Abelian and non-abelian quantum two-block codes

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

2023 12th International Symposium on Topics in Coding (ISTC) | 979-8-3503-2611-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISTC57237.2023.10273492

***Abstract*—We discuss quantum two-block codes, a large class of CSS codes constructed from two commuting square matrices. Interesting families of such codes are generalized-bicycle (GB) codes and two-block group-algebra (2BGA) codes, where a cyclic group is replaced with an arbitrary finite group, generally non-abelian. We present code construction and give several expressions for code dimension, applicable depending on whether the constituent group is cyclic, abelian, or non-abelian. This gives a simple criterion for an essentially non-abelian 2BGA code guaranteed not to be permutation-equivalent to such a code based on an abelian group. We also give a lower bound on the distance which, in particular, applies to the case when a 2BGA code reduces to a hypergraph-product code constructed from a pair of classical group codes.**

***Index Terms*—CSS codes, QECC, quantum LDPC codes, group algebra codes, group codes, two-block codes, 2BGA codes, GB codes, generalized bicycle codes**

I. Introduction

Generally, any family of quantum low-density parity-check (LDPC) codes with stabilizer generators of bounded weight and distance scaling logarithmically or faster with the block length has a finite fault-tolerant threshold to scalable error correction [1]–[4]. Recently, there was a significant progress in constructing such codes [5]–[11]. Unfortunately, many of the proposed "product" constructions, e.g., in Refs. [8]–[15], tend to give rather long codes, and the existing lower bound for the generator weight to give asymptotically good quantum LDPC codes with finite rates and linear distance scaling is also very large [11].

In comparison, much shorter quantum codes, including quantum LDPC codes with bounded generator weights, can be constructed with a two-block anzats [16], a construction based on a pair of square commuting matrices. It gives a family of Calderbank-Shor-Steane (CSS) codes [17], [18] with relatively small block lengths, twice the size of the original matrices. The commutativity can be achieved, e.g., by taking a pair of circulant matrices, which gives generalized bicycle (GB) codes [5], [16], [19], [20], or using an arbitrary finite abelian group instead of the cyclic group [21]. An important advantage of two-block quantum LDPC codes is an overcomplete set of minimum-weight stabilizer generators which may improve their performance in the fault-tolerant setting. Finally, GB and more general two-block codes include certain families of hypergraph-product (HP) codes [12] as a subclass, which guarantees the existence of finite-rate codes with $\mathcal{O}(\sqrt{n})$ distance scaling in this family, but they also include codes with linear distances [20]. In comparison, the distance of an HP code with the block length n cannot exceed $\sqrt{n}$.

In this paper we discuss general quantum two-block codes. We introduce a family of *two-block group algebra* (2BGA) codes based on an arbitrary finite group, abelian or non-abelian. Just like GB codes can be seen as CSS codes constructed from a pair of index-two quasicyclic codes, 2BGA codes are the smallest lifted-product (LP) codes [9], [11].

We give a formal expression based on idempotent matrices for the dimension of general two-block codes. The dimension is necessarily even for such codes based on an abelian group algebra [21] (which includes GB codes), as well as for more general quantum two-block codes identified by certain additional commutativity conditions. We show that this constraint is automatically satisfied for 2BGA codes based on a semi-simple group algebra; the dimension of such codes is necessarily even. This gives a simple sufficient criterion for an essentially non-abelian 2BGA code which cannot be reduced to such a code based on an abelian group. We also discuss the distance of 2BGA codes and, for a family of such codes, give a lower bound in terms of distances of classical group algebra codes. In particular, this bound applies in the case where a group algebra code reduces to an HP code.

The structure of the rest of the paper is as follows. We introduce necessary notations in Section II. Our main results are given in Sec. III, followed by conclusions in Sec. IV.

