Distance bounds for generalized bicycle codes

Renyu Wang and Leonid P. Pryadko

Department of Physics & Astronomy, University of California, Riverside, California 92521, USA
(Dated: June 16, 2022)

Generalized bicycle (GB) codes is a class of quantum error-correcting codes constructed from a pair of binary circulant matrices. Unlike for other simple quantum code ansätze, unrestricted GB codes may have linear distance scaling. In addition, low-density parity-check GB codes have a naturally overcomplete set of low-weight stabilizer generators, which is expected to improve their performance in the presence of syndrome measurement errors. For such GB codes with a given maximum generator weight w, we constructed upper distance bounds by mapping them to codes local in $D \le w-1$ dimensions, and lower existence bounds which give $d \ge \mathcal{O}(n^{1/2})$. We have also done an exhaustive enumeration of GB codes for certain prime circulant sizes in a family of two-qubit encoding codes with row weights 4, 6, and 8; the observed distance scaling is consistent with $A(w)n^{1/2}+B(w)$, where n is the code length and $A(w)$ is increasing with w.

I. INTRODUCTION

In the last two years there was an enormous progress in the theory of quantum low-density parity-check (LDPC) codes[1–6]. Such code families, with bounded weight of stabilizer generators and distance scaling logarithmically or faster with the block length, generally have a finite fault-tolerant threshold to scalable error correction[7–9]. Unlike in the case of classical LDPC codes[10, 11] where sparse random matrices can be used to define the code, due to a commutativity constraint, an algebraic ansatz is required in the case of quantum LDPC codes. For over a decade, no construction was known to give distances larger than a square root of the block size n, up to a polylogarithmic factor[1, 7, 12–19]. The $\mathcal{O}\big(\sqrt{n}\operatorname{polylog} n\big)$ barrier was broken by Hastings, Haah, and O'Donnell[2] who demonstrated a code family with the distance $\mathcal{O}(n^{3/5}/\operatorname{polylog} n)$. Soon followed related constructions[3, 4], with Panteleev and Kalachev[5] finally proving the existence of asymptotically good bounded-stabilizer-generator-weight LDPC codes, with both the asymptotic rate and the asymptotic relative distance non-zero.

Unfortunately, the constructions in Refs. 1–5 do not come with an estimate for stabilizer generator weights sufficient for getting good quantum codes, or if they do, not one small enough to give practical codes. Further, these anzätse tend to produce rather long codes; shorter codes obtained this way may have parameters not as good as with constructions known earlier.

In comparison, generalized bicycle (GB) codes[15, 20], a generalization of the bicycle construction from Ref. 21, are particularly suited for constructing short codes, as a GB code can be constructed from a pair of linear cyclic codes which are only a factor of two shorter. Second, as we show in this work, a subset of codes from several well-studied families, most notably, quantum hypergraph-product (QHP) codes in two and higher dimensions[14, 17, 18], including the codes with finite asymptotic rates and power-law distance scaling, can be mapped to bicycle codes. At the same time, the distance bound $d \le n^{1/2}$ which limits the parameters of all QHP codes, does not apply to GB codes; we show in this work that this family includes codes with linear distances. Third, regular structure of GB codes simplifies both their implementation and linear-complexity iterative decoding[20, 22–24]. Moreover, GB codes have naturally overcomplete sets of minimum-weight stabilizer generators, which may improve their performance in the fault-tolerant (FT) setting. In spite of these advantages and the long history of GB codes, their properties have not been systematically studied.

The goal of this work is to investigate the parameters of GB codes, targeting highly-degenerate codes with distances much larger than the stabilizer generator weight which for practical codes should stay under $w_{\max} \simeq 10$. While some of the present distance bounds are an easy consequence of those obtained for related codes, or are obtained with well known methods, we believe a systematic review of available results is necessary. These results include Gilbert-Varshamov-style existence bounds for unrestricted GB codes, upper bounds for parameters of GB codes with row weight w obtained by a map to codes local in $D \le w-1$ dimensions, and several expicit constructions. Other results include an exact expression for the distance in terms of an associated asymmetric quantum code, a matching set of upper and lower distance bounds for $w=4$ bicycle codes, and a lower bound which guarantees the existence of long GB codes with the distance $\mathcal{O}(n^{1/2})$ for any fixed $w \ge 4$. We also studied the family of GB codes known to include codes with linear distances numerically, by exhaustively enumerating the corresponding binary GB codes with row weights $w=4$, 6 and 8, for circulant sizes $\ell \le 217$ with primitive root 2. Although we are not able to distinguish conclusively between a power-law distance scaling $d=\mathcal{O}(n^{\alpha})$ with $\alpha=1/2$ and $\alpha>1/2$, the results are consistent with square root distance scaling and a prefactor an increasing function of w.

The structure of the paper is as follows. First, in

Sec. II we give a brief summary of relevant facts from the theory of classical and quantum error-correcting codes, including some information on cyclic and quasi-cyclic codes. Analytical results are collected in Sec. III. Namely, Sec. III A gives general information about GB codes, Sec. III B collects several lower (existence) bounds on distances of unrestricted GB codes based on the CSS map, Sec. III C gives existence bounds based on the map to hypergraph-product and related codes, Sec. III D gives a map of a weight-w GB code to a code local in $D \le w-1$ dimensions, and Sec. III E gives tight bounds for weight-four GB codes. Numerical results are collected in Sec. IV, followed by a brief Conclusion in Sec. V. Some of the formal proofs are collected in the Appendix A.

II. RELEVANT FACTS AND NOTATIONS

A. Cyclic and quasi-cyclic codes

An $[n,k,d]_q$ code $\mathcal{C}$ linear over a finite (Galois) field $\mathbb{F}_q$, with q a power of a prime, is a k-dimensional subspace of $\mathbb{F}_q^n$, the linear space of all q-ary strings of length n. The distance d is the minimum Hamming weight of a non-zero vector in the code, or infinity for a trivial $k=0$ code which only contains the zero vector. A code $\mathcal{C}_G \equiv \mathcal{C}_H^\perp$ can be specified in terms of a generating matrix G whose rows form a basis of the code, or a parity check matrix H whose rows generate the space orthogonal to the code.

A cyclic code satisfies the additional condition that for every codeword $c \equiv (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, its cyclic shift $T_n c \equiv (c_{n-1}, c_0, \dots, c_{n-2})$ also gives a codeword, $T_n c \in \mathcal{C}$. Shuch a shift is conveniently represented as multiplication in the quotient polynomial ring $\mathcal{R} \equiv \mathcal{R}_{n,q} = \mathbb{F}_q[x]/(x^n-1)$, namely, $T_n c(x) = xc(x) \bmod x^n-1$, where $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ has coefficients in $\mathbb{F}_q^n$. A cyclic code is an ideal of $\mathcal{R}$. In particular, this implies that any cyclic code can be generated as the set of all multiples in $\mathcal{R}$ of the canonical *generator polynomial* $g(x)$, where $g(x)$ is a factor of x^n-1, and any such factor generates a cyclic code.

Both a generator and a parity check matrix (with some redundant rows) of a cyclic code can be written as square circulant matrices. Algebra of circulant $n \times n$ matrices with coefficients in $\mathbb{F}_q$ is isomorphic to that of polynomials in $\mathcal{R}$. Indeed, given a polynomial $a(x) \in \mathcal{R}$, the corresponding circulant matrix

$$A = \begin{pmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \ddots & \ddots & \ddots \\ a_n & \dots & a_1 & a_0 \end{pmatrix}, \tag{1}$$

is conveniently written as the polynomial $A \equiv a(P)$ of the matrix $P \equiv P_n$, the $n \times n$ cyclic permutation matrix

$$P = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix}. \tag{2}$$

We will consider vectors in $\mathbb{F}_q^n$ as columns, so that the product Ab of a circulant matrix $A = a(P)$ and a vector b with the same coefficients as in the polynomial $b(x) \in \mathcal{R}$ corresponds to the product $a(x)b(x) \bmod x^n-1$. In particular, given a canonical generating polynomial $g(x)$, the corresponding check polynomial is $h(x) = (x^n-1)/g(x)$, and the cyclic code generated by $g(x)$ can be written as

$$\mathcal{C}_{g(x)} = \{c(x) \in \mathcal{R} : h(x)c(x) = 0 \bmod x^n - 1\}. \tag{3}$$

An index-m quasi-cyclic (QC) code of length $n = m\ell$ is usually defined as a linear code invariant under the m-step shift permutation T_n^m. Rearranging the positions, we consider the defining permutation as T_ℓ applied in each of m consecutive blocks. As a result, a generator matrix of such a code can be written as an $r \times n$ block matrix formed by $\ell \times \ell$ circulant matrices. Generally, such block matrices will be written as matrices formed by the corresponding polynomials in $\mathcal{R}_{\ell,q}$. The same applies to vectors, which will be written as columns of polynomials, with the exception of inline equations, where, e.g., a two-block vector in an index-2 QC code may be written as $[u(x), v(x)]$.

