

Generalized Bicycle Codes with Low Connectivity: Minimum Distance Bounds and Hook Errors

Reza Dastbasteh,^{1,*} Olatz Sanz Larrarte,¹ Arun John Moncy,^{1,2} Pedro M. Crespo,¹ Josu Etxezarreta Martinez,^{1,†} and Ruben M. Otxoa³

¹*Department of Basic Sciences, Tecnun - University of Navarra, San Sebastian, Spain.*

²*Donostia International Physics Center, San Sebastian, Spain.*

³*Hitachi Cambridge Laboratory, J. J. Thomson Avenue, Cambridge, United Kingdom.*

We present new upper and lower bounds on the minimum distance of certain generalized bicycle (GB) codes beyond the reach of techniques for classical codes capable of even capturing the true minimum distance for some cases. These bounds are then applied to illustrate the existence and analyze two highly degenerate GB code families with parameters $[[d^2 + 1, 2, d]]$ for odd $d \geq 3$ and $[[d^2, 2, d]]$ for even $d \geq 4$, both having the property that each check qubit is connected to exactly four data qubits similar to surface codes. For the odd-distance family, we analyze the structure of low-weight logical Pauli operators and demonstrate the existence of a fault-tolerant logical CNOT gate between the two logical qubits, achievable through a simple relabeling of data qubits. We further construct a syndrome extraction pattern for both families that does not imply minimum distance reduction arising from extraction circuit faults that propagate from the check qubits to the data qubits. Finally, we numerically evaluate their logical error rates under a code capacity depolarizing noise model using the belief propagation ordered statistics decoding (BP-OSD) and minimum-weight perfect-matching (MWPM) decoders, yielding thresholds of approximately 14–16% for the odd and even families, very similar to those of rotated surface codes.

I. INTRODUCTION

Quantum error correction (QEC) is crucial technique for unlocking the theoretical potential of quantum computing, given the extreme vulnerability of quantum information. Among all quantum error-correcting codes, the family of quantum low-density parity-check (LDPC) codes with low qubit-check connectivity enables low-overhead error correction, making them a promising candidate for large-scale, fault-tolerant quantum computation. There have been several proposals for quantum LDPC codes that aim to balance theoretical guarantees with hardware feasibility [1–7]. In particular, recently it was shown that certain quantum LDPC codes can offer a constant encoding rate and linear distance scaling [8–13].

One of the main challenges associated with general quantum LDPC codes is the difficulty of constructing codes that have very low qubit interaction, short lengths, and good parameters [14]. In particular, the block size of theoretically good codes is often large, requiring many qubits for implementation.

Therefore, shorter codes with a small, fixed number of qubit interactions (fewer than ten for most physical platforms) and greater hardware compatibility, even if their parameters are suboptimal, can be more practical in certain applications.

Generalized bicycle (GB) codes form a family of quantum codes that are particularly well-suited for constructing short codes with several desirable properties [3, 4]. These include ease of construction, connections to other code families (such as quantum hypergraph-product codes) [6], linear distance scaling, efficient decoding, redundancy of minimum-weight stabilizer generators, and various other advantageous features [3–5, 14–17]. Furthermore, the parameters of many small size degenerate GB codes and their generalization to two block group algebra codes, as well as new distance bounds for non-degenerate codes, derived from their underlying algebraic structure, have been studied in [5, 14]. However, many of the currently studied GB codes are limited either to non-degenerate codes that require large qubit connectivity, or, in the case of degenerate codes, to those that have been studied primarily through numerical methods. One of the main remaining challenges is to systematically construct families of degenerate GB codes, ideally with fewer than ten qubit connectivity, that are suitable for practical applications.

Recently, an efficient protocol was proposed for implementing a class of GB codes on neutral atom array quantum computers, offering faster logical cycles and improved hardware efficiency compared to other approaches [18]. Other practical implementations of GB codes in neutral atom array and silicon spin qubit hardware have been investigated in [18, 19].

In this work, we extend previous results by establishing a connection between GB codes and the family of additive cyclic codes [20, 21], and by presenting new general bounds (both lower and upper) on the minimum distance of GB codes. In particular, we show that our bounds can capture distance behavior beyond the classical minimum distance, making them applicable to certain degenerate GB codes. Using these bounds, we construct

* rdastbasteh@unav.es

† jetxezarreta@unav.es

two families of degenerate GB codes, where each check qubit is connected to four data qubits containing parameters $[[d^2+1, 2, d]]$ for odd $d \geq 3$ and $[[d^2, 2, d]]$ for even $d \geq 4$. We study the structure of certain logical operators in these families. In particular, we show how to perform a fault-tolerant logical CNOT on two logical qubits at zero cost for each member of the former family by using only a permutation of data qubits, a technique previously studied in the literature [22, 23], which is distinct from other fault-tolerant approaches such as transversal gates and lattice surgery. As an additional result, we provide a syndrome extraction pattern that is resilient to hook errors introduced during the extraction process. Additionally, we completely characterize the girth of the Tanner graphs for all GB codes. Finally, we study the code capacity thresholds of the mentioned two families of GB codes. In particular, we show that the extracted thresholds under the depolarizing noise and using belief propagation ordered statistics decoder (BP-OSD) and Minimum-Weight Perfect Matching (MWPM) decoders are very similar to those of rotated surface codes. Therefore, this study provides evidence supporting the idea that the mentioned GB families could be promising candidates for fault-tolerant quantum computing.

Around the same time as our work, the existence of the mentioned GB code families was also established in [24, 25], using a graph-theoretical approach independent of ours. The authors also studied equivalence of such codes and connection to other notable CSS codes derived from Cayley graphs. In contrast, our method for the existence of such families is based on the algebraic structure of generalized bicycle (GB) codes, and the minimum distance bounds we derive can be applied to GB codes containing more than two logical qubits, a capability not attainable by the mentioned works. Additionally, we use the distance bounds to find syndrome extraction patterns resistant to hook errors, and we study the structure of logical operators.

The structure of the paper is as follows. In Section II we give the preliminary background on classical linear codes, quantum codes, and GB codes. Section III gives the connection between additive cyclic codes and GB codes. In Section IV, we give our minimum distance bounds for GB codes. In Sections V and VI we study the existence of two families of (optimal) GB codes containing two logical qubits, logical operations, and a hook error resilient syndrome extraction. The characterization of the girth of GB codes and extraction of code capacity thresholds are studied in Section VII.

II. PRELIMINARIES

In this section, we review the necessary background and establish the notation for classical and quantum error-correcting codes, which will serve as the foundation for presenting our results. Through this work, we only consider binary quantum error-correcting codes.

A. Linear codes

Let \mathbb{F}_2 be the binary field and n be a positive integer. A binary *linear code* of length n is a linear subspace C of \mathbb{F}_2^n . The (*Hamming*) *weight* of a vector $v \in \mathbb{F}_2^n$ is defined by the number of its non-zero coordinates and it is denoted by $\text{wt}(v)$. The parameters of such a code are denoted by $[n, k, d]$, where k is the dimension of the code C (denoted by $k = \dim(C)$) and d is the minimum distance of C defined by

$$d = d(C) = \min\{\text{wt}(c) : 0 \neq c \in C\}.$$

A linear code $C \subseteq \mathbb{F}_2^n$ is called *cyclic* if for every $c = (c_0, c_1, \dots, c_{n-1}) \in C$, the vector $(c_{n-1}, c_0, \dots, c_{n-2})$ obtained by a cyclic shift of the coordinates of c is also in C . In the study of cyclic codes, it is more convenient to represent vectors using their polynomial representation. In particular, for each $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_2^n$ the polynomial representation of c is

$$c(x) = \sum_{i=0}^{n-1} c_i x^i.$$

It is well known that there is a one-to-one correspondence between cyclic codes of length n over \mathbb{F}_2 and ideals of the ring $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$, for example see [26, Section 4.2]. Under this correspondence, each cyclic code can be generated by a *unique monic polynomial* $g(x)$, where $g(x) \mid x^n - 1$ and it has the minimal degree. The polynomial $g(x)$ is called the *generator polynomial* of such cyclic code.

Recall that the Euclidean inner product of $u = (u_0, u_1, \dots, u_{n-1})$ and $v = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_2^n$ is defined as

$$u \cdot v = \sum_{i=0}^{n-1} u_i v_i.$$

The Euclidean dual of a binary code C of length n is defined as

$$C^\perp = \{u \in \mathbb{F}_2^n : u \cdot c = 0, \forall c \in C\}.$$

Each linear code can be represented as the row space of a given matrix, called a *generator matrix*. In particular, if C is a binary cyclic code of length

n and dimension k with the generator polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$, then the matrix

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \quad (\text{II.1})$$

is a generator matrix of C . An alternative approach to represent a linear code is by presenting it as a solution space of a matrix equation $Hx = 0, x \in C$. The matrix H is called a *parity check matrix* of such code, i.e. it defines the nullspace of matrix G . In particular, if G and H are generator and parity check matrices of a linear code, then we have $GH^T = 0$.

B. Quantum stabilizer codes

Quantum stabilizer codes serve as the quantum analogue of classical linear error-correcting codes, providing protection against decoherence and other quantum noise sources [27, 28]. In order to present them we need a number of preliminary definitions.

Let $(\mathbb{C}^2)^{\otimes n}$ be an n -qubits Hilbert space. A Pauli operator acting on an n -qubit system is an operator defined on $(\mathbb{C}^2)^{\otimes n}$ in the form of

$$P = a \bigotimes_{i=1}^n P_i,$$

where $a \in \{\pm 1, \pm i\}$ and $P_i \in \{I, X, Y, Z\}$ are the Pauli matrices. The weight of a Pauli operator P is the number of its non-identity components. The group of all Pauli operators on n -qubits P_n is a non-commutative group. Its quotient group modulo the global phase factor a is isomorphic to \mathbb{F}_2^{2n} which is given by [29]

$$\begin{aligned} \bigotimes_{i=1}^n P_i &= \bigotimes_{i=1}^n X^{x_i} Z^{z_i} \\ &\rightarrow (x_1, x_2, \dots, x_n | z_1, z_2, \dots, z_n). \end{aligned} \quad (\text{II.2})$$

Under this isomorphism, two Pauli operators commute if and only if their binary representations, namely $(x|z)$ and $(x'|z')$, satisfy

$$(x|z) * (x'|z') = x \cdot z' + x' \cdot z = 0. \quad (\text{II.3})$$

The $*$ inner product is called *symplectic inner product* [29]. A commutative subgroup S of P_n such that $-I \notin S$ is called a *stabilizer group*.

Now we recall the definition of stabilizer codes. An $[[n, k, d]]$ binary quantum stabilizer code is a 2^k -dimensional subspace of $(\mathbb{C}^2)^{\otimes n}$ defined as the common eigenspace of a stabilizer group S with eigenvalue $+1$ that has a minimal set of $n - k$

generators. The minimum distance d is the minimum weight of a Pauli operator $P \in P_n$ such that P commutes with all elements of S but $P \notin S$. A quantum code is called *degenerate* if there exists $P \in S$ with weight less than d . Degeneracy is a phenomenon unique to quantum codes, and highly degenerate codes, often characterized by low qubit connectivity, appear to offer improved error-correcting performance. In fact, the asymptotic results on the existence of good quantum LDPC codes and their finite length constructions are based on a degenerate construction [4, 30].

In order to construct a stabilizer group of P_n one can take advantage of the isomorphism (II.2) and the commuting condition (II.3). In particular, any linear subspace C of \mathbb{F}_2^{2n} that satisfies (II.3) for any $(x|z)$ and $(x'|z') \in C$ is in correspondence to a stabilizer group. One special case of such construction of quantum stabilizer codes is called the Calderbank-Shor-Steane (CSS) that is given below [31, 32].