II. Preliminaries

A classical code $\mathcal{C}$ linear over a finite field $F \equiv \mathbb{F}_q$, where $q > 1$ is a power of a prime p, the characteristic of the field, with parameters $[n, k, d]_q$, is a k dimensional vector space in F^n, the set of all length-n strings using elements of F as characters. Such a code can be specified in terms of a generator matrix G whose rows are vectors from $\mathcal{C}$ forming a complete basis, $\operatorname{rank} G = k$, or its parity-check matrix H whose rows are orthogonal to any vector in $\mathcal{C}$, with $\operatorname{rank} H = n - k$,

$$\mathcal{C} = \mathcal{C}_G \equiv \mathcal{C}_H^{\perp}, \quad GH^T = 0. \tag{1}$$

The codes $\mathcal{C}_G$ and $\mathcal{C}_H$ generated by rows of G and H, respectively, are called mutually dual. The *support* of a vector $\boldsymbol{x} \equiv (x_1, x_2, \ldots, x_n) \in F^n$ is the set of indices i corresponding to non-zero components $x_i \neq 0$, and its Hamming weight is the size of the support. The distance d of a linear code $\mathcal{C}$ is the smallest Hamming weight of a non-zero vector in $\mathcal{C}$; by convention, $d = \infty$ for a trivial code with $k = 0$.

A very important class of codes are *cyclic* linear codes [22], invariant under the group C_n of cyclic permutations. A generalization to an arbitrary group are *group codes*, or group algebra codes [23]–[26].

Given a finite field F and a finite group G, the group algebra $F[G]$ is the linear space of all formal sums

$$x \equiv \sum_{g\in G} x_g g, \quad x_g \in F, \tag{2}$$

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

$$ab = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g, \quad a, b \in F[G]. \tag{3}$$

Similar to cyclic codes, a left (right) group algebra code is isomorphic to a left (right) *ideal* J in $F[G]$, defined as a linear space such that for any $x \in J$ and any $r \in F[G]$, $rx \in J$ for the left ideal ($xr \in J$ for the right ideal).

The structure of ideals in $F[G]$ is particularly simple when characteristic of the field and the group size are mutually prime, $\gcd(p, |G|) = 1$. In this case, according to Maschke's theorem, the group algebra is semisimple, and any ideal is a principal ideal generated by an idempotent element, e.g., $J = e_J \cdot F[G]$ for a right ideal $J = J_R$, with an idempotent $e_J^2 = e_J \in J$ (see, e.g., Corollary 2.2.5 in Ref. [27]).

A quantum Calderbank-Shor-Steane (CSS) code [17], [18] $\mathcal{Q} \equiv \mathrm{CSS}(H_X, H_Z)$ can be defined as a direct sum of two quotient spaces, $\mathcal{Q} \cong \mathcal{Q}_X \oplus \mathcal{Q}_Z$,

$$\mathcal{Q}_X = \mathcal{C}_{H_Z}^{\perp}/\mathcal{C}_{H_X}, \quad \mathcal{Q}_Z = \mathcal{C}_{H_X}^{\perp}/\mathcal{C}_{H_Z}. \tag{4}$$

For example, elements of $\mathcal{Q}_X$ are equivalence classes of vectors in $\mathcal{C}_{H_Z}^{\perp}$, where two vectors are equivalent, $x \simeq y$, if they differ by an element of $\mathcal{C}_{H_X}$, $x - y \in \mathcal{C}_{H_X}$. Such a pair of equivalent vectors are called mutually *degenerate*, while any vector in the equivalence class of the zero vector is called *trivial*. The CSS *generator matrices* H_X and H_Z have equal number of columns, n, and orthogonal rows, $H_X H_Z^T = 0$. The parameters of the code (4) are denoted $[[n, k, d]]_q$, where

$$k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z \tag{5}$$

is the common dimension of the quotient spaces $\mathcal{Q}_X$ and $\mathcal{Q}_Z$, and $d \equiv \min(d_X, d_Z)$ is the minimum weight of any non-trivial vector in $\mathcal{Q}$, e.g.,

$$d_Z \equiv d(\mathcal{Q}_Z) = \min_{\boldsymbol{u}\in C_{H_X}^{\perp}\setminus C_{H_Z}} \mathrm{wgt}(\boldsymbol{u}). \tag{6}$$