B. Quantum CSS codes

A quantum Calderbank-Shor-Steane[25, 26] (CSS) code $\mathcal{Q}$ with parameters $[[n,k,d]]_q$ over a Galois field $\mathbb{F}_q$ is isomorphic to a direct sum of an X- and a Z-like codes,

$$\mathrm{CSS}(H_X, H_Z) = \mathcal{Q}_X \oplus \mathcal{Q}_Z = \mathcal{C}_{H_Z}^\perp/\mathcal{C}_{H_X} \oplus \mathcal{C}_{H_X}^\perp/\mathcal{C}_{H_Z}, \tag{4}$$

where each term in the right-hand side (r.h.s.) is a quotient of two linear spaces in $\mathbb{F}_q^n$, and rows of the matrices H_X and H_Z must be orthogonal,

$$H_X H_Z^T = 0. \tag{5}$$

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

$$k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z \tag{6}$$

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

$$d_X = \min_{c \in \mathcal{C}_{H_Z}^\perp \setminus \mathcal{C}_{H_X}} \operatorname{wgt} c, \quad d_Z = \min_{c \in \mathcal{C}_{H_X}^\perp \setminus \mathcal{C}_{H_Z}} \operatorname{wgt} c, \tag{7}$$

are the minimum weights of non-trivial vectors (any representative) in $\mathcal{C}^{\perp}_{H_Z}$ and $\mathcal{C}^{\perp}_{H_X}$, respectively.

Physically, a quantum code operates in a Hilbert space $\mathcal{H}_q^{\otimes n}$ associated with n quantum-mechanical systems, *qudits*, with q states each, and a well defined basis of X and Z operators acting in $\mathcal{H}_q^{\otimes n}$[27]. Elements 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 (5) ensures that the stabilizer group is abelian. Non-trivial vectors in $\mathcal{Q}_X$ and $\mathcal{Q}_Z$ correspond to X and Z logical operators, respectively. Codes with larger distances have logical operators which involve more qudits; such codes typically give better protection.

III. GENERALIZED BICYCLE CODES

A. Definition and general properties

Generalized bicycle (GB) code[15, 20] is a version of the bicycle ansatz[21], a quantum CSS code constructed from a pair of equivalent index-two quasi-cyclic linear codes. Namely, given any pair of polynomials $a(x), b(x) \in F[x]$ with coefficients in a finite field $F \equiv \mathbb{F}_q$ and of degrees smaller than ℓ, the generalized bicycle code GB(a,b) of length $n = 2\ell$ has CSS generator matrices specified in the block form,

$$H_X = \left(A \,|\, B \right), \quad H_Z^T = \begin{pmatrix} B \\ -A \end{pmatrix}. \tag{8}$$

Here $A = a(P)$ and $B = b(P)$ are q-ary $\ell \times \ell$ circulant matrices. Circulant matrices necessarily commute, which guarantees the CSS orthogonality condition (5). For notational convenience, we will use $[u(x), v(x)]$ to represent a Z-codeword c, a column vector whose components in the two blocks coincide with the coefficients of the two polynomials. The corresponding equation $H_X c = 0$ is equivalent to $a(x)u(x) + b(x)v(x) = 0 \bmod x^\ell - 1$.

With any code GB(a,b), there is an associated q-ary cyclic code $\mathcal{C}^{\perp}_{h(x)} \equiv \mathcal{C}_{g(x)}$ of length ℓ, with the check and generating polynomials

$$h(x) \equiv \gcd\big(a(x), b(x), x^\ell - 1\big) \text{ and } g(x) \equiv \frac{x^\ell - 1}{h(x)}, \tag{9}$$

respectively. The number of qudits encoded in such a GB code is[20]

$$k = 2 \deg h(x), \tag{10}$$

twice the dimension of the code $\mathcal{C}^{\perp}_{h(x)} \equiv \mathcal{C}_{g(x)}$.

It is easy to see that column and row permutations can be used to obtain the matrix H_Z from H_X, up to a sign of some columns. Thus, the CSS distances (7) of any GB code are equal to each other and, respectively, to the code distance d. The calculation of the distance is simplified somewhat with the help of an auxiliary *asymmetric bicycle* (AB) code $\mathcal{Q}' \equiv \mathrm{CSS}(H'_X, H_Z)$ where

$$H'_X = \left(A_1 \,|\, B_1 \right), \quad A_1 \equiv a_1(P), \quad B_1 \equiv b_1(P), \tag{11}$$

where $a_1(x) \equiv a(x)/\gcd(a,b)$, $b_1(x) \equiv b(x)/\gcd(a,b)$ are obtained by dividing the two polynomials by the common factor, and the matrix H_Z is the same as in the original GB code, see Eq. (8). The AB code encodes half as many qudits as the original GB code, $k' = \deg h(x)$. The relation between the two codes follows from an explicit expression for the Z-codewords in the original code,

$$\begin{pmatrix} u(x) \\ v(x) \end{pmatrix} = \alpha(x) g(x) \begin{pmatrix} r_1(x) \\ s_1(x) \end{pmatrix} + \beta(x) \begin{pmatrix} b_1(x) \\ -a_1(x) \end{pmatrix} \bmod x^\ell - 1, \tag{12}$$

where $r_1(x)$ and $s_1(x)$ are Bézout coefficients such that $a_1(x)r_1(x) + b_1(x)s_1(x) = 1$ whose existence follows from $\gcd(a_1, b_1) = 1$, and, for a non-trivial codeword, at least one of $\alpha(x)$ and $\beta(x)$ should not be divisible by $h(x)$. Taken separately, these two conditions yield the sets of X- and Z-codewords of the AB code, respectively. This results in the following Statement whose formal proof is given in Sec. A 2.

Statement 1. *The distance of the code* GB(a,b) *is the same as that of the associated* AB *code* CSS(H'_X, H_Z), $d = d' = \min(d'_X, d'_Z)$.

In addition, the CSS distance d'_Z (and thus the distance d of the GB code) is bounded by the distance d_g of the linear cyclic code $\mathcal{C}_{g(x)}$.

Statement 2. *Let d_g denote the distance of the $\mathbb{F}_q$-linear cyclic code with the generating polynomial $g(x)$, see Eq. (9). Then the Z-distance of the q-ary AB code* CSS(H'_X, H_Z) *satisfies $d'_Z \le d_g$.*

The formal proof in Sec. A 3 amounts to a demonstration that for any non-zero code word $e(x) \in \mathcal{C}_{g(x)}$, either $[e(x), 0]$ or $[0, e(x)]$ is a non-trivial Z-vector in the AB code.

We end this section with a short list of polynomial transformations which generate equivalent GB codes:

Statement 3. *Two codes* GB(a,b) *and* GB(a',b') *of the same size $n = 2\ell$ are equivalent if*

- **(i)** $a'(x) = a(x^m) \bmod x^\ell - 1$, $b'(x) = b(x^m) \bmod x^\ell - 1$ *for some m mutually prime with ℓ, $\gcd(m, \ell) = 1$;*
- **(ii)** $a'(x) = b(x)$, $b'(x) = a(x)$;
- **(iii)** $a'(x)$ *and* $b'(x)$ *are the reciprocal polynomials of* $a(x)$ *and* $b(x)$, *respectively.*
- **(iv)** $a'(x) = \delta a(x)$, $b'(x) = b(x)$, *for some* $0 \neq \delta \in \mathbb{F}_q$.
- **(v)** $a'(x) = f(x)a(x)$, $b'(x) = f(x)b(x)$, *for some polynomial* $f(x) \in \mathbb{F}_q[x]$ *such that* $\gcd(f, x^\ell - 1) = 1$.

The first four transformations correspond to permutations preserving the circulant symmetry[28], while the last one may be useful for constructing LDPC codes,

since minimum row weight does not necessarily correspond to minimum polynomial degrees.

While technically not an equivalence transformation, we should also mention here the case of polynomials *commensurate* with the circulant size ℓ, i.e., such that $h(x) = h_0(x^\Delta)$, where $\Delta > 1$ is a factor of ℓ. A cyclic code whose check polynomial $h(x)$ is commensurate with ℓ is merely a direct sum of Δ disconnected cyclic codes, each equivalent to the code of length $\ell_0 \equiv \ell/\Delta$ with the check polynomial $h_0(x)$. Same is true in the case of a code $\mathrm{GB}(a, b)$ whose defining polynomials have the same commensurability factor Δ:

Statement 4 (Commensurate GB code)**.** *A code* $\mathrm{GB}(a, b)$ *with parameters* $[[2\ell, k, d]]_q$ *and* $a(x) = a_0(x^\Delta)$, $b(x) = b_0(x^\Delta)$, *where* $\ell = \ell_0\Delta$, *is equivalent to a direct sum of* Δ *copies of the code* $\mathrm{GB}(a_0, b_0)$ *with parameters* $[[2\ell_0, k_0, d_0]]_q$. *In particular,* $d = d_0$ *and* $k = k_0\Delta$.

