Quantum two-block group algebra codes

Hsiang-Ku Lin and Leonid P. Pryadko
Department of Physics & Astronomy, University of California, Riverside, California 92521, USA

(Received 25 July 2023; accepted 11 December 2023; published 5 February 2024)

We consider quantum two-block group algebra (2BGA) codes, a family of smallest lifted-product (LP) codes. These codes are related to generalized-bicycle codes, except a cyclic group is replaced with an arbitrary finite group, generally non-Abelian. As special cases, 2BGA codes include a subset of square-matrix LP codes over Abelian groups, including quasicyclic codes, and all square-matrix hypergraph-product codes constructed from a pair of classical group codes. We establish criteria for permutation equivalence of 2BGA codes and give bounds for their parameters, both explicit and in relation to other quantum and classical codes. We also enumerate the optimal parameters of all inequivalent binary connected 2BGA codes with stabilizer generator weights $W \leqslant 8$, of length $n \leqslant 100$ for Abelian groups, and $n \leqslant 200$ for non-Abelian groups.

DOI: 10.1103/PhysRevA.109.022407

I. INTRODUCTION

Recent years have seen a substantial progress in theory of quantum low-density parity-check (LDPC) codes [1–5]. Generally, any code family with bounded-weight stabilizer generators and distance scaling logarithmically or faster with the block length has a finite fault-tolerant threshold to scalable error correction [6–8]. Unlike in the case of classical LDPC codes [9,10] where random matrices are commonly used to define the code, due to a commutativity constraint, an algebraic ansatz is required in the case of quantum LDPC codes. For over a decade, no construction was known to give distances larger than a square root of the block size n, up to a polylogarithmic factor [1,6,11–18]. The barrier was broken by Hastings, Haah, and O'Donnell [2] who demonstrated a quantum LDPC code family with the distance scaling as $O(n^{3/5}/\operatorname{polylog} n)$. Soon followed related constructions [3,4], with Panteleev and Kalachev [5] finally proving the existence of asymptotically good bounded-stabilizer-generator-weight quantum LDPC codes, with nonzero asymptotic relative distances for any asymptotic rate $R < 1$. Unfortunately, the constructions in Refs. [2–5] tend to give rather long codes, and the lower bound [5] for the row weight to give asymptotically good quantum codes is also very large.

In Ref. [19], in an attempt to construct shorter quantum LDPC codes with large distances, one of us studied a class of generalized-bicycle (GB) codes [14,20]. These are index-two quantum quasicyclic (qQC) codes, a special case of qQC codes [20–23] where the general upper distance bound related to the number of blocks does not apply. Important advantages of GB codes are overcomplete set of minimum-weight stabilizer generators which may improve their performance in the fault-tolerant setting, and their regular structure which simplifies implementation and iterative decoding [20,24]. Furthermore, GB codes include [19] codes with linear distance scaling, unlike, e.g., the hypergraph-product (HP) codes [13], where the distance can never exceed a square root of the block length. However, the regular structure of the corresponding matrices also implies [19] that a GB code with row weight W can be mapped to a code local in dimension $D \leqslant W - 1$, which implies a power-law upper bound on the distance, $d \leqslant O(n^{1-1/D})$ (see Ref. [25]). Numerically, it appears that fixed-weight GB codes have distance scaling as $A(W)n^{1/2}$, where $A(W)$ is an increasing function of the weight W, although a power-law scaling $d = O(n^{\alpha})$ with $\alpha - 1/2$ positive but close to zero cannot be excluded [19].

The goal of this work is to explore parameters of a class of codes similar to GB codes, where more general symmetry groups are used instead of cyclic groups (some of the present results have been announced previously, see Ref. [26]). These codes are a special case of two-block Calderbank-Shor-Steane (CSS) codes [14], and also are the smallest lifted-product (LP) codes [5]. In fact, this work was inspired by the LP codes construction, along with the related work by the same authors on two-block codes based on Abelian group algebras [27]. Our main reason to study these *two-block group algebra* (2BGA) codes, especially in the non-Abelian case, is that general upper distance bound [5] for LP codes does not apply in the two-block case, and neither do the upper distance bounds [19] for GB codes with row weight W since more general Abelian or non-Abelian groups do not give matrices with structure as regular as that of the circulant matrices. On the other hand, most of the advantages of the GB codes remain. In particular, these more general codes also have naturally overcomplete sets of minimum-weight stabilizer generators, which is expected to improve their performance in the fault-tolerant setting.

The outline of the rest of the paper is as follows. We give some background information in Sec. II. In Sec. III, we discuss general properties of quantum CSS codes constructed from two square commuting matrices. In Sec. IV we give the construction of 2BGA codes and analyze their properties, and in Sec. V discuss the parameters of 2BGA codes constructed numerically. Finally, we give the conclusions in Sec. VI. More technical proofs for Secs. III and IV are collected in Appendixes A and B, respectively. Appendix C gives additional examples of index-4 qQC 2BGA codes constructed from groups C_{mh} and D_m.

II. NOTATIONS AND KNOWN FACTS

A. Classical codes

A classical q-ary error-correcting code with parameters $(n, K, d)_q$ is a set of K strings of length n in an alphabet with q distinct characters, where any two strings differ in d or more positions [28]. In a *linear code* $C \subset F^n$ using as the alphabet a finite Galois field $F \equiv \mathbb{F}_q$, where $q = p^m$ is a power of a prime p, the field characteristic, the strings in the code form a linear space of dimension k, so that $K = q^k$. The parameters of such a code are denoted $[n, k, d]_q$, where the distance d is the minimum Hamming weight of a nonzero vector in the code. For a trivial code with $k = 0$ (empty set of nonzero vectors), we set d equal to infinity.

Rows of a *generator matrix* G of a linear code $C \equiv C_G$ are nonzero vectors in the code which include a complete basis, so that any vector of the code can be written as a linear combination of rows of G; evidently, rank $G = k$. The code $C^\perp$ *dual* to C is formed by all vectors in F^n orthogonal to the vectors in C. A generator matrix H of the code $C_G^\perp$ is called a parity-check matrix of the original code C_G, it satisfies the duality relation

$$GH^T = 0, \quad \operatorname{rank} G + \operatorname{rank} H = n. \tag{1}$$

Given a string $\boldsymbol{c} \in F^n$, denote $\mathcal{V} \equiv [n] \equiv \{1, 2, \ldots, n\}$ the set indexing the individual characters. For any *index set* $\mathcal{I} \subseteq \mathcal{V}$ of length $|\mathcal{I}| = r$, let $\boldsymbol{c}[\mathcal{I}] \in F^r$ be a substring of $\boldsymbol{c}$ with the characters in all positions $i \notin \mathcal{I}$ dropped. We say that $\boldsymbol{c}[\mathcal{I}]$ is the string $\boldsymbol{c}$*punctured* outside $\mathcal{I}$. Similarly, for an n-column matrix G, the punctured matrix $G[\mathcal{I}]$ is formed by the rows of G punctured outside $\mathcal{I}$. If $C = C_G$ is an F-linear code with the generating matrix G, then the code of length $|\mathcal{I}|$ with the generating matrix $G[\mathcal{I}]$ is the code punctured outside $\mathcal{I}$, $C_{\rm p}(\mathcal{I}) \equiv \{c[\mathcal{I}] \,|\, c \in C\}$.

The *shortened* code $C_{\rm s}(\mathcal{I})$ is formed similarly, except only from the codewords supported inside $\mathcal{I}$, $C_{\rm s}(\mathcal{I}) = \{\boldsymbol{c}[\mathcal{I}] \,|\, \boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in C \text{ and } c_i = 0 \text{ for each } i \notin \mathcal{I}\}$. The dual of a punctured code $C_{\rm p}(\mathcal{I})$ is the shortened dual code $[C_{\rm p}(\mathcal{I})]^\perp = (C^\perp)_{\rm s}(\mathcal{I})$. To express this relation in terms of matrices, consider a pair of mutually dual matrices in Eq. (1) and a code $C \equiv C_G = C_H^\perp$. Denote a generator matrix of the shortened code $C_{\rm s}(\mathcal{I})$ as $G_\mathcal{I}$. Duality between the punctured original and the shortened dual codes implies that the corresponding generator matrices $G_\mathcal{I}$ and $H[\mathcal{I}]$ are also mutually dual [28],

$$H[\mathcal{I}]\, G_\mathcal{I}^T = 0, \quad \operatorname{rank} G_\mathcal{I} + \operatorname{rank} H[\mathcal{I}] = |\mathcal{I}|. \tag{2}$$

Similarly, $H_\mathcal{I}$ is a dual of the punctured matrix $G[\mathcal{I}]$.

Relevant for this work are left and right group codes constructed in a group algebra [29,30]. Namely, for a given finite field F and a finite group G of order $|G| = \ell$, we consider the group algebra (a ring) $F[G]$ defined as an F-linear space of all formal sums

$$x \equiv \sum_{g\in G} x_g g, \quad x_g \in F \tag{3}$$

where group elements $g \in G$ serve as basis vectors, equipped with the product naturally associated with the group operation,

$$ab = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g, \quad a, b \in F[G]. \tag{4}$$

Evidently, Eq. (3) defines a one-to-one map between any vector $\boldsymbol{x} \in F^\ell$ with coefficients x_g labeled by group elements and a group algebra element $x \in F[G]$, and a similar map between sets of vectors and sets of group algebra elements. A left G code in F^ℓ is such a map of a left ideal J_L in the ring $F[G]$, defined as an F-linear space of elements of $F[G]$ such that for any $x \in J_L$ and any $r \in F[G]$, $rx \in J_L$. A right G code is defined similarly in terms of a right ideal J_R, with the opposite order in the product, $xr \in J_R$ for any $x \in J_R$ and any $r \in F[G]$.

The structure of ideals in $F[G]$ is particularly simple if characteristics of the field does not divide the group size $\gcd(p, \ell) = 1$. Then, according to Maschke's theorem, the group algebra is semisimple, and any ideal is a principal ideal generated by an idempotent, e.g., $J_L = F[G]f_J$ for a left ideal, with idempotent $f_J^2 = f_J \in J_L$, and similarly, $J_R = e_J F[G]$ for a right ideal, with idempotent $e_J^2 = e_J \in J_R$ (see, e.g., Corollary 2.2.5 in Ref. [31]).

The usual inner product in F^ℓ is related to the group trace with the help of a linear map [32]$\widehat{\ }$: $F[G] \to F[G]$,

$$\widehat{a} \equiv \sum_{g\in G} a_{g^{-1}} g = \sum_{g\in G} a_g g^{-1}. \tag{5}$$

Namely, for any $\boldsymbol{a}, \boldsymbol{b} \in F^\ell$, and the corresponding group algebra elements $a, b \in F[G]$,

$$\boldsymbol{a} \cdot \boldsymbol{b} \equiv \sum_{g\in G} a_g b_g = \operatorname{tr}_G(\widehat{a}b) = \operatorname{tr}_G(b\widehat{a}). \tag{6}$$

As a reminder, the group trace is defined as the coefficient of the group identity element $1 \in G$: for any $a \in F[G]$, $\operatorname{tr}_G(a) \equiv a_1 \in F$.

Given a right group code in a semisimple group algebra $F[G]$ equivalent to a right ideal $J_R \equiv \widehat{a} \cdot F[G]$ generated by an element $\widehat{a} \in F[G]$, any group algebra element x corresponding to a vector $\boldsymbol{x}$ in the orthogonal code satisfies [32] the equation $xa = 0$. If we denote an idempotent $e_a^2 = e_a \in F[G]$ such that $e_a a = a$, the solution of the orthogonality equation is the left ideal $J_L \equiv F[G](1 - e_a)$.

B. Quantum CSS codes

A quantum Calderbank-Shor-Steane (CSS) code [33] $Q = \mathrm{CSS}(H_X, H_Z)$ with parameters $[[n, k, d]]_q$ over a Galois field F is isomorphic to a direct sum of an X- and a Z-like code,

$$Q = Q_X \oplus Q_Z = C_{H_Z}^\perp / C_{H_X} \oplus C_{H_X}^\perp / C_{H_Z}, \tag{7}$$

where each term in the right-hand side is a quotient of two linear spaces in F^n, and rows of the stabilizer generator matrices H_X and H_Z must be orthogonal:

$$H_X H_Z^T = 0. \tag{8}$$

Explicitly, e.g., elements of Q_Z are equivalence classes of vectors orthogonal to the rows of the matrix H_X, with any two vectors whose difference is a linear combination of the rows of H_Z identified. Vectors in the same class are called mutually degenerate, while vectors in the class of the zero vector are called trivial. The codes Q_X and Q_Z have q^k degeneracy classes each, where

$$k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z \tag{9}$$

is the quantum code dimension. The distance of the code is $d \equiv \min(d_X, d_Z)$, where the two CSS distances,

$$d_X = \min_{\boldsymbol{c}\in C_{H_Z}^\perp \setminus C_{H_X}} \operatorname{wgt} \boldsymbol{c}, \quad d_Z = \min_{\boldsymbol{c}\in C_{H_X}^\perp \setminus C_{H_Z}} \operatorname{wgt} \boldsymbol{c}, \tag{10}$$

are the minimum weights of nontrivial vectors (any representative) in $C_{H_Z}^\perp$ and $C_{H_X}^\perp$, respectively. A set of logical operators' representatives in Q_X and Q_Z can be chosen to form k canonically conjugate pairs. Equivalently, logical generator matrices L_X and L_Z with k rows each can be constructed such that

$$L_X H_Z^T = 0, \quad L_Z H_X^T = 0, \quad L_X L_Z^T = I_k, \tag{11}$$

where I_k is a $k \times k$ identity matrix.

Physically, a quantum code operates in a Hilbert space $\mathcal{H}_q^{\otimes n}$ associated with n quantum-mechanical systems, Galois qudits [34], with q states each, and a well-defined basis of X and Z operators acting in $\mathcal{H}_q^{\otimes n}$ [35]. Elements of the codes C_{H_X} and C_{H_Z} correspond to X and Z operators in the stabilizer group $\mathcal{S}$ acting in the Hilbert space. Generators of $\mathcal{S}$ must be measured frequently during the operation of the code; generating matrices H_X and H_Z with smaller row weights result in codes which are easier to implement in practice. Orthogonality condition (8) ensures that the stabilizer group is Abelian. Nontrivial vectors in Q_X and Q_Z correspond to X and Z logical operators, respectively. Codes with larger distances have logical operators which involve more qudits; such codes typically give better protection.