Theorem II.1. *Let $C_2 \subseteq C_1$ be binary linear codes of length n with dimensions k_2 and k_1 , respectively. Then there exists an $[[n, k = k_1 - k_2, d]]$ binary quantum stabilizer code, where*

$$d = \min\{d(C_1 \setminus C_2), d(C_2^\perp \setminus C_1^\perp)\}.$$

The parity check (stabilizer) matrix of such CSS code is

$$H = \begin{bmatrix} H_{C_2^\perp} & 0 \\ 0 & H_{C_1} \end{bmatrix},$$

where $H_{C_2^\perp}$ and H_{C_1} are parity check matrices of C_2^\perp and C_1 , respectively. In particular, we have $H_{C_2^\perp} H_{C_1}^T = 0$ (recall that $C_2 \subseteq C_1$). In other words, in order to construct a quantum CSS code, one needs to find two matrices H_x and H_z such that $H_x H_z^T = 0$. This is because

$$H = \begin{bmatrix} H_x & 0 \\ 0 & H_z \end{bmatrix}$$

satisfies the conditions of Theorem II.1 (consider H_x parity check matrix of C_2^\perp and H_z parity check matrix of C_1). In the next section, we review quantum GB codes which is a subclass of CSS codes.

C. Generalized bicycle codes

In this subsection, we recall the construction of GB codes discussed in [3, 4]. Let $a = (a_0, a_1, \dots, a_{n-1})$ be a binary vector. Recall that the $n \times n$ circulant matrix corresponding to the vector a is defined by

$$G_a = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}. \quad (\text{II.4})$$

Note also that there exists a ring isomorphism between $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$ and binary $n \times n$ circulant matrices given by

$$\sum_{i=0}^{n-1} a_i x^i \rightarrow G_a,$$

where $a = (a_0, a_1, \dots, a_{n-1})$. From now on, we represent the matrix G_a using its polynomial representation i.e., by $G_{a(x)}$. Some properties of circulant matrices are summarized below:

- $G_{a(x)b(x)} = G_{b(x)}G_{a(x)}$ (commuting).
- $G_{a(x)}^T = G_{a(x^{-1})}$.
- If $a(x)$ is invertible modulo $x^n - 1$, then $G_{a(x)^{-1}} = (G_{a(x)})^{-1}$.

Let $G_{a(x)}$ and $G_{b(x)}$ be two $n \times n$ circulant matrices. Then the matrix

$$H = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix},$$

where $H_1 = [G_{a(x)}|G_{b(x)}]$ and $H_2 = [G_{b(x^{-1})}|G_{a(x^{-1})}]$ is a stabilizer matrix of a quantum CSS code since

$$\begin{aligned} H_1 H_2^T &= [G_{a(x)}|G_{b(x)}][G_{b(x^{-1})}|G_{a(x^{-1})}]^T \\ &= G_{a(x)b(x)} + G_{b(x)a(x)} = 0 \end{aligned}$$

Note also that, as it is shown in the proof of [4, Proposition 1], the matrices H_1 and H_2 both have rank $n - k$, where

$$k = \deg(\gcd(a(x), b(x), x^n - 1)).$$

Thus the quantum CSS code with the parity check matrix H has parameters $[[2n, 2k]]$. The quantum codes constructed this way are known as *generalized bicycle* (GB) codes. A special subclass of GB codes is by choosing $a(x) = b(x)$, which is called a *bicycle* code [33].

We highlight a connection between GB codes and quasi-cyclic codes. First, note that each circulant matrix can be obtained by adding extra rows to the generator matrix of a cyclic code, as presented in (II.1). These additional rows are, in fact, linear combinations of the original rows and are closely related to the redundancy of minimum-weight stabilizer generators in GB codes. Such redundancy has recently been exploited to improve both the accuracy and speed of syndrome-based decoding [15]. Second, the horizontal concatenation of two circulant matrices yields a generator matrix for a quasi-cyclic code. Consequently, techniques from the theory of cyclic and quasi-cyclic codes are highly valuable for studying the properties of GB codes.

III. GB CODES AND ADDITIVE CYCLIC CODES

In this section, we highlight a natural connection between additive cyclic codes and generalized bicycle (GB) codes. Given the extensive literature on additive cyclic codes, this connection enables us to take advantage of existing results to construct new families of GB codes.

Let n be a positive integer and $\mathbb{F}_4 = \{0, 1, w, w^2\}$ be the quaternary field, where $w+1 = w^2$. An \mathbb{F}_2 -subspace C of \mathbb{F}_4^n is called an *additive code* over \mathbb{F}_4 . The symplectic inner product of two vectors stated in (II.3) can be naturally redefined over \mathbb{F}_4^n as

$$\begin{aligned} (a_i + wb_i)_{i=1}^n * (c_i + wd_i)_{i=1}^n &= \\ (a_i)_{i=1}^n \cdot (d_i)_{i=1}^n + (b_i)_{i=1}^n \cdot (c_i)_{i=1}^n &= \sum_{i=1}^n a_i d_i + b_i c_i \end{aligned} \quad (\text{III.1})$$

An additive code consisting of all the vectors that are symplectic orthogonal to an additive code C will be denoted by C^{\perp_s} and will be called its *symplectic dual*.

Moreover, if the code C is closed under cyclic shifts of codewords, then it is called an *additive cyclic code* over \mathbb{F}_4 . Additive cyclic codes over \mathbb{F}_4 have been studied extensively in the literature, and many examples and families of good quantum codes are based on them [20, 34–36].

Recall also that there is an \mathbb{F}_2 -isomorphism $\phi : \mathbb{F}_4 \rightarrow \mathbb{F}_2^2$ that maps $\phi(0) = (0, 0)$, $\phi(1) = (1, 0)$, $\phi(w) = (0, 1)$, and $\phi(w^2) = (1, 1)$. This isomorphism can be extended to an \mathbb{F}_2 -isomorphism $\psi : \mathbb{F}_4^n \rightarrow \mathbb{F}_2^{2n}$ defined by

$$\psi((v_0, v_1, \dots, v_{n-1})) = (u_1, u_2), \quad (\text{III.2})$$

where we have $u_1 = (u_{10}, u_{11}, \dots, u_{1n-1})$ and $u_2 = (u_{20}, u_{21}, \dots, u_{2n-1}) \in \mathbb{F}_2^{2n}$ with $\phi(v_i) = (u_{1i}, u_{2i})$ for each $0 \leq i \leq n-1$.

Let $a(x)$ and $b(x)$ be two polynomials of $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$. Then the \mathbb{F}_2 -linear span of

$$\{x^i(a(x) + wb(x)) : 0 \leq i \leq n-1\}$$

forms a so called *one generator additive cyclic code* C of length n over \mathbb{F}_4 . We represent such a code C with $\langle a(x) + wb(x) \rangle$. Applying the map ψ to the code C gives a binary linear code of length $2n$ with the generator matrix $[G_{a(x)}|G_{b(x)}]$. Using this transformation, one can turn an additive cyclic code into a GB code of $(a(x), b(x))$. In other words, the corresponding GB code has the following properties:

- the X stabilizers are in correspondence to $\psi(C_1)$, where $C_1 = \langle a(x) + wb(x) \rangle$.
- the Z stabilizers are in correspondence to $\psi(C_2)$, where $C_2 = \langle b(x^{-1}) + wa(x^{-1}) \rangle$.

- C_1 and C_2 (hence $\psi(C_1)$ and $\psi(C_2)$) are equivalent}. Therefore, their duals, and consequently the corresponding normalizer groups are equivalent. In short, $\psi(C_1) \sim \psi(C_2)$ and $\psi(C_1)^\perp \sim \psi(C_2)^\perp$.

It should be noted, as shown in [35, Theorem 3.6], that the maximum number of generators of an additive cyclic code is two. Therefore, the above transformation can also be used to extend beyond single-generator additive cyclic codes.

Let $C = \langle a(x) + wb(x) \rangle$. We fix the following notation for additive cyclic codes:

- The *reciprocal code* of C is defined by $C^R = \langle a(x^{-1}) + wb(x^{-1}) \rangle$.
- The *conjugate code* of C is defined by $\bar{C} = \langle b(x) + wa(x) \rangle$.

One can connect the symplectic inner product and the Euclidean inner product of additive cyclic codes and their corresponding binary codes, respectively, under the map ψ using the following result.

Proposition III.1. *Let $C = \langle a(x) + wb(x) \rangle$ be an additive code of length n over \mathbb{F}_4 . Then*

$$\psi((C^R)^{\perp_s}) = \psi(\bar{C})^\perp.$$

Proof. Let $v = m(x) + wn(x) \in C$. Note that

$$\psi(\bar{v}) = \psi(n(x) + wm(x)) = (n, m) \in \mathbb{F}_2^n \times \mathbb{F}_2^n,$$

where n and m are the vector representations of $n(x)$ and $m(x)$, respectively. Hence we have $(p, q) \in \psi(\bar{C})^\perp$ if and only if $p \cdot n + q \cdot m \equiv 0 \pmod{2}$ for each $v = m(x) + wn(x) \in C$. Using the argument given in [35, Remark 4.1], we have

$$0 \equiv p(x) \cdot n(x) + q(x) \cdot m(x) \equiv (p(x) + wq(x)) * (m(x^{-1}) + wn(x^{-1})) \pmod{x^n - 1}.$$

This is true if and only if $(p(x) + wq(x)) \in (C^R)^{\perp_s}$ which happens if and only if $(p, q) \in \psi((C^R)^{\perp_s})$. Thus

$$\psi((C^R)^{\perp_s}) = \psi(\bar{C})^\perp.$$

□

The connection between additive cyclic codes and binary linear codes enables us to systematically build binary quantum CSS codes from additive cyclic codes over \mathbb{F}_4 . The following theorem summarizes this result.

Theorem III.2. *Let $C = \langle a(x) + wb(x) \rangle$ be an additive code of length n over \mathbb{F}_4 with $\dim(C) = k$ (dimension over \mathbb{F}_2). Then there exists a binary quantum (which is a GB) code with parameters $[[2n, 2(n - k), d]]_2$, where*

$$d \geq \min\{d((C^R)^{\perp_s} \setminus C)\} \geq d((C^R)^{\perp_s}).$$

In particular, if C is palindromic, i.e., $C = C^R$, then

$$d \geq \min\{d(C^{\perp_s} \setminus C)\} \geq d(C^{\perp_s}).$$

Proof. Let $g(x) = a(x) + wb(x)$. Using the argument given in [35, Remark 4.1], we have C and C^R are symplectic orthogonal as

$$\begin{aligned} g(x) * g(x)^R &= (a(x) + wb(x)) * (a(x^{-1}) + wb(x^{-1})) \\ &\equiv a(x)b(x) + a(x)b(x) \equiv 0 \pmod{x^n - 1}. \end{aligned}$$

Thus $C \subseteq (C^R)^{\perp_s}$. Now applying the map ψ to both sides and using Proposition III.1 we get

$$\psi(C) \subseteq \psi(\bar{C})^\perp.$$

The quantum CSS code, see Theorem II.1, of $\psi(C) \subseteq \psi(\bar{C})^\perp$ has dimension

$$\dim(\psi(\bar{C})^\perp) - \dim(\psi(C)) = (2n - k) - k = 2(n - k).$$

Moreover, the equivalence relation between the codes $C \sim \bar{C}$ and the result of Proposition III.1 imply that

$$d(\psi((C^R)^{\perp_s}) \setminus \psi(C)) = d(\psi((\bar{C}^R)^{\perp_s}) \setminus \psi(\bar{C}))$$

Hence such CSS code has minimum distance

$$d \geq \min\{d((C^R)^{\perp_s} \setminus C)\} \geq d(C').$$

The last inequality is due to the fact that ψ sends a vector of weight t to a vector of weight “at least” t .