A cyclic or GB code that is not commensurate is called *incommensurate*.

B. Bounds for GB codes of unrestricted weight

Here we give several existence bounds for general (non-LDPC) GB codes, using the standard map[25–27] relating the parameters of a CSS code to those of the associated pair of classical $\mathbb{F}_q$-linear mutually dual-containing codes. In the case of the code $\mathrm{GB}(a, b)$, the two codes have double-circulant parity check matrices H_X and H_Z given in Eq. (8). To be specific, we focus on the index-two QC code with the check matrix $H = H_X$, and denote such a code $\mathrm{QC}(a, b)$.

Statement 5 (CSS map for GB codes[25–27])**.** *Given the parameters* $[n_0 = 2\ell, k_0, d_0]_q$ *of the classical linear code* $\mathrm{QC}(a, b)$, *the quantum CSS code* $\mathrm{GB}(a, b)$ *has parameters* $[[2\ell, 2k_0 - 2\ell, d]]_q$, *where* $d \geq d_0$.

It is a classical result[29, 30] that index-two QC codes include good codes with rate 1/2 and asymptotically finite relative distances $d_0/n_0 \to \delta_0 > 0$. However, the codes used in the proof have parity-check matrices in a systematic form with $A = I$; for such a self-dual (up to a permutation) index-two QC code Statement 5 gives a quantum code which encodes no qudits. A number of other lower bounds on the distances of QC codes have been constructed, in particular, a version[31] of the BCH bound (for a recent review, see Ref. 32). However, none of these bounds gives a family of QC codes with $k_0 - \ell = \mathcal{O}(\ell)$ and $d_0 = \mathcal{O}(n)$. Indeed, by Statements 1 and 2, such a family of QC codes would imply that linear cyclic codes must be asymptotically good, a question which remains unresolved[33, 34].

For these reasons here we list several partial results, which demonstrate the existence of QC codes with sublinear $k_0 - \ell$ and distances scaling linearly, and of finite-rate QC codes with sublinear (power law) distances. The following bound is constructed using elementary arguments similar to those used in Ref. 35:

Statement 6. *Consider the code* $\mathrm{QC}(a, b)$ *in the special case* $a(x) = f(x)h(x)$, $b(x) = h(x)$, *where for some polynomial* $r(x)$, $\gcd\big(f(x) - r(x), x^\ell - 1\big) = p(x)$ *is a factor of the generating polynomial,* $g(x) = p(x)q(x)$. *Then the distance of the QC code satisfies the bounds:*

(a) *If* $r(x) = 0$, $\quad d_0 \geq \min\big\{d[q], 1 + d[p]\big\}$;

(b) *Otherwise, if* $\gcd\big(r(x), x^\ell - 1\big) = 1$,

$$d_0 \geq \min\Big\{2d[q], d[p]/\operatorname{wgt}(r)\Big\}.$$

Here $h(x)$ *and* $g(x)$ *are given by Eq. (9), and* $d\,[q]$ *is the distance of the linear cyclic code generated by* $q(x)$.

Unfortunately, the codes generated by $p(x)$ and $q(x) = g(x)/p(x)$, respectively, form a pair of dual-containing cyclic codes; it is well known[36] that the minimum of the two distances is bounded by $\mathcal{O}(\sqrt{\ell})$, which limits the usability of the bound in Statement 6.

The following bound obtained with the help of a counting argument is a variant of Lemma 5 from Ref. 37 in application to GB codes:

Statement 7. *Let* $x^\ell - 1 = g(x)h(x)$ *with* $g(x) \in \mathbb{F}_q[x]$ *irreducible, and*

$$d_{\mathrm{GV}} = \max d : \sum_{s=1}^{d-1} (q-1)^s \left[\binom{2\ell}{s} - \binom{\ell}{s}\right] < q^{\ell - \deg h} - 1. \tag{13}$$

Then, there exists $f(x) \in \mathbb{F}_q[x]$ *such that the length-*2ℓ *code* $\mathrm{QC}(hf, h)$ *has distance* $d \geq \min(d[g], d_{\mathrm{GV}})$, *where* $d[g]$ *is the distance of the cyclic code generated by* $g(x)$.

The counting part of this bound asymptotically approaches from above the Gilbert-Varshamov (GV) bound[38, 39] for linear q-ary codes with $k = \ell + \deg h$, which coincides with the GV bound[25] for q-ary CSS codes with $k = 2\deg h$. Unfortunately, the requirement for $g(x)$ to be irreducible is very restrictive. Generally, since $x^{ab} - 1$ has both $x^a - 1$ and $x^b - 1$ as factors, codes with ℓ prime get higher lower bounds on their relative distances under Statement 7. In particular, two well-known special cases correspond to $x^\ell - 1$ having only two and three factors, respectively:

Example 8. [GB codes with linear distance] *Let* ℓ *be such that* $\mathrm{ord}_\ell(q) = \ell - 1$, *where* $\mathrm{ord}_\ell(q)$ *is the multiplicative order function of* q *modulo* ℓ. *This ensures that* $x^\ell - 1$ *has only two irreducible factors in* $\mathbb{F}_q[x]$, $h(x) \equiv 1 - x$ *and* $g(x) = 1 + x + \ldots + x^{\ell-1}$. *Then there is a* GB *code with parameters* $[[2\ell, 2, d \geq d_{\mathrm{GV}}]]_q$, *where* d_{GV} *is given by Eq. (13). For* $q = 2$ *the corresponding set is[40]* $\{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, \ldots\}$, *and, moreover, according to Artin's primitive root conjecture, a finite fraction of all primes satisfies this condition for any* $q > 0$ *which is not a perfect square[41]. Asymptotically, at* $\ell \to \infty$, *this bound on the relative distance coincides with the* GV *bound for rate-*1/2 *linear* q*-ary codes, e.g.,* $\delta_{\mathrm{GV}} \approx 0.1100$ *for* $q = 2$.

Example 9. [GB codes with asymptotic rate 1/4] *For an odd prime ℓ let a prime p be a quadratic residue modulo ℓ, i.e., $p \equiv m^2 \bmod \ell$ for some integer m. Then, $x^\ell - 1$ has only three irreducible factors in $\mathbb{F}_p[x]$, and there is a* quadratic-residue *cyclic code $[\ell, (\ell+1)/2, d]_p$ with $d \geq \sqrt{\ell}$ and an irreducible generator polynomial[28]. According to Statement 7, a prime-field* GB *code with parameters $[[2\ell, (\ell-1)/2, d \geq \ell^{1/2}]]_p$ exists.*

C. A map to hypergraph-product and related codes

We would now like to focus on more practical GB codes with bounded-weight stabilizer generators. First, we construct an explicit map between a quantum hypergraph-product code[14] constructed from a pair of square circulant matrices of mutually prime dimensions n_1 and n_1, and a GB code with circulant size $\ell = n_1 n_2$, see Fig. 1.

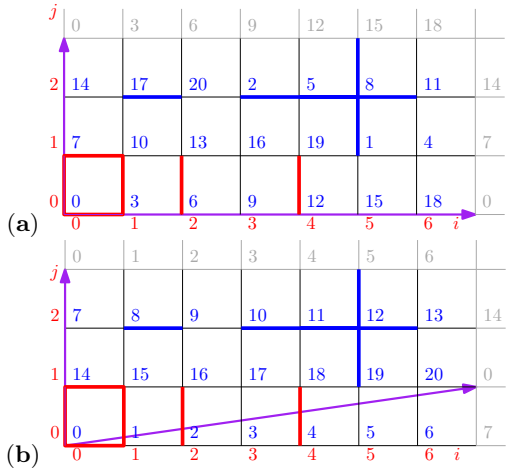

FIG. 1. (Color online) (**a**) A map (17) of an $n_1 \times n_2$ square lattice with periodic boundary conditions along the vectors $\vec{L}_1 = (n_1, 0)$ and $\vec{L}_2 = (0, n_2)$ to a chain of length $\ell = n_1 n_2$, with $n_1 = 7$ and $n_2 = 3$. Red digits below and to the left of the axes show the column i and row j indices; the index t is placed above and to the right of the corresponding vertex. The two blocks in Eq. (14) correspond to horizontal and vertical edges, respectively. Thicker red and blue edges, respectively, indicate those in an X and a Z stabilizer generators of the QHP code $[[42, 8, 3]]$ obtained from polynomials $h_1(x) = 1 + x + x^2 + x^4$ and $h_2(x) = 1 + x$. The equivalent code GB(a, b) has $a(x) = 1 + x^3 + x^6 + x^{12}$ and $b(x) = 1 + x^7$. (**b**) Same, but with a skewed periodicity vector $\vec{L}_1' = (n_1, 1)$. The corresponding map $t = i - n_1 j \bmod n_1 n_2$ is invertible, but has a different symmetry. As a result, even though the GB code with $a'(x) = 1 + x + x^2 + x^4$ and $b'(x) = 1 + x^{14}$ has the same parameters $[[42, 8, 3]]$, this is coincidental. Indeed, replacing the polynomial $h_2(x)$ with $h_2'(x) = 1 + x + x^2$ gives the QHP code $[[42, 16, 2]]$ and an equivalent code using the map (17), but the present map gives $b''(x) = h_2'(x^7)$ which is mutually prime with $a(x)$, resulting in an empty GB code.