More generally, a CSS *subsystem* code [36,37]

$$\operatorname{CSS}(G_X, G_Z) = Q_X \oplus Q_Z \tag{12}$$

can be defined by two n-column gauge generator matrices G_X and G_Z whose rows are not necessarily orthogonal. Such a code can be constructed from a regular CSS code (7) of dimension $k_{\text{orig}} = k + p_\star$ by selecting $p_\star \leqslant k_{\text{orig}}$ logical operator pairs and adding the corresponding rows [forming matrices L'_X, L'_Z such that $L'_X(L'_Z)^T = I_{p_\star}$] to the rows of the CSS generator matrices,

$$G_X = U_X \begin{pmatrix} H_X \\ L'_X \end{pmatrix}, \quad G_Z = U_Z \begin{pmatrix} H_Z \\ L'_Z \end{pmatrix}, \tag{13}$$

where U_X and U_Z are invertible matrices corresponding to arbitrary row transformations, and the subscript in $p_\star$ is to disambiguate with the field characteristic p. Respectively, for a CSS subsystem code,

$$k = n - \operatorname{rank} G_X - \operatorname{rank} G_Z + \operatorname{rank}\left(G_X G_Z^T\right), \tag{14}$$

and its distance, e.g., for the subcode Q_Z,

$$d_Z = \min_{\boldsymbol{c}\in C_{H_X}^\perp \setminus C_{G_Z}} \operatorname{wgt} \boldsymbol{c} = \min_{\boldsymbol{c}\in C_{G_X}^\perp \setminus C_{G_Z}} \operatorname{wgt} \boldsymbol{c}. \tag{15}$$

Prominent examples of subsystem codes are erasure codes obtained when matching sets of columns are removed from the stabilizer generator matrices H_X and H_Z. Equivalently, with $\mathcal{I}$ the index set of the remaining columns, a subsystem erasure code has the punctured stabilizer group $\mathcal{S}_{\mathrm{p}}(\mathcal{I})$.

III. TWO-BLOCK CSS CODES

Here we discuss general properties of two-block CSS codes [14] with generator matrices in the form

$$H_X = (A, B), \quad H_Z^T = \begin{pmatrix} B \\ -A \end{pmatrix}, \tag{16}$$

where $A, B \in M_\ell(F)$ are square commuting matrices of size $\ell \times \ell$ with elements in a Galois field F. The commutativity is important since it guarantees the CSS orthogonality condition (8).

An important tool in analyzing the parameters of such codes will be the subsystem *block-erasure* code $\operatorname{CSS}(A, B^T)$ and its CSS dual, obtained by erasing the qudits in the right and left blocks, respectively. We will denote the common parameters of these codes as

$$[[\ell, k_{\mathrm{S}}, d_{\mathrm{S}}]]_q, \quad \text{and} \quad p_\star \equiv \operatorname{rank}(AB), \tag{17}$$

with $p_\star$ the number of gauge qudits [cf. Eqs. (13) and (14)].

A. Code dimension

Given a square matrix $A \in M_\ell(F)$ of size ℓ with elements in the Galois field F, consider size-ℓ idempotent matrices E_A and F_A of the same rank as A, such that

$$E_A^2 = E_A, \quad F_A^2 = F_A, \quad E_A A = A F_A = A. \tag{18}$$

While such matrices are not unique, they can always be constructed from the Smith normal form decomposition $A = U_A D_A V_A$, where $U_A, V_A \in M_\ell(F)$ are square invertible matrices, and $D_A = \operatorname{diag}(1, \ldots, 1, 0, \ldots, 0) \in M_\ell(F)$ has exactly rank -A nonzero elements along the diagonal. Namely, we may choose

$$E_A \equiv U_A D_A U_A^{-1}, \quad F_A \equiv V_A^{-1} D_A V_A. \tag{19}$$

With idempotent matrices (18), it is now easy to calculate the ranks of matrices (16). Indeed, row and column transformations give (this is a simplified version of more general expressions in Refs. [38,39])

$$\begin{aligned} \operatorname{rank} H_X &= \operatorname{rank} \begin{pmatrix} A & E_A B \\ 0 & (I - E_A)B \end{pmatrix} \\ &= \operatorname{rank}(A) + \operatorname{rank}(I - E_A)B, \\ &= \operatorname{rank} A + \operatorname{rank} B - \operatorname{rank}(E_A B), \end{aligned} \tag{20}$$

where we also expressed $\operatorname{rank} B$ with the help of a similar decomposition, $\operatorname{rank} B = \operatorname{rank}(E_A B) + \operatorname{rank}(I - E_A)B$. Similarly, for the other matrix we get

$$\operatorname{rank} H_Z = \operatorname{rank} A + \operatorname{rank} B - \operatorname{rank}(B F_A). \tag{21}$$

We have, e.g., $\operatorname{rank} E_A B \geqslant \operatorname{rank} E_A B A = \operatorname{rank} AB = p_\star$. For a given set of idempotent matrices (18), introduce non-negative *rank-defect* parameters $\delta_X \geqslant 0$ and $\delta_Z \geqslant 0$,

$$\operatorname{rank} E_A B \equiv p_\star + \delta_X, \quad \operatorname{rank} B F_A \equiv p_\star + \delta_Z, \tag{22}$$

where $p_\star \equiv \operatorname{rank} AB$ is the number of gauge qudits in the subsystem code $\operatorname{CSS}(A, B^T)$ [see Eq. (17)]. While rank defects are introduced with respect to a specific set of idempotents E_A and F_A, Eqs. (20) and (21) guarantee that they are, in fact, independent of the choice of idempotents in Eq. (18). Moreover, the same parameters can be also introduced in terms of similarly defined idempotent matrices associated with the matrix B:

$$\operatorname{rank} E_B A = p_\star + \delta_X, \quad \operatorname{rank} A F_B = p_\star + \delta_Z. \tag{23}$$

Physically, δ_X and δ_Z are the numbers of rows in H_X and H_Z, respectively, which give nontrivial linearly independent contributions to the centers of both $\mathcal{S}[\mathcal{I}_L]$ and $\mathcal{S}[\mathcal{I}_R]$, the stabilizer group punctured to individual blocks. Combining the obtained expressions (20) and (21) with Eq. (14) and the definitions (22), we have

$$\operatorname{rank} H_X = \ell - k_S - \delta_X, \quad \operatorname{rank} H_Z = \ell - k_S - \delta_Z, \tag{24}$$

which gives for the original two-block code (16),

$$k = 2k_S + \delta_X + \delta_Z. \tag{25}$$

Most generally, $\delta_X \neq \delta_Z$, and these parameters are nonnegative. However, a rank defect is guaranteed to vanish with an additional commutativity condition (see Appendix A for the proofs).

Statement 1. If E_A commutes with B, then $\delta_X = 0$. Similarly, if F_A commutes with B, then $\delta_Z = 0$.

A similar statement is also valid in terms of the idempotents E_B and F_B, e.g., $\delta_X = 0$ if $E_B A = A E_B$.

Another special case is when there exists an invertible matrix S which can simultaneously transform both matrices A and B into their transpose

$$SAS^{-1} = A^T, \quad SBS^{-1} = B^T. \tag{26}$$

Here, with any choice of E_A, we can take $F_A^T = S E_A S^{-1}$, which, with Eq. (22), immediately gives $\delta_X = \delta_Z$, not necessarily zero. This gives the following:

Statement 2. If both matrices A and B can be simultaneously transformed into their respective transpose [see Eq. (26)], then $\delta_X = \delta_Z$.

While the condition may appear unnatural, as we discuss below, it is satisfied for Abelian 2BGA codes [27].

To summarize this section, most generally, $\delta_X \neq \delta_Z$, and $\operatorname{rank} H_X \neq \operatorname{rank} H_Z$, so that the dimension of a two-block code does not have a particular parity. However, under conditions of Statement 1 or Statement 2, we get $\operatorname{rank} H_X = \operatorname{rank} H_Z$, and code dimension k even. Furthermore, under conditions of Statement 1 we have $\delta_X = \delta_Z = 0$, so that $k = 2k_S$, exactly twice the dimension of the block-erasure subsystem code $\mathrm{CSS}(A, B^T)$.

B. Upper distance bounds

The same idempotent matrices can be used to analyze the structure of the codewords. Most generally, one can expect a given nontrivial codeword $\boldsymbol{c}_Z \equiv \binom{\boldsymbol{u}}{\boldsymbol{v}}$ either to be equivalent to such a codeword with only one of the components nonzero, or not, in which case any equivalent codeword has both $\boldsymbol{u}$ and $\boldsymbol{v}$ nonzero. Unlike the cases of HP or GB codes [13,19], for two-block codes with $\delta_X > 0$ or $\delta_Z > 0$, it is not possible to choose a full set of mutually nondegenerate and independent codewords in the former class. Nevertheless, the corresponding projections can be used to construct upper bounds on the distances. Specifically, consider two reduced-dimension codes $Q'_\mu \equiv \mathrm{CSS}(H_X^{(\mu)}, H_Z)$, $\mu \in \{L, R\}$, with

$$H_X^{(L)} = \begin{pmatrix} A & B \\ 0 & I - E_A \end{pmatrix}, \quad H_X^{(R)} = \begin{pmatrix} A & B \\ I - E_B & 0 \end{pmatrix}, \tag{27}$$

where additional rows guarantee that Z-logical operators can be chosen to be supported on one block only, two single-block Z-shortened codes, $Q''_L \equiv \mathrm{CSS}\,(A, (H_Z)_L)$ and $Q''_R \equiv \mathrm{CSS}\,(B, (H_Z)_R)$, with

$$(H_Z)_L^T = B(I - F_A), \quad (H_Z)_R^T = A(I - F_B), \tag{28}$$

and two classical codes C_L, C_R with parity-check matrices, respectively,

$$H_L \equiv \begin{pmatrix} A \\ E_B \end{pmatrix}, \quad H_R \equiv \begin{pmatrix} B \\ E_A \end{pmatrix}. \tag{29}$$

As detailed in Appendix A, for a chosen $\mu \in \{L, R\}$, these definitions correspond to a series of subsequent restrictions on Z codewords, and we get the following:

Statement 3. For a given two-block code Q and a chosen $\mu \in \{L, R\}$, consider quantum codes Q'_μ and Q''_μ, and a classical code C_μ. Distances of these codes satisfy

$$d_Z \equiv d_Z(Q) \overset{\text{(a)}}{\leqslant} d_Z(Q'_\mu) \overset{\text{(b)}}{\leqslant} d_Z(Q''_\mu) \overset{\text{(c)}}{\leqslant} d(C_\mu). \tag{30}$$

This implies the inequality $d_Z \leqslant d_Z(Q''_\mu)$, a special case of Z-shortening lemma from Ref. [17].

A particularly simple upper bound for the distance $d_Z(Q''_L)$, and thus for the distance of the original two-block code (16), is obtained when matrix A is block diagonal (see the proof in Appendix A):

Statement 4. Suppose matrix A is block diagonal with the maximum block size m, and the code Q''_L is nontrivial, $k(Q''_L) > 0$. Then the distance $d_Z(Q''_L) \leqslant m$.

Evidently, when matrix B is block diagonal, a similar bound also exists for $d_Z(Q''_R)$.

C. Lower distance bounds

Best known are the usual CSS bounds [33]

$$d_Z \geqslant d(C_{H_X}^\perp), \quad d_X \geqslant d(C_{H_Z}^\perp). \tag{31}$$

However, since the rows of H_X and H_Z are mutually orthogonal, we have, e.g., $d(C_{H_X}^\perp) \leqslant d(C_{H_Z}) \leqslant W_Z$, the minimum row weight of the matrix H_Z. Since our main interest is in highly degenerate quantum LDPC codes with bounded stabilizer weights and diverging distances, the CSS bounds (31) are not very useful.

Here we construct lower bounds for the distance in terms of the distances of single-block codes. It is easy to see that the Z-punctured stabilizer codes

$$\mathrm{CSS}\,((1 - E_B)A, B^T) \text{ and } \mathrm{CSS}\,((1 - E_A)B, A^T) \tag{32}$$

both have the dimension $k_S + \delta_X$. In the special case $\delta_X = 0$, this is the same as for single-block erasure subsystem codes (17), and the Z distances are also the same as $d_Z(A, B^T)$ and $d_Z(B, A^T)$, respectively. The condition $\delta_X = 0$ also guarantees that any nontrivial Z codeword in one of these codes becomes a nontrivial codeword in the original two-block code after it is padded with zeros. The additional condition $\delta_Z = 0$ guarantees that the full set of linearly independent Z codewords of the two-block code can be constructed this way, which coincides with the condition of Z-puncturing lemma from Ref. [17]. With the help of the fact that the two single-block erasure codes with parameters (17) are related by CSS conjugation, we obtain a simple lower distance bound:

Statement 5. Suppose both rank defects in Eq. (22) are zero, $\delta_X = \delta_Z = 0$. Then,

$$d \geqslant d_S, \quad d_S \equiv d(A, B^T). \tag{33}$$

We notice that under the conditions of Statement 5, e.g., the Z-shortened code Q_L'' in Statement 3 can also be seen as a gauge-fixed subsystem code $\mathrm{CSS}(A, B^T)$. However, this particular gauge fixing may result in the increased d_Z. Therefore, we should not necessarily expect the lower bound (33) to saturate, except when $p_\star = 0$, or, equivalently, $\mathrm{x}AB = 0$, in which case the erasure code $\mathrm{CSS}(A, B^T)$ is also a stabilizer code.

We finish this section with two more general expressions relating the distance d_Z of a two-block code with those of auxiliary quantum codes of smaller dimension. Namely, any nontrivial vector $\boldsymbol{c}_Z = \binom{\boldsymbol{u}}{\boldsymbol{v}}$ is either degenerate to a solution with $\boldsymbol{u}$ nonzero and $\boldsymbol{v} = 0$, or to a solution with any $\boldsymbol{u}$ and $\boldsymbol{v} \not\simeq 0$, but not both. This and an equivalent construction with $\boldsymbol{u}$ and $\boldsymbol{v}$ interchanged give two generalizations of Statement 1 from Ref. [19],

$$d_Z = \min\left\{d_Z(H_X^{(\mu)}, H_Z), d_Z(H_X, H_Z^{(\mu)})\right\}, \tag{34}$$

with a $\mu \in \{L, R\}$, and matrices in Eqs. (16) and (27), and

$$H_Z^{(L)} = \begin{pmatrix} B & I - F_A \\ -A & 0 \end{pmatrix}^T, \quad H_Z^{(R)} = \begin{pmatrix} B & 0 \\ -A & I - F_B \end{pmatrix}^T. \tag{35}$$

Even though Eq. (34) relates the distance of the original quantum code to those of two other quantum codes with the same block size, it may still be useful since the two codes have half as many basis vectors and exponentially fewer vectors at large k, $q^{k/2} \ll q^k$.

IV. 2BGA CODES: CONSTRUCTION AND GENERAL PROPERTIES

A. Definition

2BGA codes are a special case of two-block codes (16) where the commuting matrices are constructed with the help of a group algebra. Alternatively, 2BGA codes are a version of GB codes where a cyclic group is replaced with a general group G. They can also be thought of as the smallest LP codes.