In the case of $C = C^R$, the result follows immediately. □

It should be noted that the above distance inequality can be strict. For instance, when all minimum weight codewords of $(C^R)^{\perp_s} \setminus C$ have at least one coordinate position containing w^2 . In this case, we have

$$d > d((C^R)^{\perp_s} \setminus C).$$

On the other hand, if there exists a minimum weight codeword of $(C^R)^{\perp_s} \setminus C_1$ that only has coordinate values belonging to $\{0, 1, w\}$, then the above minimum distance bound becomes equality, i.e.,

$$d = d((C^R)^{\perp_s} \setminus C).$$

Furthermore, one can generalize the result of Theorem III.2 to cover more general additive codes (with more than one generator). In particular, a similar argument as the one in the previous proof implies that replacing C with any symplectic self-orthogonal additive code (even with more than one generator) leads to the same result.

Through the next example, we give an instance of the former case when the minimum distance improvement happens.

Example III.3. Let $n = 13$. Then applying the result of Theorem III.2 to the symplectic self-orthogonal code C obtained from Theorem 6.4 of [36] (which is in correspondence to a non-CSS code $[[13, 1, 5]]$) implies a CSS code with parameters $[[26, 2, 6]]$, which has the same rate but a larger minimum distance. Here the qubit connectivity is large than four.

An immediate application of the above theorem is in converting currently known families of additive cyclic codes, i.e., the quantum non-CSS codes, into families of GB codes that are CSS codes “at no extra cost”. For instance, several families and examples of additive cyclic codes and quantum non-CSS codes over \mathbb{F}_4 were discussed in [20, Chapter VI] and [36, Chapter 6], which can naturally be transformed into CSS codes using the above tool. Another example is based on the family of odd length XZZX cyclic codes [20, 21], that we briefly discuss below.

Example III.4. Let d be a positive odd integer and $n = \frac{d^2+1}{2}$. In [20, Example 11], it was shown that the palindromic additive cyclic code generated by

$$g(x) = w + x + x^d + wx^{d+1}$$

which is in correspondence to the Pauli operator

$$ZXI^{\otimes^{d-2}}XZI^{\otimes^{n-d-2}}$$

generates a non-CSS code with parameters $[[\frac{d^2+1}{2}, 1, d]]$. This code has a minimum codeword consisting of alphabets $\{0, 1, w\}$. Then the result of Theorem III.2 implies the existence of a GB family with parameters $[[d^2 + 1, 2, d]]$, with the corresponding polynomials $a(x) = x + x^d$ and $b(x) = 1 + x^{d+1}$. Finally, as it is been stated in [14, Statement 11], no GB code with generator polynomial of weight four and parameters $[[n, k, d]]$ can have $d > \sqrt{n-1}$. Hence the above family is an optimal class of GB codes in this sense.

The existence of the above family is also established in [25] through a graph-theoretical approach. In Section V, we revisit this family, providing an algebraic perspective on their existence, the structure of a few logical operators, and a syndrome extraction procedure that is resilient to hook errors.

Next we discuss a natural minimum distance upper bound for GB codes.

Lemma III.5. Let $a(x)$ and $b(x) = m(x)a(x)$ be two polynomials of degree less than n . If the quantum GB code of length n corresponding to polynomials of $a(x)$ and $b(x)$ has dimension larger than zero, then it has minimum distance of at most $\text{wt}(m(x)) + 1$.

Proof. The corresponding GB code has the parity check matrix

$$H = \begin{bmatrix} H_x & 0 \\ 0 & H_z \end{bmatrix},$$

where $H_x = [G_{a(x)}, G_{b(x)}]$ and $H_z = [G_{b(x^{-1})}, G_{a(x^{-1})}]$. This quantum code is the CSS code of $C_2 \subseteq C_1$, where H_x and H_z are parity check matrices of C_2^\perp and C_1 , respectively. Let $w = (u, v)$, where $u = (1, 0, \dots, 0)$ and v is the vector representation of $m(x)$. Then $w \in C_1$ because

$$\begin{aligned} H_z w^T &= b(x^{-1})u^T + a(x^{-1})v^T = \\ b(x^{-1}) + a(x^{-1})m(x^{-1}) &= b(x^{-1}) + b(x^{-1}) = 0. \end{aligned}$$

Since each $(u', v') \in C_2$ satisfies $\text{wt}(u') > 1$, as otherwise the GB code has dimension zero, we conclude that $w \notin C_2$ and it has weight $\text{wt}(m(x)) + 1$. Thus $d(C_1 \setminus C_2) \leq \text{wt}(m(x)) + 1$. \square

We consider two binary codes as *permutation equivalent* if there exists a permutation of coordinates that maps one code to another. Some equivalence criteria for GB codes is discussed in Statement 3 of [14]. The following proposition gives a new condition for GB codes to have the same parameters.

Proposition III.6. Let $a(x)$ and $b(x)$ be two binary polynomials of $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$. Then the GB codes corresponding to $a(x)$ and $b(x)$, and $a'(x) = x^i a(x)$ and $b'(x) = x^j b(x)$ both have the same parameters (length, dimension, and minimum distance) for each $0 \leq i, j \leq n-1$.

Proof. These GB codes are the CSS codes of $C_2 \subseteq C_1$ and $C'_2 \subseteq C'_1$, where C_2 and C'_2 have the generator matrices $H_x = [G_{a(x)}, G_{b(x)}]$ and $H'_x = [G_{a'(x)}, G_{b'(x)}]$, and C_1 and C'_1 have the check matrices $H_z = [G_{b(x^{-1})}, G_{a(x^{-1})}]$ and $H'_z = [G_{b'(x^{-1})}, G_{a'(x^{-1})}]$, respectively.

Applying i cyclic shifts to the first, and j shifts to the second n components of C_2 (that is a permutation action) sends the matrix H_x to H'_x . So C_2 and C'_2 are equivalent, and hence have the same parameters and weight distribution. Similarly, applying $n-j$ shifts to the first and $n-i$ shifts to the second n components of C_1 maps it to C'_1 . Thus we have

- C_1 and C'_1 are permutation equivalent,
- C_2 and C'_2 are permutation equivalent,
- $C_2 \subseteq C_1$ and $C'_2 \subseteq C'_1$.

The first two conditions imply that the corresponding GB codes have the same length and dimension. Moreover, these three conditions imply that $C_1 \setminus C_2$ and $C'_1 \setminus C'_2$ (respectively $C_2^\perp \setminus C_1^\perp$ and $C'_2^\perp \setminus C'_1^\perp$) have the same minimum weight vectors. \square

Example III.7. Consider the $[[d^2 + 1, 2, d]]$ GB code of Example III.4 with corresponding $a(x) = x + x^{d-1}$ and $b(x) = 1 + x^{d+1}$, with $n = \frac{d^2+1}{2}$. Note that since d is odd, we have $\gcd(2, n) = 1$. Moreover,

$$\frac{(d-1)(d+1)}{2} + \frac{d^2+1}{2} \equiv 1 \pmod{n}.$$

Hence $\gcd(d+1, n) = \gcd(d-1, n) = 1$ and by [14, Statement 3 (i)], we have an equivalent GB code with polynomials $a(x^{\frac{d+1}{2}}) = x^{\frac{d-1}{2}}(1+x)$ and $b(x^{\frac{d+1}{2}}) = 1 + x^d$. Hence Proposition III.6 implies that $a'(x) = 1 + x$ and $b'(x) = 1 + x^d$ form an equivalent GB code.

Moreover, note that $b'(x) = (1 + x + \dots + x^d - 1)a'(x)$. Hence the Minimum distance upper bound of Lemma III.5 gives the sharp upper bound of d , which is the actual minimum distance.

IV. NEW MINIMUM DISTANCE BOUNDS FOR GB CODES

One of the key steps in constructing large families of GB codes is the development of tools for accurately computing their minimum distance. In particular, we are interested in degenerate GB codes with low connectivity between data and check qubits. The scarcity of effective minimum distance bounds for such codes may explain the limited number of known infinite families of degenerate GB codes. Motivated by this, we develop new minimum distance bounds based on the algebraic structure of GB codes, which can be used to construct novel families of degenerate GB codes.

In the rest of this section, we present new minimum distance bounds for the GB code family. These bounds facilitate the exact calculation of the minimum distance for certain instances, significantly reduce the overall computation time, and support the construction of new GB code families. The following setup is required to present our bound.

Let n be a positive integer and $f(x) \mid x^n - 1$. Let also $p(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ such that $\gcd(p(x), x^n - 1) = 1$, i.e., $p(x)$ is a unit element of the ring. We restrict our discussion to the GB code constructed from the polynomials $a(x) = f(x)$ and $b(x) = p(x)f(x)$. Then this GB code has parameters $[[2n, 2k]]$, where $k = \deg(f(x))$. Note that $f(x)$ is the generator polynomial of a length n binary cyclic code and its Euclidean dual has generator polynomial $g(x)$, where $g(x)$ is the reciprocal polynomial of $h(x) = \frac{x^n-1}{f(x)}$ defined by $g(x) = x^{\deg(h(x))}h(x^{-1})$.

This GB code is the CSS code of $C_2 \subseteq C_1$, where $C_2 = \langle (a(x), b(x)) \rangle$ and $C_1 = C_2 + \text{Span}\{(c, c')\}$, and $c, c' \in \langle g(x) \rangle$. One can also define C_1 as $C_1 = \langle (b(x^{-1}), a(x^{-1})) \rangle^\perp$. Using the latter, each

element of C_1 can be characterized as $(u(x), v(x))$ such that

$$\begin{aligned} u(x)b(x) + v(x)a(x) &= u(x)f(x)p(x) + v(x)f(x) \\ &\equiv f(x)(u(x)p(x) + v(x)) \equiv 0 \pmod{x^n - 1}. \end{aligned} \quad (\text{IV.1})$$

This implies one of the following two cases

$$(a) \quad u(x)p(x) + v(x) \equiv 0 \pmod{x^n - 1}$$

or

$$(b) \quad \begin{aligned} u(x)p(x) + v(x) &\not\equiv 0 \pmod{x^n - 1} \\ \text{and } h(x) &\mid u(x)p(x) + v(x). \end{aligned}$$

First we consider case (b). In this case $u(x)p(x) + v(x)$ is a non-zero element of the cyclic code generated by $h(x)$, which will be called $C_{h(x)}$. A similar calculation after multiplying sides of (IV.1) by $p(x)^{-1}$ shows that $u(x) + p(x)^{-1}v(x) \in C_{h(x)}$. Let $d = d(C_{h(x)})$. Then

$$\begin{aligned} d &\leq \text{wt}(u(x)p(x) + v(x)) \\ &\leq \text{wt}(p(x))\text{wt}(u(x)) + \text{wt}(v(x)). \end{aligned} \quad (\text{IV.2})$$

and

$$\begin{aligned} d &\leq \text{wt}(u(x) + p(x)^{-1}v(x)) \\ &\leq \text{wt}(u(x)) + \text{wt}(p(x)^{-1})\text{wt}(v(x)). \end{aligned} \quad (\text{IV.3})$$

An immediate application of this is that if $m = \max\{\text{wt}(p(x)), \text{wt}(p(x)^{-1})\}$, then we get

$$\begin{aligned} (\text{wt}(p(x)) + \text{wt}(p(x)^{-1}))d &\leq \\ (m + \text{wt}(p(x))\text{wt}(p(x)^{-1}))\text{wt}((u(x), v(x))). \end{aligned}$$