Specifically, let $H_1 = h_1(P_{n_1})$ and $H_2 \equiv h_2(P_{n_2})$ be a pair of square circulant matrices of size n_1 and n_2, corresponding to polynomials $h_1(x)$ and $h_2(x)$ in $\mathbb{F}_q[x]$, respectively. Given the parameters $[n_i, k_i, d_i]_q$ for the two cyclic codes with the check polynomials h_i, $i \in \{1, 2\}$, consider the hypergraph-product code with CSS generators in a block form written as Kronecker products,

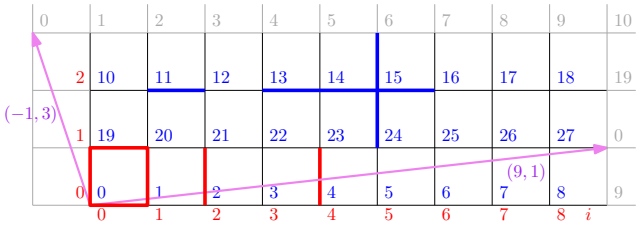

FIG. 2. (Color online) As in Fig. 1 but with periodicity vectors $\vec{L}_1 = (9, 1)$, $\vec{L}_2 = (-1, 3)$ and circulant matrices of size $\ell = |\vec{L}_1 \times \vec{L}_2| = 28$. Here stabilizer generators with the lattice structure identical to those in Fig. 1 give a rotated-QHP code $[[56, 2, 8]]$. The equivalent code GB(a, b) has $a(x) = 1 + x + x^2 + x^4$ and $b(x) = 1 + x^{19}$.

$$H_X = (I_1 \otimes H_2, H_1 \otimes I_2), \quad H_Z^T = \begin{pmatrix} H_1 \otimes I_2 \\ -I_1 \otimes H_2, \end{pmatrix}, \quad (14)$$

where I_i are the identity matrices of size n_i, $i \in \{1, 2\}$. Such a code has the parameters[14, 18]

$$[[2n_1 n_2, 2k_1 k_2, \min(d_1, d_2)]]_q \quad (15)$$

and can be put on an $n_1 \times n_2$ square lattice with periodic boundary conditions as illustrated in Fig. 1(a), with the two blocks in Eq. (14) corresponding to qubits on horizontal and vertical edges, respectively.

In the special case where n_1 and n_2 are mutually prime, $\gcd(n_1, n_2) = 1$, an equivalent GB code with circulant size $\ell = n_1 n_2$, can be constructed from the polynomials

$$a(x) = h_1(x^{n_2}), \quad b(x) = h_2(x^{n_1}), \quad (16)$$

where the values of the circulant index

$$t = n_2 i + n_1 j \bmod \ell \quad (17)$$

are in a one-to-one correspondence with the positions (i, j) on the $n_1 \times n_2$ portion of the square lattice with periodic boundary conditions introduced by identifying any pair of points connected by periodicity vectors $\vec{L}_1 = (n_1, 0)$ and $\vec{L}_2 = (0, n_2)$.

We should emphasize that in addition to being a one-to-one map, Eq. (17) has the correct translation symmetry. Different GB codes can be also obtained using skewed periodicity vectors, e.g., $\vec{L}_1' = (n_1, 1)$ instead of $\vec{L}_1$, equivalent to the index map $t = i - n_1 j \bmod \ell$. This map does not give identity transformation for the translation $i \to i + n_1$. Thus, we do not expect the corresponding code GB(a', b'), $a'(x) = h_1(x)$, $b'(x) = h_2(x^{n_1})$ to be equivalent to the original QHP code, see Fig. 1(**b**).

Generally, a quantum code on the edges of a square lattice with stabilizer generators similar to those of a QHP

code but with periodicity vectors non-collinear with the axes is called a rotated QHP code[15], a code in a more general class of lifted-product codes[3].

Statement 10. *An arbitrary GB code of length 2ℓ is equivalent to a rotated QHP code with periodicity vectors $\vec{L}_1$ and $\vec{L}_2$ such that $|\vec{L}_1 \times \vec{L}_2| = \ell$.*

Proof. Indeed, given a decomposition $\ell = n_1 n_2 + \lambda$, where n_1 and ℓ are mutually prime, $\gcd(n_1, \ell) = 1$, consider a pair of vectors,

$$\vec{L}_1 = (n_1, 1) \quad \text{and} \quad \vec{L}_2 = (\lambda, n_2). \tag{18}$$

If we use these as periodicity vectors (i.e., identify any pair of points on the square lattice connected by one of these vectors), there are exactly $\ell = |\vec{L}_1 \times \vec{L}_2|$ inequivalent points with a one-to-one map $t = i - n_1 j \bmod \ell$ to a cycle $\mathbb{Z}_\ell$, see Figs. 1(**b**) and 2. Then, given the polynomials $h_1(x)$ and $h_2(x)$ which define the lattice layout of the stabilizer generators of a rotated QHP code with the chosen periodicity vectors, the polynomials defining the corresponding GB code are $a(x) = h_1(x)$ and $b(x) = h_2(x^{n_1})$.

Conversely, let m_1 be a multiplicative inverse of n_1 modulo ℓ, $m_1 n_1 = 1 \bmod \ell$; its existence is guaranteed by the condition $\gcd(n_1, \ell) = 1$. Then, given the code $\mathrm{GB}(a, b)$, we recover the polynomials for the corresponding rotated-QHP code, $h_1(x) = a(x)$ and $h_2(x) = b(x^{m_1}) \bmod x^\ell - 1$. □

These maps show, in particular, that GB codes can be as good as QHP codes constructed from two square circulant matrices of mutually prime sizes. Given the explicit Eq. (15) relating parameters of a QHP code with those of the two cyclic codes with parity-check polynomials $h_1(x)$ and $h_2(x)$, we obtain an existence for GB codes of finite rates and a power-law distance scaling as $\mathcal{O}\big(n^{1/2}/\operatorname{polylog}(n)\big)$ or better. Indeed, the question of whether long linear cyclic codes are asymptotically good is still open, with only minor progress made in recent years[34, 42, 43]. In reality, the question is academic, since finite-length performance of cyclic codes is excellent, and already the BCH bound gives codes[44] with rate $R > 0$ and $\delta \geq (2 \ln R^{-1})/\log n$, while linear cyclic codes with $\delta > (1 - 2R)/\sqrt{2 \log n}$ can also be constructed[45].

From a practical viewpoint, more interesting are the bounds on parameters of LDPC GB codes with stabilizer generators of bounded weight. We construct such (upper) bounds in the next section with the help of general results by Bravyi, Poulin, and Terhal[46, 47], by mapping a linear cyclic code with check polynomial of weight w_1 to a code local on a D-dimensional hyper-cubic lattice, with $D \leq w_1$, and a GB code with row weight w to a quantum code local on a D-dimensional lattice, with $D \leq w - 1$.

D. A map to a code local in D dimensions

Let us first consider the case of a cyclic code of length ℓ with the parity check polynomial $h(x) \in \mathbb{F}_q[x]$ of a fixed weight w. Here we will not require that $h(x)$ be a factor of $x^\ell - 1$, as such factors do not necessarily have minimal weights, but a q-ary polynomial such that the canonical check polynomial $h_1(x) \equiv \gcd(h, x^\ell - 1)$ be non-trivial, $k = \deg h_1(x) > 0$.

