Quantum Kronecker sum-product low-density parity-check codes with finite rate

Alexey A. Kovalev and Leonid P. Pryadko

Phys. Rev. A **88**, 012311 — Published 11 July 2013

DOI: 10.1103/PhysRevA.88.012311

Quantum Kronecker sum-product low-density parity check codes with finite rate

Alexey A. Kovalev and Leonid P. Pryadko
Department of Physics & Astronomy, University of California, Riverside, California 92521, USA

We introduce an ansatz for quantum codes which gives the hypergraph-product (generalized toric) codes by Tillich and Zémor and generalized bicycle codes by MacKay et al. as limiting cases. The construction allows for both the lower and the upper bounds on the minimum distance; they scale as a square root of the block length. Many of thus defined codes have finite rate and a limited-weight stabilizer generators, an analog of classical low-density parity check (LDPC) codes. Compared to the hypergraph-product codes, hyperbicycle codes generally have wider range of parameters; in particular, they can have higher rate while preserving the estimated error threshold.

I. INTRODUCTION

Quantum computing can become a reality only with the help of some technique to protect the quantum information from decoherence due to inevitable coupling to the environment [1–4]. Quantum error correcting codes (QECCs) [5–7] offer such a protection; however, often at a high cost in the number of auxiliary qubits and with technologically difficult requirements [8–17]. Thus, an optimal choice of the employed code (or code family) is important.

Quantum codes with limited stabilizer generator weights, a quantum analog of classical low-density parity check (LDPC) codes [18, 19] could offer a viable solution: the simple structure of stabilizer generators simplify the individual measurements and enable parallelism, thus making the measurement cycle shorter. Further, by analogy with classical LDPC codes, there might exist efficient algorithms for encoding and decoding[19–23].

However, the parameters of quantum LDPC codes appear to be strongly restricted compared to their classical analogs because of the required commutativity of stabilizer generators. In fact, there are no known "good-distance" families of quantum LDPC codes with asymptotically finite relative distances, or any bounds suggesting their existence or nonexistence. It then becomes an intriguing question of the best asymptotic properties achievable with quantum LDPC codes. In such a setting explicit code designs become important, in particular, for establishing the lower bounds on the parameters: the number of encoded qubits k and minimum distance d for a given block length n (which also defines the code rate k/n), e.g., given the upper limit on the weight of stabilizer generators.

The best-known quantum LDPC codes (that are also local) are Kitaev's toric codes and related surface codes with the minimum distance scaling as $\sqrt{n}$ [10, 17, 24, 25]. Existence of single-qubit-encoding LDPC codes with the distance scaling as $\sqrt{n}\log n$ has been proved in Ref. 26. Tillich and Zémor proposed a finite-rate generalization of toric codes [27]. The construction relates a quantum code to a direct product of hypergraphs corresponding to two classical binary codes. Generally, thus obtained quantum LDPC codes have finite rates and the distances that scale as a square root of the block length.

In one of the first studies of quantum LDPC codes MacKay et al. [19] constructed so called bicycle codes. Numerically, these codes exhibit good decoding properties; however, the minimum distance of such codes is unknown. The quantum hypergraph-product codes [27], on the other hand, are an example of LDPC codes with known parameters; however, decoding such codes may be difficult. We recently established[28] the existence of a finite noise threshold, with and without syndrome measurement errors, for limited-stabilizer-weight quantum hypergraph-product codes, as well as for any such LDPC code family with the distance scaling as the square root of block length. These results, however, might not apply to the constructions of quantum LDPC codes based on finite geometries[29, 30] and to the constructions based on Cayley graphs[21] due to the unbounded weight of stabilizer generators.

In this work, we introduce a general bipartite ansatz for quantum CSS codes, and use it to construct a large family of codes that in the limiting cases reduce to (generalized) bicycle and hypergraph-product codes—the *hyperbicycle* codes. The bipartite ansatz comprises a number of known quantum code families, and can be used to obtain a double-size CSS code from a generic (non-CSS) stabilizer code. The hyperbicycle codes contain new quantum LDPC code families with finite rates and distances that scale as a square root of the block length. In addition, the hyperbicycle construction can improve the rate of the hypergraph-product codes while preserving the estimated error threshold.

II. PRELIMINARIES

In this section, we define classical and quantum error correcting codes. We also review some of the known LDPC code constructions.

A. Classical error correcting codes

A *classical* q-ary block error-correcting code $(n, K, d)_q$ is a set of K length-n strings over an alphabet with q symbols. Different strings represent K distinct messages which can be transmitted. The (Hamming) distance be-

tween two strings is the number of positions where they differ. Distance d of the code $\mathcal{C}$ is the minimum distance between any two different strings from $\mathcal{C}$.

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

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

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

For non-binary codes, there is also a distinct class of *additive* classical codes, defined as subsets of $\mathbb{F}_q^n$ closed under addition (in the binary case these are just linear codes).

A code $\mathcal{C}$ is cyclic if inclusion $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Codes that are both linear and cyclic are particularly simple: by mapping vectors to polynomials in the natural way, $\mathbf{c} \to c(x) \equiv c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$, it is possible to show that any such code consists of polynomials which are multiples of a canonical generator polynomial $g(x)$, which must divide $x^n - 1$ (using the algebra corresponding to the field $\mathbb{F}_q$). The quotient defines the *check polynomial* $h(x)$,

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

which is the reverse of the canonical generator polynomial of the dual code, $h^{\mathrm{rev}}(x) \equiv x^{\deg(h)}h(1/x)$. The degree of the generator polynomial is $\deg g(x) = n - k$. The corresponding generator matrix G can be chosen as the first k rows of the *circulant matrix* C_n formed by subsequent shifts of the vector that corresponds to $g(x)$, explicitly:

$$C_n = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-1} \\ g_{n-1} & g_0 & g_1 & & \\ g_{n-2} & g_{n-1} & g_0 & & \vdots \\ \vdots & & & \ddots & \\ g_1 & g_2 & g_3 & \cdots & g_0 \end{pmatrix}. \tag{3}$$

B. Quantum stabilizer codes

Qubit-based quantum error correcting codes (QECCs) are defined on the complex Hilbert space $\mathcal{H}_2^{\otimes n}$ where $\mathcal{H}_2$ is the complex Hilbert space of a single qubit $\alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. Any operator acting on such an n-qubit state can be represented as a combination of Pauli operators which form the Pauli group $\mathscr{P}_n$ of size 2^{2n+2}:

$$\mathscr{P}_n = i^m \{I, X, Y, Z\}^{\otimes n}, \; m = 0, \ldots, 3\,, \tag{4}$$

where i^m is the phase, X, Y, Z are the usual Pauli matrices, and I is the two-by-two identity matrix. It is customary to map the Pauli operators, up to a phase, to two binary strings, $\mathbf{v}, \mathbf{u} \in \{0,1\}^{\otimes n}$ [31],

$$U \equiv i^{m'} X^{\mathbf{v}} Z^{\mathbf{u}} \to (\mathbf{v}, \mathbf{u}), \tag{5}$$

where $X^{\mathbf{v}} = X_1^{v_1} X_2^{v_2} \ldots X_n^{v_n}$ and $Z^{\mathbf{u}} = Z_1^{u_1} Z_2^{u_2} \ldots Z_n^{u_n}$. A product of two quantum operators corresponds to a sum (mod 2) of the corresponding pairs $(\mathbf{v}_i, \mathbf{u}_i)$.

An $[[n,k,d]]$ stabilizer code $\mathcal{Q}$ is a 2^k-dimensional subspace of the Hilbert space $\mathcal{H}_2^{\otimes n}$ stabilized by an Abelian stabilizer group $\mathscr{S} \subset \mathscr{P}_n$ such that $-\mathbb{1} \notin \mathscr{S}$ [32]. Explicitly,

$$\mathcal{Q} = \{|\psi\rangle : S|\psi\rangle = |\psi\rangle, \forall S \in \mathscr{S}\}. \tag{6}$$

The group $\mathscr{S}$ is generated by the necessarily-Hermitian commuting Pauli operators (*stabilizer generators*) $G_1, \ldots, G_{n-k}$, $\mathscr{S} = \langle G_1, \ldots, G_{n-k}\rangle$. Each generator $G_i \in \mathscr{S}$ is mapped according to Eq. (5) in order to obtain the binary generator matrix $H = (A_X|A_Z)$ in which each row corresponds to a generator, with rows of A_X formed by $\mathbf{v}$ and rows of A_Z formed by $\mathbf{u}$ vectors. For generality, we assume that the matrix H may also contain unimportant linearly dependent rows which are added after the mapping has been done. The commutativity of stabilizer generators corresponds to the following condition on the binary matrices A_X and A_Z:

$$A_X A_Z^T + A_Z A_X^T = 0 \pmod 2. \tag{7}$$

A more narrow set of Calderbank-Shor-Steane (CSS) codes [33] contains codes whose stabilizer generators can be chosen to contain products of only Pauli X or Pauli Z operators. For these codes the stabilizer generator matrix can be chosen in the form:

$$H = \left(\begin{array}{c|c} G_X & 0 \\ 0 & G_Z \end{array}\right), \tag{8}$$

where the commutativity condition simplifies to $G_X G_Z^T = 0$.

The dimension of a quantum code is

$$k = n - \mathrm{rank}\, H; \tag{9}$$

for a CSS code this simplifies to

$$k = n - \mathrm{rank}\, G_X - \mathrm{rank}\, G_Z. \tag{10}$$

The distance d of a quantum stabilizer code is given by the minimum weight of an operator U which commutes with all operators from the stabilizer $\mathscr{S}$, but is not a part of the stabilizer, $U \notin \mathscr{S}$. In terms of the binary vector pairs $(\mathbf{a}, \mathbf{b})$, this is equivalent to a minimum weight of

the bitwise OR$(\mathbf{a}, \mathbf{b})$ of all pairs satisfying the symplectic orthogonality condition,

$$A_X \mathbf{b} + A_Z \mathbf{a} = 0, \tag{11}$$

which are not linear combinations of the rows of H. A code of distance d can detect any error of weight up to $d-1$, and correct any error of weight up to $\lfloor d/2 \rfloor$.

In an equivalent representation, one can map any Pauli operator U in Eq. (5), to a quaternary vector over $\mathbb{F}_4$, $\mathbf{e} \equiv \mathbf{u} + \omega \mathbf{v}$. A product of two quantum operators corresponds to a sum (mod 2) of the corresponding vectors. Two Pauli operators commute if and only if the *trace inner product* $\mathbf{e}_1 * \mathbf{e}_2 \equiv \mathbf{e}_1 \cdot \overline{\mathbf{e}}_2 + \overline{\mathbf{e}}_1 \cdot \mathbf{e}_2$ of the corresponding vectors is zero (which is equivalent to the symplectic orthogonality condition), where $\overline{\mathbf{e}} \equiv \mathbf{u} + \overline{\omega} \mathbf{v}$. With this map, generators of a stabilizer group are mapped to rows of a generator $\mathbb{G}$ of an additive code over $\mathbb{F}_4$, with the condition that the trace inner product of any two rows vanishes[31] [see Eq. (7)]. The vectors generated by rows of $\mathbb{G}$ correspond to stabilizer generators which act trivially on the code; these vectors form the *degeneracy group* and are omitted from the distance calculation. For CSS codes in Eq. (8) the generator matrix is a direct sum $\mathbb{G} = G_x \oplus \omega G_z$. In the following, we will use both, quaternary and binary, representations.

A classical LDPC code is a code with a sparse parity-check matrix H. For a regular (j, l) quantum LDPC code, every column and every row of $\mathbb{G}$ have weights j and l respectively, while for a (j, l)-limited quantum LDPC code these weights are limited from above by j and l.