Physically, a quantum code $\mathrm{CSS}(H_X, H_Z)$ operates in a Hilbert space $\mathcal{H}_q^{\otimes n}$ associated with n quantum-mechanical systems of dimension q each, Galois-qudits [28], and a well defined basis of X and Z operators acting in $\mathcal{H}_q^{\otimes n}$ [29]. Vectors of the codes $\mathcal{C}_{H_X}$ and $\mathcal{C}_{H_Z}$ correspond to X- and Z- operators in the stabilizer group whose generators 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 $H_X H_Z^T = 0$ ensures that the stabilizer group is abelian. Non-trivial vectors in $\mathcal{Q}_Z$ and $\mathcal{Q}_X$ correspond to Z and X logical operators, respectively. Codes with larger distances have logical operators which involve more qudits; such codes typically give better protection against errors.

III. Two-block codes

In this work we discuss two-block CSS codes with generator matrices in the form [16]

$$H_X = (A, B), \quad H_Z^T = \begin{pmatrix} B \\ -A \end{pmatrix}, \tag{7}$$

where A and B are square commuting $\ell \times \ell$ matrices with elements in F. The commutativity guarantees the CSS orthogonality condition, $H_X H_Z^T = 0$.

Code dimension: Given a square size-ℓ matrix A with elements in a finite field F, consider square idempotent matrices E_A and F_A of the same size and rank such that

$$E_A^2 = E_A, \quad F_A^2 = F_A, \quad E_A A = A F_A = A. \tag{8}$$

While these 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 and V_A are square invertible matrices, and $D_A = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0)$ has exactly $\operatorname{rank} A$ non-zero elements along the diagonal. Namely, we may choose

$$E_A \equiv U_A D_A U_A^{-1}, \quad F_A \equiv V_A^{-1} D_A V_A. \tag{9}$$

With idempotent matrices (8), it is easy to express the ranks of block matrices (7). Indeed, row and column transformations give (this is a simplified version of more general expressions in Refs. [30], [31])

$$\begin{aligned} \operatorname{rank} H_X &= \operatorname{rank} \begin{pmatrix} A & E_A B \\ 0 & (I - E_A)B \end{pmatrix} \\ &= \operatorname{rank}(A) + \operatorname{rank}(I - E_A)B, \end{aligned} \tag{10}$$

and a similar result for the rank of the other matrix,

$$\operatorname{rank} H_Z = \operatorname{rank} A + \operatorname{rank} B(I - F_A). \tag{11}$$

In general, $\operatorname{rank} H_Z \neq \operatorname{rank} H_X$. However, the equality can be achieved with some additional commutativity conditions. For example, if both E_A and F_A commute with B, the second terms in the r.h.s. of Eqs. (10) and (11) are both equal $\operatorname{rank} B - \operatorname{rank} AB$. This gives

Statement 1. *Suppose that idempotents E_A and F_A in Eq. (8) commute with B in Eq. (7). Then,*

$$\operatorname{rank} H_X = \operatorname{rank} H_Z, \quad \textit{and} \quad k = 2(\ell - \operatorname{rank} H_X). \tag{12}$$

Evidently, Eq. (12) also remains true after interchanging the blocks, e.g., if idempotents E_B and F_B commute with A.

In particular, the conditions of Statement 1 are satisfied if A has a square-free minimal polynomial. Indeed, in such a case A can be diagonalized, $A = S^{-1}\Lambda S$, where square matrix S over F is invertible, and the idempotents can be constructed as $E_A = F_A = S^{-1} D S$, with D a diagonal matrix with elements equal to zero or one according to whether the corresponding element of Λ is zero or not. It is easy to check that thus constructed $E_A = F_A$ necessarily commute with B if A does.