The following is a generalization of Statement 10:

Statement 11. *An incommensurate linear cyclic code of length ℓ with check polynomial $h(x)$ of weight w is equivalent to a code with all checks local on a hypercubic lattice of dimension $D \leq w$, and $D \leq w - 1$ if ℓ is prime.*

Proof. For a polynomial $h(x)$ with monomial degrees $0 = t_0 < t_1 < \ldots < t_{w-1}$, consider a set of w integer vectors in $\mathbb{Z}^w$, written as the rows of the lower-triangular matrix

$$M = \begin{pmatrix} \ell & & & & \\ t_1 & -1 & & & \\ t_2 & & -1 & & \\ \vdots & & & \ddots & \\ t_{w-1} & & & & -1 \end{pmatrix}. \tag{19}$$

The determinant of M equals $\pm\ell$, and by the incommensurability condition, there exists a map from the chain $0 \leq t < \ell$ to the region in $\mathbb{Z}^w$ given by the inequalities $0 \leq x_i < \ell_i$, $0 \leq i < w$, where $\ell_0 = t_1$, $\ell_i = \lceil t_{i+1}/t_i \rceil$ for $0 < i < w - 1$, and $\ell_{w-1} = \lceil \ell / t_{w-1} \rceil$. With these notations, the check polynomial becomes $a_0 + a_{t_1} x_1 + \ldots a_{t_{w-1}} x_{w-1}$, i.e., the checks are one-local in the bulk of the region (with the structure as in quantum fractal codes[48, 49]), and at most two-local near the region's boundary.

When ℓ is a prime (or one of the original degrees $t_i \neq 0$ is mutually prime with ℓ), there exists $m \in \mathbb{Z}_\ell$ such that $m t_i = 1 \bmod \ell$, and $x^i \to x^{im} \bmod x^\ell - 1$ gives an equivalent code, see Statement 3. The modified check polynomial $h'(x) \equiv h(x^m) \bmod x^\ell - 1$ $h'(x)$ has a degree-one monomial, and the region defined by the periodicity vectors (19) has $x_0 = x_1$, thus $D \leq w - 1$.

The dimension can be additionally reduced if there is a simple relation between the monomial degrees, e.g., $t_3 = t_1 + t_2$, in which case the third axis can be skipped and the corresponding monomial written as $a_{t_3} x_1 x_2$. □

Given such a map to a code local in D dimensions, with the help of the general result in the appendix of Ref. 47, we immediately obtain:

Corollary 12. *Parameters $[\ell, k_1, d_1]_q$ of any $\mathbb{F}_q$-linear cyclic code of length ℓ with the check polynomial of weight w_1 which is equivalent to a code local in $D_1 \leq w_1$ dimensions, satisfy $k_1 d_1^{1/D_1} = \mathcal{O}(\ell)$.*

The case of a GB code with polynomials $a(x)$ and $b(x)$ with the total weight w is considered similarly, except

that each vertex of the hypercubic lattice must now contain two qudits, one from each block, and the maximum dimension is additionally reduced by one since both polynomials have zero-degree monomials. It is also easy to check that a local map for H_X to $\mathbb{Z}^D$ automatically implies the locality of the corresponding H_Z. We have, combining the results from Refs. 46 and 47:

Statement 13. *An incommensurate GB code with row weight w and parameters $[[n = 2\ell, k, d]]_q$ is equivalent to a CSS code local in $D \le w-1$ dimensions ($D \le w-2$ if ℓ is prime). Its parameters satisfy the inequalities*

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

Notice that the last equation implies that any GB code family with a fixed weight w has an asymptotically zero rate, since $k/n \to 0$ when the distance d becomes infinite.

E. Exact bound for GB codes of weight four

Here we consider in detail the special case of codes with $w = 4$. According to Statement 13, any such code is equivalent to a code local in two dimensions. The case of $D = 2$ is special, since Refs. 46 and 47 give asymptotically exact bounds for such codes.

A non-trivial GB code of weight $w = 4$ can only be constructed when both $a(x)$ and $b(x)$ have equal weights. Moreover, weight-two polynomials of equal degrees, or a polynomial of degree $\ell/2$ with ℓ even, always give an empty code or a distance-two code. Therefore, for a non-trivial incommensurate GB code with distance $d \ge 3$, with the help of Statement 3, without restricting generality, we can request that the degrees $\alpha = \deg a(x)$ and $\beta = \deg b(x)$ satisfy $\alpha < \beta < \ell/2$, with $\gcd(\alpha, \beta, \ell) = 1$.

These additional properties guarantee that any pair of rows of a generator matrix H_X (or H_Z) in Eq. (8) intersect in at most one column, and any column has exactly two non-zero elements, as in a vertex-edge incidence matrix of a simple graph. The analogy can be made exact by considering a pair of binary matrices J, F constructed from H_X and H_Z, respectively, by replacing any non-zero element with 1. The rows of the two matrices are necessarily orthogonal, $JF^T = 0$ (over $\mathbb{Z}_2$). Thus, these matrices can be readily identified as a vertex-edge and a face-edge incidence matrices of a locally planar $(4, 4)$ graph $\mathcal{G}$, i.e., with each vertex of $\mathcal{G}$ and the corresponding dual graph $\widetilde{\mathcal{G}}$ of equal degree 4. Finally, it is also easy to see that the graph $\mathcal{G}$ is locally (i.e., as long as the current position does not close a circle $t \to t + \ell$) isomorphic to a square lattice, with the two blocks, respectively, corresponding to horizontal and vertical edges, and oriented in the direction of increasing index. Namely, any (local) sequence of horizontal $x_i = \pm 1$ and vertical $y_j = \pm 1$ steps, where the signs indicate the direction, arrives at the same final position as long as the total displacements $\sum x_i$ and $\sum y_j$ coincide. That is, the graph $\mathcal{G}$ is *covered* by the infinite square lattice graph $\mathcal{H}$, with the covering function $f : \mathcal{H} \to \mathcal{G}$ such that a path between a pair of vertices on $\mathcal{H}$ with the same covering map image corresponds to a non-trivial cycle on $\mathcal{G}$, or one or more "large" displacements $t \to t \pm \ell$ of the circulant index.

With such a map, it is evident that a non-trivial GB code of weight-four and distance $d \ge 3$ is a square-lattice surface code, with Z-codewords corresponding to homologically non-trivial cycles, with the homology fixed by the covering map f (see, e.g., Ref. 50). Then, the distance d_Z is the length of a shortest path connecting a pair of distinct vertices on $\mathcal{H}$ whose covering-map images coincide on $\mathcal{G}$.

To construct an actual distance bound, start with an arbitrary vertex $i \in \mathcal{V}_\mathcal{H}$ (where $\mathcal{V}_\mathcal{H}$ is the vertex set of $\mathcal{H}$), and consider a vertex-centered ball $B_r(i)$ on $\mathcal{H}$, a set of all vertices $j \in \mathcal{V}_\mathcal{H}$ such that the graph distance $d(i, j) \le r$, see Fig. 3 (left). With the circulant size ℓ, the graph $\mathcal{G}$ has exactly ℓ vertices. Thus, if the size of the ball satisfies $|B_r(i)| > \ell$, the ball must include at least two equivalent vertices, which gives for the code distance, $d_Z \le 2r$, the *diameter* of the ball. The size of a ball on the square lattice is computed easily by summing the arithmetic sequence,

$$|B_r(i)| - 1 = 4 + 8 + \ldots + 4r = 2r(r + 1),$$

which gives the upper bound $d_Z \le 2r$ for any circulant size $\ell < 1 + 2r(r + 1)$. A similar calculation for an edge-centered ball on $\mathcal{H}$ gives an odd-valued upper bound $d_Z \le 2r + 1$ for any $\ell < 2(r + 1)^2$, see Fig. 3 (right). We rewrite these inequalities equivalently as lower bounds on the code length $n = 2\ell$ for a given value of the distance $d = d_Z$:

Statement 14. *Consider a weight-four GB code of an odd distance $d = 2r + 1$, then its length $n \ge 1 + d^2$. For an even distance $d = 2r$, the length $n \ge d^2$.*

The argument above is valid for $d \ge 3$. We verified by exhaustive search that these inequalities are also valid for $d \in \{1, 2\}$.

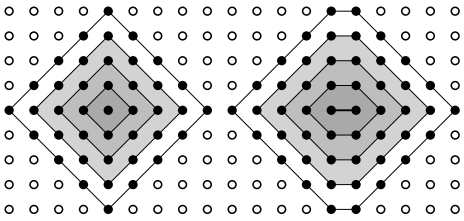

FIG. 3. Left: squares with progressively ligher shading indicate vertex-centered balls of radius $r = 1$, 2, 3, and 4 on the square lattice; the numbers of vertices on the boundary are 4, 8, 12, and 16, respectively. Right: same for edge-centered regions where each distance-r boundary has exactly two additional vertices.