Given two elements $a, b \in F[G]$ of the group algebra $F[G]$ [see Eq. (3)], with the group size $\ell \equiv |G|$, the $\ell \times \ell$ matrices $A \equiv \mathrm{L}(a)$ and $B \equiv \mathrm{R}(b)$, respectively, are defined by the left and right action on group elements,

$$[\mathrm{L}(a)]_{\alpha,\beta} \equiv \sum_{g\in G} a_g \delta_{\alpha, g\beta}, \quad [\mathrm{R}(b)]_{\alpha,\beta} \equiv \sum_{g\in G} b_g \delta_{\alpha, \beta g}, \tag{36}$$

where group elements $\alpha, \beta \in G$ are used to index rows and columns, and $\delta_{\alpha,\beta} = 1$ if $\alpha = \beta$ and 0 otherwise is the Kronecker delta. It is easy to verify that for group elements $g \in G$, matrices $\mathrm{L}(g)$ form the regular F-linear representation of G. Further, for any $a, b \in F[G]$, $\mathrm{L}(a)\,\mathrm{L}(b) = \mathrm{L}(ab)$, $\mathrm{R}(a)\,\mathrm{R}(b) = \mathrm{R}(ba)$, while any two matrices from different sets commute with each other [5], $\mathrm{L}(a)\,\mathrm{R}(b) = \mathrm{R}(b)\,\mathrm{L}(a)$; it is the latter property that gives the CSS orthogonality condition (8). The map between $\mathrm{L}(a)$ and $\mathrm{R}(b)$ can be given in terms of the permutation matrix P with components $P_{\alpha,\beta} \equiv \delta_{\alpha,\beta^{-1}}$, $\alpha, \beta \in G$,

$$\mathrm{L}(a) = P[\mathrm{R}(a)]^T P, \tag{37}$$

where $[\,\cdot\,]^T$ denotes matrix transposition. The symmetric permutation operator P acting in F^ℓ is equivalent to the map $\widehat{\ }: F[G] \to F[G]$ in Eq. (5), $P\boldsymbol{a} = \widehat{\boldsymbol{a}}$. It is also easy to verify that for all $a \in F[G]$,

$$[\mathrm{L}(a)]^T = \mathrm{L}(\widehat{a}), \quad [\mathrm{R}(a)]^T = \mathrm{R}(\widehat{a}). \tag{38}$$

In the following, $\mathrm{LP}[a, b]$ denotes the 2BGA code constructed from group algebra elements $a, b \in F[G]$, the CSS code (16) with $A \equiv \mathrm{L}(a)$ and $B \equiv \mathrm{R}(b)$ given by Eq. (36). This notation refers to more general LP codes [5], defined in terms of a pair of matrices with elements in $F[G]$. Namely, 2BGA codes are a degenerate case of LP codes with both matrices of dimension 1×1. Previously considered special cases are GB codes [14,19,20], with G a cyclic group, and *Abelian* 2BGA codes [27], with G an Abelian group.

B. Code equivalence

The complexity of enumerating 2BGA codes can be significantly reduced by excluding permutation-equivalent codes (the proof is given in Appendix B):

Theorem 1. For any $a, b \in F[G]$, the 2BGA code $\mathrm{LP}[a, b]$ is equivalent to

(i) $\mathrm{LP}[\varphi(a), \varphi(b)]$, for any automorphism $\varphi : G \to G$;
(ii) $\mathrm{LP}[\alpha^{-1}a\alpha, \beta^{-1}b\beta]$, for any $\alpha, \beta \in G$;
(iii) $\mathrm{LP}[xa, yb]$, for any nonzero $x, y \in F$.
(iv) $\mathrm{LP}[a\alpha, \beta b]$, for any $\alpha, \beta \in G$;
(v) $\mathrm{LP}[\widehat{b}, \widehat{a}]$;
(vi) in addition, the code CSS dual to $\mathrm{LP}[a, b]$, with interchanged H_X and H_Z matrices, is permutation equivalent to $\mathrm{LP}[\widehat{a}, -\widehat{b}] \cong \mathrm{LP}[b, a]$.

Notice that with $\alpha = \beta$, Theorem 1(ii) is a special case of (i) for inner automorphisms. These, and, more generally, item (ii), would be trivial for an Abelian group. On the other hand, with an Abelian group G, for any $a \in F[G]$, $\mathrm{L}(a) = \mathrm{R}(a)$, which also gives $\mathrm{LP}[a, b] \cong \mathrm{LP}[b, a]$, and an immediate consequence, $d_X = d_Z$. These properties need not to be true with a non-Abelian group G.

C. Connectivity of 2BGA codes

It is convenient to rewrite the CSS equations, e.g., defining a nontrivial codeword $\boldsymbol{c}_Z = \binom{\boldsymbol{u}}{\boldsymbol{v}} \in \mathcal{C}_{H_X}^\perp \setminus \mathcal{C}_{H_Z} \subset F^{2\ell}$ in a 2BGA code $\mathrm{LP}[a, b]$, in terms of the corresponding pair of group algebra elements $u, v \in F[G]$. Direct calculation gives

$$au + vb = 0, \tag{39}$$

$$[u + wb, v - aw] \neq [0, 0], \quad \forall\, w \in F[G], \tag{40}$$

where Eq. (40) enumerates the degeneracy class.

For a given $a \in F[G]$, consider the subgroup

$$G_a \equiv \langle \{g \in G : a_g \neq 0\} \rangle, \tag{41}$$

the *support group* [40] generated by group elements with nonzero coefficients in a [cf. Eq. (3)]. Evidently, if we start with any group element $x \in G$, repeated left multiplication by a can only generate group algebra elements ax, a^2x, ..., supported on the left coset $G_a x$ of x. Sizes of left cosets being equal, we have that the matrix $\mathrm{L}(a)$ is block diagonal, with m_a blocks of size $|G_a|$, where m_a is the index of the support group G_a in G, $m_a \equiv [G : G_a]$. The same is true for $\mathrm{R}(b)$, except in this case we are dealing with the right cosets xG_b [cf. Eq. (39)], and we may need to order group elements differently.

Overall, Eq. (39) implies the block structure of the code: the row of matrix H_X labeled by the group element $x \in G$ is in the block associated with the double coset $G_a x G_b$. Since matrix transposition does not change the support group, $G_{\hat{a}} = G_a$, the same is true for the xth row of matrix H_Z. Therefore, if the product of the two subgroups (the double coset associated with the group identity element $1 \in G$) does not contain all group elements, $G_a G_b \subsetneq G$ (as sets), the code LP$[a, b]$ is decomposed into smaller mutually disconnected subcodes associated with different double cosets in $G_a \backslash G / G_b$. It is well known that double cosets do not necessarily have the same sizes [41], so the individual double-coset subcodes are not expected to be equivalent.

To analyze the structure of the matrices in more detail, let us fix an ordering so that elements of the subgroup $G_a = \{1, g_2, g_3, \ldots\}$ go first in this order, followed by elements of each right coset $G_a x$, with elements of G_a taken in the same order, $\{x, g_2 x, g_3 x, \ldots\}$, and $x \in \mathcal{A}$, a transversal set of elements from $G_a \backslash G$ of size m_a. With this choice, it is easy to see from Eq. (36) that the m_a blocks of the matrix A associated with different cosets are identical $A = A_1 \otimes I_{m_a}$, where $A_1 \equiv \mathrm{L}_{G_a}(a)$, and the subscript indicates the subgroup that row and column indices are restricted to. The same is true for the matrix B, except to reveal the block structure, we may need to take group elements in a different order. Denoting the corresponding permutation matrix as S, we have

$$B = S(I_{m_b} \otimes B_1)S^{-1}, \quad B_1 \equiv \mathrm{R}_{G_b}(b). \tag{42}$$

With the ordering of the group G_a fixed, the only remaining freedom is to order the elements of $\mathcal{A}$; we can ensure that elements of each double coset come together, so that decomposition of the 2BGA code into a direct sum of individual double-coset subcodes be evident.

In general, a (double) coset is not a subgroup of G; most of cosets do not even contain the group identity element. However, different double cosets are related to each other by conjugation. In the case of support subgroups, we can write $G_a x G_b = G_a 1 G_{xbx^{-1}}$, which allows to map any double coset to a double coset containing the group identity element. The corresponding double-coset subcodes of 2BGA codes are also related:

Statement 6. A subcode of a disconnected 2BGA code LP$[a, b]$, with some $a, b \in F[G]$, supported in the double coset $G_a x G_b$, $x \in G$, is equivalent to a subcode of LP$[a, xbx^{-1}]$ supported in the double coset $G_a 1 G_{xbx^{-1}}$.

In particular, this implies that in the case of an Abelian group G, a code equivalent to any double-coset subcode of a 2BGA code LP$[a, b]$ over $F[G]$ can be constructed as a 2BGA code over a subgroup of G. A bit more generally, note the following:

Statement 7. If the intersection subgroup $N \equiv G_a \cap G_b$ is Abelian and normal in both support groups, the subcode of LP$[a, b]$ supported in the double coset $G_a 1 G_b$ is equivalent to a 2BGA code over a group G' of rank $|G_a 1 G_b|$.

In particular, with disjoint subgroups $G_a \cap G_b = \{1\}$, the group in Statement 7 is just a direct product of the two subgroups $G' = G_a \times G_b$. In this case we can independently choose the order of elements in each subgroup, and both matrices may simultaneously have the form of Kronecker products, $A = A_1 \otimes I_{n_b}$, $B = I_{n_a} \otimes B_1$, with $n_b \equiv |G_b| = m_a$ and $n_a \equiv |G_a| = m_b$. This is exactly the block structure of an HP code [13], constructed from square matrices A_1 and B_1. If we denote the parameters of classical linear codes with parity-check matrices A_1 and B_1, respectively, as $[n_a, k_a, d_a]_q$ and $[n_b, k_b, d_b]_q$ (these parameters remain the same when the transposed matrices are used), the parameters of the quantum HP code are known explicitly $[[2n_a n_b, 2k_a k_b, \min(d_a, d_b)]]_q$. Additional lower and upper distance bounds on more general codes under conditions of Statement 7 are discussed in Sec. IV F.

D. Symmetry group of a 2BGA code

With Eqs. (39) and (40), it is easy to check the symmetry of a given 2BGA code. Indeed, for any $g \in \mathcal{C}_G(G_a)$, the centralizer of the subgroup G_a in G, if a pair $[u, v]$ is in the code, then the corresponding left-multiplied pair $[gu, gv]$ is also in the code. The same is true for the right-multiplied pairs $[uh, vh]$, $\forall\, h \in \mathcal{C}_G(G_b)$.

For an Abelian group G, we obtain G-symmetric analogs of index-two qQC codes, quasi-Abelian codes [3,27]. With a non-Abelian G, the overall symmetry group of a 2BGA code is generally smaller than G. In any case, it includes $\mathrm{Z}(G)$, the center of G.

E. Code dimension and related codes

Since 2BGA codes are a subset of general two-block codes, all general properties from Sec. III apply. The case of GB codes [14,19,20] is recovered when G is a cyclic group,

$$C_\ell \equiv \langle r | r^\ell = 1 \rangle = \{1, r, r^2, \ldots, r^{\ell-1}\},$$

where $r^\ell = 1$ is implicit in the set notation. There is an obvious one-to-one map between the group algebra $F[C_\ell]$ and the ring of modular polynomials $F[x]/(x^\ell - 1)$. Then, a 2BGA code LP$[a, b]$ is also a generalized-bicycle code GB$[a(x), b(x)]$ specified by polynomials $a(x), b(x) \in F[x]/(x^\ell - 1)$, and the square blocks in Eq. (16) are just the circulant matrices $A = a(P)$ and $B = b(P)$, where

$$P = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} \tag{43}$$

is an $\ell \times \ell$ cyclic permutation matrix. A simple expression for the dimension of a code GB$[a, b]$ was given in Ref. [20]. In this case, rank $H_X = \operatorname{rank} H_Z = \ell - \deg h(x)$, and

$$k = 2 \deg h(x), \quad h(x) \equiv \gcd(a(x), b(x), x^\ell - 1). \tag{44}$$

In fact, $\deg h(x)$ also coincides with the dimension k_S of the quantum cyclic code $\mathrm{CSS}(A, B^T)$, the single-block subsystem erasure code (17), and Eq. (25) guarantees that for any cyclic group G, $\delta_X = \delta_Z = 0$.

More generally, for an Abelian group G, it is known that rank $H_X = \operatorname{rank} H_Z$, and the code dimension is even [27]. An equivalent statement, $\delta_X = \delta_Z$, also follows from Statement 2 and Eq. (37), if we remember that in the case of an Abelian group G, for any $a \in F[G]$, $\mathrm{L}(a) = \mathrm{R}(a)$. A stronger statement can be made whenever a 2BGA code can be decomposed as a direct sum of GB or HP codes, e.g., under conditions of Statement 7:

Statement 8. Consider a code LP$[a, b]$ with $a, b \in F[G]$. If the intersection subgroup $N \equiv G_a \cap G_b$ is Abelian and normal in both support groups, the rank defects of the corresponding CSS matrices vanish, $\delta_X = \delta_Z = 0$.

In particular, $\delta_X = \delta_Z = 0$ for any Abelian 2BGA code.

An alternative sufficient condition follows from Statement 1 in the special case of a *semisimple* group algebra $F[G]$, i.e., when the field characteristic p and the group rank ℓ are mutually prime. Indeed, any ideal in a semisimple group algebra is a summand, and for any $a \in F[G]$, there exist idempotent elements $e_a, f_a \in F[G]$ such that $e_a^2 = e_a$, $f_a^2 = f_a$, and $e_a a = a$, $a f_a = a$. In this case, we can choose $E_A = \mathrm{L}(e_a)$, $F_A = \mathrm{L}(f_a)$, which are guaranteed to commute with $B \equiv \mathrm{R}(b)$. A bit of thought gives a more general sufficient condition:

Statement 9. Consider a code LP$[a, b]$ over group algebra $R \equiv F[G]$ such that the ideals aR and Ra (or the two ideals generated by b) be semisimple. Then, rank defects of the corresponding CSS matrices vanish, $\delta_X = \delta_Z = 0$.

A somewhat less general but easier to apply condition is, e.g., that the group algebra $F[G_a]$ be semisimple, i.e., rank of the support group G_a be mutually prime with the field characteristic p.

The *semi-Abelian* 2BGA codes whose CSS generator matrices have the property $\delta_X = \delta_Z = 0$ are special: their codeword basis can be chosen so that each codeword is supported on only one block, similarly to GB codes [14,19,20] and HP codes [13,16,17]. In particular, this gives a lower distance bound (33) in terms of the single-block erasure code, and guarantees the condition of Statement 4, giving a simple upper bound on the distance in terms of matrix block sizes $d \leqslant \min(|G_a|, |G_b|)$.

However, not all 2BGA codes have this property. In particular, there exist *essentially non-Abelian* 2BGA codes where $\delta_X \neq \delta_Z$ or $\delta_X = \delta_Z \neq 0$.

Example 1. Consider the alternating group A_4, also known as the rotation group T of a regular tetrahedron,

$$T = \langle x, y | x^3 = (yx)^3 = y^2 = 1 \rangle, \quad |T| = 12$$

and the binary algebra $\mathbb{F}_2[T]$. Select $a = 1 + x + y + x^{-1}yx$ and $b = 1 + x + y + yx$ to get a 2BGA code LP$[a, b]$ with parameters $[[24, 5, 3]]_2$.