Therefore, this GB code has minimum distance d_{GB} , which satisfies

$$\frac{(\text{wt}(p(x)) + \text{wt}(p(x)^{-1}))d}{(m + \text{wt}(p(x))\text{wt}(p(x)^{-1}))} \leq d_{GB}. \quad (\text{IV.4})$$

Now we consider case (a). First, let

$$r(x) + p(x)s(x) \equiv h(x) \pmod{x^n - 1}, \quad (\text{IV.5})$$

for some $r(x)$ and $s(x) \in \mathbb{F}_2[x]$. Then for each $u(x)$ such that $f \nmid u(x)$ we have

$$u(x)r(x) + u(x)p(x)s(x) \equiv u(x)h(x) \pmod{x^n - 1},$$

which is a nonzero codeword of $C_{h(x)}$. Therefore,

$$\begin{aligned} d &\leq \text{wt}(u(x)r(x) + u(x)p(x)s(x)) \\ &\leq \text{wt}(r(x))\text{wt}(u(x)) + \text{wt}(s(x))\text{wt}(u(x)p(x)). \end{aligned} \quad (\text{IV.6})$$

Hence if $m = \max\{\text{wt}(r(x)), \text{wt}(s(x))\}$, then

$$\frac{d}{m} \leq d_{GB}.$$

A similar argument using the polynomial $p(x)^{-1}$ results in a new equation

$$r'(x) + p(x)^{-1}s'(x) \equiv h(x) \pmod{x^n - 1},$$

and if $m' = \max\{\text{wt}(r'(x)), \text{wt}(s'(x))\}$, then

$$\max\left\{\frac{d}{m}, \frac{d}{m'}\right\} \leq d_{GB}.$$

Moreover, one can easily verify, for example using Lemma III.5, that $(1, p(x))$ and $(p(x)^{-1}, 1) \in C_1 \setminus C_2$ and both satisfy (a). Hence one gets

$$\frac{d}{m'} \leq d_{GB} \leq \min\{\text{wt}(p(x)), \text{wt}(p(x)^{-1})\} + 1. \quad (\text{IV.7})$$

Note also that if $f \nmid s(x)$ in (IV.5), then $(s(x), p(x)s(x) + h(x)) = (s(x), r(x)) \in C_1 \setminus C_2$ and satisfies case (b). Therefore, we also have

$$d_{GB} \leq \text{wt}(s(x)) + \text{wt}(r(x)). \quad (\text{IV.8})$$

We now formally state a particular application of the above discussion.

Theorem IV.1. *Let n be a positive integer, $f(x) \mid x^n - 1$, and $p(x) \in \mathbb{F}_2[x]$ such that $\gcd(p(x), x^n - 1) = 1$. Let also*

$$r(x) + p(x)s(x) \equiv \frac{x^n - 1}{f(x)} \pmod{x^n - 1}$$

and

$$r'(x) + p(x)^{-1}s'(x) \equiv \frac{x^n - 1}{f(x)} \pmod{x^n - 1}$$

for some $r(x), s(x), r'(x), s'(x) \in \mathbb{F}_2[x]$ and d be the minimum distance of the length n binary cyclic code generated by $\frac{x^n - 1}{f(x)}$. Then the GB code corresponding to $(f(x), p(x)f(x))$ has parameters $[[2n, 2\deg(f(x)), d_{GB}]]$ where

$$\min\left\{\frac{(\text{wt}(p(x)) + \text{wt}(p(x)^{-1}))d}{(m + \text{wt}(p(x))\text{wt}(p(x)^{-1}))}, \frac{d}{m'}\right\} \leq d_{GB} \leq \min\{\text{wt}(p(x)) + 1, \text{wt}(p(x)^{-1}) + 1, \text{wt}(s(x)) + \text{wt}(t(x))\},$$

where $m = \max\{\text{wt}(p(x)), \text{wt}(p(x)^{-1})\}$ and

$$m' \in \{\max\{\text{wt}(r(x)), \text{wt}(s(x))\}, \max\{\text{wt}(r'(x)), \text{wt}(s'(x))\}\}.$$

Moreover, there exist non-trivial logical operators of weights $\text{wt}(p(x)) + 1$ and $\text{wt}(s(x)) + \text{wt}(t(x)) \in C_1 \setminus C_2$.

It is important to emphasize that the above result is merely a special case of the distance lower and upper bounds given in (IV.2)–(IV.8); in fact, tighter bounds may be obtained using these general equations. Moreover, our discussion of the

minimum distance does not rely entirely on the existence of $p(x)^{-1}$ and remains valid even when the condition $\gcd(p(x), x^n - 1)$ is relaxed. The following examples illustrate applications of these observations and demonstrate how the above theorem can be used.

Example IV.2. Let $n = 48$, $f(x) = 1 + x + x^2$ (where $f(x) \mid x^n - 1$), and $p(x) = 1 + x^3 + x^6 + \dots + x^{18}$. Note that $p(x)$ is invertible modulo $x^n - 1$ with the inverse

$$p(x)^{-1} = x^3 + x^6 + x^{12} + x^{18} + x^{24} + x^{27} + x^{33} + x^{39} + x^{45}.$$

Also, the cyclic code generated by $h(x) = \frac{x^n - 1}{f(x)}$ has distance $\frac{2n}{3} = 32$ and we have

$$h(x) = p(x)(x^6 + x^7 + x^{27} + x^{28}) + (1 + x + x^3 + x^4).$$

Applying the result of Theorem IV.1 implies that the pair of polynomials $(f(x), f(x)p(x))$ forms a GB code with parameters $[[96, 4, d_{GB}]]$, where

$$7 < \min\left\{\frac{(9+7)32}{9+63}, \frac{32}{4}\right\} \leq d_{GB} \leq \min\{8, 10\},$$

which implies that $d_{GB} = 8$.

Example IV.3. Let $n = 27$, $f(x) = 1 + x + x^2$, and $p(x) = 1 + x^3 + x^6 \dots + x^{18}$. Next we apply Theorem IV.1 and show that the GB code corresponding to the polynomials $f(x)$ and $f(x)p(x)$ has parameters $[[54, 4, 6]]$. First, since $\deg(f(x)) = 2$ the claim about dimension follows immediately.

Note that the cyclic code generated by $h(x) = \frac{x^n - 1}{f(x)}$ has distance $\frac{2n}{3} = 18$. Also one can verify that

$$h(x) = p(x)(x^6 + x^7) + (1 + x + x^3 + x^4).$$

and

$$p(x)^{-1} = x^3 + x^6 + x^{12} + x^{18} + x^{24}.$$

Now applying the minimum distance bound of Theorem IV.1 implies that

$$\min\left\{\frac{12 \times 18}{42} \approx 5.14, \frac{18}{4}\right\} \leq d_{GB} \leq \min\{8, 6\}.$$

This gives the bound $5 \leq d_{GB} \leq 6$. Next, we use (IV.6) to improve the lower bound $\frac{18}{4}$ given above. Note that as we mentioned earlier all the $(u(x), v(x)) \in C_1$ that are equivalent to an X -normalizer satisfy

$$(a) \quad u(x)p(x) + v(x) \equiv 0 \pmod{x^n - 1}$$

or

$$(b) \quad u(x)p(x) + v(x) \not\equiv 0 \pmod{x^n - 1} \text{ and } h(x) \mid u(x)p(x) + v(x).$$

Moreover, all satisfying (b) have the property that $5 < \text{wt}(u(x), v(x))$ by the above lower bound. All $(u(x), v(x))$ satisfying (a) have the property that $v(x) = u(x)p(x)$ and

$$18 \leq 2\text{wt}(u(x)p(x)) + 4\text{wt}(u(x)).$$

If $\text{wt}(u(x)) \leq 3$, then $\text{wt}(v(x)) \geq 3$ and thus $6 \geq \text{wt}((u(x), v(x)))$. If $\text{wt}(u(x)) = 4$, then $\text{wt}(v(x)) \geq 2$ and again $6 \geq \text{wt}((u(x), v(x)))$. Finally, If $\text{wt}(u(x)) = 5$, then $\text{wt}(v(x)) \geq 1$ (because $u(x) = 0$ iff $u(x)p(x) = 0$) and again $6 \geq \text{wt}((u(x), v(x)))$.

Therefore for all vectors satisfying either (a) or (b) we have $6 \geq \text{wt}((u(x), v(x)))$ which implies $6 \leq d_{GB}$. Combining it with the previous bound, we obtain $d_{GB} = 6$ and this is a $[[54, 4, 6]]$ GB code.

It should also be noted that $((1+x)f(x), (1+x)f(x)p(x)) = (1+x^3, 1+x^{21})$ is a weight four stabilizer and hence this GB code is a degenerate code.

As we saw in the previous examples, our distance bound is capable of giving a lower bound that goes beyond the degeneracy of the code. There are not many such distance bounds for quantum LDPC codes, or specifically for GB codes, in the literature. To the best of our knowledge, this is the only bound capable of providing both upper and lower bounds on the minimum distance, or even determining the exact minimum distance, for GB codes with varying dimensions, and also surpassing classical methods by accounting for degeneracy.

In the next section, we apply the minimum distance bound discussed in this section in order to form two families of GB codes with dimension two, where each check qubit is connected to four physical qubits. We also use the distance bounds to reveal some interesting properties of such codes.

We conclude this section by noting that, as illustrated in the previous examples, although the main focus of our work is on GB codes with dimension two, the proposed minimum distance bound is also capable of identifying the true minimum distance in the case of GB codes with dimension greater than two. Hence a careful design of GB codes using this minimum distance may also result in other families of quantum codes with higher dimensions.

V. EXISTENCE, LOGICAL OPERATORS, AND HOOK ERRORS IN $[[d^2 + 1, 2, d]]$ GB CODE WITH ODD d

In this section, we present a new algebraic proof for the minimum distance of the GB family $[[d^2 + 1, 2, d]]$ for each odd integer d , using the technique developed in the previous section. This

sheds light on the structure of GB codes and opens up new perspectives for systematically constructing other families of GB codes. As we mentioned earlier, this GB family was recently discussed in [24] using a graph-theoretical approach, and was previously considered in [21]. However, our approach is different, and the following subsection reveals some new applications of our algebraic perspective.

First recall that a quantum code with stabilizer matrix H is called (w_c, w_r) -regular, if each column and each row of H have weights w_c and w_r , respectively. In general, quantum codes with smaller w_c and w_r are desirable because that implies the application of less gates to extract the syndrome. In reality, those gates are noisy so having too much of them may introduce too many errors, significantly hindering the true performance of the code.

Recall also that, all the weight two polynomials of length n belong to the length n cyclic code $\langle(1-x)\rangle$.

In general, GB codes constructed from two polynomials of weight two can have different dimensions. In this section, we only consider the case when the GB code corresponding to two polynomials $a(x)$ and $b(x)$ has dimension two or equivalently when $\langle a(x), b(x) \rangle = \langle(1-x)\rangle$. We define $P_n(x) = \frac{x^n - 1}{x - 1} = 1 + x + \dots + x^{n-1}$ over $\mathbb{F}_2[x]$.

First we need some preliminary results.