We notice that the inequalities in Statement 14 are sharp for surface codes. Namely, the odd-distance bound is reached by a family[51] of square lattice surface codes

with periodicity vectors $(r+1, r)$ and $(-r, r+1)$ and parameters $[[(2r+1)^2+1, 2, 2r+1]]_q$, while the even-distance bound is achived by the 45°-rotated surface codes[52]. These latter codes have periodicity vectors $(\pm r, \pm r)$ and parameters $[[4r^2, 2, 2r]]_q$. However, the corresponding translation group $\langle x, y \mid xyx^{-1}y^{-1} = x^r y^r = x^r y^{-r} = 1\rangle$ is not cyclic for any $r > 1$, which proves that there are no corresponding GB codes except for $r = 1$, with parameters $[[4, 2, 2]]_q$.

The next-shortest family of even-distance surface codes has periodicity vectors $(r \pm 1, 1 \pm r)$ and parameters $[[4r^2 + 4, 2, 2r]]_q$, $r \in \mathbb{N}$; these have GB code representations when r is even, which requires the distance $2r$ be a multiple of four.

IV. NUMERICAL RESULTS

To summarize our results so far, we expect the highest distances for GB codes encoding $k = 2$ qudits, with $b(x) = 1 + x$ and $a(x)$ of even weight, which ensures the corresponding check polynomial (9) to be $h(x) = 1 + x$ for any $\ell \geq 2$. For the qubits (quantum codes over the binary field $\mathbb{Z}_2$), Example 8 based on Statement 7 shows that for prime circulant sizes ℓ with a primitive root 2, GB codes in this family exist with relative distance $d/n > \delta_{\rm GV} \approx 0.11$. However, the upper and lower bounds for the codes of row weight w (which corresponds to $\mathrm{wgt}(a) = w - 2$) differ strongly for $w > 4$. Namely, Statement 6, the map to QHP codes in Sec. III C, and several explicit $w = 4$ code families in Sec. III E agree that such codes with the distances $d > \mathcal{O}(n^{1/2})$ scaling as a square root of the block size exist. On the other hand, the upper bound in Statement 13 for such codes suggests a power-law distance scaling with the exponent that may change with w, $d < \mathcal{O}(n^\gamma)$, where $\gamma = 1 - 1/D$, with the effective dimension $D(w) \leq w - 2$ for a prime ℓ. The two bounds give the same exponent $\gamma = 1/2$ only for $w = 4$, while there is an interval of possible exponent values for $w > 4$. Notice that any exponent, including $\gamma_{\min} = 1/2$, may be consistent with the linear distance scaling at large w, if the corresponding prefactor $A(w)$ in the power-law $d \propto A(w) n^\gamma$ diverges at $w \to \infty$.

To address this issue, we set up to find largest-distance GB codes based on qubits and row weights $w \in \{4, 6, 8\}$, fixing $b(x) = 1 + x$. Namely, for every prime $\ell \leq 227$ such that 2 is a primitive root, we calculated the maximum distance of GB codes over inequivalent polynomials $a(x)$ of weights 2, 4, and 6 (also, for every prime $\ell \leq 127$ in the case of $\mathrm{wgt}\, a = 4$, which did not substantially modify the results). We used equivalence maps (**iii**) and (**v**) [with $f(x) = x^s$, $s < \ell$] in Statement 3 to define a canonical form of $a(x) \in \mathbb{F}_2[x]$ of degree Δ, with $a_0 = a_\Delta = 1$, and smallest alphabetically. In particular, this implies a smallest-degree polynomial in each equivalence class. When enumerating polynomials, we discarded any which did not coincide with the corresponding canonical form. Actual distance calculation were done using the GAP package `QDistRnd`[53], with the help of the auxiliary AB code as in Statement 1, and only for those polynomials $a(x) = f(x)(1 + x)$ with a sufficiently large $1 + \mathrm{wgt}\, f$ (such an upper bound on the distance is a trivial consequence of Statement 3). The resulting data and the actual codes are available for download at the GitHub repository `QEC-pages/GB-codes`[54].

The computed distances d are plotted in Fig. 4 as a function of the square root of the code length n, with different symbols and colors for GB codes of row weight 4, 6, and 8, as indicated in the figure caption. For clarity, for each w, only the codes with the smallest n giving the particular distance are shown on the plots. As expected, for each value of n, optimal codes with larger w show larger distances, with the $w = 8$ codes giving approximately a factor of two distance improvement compared to codes with $w = 4$ (equivalent to square lattice surface codes), e.g., $d_4 = 13$, $d_6 = 21$, and $d_8 = 23$ for $n = 202$; the actual improvement factors are different for different values of n. We also notice that codes with $n \gtrsim 10^2$ are highly degenerate: their distances d are factor of two or larger than the corresponding stabilizer generator weights w.

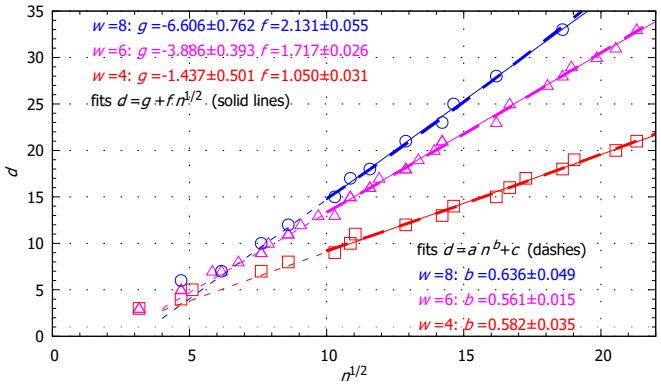

FIG. 4. (Color online) Distance d plotted as a function of the square root of the block length n for a family of GB codes encoding $k = 2$ qubits. Squares, triangles, and circles correspond to row weight $w = 4$, 6, and 8, respectively. The fits to $d = g + fn^{1/2}$ using only the data with $n^{1/2} > 10$ are shown with thin solid lines; the corresponding coefficients are given in the upper-left inset. Thin dashed lines in the range $n^{1/2} < 10$ are the continuation of the same plots outside of the range used for fitting. Thick long dashes show the three-parameter fits to $d = an^b + c$; the corresponding exponents b are shown in the lower-right inset.

Visually, the data in Fig. 4 do not show much curvature, indicating distance scaling close to a square root. This is confirmed by fitting the data to a general three-parameter power-law form $d = an^b + c$ (thick long dashes), and a similar two-parameter fit with a fixed power $b = 1/2$ (thin lines): the corresponding lines lie more or less on top of each other, even though there is some upward curvature as indicated by the fitted exponents b whose values exceed 1/2 for all three sets of data.

We should also notice that in an attempt to capture

the large-n features, only the data in the range $n > 100$ was used in the fits. In fact, the three fitted values of the exponent b remain the same to three decimal places when the distance data for codes with $n \geq 25$ are included, while the square-root slope coefficients f show a minor reduction by around 5%.

V. CONCLUSION

To summarize, we have constructed several bounds on distances of generalized bicycle codes. Without a weight restriction, GB codes with linear in the block length n distances and encoding a sublinear number of qubits, GB codes of rate 1/4 with the distance scaling as a square root of n, as well as codes with other rates and the distances $\mathcal{O}(n/\log n)^{1/2}$ are known to exist.

More important practically are LDPC GB codes with a finite row weight w. Technically, these are zero-rate codes, since any such code is equivalent to a code local in a finite dimension D, see Statement 13. On the other hand, compared to the QHP and conventional toric codes, GB codes with row weights $w \leq 8$ may have a factor-of-two larger distances with the same block sizes. While any power-law distance scaling is sufficient to maximize the lower bound on the fault-tolerant threshold for Pauli channel errors[9] and saturate the upper (percolation threshold) bound for erasure errors on graph-based codes[50], higher distances allow for better error-correction performance in the practically important regime of low block error rates. It remains to be seen whether the improved distances would be sufficient to offset the increased measurement complexity (compared to the surface codes) due to higher stabilizer generator weights and their non-locality.

The questions remaining for future studies include further numerical and analytical studies of GB codes encoding $k > 2$ qubits. In addition to studying their parameters, of interest is the analysis of their performance in the fault-tolerant setting, as larger k values also increase the redundancy for minimum-weight stabilizer generators.

Second, remains open the question of the distance scaling for GB codes with a bounded generator weight. More generally, while quantum LDPC codes with power-law distance scaling higher than a square root of the block length have been constructed, it remains unknown whether local in a finite dimension $D > 2$ codes can beat the square root distance bound (ignoring any logarithmic corrections).

Finally, it is the regular structure of finite-weight GB codes that makes it possible to represent them as codes local in a D-dimensional space. Perhaps other classes of matrices in the same CSS ansatz (8) based on two commuting square matrices would produce LDPC codes with better parameters?