Construction from classical group algebra codes: To get a pair of commuting matrices, we use an ansatz introduced by Panteleev and Kalachev [9], [11]. Namely, given an element $x \in F[G]$ of the group algebra with the group size $\ell \equiv |G|$,

the $\ell \times \ell$ square matrices $\mathrm{L}(x)$ and $\mathrm{R}(x)$, respectively, are defined by the left and right action on group elements,

$$[\mathrm{L}(x)]_{\alpha,\beta} \equiv \sum_{g\in G} x_g \delta_{\alpha,g\beta}, \quad [\mathrm{R}(x)]_{\alpha,\beta} \equiv \sum_{g\in G} x_g \delta_{\alpha,\beta g}, \quad (13)$$

where group elements $\alpha, \beta \in G$ are used to index rows and columns, cf. Eq. (2), and $\delta_{\alpha,\beta} = 1$ if $\alpha = \beta$ and 0 otherwise is the Kronecker delta. Row and column weights of $\mathrm{L}(x)$ and $\mathrm{R}(x)$ are equal to $\mathrm{wgt}(x)$, the Hamming weight of the vector in F^ℓ with components x_α, $\alpha \in G$, which makes it easy to construct sparse matrices. Furthermore, 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 a left and a right matrices always commute,

$$\mathrm{L}(a)\,\mathrm{R}(b) = \mathrm{R}(b)\,\mathrm{L}(a). \quad (14)$$

With a group algebra element entirely supported on a subgroup, $x_g \neq 0$ only if $g \in K < G$, one can also form smaller matrices, e.g., $[\mathrm{L}_K(x)]_{\alpha,\beta}$ of size $|K| \times |K|$, with indices restricted to the same subgroup, $\alpha, \beta \in K$. If we introduce the *support group* [32]

$$G_x \equiv \langle \{g \in G : x_g \neq 0\} \rangle \quad (15)$$

generated by elements of G in the support of x, it is evident that matrices $\mathrm{L}(x)$ and $\mathrm{R}(x)$ are block-diagonal (up to a permutation), with square blocks of equal size $|G_x|$, corresponding to, respectively, right and left cosets of the support group G_x in G.

With these definitions, the *two-block group algebra* (2BGA) codes, the CSS codes (7) with $A \equiv \mathrm{L}(a)$ and $B \equiv \mathrm{R}(b)$ given by Eq. (13), are the smallest lifted-product codes [11] $\mathrm{LP}[a, b]$, where group algebra elements a, b are treated as 1×1 matrices over $F[G]$. Previously considered special cases are GB codes [5], [16], [20], with G a cyclic group, and *abelian* 2BGA codes [21], with G an abelian group.

The structure of matrices A and B is such that the row labeled by a group element $x \in G$ is associated, respectively, with the block supported in the right coset $G_a x$ and that in the left coset xG_b. When the product of the two support groups (the double coset associated with the group identity element $1 \in G$) does not contain all group elements, $G_a G_b \subsetneq G$, the code $\mathrm{LP}[a, b]$ is decomposed into smaller mutually disconnected subcodes associated with different double cosets in $G_a \backslash G / G_b$. The individual *double-coset* subcodes are not necessarily equivalent to each other; it is well known that even the sizes of double cosets may differ.

The case of GB codes [5], [16], [20] is recovered when G is a cyclic group,

$$C_\ell \equiv \langle x \rangle \equiv \{1, x, x^2, \ldots, x^{\ell-1}\}, \quad x^\ell = 1.$$

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 $\mathrm{LP}[a, b]$ is also a generalized-bicycle code $\mathrm{GB}[a(x), b(x)]$ specified by a pair of polynomials $a(x), b(x) \in F[x]/(x^\ell - 1)$, and the square blocks in Eq. (7) are just the circulant matrices $A = a(P)$ and $B = b(P)$, where

$$P = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} \quad (16)$$

is an $\ell \times \ell$ cyclic permutation matrix. A simple expression for the dimension of a code $\mathrm{GB}[a, b]$ was given in Ref. [5]. In this case $\mathrm{rank}\, H_X = \mathrm{rank}\, H_Z = \ell - \deg h(x)$, and

$$k = 2 \deg h(x), \quad h(x) \equiv \gcd\left(a(x), b(x), x^\ell - 1\right). \quad (17)$$

Evidently, Eq. (12) is satisfied, as it also does when the group G is abelian [21], or when one of the subgroups, G_a or G_b [see Eq. (15)], is cyclic. In the latter case the GB code is equivalent to a quasi-cyclic LP code [9].

