $r(x)$. In this case, the answer is unique [mod $q(x)$]. On the other hand, multiple solutions for $r(x)$ are possible when $\gcd[v(x),q(x)] \neq 1$. In this work, we avoid the complications caused in the latter case[2] and only consider irreducible polynomials $q(x)$.

Overall, for any irreducible $q(x)$ and any $\mathbf{e}$ with $\mathbf{v} \neq \mathbf{0}$ and $\operatorname{wgt} \mathbf{e} < d(\mathcal{C})$, Eq. (37) has a unique solution for $r(x)$ such that $\deg r(x) < \deg q(x) = n - k$. Respectively, there is no more than one additive quantum code such that $\mathbf{e} \in C_\perp$. Generally, only some of thus obtained $r(x)$ correspond to self-orthogonal codes; see Eq. (33).

Below we complete the greedy argument by counting the polynomials $r(x)$ corresponding to self-orthogonal codes, Eq. (33). We consider separately the case when the irreducible polynomial $q(x)$ is palindromic [see Eq. (35)] in Lemma 7 below, and when it is not in

Lemma 5. Consider a cyclic binary code $\mathcal{C}[n,k,d_\mathcal{C}]$ with the generator polynomial $q(x)$ which is both irreducible and nonpalindromic, $x^{\deg q(x)} q(x^{-1}) \neq q(x)$. Then, there exists a single-generator additive cyclic code $[[n,k,d]]$ with distance

$$d = \min(d_\mathcal{C}, d_{\mathrm{GV}}),$$

restricted by both the distance $d_\mathcal{C}$ of the binary code and the following variant of GV bound

$$d_{\mathrm{GV}} = \max d : \sum_{s=1}^{d-1} (3^s - 3) \frac{\gcd(s,n)}{n} \binom{n}{s} \leqslant 2^{n-k} - 2. \tag{38}$$

Proof. The nonpalindromic generator polynomial $q(x)$ is one of the factors in $x^n - 1$, which also contains its reciprocal, $x^{\deg q(x)} q(x^{-1})$. This implies that the corresponding parity-check polynomial $p(x)$ satisfies Eq. (33). Further, since $q(x)$ is irreducible, the solution $r(x)$ of Eq. (37) is unique, assuming $v(x) \neq 0$ and $\deg r(x) < n - k$, which gives the exponential term in the r.h.s. of Eq. (38). Equation (38) improves on the standard GV inequality of Eq. (27) by discarding a few sets of vectors. The first set are vectors with $u(x) = 0$, which implies $r(x) = 0 \mod q(x)$. The second set are vectors with $u(x) = v(x)$, which all give $r(x) = 1 \mod q(x)$. The third set are nonzero vectors with $v(x) = 0$, which can never be in $C_\perp$ corresponding to the generator, Eq. (30). Finally, note that any error vector of weight s produces at least $n/\gcd(s,n)$ different cyclic shifts. All of these cyclic shifts give the same polynomial $r(x)$ and can be discounted. The condition $d \leqslant d_\mathcal{C}$ comes from Lemma 1. ■

Note. The l.h.s. of bound Eq. (38) limits the number of cyclic classes for 4-ary vectors $\mathbf{e}$ of weight $s \leqslant d - 1$. Most of these vectors have the maximum period n. Therefore, it can be proven that the term $\gcd(s,n)/n$ in Eq. (38) can be replaced with the smaller term that rapidly tends to 1/n for large n. In turn, bound Eq. (38) adds about $\log_2 n$ information qubits to bound Eq. (27) but tends to the standard quantum GV bound Eq. (23) as $n \to \infty$.

In the following example, this bound coincides with inequality $d \leqslant d_\mathcal{C}$, which uniquely sets code distance d.

Example 8. The family of the binary codes with the parameters $[n = 2^{4h} + 2^{3h} - 2^h - 1, k = n - 6h, 3]$, $h = 1,2\cdots$ constructed in Ref. [52], has irreducible nonpalindromic generator polynomials as required in Lemma 5. For $d_\mathcal{C} = 3$, the sum in Eq. (38) has just one term at $s = 2$; for n odd $\gcd(n,2) = 1$. Explicit calculation confirms that the parameters of these codes satisfy inequality Eq. (38), which proves the existence of single-generator cyclic quantum codes with exactly the same parameters, $[[n = 2^{4h} + 2^{3h} - 2^h - 1, k = n - 6h, 3]]$, but not necessarily cyclic CWS codes. The smallest of these codes, [[21,15,3]], corresponds to a polynomial $q(x) = 1 + x + x^2 + x^4 + x^6$ (unique up to a reversal) and can be obtained from an order-21 circulant graph corresponding to $r(x) = x + x^4 + x^{17} + x^{20}$. This particular combination of parameters gives the best existing code [23].