F. The case of quasi-Abelian lifted-product codes

Here we consider in more detail the special case of codes in Statements 7 and 8, 2BGA codes LP$[a, b]$, with $a, b \in F[G]$ such that the support groups G_a and G_b have Abelian intersection group $N \equiv G_a \cap G_b$ normal both in G_a and G_b. As discussed, such codes can be seen as F-linear *quasi-Abelian* LP codes or, equivalently, as HP codes over the Abelian group algebra $F[N]$. Their structure and parameters can be analyzed using the techniques specific to such codes.

The following lower and upper bounds are constructed by analogy with the corresponding theorems from Ref. [14]:

Statement 10 (Version of Theorem 5 from Ref. [14]). Given elements $a, b \in F[G]$ such that the intersection subgroup $N \equiv G_a \cap G_b$ of rank c is Abelian and normal in both support groups, let $d_A^\perp$ and $d_B^\perp$ be the distances of classical F-linear group algebra codes with parity-check matrices $A = \mathrm{L}(a)$ and $B = \mathrm{R}(b)$. Then the distance d_Z of the code LP$[a, b]$ satisfies $d_Z \geqslant d_0 \equiv \lceil \min(d_A^\perp, d_B^\perp)/c \rceil$.

To get a matching upper bound, we need an additional condition to ensure that, e.g., vectors in $C_A^\perp$ have vectors matching by symmetry in $C_B^\perp$ to form nontrivial GB codes [see Eq. (B2) in the proof of Statement 8]. It is implicit in the decomposition (B2) that we can characterize the symmetry by ideals of $F[N]$.

Let J be a *maximal* ideal in $F[N]$, and $\overline{J} = \langle G_a J G_b \rangle$ its extension to the subspace associated with the coset $G_a 1 G_b$. Namely, if $\mathcal{A}$ and $\mathcal{B}$, respectively, are transversal sets of representatives from G_a/N and $N \backslash G_b$, every element $x \in \overline{J}$ can be uniquely written as

$$x = \sum_{\alpha \in \mathcal{A}} \sum_{\beta \in \mathcal{B}} \alpha\, x_{\alpha,\beta}\, \beta, \quad x_{\alpha,\beta} \in J. \tag{45}$$

The corresponding code C_J, the *two-sided coset code* generated by J, is simply a set of vectors in F^ℓ corresponding to elements of $\overline{J}$. The proof of the following upper bound is based on the fact that the product of any two nonzero elements in a maximum ideal is nonzero.

Statement 11 (Version of Theorem 6 from Ref. [14]). Let J be a maximal ideal in $F[N]$, C_J the two-sided coset code generated by J, and $\widehat{C}_J \equiv P C_J$ its image under the linear map (5). Denote d' the distance of the subcode $C_A^\perp \cap C_J$. Then, if $C_{B^T}^\perp \cap \widehat{C}_J \neq \{0\}$, the distance of the 2BGA code LP$[a, b]$ satisfies the upper bound $d_Z \leqslant d'$.

Evidently, there is also an upper bound in terms of the distance of the subcode $C_B^\perp \cap C_J$.

If we denote the indices of N in the two support groups as $\ell_a \equiv [G_a : N]$ and $\ell_b \equiv [G_b : N]$, as discussed in Sec. IV C, matrices A and B have blocks of size $c\ell_a$ and $c\ell_b$, respectively. Then, for a nontrivial 2BGA code, the parameter d_0 in Statement 10 satisfies $d_0 \leqslant \min(\ell_a, \ell_b)$, while the upper bounds guarantee $d_Z \leqslant c \min(\ell_a, \ell_b)$, as would also be expected from Statement 4.

The upper and the lower bounds on d_Z coincide when $c = 1$: in this case the subgroup $N = \{1\}$ is trivial so that $F[N]$ is just the field F, and the auxiliary codes in statements 10 and 11 coincide, which gives $d_Z = \min(d_A^\perp, d_B^\perp)$. Of course, the same result for the distance can be also obtained from the map to a hypergraph-product code constructed from the single-block classical group algebra codes with groups G_a and G_b.

It is known [32] that classical group algebra codes include good codes with finite rates and finite relative distances. This guarantees the existence of finite-rate 2BGA codes with distance scaling as a square root of block length.

G. 2BGA codes with row weights $W \leqslant 4$

Let us discuss 2BGA codes with small row weights $W \equiv \mathrm{wgt}\,(a) + \mathrm{wgt}\,(b)$. Evidently, a code LP$[a, b]$ with, e.g., $a = 0$ has one block zero, which immediately gives $d_X = d_Z = 1$, as long as the code is nontrivial. Similarly, according to Theorem 1, any group algebra element with $\mathrm{wgt}\,(a) = 1$ can be equivalently replaced with $a = 1$, giving $A = I_\ell$, the identity matrix, which gives rank $H_X =$ rank $H_Z = \ell$, and thus a trivial code with $k = 0$. Thus, to get a useful code with row weight $W \leqslant 4$, we must have $\mathrm{wgt}\,(a) = \mathrm{wgt}\,(b) = 2$.

In this case, up to code equivalence, we can choose $a = 1 + \lambda f$, $b = 1 + \mu h$, with nonzero $\lambda, \mu \in F$ and nonidentity group elements $f, h \in G$, so that the support groups $G_a = \langle f\rangle$ and $G_b = \langle h\rangle$ be cyclic. Thus, according to Statement 7, all nontrivial 2BGA codes with row weight $W = 4$ are equivalent to direct sums of Abelian-group codes. Similarly to GB codes with row weight 4, these codes can be mapped to rotated surface codes [19].

Indeed, given a group element $g_{0,0} \equiv g \in G$, the double coset $G_a g G_b$ can be parametrized as $g_{x,y} = f^x g h^y$, with the positions $(x, y) \in \mathbb{Z}^2$ on the integer plane corresponding to the same group elements identified. In particular, $(x, y) \simeq (x + \mathrm{ord}\, f, y) \simeq (x, y + \mathrm{ord}\, h)$, where $\mathrm{ord}\, f$ is the order of the group element f. Positive displacements along horizontal and vertical edges correspond to multiplication by λg and μh, respectively. This way, we obtain a finite locally planar graph covered by the infinite square lattice. It is easy to check that the local structure of the CSS code associated with the double coset $G_a g G_b$ is exactly that of a square-lattice surface code, so that the corresponding codewords are homologically nontrivial chains (or co-chains) connecting pairs of identified vertices (faces) on the integer plane.

The nature of the resulting double-coset subcodes depends on the homology group associated with the covering map $\varphi : \mathbb{Z}^2 \to \{g_{x,y} | x, y \in \mathbb{Z}\}$. For example, with $g = 1$, we get a toric code if $\langle f\rangle \cap \langle h\rangle = \{1\}$. More generally, we get a surface code on a finite transitive graph which locally looks like a square lattice. The hand-shaking lemma guarantees that every connected component with V vertices has $2V$ edges, and its dual version gives V faces, which gives a $k = 2$ surface code for any connected component.

Further, a counting argument identical to that used in the proof of Statement 14 from Ref. [19] gives an upper bound for the $W = 4$ double-coset subcode distances $d_X^{(g)}$ and $d_Z^{(g)}$ in terms of its length $n^{(g)} = 2|G_a g G_b|$,

$$\left(d_\mu^{(g)}\right)^2 \leqslant n^{(g)}, \quad \mu \in \{X, Z\}, \tag{46}$$

which also gives $d^2 \leqslant n^{(g)} - 1$ when $d \equiv d^{(g)}$ is odd. For both inequalities, we found many cases of saturation.

V. NUMERICAL RESULTS

In this section, we present optimal parameters of short qubit-based connected 2BGA codes found numerically. Namely, we computed the parameters of all inequivalent nontrivial connected binary 2BGA codes LP$[a, b]$ with $\mathrm{wgt}\,(a) + \mathrm{wgt}\,(b) \leqslant 8$, for all non-Abelian groups G of orders $\ell \leqslant 100$, and all Abelian groups of orders $\ell \leqslant 50$, for each group keeping only the first found code with a given dimension k and distance d.

We should point out that the double-coset subcodes could, potentially, have better parameters than connected 2BGA codes of equal size. Nevertheless, for a given block length n, we do not have a way to limit the group sizes which would result in subcodes of length n. Therefore, to speed up the calculation, we decided to only consider the connected codes.

We used the Small Groups library distributed with GAP [42] to enumerate inequivalent groups, and the GAP package QDISTRND [43] to calculate the code distances. The calculations were performed at the UCR High Performance Computing Center. The resulting data and the scripts to generate the code matrices and calculate the distances are available for download at the GitHub repository `QEC-pages/2BGA-codes` [44].

Specifically, to eliminate permutation-equivalent codes for a given group G, we used the default order of group elements in GAP to establish the alphabetical order of subsets of G, which also gives an ordering for elements of $\mathbb{F}_2[G]$. In the following, we write $a < b$ if a goes before b in this order. Given the weights W_a and W_b, for each pair (a, b) generated consecutively with $\mathrm{wgt}\,(a) = W_a$, $\mathrm{wgt}\,(b) = W_b$, and also $a < b$ if $W_a = W_b$, we discarded all pairs where $\alpha a \beta < a$ or $\alpha b \beta < b$ for any $\alpha, \beta \in G$. Indeed, according to Theorem 1, these inequalities indicate that a permutation-equivalent code has already been encountered. Since the identity group element 1 is always the first in the list, we only needed to consider group algebra elements with $a_1 = b_1 = 1$. In addition, with $W_a = W_b$, we discarded the pairs with $\widehat{b} < a$ [see Theorem 1

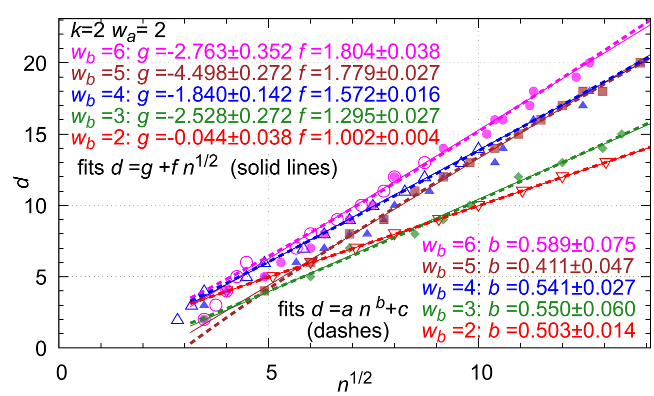

FIG. 1. Distance d of connected 2BGA codes encoding $k = 2$ qubits, with weights $W_a = 2$ and W_b as indicated, plotted as a function of the square root of the block size n. Red upside-down triangles $\triangledown$, green diamonds $\diamond$, blue triangles $\triangle$, brown squares $\square$, and purple circles $\bigcirc$, respectively, correspond to total weights $W = 4, 5, 6, 7,$ and 8. Open symbols correspond to Abelian groups, filled symbols to non-Abelian groups. Only the shortest codes with each k and d found are shown. The solid and dashed lines, respectively, are the fits using $d = g + f n^{1/2}$ and $d = a n^b + c$; the coefficients are listed in the captions.

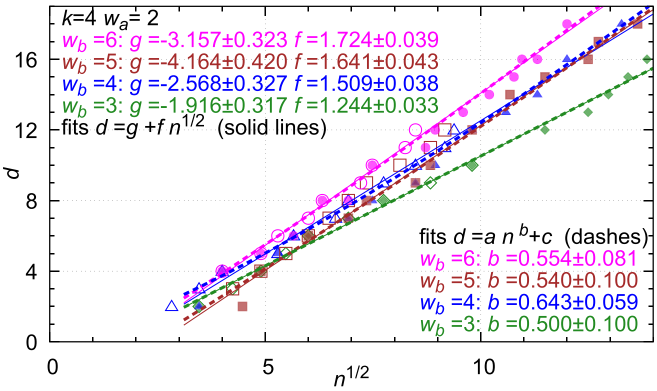

FIG. 2. As in Fig. 1 but for codes encoding $k = 4$ qubits. In agreement with the results in Sec. IV G, there are no connected codes with $k > 2$ and $W_a = W_b = 2$.

(v)]. After constructing the matrices, we also made sure to drop all disconnected codes.

We note that for *even-even* codes, with both W_a and W_b even, rows and columns of the matrices (36) have even numbers of elements. For the binary field $\mathbb{F}_2$, this guarantees that the rows of the matrices A, B, and thus of the stabilizer generator matrices H_X, H_Z add to zero; Eq. (9) guarantees that we get nontrivial codes with $k \geqslant 2$. In comparison, with one or both weights odd, there are many trivial codes with $k = 0$.

The computed distances d for codes with $W_a = 2$ are plotted as a function of the square root of the block size n in Figs. 1 and 2 for codes with $k = 2$ and 4, respectively. Different symbols and colors correspond to row weights $W \in \{4, 5, 6, 7, 8\}$ as indicated in the caption of Fig. 1, with open and closed symbols corresponding to codes obtained from Abelian and non-Abelian groups, respectively. Figures 3 and 4 give similar data for codes with $W_a = 3$ and W_b as indicated, and Fig. 5 shows distances for small-k codes with $W_a = W_b = 4$. These plots all look similar to a family of GB codes with $k = 2$ studied in Ref. [19]. Namely, the available largest distances show reasonable agreement with asymptotic distance scaling $d = g + f n^{1/2}$, with the slope $f \equiv f(W_a, W_b)$ an increasing function of the total row weight $W = W_a + W_b$, while different

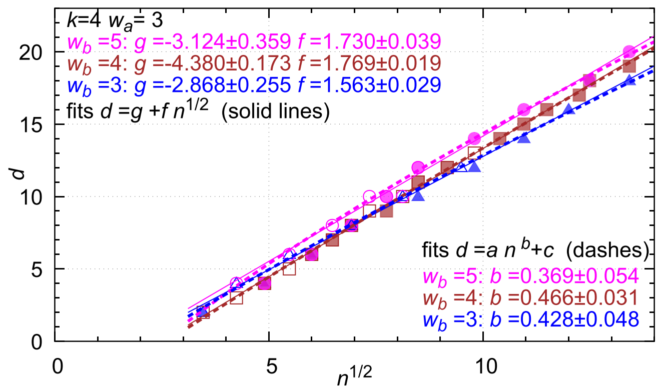

FIG. 4. As in Fig. 3 but for 2BGA codes encoding $k = 4$ qubits.

values of $W_a \geqslant 2$ and $W_b \geqslant W_a$ have a relatively minor effect on the coefficients g and f.

Square-root scaling of the distance is in agreement with the lower bound in Statement 10 and, in particular, with the case $G_a \cap G_b = \{1\}$, where 2BGA codes can be represented as hypergraph-product codes constructed from a pair of classical group-algebra codes. To compare, we also tried fitting the distances with $d = an^b + c$, where a, b, and c are parameters. While an upward or downward curvature corresponding to exponent $b > \frac{1}{2}$ or $b < \frac{1}{2}$, respectively, can be seen on some of the fits, the actual deviations from the linear (in $n^{1/2}$) fits are small, $\Delta d \lesssim 0.2$ on most plots. We conclude that 2BGA codes with dimensions $k \leqslant 4$, row weights $W \leqslant 8$, and group sizes studied so far are not nearly large enough to resolve the question about the scaling of the code distances of such codes with the block size.