Lemma V.1. *Let $d \geq 1$ be a positive odd integer and $n = \frac{d^2+1}{2}$.*

1. *The inverse of the polynomial $P_d(x)$ modulo $x^n - 1$ and modulo $P_n(x)$ is $xP_d(x^d)$. In particular, the polynomial $P_d^{-1}(x)$, in both cases, has weight d .*

2. *We have*

$$P_n = P_d(x)(1 + x^d + x^{2d} + \dots + x^{d(\frac{d-1}{2}-1)}) + (x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1}).$$

Proof. First, we compute the product of $P_d(x)P_d(x^d)$ in $\mathbb{F}_2[x]$. Recall that $2n = d^2 + 1$. Then we have

$$P_d(x)P_d(x^d) = \frac{1+x^d}{1+x} \frac{1+x^{d^2}}{1+x^d} = \frac{1+x^{d^2}}{1+x} \quad (\text{V.1}) \\ = 1 + x + \dots + x^{2n-2}.$$

Thus

$$P_d(x)(xP_d(x^d)) \equiv (x + x^2 + \dots + x^{n-1}) \\ + (1 + x + x^2 + \dots + x^{n-1}) \equiv 1 \pmod{x^n - 1}$$

and

$$P_d(x)(xP_d(x^d)) \equiv (x + x^2 + \dots + x^{n-1}) \\ + x^n(1 + x + x^2 + \dots + x^{n-1}) \\ \equiv 1 \pmod{P_n(x)}.$$

The last part of (1) follows by counting the number of terms in $xP_d(x^d)$, which is d .

The second part follows from a straightforward calculation. \square

Now we give an algebraic proof for the existence of the GB family $[[d^2+1, 2, d]]$ for each odd integer $d \geq 3$.

Theorem V.2. *Let $d \geq 3$ be an odd integer. Then there exists a family of $[[d^2+1, 2, d]]$ which is $(2, 4)$ -regular. Except for $d = 3$, all such codes are degenerate to 4.*

Proof. Let $d \geq 3$ be a positive odd integer and $n = \frac{d^2+1}{2}$. Fix $f(x) = 1 + x$ and $f(x)P_d(x)$ as the corresponding polynomials of the GB code. Note that using Lemma V.1 we have:

$$P_n = P_d(x)s(x) + r(x), \quad (\text{V.2})$$

where $s(x) = (1 + x^d + x^{2d} + \dots + x^{d(\frac{d-1}{2}-1)})$ and $r(x) = (x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1})$. To compute the parameters of such GB code, we use the result of Theorem IV.1. In particular such GB code has parameters $[[2n, 2, d_{GB}]]$, where

$$\min\{\frac{2n}{d+1}, \frac{n}{d+1}\} \leq d_{GB} \leq \min\{d+1, d\}.$$

Here we used the fact that the cyclic code generated by $P_n(x) = \frac{x^n-1}{x-1}$ has distance n (repetition code of length n). Hence we get

$$d \leq d_{GB} \leq \min\{d+1, d\},$$

which implies that $d_{GB} = d$. Moreover, this code has logical operators of weights d and $d+1$.

As all the stabilizer generators of such GB codes have weight four. Hence the degeneracy claim follows immediately. \square

Later, we prove that all such $[[d^2+1, 2, d]]$ GB codes have girth 8 except when $d = 3$, where the girth is 6.

1. Logical Pauli and CNOT operators of $[[d^2+1, 2, d]]$ GB codes

Let D be the $2 \times 2n$ matrix with the rows $v_1 = [1, 1, \dots, 1, 0, 0, \dots, 0]$ and $v_2 = [0, 0, \dots, 0, 1, 1, \dots, 1]$, then for each $u \in \mathbb{F}_2^{2n}$, the encoded logical state corresponding to u in such quantum codes, up to a normalizer constant, is defined by

$$|u\rangle_L = \sum_{c \in C_2} |c + (uD)\rangle. \quad (\text{V.3})$$

In particular, the four logical states are $|00\rangle_L = \sum_{c \in C_2} |c\rangle$, $|10\rangle_L = \sum_{c \in C_2} |c + v_1\rangle$, $|01\rangle_L =$

$$\sum_{c \in C_2} |c + v_2\rangle, \text{ and } |11\rangle_L = \sum_{c \in C_2} |c + v_1 + v_2\rangle.$$

Thus the logical operators XI , IX , and XX (respectively ZI , IZ , and ZZ) can be achieved by operating on n or $2n$ qubits. However, by applying the discussion in the proof of Theorem V.2, one can identify more optimal choices for such operations, requiring interaction with fewer qubits.

Theorem V.3. *In the $[[d^2+1, 2, d]]$ GB code with an odd d , one can perform X -logical operators as follows.*

- XI by performing $(u(x), v(x))$ (or any cyclic shift of it),
- XX by performing $(xv(x^d), u(x^d))$ (or any cyclic shift of it),
- IX by performing $(1, P_d(x))$ or $(P_d(x)^{-1}, 1)$ (or any cyclic shift of them),

where

$$u(x) = 1 + x^d + x^{2d} + \dots + x^{(\frac{d-1}{2}-1)d}$$

and

$$v(x) = x^{n-\frac{d+1}{2}} + x^{n-\frac{d+1}{2}+1} + \dots + x^{n-1}.$$

The first two operators require interaction with d and the last one with $d+1$ data qubits, and all are optimal in this sense.

Proof. As we showed in the proof of Theorem V.2, for $u(x) = 1 + x^d + x^{2d} + \dots + x^{(\frac{d-1}{2}-1)d}$, the vector $(u(x), v(x) = u(x)P_d(x) + P_n(x))$, which has weight d , is a logical operator. Hence it can be chosen as XI logical operator. Moreover, (V.2) implies

$$\begin{aligned} P_n(x) &= P_d(x)u(x) + v(x) = \\ &P_d(x)(1 + x^d + x^{2d} + \dots + x^{d(\frac{d-1}{2}-1)}) \\ &+ (x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1}). \end{aligned}$$

Substituting x with x^d and multiplying both sides by x (and computing modulo $x^n - 1$) implies that

$$\begin{aligned} P_n(x) &= xP_d(x^d)u(x^d) + xv(x^d) \\ &= P_d(x)^{-1}u(x^d) + xv(x^d). \end{aligned}$$

Hence $(u(x^d)P_d(x)^{-1} + P_n(x), u(x^d)) = (xv(x^d), u(x^d))$ is also a logical operator. This operation has different parity in compare to the logical operation corresponding to XI (their sum is not a stabilizer). So we choose it to be XX . Finally, note that $(u(x), v(x)) + (xv(x^d), u(x^d))$ has an odd weight vector in the first and the second component. So the minimum weight of a logical IX operator is at least $d+1$. Indeed, one can fix the operation IX to be $(1, P_d(x))$ or $(P_d(x)^{-1}, 1)$. \square

Note that so far we have only talked about logical X -operators above. Since each X -stabilizer (or X -normalizer) of the form $(a(x), b(x))$ is equivalent, via a one-to-one mapping, to $(b(x^{-1}), a(x^{-1}))$, which is a Z -stabilizer (or Z -normalizer), one can apply the result of Theorem V.3 to obtain minimum-weight candidates for implementing the logical operators ZI , IZ , and ZZ .

Next we show that logical CNOT operator, i.e., the CNOT gate between the two logical qubits, can be done at “zero cost” by solely permuting (relabeling) the data qubits. Such permutation technique previously studied in the literature [22, 23] for general quantum codes and it is distinct from other fault-tolerant approaches such as transversal gates and lattice surgery. Recall that in the $[[d^2 + 1, 2, d]]$ GB family, each data qubit has a label from

$$\mathbb{Z}_n \times \mathbb{Z}_n = \{0, 1, \dots, n-1\} \times \{0, 1, \dots, n-1\}.$$

So each vector in $\mathbb{F}_2^n \times \mathbb{F}_2^n$ can be expressed as $(a(x), b(x)) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle \times \mathbb{F}_2[x]/\langle x^n - 1 \rangle$. We will take advantage of the following permutations in the next theorem:

$$S((a(x), b(x))) \rightarrow (b(x), a(x)),$$

$$E_d((a(x), b(x))) \rightarrow (a(x^d), b(x^d)),$$

and

$$\Pi_{1,0}((a(x), b(x))) \rightarrow (xa(x), b(x)),$$

where the first permutation swaps the first n components with the second n components, the second permutation send the element in coordinate i to $(d \times i) \bmod n$, and the third one applies a cyclic shift to the first component.

Theorem V.4. *Let d be a positive odd integer. In the GB family $[[d^2 + 1, 2, d]]$, the logical operator CNOT can be implemented by applying the permutation $\Pi_{1,0}E_dS$.*

Proof. Let $O = \Pi_{1,0}E_dS$. It acts as

$$O((u(x), v(x))) = (xv(x^d), u(x^d)).$$

The operator O maps each X -stabilizer generator $(x^i(1+x), x^i(1+x^d))$ to another stabilizer generator namely $(x^{id+1}(1+x^{d^2}), x^{id}(1+x^d))$, where, using the fact that $d^2 \equiv -1 \pmod{n}$, it can be equivalently represented as $(x^{id}(1+x), x^{id}(1+x^d))$ which is another X -stabilizer. Since $\gcd(n, d) = 1$, this permutation gives a one-to-one mapping of the stabilizer generators. Therefore, using (V.3), one can verify that O , at the logical level, maps

- $|00\rangle \rightarrow |00\rangle$.
- $|01\rangle \rightarrow |01\rangle$ because applying O to $(1, P_d(x))$ gives $(P_d(x)^{-1}, 1)$.
- $|10\rangle \leftrightarrow |11\rangle$ because it swaps the first two operators given in Theorem V.3.

Hence O acts as CNOT at the logical level.

2. Hook error and the effective weight

Correlated errors that occur during the measurement of stabilizer generators during quantum error correction can reduce the effective minimum distance of a quantum code by forming a logical error at a lower cost [37–41].

A particularly dangerous class of syndrome measurement circuit faults arises when a single check qubit error propagates through syndrome extraction circuit, i.e., entangling operations such as CNOT gates, causing multiple data qubit errors, see Figure 1. These errors are especially problematic because they can form a logical error at lower cost, if these two data qubit errors align with a minimum weight logical error (bad hooks), making them harder to detect and correct. Therefore, avoiding bad hook errors can enhance the overall performance of an error-correcting code. Following the approach of [41], we define *effective distance* of a quantum, GB, code to be the minimum number of physical (both data and check) errors required for an undetectable logical error. Also, it should be emphasized that only check qubit errors propagating to data qubits can reduce the effective distance, as data qubit errors never spread to neighboring data qubits.

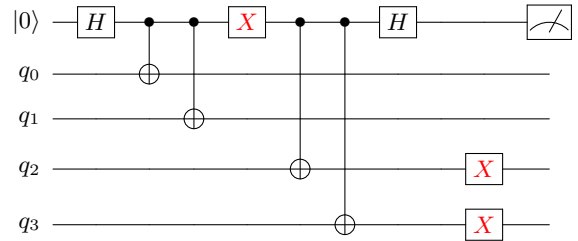


Figure 1: An example of a hook error, where one error on the check qubit (top qubit) spreads to two data qubits (q_2 and q_3).

In this section, we present a syndrome extraction pattern for the $[[d^2 + 1, 2, d]]$ family in which hook errors do not reduce the minimum distance of the code. Our approach is based on the minimum distance bounds developed in the previous sections. Since applying a permutation to all X -stabilizers yields all Z -stabilizers, we restrict our discussion to the former type. It is important to note that a general syndrome extraction pattern for such GB family is not necessarily immune to hook errors. Indeed, at the end of this section we provide an example of a syndrome extraction pattern in which hook errors align with the structure of minimum-weight logical errors, thereby reducing the effective distance of the code.

First recall that there exists a basis of the X -stabilizer group which consists of $x^i(1+x, 1+x^d)$, for each $0 \leq i \leq n-2$. So, in order to extract the

syndrome, one needs to only operate on such basis with the aid of $n-1$ check qubits. Moreover, recall that the i -th check qubit acts as $x^i(1+x, 1+x^d)$, namely it acts on physical qubits $i, i+1$ (corresponding to $x^i + x^{i+1}$ so called left qubits) and $x^i + x^{i+d}$ (corresponding to $x^i + x^{i+d}$ so called right qubits). Thus if we represent the first n qubits by q_0, q_1, \dots, q_{n-1} , and the second n qubits by $q'_0, q'_1, \dots, q'_{n-1}$, we conclude that the i -th check operates on q_i, q_{i+1}, q'_i , and q'_{i+d} .