In the case when a quantum LDPC code is represented in terms of the binary matrix H, the same restrictions apply to the matrix OR(A_X, A_Z).

C. Bicycle codes

In one of the first studies of quantum LDPC codes, MacKay et. al. proposed a CSS code construction[19] which can be written in a block form as:

$$G_X = G_Z = \left(A, A^T\right), \tag{12}$$

where A is a binary circulant matrix. Bicycle codes are obtained after some of the rows in G_X or G_Z are deleted. Numerically, such codes show good error-correction capabilities[19, 20]; however, the distance of such codes is unknown.

D. Hypergraph-product codes

Tillich and Zémor proposed a CSS construction which can be interpreted as a finite-rate generalization of toric codes[27] and allows for LDPC constructions. For such codes, the generator matrix is constructed from a product of two hypergraphs, each corresponding to a parity check matrix of a classical binary code. The resulting CSS code

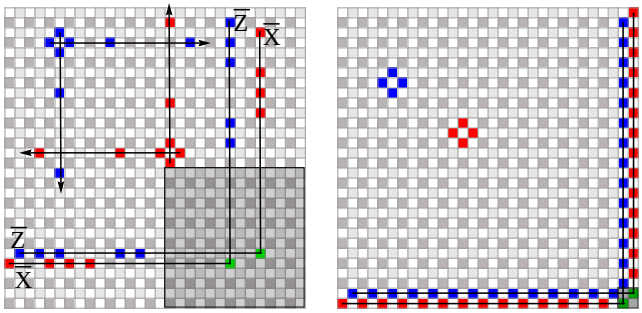

FIG. 1: (Color online) Left: Two stabilizer generators (marked by arrows) and two pairs of anticommuting logical operators (marked by lines) of a $[[450, 98, 5]]$ code in Eq. (13) formed by circulant matrices $\mathcal{H}_1 = \mathcal{H}_2$ corresponding to coefficients of the polynomial $h(x) = 1 + x + x^3 + x^7$ (red squares – X operators, blue squares – Z operators, green squares – overlap of Z and X operators, dark and light gray squares – dual sublattices of physical qubits, white squares – empty spaces). All other stabilizer generators are obtained by shifts over the same sublattice with periodic boundaries. In the shaded region, each gray square uniquely corresponds to a different logical operator, thus 98 encoded logical qubits. Right: same for the toric code $[[450, 2, 15]]$.

can be recast in a matrix form with the generators given by[34]

$$\begin{aligned} G_X &= (E_2 \otimes \mathcal{H}_1, \mathcal{H}_2 \otimes E_1), \\ G_Z &= (\mathcal{H}_2^T \otimes \widetilde{E}_1, \widetilde{E}_2 \otimes \mathcal{H}_1^T). \end{aligned} \tag{13}$$

Here each sublattice block is constructed as a Kronecker product (denoted with "$\otimes$") of two binary matrices $\mathcal{H}_1$ (dimensions $r_1 \times n_1$) and $\mathcal{H}_2$ (dimensions $r_2 \times n_2$), and E_i and $\widetilde{E}_i$, $i = 1, 2$, are unit matrices of dimensions given by r_i and n_i, respectively. The matrices G_X and G_Z, respectively, have $r_1 r_2$ and $n_1 n_2$ rows (not all of the rows are necessarily linearly independent), and they both have $n \equiv r_2 n_1 + r_1 n_2$ columns, which gives the block length of the quantum code. The commutativity condition $G_X G_Z^T = 0$ is obviously satisfied by Eq. (13) since the Kronecker product obeys $(A \otimes B)(C \otimes D) = AC \otimes BD$.

The parameters $[[n, k, d]]$ of thus constructed quantum code are determined by those of the four classical codes which use the matrices $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_1^T$, and $\mathcal{H}_2^T$ as the parity-check matrices. The corresponding parameters are introduced as

$$\mathcal{C}_{\mathcal{H}_i} = [n_i, k_i, d_i], \quad \mathcal{C}_{\mathcal{H}_i^T} = [\widetilde{n}_i, \widetilde{k}_i, \widetilde{d}_i], \quad i = 1, 2, \tag{14}$$

where we use the convention [27] that the distance $d_i(\widetilde{d}_i) = \infty$ if $k_i(\widetilde{k}_i) = 0$. The matrices $\mathcal{H}_i$ are arbitrary, and are allowed to have linearly-dependent rows and/or columns. As a result, both $k_i = n_i - \operatorname{rank} \mathcal{H}_i$ and $\widetilde{k}_i = \widetilde{n}_i - \operatorname{rank} \mathcal{H}_i$ may be non-zero at the same time as the block length of the "transposed" code $\mathcal{C}_{\mathcal{H}_i^T}$ is given by the number of rows of $\mathcal{H}_i$, $\widetilde{n}_i = r_i$.

Specifically, for the hypergraph-product code (13), we have $n = r_2 n_1 + r_1 n_2$, $k = 2k_1 k_2 - k_1 s_2 - k_2 s_1$ with

$s_i = n_i - r_i$, $i = 1, 2$ (Theorem 7 from Ref. 27), while the distance d satisfies the conditions $d \geq \min(d_1, d_2, \widetilde{d}_1, \widetilde{d}_2)$ (Theorem 9 from Ref. 27), and two upper bounds (Lemma 10 from Ref. 27): if $k_1 > 0$ and $\widetilde{k}_2 > 0$, then $d \leq \min(d_1, \widetilde{d}_2)$; if $k_2 > 0$ and $\widetilde{k}_1 > 0$, then $d \leq \min(d_2, \widetilde{d}_1)$.

A full-rank parity check matrix $\mathcal{H}_1$ of a binary code with parameters $\mathcal{C}_{\mathcal{H}_1} = [n_1, k_1, d_1]$ ($r_1 = n_1 - k_1$, $\widetilde{k}_1 = 0$) and $\mathcal{H}_2 = \mathcal{H}_1^T$ defines a quantum code with parameters $[[(n_1 - k_1)^2 + n_1^2, k_1^2, d_1]]$[27]. Furthermore, a family of finite-rate (h, v)-limited classical LDPC codes with asymptotically finite relative distance will correspond to a family of finite-rate $(v, h + v)$-limited quantum LDPC codes with the distance scaling as $d \propto \sqrt{n}$.

III. TWO-SUBLATTICE CODES

The commutativity condition for QECCs in Eq. (7) puts a strong limitation on suitable parity check matrices. The problem becomes even more difficult when the additional requirement of LDPC structure is imposed. In particular, this strongly limits possible counting arguments for establishing bounds on code parameters. In such a setting, constructions based on some ansatz become very useful. In the following, we study several CSS constructions based on two sublattices corresponding to the columns of the binary matrices $A_1(B_2^T)$ and $B_1(A_2^T)$:

$$G_X = (A_1, B_1), \quad G_Z = \left(B_2^T, A_2^T\right), \tag{15}$$

where the matrices A_i, B_i, $i = 1, 2$, satisfy the condition $A_1 B_2 + B_1 A_2 = 0$ (we assume binary linear algebra throughout this paper).

A. Two-sublattice CSS code from a generic stabilizer code

A large number of two-sublattice CSS codes (15) can be obtained from regular stabilizer codes by the following

Theorem 1. *For any quantum stabilizer code* $[[n, k, d]]$ *with the generator matrix*

$$H = (A|B), \tag{16}$$

there is a reversible mapping to a two-sublattice quantum CSS code (15) with $A_1 = A_2^T = A$, $B_1 = B_2^T = B$ *and the parameters* $[[2n, 2k, d']]$, *where* $d \leq d' \leq 2d$.

Proof. Explicitly, the generator matrices are

$$G_X = (A, B), \quad G_Z = (B, A). \tag{17}$$

The dimension of the code simply follows from Eqs. (9), (10), given that $\operatorname{rank} G_X = \operatorname{rank} G_Z = \operatorname{rank} H$. Any binary vector $\mathbf{e} = (\mathbf{a}|\mathbf{b})$ such that $A\mathbf{b} + B\mathbf{a} = 0$ maps to a pair of double-size vectors $\mathbf{e}_z = (\mathbf{b}, \mathbf{a})$, $\mathbf{e}_x = (\mathbf{a}, \mathbf{b})$ which satisfy $G_X \mathbf{e}_z = 0$, $G_Z \mathbf{e}_x = 0$; the corresponding weights obey the inequality $\operatorname{wgt} \mathrm{OR}(\mathbf{a}, \mathbf{b}) \leq \operatorname{wgt}(\mathbf{a}, \mathbf{b}) \leq 2 \operatorname{wgt} \mathrm{OR}(\mathbf{a}, \mathbf{b})$, which ensures the conditions on the distance. It is easy to check that the reverse mapping also works. □

Note that an original code that exceeds the generic quantum Gilbert-Varshamov (GV) bound[35] is mapped to a CSS code that exceeds the version of the GV bound specific for such codes[33]. Also, an original sparse code is mapped to a sparse code, with the same limit on the column weight, and row weight at most doubled. So, if one has a non-CSS code and wants to use one of the measurement techniques designed for such codes, this can be done by first constructing the corresponding CSS code.

We use the reverse version of this mapping in Sec. IV H to construct the non-CSS versions of hyperbicycle codes.

B. Generalized bicycle codes

Let us now start with two commuting square n by n binary matrices, $AB + BA = 0$. Then, we can satisfy the general two-sublattice ansatz (15) by taking $A_1 = A_2 = A$, $B_1 = B_2 = B$, which gives

$$G_X = (A, B), \quad G_Z = \left(B^T, A^T\right). \tag{18}$$

In particular, the commutativity is guaranteed for circulant matrices A and B, which corresponds to a generalization of the bicycle codes[19], see Eq. (12). In this case, we map the linear combinations of rows in G_X to a classical length-n additive cyclic code over $\mathbb{F}_4$, where elements of the code are constructed from the generator matrix $\mathbb{G} = \omega A + B$. If the circulant matrices A and B are generated by the polynomials $f_1(x)$ and $f_2(x)$, respectively, the space of the additive code corresponding to the stabilizer is generated by the polynomial $g(x) = f_1(x)\omega + f_2(x)$ modulo $x^n - 1$. That is, elements of the stabilizer are given by the coefficients of the polynomials $b(x)g(x) \bmod (x^n - 1)$, with arbitrary binary $b(x)$.

A canonical form of cyclic additive codes over $\mathbb{F}_4$ has been introduced in Ref. 31, where Theorem 14 states that any cyclic additive code can be represented via two generators as $\langle \omega p(x) + q(x), r(x) \rangle \bmod (x^n - 1)$ with $p(x) = \gcd[f_1(x), x^n - 1]$, $r(x) = \gcd[(x^n - 1) f_2(x)/p(x), x^n - 1]$ and $\deg q(x) < \deg r(x)$ (gcd stands for the greatest common divisor). The code dimensionality is $k = 2n - \deg p(x) - \deg r(x)$. The special case of cyclic additive codes with a single generator has been analyzed in Ref. 36 in which case the code dimensionality simplifies to $k = n - \deg p(x)$, which formally corresponds to $r(x) = x^n - 1$. Note that, unlike the case of the usual quantum additive cyclic codes[31, 36], the mapping from Eq. (18) works for any circulant matrices A and B; no additional commutativity condition is needed for the generator polynomials $p(x)$, $q(x)$, and $r(x)$. The parameters of thus obtained quantum codes are given by

Theorem 2. *The generalized bicycle codes in Eq. (18) have the block length $n' = 2n$, the number of encoded qubits $k = 2\deg p(x) + 2\deg r(x) - 2n$ [$k = 2\deg p(x)$ in the single generator case] and the distance exceeding or equal that of the classical code over $\mathbb{F}_4$ formed by codewords orthogonal to $\mathbb{G}$ with respect to the trace inner product.*

Proof. The code dimensionality immediately follows from the parameters of the canonical form of the code generated by $g(x)$. The orthogonal code contains the quantum code, hence the distance estimate. □

Note that the distance estimate in Theorem 2 is tight only for pure codes since a possibility for degeneracy is not taken into consideration.