While constructed 2BGA codes with $k > 4$ also have maximum distances d scaling near linearly with $n^{1/2}$, the corresponding coefficients show relatively little dependence on k (data not shown). For this reason, and to reveal the patterns in code parameters, in Figs. 6 and 7, we plot the distances d of the found 2BGA codes with $k \geqslant 4$ as a function of n, for codes with $W_a = 2$ and $W_b = 6$ obtained from Abelian and non-Abelian groups, respectively. Most prominent in Fig. 6 are the sequences of codes with $kd = n$ with $k \geqslant 6$ and the distances $d = \{2, 3, \ldots, d_{\max}(k, n)\}$, where the sequence cut-

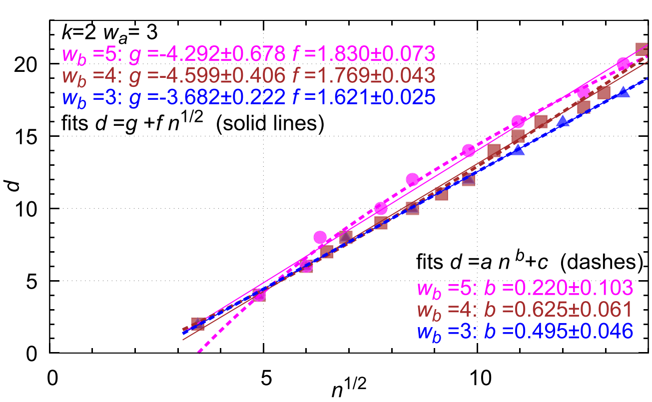

FIG. 3. As in Fig. 1 but for 2BGA codes with weights $W_a = 3$ and W_b as indicated. We have not found any Abelian-group codes with these weights and $k = 2$.

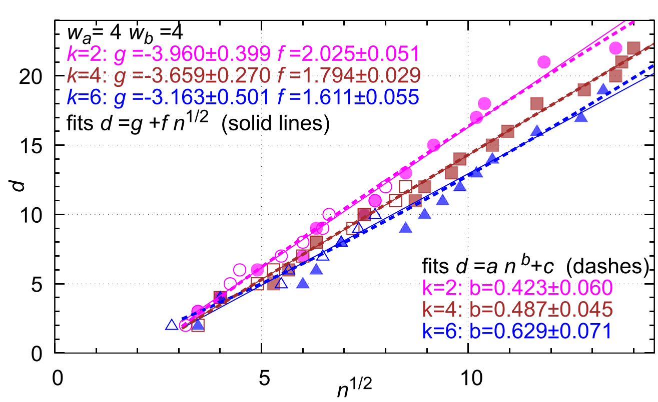

FIG. 5. As in Fig. 1 but for 2BGA codes with weights $W_a = W_b = 4$ and encoding k qubits as indicated. Circles ○, squares □, and triangles △, respectively, correspond to $k = 2$, 4, and 6.

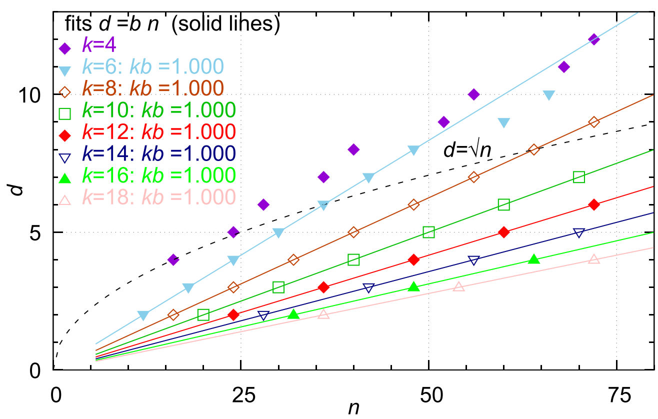

FIG. 6. Distances d of Abelian connected 2BGA codes with $W_a = 2$, $W_b = 6$, and $k \geqslant 4$, plotted as a function of the block length n. Different symbols correspond to actual codes found, with k values as indicated in the caption. Solid lines are fits to $d = bn$ using only the data on or below the black dashed line, $d = n^{1/2}$. Parameters of most of the codes with $k \geqslant 6$ satisfy the relation $kd = n$ exactly. This can be seen from the values of the product kb shown in the caption; the sequences terminate at $d = O(n^{1/2})$ more or less independent of the value of k. All the codes fitting this pattern can be obtained from the groups $C_{mh} = C_m \times C_2$, $m \geqslant 3$, of order $\ell = 2m$, producing index-4 qQC CSS codes of length $n = 4m$.

off $d_{\max}(k, n) = O(n^{1/2})$ shows relatively little dependence on k. Codes with $W_a = 2$, $W_b = 6$ obtained from non-Abelian groups (Fig. 7) also have sequences with $kd = n$, but only for $k = 6$ or doubly even $k \in \{4, 8, 12, 16, \ldots\}$; there are also sequences of codes with $k = 4s + 2$, $s \geqslant 2$, whose parameters satisfy the relation $(k + 2)d = n$. As we demonstrate in Appendix C, codes with the same parameters as the codes found in the sequences with $kd = n$ can be obtained starting with groups C_{mh} and D_m, both of which give index-4 qQC codes of length $n = 4m$.

Figure 8 shows the same data as Fig. 7 but with kd plotted as a function of n. It demonstrates that for all constructed codes with $W_a = 2$ we have $kd \leqslant n$. By this measure, the best among codes with $W_a = 2$ are index-4 qQC codes from groups C_{mh} and D_m with $kd = n$. We should note that, according to Example 12 in Ref. [45], sufficiently long codes with $kd = n$ can be obtained as additive cyclic codeword-stabilized (CWS) codes [46–48] from a set of k classical repetition codes, although such codes do not necessarily have bounded stabilizer weights. Of course, asymptotically the ratio kd/n increases without a bound for many families of quantum LDPC codes, e.g., as $O(n^{1/2})$ for hypergraph-product codes [13]. However, it is not trivial to get $kd > n$ in a degenerate quantum code of length $n \lesssim 10^2$. Some of such 2BGA codes constructed in this work are listed in Table I.

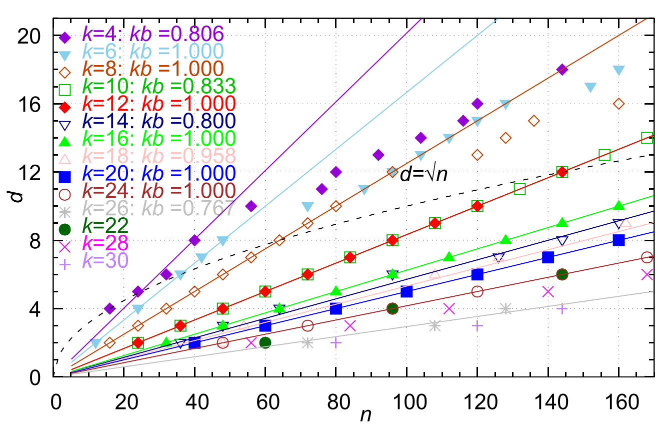

FIG. 7. As in Fig. 6 but for connected 2BGA codes with $W_a = 2$, $W_b = 6$, and $k \geqslant 4$ even, obtained from non-Abelian groups. As can be seen from Table III in Appendix C, sequences of codes with $kd = n$ and doubly even $k = 4s$, $s \geqslant 1$, can be obtained from the groups D_m which give index-4 qQC codes of length $n = 4m$; the sequences terminate at $d = O(n^{1/2})$.

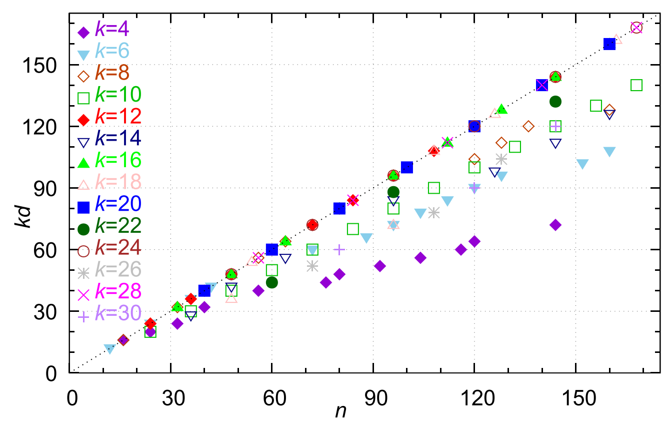

FIG. 8. Same data as in Fig. 7, but with the products kd plotted as a function of n. The dotted line is the diagonal, $kd = n$; all of the found codes with $W_a = 2$ and $W_b = 6$ have $kd \leqslant n$.

Most of the constructed 2BGA codes with $W_a = W_b = 4$ do not have simple relations between their parameters, and the plots of d vs n are not illuminating. For this reason, we decided to illustrate the parameters of such codes with $k \geqslant 4$ by plotting kd vs n, for Abelian codes in Fig. 9 and for non-Abelian codes in Fig. 10. Only codes with even values of k are shown. As evident from the plots, many of the constructed codes have $kd > n$, including the Abelian code [[64,18,8]] with $kd/n > 2$ obtained from the group $C_4 \times C_4 \times C_2$.

VI. CONCLUSIONS

In conclusion, we introduced and studied analytically and numerically a family of quantum 2BGA codes, an ansatz particularly suitable for constructing short- and intermediate-length quantum LDPC codes. Indeed, unlike for many of the "product" constructions [2–5,13] which tend to give very long quantum codes, the block length of a 2BGA code is twice the size of the group used in the construction. Further, unlike for quantum group algebra codes in Ref. [49] which are analogs of quantum cyclic codes, here the CSS orthogonality constraint is naturally satisfied for any pair of group algebra elements.

Moreover, the 2BGA codes are a generalization of GB codes from cyclic to more general groups, and share many of the nice properties of the GB codes. In particular, we show that 2BGA codes include as a special case quantum hypergraph-product codes constructed from classical left (right) group algebra codes, which guarantees the existence of finite-rate 2BGA codes with $d = O(n^{1/2})$.

TABLE I. Parameters of degenerate connected 2BGA codes with $n < 10^2$, $kd \geqslant n$, and $d > W$. Only codes with the largest examined row weight $W = 8$ have been found with such parameters. Here ℓ is the group order, "#" is the group number specific to GAP, n, k, d are parameters of the code LP$[a, b]$ with a and b as indicated, "presentation" is the shortest group presentation, and "structure" is the output of a function call "`StructureDescription(SmallGroup(ℓ,#));`" in GAP, with C_m an order-m cyclic group, S_3 the order-6 symmetric group, "$\times$" the direct product of groups, and "$\ltimes$" the semidirect product, with the normal subgroup on the left. The four row blocks, respectively, list codes with $W_a = 2$, $W_b = 6$, first Abelian then non-Abelian, followed by codes with $W_a = W_b = 4$, first Abelian then non-Abelian. The terms in group algebra elements a and b are sorted according to the internal presentation in GAP.

ℓ	#	n	k	d	a	b	Presentation	Structure
36	2	72	8	9	$1+r^{28}$	$1+r^9+r^{18}+r^{12}+r^{29}+r^{14}$	$\langle r\vert r^{36}\rangle$	C_{36}
36	1	72	8	9	$1+r$	$1+s+r^6+s^3r+sr^7+s^3r^5$	$\langle r,s\vert s^4,r^6,s^{-1}rsr\rangle$	$C_9\ltimes C_4$
40	1	80	8	10	$1+sr^4$	$1+r+r^2+s+s^3r+s^2r^6$	$\langle r,s\vert s^5,r^8,r^{-1}srs\rangle$	$C_5\ltimes C_8$
48	10	96	8	12	$1+sr^2$	$1+r+s^3+s^4+s^2r^5+s^4r^6$	$\langle r,s\vert s^6,r^8,(rs)^8\rangle$	$(C_3\ltimes C_8)\ltimes C_2$
27	1	54	6	9	$1+r+r^3+r^7$	$1+r+r^{12}+r^{19}$	$\langle r\vert r^{27}\rangle$	C_{27}
30	4	60	6	10	$1+r^{10}+r^6+r^{13}$	$1+r^{25}+r^{16}+r^{12}$	$\langle r\vert r^{30}\rangle$	C_{30}
35	1	70	8	10	$1+r^{15}+r^{16}+r^{18}$	$1+r+r^{24}+r^{27}$	$\langle r\vert r^{35}\rangle$	C_{35}
36	2	72	8	10	$1+r^9+r^{28}+r^{31}$	$1+r+r^{21}+r^{34}$	$\langle r\vert r^{36}\rangle$	C_{36}
36	2	72	10	9	$1+r^9+r^{28}+r^{13}$	$1+r+r^3+r^{22}$	$\langle r\vert r^{36}\rangle$	C_{36}
36	1	72	8	9	$1+s+r+sr^6$	$1+s^2r+s^2r^6+r^2$	$\langle r,s\vert s^4,r^9,s^{-1}rsr\rangle$	$C_9\ltimes C_4$
40	1	80	8	10	$1+r+s+s^3r^5$	$1+r^2+sr^4+s^3r^2$	$\langle r,s\vert s^5,r^8,s^{-1}rsr\rangle$	$C_5\ltimes C_8$
48	1	96	8	12	$1+r+s+r^{14}$	$1+r^2+sr^4+r^{11}$	$\langle r,s\vert s^3,r^{16},r^{-1}srs\rangle$	$C_3\ltimes C_{16}$
40	8	80	9	9	$1+sr^5+r^5+sr^6$	$1+s^2+r+s^2r^3$	$\langle r,s\vert s^4,r^{10},(rs)^2\rangle$	$(C_{10}\times C_2)\ltimes C_2$
42	3	82	10	9	$1+r^7+r^8+sr^{10}$	$1+s+r^5+s^2r^{13}$	$\langle r,s\vert s^3,r^{14},r^{-1}srs\rangle$	$C_7\times S_3$
48	13	96	10	12	$1+s+r^9+sr$	$1+s^2r^9+r^7+r^2$	$\langle r,s\vert s^4,r^{12},s^{-1}rsr\rangle$	$C_{12}\ltimes C_4$
48	5	96	11	9	$1+s+r^9+sr^{13}$	$1+r^9+sr^{18}+r^7$	$\langle r,s\vert s^2,r^{24},(rs)^8\rangle$	$C_{24}\ltimes C_2$
48	9	96	12	10	$1+r+s^3r^2+s^2r^3$	$1+r+s^4r^6+s^5r^3$	$\langle r,s\vert s^6,r^8,r^{-1}srs\rangle$	$C_2\times(C_3\ltimes C_8)$

Although we have not been able to give explicit expressions for the parameters of 2BGA codes, we constructed a number of equalities and inequalities relating the parameters to those of other classical and quantum codes. From the practical point of view, most important results are the code equivalence relations in Theorem 1, and the analysis of block structure of 2BGA codes in Sec. IV C.