The syndrome extraction order that we choose is to first operate as $(0, x^i(1+x^d))$ and then $(x^i(1+x), 0)$. We call such order *Right-Left (RL)* and it is shown in Figure 2. This pattern implies that

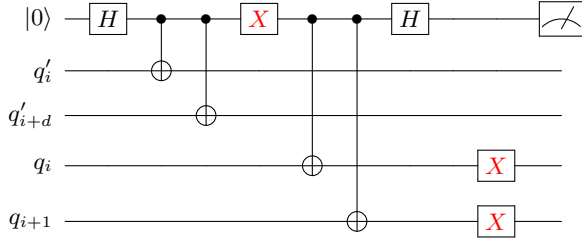


Figure 2: RL extraction pattern for the i -th check qubit corresponding to $x^i(1+x, 1+x^d)$ X-stabilizer, and propagation of an error.

all the hook errors resulted from a single error in the check qubit will be in the form of $(x^i(1+x), 0)$ for some $0 \leq i \leq n-2$. All other type single errors on a check qubits can be translated to an equivalent single data qubit error. So we discard them in our conversation as they do not induce error propagation. An arbitrary combination of hook errors has the form $(e(x)(1+x), 0)$ for some $e(x) \in \mathbb{F}_2[x]/\langle x^n-1 \rangle$. The number of errors in the check qubits, in order to obtain such combination, is $\text{wt}(e(x))$.

Next we show that such errors would not reduce the minimum distance of the GB codes under discussion. Recall that effective minimum distance of a code is less than or ideally equal to its theoretical minimum distance.

Theorem V.5. *Let $d \geq 3$ be an odd integer. Then the GB family $[[d^2+1, 2, d]]$ has effective distance d if all the syndrome extractions are performed using RL pattern.*

Proof. Recall that $n = \frac{d^2+1}{2}$. Let $e = (u(x), v(x)) + (j(x)(1+x), 0)$ be a non-trivial logical error implied by $\text{wt}(j(x))$ check qubits errors, and the arbitrary $(u(x), v(x))$ error on the data qubits. Hence the number of errors required to obtain e is $\text{wt}(j(x)) + \text{wt}(u(x)) + \text{wt}(v(x))$, and we show that it is at least d . We will use the argument developed in Section IV.

Recall from (IV.1) that such error satisfies

$$(1+x)(P_d(x)(j(x)(1+x) + u(x)) + v(x)) \equiv 0 \pmod{x^n-1}.$$

Hence two cases can happen:

$$(P_d(x)(j(x)(1+x) + u(x)) + v(x)) \equiv 0 \pmod{x^n-1}$$

or

$$(P_d(x)(j(x)(1+x) + u(x)) + v(x)) \equiv P_n(x) \pmod{x^n-1}.$$

First we consider the former case. Recall that, as we showed in Lemma V.1, we have

$$P_n = P_d(x)(1+x^d+x^{2d}+\dots+x^{d(\frac{d-1}{2}-1)}) + (x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1}).$$

Multiplying all sides by $j(x)(1+x) + u(x)$ implies that

$$P_n = v(x)(1+x^d+x^{2d}+\dots+x^{d(\frac{d-1}{2}-1)}) + (j(x)(1+x) + u(x))(x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1}).$$

Next we bound the weight of right hand side using the left one. In particular, using the fact that $(1+x)(x^{d\frac{d-1}{2}} + x^{d\frac{d-1}{2}+1} + \dots + x^{n-1})$ has weight two, we have

$$\begin{aligned} n &\leq \frac{d-1}{2} \text{wt}(v(x)) + \frac{d+1}{2} \text{wt}(u(x)) + 2\text{wt}(j(x)) \\ &\leq \frac{d+1}{2} (\text{wt}(j(x)) + \text{wt}(u(x)) + \text{wt}(v(x))). \end{aligned}$$

Therefore,

$$d \leq \text{wt}(j(x)) + \text{wt}(u(x)) + \text{wt}(v(x))$$

which implies that the number of faults should be at least d in order to achieve such logical operator.

Next we consider the second possibility above. Again calculating the weights of the sides implies

$$\begin{aligned} n &\leq 2\text{wt}(j(x)) + d\text{wt}(u(x)) + \text{wt}(v(x)) \\ &\leq d(\text{wt}(j(x)) + \text{wt}(u(x)) + \text{wt}(v(x))). \end{aligned}$$

which again implies that

$$d \leq \text{wt}(j(x)) + \text{wt}(u(x)) + \text{wt}(v(x)).$$

Thus this GB family has effective distance d .

It should be noted that replacing the RL extraction with LR implies the same result as above. It is mainly because that each stabilizer in the form of $x^i(1+x, 1+x^d)$ can be decomposed as $(x^i(1+x), 0) + (0, x^i(1+x^d))$. Therefore, RL extraction preserves the minimum distance if and only if LR also preserves the minimum distance.

Our computations show that replacing the RL extraction with other syndrome extraction patterns can reduce the effective minimum distance to approximately half of the theoretical minimum distance. One example of such patterns is to first operate as (x^i, x^i) and then as (x^{i+1}, x^{i+d}) , and one can obtain the corresponding circuit by swapping the order of two middle CNOTs in Figure 2. In this case, our computations, employed in Magma Computer Algebra System [42], for $3 \leq d \leq 11$ show that the effective minimum distance of such GB codes is $\lceil \frac{d}{2} \rceil$.

VI. THE FAMILY OF $[[d^2, 2, d]]$ GB CODE WITH EVEN d

Although the odd-distance GB code discussed in the previous section has been considered in the literature, the existence of an even-distance GB code family of the form $[[d^2, 2, d]]$ has been overlooked [14]. Moreover, around the same time as us, a graph theoretical proof for the existence of such family was proposed in [24]. However, the foundation of our discussions is based on algebraic properties of GB codes.

In this section, we follow similar steps to those in the previous section to construct this family. First, we need the following lemma. Recall that $P_n(x) = 1 + x + \dots + x^{n-1}$.

Lemma VI.1. *Let d be a positive even integer and $n = \frac{d^2}{2}$. Then the following holds.*

1. $P_{d+1}(x)$ is invertible and

$$\begin{aligned} P_{d+1}(x)^{-1} &\equiv x(1 + x^{d+1} + x^{2(d+1)} + \dots \\ &+ x^{(\frac{d}{2}-1)(d+1)}) + x^{\frac{d}{2}+1}(1 + x^{d+1} + x^{2(d+1)} + \dots \\ &+ x^{(\frac{d}{2}-2)(d+1)}) \pmod{x^n - 1}. \end{aligned}$$

Moreover, $\text{wt}(P_{d+1}(x)^{-1}) = d - 1$.

2. We have

$$\begin{aligned} P_n &= P_{d+1}(x)(x^{\frac{d}{2}+1})(1 + x^{d+1} + x^{2(d+1)} + \dots \\ &+ x^{(\frac{d}{2}-2)(d+1)}) + (1 + x + x^2 + \dots + x^{\frac{d}{2}}) \end{aligned}$$

and

$$\begin{aligned} P_n &= P_{d+1}(x)^{-1}(1 + x + x^2 + \dots + x^{(\frac{d}{2}-1)}) \\ &+ (1 + x^{d+1} + x^{2(d+1)} + \dots + x^{(\frac{d}{2}-1)(d+1)}). \end{aligned}$$

Proof. The proof follows from a straightforward calculation modulo $x^n - 1$.

Next we use the result of Theorem IV.1 to prove the existence of $[[d^2, 2, d]]$ family of GB code, where all the stabilizer generators have weight four.

Theorem VI.2. *Let $d \geq 4$ be an odd integer. Then there exists a family of $[[d^2, 2, d]]$ which is $(2, 4)$ -regular. All such codes are degenerate to 4, except when $d = 4$.*

Proof. Consider the GB code with the associated polynomials $f(x) = 1 + x$ and $f(x)P_{d+1}(x)$. The proof follows in a similar fashion as the proof of Theorem V.2, except the argument about the minimum distance. Therefore, we only prove the claim about the minimum distance.

Let d_{GB} be the minimum distance of such code. Using the above lemma, we have $\text{wt}(P_{d+1}(x)) = d + 1$, $\text{wt}(P_{d+1}(x)^{-1}) = d - 1$, and

$$P_n = P_{d+1}(x)^{-1}s(x) + r(x),$$

where $\text{wt}(s(x)) = \frac{d}{2}$ and $\text{wt}(r(x)) = \frac{d}{2}$.

Applying the minimum distance bounds given in Theorem IV.1 implies that

$$\min\left\{\frac{2dn}{d(d+1)}, \frac{n}{\frac{d}{2}}\right\} \leq d_{GB} \leq \min\{d+2, d, d\}$$

which implies that

$$\min\left\{\frac{d^2}{(d+1)}, d\right\} \leq d_{GB} \leq \min\{d\}.$$

Therefore, $d - 1 < d_{GB} \leq d$, which forces the minimum distance to be $d_{GB} = d$. The degeneracy part follows immediately as the stabilizer generators all have weight four.

In the previous section, Theorem V.5, we showed that the RL syndrome extraction pattern implies the effective minimum distance equal to the theoretical minimum distance for the $[[d^2 + 1, 2, d]]$ GB family. The following theorem shows the same outcome for the GB family discussed in this section.

Theorem VI.3. *Let $d \geq 4$ be an even integer. Then the $[[d^2, 2, d]]$ GB family has effective distance d considering the RL pattern syndrome extraction.*

Proof. The proof follows from an argument similar to that of Theorem V.5.

It is worth noting that low-weight logical X and Z operators for this family of GB codes can also be found using the approach described in Section V.1. Therefore, we omit such discussions here.

VII. GIRTH AND CODE-CAPACITY THRESHOLDS OF GB CODES

A. Girth of GB codes

In graph theory, the *girth* of a graph provides a fundamental measure of its cyclic structure. Let

$G = (V, E)$ be an undirected graph, where V represents the set of vertices and E the set of edges. Then, the *girth* of G , denoted as $g(G)$, is the length of the shortest cycle in the graph. The girth is a critical parameter because it directly impacts the performance of message-passing decoders, such as belief propagation (BP) [43]. Since many qLDPC codes are decoded using a post-processing algorithm followed by BP, making the former more robust makes decoders to be more accurate and faster.

The importance of girth arises from the role of cycles in the Tanner graph during iterative decoding. In the absence of cycles, message-passing algorithms can achieve optimal performance, as messages propagated along the graph remain uncorrelated and independent. However, the presence of cycles introduces correlation effects, where messages can traverse a cycle and return to their origin, creating feedback loops that distort the reliability of the decoding process. Shorter cycles exacerbate this problem, as they allow correlations to build up more quickly, degrading the decoder's performance [29]. For generalized bicycle codes, the girth is closely tied to the algebraic properties of the code (the corresponding polynomials), and careful design can yield Tanner graphs with desirable cyclic properties.

In this section, we analyze the girth conditions for generalized bicycle codes by studying the cyclic structure of their Tanner graphs. Specifically, we characterize all codes with girths 4, 6, and 8 which is the maximum possible girth of a GB code.

Theorem VII.1. *Let $a(x)$ and $b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ be two polynomials that define a GB code. The Tanner graph associated with this code has girth $g(G) = 4$ if and only if there exist indices $i, j \neq j' \in \{0, 1, \dots, n-1\}$ such that at least one of the following conditions holds:*

- $a_j = a_{j+i} = 1$ and $a_{j'} = a_{j'+i} = 1$,
- $b_j = b_{j+i} = 1$ and $b_{j'} = b_{j'+i} = 1$,
- $a_j = b_{j+i} = 1$ and $a_{j'} = b_{j'+i} = 1$,

where all indices are taken modulo n .