Example 9. According to the BCH bound [50], a cyclic code has distance $d \geqslant r + 1$ ($r + 1$ is the "*designed*" distance) if the corresponding generator polynomial $q(x)$ has r consecutive roots, e.g., $\alpha, \alpha^2 \cdots \alpha^r$, where α is the primitive n-th root of unity. A polynomial $m_\alpha(x)$, which has root α, necessarily has s distinct roots α^{2^j} for all $j = 0 \cdots s - 1$, if s is the smallest number such that $2^s = 1 \mod n$. We say that the code has zeros α^i, where exponents i form the set $I = \{2^j (\mathrm{mod}\, n),\ j = 0,\ldots,s - 1\}$. The code generated by $m_\alpha(x)$ has designed distance 5 if $3 \in I$ or, equivalently, if $2^s = 3 \mod n$ for some s. The polynomial $m_\alpha(x)$ is nonpalindromic if $-1 \notin I$. We can further obtain codes with irreducible nonpalindromic generators and designed distances 7, 9, etc., by imposing additional conditions, e.g., $5 \in I$, $7 \in I$, etc. The values of n, for which this is possible form an infinite set, $\{23_5, 47_5, 71_7, 95_5, 115_5, 143_5, 167_5, 191_7, 235_5, 239_7, \ldots\}$, where the subscripts indicate the designed distances. In fact, the first three codes represent the well known quadratic-residue codes with the higher distances (exceeding the BCH bound) equal to 7, 11, and 11, respectively. GV bound proves the existence of additive quantum CWS codes with the parameters [[23,12,4]], $[[47,24,d \geqslant 6]]$, $[[71,36,d \geqslant 7]]$, [[95,59,5]], [[115,71,5]], [[143,83,11]], etc. The first three codes have the parameters as good as any known codes with such n and k.

Now let us consider the case of a palindromic polynomial $q(x)$. First, we prove

Lemma 6. Consider a binary code $\mathcal{C}$ generated by a palindromic polynomial $q(x)$ such that $q(1) = 1$. Then, any quantum code [Eq. (30)] that satisfies self-orthogonality condition Eq. (33) is equivalent to a cyclic CWS code with a symmetric polynomial $r(x)$; see Eq. (31).

Proof. The corresponding check polynomial $p(x)$ is symmetric, thus the condition Eq. (33) can be rewritten as

$$r(x) + r(x^{n-1}) = 0 \mod q(x). \tag{39}$$

[2] For polynomials $q(x)$ with multiple factors, distance estimates of quantum codes lead to the estimates of weight spectra of classical cyclic codes that contain the code generated by $q(x)$, which is beyond the scope of this work.

The condition $q(1) = 1$ guarantees that the palindromic polynomial $q(x)$ has odd weight and even degree $2m$, in which case the "central" monomial x^m has nonzero coefficient $q_m = 1$. Given the block length n, let us choose an equivalent code [see Eq. (32)] with $r(x)$ such that the coefficients

$$r_{m+1} = r_{m+2} = \ldots = r_{n-m} = 0. \tag{40}$$

The coefficients of the polynomial in the l.h.s. of Eq. (39) satisfy the same condition, except for the term x^{n-m}, which has coefficient r_m. The coefficients are arranged in such a way that the l.h.s. of Eq. (39) can only equal zero or $x^{n-m}q(x) \bmod x^n - 1$. However, the latter possibility can be excluded by comparing the corresponding coefficients of the free term x^0. The only remaining case corresponds to a symmetric $r(x)$. ∎

It is now clear that for a palindromic irreducible generator polynomial $q(x) \neq 1 + x$, one should reduce the count in the r.h.s. of Eq. (38) by replacing 2^{n-k} with $2^{(n-k)/2}$, the number of symmetric polynomials that satisfy Eq. (40). This gives the following version of GV bound:

$$d_{\mathrm{GV}} = \max d : \sum_{s=1}^{d-1} (3^s - 3)\frac{\gcd(s,n)}{n}\binom{n}{s} \leqslant 2^{(n-k)/2} - 2. \tag{41}$$