Example 1. *Suppose a cyclic linear code $[n, k, d]$ over $\mathbb{F}_4$ with a generator polynomial $\varrho(x)$ that divides $x^n - 1$ generates a code space $\mathbb{G}^\perp$. Then the parameters of the quantum CSS code in Eq. (18) are $[[2n, 2n - 4\deg \varrho(x), \geq d]]$. This construction is similar to non-CSS code construction from linear cyclic codes in Ref. 31, except that here the dual code does not have to be self-orthogonal. For a cyclic $[30, 25, 4]$ code with $\varrho(x) = (1 + x)^2(1 + \omega x)(1 + x + \omega x^2)$ we obtain a quantum code $[[60, 40, 4]]$.*

Example 2. *A CSS family of odd-distance rotated toric codes [34] is obtained for $f_1(x) = (1+x^{2t^2+1})$ and $f_2(x) = x(1 + x^{2t^2-1})$, $t = 1, 2, \ldots$ by construction in Eq. (18). These codes have the parameters $[[2t^2 + 2(t + 1)^2, 2, 2t + 1]]$. Explicitly, $[[10, 2, 3]]$, $[[26, 2, 5]]$, $[[50, 2, 7]]$, $[[82, 2, 9]]$, ...*

The constructions in Theorems 1 and 2 [Eqs. (17) and (18) respectively] coincide for symmetric matrices, $A = A^T$, $B = B^T$. Then, from a generalized bicycle code with symmetric matrices corresponding to two palindromic polynomials $f_i(x) = x^{\deg f_i(x)} f_i(1/x)$, $i = 1, 2$, we can obtain non-CSS halved bicycle codes in Eq. (16) by applying the reverse of Theorem 1 to the matrices A and B [34].

Example 3. *A non-CSS family of smallest odd-distance rotated toric codes [36] is obtained for palindromic $f_1(x) = x^t(1 + x^{2t^2+1})$ and $f_2(x) = x^{t+1}(1 + x^{2t^2-1})$, $t = 1, 2, \ldots$ by construction in Eq. (16). These codes have the parameters $[[t^2 + (t + 1)^2, 1, 2t + 1]]$. Explicitly, $[[5, 1, 3]]$, $[[13, 1, 5]]$, $[[25, 1, 7]]$, $[[41, 1, 9]]$, ...*

The codes in the last two examples exceed the lower bound in Theorem 2 due to degeneracy.

C. Tensor-product constructions and Haah's codes

Further generalization of the bicycle-like construction in Eq. (18) can be achieved by combining tensor products with commuting (e.g., circulant) matrices. The most general form of two-sublattice tensor-product codes has the form:

$$A = \textstyle\sum_{i_1 \ldots i_k} \mathcal{H}^A_{i_1,1} \otimes \ldots \otimes \mathcal{H}^A_{i_k,k},$$
$$B = \textstyle\sum_{i_1 \ldots i_k} \mathcal{H}^B_{i_1,1} \otimes \ldots \otimes \mathcal{H}^B_{i_k,k},$$

where $\mathcal{H}^A_{i,l}$ and $\mathcal{H}^B_{i,l}$ are matching, pairwise-commuting binary square matrices (i.e., $\mathcal{H}^A_{i,l}\mathcal{H}^B_{j,l} + \mathcal{H}^B_{j,l}\mathcal{H}^A_{i,l} = 0$ for any i and j). For circulant matrices $\mathcal{H}^A_{i,l}$ and $\mathcal{H}^B_{j,l}$ the commutativity is automatically satisfied.

Several examples of such codes are given by the Haah's codes[37]. These are local codes in 3D without string logical operators, and thus may lead to realizations of self-correcting quantum memories. Such codes are defined on two sublattices and have exactly the tensor-product structure discussed here. In Table I, we list four codes presented in Ref. 37. These codes are essentially constructed from a repetition code and it is straightforward to generalize this construction to arbitrary cyclic binary codes by using the corresponding binary circulant matrix $\mathcal{H}_1$. The commutativity of matrices A and B in Eq. (15) immediately follows.

A non-CSS generalization of construction in Table I can be achieved by using symmetric circulant matrices [see non-CSS construction in Eq. (16)].

IV. CSS AND NON-CSS HYPERBICYCLE CODES

This section contains our most important results. We show that the families of hypergraph-product and generalized bicycle codes can be obtained as limiting cases of a larger family of *hyperbicycle* codes. The main advantage of this construction is that it gives a number of previously unreported families of quantum codes with tight bounds on, or even explicitly known distance. This includes many strongly degenerate LDPC codes with the distance much greater than the maximum weight of a stabilizer generator. In this section we discuss the construction of such codes, their parameters, and give examples.

A. CSS hyperbicycle codes: construction

We define the hyperbicycle CSS codes as follows:

$$\begin{aligned} G_X &= \left(E_b \otimes \textstyle\sum_i I_i^{(\chi)} \otimes a_i,\ \sum_i b_i \otimes I_i^{(\chi)} \otimes E_a\right), \\ G_Z &= \left(\textstyle\sum_i b_i^T \otimes \widetilde{I}_i^{(\chi)} \otimes \widetilde{E}_a,\ \widetilde{E}_b \otimes \sum_i \widetilde{I}_i^{(\chi)} \otimes a_i^T\right). \end{aligned} \tag{19}$$

Here we introduce two sets of binary matrices a_i (dimensions $r_1 \times n_1$, $i = 0, \ldots, c-1$) and b_i (dimensions $r_2 \times n_2$, $i = 0, \ldots, c-1$); E_a, E_b, $\widetilde{E}_a$ and $\widetilde{E}_b$ are unit matrices of dimensions given by r_1, r_2, n_1 and n_2, respectively. Matrices $I_i^{(\chi)}$ ($\widetilde{I}_i^{(\chi)}$) are permutation matrices (dimensions $c \times c$) given by a product of two permutation matrices, i.e. $I_i^{(\chi)} = S_\chi I_i$ ($\widetilde{I}_i^{(\chi)} = S_\chi^T I_i^T$) where

Code 1.	$A = \mathcal{H}_1 \otimes E \otimes E + E \otimes \mathcal{H}_1 \otimes E + E \otimes E \otimes \mathcal{H}_1$ $B = \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes E + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes E \otimes \mathcal{H}_1$
Code 2.	$A = \mathcal{H}_1 \otimes E \otimes E + E \otimes \mathcal{H}_1 \otimes E + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes E \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_1$ $B = E \otimes E \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes E + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes E \otimes \mathcal{H}_1$
Code 3.	$A = \mathcal{H}_1 \otimes E \otimes E + E \otimes \mathcal{H}_1 \otimes E + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes E \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_1$ $B = \mathcal{H}_1 \otimes E \otimes E + E \otimes \mathcal{H}_1 \otimes E + E \otimes E \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes E + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_1$
Code 4.	$A = E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes E \otimes \mathcal{H}_1 + E \otimes \mathcal{H}_1 \otimes E$ $B = \mathcal{H}_1 \otimes E \otimes E + E \otimes E \otimes \mathcal{H}_1 + E \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 + \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_1$

TABLE I: Tensor-product two-sublattice representation of Haah's codes corresponding to Eq. (15) where $\mathcal{H}_1$ is a circulant matrix corresponding to parity check polynomial $p(x) = 1 + x$ of a repetition code, E is a unit matrix of the same dimensions with $\mathcal{H}_1$ and the summation is mod 2.

$(I_i)_{kj} = \delta_{j-k,i \bmod c}$ is a circulant permutation matrix, $(S_\chi)_{kj} = \delta_{j-k,(k-1)(\chi-1) \bmod c}$ and the positive integers c and χ are coprime . A version of this construction for $c = 2$ and $\chi = 1$ has been previously reported by us in Ref. 34.

The matrices G_X and G_Z, respectively, have cr_1r_2 and cn_1n_2 rows (not all of the rows are linearly independent), and they both have

$$n \equiv c(r_1n_2 + r_2n_1) \tag{20}$$

columns, which gives the block length of the quantum code. The commutativity condition $G_X G_Z^T = 0$ is obviously satisfied by Eq. (19) since the permutation matrices commute with each other. Note that for $c = 1$ and $\chi = 1$ we recover the hypergraph-product codes in Eq. (13) and for $r_i = n_i = 1$, $i = 1, 2$, (i.e., a_i and b_i given by binary numbers) we recover the generalized bicycle code construction in Eq. (18).

In order to characterize codes in Eq. (19) it is convenient to introduce the "tiled" binary matrices:

$$\begin{array}{ll} \mathcal{H}_1 = \sum_i I_i^{(\chi)} \otimes a_i, & \mathcal{H}_2 = \sum_i b_i \otimes I_i^{(\chi)}, \\ \widetilde{\mathcal{H}}_1 = \sum_i \widetilde{I}_i^{(\chi)} \otimes a_i^T, & \widetilde{\mathcal{H}}_2 = \sum_i b_i^T \otimes \widetilde{I}_i^{(\chi)}. \end{array} \tag{21}$$

For example, for $c = 5$ and $\chi = 2$ we have

$$\mathcal{H}_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 & a_5 & a_1 \\ a_5 & a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}; \tag{22}$$

note that the subsequent block rows are shifted by $\chi = 2$ positions.

For the following discussion it is useful to define auxiliary binary matrices:

$$\mathcal{H}_1^0 = \sum_i I_i \otimes a_i, \quad \mathcal{H}_2^0 = \sum_i b_i \otimes I_i. \tag{23}$$

In addition, we will also be using the matrix

$$\overleftrightarrow{\mathcal{H}}_2^0 = \sum_i I_i \otimes b_i. \tag{24}$$

which can be obtained from $\mathcal{H}_2^0$ by row and column permutations. In terms of the matrices (23) we can write:

$$\begin{array}{ll} \mathcal{H}_1 = (S_\chi \otimes E_a) \cdot \mathcal{H}_1^0, & \mathcal{H}_2 = (E_b \otimes S_\chi) \cdot \mathcal{H}_2^0, \\ \widetilde{\mathcal{H}}_1 = (S_\chi^T \otimes E_a) \cdot \mathcal{H}_1^{0T}, & \widetilde{\mathcal{H}}_2 = (E_b \otimes S_\chi^T) \cdot \mathcal{H}_2^{0T}. \end{array} \tag{25}$$

With this notation, it is clear that the generator matrices (19) correspond to the hypergraph code generators (13), except that the identity matrices E_i, $\widetilde{E}_i$ are now reduced in size by a factor of $1/c$. Respectively, the hyperbicycle codes defined by Eq. (19) with $c > 1$ can be viewed as reduced hypergraph codes. Indeed, the block length of the original hypergraph code (13) defined with the present binary matrices (21) is

$$n_{\rm orig} = c^2(r_1n_2 + r_2n_1). \tag{26}$$

B. CSS hyperbicycle codes: dimension

Just as for the hypergraph codes, the parameters of classical codes $\mathcal{C}_{\mathcal{H}_i}$ and $\mathcal{C}_{\widetilde{\mathcal{H}}_i}$ with parity check matrices $\mathcal{H}_i$ and $\widetilde{\mathcal{H}}_i$ in Eq. (21) contain information about the parameters of the quantum code in Eq. (19). We denote the distances of these binary codes as d_i and $\widetilde{d}_i$, and their dimensions as k_i and $\widetilde{k}_i$, $i = 1, 2$.