We used these symmetries to enumerate the inequivalent parameters of binary (designed for qubits) 2BGA codes with stabilizer generator weights $W \leqslant 8$ for all Abelian groups of ranks $\ell \leqslant 50$ and non-Abelian groups of ranks $\ell \leqslant 100$. Although the sample is too small to identify the asymptotic form of the distance scaling, some of the constructed codes have parameters substantially better than those of GB codes of similar size. Some of the constructed codes with row weights $W = 8$, distances $d \geqslant 8$, and dimensions $k \geqslant 8$ have $kd > n$, a condition difficult to reach for a short quantum LDPC code. These codes with larger k have many redundant minimum-weight stabilizer generators and are expected to perform well in a fault-tolerant setting as data-syndrome codes [50–53].

The 2BGA codes based on non-Abelian groups have a bigger set of possible parameters than the Abelian 2BGA or GB codes; in particular, only the former codes may have a dimension k given by an odd number, and there are more short degenerate non-Abelian codes with large k (see Table I), especially for larger n. On the other hand, some of Abelian-group codes found have better parameters than any of the non-Abelian 2BGA codes with the same sizes, and the

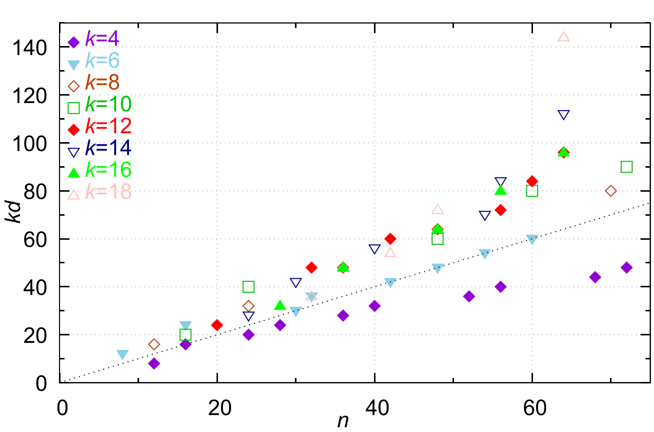

FIG. 9. As on Fig. 8 but for Abelian connected 2BGA codes with $W_a = W_b = 4$ and $k \geqslant 4$.

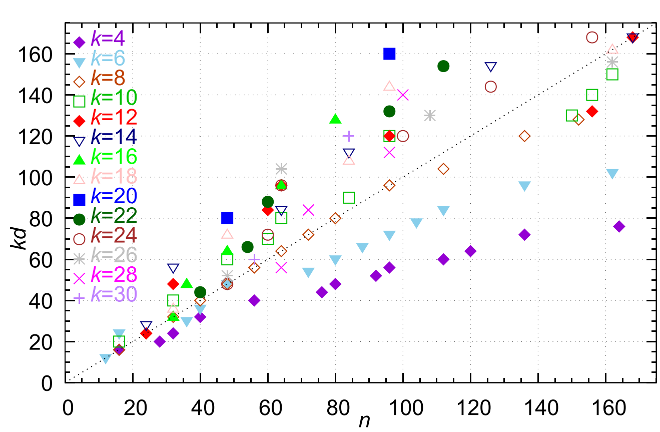

FIG. 10. As on Fig. 9 but for codes with $W_a = W_b = 4$ and $k \geqslant 4$ even obtained from non-Abelian groups.

Abelian codes in Table I are all obtained from cyclic groups (and thus are GB codes). Thus, at least for group sizes studied here, there is no clear advantage of Abelian vs non-Abelian 2BGA codes. Definitely, GB codes and Abelian 2BGA codes, because of the simpler structure, are much more convenient to use.

Note added. Recently, Bravyi *et al.* posted a related papeer [54] describing quasicyclic codes equivalent to 2BGA codes over two-generator Abelian groups. Specifically, the authors constructed several CSS codes with stabilizer generator weight $W = 6$ and high encoding rates, suggested a feasible implementation of these codes in a two-layer planar geometry, constructed near-optimal syndrome measurement circuits, and demonstrated fault-tolerant quasithresholds close to 0.8%. This is close to a threshold of around 1% for the surface code under depolarizing noise, despite a significant increase in the encoding rate.

ACKNOWLEDGMENTS

We are grateful to P. Panteleev for enlightening comments on an early version of this work. This work was supported in part by the APS M. Hildred Blewett Fellowship (H.K.L.) and the NSF Division of Physics via the Grant No. 2112848 (L.P.P.).

APPENDIX A: DETAILED PROOFS FOR SEC. III

1. Proof of Statement 1

Proof. It is enough to prove the statement for $E \equiv E_A$; the statement for F_A is obtained by a similar argument (or by a transposition).

First, any idempotent matrix $E = E^2 \in M_\ell(F)$ is diagonalizable by a change of basis since its minimal polynomial $\mu_E(x) = x(1-x)$ factors into distinct linear terms. Let $E_A = U^{-1}DU$, $U \in M_\ell(F)$ an invertible matrix, and D a diagonal (0,1) matrix with a block of $r \equiv \operatorname{rank} E_A = \operatorname{rank} A$ ones in the top left corner. Use U to transform each square matrix, $A' = UAU^{-1}$, $B' = UBU^{-1}$, and $E'_A = D$. Such an invertible transformation preserves both ranks and commutativity, thus, B' must be block diagonal, with two square blocks of size r and $\ell - r$, and ranks $\operatorname{rank} E_A B$ and $\operatorname{rank}(I - E_A)B$, respectively. Similarly, since $DA' = A'$ and their ranks coincide, the matrix A' has only the first rank -A rows nonzero and linearly independent. This gives that the rank of the product $B'A'$ coincides with that of the first block of B', i.e., $\operatorname{rank} BA = \operatorname{rank} E_A B$, giving $\delta_X = 0$. ■

2. Proof of statement 2

Proof. Using the definitions in Eq. (26), write

$$SE_ABS^{-1} = F_A^T B^T = (BF_A)^T.$$

The ranks on the left-hand side and on the right-hand side are $p_\star + \delta_X$ and $p_\star + \delta_Z$, respectively, which gives $\delta_X = \delta_Z$. ■

3. Proof of Statement 3

Proof. To be specific, we only consider $\mu = L$; the case $\mu = R$ is similar. The proof amounts to a demonstration that the set contributing to the distance (15) for each subsequent code is a subset of the previous one. (a) The additional row block in matrix $H_X^{(L)}$ (compared to H_X) guarantees that any Z-like codeword in Q'_L is also a Z-like codeword in LP[a, b], but not necessarily the other way. (b) Any nontrivial Z codeword $\boldsymbol{u}$ in Q''_L is also a nontrivial codeword $\binom{\boldsymbol{u}}{\boldsymbol{0}}$ in Q'_L. (c) Any nonzero codeword $\boldsymbol{u} \in C_L$ is a Z codeword in Q''_L, with an extra row block in H_L fully suppressing the degeneracy. The condition $E_B\boldsymbol{u} = 0$ guarantees that $\boldsymbol{u} \neq 0$ cannot be set to zero by adding linear combinations of the rows of $(H_Z)_L$. ■

4. Proof of statement 4

Proof. Indeed, since A is block diagonal with the maximum block size m, we can choose a set of basis vectors $\mathcal{U} \equiv \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots\}$ of the code $C_A^\perp$ so that the support of each vector fits entirely in a single block, which implies $\operatorname{wgt}(\boldsymbol{u}_j) \leqslant m$. By the condition, this code contains a nonzero vector $\boldsymbol{u}$ linearly independent from the columns of B. Linear independence can be also written as $(I - E_B)\boldsymbol{u} \neq 0$ [see Eq. (19)]. Since $\boldsymbol{u}$ is a linear combination of the basis vectors in $\mathcal{U}$, at least one of these satisfies the equation $(I - E_B)\boldsymbol{u}_j \neq 0$, which gives the upper bound in question $d_Z(A, B^T) \leqslant \operatorname{wgt} \boldsymbol{u}_j \leqslant m$. ■

5. Proof of statement 5

The proof is based on the following lemma (note that the formulation in the original paper [17] is missing a condition; this was corrected in the Erratum).

Lemma 1 (Z-puncturing bound [17]). Consider a stabilizer code $Q = \mathrm{CSS}(H_X, H_Z)$ with the parameters $[[n, k, (d_X, d_Z)]]_q$ and a qudit index set $\mathcal{V} = [n]$. Given a partition into complementary sets $\mathcal{I} \subset \mathcal{V}$ and $\mathcal{J} = \mathcal{V} \setminus \mathcal{I}$, suppose a logical generator matrix L_X can be chosen so that none of its k rows is supported both in $\mathcal{I}$ and in $\mathcal{J}$. Let $Q' = \mathrm{CSS}\left((H_X)_\mathcal{I}, H_Z[\mathcal{I}]\right)$ and $Q'' = \mathrm{CSS}\left((H_X)_\mathcal{J}, H_Z[\mathcal{J}]\right)$ be the codes whose X-generator matrices are shortened and Z-generator matrices punctured to $\mathcal{I}$ and $\mathcal{J}$, respectively. Then the Z distances of the three codes satisfy the inequality $d_Z \geqslant \min(d'_Z, d''_Z)$.

Proof of Statement 5. We construct the lower bound for Z codewords; CSS symmetry combined with the block permutation symmetry gives the other bound. The proof amounts to a demonstration that the condition of the Z-puncturing bound lemma applies, which relates d_Z to the Z distances of the gauge-fixed codes (32), which are known to have the same Z distances as the corresponding single-block erasure codes [see Eq. (15)]. Indeed, with $\delta_X = \delta_Z = 0$, the total number of independent codewords in the original code matches the sum of those for the two Z-punctured codes. Thus, we just need to show that any nontrivial Z codeword in one of the Z-punctured codes can be padded with zeros to become a nontrivial codeword of the original code, and independent from the codewords coming from the other punctured code. To this end, take $\boldsymbol{u} \in F^\ell$ a nontrivial Z codeword from the left Z-punctured code,

$$A\boldsymbol{u} = 0, \quad \boldsymbol{u} + B\boldsymbol{w} \neq 0 \quad \forall\, \boldsymbol{w} \in F^\ell. \tag{A1}$$

Immediately, the pair $\boldsymbol{c}_Z \equiv \binom{\boldsymbol{u}}{\boldsymbol{0}}$ is a Z-like codeword in the original two-block code and, from the second part of Eq. (A1), the top component remains nonzero when arbitrary linear combinations of rows of H_Z are added. Thus, $\boldsymbol{c}_Z$ is a nontrivial Z codeword, and it is not degenerate to any codeword coming from the other punctured code. This argument is repeated identically for the second code in Eq. (32), up to an interchange of the A and B matrices. ■

6. Proof of Eq. (34)

Proof. Without limiting generality, take $\mu = L$. We are going to show that the set of nontrivial Z codewords of the original two-block code Q is split without an intersection between those of the codes $Q_1 \equiv \mathrm{CSS}(H_X^{(L)}, H_Z)$ and $Q_2 \equiv \mathrm{CSS}(H_X, H_Z^{(L)})$.

Indeed, a nontrivial Z codeword in Q_1 or Q_2 is also a nontrivial codeword in Q, and a nontrivial codeword in Q is necessarily a codeword in Q_2 (possibly trivial). Second, the ranks of the extended matrices $H_X^{(L)}$ and $H_Z^{(L)}$ both equal to ℓ; the two codes have dimensions $k_1 = k_S + \delta_Z$ and $k_2 = k_S + \delta_X$, adding up to the dimension (25) of the code Q.

Third, consider a nontrivial codeword $\boldsymbol{c}_Z \equiv \binom{\boldsymbol{u}}{\boldsymbol{v}}$ in Q. Suppose it also happens to be a (necessarily nontrivial) Z codeword in Q_1, i.e., $(1 - E_A)\boldsymbol{v} = 0$. This implies $\boldsymbol{v} = A\boldsymbol{s}$, for some $\boldsymbol{s} \in F^{\ell}$, which, in turn, gives $\boldsymbol{u} = B\boldsymbol{s} + (I - F_A)\boldsymbol{w}$, a trivial codeword in Q_2. On the other hand, c_Z is necessarily a codeword in Q_2, and any linear combination of the columns of $H_Z^{(L)}$ cannot modify the value of $(1 - E_A)\boldsymbol{v}$. That is, when this value is nonzero (i.e., $\boldsymbol{c}_Z \notin Q_1$), $\boldsymbol{c}_Z$ is a nondegenerate codeword in Q_2. This completes the dichotomy and the proof. ■

APPENDIX B: DETAILED PROOFS FOR SEC. IV

Proof of Theorem 1. (i) A group automorphism is a permutation of group elements preserving the action of group operation $\varphi(a)\varphi(b) = \varphi(ab)$, $a, b \in G$. Further, for any size-ℓ permutation matrix S we can write, for $H_X = (A, B)$,

$$SH_X\begin{pmatrix}\boldsymbol{u}\\ \boldsymbol{v}\end{pmatrix} = (SAS^{-1}, SBS^{-1})\begin{pmatrix}S\boldsymbol{u}\\ S\boldsymbol{v}\end{pmatrix},$$

and similarly for $H_Z = (B^T, -A^T)$. Using $S^T = S^{-1}$, it is easy to verify that scalar products and, in particular, the row orthogonality (8), are preserved by this transformation. (ii) This follows from the proof of (i) if we choose the permutation matrix $S = \mathrm{L}(\alpha^{-1})\,\mathrm{R}(\beta)$ and remember that L and R matrices commute. (iii) This is proved similarly, by rescaling block components of $\boldsymbol{c}_Z$, $\boldsymbol{u} \to x^{-1}\boldsymbol{u}$, $\boldsymbol{v} \to y^{-1}\boldsymbol{v}$, and doing a similar weight-preserving transformation of $\boldsymbol{c}_X$. (iv) This also is a consequence of commutativity of left and right matrices. Indeed, if we denote $L \equiv \mathrm{L}(\alpha)$ and $R \equiv \mathrm{R}(\beta)$, it is easy to verify that the modified block matrices in Eq. (16) are $A' = AL$, $B' = BR$, so that components of a $\boldsymbol{c}_Z$ vector are transformed as $\boldsymbol{u} \to L^T\boldsymbol{u}$, $\boldsymbol{v} \to R^T\boldsymbol{v}$, and an identical transformation for the components of a $\boldsymbol{c}_X$ vector, $\boldsymbol{u}_X \to L^T\boldsymbol{u}_X$, $\boldsymbol{v} \to R^T\boldsymbol{v}$. This obviously preserves the scalar products between X and Z codewords, and we only need to verify

$$\begin{aligned}H_Z'\boldsymbol{c}_X' &= (R^TB^T, -L^TA^T)\begin{pmatrix}L^T\boldsymbol{u}_X\\ R^T\boldsymbol{v}_X\end{pmatrix}\\ &= R^TL^T(B^T, -A^T)\begin{pmatrix}\boldsymbol{u}_X\\ \boldsymbol{v}_X\end{pmatrix} = 0.\end{aligned}$$