While the resulting estimate is much weaker than the GV bound Eq. (38), it still gives asymptotically good codes. A better (especially, for small d) bound is given in the following:

Lemma 7. Consider a cyclic binary code $\mathcal{C}[n,k,d_{\mathcal{C}}]$, with $d_{\mathcal{C}} \geqslant 3$ and the generator polynomial $q(x)$, which is both palindromic and irreducible. Then there exists a cyclic CWS code $[[n,k,d]]$ with the distance $d = \min(d_{\mathcal{C}}, \lfloor d_{\mathrm{GV}}/2 \rfloor)$, where $d_{\mathrm{GV}} = \max d$:

$$\sum_{s=1}^{d-1} (3^{\lceil s/2 \rceil} - 3)\frac{\gcd(s,n)}{n}\binom{\lfloor n/2 \rfloor}{\lfloor s/2 \rfloor} \leqslant 2^{(n-k)/2} - 2. \tag{42}$$

Proof. The restriction on the distance guarantees that $q(x) \neq 1 + x$, and, therefore, $q(x)$ satisfies the conditions of Lemma 6; in particular, $n - k$ is even. The inequality just corresponds to symmetric polynomials $r(x)$ and the errors that are also symmetric, $e(x^{n-1}) = e(x) \bmod x^n - 1$. The statement of the Lemma follows from the fact that for any general error $e(x)$, there is a symmetric error $e_{\mathrm{sym}}(x) \equiv e(x) + e(x^{n-1}) \bmod x^n - 1$ whose weight is even and is limited by $\mathrm{wgt}\, e_{\mathrm{sym}}(x) \leqslant 2\, \mathrm{wgt}\, e(x)$. ∎

Example 10. Among classical codes, the largest distance is obtained for the repetition codes, with the parameters $\mathcal{C} = [n,1,n]$. The parity-check polynomial is $p(x) = x + 1$; the generator polynomial $q(x) = 1 + x + \cdots + x^{n-1}$ is irreducible and palindromic for $n = 2$, and for all $n > 2$ that satisfy the condition $\mathrm{ord}_m(2) = m - 1$, where $\mathrm{ord}_m(q)$ is the multiplicative order of q modulo m. This includes the following $n \leqslant 100$:

$$\{3,5,11,13,19,29,37,53,59,61,67,83 \cdots\}. \tag{43}$$

Lemma 7 shows that for n from the set Eq. (43), additive cyclic CWS codes with parameters $[[n,1,\lfloor d_{GV}(n,1)/2 \rfloor]]$ exist, where $d_{GV}(n,1)$ is obtained from Eq. (42) with $k = 1$. Asymptotically, at large n, this corresponds to cyclic codes with the relative distance given by half of that given by Eq. (28).

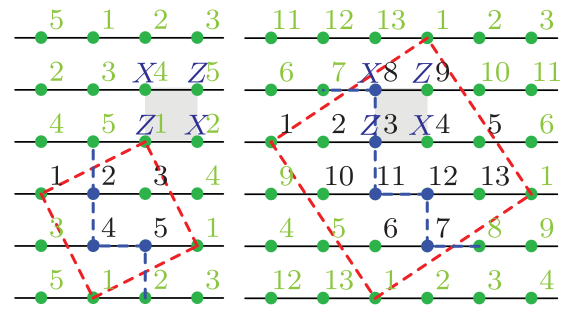

FIG. 3. (Color online) Left: Correspondence between the cyclic code [[5,1,3]] with generators $ZXIXZ$ and a generalized toric code on a square lattice. The generators of the latter are all possible translations of the highlighted plaquette. Only qubits within the dashed square are participating in the code (numbering in black); the two-dimensional square lattice is numbered according to the periodic boundary conditions that are given by two translation vectors. The dashed line indicates a topologically nontrivial chain of errors that limits the distance of the code: $X_2Z_4Z_5$ is equivalent to $Z_1Z_2Z_3Z_4Z_5$. Right: same for the code [[13,1,5]] with the generator $ZXIIIXZ$ corresponding to the highlighted plaquette.