ACKNOWLEDGMENTS

L.P.P. was financially supported in part by the NSF Division of Physics via grants 1820939 and 2112848, and by the Government of the Russian Federation through the ITMO Fellowship and Professorship Program.

Appendix A: Formal proofs

1. The dimensions of GB and AB codes

This version of the proof is equivalent to the one in Ref. [20]; we give it for completeness.

Proof. Let $h(x) = \gcd(a(x), b(x), x^\ell - 1)$, then the ranks of the double-circulant matrices (8) are given by

$$\operatorname{rank} H_X = \operatorname{rank} H_z = \ell - \deg h(x). \tag{A1}$$

Indeed, the ranks can be computed using the column space, as the number of linearly independent vectors of the form $\alpha A + \beta B$, where α and β are length-ℓ q-ary vectors. Using the polynomial representation, these are equivalent to linearly independent polynomials of the form

$$\alpha(x)a(x) + \beta(x)b(x) \bmod x^\ell - 1.$$

Each term in this expression contains $h(x)$ as a factor, thus there can be no more than $\ell - \deg h(x)$ independent linear combinations. Further, $\gcd(a(x), b(x), x^\ell - 1) = h(x)$ implies the existence of polynomials $u(x)$, $v(x)$, and $w(x)$ (Bézout coefficients) such that

$$u(x)a(x) + v(x)b(x) + w(x)(x^\ell - 1) = h(x),$$

or, equivalently,

$$u(x)a(x) + v(x)b(x) = h(x) \bmod x^\ell - 1.$$

Multiplying by x^m, we get independent linear combinations for $0 \leq m < \ell - \deg h(x)$. This proves Eq. (A1), so that the dimension of a GB code is

$$k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z = 2 \deg h(x).$$

In the case of AB codes, Eq. (A1) gives $\operatorname{rank} H'_X = \ell$, thus $k' = \deg h(x)$. □

2. Proof of Statement 1

Proof. Let $[u(x), v(x)]$ be an X-like codeword of the GB code, it satisfies the polynomial equation

$$a(x)u(x) + b(x)v(x) = 0 \bmod x^\ell - 1, \tag{A2}$$

and, in addition, in order for the codeword to be non-trivial, for any $\alpha(x) \in F[x]/(x^\ell - 1)$,

$$\begin{pmatrix} u(x) \\ v(x) \end{pmatrix} \neq \alpha(x) \begin{pmatrix} b(x) \\ -a(x) \end{pmatrix} \bmod x^\ell - 1. \tag{A3}$$

The coefficients of Eq. (A2) can be divided term-by-term by $\gcd(a,b)$, which gives

$$a_1(x)u(x) + b_1(x)v(x) = 0 \bmod g(x). \tag{A4}$$

Indeed, if we denote $\chi(x) \equiv \gcd(a,b)$, according to Eq. (9), $\gcd(x^\ell - 1, \chi) = h(x)$, so that $\chi(x)$ must contain $h(x)$ as a factor, $\chi(x) = \chi_1(x)h(x)$, where $\chi_1(x)$ is relatively prime with $g(x)$ and, therefore, must be invertible modulo $g(x)$.

Eq. (A4) has a general solution

$$\begin{pmatrix} u(x) \\ v(x) \end{pmatrix} = \xi(x) \begin{pmatrix} b_1(x) \\ -a_1(x) \end{pmatrix} + g(x) \begin{pmatrix} i_1(x) \\ i_2(x) \end{pmatrix} \bmod x^\ell - 1, \tag{A5}$$

where $\xi(x)$, $i_1(x)$, and $i_2(x)$ are arbitrary polynomials in $F[x]/(x^\ell - 1)$. Now, if we take $i_1(x) = i_2(x) = 0$ with $\xi(x) \neq 0$ and $\deg \xi(x) < \deg g(x)$, we obtain exactly the set of pairs $[u(x), v(x)]$ which define the distance d'_Z of the AB code. The condition on the degree of $\xi(x)$ follows from the equivalent form of the orthogonality condition (A4),

$$\begin{pmatrix} u(x) \\ v(x) \end{pmatrix} \neq \alpha'(x)h(x) \begin{pmatrix} b_1(x) \\ -a_1(x) \end{pmatrix} \bmod x^\ell - 1.$$

Similarly, if we compare Eq. (A5) with the set of pairs which define the distance d'_X of the AB code, the codewords are generated by the polynomials $i_1(x)$, $i_2(x)$; for a non-trivial vector in the AB code we must ensure that it remains non-zero zero with any $\xi(x)$. Finally, notice that all vectors (A5) that *can* be made zero by choosing $\xi(x)$ but satisfy the condition (A2) contribute to the distance d'_X; the distance d_X is given by the minimum of the union of the two sets, or, equivalently, $d' \equiv \min(d'_X, d'_Z)$. □

3. Proof of Statement 2

Proof. Consider a vector $0 \neq e(x) = i(x)g(x)$ in the code $\mathcal{C}_{g(x)}$, where we must have $\deg i(x) < \deg h(x)$. The condition for $[e(x), 0]$ to be a trivial Z-vector (degenerate to zero) in the AB code $\mathrm{CSS}(H'_X, H_Z)$ reads

$$\begin{pmatrix} i(x)g(x) \\ 0 \end{pmatrix} = \xi(x) \begin{pmatrix} b_1(x) \\ -a_1(x) \end{pmatrix} \bmod x^\ell - 1. \tag{A6}$$

To analyze this expression, it is convenient to denote

$$a_2(x) = \gcd(a_1, x^\ell - 1), \quad b_2 = \gcd(b_1, x^\ell - 1),$$

where $\gcd(a_2, b_2) = 1$ since $\gcd(a_1, b_1) = 1$. The degeneracy condition (A6) then implies that $i(x)$ must contain a factor $h(x)/\gcd\big(h(x), a_2(x)\big)$. A similar condition for the other vector to be trivial gives that $i(x)$ must contain a factor $h(x)/\gcd\big(h(x), b_2(x)\big)$. These conditions cannot be simultanelously satisfied, as in this case $i(x)$ would be divisible by $h(x)$, which contradicts the assumption. □

4. Proof of Statement 6

Proof. Notice that the result in case (a) also follows directly from the bound constructed in Proposition 12 of Ref. 35.

In both cases, the components of the codeword $[u(x), v(x)]$ satisfy the equation

$$f(x)u(x) + v(x) = \xi(x)g(x) \bmod x^\ell - 1,$$

where $\xi(x) \in \mathbb{F}_q[x]$ is arbitrary. Thus, in case (a), with $u(x) = 0$, non-zero $v(x)$ must have $\mathrm{wgt}\, v(x) \geq d[g]$. Otherwise, with $u(x) \neq 0$, in case (a), assuming $f(x) = f_1(x)p(x)$ with $f_1(x)$ and $x^\ell - 1$ relatively prime, $v(x) = p(x)[\xi(x)q(x) - f_1(x)u(x)] \bmod x^\ell - 1$, where we used the assumption $g(x) = p(x)q(x)$. Then, any $v(x) \neq 0$ is in the code generated by $p(x)$ and thus $\mathrm{wgt}\, v(x) \geq d[p]$, while $u(x)$ is any non-zero, $\mathrm{wgt}\, u(x) \geq 1$. Otherwise, if $v(x) = 0$, a non-zero $u(x)$ must be in the code generated by $q(x)$, which gives $\mathrm{wgt}\, u(x) \geq d[q]$. The result in case (a) is obtained if we notice $d[pq] \geq d[q]$ because of the inclusion $\mathcal{C}_{pq} \subset \mathcal{C}_q$.