Regardless of the choice of the matrices a_i, b_i, the codes $\mathcal{C}_{\mathcal{H}_i}$ and $\mathcal{C}_{\widetilde{\mathcal{H}}_i}$ are quasicyclic, with the cycle of length equal to the dimension c of the cyclic permutation matrices $I_i^{(\chi)}$ ($\widetilde{I}_i^{(\chi)}$), $i = 1, 2$. Indeed, the corresponding block shifts merely lead to permutations of rows of the check matrices $\mathcal{H}_i$, $\widetilde{\mathcal{H}}_i$ [see Eq. (22)]. In order to define the dimension of the corresponding hyperbicycle codes with generators (19), we first classify the vectors in $\mathcal{C}_{\mathcal{H}_i}$ and $\mathcal{C}_{\widetilde{\mathcal{H}}_i}$ with respect to this circulant symmetry.

We start with the case of a binary cyclic code with block length c, with the generator polynomial $g(x)$, which divides $x^c - 1$. [Polynomial algebra in this section is done modulo 2.] Any codeword corresponds to a polynomial $w(x)$ which contains $g(x)$ as a factor, and, therefore, every cyclotomic root of $g(x)$ is also a root of $w(x)$. However, the particular polynomial $w(x) = g(x)f(x)$ may

also contain other factors of x^c-1 and thus have symmetry different from that of $g(x)$. We can define a linear space $\mathcal{C}^{(p)}$ of length-c vectors corresponding to $w(x)$ with the exact symmetry of $g(x)$ where $p(x)\equiv(x^c-1)/g(x)$ by defining the equivalence $w_1(x)\equiv w_2(x)$ for a given $g(x)$ as $f_1=f_2 \bmod p'(x)$ for all $p'(x)$ such that $p'(x)\neq p(x)$ is a factor of $p(x)$. The same equivalence can be also defined modulo greatest common divisor (gcd) of all such polynomials $p'(x)$. In terms of the corresponding check polynomial $p(x)$, the dimension $k_0^{(p)}$ of thus defined space $\mathcal{C}^{(p)}$ is zero unless $p(x)$ is a non-zero power of an irreducible polynomial $p_\alpha(x)$, in which case $k_0^{(p)}=\deg p_\alpha(x)$.

For the quasicyclic code $\mathcal{C}_{\mathcal{H}_1}$ with the first check matrix in Eq. (21), the vector $\mathbf{w}$ is in the symmetry class of $p(x)$, where $p(x)$ divides x^c-1, if $\mathbf{w}$ satisfies the condition $[p(I_1)\otimes E_a]\,\mathbf{w}=0$ and is not a member of such a symmetry class of any factor of $p(x)$. For each polynomial $p(x)$, the l.h.s. in these equations is a sum of cyclic shifts of the vector $\mathbf{w}$ corresponding to each non-zero coefficient of $p(x)$. We denote the dimension of the subcode of $\mathcal{C}_{\mathcal{H}_1}$ with all vectors in the symmetry class of $p(x)$ as $k_1^{(p)}$. The symmetry implies that $k_1^{(p)}$ must contain the dimension $k_0^{(p)}$ introduced in the previous paragraph as a factor, and, in particular, $k_1^{(p)}$ must be zero whenever $k_0^{(p)}$ is zero. A convenient basis of $\mathcal{C}^{(p)}_{\mathcal{H}_1}$ can be constructed using the following

Lemma 1. *Any vector of the subcode $\mathcal{C}^{(p)}_{\mathcal{H}_1}$ can be chosen in the form*

$$\mathbf{w}=\sum_{i=0}^{k_0^{(p)}-1}(I_i\cdot\mathbf{g})\otimes\boldsymbol{\alpha}_i, \tag{27}$$

where the vector $\mathbf{g}$ corresponds to the generating polynomial $g(x)\equiv(x^c-1)/p(x)$; the vectors $(I_s\otimes E_a)\mathbf{w}$, $0\le s<k_0^{(p)}$, are linearly independent.

Proof. Any vector of the subcode $\mathcal{C}^{(p)}_{\mathcal{H}_1}$ can be expanded in the form $\boldsymbol{\omega}_i^{(p)}\otimes\mathbf{e}_i$, where $\mathbf{e}_i$ are all distinct weight-one vectors, and $\boldsymbol{\omega}_i^{(p)}$ are vectors from $\mathcal{C}^{(p)}$. Generally, any vector $\boldsymbol{\omega}\in\mathcal{C}^{(p)}$ can be written as a sum of shifts of the vector $\mathbf{g}$, $\sum_{s=0}^{k_0^{(p)}-1}I_s\cdot\mathbf{g}$; we obtain Eq. (27) by rearranging the summations. Linear independence follows from the symmetry of the vectors $\boldsymbol{\omega}_i^{(p)}\in\mathcal{C}^{(p)}$. □

Note that, in addition to the symmetric vectors, the code $\mathcal{C}_{\mathcal{H}_1}$ may contain vectors with no special symmetry with respect to the discussed block shifts. We will formally assign these to the check polynomial $p(x)=x^c-1$, and define $k_0^{(x^c-1)}\equiv 1$.

For the vectors of the code $\mathcal{C}_{\mathcal{H}_2}$ with the second check matrix in Eq. (21), the condition to be in the symmetry class of $p(x)$ reads $[E_b\otimes p(I_1)]\mathbf{w}=0$ while $[E_b\otimes p'(I_1)]\mathbf{w}\neq 0$ for all $p'(x)\neq p(x)$ that divide $p(x)$. We denote the dimension of the corresponding subcode as $k_2^{(p)}$. The same classification can be done for codes $\mathcal{C}_{\widetilde{\mathcal{H}}_i}$ with the transposed check matrices; the corresponding dimensions are $\widetilde{k}_i^{(p)}$, $i=1,2$.

The introduced symmetry classification is in the heart of the following

Lemma 2. *A vector $\boldsymbol{\upsilon}$ that belongs to both $\mathcal{C}_{E_b\otimes\mathcal{H}_1}$ and $\mathcal{C}_{\mathcal{H}_2\otimes E_a}$ must be in the same symmetry class $p(x)$ with respect to both codes $\mathcal{H}_1$ and $\mathcal{H}_2$, including the no-symmetry case $p(x)=x^c-1$. Any such vector can be generally expanded in terms of*

$$\boldsymbol{\upsilon}_{\alpha,\beta}=\sum_{i,j=0}^{k_0^{(p)}-1}\boldsymbol{\beta}_i\otimes(I_{i+j}\cdot\mathbf{g})\otimes\boldsymbol{\alpha}_j, \tag{28}$$

where $\sum_i\boldsymbol{\beta}_i\otimes(I_i\cdot\mathbf{g})\in\mathcal{C}^{(p)}_{\mathcal{H}_2}$ and $\sum_i(I_i\cdot\mathbf{g})\otimes\boldsymbol{\alpha}_i\in\mathcal{C}^{(p)}_{\mathcal{H}_1}$ and $\mathbf{g}$ corresponds to the polynomial $g(x)\equiv(x^c-1)/p(x)$.

Proof. The parameter χ does not enter this discussion since it corresponds to permutations of rows in matrices $\mathcal{H}_1^0$ and $\mathcal{H}_2^0$. That the symmetry must be the same becomes evident if we write the most general expansion

$$\boldsymbol{\upsilon}=\sum_{ij}\mathbf{e}_i^2\otimes\boldsymbol{\gamma}_{ij}\otimes\mathbf{e}_j^1, \tag{29}$$

where $\boldsymbol{\gamma}_{ij}$ are length-c vectors and $\mathbf{e}_i^{1(2)}$ are distinct weight-1 vectors. Indeed, the condition to be in the symmetry class of $p(x)$ is the same for both codes: $[E_b\otimes p(I_1)\otimes E_a]\boldsymbol{\upsilon}=0$ for $p(x)$ itself but not for any of its factors; thus $\boldsymbol{\gamma}_{ij}$ must be in $\mathcal{C}^{(p)}$. The expansion (28) follows from Lemma 1. □

We can now count linearly-independent rows in the generator matrices:

Lemma 3. *The numbers of linearly independent rows in matrices (19) are*

$$\begin{aligned}\operatorname{rank}G_X &= r_1r_2c-\sum_l\widetilde{k}_1^{(p_l)}\widetilde{k}_2^{(p_l)}/k_0^{(p_l)},\\ \operatorname{rank}G_Z &= n_1n_2c-\sum_l k_1^{(p_l)}k_2^{(p_l)}/k_0^{(p_l)},\end{aligned} \tag{30}$$

where $p_l(x)$ are all binary factors of x^c-1 such that $k_0^{(p_l)}\neq 0$, including x^c-1 itself.

Proof. We first count linearly-dependent rows in G_Z. Notice that the equations $\boldsymbol{\upsilon}^T\cdot(E_b\otimes\widetilde{\mathcal{H}}_1)=0$ and $\boldsymbol{\upsilon}^T\cdot(\widetilde{\mathcal{H}}_2\otimes E_a)=0$ are both satisfied for $\boldsymbol{\upsilon}$ in Eq. (28) [Lemma 2]. Each pair $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generates $k_0^{(p)}$ linearly-independent vectors, same as each of them generates for the corresponding subcodes $\mathcal{C}^{(p)}_{\mathcal{H}_i}$, $i=1,2$, respectively. Thus there are exactly $k_1^{(p)}k_2^{(p)}/k_0^{(p)}$ linearly-independent vectors corresponding to every $p(x)$ with non-empty $\mathcal{C}^{(p)}$. Such vectors have to be complemented with the pairs of vectors of no symmetry (if any) which formally correspond to $p(x)=x^c-1$ and $k_0^{(p)}=1$. According to Lemma

2 these are all possible solutions, which gives $\operatorname{rank} G_Z$ in Eq. (30). We obtain $\operatorname{rank} G_X$ by substituting the parameters of the codes with the parity check matrices $\widetilde{\mathcal{H}}_1$, $\widetilde{\mathcal{H}}_2$. □

We finally obtain

Theorem 3. *A quantum CSS code with generators (19) encodes*

$$k = 2\sum_l k_1^{(p_l)} k_2^{(p_l)}/k_0^{(p_l)} - k_1 s_2 - k_2 s_1 \qquad (31)$$

qubits, where $p_l(x)$ are all binary factors of $x^c - 1$ such that $k_0^{(p_l)} \neq 0$, including $x^c - 1$ itself, and $s_i = n_i - r_i$, $i = 1, 2$.