Example 11. (Cyclic analogs of the toric code) In the setting of the previous example, cyclic CWS codes [[5,1,3]], [[13,1,5]], [[25,1,7]], [[41,1,9]] with $p(x) = 1 + x$ were obtained numerically. The corresponding graph-state generators are ZXZ for $d = 3$, $ZZXZZ$ for $d = 5$, etc. We obtain a family of cyclic codes with the weight-4 generators, $S_3 = ZXXZ$, $S_5 = ZIXXIZ$, etc. Codes with generators $S_3 = ZXIXZ$, $S_5 = ZXIIIXZ$, $S_7 = ZXIIIIIXZ$, and $S_9 = ZXIIIIIIIXZ$ have the same parameters (the corresponding graphs are somewhat more complicated). The latter family can be generalized to codes with $n = t^2 + (t+1)^2, k = 1,\ d = 2t + 1,\ t = 1,2\cdots$; the corresponding stabilizer generators S_{2t+1} having $2t - 1$ identity operators separating ZX and XZ. These cyclic codes correspond to a generalization of the toric code construction [53] that in some cases yields better code parameters compared to other known generalizations of toric codes [54–56]; the square-lattice qubit layout preserving the circulant symmetry is illustrated in Fig. 3 for $t = 1,2$.

Example 12. (CWS codes from k copies of the repetition code) Let us take the binary code $\mathcal{C}$ to be formed by k copies of the repetition code with the distance $d_2 = m$. Then, the block size is $n = km$, and the check polynomial is $p(x) = x^k - 1$. The generator polynomial $q(x) = 1 + x^k + \cdots + x^{k(m-1)}$ is always palindromic; it is also irreducible if m belongs to the set Eq. (43), while $k = m^s$, $s = 0,1,2\cdots$. For sufficiently large n, Lemma 7 gives asymptotically good codes with $kd \propto n^2$. Since these parameters cannot exceed those of the binary code $\mathcal{C}$, which correspond to $kd = n$ (thus $\delta = 1/k$), for these values of m and $k > 10$, there exist cyclic CWS codes with the parameters of the corresponding binary code, $[[n = m^{s+1}, m^s, d = m]]$. This prediction is readily verified empirically; see Table I. Note that, as in the Example 11, many of these codes have stabilizer generators with small weight.

VII. CONCLUSIONS

In this paper, we analyze how the general CWS framework can facilitate the search of the additive quantum codes with reasonably good parameters. Unlike complete optimization of CWS codes [26], which involves all nonisomorphic LC-inequivalent order-n graphs and all binary codes of length n, here one can independently pick a suitable graph $\mathcal{G}$ and then search for a linear binary code $\mathcal{C}$ that can correct the error patterns induced by $\mathcal{G}$; see Eq. (22).

The choice of the graph is discussed in Sec. III. In the simplest case of pure codes, one has to pick a graph with a sufficiently large graph-state distance $d'(\mathcal{G})$. Assuming that a regular graph is being sought in this design, we consider graphs with minimal vertex degrees $d'(\mathcal{G}) - 1$ or more.

After the graph is chosen, the second step involves the search of an appropriate binary code. In Sec. V we prove the existence of the binary codes that give good quantum CWS codes. The corresponding lower bound on the distance is given by the quantum Gilbert-Varshamov bound Eq. (27). Note that while this bound is proved for a given graph, it is the same bound that holds for a generic stabilizer code.

Our results show that by restricting the graph $\mathcal{G}$ of a CWS code to regular lattices, one can lower the complexity of the code search and still obtain codes with relatively good parameters. On the other hand, the graph structure could be mapped directly to a physical qubit layout. Therefore, such codes can simplify both the hardware design and the error-correcting procedures, which will easily admit the property of translational invariance.

An unexpected byproduct of this work is the discovery of a previously unexplored family of single-generator quantum cyclic codes (Sec. VI A). These codes are relatively easy to construct, and they are plentiful. We construct (or prove the existence) of several simple families of such codes that have unbounded distances. These include cyclic CWS codes with weight-4 stabilizer generators, which turned out to be toric codes in disguise (Example 11), as well as a code family with the parameters of generalized repetition codes, $[[kd,k,d]]$ (Example 12). The main advantage of these families is a simple structure of their stabilizers.

ACKNOWLEDGMENTS

We are grateful to M. Grassl for helpful comments. This work was supported in part by the Army Research Office under Grant No. W911NF-11-1-0027 (L.P. and I.D.), and by the NSF under Grant No. 1018935 (L.P.).