(v) The proof is also similar to (i), except we use the symmetric permutation matrix $S = P = P^T$ from Eq. (37) and, in addition, interchange the blocks $\boldsymbol{u}_\mu' = P\boldsymbol{v}_\mu$, $\boldsymbol{v}_\mu' = \pm P\boldsymbol{u}_\mu$, $\mu \in \{X, Y\}$. (vi) After a permutation of the blocks, this is an immediate consequence of Eq. (38). The second form follows from (iii) and (v). ■

1. Proof of Statement 6

Proof. The equivalence of the two codes is evident from Theorem 1(ii). With Eqs. (39) and (40), the corresponding transformation for a pair of group algebra elements is $[u, v] \to [u, vx^{-1}]$; in particular, the row x goes to 1. Finally, this invertible map sends the original double coset G_axG_b to $G_axG_bx^{-1} = G_a1G_{xbx^{-1}}$. ■

2. Proof of Statement 7

Proof. The subgroup N being normal both in G_a and G_b guarantees that we can decompose $G_a = H_a \rtimes N$ and $G_b = N \ltimes H_b$ as semidirect products [41], where $H_a = G_a/N$ and $H_b = N\backslash G_b$ are sets of cosets. The semidirect product, e.g., with the normal group on the right, is defined as a group with elements from the set of all pairs $H_a \rtimes N = \{(h, \gamma)|h \in H_a, \gamma \in N\}$ and the group product

$$(h_1, \gamma_1)(h_1, \gamma_2) \equiv \big(h_1h_2, h_2^{-1}\gamma_1h_2\,\gamma_2\big).$$

Similarly, any element of the double coset G_a1G_b can be written as a triplet (α, γ, β), with $\alpha \in G_a$, $\gamma \in N$ and $\beta \in G_b$, with all triplets in the form $(\alpha x, x^{-1}\gamma y^{-1}, y\beta)$, $x, y \in N$ united into product-preserving equivalence classes. The group product is defined as

$$(\alpha_1, \gamma_1, \beta_1)(\alpha_2, \gamma_2, \beta_2) = \big(\alpha_1\alpha_2, \alpha_2^{-1}\gamma_1\alpha_2\,\beta_1\gamma_2\beta_1^{-1}, \beta_1\beta_2\big),$$

where the elements from H_a and H_b are forced to commute, and the Abelian property of N is used to ensure the consistency of the definition. It is easy to verify the group axioms: thus defined product is associative, the identity element is the equivalence class of (1,1,1), and the inverse of (α, γ, β) is $(\alpha^{-1}, \alpha\beta^{-1}\gamma^{-1}\beta\alpha^{-1}, \beta^{-1})$, which is both a left and a right inverse. Finally, this map also gives a natural map for the group algebra elements a and b, with the multiplication by an element of G_a from the left or an element of G_b from the right giving the expected results. ■

3. Proof of statement 8

Proof of statement 8. As discussed in the previous section, the square matrices of 2BGA codes under consideration here have the form of Kronecker products $A = A_1 \otimes I_{m_b}$, $B = I_{m_a} \times B_1$, where m_a and m_b are indices of the support groups in G, with $\ell = m_am_bc$ and $c \equiv |N|$. Further, A_1 and B_1 have square blocks of size c which can be readily seen to have the form of group algebra matrices $\mathrm{L}_N(x_{ij}) = \mathrm{R}_N(x_{ij})$ and $x_{ij} \in F[N]$. That is, the original 2BGA code is an Abelian LP code, which can also be seen as an HP code over the ring $R = F[N]$. As explained in the Appendix of Ref. [3], any such code can be decomposed further as a direct sum of HP codes over cyclic rings $F[C_{\ell_i}]$, $1 \leqslant i \leqslant s$, where the groups C_{ℓ_i} are those in the decomposition of finite Abelian group $N = C_{\ell_1} \times C_{\ell_2} \times \cdots \times C_{\ell_s}$ into a direct product of cyclic groups. Each of these HP codes can be also seen as an F-linear quasicyclic LP code, and as a special case of a hyperbicycle code [14]. Importantly, at each step, we can reconstruct matrices over the original field F as block-diagonal matrices, with the blocks given by the corresponding matrices of the quasicyclic codes in the decomposition; these transformations preserve the total matrix rank and the dimension k of the original code.

The final step of the proof is to use Smith normal form (SNF) decomposition over the polynomial ring $F[x]$ to show that a quasicyclic LP code can be further decomposed as a direct sum of GB codes (see Lemma 2) below. Since matrix ranks are additive, and rank defects vanish for GB codes, this proves $\delta_X = \delta_Z = 0$ for 2BGA codes under consideration, and also for all quasi-Abelian LP codes. ∎

Lemma 2 (Decomposition of a quasicyclic LP code). Given $R \equiv F[x]/(x^\ell - 1)$, a ring of modular polynomials isomorphic to circulant matrices over the finite field F, let A and B be arbitrary matrices over R. The code $\mathrm{LP}[A, B]$ is isomorphic a direct sum of GB codes.

As a reminder, the quasicyclic LP code [3,20] is constructed by replacing matrix elements of the associated HP code over R, polynomials $h(x) \in R$, with the cyclic permutation matrices $h(P)$ [see Eq. (43)]. The transformation in the proof below is done with the help of SNF decomposition. In general, this requires a nontrivial basis change. That is, only the dimensions of the corresponding spaces are preserved, but not the code distances.

Proof of Lemma 2. Denote the dimensions of matrices A and B, respectively, as $r_A \times n_A$ and $r_B \times n_B$. Then the associated HP code over R has CSS generators

$$H_X = (A \otimes I_B, I_A \otimes B), \quad H_Z^T = \begin{pmatrix} I_A' \otimes B \\ -A \otimes I_B' \end{pmatrix}, \tag{B1}$$

where I_A, I_B, I_A', and I_B', respectively, are identity matrices of dimensions r_A, r_B, n_A, and n_B. The matrix elements of the original matrices A and B are polynomials from R. Considering the polynomials as elements of $F[x]$, a principal ideal domain, SNF of such matrices can be readily constructed using elementary row and column transformations, e.g., $A = U_A D_A V_A$, where U_A and V_A are square matrices of size r_A and n_A with unit determinants, respectively, and $D_A = \operatorname{diag}(a_1(x), a_2(x), \ldots)$, where $a_j(x)$ along the diagonal are *SNF invariants*, with each subsequent polynomial divided by the previous one, $a_j(x) \mid a_{j+1}(x)$, $0 < j < \min(r_a, n_a)$. The SNF over $F[x]/(x^\ell - 1)$ is obtained by taking these matrices modulo $x^\ell - 1$ elementwise. This preserves the unit determinants of the matrices U_A and V_A, i.e., these matrices remain invertible. Denoting the SNF invariants of the matrix B as $b_j(x)$, $0 < j \leqslant \min(r_B, n_B)$, it is easy to see that the invertible matrices can be factored out in the CSS generator matrices (B1), e.g.,

$$\begin{aligned} &(U_A D_A V_A \otimes I_B, I_A \otimes U_B D_B V_B) \\ &= (U_A \otimes U_B)\,(D_A \otimes I_B, I_A \otimes D_B) \begin{pmatrix} V_A \otimes U_B^{-1} & \\ & U_A^{-1} \otimes V_B \end{pmatrix}, \end{aligned}$$

which preserves the orthogonality between the rows of the transformed matrices H_X' and H_Z'. Evidently, the transformed matrices are constructed similarly to Eq. (B1), but from the diagonal matrices D_A and D_B, so that each row contains just two polynomials, e.g., the row $i + (j-1)r_A$ of H_X has $a_i(x)$ in the first block and $b_j(x)$ in the second. This gives a block-diagonal form of the original HP code, with individual blocks forming the codes $\mathrm{GB}[a_i(x), b_j(x)]$ constructed from all pairwise combinations of SNF invariants of the original matrices A and B. In particular, this gives the dimension of the original quasicyclic LP code as

$$k = 2 \sum_{i=1}^{\min(r_A, n_A)} \sum_{j=1}^{\min(r_B, n_B)} \gcd\,(a_i(x), b_j(x), x^\ell - 1). \tag{B2}$$

Unlike the corresponding expressions in Appendix B of Ref. [3], this formula does not require that the group algebra $F[C_\ell]$ be semisimple. ∎

4. Proof of Statement 9

Proof. The result follows from Statement 1. Indeed, semisimple ideals aR and Ra are summands in R, and can be generated by idempotents e_a and f_a, respectively, such that $a = e_a a = a f_a$. The conditions of Statement 1 are satisfied by taking $E_A = \mathrm{L}(e_a)$ and $F_A = \mathrm{L}(f_a)$ which necessarily commute with $B = \mathrm{R}(b)$. ∎

5. Proof of Statement 10

The proof is based on the following.

Lemma 3 (Trivial quasi-Abelian LP codes). Given an Abelian group N and a finite field F, consider the Abelian group algebra $R \equiv F[N]$. Let A and B be matrices with elements in R such that the classical codes $C_A^\perp$ and $C_B^\perp$ both have zero dimensions. Then the quasi-Abelian code $\mathrm{LP}[A, B]$ is trivial, $\dim \mathrm{LP}[A, B] = 0$.

Proof. This result is proved similarly to Statement 8. Namely, we start from the decomposition of the LP code as a direct sum of quasicyclic LP codes (see Appendix B in Ref. [3]), combined with the decomposition in Lemma 2. With both $C_A^\perp$ and $C_B^\perp$ trivial, the SNF invariants of both matrices must all be unit. As a result, every GB code in the decomposition of Lemma 2 is trivial, which gives the result immediately.

Alternatively, we can say that all-unit SNF invariants of A and B imply that these matrices have well-defined ranks over R, and follow the conventional rank-based derivation for the dimension of HP code [13]. It gives zero when both matrices have full row ranks. ∎

Proof of Statement 10. The proof goes along the lines of that for the lower bound on the distance of conventional HP codes [13]; it is based on Lemma 3. In this proof, matrices over R are labeled by capital letters in the usual math italic font, while the corresponding matrices over F are labeled in bold italic, e.g, A with matrix elements $a_{ij} \in R$ and $\boldsymbol{A}$ formed by blocks $\mathrm{L}_N(a_{ij}) = \mathrm{R}_N(a_{ij})$. We also denote $\ell_a \equiv [G_a : N]$ and $\ell_b \equiv [G_b : N]$ the indices of the intersection group N in the two support subgroups, so that $\ell = c\ell_a\ell_b$.

The 2BGA code $\mathrm{LP}[a, b]$ is a two-block code constructed from matrices $\boldsymbol{A} = \boldsymbol{A}_1 \otimes \boldsymbol{I}_{\ell_b}$ and $\boldsymbol{B} = \boldsymbol{I}_{\ell_a} \otimes \boldsymbol{B}_1$, where $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$, respectively, are block matrices equivalent to $A_1 \in M_{\ell_a}[R]$ and $B_1 \in M_{\ell_b}[R]$. Thus, the original code is equivalent to the R-linear code $\mathrm{HP}[A_1, B_1]$, and it is this equivalence that is used to construct the lower distance bound.

TABLE II. Largest-distance 2BGA codes from Abelian groups $C_{mh} = C_m \times C_2$, with k a factor of $n = 4m$ and $W_a = 2$, $W_b = 6$. The group generators are x and s, with $x^m = 1$, $s^2 = 1$, and $xs = sx$. The distances which *fail* to satisfy the condition $kd = n$ are given in bold.

m	ℓ	n	k	d	a	b
4	8	16	2	**4**	$1+x$	$1+x+s+x^2+sx+sx^3$
			4	4	$1+x$	$1+x+s+x^2+sx+x^3$
			8	2	$1+s$	$1+x+s+x^2+sx+sx^2$
6	12	24	4	**5**	$1+x$	$1+x^3+s+x^4+x^2+sx$
			12	2	$1+x^3$	$1+x^3+s+x^4+sx^3+x$
8	16	32	8	4	$1+x^6$	$1+sx^7+sx^4+x^6+sx^5+sx^2$
			16	2	$1+sx^4$	$1+sx^7+sx^4+x^6+x^3+sx^2$
10	20	40	4	**8**	$1+x$	$1+x^5+x^6+sx^6+x^7+sx^3$
			8	5	$1+x^6$	$1+x^5+s+x^6+x+sx^2$
			20	2	$1+x^5$	$1+x^5+s+x^6+sx^5+x$
12	24	48	8	6	$1+sx^{10}$	$1+x^3+sx^6+x^4+x^7+x^8$
			12	4	$1+x^3$	$1+x^3+sx^6+x^4+sx^9+x^7$
			16	3	$1+x^4$	$1+x^3+sx^6+x^4+x^7+sx^{10}$
			24	2	$1+sx^6$	$1+x^3+sx^6+x^4+sx^9+sx^{10}$
14	28	56	4	**10**	$1+x$	$1+x^7+sx^8+x^2+x^3+sx^{11}$
			8	7	$1+x^8$	$1+x^7+s+x^8+x^9+sx^4$
			28	2	$1+x^7$	$1+x^7+s+x^8+sx^7+x$

Given a vector $\boldsymbol{e} \in F^{2\ell}$ orthogonal to the rows of the generator matrix $\boldsymbol{H}_X$ of the 2BGA code LP$[a, b]$ equivalent to HP$[A_1, B_1]$, we construct sets $\mathcal{I}_A \subset [\ell_a]$ and $\mathcal{I}_B \subset [\ell_b]$ indexing only the columns of the matrices A_1 and B_1 incident on nonzero elements of $\boldsymbol{e}$ in the product $\boldsymbol{H}_X\,\boldsymbol{e} = 0$, the sets $\mathcal{I}'_A$ and $\mathcal{I}'_B$ labeling all columns in the corresponding blocks of $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$, and the set $\mathcal{I} = \mathcal{I}'_A \times [\ell_b] \bigsqcup [\ell_a] \times \mathcal{I}'_B$ labeling all such columns in $\boldsymbol{H}_X$, a disjoint union of the corresponding sets in the left and in the right blocks. Each element of R corresponds to a block of size $c \equiv |N|$ in matrices $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$, thus,

$$|\mathcal{I}'_\mu| = c\,|\mathcal{I}_\mu| \leqslant c\,\mathrm{wgt}\,(\boldsymbol{e}), \quad \mu \in \{A, B\}.$$

Denote $\boldsymbol{H}'_X$, $\boldsymbol{H}'_Z$ the CSS generator matrices of the LP code constructed from punctured matrices $A_1[\mathcal{I}_A]$ and $B_1[\mathcal{I}_B]$. By construction, the shortened vector $\boldsymbol{e}[\mathcal{I}]$ is a Z-like codeword in the modified LP code, $\boldsymbol{H}'_X\,\boldsymbol{e}[\mathcal{I}] = 0$. On the other hand, if $|\mathcal{I}'_A| < d_A^\perp$ and $|\mathcal{I}'_B| < d_B^\perp$, the modified LP code must be trivial by Lemma 3, i.e., $\boldsymbol{e}[\mathcal{I}]$ can only be a trivial codeword, and thus a linear combination of the rows of $\boldsymbol{H}'_Z$. These latter rows can be constructed by shortening a subset of the rows of the original matrix $\boldsymbol{H}_X$ (where we drop only positions equal to zero in each row of the subset), thus, the full vector $\boldsymbol{e}$ is a linear combination of the rows of the original matrix $\boldsymbol{H}_Z$. The inequality on the subset sizes is satisfied whenever $c\,\mathrm{wgt}\,(\boldsymbol{e}) < \min(d_A^\perp, d_B^\perp)$, which proves that the distance of the original LP code satisfies $d_Z \geqslant \min(d_A^\perp, d_B^\perp)/c$, and, since d_Z is an integer, $d_Z \geqslant d_0$ as stated. ■

6. Proof of Statement 11

Proof. If the code $C_A^\perp \cap C_J$ is trivial, its distance is infinite, and the upper bound in question is definitely satisfied. Assuming otherwise, take any nonzero vector $\boldsymbol{u} \in C_A^\perp \cap C_J$; the corresponding pair $\binom{\boldsymbol{u}}{\boldsymbol{0}}$ is clearly a Z codeword in the 2BGA code, and we just need to verify that it is not degenerate to a zero vector.