Proof. The number of encoded qubits k can be deduced from Lemma 3 using the relation

$$k_i^{(p)} - \widetilde{k}_i^{(p)} = s_i k_0^{(p)},\ i = 1, 2. \qquad (32)$$

The latter follows from the fact that the rank of a matrix does not change under transposition (and also under permutations of rows and columns, e.g., as needed to transform $\mathcal{H}_i$ into $\widetilde{\mathcal{H}}_i$). Specifically, restricting the action of matrices $\mathcal{H}_i$ and $\widetilde{\mathcal{H}}_i$ to subspace $\mathcal{C}^{(p)}$, we obtain reduced mutually transposed matrices of dimensions given by $r_i k_0^{(p)} \times n_i k_0^{(p)}$ and $n_i k_0^{(p)} \times r_i k_0^{(p)}$, which immediately gives Eq. (32). □

By construction, any $k_i^{(p)}$ may only be non-zero if the corresponding $k_i > 0$, $i = 1, 2$. Then, Eq. (31) gives

Consequence 4. *A quantum CSS code with generators (19) can only have $k > 0$ if at least one of the binary codes with the parity check matrices (21) is non-empty.*

C. CSS hyperbicycle codes: general distance bounds

Theorem 5. *The minimum distance of the code with generators (19) satisfies the lower bound*

$$d \geq \lfloor d_0/c \rfloor, \quad d_0 \equiv \min(d_1, d_2, \widetilde{d}_1, \widetilde{d}_2). \qquad (33)$$

Proof. Consider a vector $\mathbf{u}$ such that $G_X \cdot \mathbf{u} = 0$. We construct a reduced quantum code in the form (19), with the same c, by keeping only those columns of the matrices a_i, b_i that are involved in the product $G_X \cdot \mathbf{u}$. This way, for every non-zero bit of $\mathbf{u}$, one of the reduced matrices $\mathcal{H}'_1$, $\mathcal{H}'_2$ [see Eq. (21)] may get c columns, so that these matrices have no more than $c\,\mathrm{wgt}(\mathbf{u})$ columns. If we take $\mathrm{wgt}(\mathbf{u}) < \lfloor d_0/c \rfloor$, according to Consequence 4, the reduced code encodes no qubits, thus the corresponding reduced $\mathbf{u}'$, $G'_X \cdot \mathbf{u}' = 0$, has to be a linear combination of the rows of G'_Z. The rows of G'_Z are a subset of those of G_Z, with some all-zero columns removed; thus the full vector $\mathbf{u}$ is also a linear combination of the rows of G_Z. Similarly, a vector $\mathbf{v}$ such that $G_Z \cdot \mathbf{v} = 0$ and $\mathrm{wgt}(\mathbf{v}) < \lfloor d_0/c \rfloor$, is a linear combination of rows of G_X. □

Let us introduce the minimum distances $d_i^{(p)}$ corresponding to the subset of the vectors of the code $\mathcal{C}_{\mathcal{H}_i}$ which *contain* one of the vectors with the exact symmetry of $p(x)$,

$$d_i^{(p)} = \min\{\mathrm{wgt}(\mathbf{a}+\mathbf{b}) | \mathbf{0} \neq \mathbf{a} \in \mathcal{C}^{(p)}_{\mathcal{H}_i},\ \mathbf{b} \in \mathcal{C}_{\mathcal{H}_i} \setminus \mathcal{C}^{(p)}_{\mathcal{H}_i}\}. \qquad (34)$$

Evidently, thus introduced distances satisfy

$$d_i^{(p)} \geq d_i, \quad \min_l d_i^{(p_l)} = d_i,\ i = 1, 2; \qquad (35)$$

the minimum is taken over all $p_l(x)$ as in Theorem 3. We will also introduce the distances $\widetilde{d}_i^{(p)}$ corresponding to the matrices $\widetilde{\mathcal{H}}_i$, $i = 1, 2$.

The upper bound on the distance of the code with generators (19) is formulated in terms of thus introduced subset-distances $d_i^{(p)}$, $\widetilde{d}_i^{(p)}$, $i = 1, 2$:

Theorem 6. *For every $p(x)$, a binary factor of $x^c - 1$ such that $k_1^{(p)} > 0$ and $\widetilde{k}_2^{(p)} > 0$, the minimum distance d of the code with generators (19) satisfies $d \leq \min(d_1^{(p)}, \widetilde{d}_2^{(p)})$. Similarly, when $k_2^{(p)} > 0$ and $\widetilde{k}_1^{(p)} > 0$, we have $d \leq \min(d_2^{(p)}, \widetilde{d}_1^{(p)})$.*

Proof. Given $k_1^{(p)} > 0$, consider vector $\mathbf{u} \equiv (\mathbf{e} \otimes \mathbf{c}, 0)$, where $\mathbf{c} \in \mathcal{C}^{(p)}_{\mathcal{H}_1}$ and $\mathrm{wgt}(\mathbf{e}) = 1$. As long as $\widetilde{k}_2^{(p)} > 0$, we can always select such $\mathbf{e}$ that $\mathbf{u}$ is not a linear combination or rows of G_Z, which would indicate that $d \leq \mathrm{wgt}(\mathbf{c})$.

Indeed, by construction, vector $\mathbf{c}$ can be written in the form (27); let us pick a bit s which is not identically zero in all α_i and construct a vector [cf. Eq. (28)]

$$\mathbf{u}^{(p),s} = (\underbrace{\mathbf{e} \otimes \sum_i \alpha_{is}(I_i \cdot \mathbf{g})}) \otimes \mathbf{e}^1_s, 0). \qquad (36)$$

Taking all r_2 different vectors $\mathbf{e}$ and all $k_0^{(p)}$ linearly-independent translations [Lemma 1], we obtain the vector space [as indicated in Eq. (36) with a brace] isomorphic to that on which the subcode $\mathcal{C}^{(p)}_{\widetilde{\mathcal{H}}_2}$ operates. On the other hand, there are only $r_2 k_0^{(p)} - \widetilde{k}_2^{(p)}$ linearly-independent combinations of rows of the matrix $\widetilde{\mathcal{H}}_2$ restricted to the subspace $\mathcal{C}^{(p)}$. Since $\widetilde{k}_2^{(p)} > 0$, at least one of vectors $\mathbf{u}^{(p),s}$ is linearly independent of the rows of the matrix $\widetilde{\mathcal{H}}_2$ restricted to the subspace $\mathcal{C}^{(p)}$.

Now, we can construct such a vector $\mathbf{u}$ for every $\mathbf{c}$ from the set in Eq. (35), which proves $d \leq d_1^{(p)}$. The other bounds in the Theorem can be obtained from this one by considering isomorphic codes [e.g., interchanging $\widetilde{\mathcal{H}}_2$ and $\mathcal{H}_1$, and also $\mathcal{H}_1$ and $\mathcal{H}_2$]. □

The meaning of the condition on $p(x)$ in Theorem 6 can be elucidated if we rewrite the number of encoded qubits (31) with the help of identity (32),

$$k = \sum_l k_1^{(p_l)} \widetilde{k}_2^{(p_l)}/k_0^{(p_l)} + \sum_l k_2^{(p_l)} \widetilde{k}_1^{(p_l)}/k_0^{(p_l)}. \qquad (37)$$

Obviously, every term in Eq. (37) giving a non-zero contribution to k, also gives an upper bound on the minimum distance of the quantum code.

D. Codes with finite rate and distance scaling as square root of block length

Here we show explicitly that the family of hyperbicycle codes contains $(v, h+v)$-limited LDPC codes with the distance $d \propto \sqrt{n}$ that are distinct from the hypergraph product codes. Let us start with a *random* (h, v)-regular parity check matrix of a classical LDPC code, where $h < v$. By removing linearly dependent rows, we can form full-rank (h, v)-limited parity check matrix a_1 that, along with $b_j = a_1^T$ ($j \neq 1$ and χ are arbitrary; in case when $j = 1$ and $\chi = 1$ we recover the hypergraph-product codes), we use in Eq. (19) in order to construct the hyperbicycle code where only one term in each summation in Eq. (19) is taken. The rate of the classical code defined by the parity check matrix a_1 is bounded from below, i.e. $R_c \equiv k_c/n_c \geq 1 - h/v$. With high probability at large n_c, the classical code will also have the relative distance in excess of some finite number δ_c[38]. If the classical LDPC code defined by a_1 has parameters $[n_1, k_1, d_1]$ then, according to Theorem 3, 6 and 5, the quantum code will have parameters $[[c(n_1 - k_1)^2 + cn_1^2, ck_1^2, \geq d_1/c]]$. It follows that a finite rate (h, v)-limited classical LDPC code (defined by the parity check matrix a_1) with finite relative distance (we expect the subset relative distance in (35) to be finite as well) will correspond to a finite rate $(v, h+v)$-limited quantum LDPC code with the distance $d \propto \sqrt{n}$.

E. Codes with repeated codewords

In some cases, the distance of the hyperbicycle codes is larger than the lower bound in Theorem 5. In this section, we consider the special case of square matrices a_i, b_i ($r_i = n_i$), with the additional restriction that the codes $\mathcal{C}_{\mathcal{H}_i}$, $\mathcal{C}_{\widetilde{\mathcal{H}}_i}$ are non-empty ($k_i = \widetilde{k}_i > 0$) and contain only fully-symmetric vectors in the symmetry class of $p(x) = 1 + x$. The results we proved so far give the parameters of such codes summarized by (see also Theorem 3 in Ref. 34)

Consequence 7. *Suppose a_i and b_i in Eq. (21) are such that $k_i^{(1+x)} = k_i > 0$ and $r_i = n_i$. Then the CSS code with generators (19) has the block length $n = 2cn_1n_2$, encodes $k = 2k_1k_2$ qubits, and has the minimum distance d limited by $\lfloor d_0/c \rfloor \leq d \leq d_0$, $d_0 \equiv \min(d_1, d_2, \widetilde{d}_1, \widetilde{d}_2)$.*

Proof. By assumption, all vectors in the codes $\mathcal{C}_{\mathcal{H}_i}$, $i = 1, 2$, are in the symmetry class of $p(x) = 1 + x$, which corresponds to $k_0^{(p)} = 1$ and block-symmetric vectors in the form

$$\mathbf{w}_1 = \mathbf{g} \otimes \boldsymbol{\alpha}, \quad \mathbf{w}_2 = \boldsymbol{\beta} \otimes \mathbf{g}, \qquad (38)$$

respectively, with $\mathbf{g} = (1, \ldots, 1)$ [see Eq. (27)]. The number of encoded qubits k immediately follows from Theorem 3, the block length n from Eq. (20), and the lower bound on the distance from Theorem 5. Furthermore, with all vectors in the binary codes having the same symmetry, the upper bound in Theorem 6 is just $d \leq d_0$. □

At this point, we notice that the proof of the lower bound $\lfloor d_0/c \rfloor$ on the distance in Theorem 5 implies that there may be uncorrectable errors of the form $\sum_s (\boldsymbol{\beta}_s \otimes \mathbf{g}_s \otimes \boldsymbol{\beta}'_s, \boldsymbol{\alpha}'_s \otimes \mathbf{g}_s \otimes \boldsymbol{\alpha}_s)$, where all $\mathbf{g}_s$ have $\mathrm{wgt}(\mathbf{g}_s) = 1$. On the other hand, if we were to consider only fully-symmetric vectors, with $\mathbf{g}_s = \mathbf{g} = (1, \ldots, 1)$, the factor of $1/c$ would be unnecessary. We formulate this result as

Lemma 4. *A symmetric vector $\mathbf{u} = (\mathbf{w}_1, \mathbf{w}_2)$, $\mathbf{w}_i = \sum_s \boldsymbol{\beta}_s^i \otimes \mathbf{g} \otimes \boldsymbol{\alpha}_s^i$ with $\mathbf{g} = (1, \ldots, 1)$, $i = 1, 2$, that satisfies $G_X \mathbf{u} = 0$ and is linearly independent from the rows of G_Z, has sublattice weights $\mathrm{wgt}(\mathbf{w}_i)$ either zero or $\geq d_0$.*

Let us first consider the case $c = 2$ (then χ must be equal to 1); we previously formulated the sufficient conditions to increased lower distance bound as Theorem 3 in Ref. 34 which was given without a proof.