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[4] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998).
[5] B. Rahn, A. C. Doherty, and H. Mabuchi, Phys. Rev. A **66**, 032304 (2002).
[6] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[7] A. M. Steane, Phys. Rev. A **68**, 042322 (2003).
[8] A. G. Fowler, C. D. Hill, and L. C. L. Hollenberg, Phys. Rev. A **69**, 042314 (2004).
[9] A. G. Fowler, S. J. Devitt, and L. C. L. Hollenberg, Quant. Info. Comput. **4**, 237 (2004).
[10] A. G. Fowler, Ph.D. thesis, Cornell University, 2005.
[11] E. Knill, Nature (London) **434**, 39 (2005).
[12] E. Knill, Phys. Rev. A **71**, 042322 (2005).
[13] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).
[14] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, Phys. Rev. Lett. **85**, 5452 (2000).
[15] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 883 (2001).
[16] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) **421**, 48 (2003).
[17] J. Chiaverini *et al.*, Nature (London) **432**, 602 (2004).
[18] A. Friedenauer, H. Schmitz, J. T. Glueckert, D. Porras, and T. Schaetz, Nature Physics (2008), doi:10.1038/nphys1032.
[19] J. M. Martinis, Quant. Info. Proc. **8**, 81 (2009).
[20] K. Kim, M.-S. Chang, S. Korenblit, R. Islam, E. E. Edwards, J. K. Freericks, G.-D. Lin, L.-M. Duan, and C. Monroe, Nature (London) **465**, 590 (2010).
[21] D. Gottesman, Ph.D. thesis, Caltech, 1997.
[22] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Th. **44**, 1369 (1998).
[23] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes" (2007) [http://www.codetables.de].
[24] J. A. Smolin, G. Smith, and S. Wehner, Phys. Rev. Lett. **99**, 130505 (2007).
[25] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, IEEE Trans. Inf. Theory **55**, 433 (2009).
[26] I. L. Chuang, A. W. Cross, G. Smith, J. A. Smolin, and B. Zeng, J. Math. Phys. **50**, 042109 (2009).
[27] X. Chen, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 062315 (2008).
[28] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Phys. Rev. Lett. **101**, 090501 (2008).
[29] S. Yu, Q. Chen, and C. H. Oh, e-print arXiv:0709.1780v1.
[30] M. Grassl and M. Roetteler, in *Proceedings IEEE International Symposium on Information Theory* (Toronto, Canada, 2008), pp. 300–304.
[31] M. Grassl and M. Roetteler, in *Proceedings IEEE Information Theory Workshop Porto, Portugal*, (2008), pp. 396–400.
[32] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, Phys. Rev. A **79**, 050306 (2009).
[33] Y. Li, I. Dumer, and L. P. Pryadko, Phys. Rev. Lett. **104**, 190501 (2010).
[34] Y. Li, I. Dumer, M. Grassl, and L. P. Pryadko, Phys. Rev. A **81**, 052337 (2010).
[35] A. Y. Kitaev, Ann. Phys. **303**, 2 (2003).
[36] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).

[37] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Infomation* (Cambridge University Press, Cambridge, 2000).

[38] M. M. Wilde, Phys. Rev. A **79**, 062322 (2009).

[39] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[40] A. M. Steane, Phys. Rev. A **54**, 4741 (1996).

[41] M. Grassl and T. Beth, e-print arXiv:quant-ph/9703016.

[42] M. Grassl, A. Klappenecker, and M. Rötteler, in *Proceedings of the 2002 IEEE International Symposium on Information Theory* (Lausanne, Switzerland, 2002), p. 45.

[43] D. Schlingemann, Quant. Info. Comput. **2**, 307 (2002).

[44] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).

[45] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel, in *Quantum Computation, Algorithms, and Chaos: Proceedings of the International School of Physics "Enrico Fermi"* (IOS Press, Amsterdam, 2005), Vol. 162, pp. 115–218.

[46] A. Bouchet, Discrete Math. **114**, 75 (1993).

[47] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).

[48] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[49] K. Feng and Z. Ma, IEEE Trans. Inf. Theory **50**, 3323 (2004).

[50] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1981).

[51] E. M. Rains and N. J. A. Sloane, in *Handbook of Coding Theory*, edited by V. S. P. and W. C. Huffman (North-Holland, Amsterdam, 1998), Vol. I, pp. 177–294.

[52] C. Ding, T. Helleseth, H. Niederreiter, and C. Xing, IEEE Trans. Inf. Theory **48**, 2679 (2002).

[53] A. A. Kovalev, I. Dumer, and L. P. Pryadko (unpublished).

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

[55] M. H. Freedman and D. A. Meyer, e-print arXiv:quant-ph/9810055.

[56] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **76**, 012305 (2007).