The minimum-weight elements in $C_A^\perp$ are associated with a single block of $A \equiv \mathrm{L}(a)$, e.g., the terms in Eq. (45) with $\beta = 1$, the element of $F[G]$ corresponding to $\boldsymbol{u}$ has the form $u =$

TABLE III. As in Table II but for non-Abelian dihedral groups $D_m = \langle r, s | r^m = s^2 = (rs)^2 = 1\rangle$, with k a factor of $n = 4m$. Parameters of all codes listed satisfy the condition $kd = n$.

m	ℓ	n	k	d	a	b
6	12	24	8	3	$1+r^4$	$1+sr^4+r^3+r^4+sr^2+r$
			12	2	$1+r^3$	$1+sr+r^3+r^4+sr^4+r$
8	16	32	8	4	$1+r^2$	$1+sr^5+sr^4+r^2+sr^7+sr^6$
			16	2	$1+r^4$	$1+sr^3+sr^6+r^4+sr^7+sr^2$
9	18	36	12	3	$1+r^3$	$1+s+r+r^3+sr^3+r^4$
10	20	40	8	5	$1+r^2$	$1+sr^4+r^5+r^2+sr^6+r$
			20	2	$1+r^5$	$1+sr^2+r^5+r^6+sr^7+r$
12	24	48	8	6	$1+r^{10}$	$1+sr^8+r^9+r^4+sr^2+r^5$
			12	4	$1+r^3$	$1+sr^7+r^3+r^4+sr^{10}+r^7$
			16	3	$1+r^8$	$1+sr^8+r^9+r^8+sr^4+r^5$
			24	2	$1+r^6$	$1+sr^{11}+r^6+sr^5+r+r^7$
14	28	56	8	7	$1+r^4$	$1+sr^{11}+r^7+sr^5+r^{12}+r^9$
			28	2	$1+r^7$	$1+sr^2+r^7+r^8+sr^9+r$
15	30	60	12	5	$1+r^{12}$	$1+sr^{14}+r^5+r^{12}+sr^{11}+r^{14}$
			20	3	$1+r^5$	$1+sr^{13}+r^5+r^{12}+sr^3+r^2$
16	32	64	8	8	$1+r^6$	$1+sr^{12}+sr^9+r^6+s+sr$
			16	4	$1+r^4$	$1+sr^{10}+sr^3+r^4+sr^{14}+sr^7$
			32	2	$1+r^8$	$1+sr^{11}+sr^{12}+r^8+sr^3+sr^4$

$\sum_{\alpha\in\mathcal{A}} \alpha\, u_\alpha$; intersection with C_J ensures that all $u_\alpha \in \mathcal{I}$. The code $C_{B^T}^\perp \cap \widehat{C}_J$ contains vectors $\boldsymbol{z} \equiv P\boldsymbol{y}$, such that $\boldsymbol{y} \in C_J$ and $B^T \boldsymbol{z} = 0$, where $B \equiv \mathrm{R}(b)$ and P is the permutation matrix in Eq. (37). Rewrite the condition $B^T\boldsymbol{z} = 0$ in terms of the group algebra element associated with $\boldsymbol{y}$; with the help of Eq. (37) it reads as

$$0 = \mathrm{R}(b)^T P\, \mathrm{L}(y) = P\, \mathrm{L}(b)\, \mathrm{L}(y) = P\, \mathrm{L}(by),$$

or simply $by = 0$. Again, block structure of B and group symmetry guarantees that we can choose y in the form $y = \sum_{\beta\in\mathcal{B}} y_\beta \beta$. By construction, $y_\alpha \in J$, a maximal ideal, which ensures that $uy = \sum_\alpha \sum_\beta \alpha u_\alpha y_\beta \beta \neq 0$, and thus for any $w \in F[G]$, $(u - wb)y = uy \neq 0$, which guarantees that the pair $\binom{u}{0}$ be a nondegenerate Z codeword in $\mathrm{LP}[a, b]$. ■

APPENDIX C: ADDITIONAL EXAMPLES

Table II gives explicitly the group algebra elements for constructing Abelian 2BGA codes from the sequences $kd = n$. Namely, for a given group $C_{mh} = C_m \times C_2 = \langle x, s | x^m = s^2 = xsx^{-1}s^{-1} = 1\rangle$, $m \geqslant 1$, only the maximum-distance codes with $k/2$ a factor of n are shown. With polynomial decomposition $a = a_0(x) + sa_1(x)$ and $b = b_0(x) = sb_1(x)$, these codes can be also seen as index-4 qQC two-block codes constructed from the circulant matrices

$$A = \begin{pmatrix} a_0(x) & a_1(x) \\ a_1(x) & a_0(x) \end{pmatrix}, \quad B = \begin{pmatrix} b_0(x) & b_1(x) \\ b_1(x) & b_0(x) \end{pmatrix}.$$

Table III gives explicitly the group algebra elements for constructing non-Abelian 2BGA codes with $kd = n$. All codes are constructed from the groups $D_m = C_m \ltimes C_2 = \langle r, s | r^m = s^2 = (rs)^2 = 1\rangle$, $m \geqslant 1$. With polynomial decomposition $a = a_0(r) + sa_1(r)$ and $b = b_0(r) + sb_1(r)$, these codes can be also seen as index-4 qQC two-block codes constructed from circulant matrices

$$A = \begin{pmatrix} a_0(x) & \overline{a_1(x)} \\ a_1(x) & \overline{a_0(x)} \end{pmatrix}, \quad B = \begin{pmatrix} b_0(x) & \overline{b_1(x)} \\ b_1(x) & \overline{b_0(x)} \end{pmatrix},$$

where $\overline{a_0(r)} = a_0(r^{-1}) \equiv sa_0(r)s$ is the reverse of the polynomial $a_0(r)$.

[1] S. Evra, T. Kaufman, and G. Zémor, Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders, *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2020), pp. 218–227.

[2] M. B. Hastings, J. Haah, and R. O'Donnell, Fiber bundle codes: Breaking the $N^{1/2}$ polylog(N) barrier for quantum LDPC codes, in *STOC 2021: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing* (Association for Computing Machinery, New York, 2021), p. 1276–1288.

[3] P. Panteleev and G. Kalachev, Quantum LDPC codes with almost linear minimum distance, IEEE Trans. Inf. Theory **68**, 213 (2022).

[4] N. P. Breuckmann and J. N. Eberhardt, Balanced product quantum codes, IEEE Trans. Inf. Theory **67**, 6653 (2021).

[5] P. Panteleev and G. Kalachev, Asymptotically good quantum and locally testable classical LDPC codes, arXiv:2111.03654.

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

[7] A. A. Kovalev and L. P. Pryadko, Fault tolerance of quantum low-density parity check codes with sublinear distance scaling, Phys. Rev. A **87**, 020304(R) (2013).

[8] I. Dumer, A. A. Kovalev, and L. P. Pryadko, Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes, Phys. Rev. Lett. **115**, 050502 (2015).

[9] R. G. Gallager, *Low-Density Parity-Check Codes* (M.I.T. Press, Cambridge, MA, 1963).

[10] S.-Y. Chung, G. D. Forney Jr, T. J. Richardson, and R. Urbanke, On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit, IEEE Commun. Lett. **5**, 58 (2001).

[11] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. **303**, 2 (2003).

[12] M. H. Freedman, D. A. Meyer, and F. Luo, Z_2-systolic freedom and quantum codes, in *Computational Mathematics* (CRC Press, Boca Raton, FL, 2002), pp. 287–320.

[13] J.-P. Tillich and G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, NJ, 2009), pp. 799–803.

[14] A. A. Kovalev and L. P. Pryadko, Quantum Kronecker sum-product low-density parity-check codes with finite rate, Phys. Rev. A **88**, 012311 (2013).

[15] L. Guth and A. Lubotzky, Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds, J. Math. Phys. **55**, 082202 (2014).

[16] W. Zeng and L. P. Pryadko, Higher-dimensional quantum hypergraph-product codes with finite rates, Phys. Rev. Lett. **122**, 230501 (2019).

[17] W. Zeng and L. P. Pryadko, Minimal distances for certain quantum product codes and tensor products of chain complexes, Phys. Rev. A **102**, 062402 (2020). Erratum: Minimal distances for certain quantum product codes and tensor products of chain complexes [Phys. Rev. A 102, 062402 (2020)], **104**, 029902(E) (2021).

[18] T. Kaufman and R. J. Tessler, New cosystolic expanders from tensors imply explicit quantum LDPC codes with $\Omega(\sqrt{n}\log^k n)$ distance, in *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing* (Association for Computing Machinery, New York, 2021), p. 1317–1329.

[19] R. Wang and L. P. Pryadko, Distance bounds for generalized bicycle codes, Symmetry **14**, 1348 (2022).

[20] P. Panteleev and G. Kalachev, Degenerate quantum LDPC codes with good finite length performance, Quantum **5**, 585 (2021).

[21] M. Hagiwara and H. Imai, Quantum quasi-cyclic LDPC codes, in *2007 IEEE International Symposium on Information Theory* (IEEE, Piscataway, NJ, 2007), pp. 806–810.

[22] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, Quantum error correction beyond the bounded distance decoding limit, IEEE Trans. Inf. Theory **58**, 1223 (2012).
[23] C. Galindo, F. Hernando, and R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields and Their Applications **52**, 261 (2018).
[24] N. Raveendran and B. Vasić, Trapping sets of quantum ldpc codes, Quantum **5**, 562 (2021).
[25] S. Bravyi and B. Terhal, A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes, New J. Phys. **11**, 043029 (2009); S. Bravyi, D. Poulin, and B. Terhal, Tradeoffs for reliable quantum information storage in 2D systems, Phys. Rev. Lett. **104**, 050503 (2010).
[26] R. Wang, H.-K. Lin, and L. P. Pryadko, Abelian and nonabelian quantum two-block codes, arXiv:2305.06890.
[27] G. V. Kalachev and P. A. Panteleev, On the minimum distance in one class of quantum LDPC codes, Intelligent systems. Theory Applicat. **24**, 87 (2020) (in Russian).
[28] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1981).
[29] C. Polcino Milies, Group algebras and coding theory: a short survey, Revista Integración **37**, 153 (2019).
[30] R. A. Ferraz, C. P. Milies, and E. Taufer, Left ideals of matrix rings and error-correcting code, AAECC **32**, 311 (2021).
[31] Y. A. Drozd and V. V. Kirichenko, *Finite Dimensional Algebras* (Springer, Berlin, 1994).
[32] M. Borello, J. De La Cruz, and W. Willems, On checkable codes in group algebras, J. Algebra Applicat. **21**, 2250125 (2022).
[33] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A **54**, 1098 (1996). A. M. Steane, Simple quantum error-correcting codes, *ibid.* **54**, 4741 (1996).
[34] Galois-qudit code, The Error Correction Zoo (V. V. Albert & P. Faist, eds.), 2022, https://errorcorrectionzoo.org/c/galois_into_galois.
[35] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inf. Theory **52**, 4892 (2006).
[36] D. Poulin, Stabilizer formalism for operator quantum error correction, Phys. Rev. Lett. **95**, 230504 (2005).
[37] D. Bacon, Operator quantum error-correcting subsystems for self-correcting quantum memories, Phys. Rev. A **73**, 012340 (2006).
[38] C. D. Meyer, Generalized inverses of block triangular matrices, SIAM J. Appl. Math. **19**, 741 (1970).
[39] C. D. Meyer, Generalized inverses and ranks of block matrices, SIAM J. Appl. Math. **25**, 597 (1973).
[40] I. G. Connell, On the group ring, Can. J. Math. **15**, 650 (1963).
[41] H. Bechtell, *The Theory of Groups* (Addison-Wesley, 1971).
[42] GAP, GAP (Groups, Algorithms, and Programming), a System for Computational Discrete Algebra, The GAP Group.
[43] L. P. Pryadko, V. A. Shabashov, and V. K. Kozin, QDistRnd: A GAP package for computing the distance of quantum error-correcting codes, J. Open Source Software **7**, 4120 (2022).
[44] H.-K. Lin and L. P. Pryadko, Collection of codes constructed for "Quantum two-block group algebra codes", `GitHub` repository, https://github.com/QEC-pages/2BGA-codes.
[45] A. A. Kovalev, I. Dumer, and L. P. Pryadko, Design of additive quantum codes via the code-word-stabilized framework, Phys. Rev. A **84**, 062319 (2011).
[46] I. L. Chuang, A. W. Cross, G. Smith, J. A. Smolin, and B. Zeng, Codeword stabilized quantum codes: Algorithm and structure, J. Math. Phys. **50**, 042109 (2009).
[47] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, Codeword stabilized quantum codes, IEEE Trans. Inf. Theory **55**, 433 (2009).
[48] X. Chen, B. Zeng, and I. L. Chuang, Nonbinary codeword-stabilized quantum codes, Phys. Rev. A **78**, 062315 (2008).
[49] A. Naghipour, M. A. Jafarizadeh, and S. Shahmorad, Quantum stabilizer codes from abelian and non-abelian groups association schemes, Int. J. Quantum Inf. **13**, 1550021 (2015).
[50] Y. Fujiwara, Ability of stabilizer quantum error correction to protect itself from its own imperfection, Phys. Rev. A **90**, 062304 (2014).
[51] A. Ashikhmin, C. Y. Lai, and T. A. Brun, Robust quantum error syndrome extraction by classical coding, in *2014 IEEE International Symposium on Information Theory* (IEEE, Piscataway, NJ, 2014), pp. 546–550.
[52] A. Ashikhmin, C. Y. Lai, and T. A. Brun, Correction of data and syndrome errors by stabilizer codes, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, NJ, 2016), pp. 2274–2278.
[53] W. Zeng, A. Ashikhmin, M. Woolls, and L. P. Pryadko, Quantum convolutional data-syndrome codes, in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)* (IEEE, Piscataway, NJ, 2019), pp. 1–5.
[54] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, High-threshold and low-overhead fault-tolerant quantum memory, arXiv:2308.07915.