Theorem 8. *Suppose $c = 2$, a_i and b_i in Eq. (21) are such that $k_i^{(1+x)} = k_i > 0$, $r_i = n_i$ and binary codes with generator matrices $\sum a_i$, $\sum a_i^T$, $\sum b_i$ and $\sum b_i^T$ have distances at least 2. Then the CSS quantum code with generators Eq. (19) has parameters $[[4n_1n_2, 2k_1k_2, d_0]]$, where $d_0 = \min(d_1, d_2, \widetilde{d}_1, \widetilde{d}_2)$.*

Proof. In addition to what is stated in Consequence 7, we only need to prove that d_0 is also the lower bound on the distance. To this end, notice that any vector $\mathbf{u}$ such that $G_X \mathbf{u} = 0$ can be decomposed as the sum of an "actual" solution plus degeneracy, $\mathbf{u}^{(1+x)} + \boldsymbol{\gamma}^T G_Z$, where $\mathbf{u}^{(1+x)} \equiv (\mathbf{w}_1, \mathbf{w}_2)$ is a block-symmetric vector satisfying the conditions of Lemma 4 and linearly-independent from the rows of G_Z. This decomposition can be verified by comparing k with the number of linearly-independent solutions in the form (36), as well as those on the other sublattice. First, let us assume $\mathrm{wgt}(\mathbf{w}_1) > 0$ and therefore $\mathrm{wgt}(\mathbf{w}_1) \geq d_0$. We can rewrite the corresponding decomposition as $\mathbf{w}_1 = \sum_s \boldsymbol{\beta}_s \otimes \mathbf{g} \otimes \mathbf{e}_s^1$, where $\mathbf{g} \equiv (1, 1)$, each $\mathbf{e}_s^1$ has length n_1 and $\mathrm{wgt}(\mathbf{e}_s^1) = 1$, with the non-zero element in the position s; there must be at least $d_0/2$ non-zero vectors $\boldsymbol{\beta}_s$. The full solution including the degeneracy can be formally written as $\sum_s \mathbf{w}'_{1s} \otimes \mathbf{e}_s^1$, where

$$\mathbf{w}'_{1s} \equiv \boldsymbol{\beta}_s \otimes \mathbf{g} + \boldsymbol{\gamma}'_s \otimes (1, 0) + \boldsymbol{\gamma}''_s \otimes (0, 1), \qquad (39)$$

where the sum of the last two vectors is a linear combination of rows of $\widetilde{\mathcal{H}}_2$. The key to the proof is the observation

that $\boldsymbol{\gamma}'_s + \boldsymbol{\gamma}''_s$ is a linear combination of rows of $b_0^T + b_1^T$, and therefore is in the binary code generated by $\sum_s b_s^T$; by condition the corresponding weight is either zero or ≥ 2. Without limiting generality, we can drop the case $\boldsymbol{\gamma}'_s = \boldsymbol{\gamma}''_s \neq \mathbf{0}$ which corresponds to a symmetric vector and can be included as a part of $\mathbf{u}^{(1+x)}$. We are left with the trivial $\boldsymbol{\gamma}'_s = \boldsymbol{\gamma}''_s = 0$, in which case $\mathbf{w}'_{1s} = \boldsymbol{\beta}_s \otimes (1,1)$ remains unchanged; otherwise $\boldsymbol{\gamma}'_s \neq \boldsymbol{\gamma}''_s$, in which case the weight of the modified $\mathbf{w}'_{1s}$ can be lower bounded by that of the sum of the components corresponding to $(1,0)$ and $(0,1)$,

$$\mathrm{wgt}(\mathbf{w}'_{1s}) \geq \mathrm{wgt}(\boldsymbol{\gamma}'_s + \boldsymbol{\gamma}''_s) \geq 2; \tag{40}$$

with at least $d_0/2$ such terms the total weight is d_0 or greater. The same arguments can be repeated in the case $\mathrm{wgt}(\mathbf{w}_2) \neq 0$, as well as for the space orthogonal to G_X. Overall, this proves the lower bound $d \geq d_0$; combined with the upper bound we get $d = d_0$. □

Theorem 9. *Suppose c is even, a_i and b_i in Eq. (21) are such that $k_i^{(1+x)} = k_i$, $r_i = n_i$ and binary codes with generator matrices $\sum a_i$, $\sum a_i^T$, $\sum b_i$ and $\sum b_i^T$ have distance at least 2. Then the quantum code in Eq. (19) has parameters $[[2n_1n_2c, 2k_1k_2, d]]$, where $(2/c)d_0 \leq d \leq d_0$ and $d_0 \equiv \min(d_1, d_2, \widetilde{d}_1, \widetilde{d}_2)$.*

Proof. The proof is similar to the proof of Theorem 8, except that now vectors $\mathbf{w}'_{1s}$ are defined by the analog of Eq. (39) which has $\mathbf{g} = (1, \ldots, 1)$ with c components and more terms with $\gamma_s^{(j)}$ in the r.h.s., $j = 1, \ldots, c$. We need to show that a non-zero $\mathbf{w}'_{1s}$ has $\mathrm{wgt}(\mathbf{w}'_{1s}) \geq 2$, which ensures that the minimum distance of the code is at least $2d_0/c$.

With $c > 2$ and even, after the summation over all possible shifts of the vector $\mathbf{w}'_{1s}$ with respect to the block structure the symmetric term disappears, and we obtain the inequality $c\,\mathrm{wgt}(\mathbf{w}'_{1s}) \geq c\,\mathrm{wgt}(\boldsymbol{\gamma}_s^1 + \boldsymbol{\gamma}_s^2 + \ldots + \boldsymbol{\gamma}_s^c)$. The sum in the r.h.s. is a linear combination of rows of $\sum b_i^T$; by assumption, it's weight is either ≥ 2 or zero. The only non-trivial situation corresponds to the latter case with some $\boldsymbol{\gamma}_s^{\ell_1} \neq 0$. For the sum to be zero, either there is an even number m of identical vectors $\boldsymbol{\gamma}_s^{\ell_1} = \boldsymbol{\gamma}_s^{\ell_2} = \ldots = \boldsymbol{\gamma}_s^{\ell_m}$, with $m < c$ and all indices different [this situation results in $\mathrm{wgt}(\mathbf{w}'_{1s}) \geq (c-m) \geq 2$ since both m and c are even and $\boldsymbol{\beta}_s \neq \mathbf{0}$], or there are at least two pairs of unequal vectors $\boldsymbol{\gamma}_s^{\ell_1} \neq \boldsymbol{\gamma}_s^{\ell_2}$ and $\boldsymbol{\gamma}_s^{\ell_3} \neq \boldsymbol{\gamma}_s^{\ell_4}$, with $\boldsymbol{\gamma}_s^{\ell_2} \neq \boldsymbol{\gamma}_s^{\ell_4}$, which also gives $\mathrm{wgt}(\mathbf{w}'_{1s}) \geq 2$. □

In order to obtain codes with repeated structure (see Fig. 2), one can start with two cyclic LDPC codes with block lengths n_i, $i = 1, 2$, and the check polynomials $h_i(x)$ that divide $x^{n_i} - 1$. The polynomials $h_i(x)$ will also divide $x^{cn_i} - 1$, thus the corresponding circulant parity-check matrix $\mathcal{H}_i$ of dimensions $cn_i \times cn_i$ will lead to a code with repeated structure satisfying Theorem 9 since the corresponding generator polynomial is $g_i(x) = (x^{(c-1)n_i} + x^{(c-2)n_i} + \ldots + 1)\,(x^{n_i} + 1)/h_i(x)$, $i = 1, 2$.

Example 4. *Suppose we use the polynomial $h(x)$ corresponding to the shortened Reed-Muller cyclic code with parameters $[2^m - 1, m + 1, 2^{m-1} - 1]$ in order to construct circulant matrices $\mathcal{H}_1 = \mathcal{H}_2$ of dimensions $2(2^m - 1) \times 2(2^m - 1)$. According to Theorem 9, a code in Eq. (19) with $c = 2$ and $\chi = 1$ will have parameters $[[4(2^m-1)^2, 2(m+1)^2, 2(2^{m-1}-1)]]$. This family leads to weight limited LDPC codes and up to $m = 11$ there is always a choice of polynomial $h(x)$ of weight 4 which leads to quantum LDPC code with stabilizer generators of weight 8.*

Example 5. *Given two "small" cyclic codes $[n_i, k_i, d_i]$ with check polynomials $h_i(x)$, $i = 1, 2$, we can construct a $c = 1$ hypergraph-product quantum code with the parameters $[[2n_1n_2, 2k_1k_2, d_0]]$, $d_0 = \min(d_1, d_2)$, a repeated even-c code with the parameters $[[2cn_1n_2, 2k_1k_2, d]]$, $2d_0 \leq d \leq cd_0$, or a hypergraph-product code $[[2c^2n_1n_2, 2k_1k_2, d_0c]]$ using the "large" cyclic codes with the same check polynomials and the block lengths cn_i.*

Note that in this Example the code rate goes down compared to the hypergraph-product code constructed from the "small" cyclic codes and goes up compared to the hypergraph-product code constructed from the "large" cyclic codes.

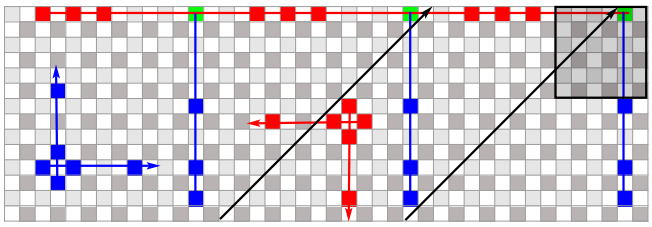

FIG. 2: (Color online) Same as Fig. 1 for the $[[294, 18, 8]]$ code in Eq. (19) formed by circulant matrices $\mathcal{H}_1^0 = \overleftrightarrow{\mathcal{H}}_2^0$ corresponding to coefficients of the polynomial $h(x) = 1 + x + x^3$ with $c = 3$ and $\chi = 1$. Two stabilizer generators are marked by red and blue arrows, respectively, and two anticommuting logical operators are marked by red and blue lines, respectively. All other stabilizer generators are obtained by shifts over the same sublattice with periodicity in the horizontal direction and shifted periodicity (shown by arrows) in the vertical direction. In the shaded region, each gray square uniquely corresponds to a different logical operator, thus 18 encoded logical qubits. One can observe the tripling of the logical operators, thus the overlap (green square) is also repeated three times. Note that according to Consequence 7 the code distance is bounded by $4 \leq d \leq 12$; the actual $d = 8$ was found numerically.

F. Planar qubit layout of hyperbicycle codes and encoding

The stabilizer generators corresponding to Eq. (19) can be graphically represented on two rectangular regions

corresponding to two sublattices. In case, when matrices $\mathcal{H}_1$ and $\mathcal{H}_2$ are square, the rectangular regions of sublattices have the same dimensions and can be drawn together with parameters c and χ corresponding to the number of square blocks and boundary shift, respectively, see, e.g., Fig. 2 and 3. Furthermore, in some cases, we can represent logical operators by line-like operators with a possibility of using this layout for encoding.

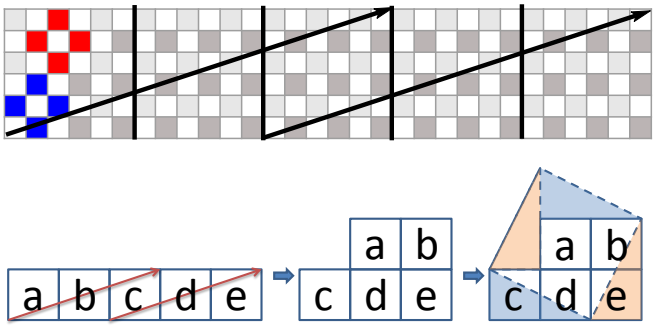

FIG. 3: (Color online) Upper plot: visualization of a $[[90, 2, 9]]$ hyperbicycle code in Eq. (19) formed by 3×3 circulant matrices $\mathcal{H}_1^0 = \overleftrightarrow{\mathcal{H}}_2^0$ corresponding to coefficients of the polynomial $h(x) = 1 + x$, $c = 5$ and $\chi = 3$. The boundaries are periodic if one moves in the horizontal direction and shifted by $\chi = 3$ blocks (as shown by arrows) if one moves in the vertical direction. Lower plot: a general block construction leading to rotated periodic boundaries of hyperbicycle codes for $c = 5$ blocks and for the shift $\chi = 3$. This corresponds to $\alpha = 1$ and $\beta = 2$ case of the infinite series of block constructions with $c = \alpha^2 + \beta^2$, $\chi = \alpha + \beta$ and $\beta = \alpha + 1$. In case of a toric code stabilizer generators, this maps to a rotated toric code from Ref. 34, or to the $t = 1$ case of the infinite series of block constructions with $c = t^2 + (t + 1)^2$ and $\chi = 2t + 1$ in Example 7.