More generally, consider *semi-abelian* 2BGA codes satisfying the conditions of Statement 1. Namely, take a code $\mathrm{LP}[a, b]$ where, e.g., $a \in F[G]$ is such that the corresponding right $a \cdot F[G]$ and left $F[G] \cdot a$ ideals are generated by idempotents e_a and f_a, $e_a a = a f_a = a$, and choose $E_A = \mathrm{L}(e_a)$ and $F_A = \mathrm{L}(f_a)$ to guarantee their commutativity with $B = \mathrm{R}(b)$. In particular, a semi-abelian 2BGA code is always obtained if the group algebra $F[G]$ is semisimple. Alternatively, we can select a so that the corresponding subgroup G_a in Eq. (15) has the order mutually prime with the field characteristic p, $\gcd(p, |G_a|) = 1$, so that only the subalgebra $F[G_a]$ be semisimple. Then, the idempotents $e_a \in F[G_a]$ and $f_a \in F[G_a]$ also generate the right and left ideals of a in $F[G]$, and, again, we can choose $E_A = \mathrm{L}(e_a)$ and $F_A = \mathrm{L}(f_a)$, so that the conditions of Statement 1 be satisfied.

To summarize, any abelian 2BGA code (including any GB code) or any semi-abelian 2BGA code, e.g., based on a semisimple group algebra, has an even dimension, see Eq. (12). Thus, any 2BGA code with an odd dimension k is *essentially non-abelian*, i.e., it is not permutation-equivalent to an abelian or a semi-abelian 2BGA code.

Example 2. *Consider the alternating group A_4, also known as the rotation group 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 an essentially non-abelian *2BGA code $\mathrm{LP}[a, b]$ with parameters $[[24, 5, 3]]_2$.*

Distances of GB codes: Several existence bounds for unrestricted GB codes (without the limit on row weight) are given in Ref. [20]. In particular, with $g(x) \equiv (x^\ell - 1)/h(x)$ irreducible, cf. Eq. (17), a counting argument in the style of Gilbert-Varshamov bound proves the existence of GB codes with $k = 2$ and linear distance scaling (Example 8 in Ref. [20]), and rate-1/4 GB codes with $d \geq \sqrt{\ell}$ related to quadratic-residue cyclic codes (Example 9 in Ref. [20]). This should be contrasted with, e.g., HP codes whose distances satisfy the upper bound $d < \sqrt{n}$.

In practice, we are more interested in quantum LDPC codes, with weight of stabilizer generators not exceeding some fixed w. Unfortunately, the regular structure of GB codes is a disadvantage in this case, as any such code is equivalent to a code local on a hypercubic lattice $\mathbb{Z}^D$, with $D \leq w-1$, or $D \leq w-2$ if ℓ is prime (Statement 13 from Ref. [20]). With general results from Refs. [33], [34], this gives upper bounds

$$d \leq \mathcal{O}(n^{1-1/D}) \text{ and } kd^{2/(D-1)} \leq \mathcal{O}(n). \tag{18}$$

Numerically, for a family of GB codes with $k=2$, the distance scaling is consistent with $d = A(w)n^{1/2} + B(w)$, with $A(w)$ an increasing function of w, although $d = \mathcal{O}(n^{\alpha})$ with some $\alpha = 1/2 + \epsilon$ with a small $\epsilon > 0$ cannot be excluded [20].