In case (b), for $u(x) \neq 0$ we have, instead,

$$v(x) = p(x)[\xi(x)q(x) - f_1(x)u(x)] - r(x)u(x) \bmod x^\ell - 1.$$

With the first term non-zero, its weight is bounded by $d[p]$, so that the total weight satisfies

$$\mathrm{wgt}(u) + \mathrm{wgt}(v) \geq \mathrm{wgt}(u) + \min\big(0, d[p] - \mathrm{wgt}(r)\,\mathrm{wgt}(u)\big);$$

taking the minimum over $\mathrm{wgt}(u)$ gives $d_0 \geq d[p]/\,\mathrm{wgt}(r)$. Otherwise, under assumptions we have, both $u(x)$ and $v(x)$ must be non-zero and in the code generated by $q(x)$, which gives $d_0 \geq 2d[q]$. □

5. Proof of Statement 7

Proof. Consider $e = [u(x), v(x)]$ of weight $s < d_g$ with $u(x)$ non-zero. In order for it to be a non-trivial codeword in $\mathrm{GB}(hf, h)$, we need

$$hfu + hv = 0 \bmod x^\ell - 1, \quad \text{and}$$
$$\begin{pmatrix} u(x) \\ v(x) \end{pmatrix} \neq \xi(x) \begin{pmatrix} h(x) \\ h(x)f(x) \end{pmatrix} \bmod x^\ell - 1.$$

The first statement is equivalent to $fu + v = 0 \bmod g$. Condition on the weight implies that u cannot be a factor of g; with g irreducible it further implies that $\gcd(u, g) = 1$. In this case we can find unique solution $f = v(x)/u(x) \bmod g(x)$. Indeed, $\gcd(u, g) = 1$ implies existence of polynomials A, B such that $Au + Bg = 1$. Thus, starting from $fu + v = wg$ with some w, we have

$$A(fu + v) + Bg = Awg + Bg, \quad u + Av = 0 \bmod g.$$

With $u \neq 0$, there is exactly one polynomial f with $\deg f < m - \deg h$ in this class. On the other hand, if

$u = 0$, the condition reads $v = 0 \bmod g$, which is impossible since it contradicts the assumption $s < d_g$. Now, the number of errors $e = [u(x), v(x)]$ of weight s and $u \neq 0$ is $\binom{2m}{s} - \binom{m}{s}$. Inequality (13) is a greedy bound that implies the existence of a polynomial f of degree smaller than $\ell - \deg h$ such that the code $\mathrm{GB}(hf, h)$ contains no non-trivial codewords of weight up to y. □

[1] S. Evra, T. Kaufman, and G. Zémor, Decodable quantum LDPC codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders, arXiv:2004.07935 (2020), unpublished.

[2] 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* (Association for Computing Machinery, New York, NY, USA, 2021) p. 1276–1288, 2009.03921.

[3] P. Panteleev and G. Kalachev, Quantum LDPC codes with almost linear minimum distance, IEEE Transactions on Information Theory **68**, 213 (2022), arXiv:2012.04068.

[4] N. P. Breuckmann and J. N. Eberhardt, Balanced product quantum codes, IEEE Transactions on Information Theory **67**, 6653 (2021), arXiv:2012.09271.

[5] P. Panteleev and G. Kalachev, Asymptotically good quantum and locally testable classical LDPC codes, arXiv:2111.03654 (2021), [Unpublished].

[6] N. P. Breuckmann and J. N. Eberhardt, Quantum low-density parity-check codes, PRX Quantum **2**, 10.1103/prxquantum.2.040101 (2021).

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

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

[9] I. Dumer, A. A. Kovalev, and L. P. Pryadko, Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes, Phys. Rev. Lett. **115**, 050502 (2015), 1412.6172.

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

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

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

[13] M. H. Freedman, D. A. Meyer, and F. Luo, Z_2-systolic freedom and quantum codes, in *Computational Mathematics* (Chapman and Hall/CRC, 2002) pp. 287–320.

[14] 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)* (2009) pp. 799–803.

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

[16] L. Guth and A. Lubotzky, Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds, Journal of Mathematical Physics **55**, 082202 (2014), arXiv:1310.5555.

[17] W. Zeng and L. P. Pryadko, Higher-dimensional quantum hypergraph-product codes with finite rates, Phys. Rev. Lett. **122**, 230501 (2019), 1810.01519.

[18] W. Zeng and L. P. Pryadko, Minimal distances for certain quantum product codes and tensor products of chain complexes, Phys. Rev. A **102**, 062402 (2020), arXiv:2007.12152.

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

[20] P. Panteleev and G. Kalachev, Degenerate quantum LDPC codes with good finite length performance, Quantum **5**, 585 (2021), 1904.02703.

[21] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, Sparse-graph codes for quantum error correction, IEEE Trans. Info. Th. **59**, 2315 (2004).

[22] N. Raveendran and B. Vasić, Trapping sets of quantum ldpc codes, Quantum **5**, 562 (2021), 2012.15297.

[23] A. Rigby, J. C. Olivier, and P. Jarvis, Modified belief propagation decoders for quantum low-density parity-check codes, Physical Review A **100**, 10.1103/physreva.100.012330 (2019).

[24] K.-Y. Kuo and C.-Y. Lai, Refined belief propagation decoding of sparse-graph quantum codes, IEEE Journal on Selected Areas in Information Theory **1**, 487 (2020).

[25] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A **54**, 1098 (1996).

[26] A. M. Steane, Simple quantum error-correcting codes, Phys. Rev. A **54**, 4741 (1996).

[27] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Info. Th. **52**, 4892 (2006), arXiv:quant-ph/0508070.

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

[29] C. L. Chen, W. W. Peterson, and E. J. Weldon, Some results on quasi-cyclic codes, Information and Control **15**, 407 (1969).

[30] T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2, IEEE Transactions on Information Theory **20**, 679 (1974).

[31] P. Semenov and P. Trifonov, Spectral method for quasi-cyclic code analysis, IEEE Communications Letters **16**, 1840 (2012).

[32] C. Güneri, S. Ling, and B. Özkaya, Quasi-cyclic codes, arXiv:2007.16029 (2020), to appear in "A Concise Encyclopedia of Coding Theory" by CRC Press.

[33] S. Lin and E. J. Weldon, Long BCH codes are bad, Information and Control **11**, 445 (1967).

[34] C. Martinez-Perez and W. Willems, Is the class of cyclic codes asymptotically good?, IEEE Transactions on Information Theory **52**, 696 (2006).

[35] C. Galindo, F. Hernando, and R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields and Their Applications **52**, 261 (2018).

[36] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, On quantum and classical bch codes, IEEE Transactions on Information Theory **53**, 1183 (2007), quant-ph/0604102.

[37] A. A. Kovalev, I. Dumer, and L. P. Pryadko, Design of additive quantum codes via the code-word-stabilized framework, Phys. Rev. A **84**, 062319 (2011).

[38] E. N. Gilbert, A comparison of signalling alphabets, Bell Labs Technical Journal **31**, 504 (1952).

[39] R. R. Varshamov, Estimate of the number of signals in error correcting codes, Dokl. Akad. Nauk SSSR **117**, 739 (1957), (In Russian).

[40] N. J. A. Sloane, Sequence A001122 on OEIS, downloaded on 2022/02/22.

[41] D. R. HEATH-BROWN, Artin's conjecture for primitive roots, The Quarterly Journal of Mathematics **37**, 27 (1986), https://academic.oup.com/qjmath/article-pdf/37/1/27/4354561/37-1-27.pdf.

[42] I. Haviv, M. Langberg, M. Schwartz, and E. Yaakobi, Non-linear cyclic codes that attain the Gilbert-Varshamov bound, in *2017 IEEE International Symposium on Information Theory (ISIT)* (2017) pp. 586–588.

[43] M. Shi, R. Wu, and P. Solé, Asymptotically good additive cyclic codes exist, IEEE Communications Letters **22**, 1980 (2018), arXiv:1709.09865.

[44] E. Berlekamp, Long primitive binary BCH codes have distance $d \sim 2n \ln R^{-1}/\log n \cdots$, IEEE Transactions on Information Theory **18**, 415 (1972).

[45] E. Berlekamp and J. Justesen, Some long cyclic linear binary codes are not so bad, IEEE Transactions on Information Theory **20**, 351 (1974).

[46] 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 **11**, 043029 (2009).

[47] S. Bravyi, D. Poulin, and B. Terhal, Tradeoffs for reliable quantum information storage in 2D systems, Phys. Rev. Lett. **104**, 050503 (2010), 0909.5200.

[48] B. Yoshida, Exotic topological order in fractal spin liquids, Phys. Rev. B **88**, 125122 (2013).

[49] G. V. Kalachev and P. A. Panteleev, On the minimum distance in one class of quantum LDPC codes, Intelligent systems. Theory and applications **24**, 87–117 (2020), [In Russian].

[50] M. Woolls and L. P. Pryadko, Homology-changing percolation transitions on finite graphs, arXiv:2011.02603 (2020), unpublished.

[51] A. A. Kovalev and L. P. Pryadko, Improved quantum hypergraph-product LDPC codes, in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)* (2012) pp. 348–352, arXiv:1202.0928.

[52] H. Bombin and M. A. Martin-Delgado, Optimal resources for topological two-dimensional stabilizer codes: Comparative study, Phys. Rev. A **76**, 012305 (2007).

[53] L. P. Pryadko, V. A. Shabashov, and V. K. Kozin, QDistRnd: A GAP package for computing the distance of quantum error-correcting codes (2022).

[54] R. Wang and L. P. Pryadko, Collection of codes constructed for "Distance bounds for generalized bicycle codes" (2022), `GitHub` repository; updated on 2022-03-30.