We start by considering the case $c = 1$ and $\chi = 1$ corresponding to the hypergraph-product codes. The stabilizer generators for the quantum code in Eq. (13) can be graphically represented by two (dotted) lines living on different sublattices with the dots (red and blue squares in Fig. 1 marked by arrows) placed in the positions corresponding to 1s in the rows of the binary matrices $\mathcal{H}_1$, $\mathcal{H}_2$, $\widetilde{\mathcal{H}}_1 = \mathcal{H}_1^T$ and $\widetilde{\mathcal{H}}_2 = \mathcal{H}_2^T$. For cyclic codes, e.g., in Fig. 1, the relative position of dots stays the same and we can translate each stabilizer generator over the corresponding sublattice. In general, the form of stabilizer generators is position dependent and the characteristic two-line structure (see Fig. 1) ensures commutativity.

The logical operators $\overline{X}_j$, $\overline{Z}_j$, $j = 1, ..., k$ can be chosen among the rows of the matrices

$$\overline{\mathcal{X}}_1 = (\widetilde{\mathcal{H}}_2^{\perp} \otimes \widetilde{E}_1, 0), \quad \overline{\mathcal{X}}_2 = (0, \widetilde{E}_2 \otimes \widetilde{\mathcal{H}}_1^{\perp}), \tag{41}$$

and

$$\overline{\mathcal{Z}}_1 = (E_2 \otimes \mathcal{H}_1^{\perp}, 0), \quad \overline{\mathcal{Z}}_2 = (0, \mathcal{H}_2^{\perp} \otimes E_1), \tag{42}$$

where the index corresponds to the sublattice number on which the logical operator lives and $\perp$ stands for the orthogonal space mod 2. It is convenient to choose the matrices $\mathcal{H}_1^{\perp}$, $\mathcal{H}_2^{\perp}$, $\mathcal{H}_1^{T\perp}$ and $\mathcal{H}_2^{T\perp}$ in the canonical row echelon form (which may require some row and column permutation of the original matrices $\mathcal{H}_1$ and $\mathcal{H}_2$). In such a case, the logical operators can be represented by vertical and horizontal (dotted) lines that have only one non-zero element in the region of the size $k_1 \times \tilde{k}_2$ for the first sublattice and of the size $\tilde{k}_1 \times k_2$ for the second sublattice (shaded region in Fig. 1) resulting in $k = k_1\tilde{k}_2 + \tilde{k}_1 k_2$ logical qubits. Thus, for such a representation, each physical qubit in the region of size $k_1\tilde{k}_2 + \tilde{k}_1 k_2$ (shaded region in Fig. 1) overlaps with only one logical qubit and can be used for encoding. Note that in general the two sublattices cannot be drawn together as they will have different dimensions for non-square matrices $\mathcal{H}_1$ and $\mathcal{H}_2$. In such a case, the sublattices can be represented by two different rectangular regions and the stabilizer generators have one line per sublattice.

The hyperbicycle construction in Eq. (19) for arbitrary c and χ has a block structure of several rectangular regions stitched together with one of the periodic boundaries being shifted by χ blocks (see Fig. 3, lower plot). The stabilizer generators can be graphically represented by two (dotted) lines with the dots (red and blue squares in Fig. 4) placed in the positions corresponding to 1s in rows of the binary matrices $\mathcal{H}_1$, $\mathcal{H}_2$, $\widetilde{\mathcal{H}}_1$ and $\widetilde{\mathcal{H}}_2$. For cyclic codes, e.g., in Fig. 4, the relative position of dots stays the same and we can translate the stabilizer generator with (shifted) periodic boundaries. Just like for the hypergraph product codes, the form of stabilizer generators is position dependent in case of non-cyclic codes.

Generally, the logical operators of hyperbicycle codes cannot all be chosen to have a simple planar layout (see Example 6 below and Fig. 4, Left). However, the simple structure of the logical operators is preserved in the special case of CSS codes with c odd and $k_i^{(1+x)} = k_i$ (see Theorem 3). Here, similar to the $c = 1$ case, the logical operators $\overline{X}_j$, $\overline{Z}_j$, $j = 1, ..., k$, can be chosen among the rows of the matrices (41) and (42). The only difference is that the logical operators are now repeated c times, which can lead to codes with increased distance (see Fig. 2). Again, one-to-one correspondence between a set of physical qubits (shaded regions in Figs. 1 and 2) and logical qubits can be used for encoding.

Example 6. *A CSS hyperbicycle code in Eq. (19) with parameters* $[[900, 50, 14]]$ *is obtained from circulant matrices* $\mathcal{H}_1^0 = \overleftrightarrow{\mathcal{H}}_2^0$ *corresponding to the polynomial* $h(x) = (1 + x + x^3 + x^5)$, $n_i = 15$, $c = 2$, $\chi = 1$, *and* $b_i = a_i$. *The corresponding layout is shown in Fig. 4, Left.*

G. Codes from two circulant matrices

We note that any circulant matrix has the block form required for the hyperbicycle construction in Eq. (19). Specifically, the matrices $\mathcal{H}_1^0$ and $\overleftrightarrow{\mathcal{H}}_2^0$ in Eqs. (23) and (24)

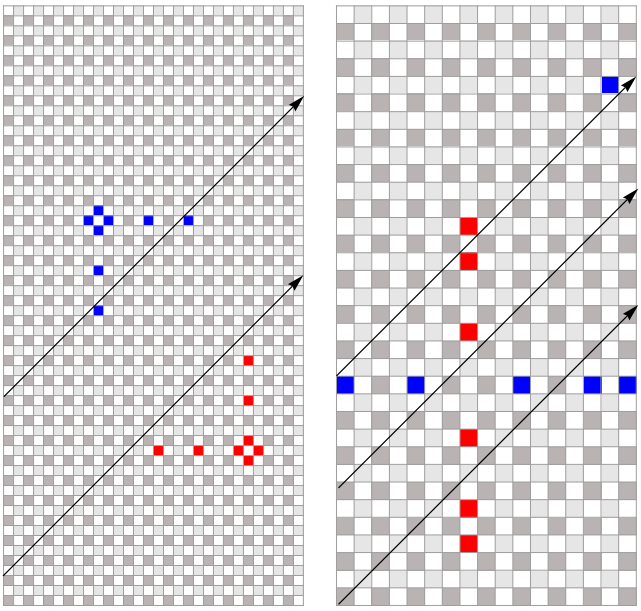

FIG. 4: (Color online) Same as Fig. 1. Left: X and Z stabilizer generators for the CSS hyperbicycle code $[[900, 50, 14]]$ formed by circulant matrices corresponding to coefficients of a polynomial $h(x) = 1 + x + x^3 + x^5$ and $c = 2$, $\chi = 1$. Right: a single stabilizer generator of a $[[289, 81, 5]]$ non-CSS hyperbicycle code in Eq. (16) formed by symmetric circulant matrices corresponding to coefficients of a polynomial $h(x) = 1 + x + x^3 + x^6 + x^8 + x^9$ and $c = 1$. The division into two sublattices is impossible and all other stabilizer generators are obtained by shifts over the light and dark gray qubits with periodicity in the vertical direction and shifted periodicity (shown by arrows) in the horizontal direction.

can correspond to any pair of circulant matrices of appropriate size. Thus, well known families of cyclic binary codes can be employed for this construction. As mentioned in the previous section, this leads to planar qubit layouts where the stabilizer generators are translationally invariant with (shifted) periodic boundary conditions.

The choice of $\chi \neq 1$ can lead to codes with increased distance. This can be best seen on the example with the toric code (Fig. 3) where by rearranging the qubits we can bring the code into a new layout with proper periodic but rotated boundaries[34]. Then, it will be the Manhattan distance (defined on blocks, e.g., of size 3×3 in Fig. 3) between the boundaries that will actually determine the distance of the code.

For a given area, the largest Manhattan distance can be expected for a square. Let us choose a square with the edges defined by the vectors $\mathbf{L}_1 = (\alpha, \beta)$ and $\mathbf{L}_2 = (-\beta, \alpha)$, with mutually prime $\alpha > 0$ and $\beta > 0$, i.e., $\gcd(\alpha, \beta) = 1$. There exists an integer pair of α', β' such that $\alpha\alpha' + \beta\beta' = 1$. An equivalent domain on the plane can be also chosen using the vectors $\mathbf{L}'_1 = (c, 0)$ and $\mathbf{L}'_2 = (\chi, 1)$, where $c = \alpha^2 + \beta^2$ and $\chi = \alpha\beta' - \beta\alpha'$ are mutually prime. These then define a geometric block construction of quantum codes with rotated boundaries (see Fig. 3, lower plot). In addition, this construction corresponds to a hyperbicycle code (19) with c and χ given above. For the rotated toric code we obtain the code parameters: $n = cn_1^2$, $k = 2$, and the distance $d = (\alpha+\beta)n_1$ or in terms of the distance bound in Theorem 5, $d = (\alpha + \beta)d_0/c$.

Note that the described construction requires $|\chi| \geq \alpha + \beta > 1$ [The example in Fig. 3 corresponds to $\alpha = 1$, $\beta = 2$, which gives $c = 5$ and the equality $\chi = \alpha + \beta = 3$.] Thus, for codes equivalent to rotated toric codes this gives a distance improvement compared to the general distance bound in Theorem 5.

Example 7. *If we take $\alpha = t$, $\beta = t+1$, $t = 1, 2, \ldots$, we get $c = t^2 + (t + 1)^2$, $\chi = \alpha + \beta = 2t + 1$. A CSS family of rotated toric codes is obtained when $\mathcal{H}_1^0$ corresponds to the polynomial $h(x) = (1+x)$ (for $\mathcal{H}_2^0$ we use $b_i = a_i$). By construction in Eq. (19) we obtain codes with parameters $[[2n_1^2 c, 2, n_1\chi]]$. Explicitly for $n_1 = 2$ we obtain $[[40, 2, 6]]$, $[[104, 2, 10]]$, ..., and for $n_1 = 3$ $[[90, 2, 9]]$, $[[234, 2, 15]]$, ...*

As the following examples confirm, numerically we see that $\chi > 1$ can also produce codes exceeding the lower distance bound in Theorem 5, and in some cases even saturate the upper distance bound in Theorem 6.

Example 8. *A $[[90, 8, 8]]$ CSS hyperbicycle code is obtained when $\mathcal{H}_1^0$ corresponds to the classical cyclic code $[15, 4, 8]$ with the generator polynomial $g(x) = (1 + x^3 + x^4)$ (for $\mathcal{H}_2^0$ we use $b_i = a_i$), $c = 5$ and $\chi = 3$.*

Example 9. *A $[[90, 10, 7]]$ CSS hyperbicycle code is obtained when $\mathcal{H}_1^0$ corresponds to the classical cyclic code $[15, 5, 7]$ with the check polynomial $h(x) = (1+x+x^3+x^5)$ (for $\mathcal{H}_2^0$ we use $b_i = a_i$), $c = 5$ and $\chi = 3$.*

Example 10. *A $[[126, 8, 10]]$ CSS hyperbicycle code is obtained when $\mathcal{H}_1^0$ corresponds to the classical cyclic code $[21, 5, 10]$ with the check polynomial $h(x) = (1 + x + x^5)$ (for $\mathcal{H}_1^0$ we use $b_i = a_i$), $c = 7$ and $\chi = 3$. Same construction with $\chi = 1$ results in the code $[[126, 14, 6]]$.*

Example 11. *Same construction starting with the classical cyclic code $[30, 8, 8]$ with the check polynomial $h(x) = (1 + x^2 + x^8)$, $c = 10$ and $\chi = 3$ gives a code $[[180, 16, 8]]$, while $\chi = 1$ gives $[[180, 16, 6]]$ with a smaller distance.*

Example 12. *Same construction starting with the classical cyclic code $[[30, 8, 8]]$ corresponding to the check polynomial $h(x) = (1 + x^2 + x^8)$ with $c = 15$ and $\chi = 2$ gives a $[[120, 32, 4]]$ CSS hyperbicycle code; $\chi = 1$ gives a code $[[120, 32, 2]]$.*

Note that in many cases the code rate goes up compared to the hypergraph-product code constructed from the same ("large") cyclic codes, while the construction from the "small" cyclic codes is not possible (cf. Example 5), e.g. this is the case for Examples 7-12.