The conditions for a GB code to have girth six is summarized below.

Theorem VII.2. *Let $a(x), b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ be two polynomials that define a GB code. The Tanner graph associated with this code has girth $g(G) = 6$ if and only if there exist indices $i \neq j, \ell, \ell', \ell'' \in \{0, 1, \dots, n-1\}$ such that at least one of the following conditions holds:*

- $a_\ell = a_{\ell+i} = 1$, $a_{\ell'} = a_{\ell'+j} = 1$ and $a_{\ell''} = a_{\ell''+i+j} = 1$
- $b_\ell = b_{\ell+i} = 1$, $b_{\ell'} = b_{\ell'+j} = 1$ and $b_{\ell''} = b_{\ell''+i+j} = 1$

- $a_\ell = a_{\ell+i} = 1$, $a_{\ell'} = a_{\ell'+j} = 1$ and $b_{\ell''} = b_{\ell''+i+j} = 1$.
- $b_\ell = b_{\ell+i} = 1$, $b_{\ell'} = b_{\ell'+j} = 1$ and $a_{\ell''} = a_{\ell''+i+j} = 1$.

where all indices are taken modulo n .

Next we show that the girth of a GB code cannot exceed eight. The proof follows in two steps. First we have the following lemma.

Lemma VII.3. *Let $a(x) = 1 + x^i$ and $b(x) = x^j + x^{j+k}$ be two polynomials with weight two in $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$. Then, the girth of the Tanner graph associated with the GB code defined by $a(x)$ and $b(x)$ satisfies $g(G) \leq 8$.*

The following corollary is a straightforward consequence of the previous Lemma.

Corollary VII.4. *Let $a(x)$ and $b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ with weights at least two. Then, the girth of the Tanner graph associated with such GB code satisfies $g(G) \leq 8$.*

Using the above results, one can show that the girth eight case is achievable by the GB codes discussed in Sections V and VI. In particular, these GB codes do not satisfy the conditions of Theorems VII.1 and VII.2. Hence Corollary VII.4 implies that they have girth eight.

B. Code capacity thresholds

The algebraic structure, low connectivity, and high Tanner graph girth of the GB families discussed in Sections V and VI indicate that they can potentially have high thresholds. Motivated by this, we extracted the logical error rate as a function of physical error rate for these two families of GB codes.

First, we analyzed the performance of GB codes in terms of the logical error probability p_{\log} , defined as the probability that the decoder fails to correctly identify an error given its syndrome, as a function of the physical error probability $p_{\text{phys}} = p_X + p_Y + p_Z$, using the BP-OSD and MWPM decoders [4, 44]. MWPM can be used because the GB codes have a matching structure, i.e. the syndromes triggered by errors have weight two. We adopt an independent and identically distributed depolarizing error model, where each physical qubit independently experiences one of the three nontrivial Pauli errors with equal probability $p_X = p_Y = p_Z = \frac{p_{\text{phys}}}{3}$, where p_{phys} is the total probability of a physical error.

To estimate the logical error rate p_{\log} as a function of p_{phys} , a Monte Carlo simulations were employed. For each code instance, the logical failure rate under the mentioned decoders was estimated across a range of physical error rates, where

$10^{-4} \leq p_{\text{phys}} \leq 10^{-0.1} \approx 0.79$, using 10^5 repeated trials. This procedure was carried out using the open-source package `qLDPC` [45], where the decoders are based on the packages `ldpc` [46] and `Pymatching` [44].

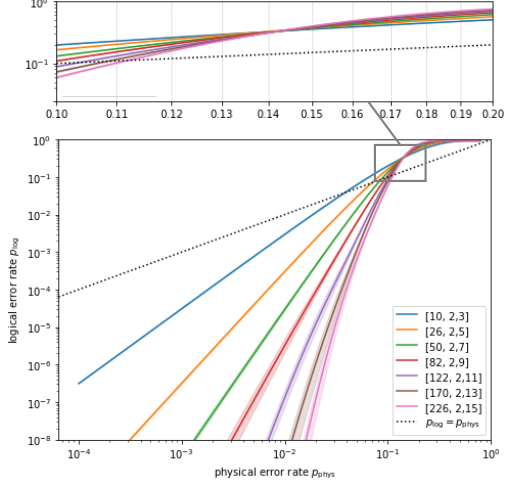


Figure 3: Logical versus physical error rate for $[[d^2 + 1, 2, d]]$ GB family and odd d using BP-OSD. Wide view shows the full range of error rates, while close-up focuses on the threshold region.

It should be mentioned that a code capacity threshold of about 15% was previously reported for another family of GB codes with the check connectivity six, under depolarizing noise, and using the BP-OSD decoder [4, Figure 9].

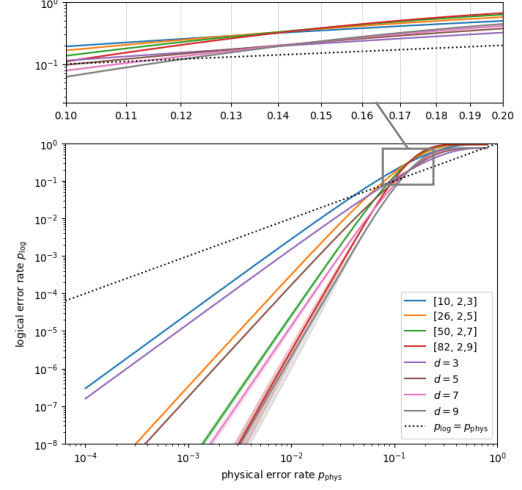


Figure 5: Logical versus physical error rate for $[[d^2 + 1, 2, d]]$ GB family and odd d compared to rotated surface codes of the same distance (showed by $d = 3, 5, 7, 9$). Wide view shows the full range of error rates, while close-up focuses on the threshold region.

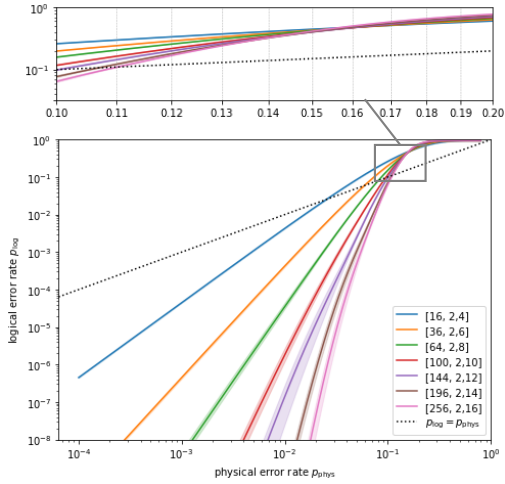


Figure 4: Logical versus physical error rate for $[[d^2, 2, d]]$ GB family and even d using BP-OSD. Wide view shows the full range of error rates, while close-up focuses on the threshold region.

The resulting functions based on BP-OSD decoder are illustrated in Figures 3 and 4, corresponding to the GB code families described in Sections V and VI, respectively. As evidenced by the plots, an estimated threshold of approximately 14.5% is observed for the odd-distance family, while the even-distance family exhibits a threshold near 16%.

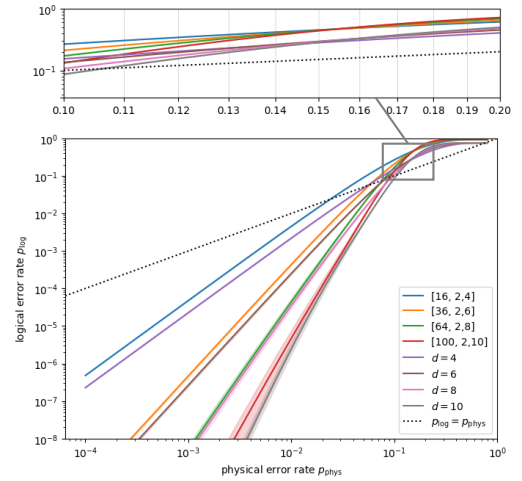


Figure 6: Logical versus physical error rate for $[[d^2, 2, d]]$ GB family and even d compared to rotated surface codes of the same distance (showed by $d = 4, 6, 8, 10$). Wide view shows the full range of error rates, while close-up focuses on the threshold region.

We also compared the performance of the GB code families with that of the rotated surface code having the same minimum distance, under the same noise model and MWPM decoder [44, 47]. For further details on the performance of surface

codes under various decoders and noise models, see [43]. The results, shown in Figures 5 and 6, indicate comparable performance. Specifically, the odd-distance GB family achieves a threshold of approximately 14%, which is nearly identical to that of the surface code. For the even-distance GB family, the threshold is around 15.5%, also closely matching the performance of the surface code.

The close similarity in threshold performance between GB codes and surface codes highlights the strong potential of GB codes, making them alternative candidates for fault-tolerant quantum computing. This result is particularly interesting considering the better rate, low-weight parity checks, and highly regular structure of GB codes, which may facilitate more efficient hardware implementation while preserving threshold performance comparable to that of surface codes.

VIII. CONCLUSION AND FUTURE DIRECTIONS

In this work, we first established a natural connection between GB codes and additive cyclic codes over \mathbb{F}_4 . We then proposed novel minimum distance bounds for certain GB codes, enabling us to demonstrate the existence of two families of highly degenerate GB codes with parameters $[[d^2 + 1, 2, d]]$ for odd $d \geq 3$ and $[[d^2, 2, d]]$ for even $d \geq 4$, both exhibiting check-connectivity four. We analyzed the structure of specific logical operators within the first family, identifying configurations that require only minimal interaction or simple relabeling of physical qubits.

A syndrome extraction pattern was proposed for both families, ensuring that the effective distance of the code remains equal to its theoretical distance even in the presence of check qubit errors. We also characterized all possible girths for GB codes, showing that these two families attain the

maximum girth achievable within the GB family.

Finally, we evaluated the code capacity performance of these GB families under depolarizing noise using both BP-OSD and MWPM decoders. The matching structure of these codes is desirable, making it possible to efficiently decode those with fast decoders such as MWPM or BP plus Ordered Tanner Forest (BP+OTF) decoders [48]. The results indicate threshold behavior and performance comparable to those of rotated surface codes.

This work highlights two families of GB codes as promising candidates among a broader, largely unexplored family of GB codes. The observed threshold similarity with surface codes motivates future research into the systematic construction of additional GB code classes, potentially by means of a similar approach as of the distance bounds introduced in Section IV. We also plan to assess the performance of the proposed GB families under more realistic conditions, such as circuit-level noise models, and to study their connection to other related quantum code families.

IX. ACKNOWLEDGEMENT

This work has been supported by the Spanish Ministry of Economy and Competitiveness through the MADDIE project (Grant No. PID2022-137099NB-C44); and the Ministry of Economic Affairs and Digital Transformation of the Spanish Government through the QUANTUM ENIA project call - Quantum Spain project, and by the European Union through the Recovery, Transformation and Resilience Plan - NextGenerationEU within the framework of the “Digital Spain 2026 Agenda”. We would like to thank the members of the Quantum Information Group at Tecnun-University of Navarra for their support and valuable discussions.