Lower distance bounds for 2BGA codes: Best known are the usual CSS bounds,

$$d_Z \geq d(C^{\perp}_{H_X}), \quad d_X \geq d(C^{\perp}_{H_Z}). \tag{19}$$

However, since the rows of H_X and H_Z are mutually orthogonal, we have, e.g., $d(C^{\perp}_{H_X}) \leq w_Z$, 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 (19) are not very useful.

Consider the special case of a 2BGA code $\mathrm{LP}[a,b]$, with $a, b \in F[G]$ such that the intersection subgroup $N \equiv G_a \cap G_b$ is central in G. In such a case, if we choose two transversal sets of coset representatives, $\mathcal{A}$ from G_a/N and $\mathcal{B}$ from G_b/N, any element of a double coset $G_a \backslash x / G_b$ can be written as $\alpha x \beta \gamma$, with $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$, and $\gamma \in N$. This gives matrices A and B with individual square blocks of size $c \equiv |N|$ given by, respectively, $\mathrm{L}_N(a_{\alpha,\alpha'})$ and $\mathrm{R}_N(b_{\beta,\beta'})$, with matrix elements $a_{\alpha,\alpha'}, b_{\beta,\beta'} \in N$ defined by the action of the two group algebra elements on the corresponding cosets, and indices $\alpha, \alpha' \in \mathcal{A}$ and $\beta, \beta' \in \mathcal{B}$. Explicitly, e.g., given the expansion (2) of $a \in F[G]$, $a_{\alpha',\alpha} = \sum_{\gamma \in N} a_{\alpha' \alpha^{-1} \gamma} \gamma$. This gives exactly the structure of a square-matrix *quasi-abelian* LP code [9] over the group algebra $F[N]$, and also the following lower bound:

Statement 3 (Version of Theorem 5 from Ref. [16])**.** *Given any two group algebra elements $a, b \in F[G]$ such that the intersection subgroup $N \equiv G_a \cap G_b$ of size $c \equiv |N|$ is central in G, consider classical codes with parity check matrices $A = \mathrm{L}(a)$ and $B = \mathrm{R}(b)$. Let $d_0 = \min\left\{d(C^{\perp}_A), d(C^{\perp}_B)\right\}$ be the minimum of their distances. Then, the distance d_Z of the 2BGA code $\mathrm{LP}[a,b]$ satisfies the inequality $d_Z \geq \lceil d_0/c \rceil$.*

In fact, this lower bound becomes exact when the intersection subgroup is trivial, $N = \{1\}$. In this case each double-coset subcode of the 2BGA code $\mathrm{LP}[a,b]$ is equivalent to a hypergraph-product code constructed from classical codes with parity-check matrices $\mathrm{L}_{G_a}(a)$ and $\mathrm{R}_{G_b}(b)$ over the corresponding subgroups, the individual blocks of $\mathrm{L}(a)$ and $\mathrm{R}(b)$.

It is known [26] that 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. Unfortunately, we do not have a matching upper bound for finite-rate 2BGA codes.

IV. Conclusions

In conclusion, we considered a family of quantum two-block codes, an ansatz particularly suitable for constructing short and intermediate-length quantum LDPC codes. This family includes previously studied GB codes and their generalization, 2BGA codes, which may be based on an abelian or a non-abelian group. Compared to "single-block" quantum cyclic codes [35]–[37] and a related construction based on a general finite group [38], the 2BGA codes have much more freedom: here the CSS orthogonality constraint is naturally satisfied for any pair of group algebra elements, and it is much easier to construct highly-degenerate quantum LDPC codes.

We constructed a general expression relating the dimension of a two-block code to those of single-block codes and, in the case of 2BGA code $\mathrm{LP}[a,b]$, identified the cases of abelian, semi-abelian, and non-abelian 2BGA codes, depending on the group G, the chosen group algebra elements $a, b \in F[G]$, and the associated support groups G_a and G_b. We also constructed a lower distance bound applicable when the subgroup $N \equiv G_a \cap G_b$ is central in G. The bound becomes exact when $N = \{1\}$, a trivial subgroup, in which case the 2BGA code is equivalent to an HP code constructed from a pair of group algebra codes.