-
- [1] Nikolas P Breuckmann and Barbara M Terhal. Constructions and noise threshold of hyperbolic surface codes. *IEEE transactions on Information Theory*, 62(6):3731–3744, 2016.
 - [2] O Higgott and NP Breuckmann. Constructions and performance of hyperbolic and semi-hyperbolic floquet codes. *arXiv preprint arXiv:2308.03750*, 2023.
 - [3] Alexey A Kovalev and Leonid P Pryadko. Quantum kronecker sum-product low-density parity-check codes with finite rate. *Physical Review A—Atomic, Molecular, and Optical Physics*, 88(1):012311, 2013.
 - [4] Pavel Panteleev and Gleb Kalachev. Degenerate quantum LDPC codes with good finite length performance. *Quantum*, 5:585, 2021.
 - [5] Hsiang-Ku Lin and Leonid P Pryadko. Quantum two-block group algebra codes. *Physical Review A*, 109(2):022407, 2024.
 - [6] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the block-length. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013.
 - [7] Sergey Bravyi, Andrew W Cross, Jay M Gambetta, Dmitri Maslov, Patrick Rall, and Theodore J Yoder. High-threshold and low-overhead fault-tolerant quantum memory. *Nature*, 627(8005):778–782, 2024.
 - [8] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. Good quantum LDPC codes with linear time decoders. In *Proceedings of the 55th Annual ACM Symposium on Theory of Comput-*

- ing, STOC 2023, page 905–918, New York, NY, USA, 2023. Association for Computing Machinery.
- [9] Louis Golowich and Venkatesan Guruswami. Quantum LDPC codes of almost linear distance via homological products. *arXiv e-prints*, page arXiv:2411.03646, November 2024.
 - [10] Anthony Leverrier and Gilles Zémor. Quantum Tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883, 2022.
 - [11] Ting-Chun Lin and Min-Hsiu Hsieh. Good quantum LDPC codes with linear time decoder from lossless expanders. *arXiv e-prints*, page arXiv:2203.03581, March 2022.
 - [12] Tibor Rakovszky and Vedika Khemani. The Physics of (good) LDPC Codes I. Gauging and dualities. *arXiv e-prints*, page arXiv:2310.16032, October 2023.
 - [13] Tibor Rakovszky and Vedika Khemani. The Physics of (good) LDPC Codes II. Product constructions. *arXiv e-prints*, page arXiv:2402.16831, February 2024.
 - [14] Renyu Wang and Leonid P Pryadko. Distance bounds for generalized bicycle codes. *Symmetry*, 14(7):1348, 2022.
 - [15] Hsiang-Ku Lin, Xingrui Liu, Pak Kau Lim, and Leonid P Pryadko. Single-shot and two-shot decoding with generalized bicycle codes. *arXiv preprint arXiv:2502.19406*, 2025.
 - [16] N Koukoulekidis, F Šimkovic IV, M Leib, and FRF Pereira. Small quantum codes from algebraic extensions of generalized bicycle codes (2024). *arXiv preprint arXiv:2401.07583*, 2024.
 - [17] Renyu Wang, Hsiang-Ku Lin, and Leonid P Pryadko. Abelian and non-abelian quantum two-block codes. In *2023 12th International Symposium on Topics in Coding (ISTC)*, pages 1–5. IEEE, 2023.
 - [18] Joshua Visslitz, Willers Yang, Sophia Fuhui Lin, Junyu Liu, Natalia Nottingham, Jonathan M Baker, and Frederic T Chong. Matching generalized-bicycle codes to neutral atoms for low-overhead fault-tolerance. *arXiv preprint arXiv:2311.16980*, 2023.
 - [19] Adam Siegel, Armands Strikis, and Michael Fogarty. Towards early fault tolerance on a $2 \times n$ array of qubits equipped with shuttling. *PRX Quantum*, 5(4):040328, 2024.
 - [20] Alexey A Kovalev, Ilya Dumer, and Leonid P Pryadko. Design of additive quantum codes via the code-word-stabilized framework. *Physical Review A—Atomic, Molecular, and Optical Physics*, 84(6):062319, 2011.
 - [21] Alexey A Kovalev and Leonid P Pryadko. Improved quantum hypergraph-product LDPC codes. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 348–352. IEEE, 2012.
 - [22] Markus Grassl and Martin Roetteler. Leveraging automorphisms of quantum codes for fault-tolerant quantum computation. In *2013 IEEE International Symposium on Information Theory*, pages 534–538. IEEE, 2013.
 - [23] Hasan Sayginel, Stergios Koutsoumpas, Mark Webster, Abhishek Rajput, and Dan E Browne. Fault-tolerant logical clifford gates from code automorphisms. *arXiv preprint arXiv:2409.18175*, 2024.
 - [24] François Arnault, Philippe Gaborit, and Nicolas Saussay. (2,2)-gb codes: Classification and comparison with weight-4 surface codes, 2025.
 - [25] François Arnault, Philippe Gaborit, and Nicolas Saussay. On the generalization of kitaev codes as generalized bicycle codes. *arXiv preprint arXiv:2504.18360*, 2025.
 - [26] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.
 - [27] A Robert Calderbank, Eric M Rains, PM Shor, and Neil JA Sloane. Quantum error correction via codes over $gf(4)$. *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.
 - [28] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Physical Review A*, 54(3):1862, 1996.
 - [29] Patricio Fuentes, Josu Etxezarreta Martinez, Pedro M. Crespo, and Javier Garcia-Frías. Degeneracy and its impact on the decoding of sparse quantum codes. *IEEE Access*, 9:89093–89119, 2021.
 - [30] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th annual ACM SIGACT symposium on theory of computing*, pages 375–388, 2022.
 - [31] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, 1996.
 - [32] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
 - [33] David JC MacKay, Graeme Mitchison, and Paul L McFadden. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory*, 50(10):2315–2330, 2004.
 - [34] Jürgen Bierbrauer and Yves Edel. Quantum twisted codes. *Journal of Combinatorial Designs*, 8(3):174–188, 2000.
 - [35] Reza Dastbasteh and Khalil Shivji. Polynomial representation of additive cyclic codes and new quantum codes. *Advances in Mathematics of Communications*, 19(1):49–68, 2025.
 - [36] Reza Dastbasteh and Petr Lisoněk. Additive twisted codes: new distance bounds and infinite families of quantum codes. *Designs, Codes and Cryptography*, pages 1–38, 2025.
 - [37] Austin G Fowler, Matteo Mariantoni, John M Martinis, and Andrew N Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A—Atomic, Molecular, and Optical Physics*, 86(3):032324, 2012.
 - [38] Yu Tomita and Krysta M Svore. Low-distance surface codes under realistic quantum noise. *Physical Review A*, 90(6):062320, 2014.
 - [39] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.
 - [40] György P Gehér, Campbell McLauchlan, Earl T Campbell, Alexandra E Moylett, and Ophelia

- Crawford. Error-corrected hadamard gate simulated at the circuit level. *Quantum*, 8:1394, 2024.
- [41] Argyris Giannisis Manes and Jahan Claes. Distance-preserving stabilizer measurements in hypergraph product codes. *Quantum*, 9:1618, 2025.
- [42] Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.
- [43] Antonio deMarti iOlius, Patricio Fuentes, Román Orús, Pedro M Crespo, and Josu Etzezarreta Martinez. Decoding algorithms for surface codes. *Quantum*, 8:1498, 2024.
- [44] Oscar Higgott. Pymatching: A python package for decoding quantum codes with minimum-weight perfect matching. <https://github.com/oscarhiggott/PyMatching>, 2021.
- [45] Michael A. Perlin. qLDPC. <https://github.com/qLDPCOrg/qLDPC>, 2023.
- [46] Joschka Roffe. LDPC: Python tools for low density parity check codes. <https://pypi.org/project/ldpc/>, 2022.
- [47] Austin G Fowler, Adam C Whiteside, and Lloyd CL Hollenberg. Towards practical classical processing for the surface code. *Physical review letters*, 108(18):180501, 2012.
- [48] Antonio deMarti iOlius, Imanol Etzezarreta Martinez, Joschka Roffe, and Josu Etzezarreta Martinez. An almost-linear time decoding algorithm for quantum LDPC codes under circuit-level noise. *arXiv e-prints*, page arXiv:2409.01440, September 2024.

Appendix A: Proofs of Section VII A

For the rest of this section, we label qubits in a GB codes corresponding to polynomials $a(x)$ and $b(x)$ with q_i and q'_i , respectively.

Proof. Theorem VII.1:

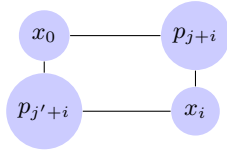


Figure 7: An example of a girth four. Here x_0 and x_i are check qubits, and the rest are data qubits.

Each cycle of length 4 is equivalent to a graph of shown in Figure 7. So we consider this graph as our base case and, WLOG, we assume that the 4 cycle is happening at check qubits 0 and i for some $1 \leq i \leq n-1$. Such cycle is in correspondence to $(a(x), b(x))$ and $(x^i a(x), x^i b(x))$. Such 4 cycle consists of two physical qubits p_{j+i} and p'_{j+i} . such physical qubits can be the label of non-zero coefficients of $a(x)$, $b(x)$, or one coefficient in $a(x)$ and one in $b(x)$. This gives precisely the three cases above. \square

Proof. Theorem VII.2:

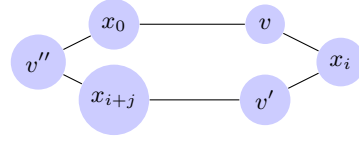


Figure 8: An example of a girth six. Here x_0 , x_i , and x_{i+j} are check qubits, and the rest are data qubits.

Again we consider the graph shown in Figure 8 as our base case, and base our reasoning using that. First, note that the case $i = j$ implies that the girth is four by Theorem VII.1. So we assume that $i \neq j$.

The connection between v , x_0 , and x_i implies that there exists $\ell \in \{0, 1, \dots, n-1\}$ such that $a_\ell = a_{\ell+i} = 1$ (or $b_\ell = b_{\ell+i} = 1$). In this case, $v = a_{\ell+i}$ (respectively $v = b_{\ell+i}$).

The connection between v' , x_i , and x_{i+j} implies that there exists $\ell' \in \{0, 1, \dots, n-1\}$ such that $a_{\ell'} = a_{\ell'+j} = 1$ (or $b_{\ell'} = b_{\ell'+j} = 1$). In this case, $v' = a_{\ell'+i+j}$ (respectively $v' = b_{\ell'+i+j}$).

Finally, the connection between v'' , x_{i+j} , and x_0 implies that there exists $\ell'' \in \{0, 1, \dots, n-1\}$ such that $a_{\ell''} = a_{\ell''+i+j} = 1$ (or $b_{\ell''} = b_{\ell''+i+j} = 1$). In this case, $v'' = a_{\ell''+i+j}$ (respectively $v'' = b_{\ell''+i+j}$).

A combination of the above possibilities give one of the four cases given in the theorem. \square

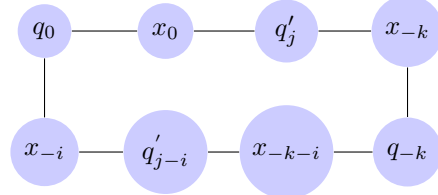
Proof. Lemma VII.3: Note that each check node x_t is connected to four physical qubits, namely:

$$q_t, \quad q_{t+i}, \quad q'_{t+j}, \quad q'_{t+j+k}.$$

More specifically, we have

- A qubit node q_t (corresponding to t -th coefficient of $a(x)$) is connected to check nodes x_t and x_{t-i} .
- A qubit node q'_t (corresponding to t -th coefficient of $b(x)$) is connected to check nodes x_{t-j} and x_{t-j-k} .

Now, we construct an explicit cycle of length 8 as:



Thus, $g(G) \leq 8$. \square

Proof. Corollary VII.4: The proof follows from the previous lemma and the fact that Tanner graph of such GB code has a subgraph which is the Tanner graph of the GB code of Lemma VII.3. \square