Research in progress [39] includes enumeration of 2BGA codes with row weights $w \leq 8$ for all inequivalent small groups of size $\ell \leq 50$. Of particular interest are 2BGA codes with larger k which have many redundant minimum-weight stabilizer generators and are expected to perform well in a fault-tolerant setting as data-syndrome codes [40]–[43]. This could enable single-shot fault-tolerant quantum error correction [44], [45].

Acknowledgments

We are grateful to Pavel Panteleev for helpful comments on an early version of the manuscript. This work was supported in part by the APS M. Hildred Blewett Fellowship (HKL) and the NSF Division of Physics via the grant 2112848 (LPP).

References

[1] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *J. Math. Phys.*, vol. 43, p. 4452, 2002. [Online]. Available: http://dx.doi.org/10.1063/1.1499754

[2] A. A. Kovalev and L. P. Pryadko, "Fault tolerance of quantum low-density parity check codes with sublinear distance scaling," *Phys. Rev. A*, vol. 87, p. 020304(R), Feb 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.87.020304

[3] D. Gottesman, "Fault-tolerant quantum computation with constant overhead," *Quant. Information and Computation*, vol. 14, pp. 1338–1371, 2014. [Online]. Available: http://www.rintonpress.com/journals/qicabstracts/qicabstracts14-1516.html

[4] 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.*, vol. 115, p. 050502, Jul 2015. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.115.050502

[5] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," *Quantum*, vol. 5, p. 585, 2021.

[6] S. Evra, T. Kaufman, and G. Zémor, "Decodable quantum LDPC codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders," 2020, unpublished.

[7] T. Kaufman and R. J. Tessler, *New Cosystolic Expanders from Tensors Imply Explicit Quantum LDPC Codes with $\Omega(\sqrt{n}\log^k n)$ distance*. New York, NY, USA: Association for Computing Machinery, 2021, p. 1317–1329.

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

[9] P. Panteleev and G. Kalachev, "Quantum LDPC codes with almost linear minimum distance," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 213–229, 2022.

[10] N. P. Breuckmann and J. N. Eberhardt, "Balanced product quantum codes," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6653–6674, 2021.

[11] P. Panteleev and G. Kalachev, "Asymptotically good quantum and locally testable classical LDPC codes," 2021, [Unpublished]. [Online]. Available: http://arxiv.org/abs/2111.03654

[12] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, June 2009, pp. 799–803.

[13] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proc. of the 46th ACM Symposium on Theory of Computing (STOC 2014)*, 2014, pp. 273–282. [Online]. Available: https://arxiv.org/abs/1311.0885

[14] W. Zeng and L. P. Pryadko, "Higher-dimensional quantum hypergraph-product codes with finite rates," *Phys. Rev. Lett.*, vol. 122, p. 230501, Jun 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.122.230501

[15] ——, "Minimal distances for certain quantum product codes and tensor products of chain complexes," *Phys. Rev. A*, vol. 102, p. 062402, 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.102.062402

[16] A. A. Kovalev and L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate," *Phys. Rev. A*, vol. 88, p. 012311, 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.88.012311

[17] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug 1996.

[18] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, vol. 54, pp. 4741–4751, 1996. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.54.4741

[19] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Info. Th.*, vol. 59, pp. 2315–30, 2004. [Online]. Available: http://dx.doi.org/10.1109/TIT.2004.834737

[20] R. Wang and L. P. Pryadko, "Distance bounds for generalized bicycle codes," *Symmetry*, vol. 14, no. 7, p. 1348, 2022. [Online]. Available: https://www.mdpi.com/2073-8994/14/7/1348

[21] G. V. Kalachev and P. A. Panteleev, "On the minimum distance in one class of quantum LDPC codes," *Intelligent systems. Theory and applications*, vol. 24, p. 87–117, 2020, [In Russian]. [Online]. Available: http://mi.mathnet.ru/eng/ista284

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

[23] L. M. Bazzi and S. K. Mitter, "Some randomized code constructions from group actions," *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 3210–3219, 2006.

[24] G. Olteanu and I. Van Gelder, "Construction of minimal non-abelian left group codes," *Designs, Codes and Cryptography*, vol. 75, pp. 359–373, 2015. [Online]. Available: https://doi.org/10.1007/s10623-014-9922-z

[25] C. Polcino Milies, "Group algebras and coding theory: a short survey," *Revista Integración*, vol. 37, pp. 153–166, 2019. [Online]. Available: https://www.redalyc.org/articulo.oa?id=327062425008

[26] M. Borello, J. De La Cruz, and W. Willems, "On checkable codes in group algebras," *Journal of Algebra and Its Applications*, vol. 21, p. 2250125, 2022. [Online]. Available: https://doi.org/10.1142/S0219498822501250

[27] Y. A. Drozd and V. V. Kirichenko, *Finite Dimensional Algebras*. Springer-Verlag, 1994. [Online]. Available: https://doi.org/10.1007/978-3-642-76244-4

[28] "Galois-qudit code," in *The Error Correction Zoo*, V. V. Albert and P. Faist, Eds., 2022. [Online]. Available: https://errorcorrectionzoo.org/c/galois_into_galois

[29] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Info. Th.*, vol. 52, no. 11, pp. 4892–4914, Nov 2006.

[30] C. D. Meyer, "Generalized inverses of block triangular matrices," *SIAM Journal on Applied Mathematics*, vol. 19, no. 4, pp. 741–750, 1970. [Online]. Available: http://www.jstor.org/stable/2100157

[31] ——, "Generalized inverses and ranks of block matrices," *SIAM Journal on Applied Mathematics*, vol. 25, pp. 597–602, 1973. [Online]. Available: http://www.jstor.org/stable/2100027

[32] I. G. Connell, "On the group ring," *Canadian Journal of Mathematics*, vol. 15, p. 650–685, 1963.

[33] S. Bravyi and B. Terhal, "A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes," *New Journal of Physics*, vol. 11, no. 4, p. 043029, 2009. [Online]. Available: http://stacks.iop.org/1367-2630/11/i=4/a=043029

[34] S. Bravyi, D. Poulin, and B. Terhal, "Tradeoffs for reliable quantum information storage in 2D systems," *Phys. Rev. Lett.*, vol. 104, p. 050503, Feb 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.104.050503

[35] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Info. Theory*, vol. 44, pp. 1369–1387, 1998. [Online]. Available: http://dx.doi.org/10.1109/18.681315

[36] A. Thangaraj and S. W. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1176–1178, 2001.

[37] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.

[38] A. Naghipour, M. A. Jafarizadeh, and S. Shahmorad, "Quantum stabilizer codes from abelian and non-abelian groups association schemes," *International Journal of Quantum Information*, vol. 13, p. 1550021, 2015. [Online]. Available: https://doi.org/10.1142/S0219749915500215

[39] H.-K. Lin and L. P. Pryadko, "Quantum two-block group algebra codes," 2023, unpublished. [Online]. Available: https://arxiv.org/abs/2306.16400

[40] Y. Fujiwara, "Ability of stabilizer quantum error correction to protect itself from its own imperfection," *Phys. Rev. A*, vol. 90, p. 062304, Dec 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.90.062304

[41] 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*, 2014, pp. 546–550.

[42] ——, "Correction of data and syndrome errors by stabilizer codes," in *2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 2274–2278.

[43] 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)*, 2019, pp. 1–5.

[44] H. Bombín, "Single-shot fault-tolerant quantum error correction," *Phys. Rev. X*, vol. 5, p. 031043, Sep 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.5.031043

[45] E. T. Campbell, "A theory of single-shot error correction for adversarial noise," *Quantum Science and Technology*, vol. 4, p. 025006, 2019. [Online]. Available: https://doi.org/10.1088/2058-9565/aafc8f