H. Non-CSS versions of hyperbicycle codes

We observe that when $\mathcal{H}_1 = \widetilde{\mathcal{H}}_1$ and $\mathcal{H}_2 = \widetilde{\mathcal{H}}_2$, the construction in Eqs. (19) can be mapped to non-CSS codes in Eq. (16) that in many cases have the same distance but half the number of encoded and physical qubits. In particular, this happens when $\chi = 1$ and matrices $\mathcal{H}_1$ and $\mathcal{H}_2$ are symmetric. By non-CSS hyperbicycle codes we then mean a result of the mapping in Theorem 1 of the code in Eq. (19). The dimensions of such codes can be readily found by applying Theorem 3 where $s_1 = s_2 = 0$.

Theorem 10. *A quantum non-CSS code constructed from matrices (25) such that $\mathcal{H}_1 = \widetilde{\mathcal{H}}_1$ and $\mathcal{H}_2 = \widetilde{\mathcal{H}}_2$ and the stabilizer generator matrix*

$$G = (E_b \otimes \mathcal{H}_1 | \mathcal{H}_2 \otimes E_a), \tag{43}$$

encodes $k = \sum_l k_1^{(p_l)} k_2^{(p_l)} / k_0^{(p_l)}$ logical qubits into $n = cn_1n_2$ physical qubits, where $p_l(x)$ are all binary factors of $x^c - 1$ such that $k_0^{(p_l)} \neq 0$, including $x^c - 1$ itself. The distance of such a code is bounded by $d \geq \lfloor d_0/c \rfloor$, $d_0 \equiv \min(d_1, d_2)$ (same notations as in Theorem 5). In addition, for every $p_l(x)$, such that $k_1^{(p_l)} > 0$ and $k_2^{(p_l)} > 0$, the minimum distance d of the code satisfies $d \leq \min(d_1^{(p_l)}, d_2^{(p_l)})$ (same notations as in Theorem 6).

Proof. The lower distance bound follows from the proof of Theorem 5 given the fact that any code word of the original quantum code has to have support on at least one of the sublattices with weight exceeding $\lfloor d_0/c \rfloor$. The upper distance bound in Theorem 6 also applies to non-CSS hyperbicycle codes since by construction this bound involves only one sublattice. □

Theorem 11. *Suppose c is even, a_i and b_i in Eq. (21) are such that $k_i^{(1+x)} = k_i$, $r_i = n_i$ and binary codes with generator matrices $\sum a_i$ and $\sum b_i$ have distances at least 2. Then quantum non-CSS code with generators in Eq. (19) that have been reduced by construction in Eq. (16) has parameters $[[n_1n_2c, k_1k_2, d]]$ where $(2/c)d_0 \leq d \leq d_0$ and $d_0 \equiv \min(d_1, d_2)$.*

Proof. The improved lower distance bound follows from the proof of Theorem 8 given the fact that any code word of the original quantum code has to have support on at least one of the sublattices with weight exceeding $(2/c)d_0$. □

For $\chi = 1$ we can use *palindromic* check polynomials $h(x)$, i.e. $h^{\rm rev}(x) = h(x)$, such that $cn - \deg h(x)$ is even, in order to construct symmetric circulant matrices $\mathcal{H}_i$ from the polynomial $x^{[cn - \deg h(x)]/2} h(x)$.

Example 13. *A $[[289, 81, 5]]$ non-CSS hyperbicycle code (see Fig. 4) is obtained from Eqs. (16), (19) and (25) using symmetric circulant matrices $\mathcal{H}_1 = \mathcal{H}_2$ corresponding to coefficients of the palindromic polynomial $h(x) = 1 + x + x^3 + x^6 + x^8 + x^9$ where $c = 1$ and $\chi = 1$.*

V. CONCLUSIONS

We introduced and started to explore a general bipartite ansatz for quantum CSS codes. Among the better-studied families of quantum CSS codes, this ansatz can be used to describe the bicycle codes[19], hypergraph-product codes[27], Haah's codes[37], the CSS codes constructed over higher alphabets[22, 39], and it also can be used to construct a double-size CSS code from an arbitrary non-CSS stabilizer code.

Within this framework, we introduced a large family of hyperbicycle codes that includes as subclasses the best of the known LDPC code families. The construction allows for explicit upper and lower bounds on the code distance. We also described a number of new LDPC code families with finite rates and distances scaling as a square root of block length. Our discussion is accompanied with geometrical interpretations of the hyperbicycle codes which can facilitate design and applications of such codes. The construction is particularly useful for designing LDPC codes with relatively small block lengths which is important since the original hypergraph product codes have relatively poor parameters at small block lengths. Furthermore, hyberbicycle codes allow for code constructions with a wide range of parameters which might be useful for designing fault-tolerant gates (e.g., gates performed by code deformations).

Another advantage of hyperbicycle construction is that it can be based on a pair of very well studied classical cyclic codes. This leads to codes with good parameters up to limited but relatively large block lengths (in general, cyclic codes with asymptotic rates below one have poor asymptotic parameters). The planar layout of thus constructed quantum codes possess translational invariance of stabilizer generators which may simplify the implementation (see, e.g., Ref. 40).

The quantum LDPC codes discussed in this work have been shown to possess a finite noise threshold [28] since the lower bound on the distance scales as a square root of the block length. This threshold, however, corresponds to the maximum-likelihood (ML) decoding. While an efficient general-purpose decoder comparable with belief-propagation remains unknown for quantum codes[20], at smaller error rates efficient decoding is possible by employing the ideas expressed in Ref. 28.

Even though the lower distance bounds presented in this paper are in some cases inferior compared to the hypergraph-product codes, we do not expect that this will have a significant effect on the value of the noise threshold as the distance still scales as a square root of the block length while the LDPC structure of the stabilizer generators is preserved [28]. Given that, we expect that one can achieve better encoding rates with hyperbicycle codes compared to hypergraph product codes without affecting the threshold.

Our results notwithstanding, there are several open questions in regard to the hyperbicycle codes. In particular, it would be interesting to establish conditions

under which the hyperbicycle codes reach the upper distance bound. Furthermore, the case when the block shift χ and the number of blocks c are commensurate has not been analyzed. It would also be interesting to explore the exact relation between the hyperbicycle codes and the CSS codes constructed over higher alphabets[22, 39].

Acknowledgments

We are grateful to I. Dumer and M. Grassl for multiple helpful discussions. This work was supported in part by the U.S. Army Research Office under Grant No. W911NF-11-1-0027, and by the NSF under Grant No. 1018935.

[1] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, Phys. Rev. Lett. **85**, 5452 (2000), URL http://link.aps.org/abstract/PRL/v85/p5452. I

[2] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature **414**, 883 (2001), URL http://dx.doi.org/10.1038/414883a.

[3] J. Chiaverini, D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, et al., Nature **432**, 602 (2004), URL http://dx.doi.org/10.1038/nature03074.

[4] J. M. Martinis, Quantum Information Processing **8**, 81 (2009), URL http://dx.doi.org/10.1007/s11128-009-0105-1. I

[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995), URL http://link.aps.org/abstract/PRA/v52/pR2493. I

[6] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997), URL http://dx.doi.org/10.1103/PhysRevA.55.900.

[7] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996), URL http://dx.doi.org/10.1103/PhysRevA.54.3824. I

[8] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998), URL http://www.sciencemag.org/cgi/content/abstract/279/5349/342. I

[9] B. Rahn, A. C. Doherty, and H. Mabuchi, Phys. Rev. A **66**, 032304 (2002), URL http://dx.doi.org/10.1103/PhysRevA.66.032304.

[10] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002), URL http://dx.doi.org/10.1063/1.1499754. I

[11] A. M. Steane, Phys. Rev. A **68**, 042322 (2003), URL http://dx.doi.org/10.1103/PhysRevA.68.042322.

[12] A. G. Fowler, C. D. Hill, and L. C. L. Hollenberg, Phys. Rev. A **69**, 042314 (2004), URL http://link.aps.org/abstract/PRA/v69/e042314.

[13] A. G. Fowler, S. J. Devitt, and L. C. L. Hollenberg, Quant. Info. Comput. **4**, 237 (2004), quant-ph/0402196, URL http://arxiv.org/abs/quant-ph/0402196.

[14] A. G. Fowler (2005), arXiv:quant-ph/0506126, URL http://arxiv.org/abs/quant-ph/0506126.

[15] E. Knill, Nature **434**, 39 (2005), URL http://dx.doi.org/10.1038/nature03350.

[16] E. Knill, Phys. Rev. A **71**, 042322 (2005), URL http://dx.doi.org/10.1103/PhysRevA.71.042322.

[17] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007), URL http://link.aps.org/abstract/PRL/v98/e190504. I

[18] M. S. Postol (2001), unpublished, arXiv:quant-ph/0108131v1, URL http://arxiv.org/abs/quant-ph/0108131. I

[19] D. MacKay, G. Mitchison, and P. McFadden, Information Theory, IEEE Transactions on **50**, 2315 (2004). I, II C, II C, III B, V

[20] D. Poulin and Y. Chung, Quant. Info. and Comp. **8**, 987 (2008). II C, V

[21] A. Couvreur, N. Delfosse, and G. Zémor (2012), cs/arXiv:1206.2656. I

[22] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, Information Theory, IEEE Transactions on **58**, 1223 (2012). V

[23] A. Hutter, J. R. Wootton, and D. Loss, arXiv1302.2669 (unpublished). I

[24] A. Y. Kitaev, Ann. Phys. **303**, 2 (2003), URL http://arxiv.org/abs/quant-ph/9707021. I

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

[26] M. Freedman, D. Meyer, and F. Luo, in *Computational Mathematics* (Chapman and Hall/CRC, 2002), URL http://dx.doi.org/10.1201/9781420035377.ch12. I

[27] J.-P. Tillich and G. Zemor, in *IEEE Int. Symp. on Inf. Th., 2009. ISIT 2009.* (2009), pp. 799–803. I, II D, II D, II D, II D, II D, II D, V

[28] A. A. Kovalev and L. P. Pryadko, Phys. Rev. A **87**, 020304(R) (2013), arXiv:1208.2317, URL http://link.aps.org/doi/10.1103/PhysRevA.87.020304. I, V

[29] S. Aly, in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (2008), pp. 1 –5. I

[30] J. Farinholt (2012), quant-ph/arXiv:1207.0732. I

[31] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Th. **44**, 1369 (1998), URL http://dx.doi.org/10.1109/18.681315. II B, II B, III B, III B, 1

[32] D. Gottesman, Ph.D. thesis, Caltech (1997), URL http://arxiv.org/abs/quant-ph/9705052. II B

[33] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996). II B, III A

[34] A. A. Kovalev and L. P. Pryadko, in *Proc. 2012 IEEE Int. Symp. Inf. Th. (ISIT)* (2012), pp. 348–352, ISSN 2157-8095, arXiv:1202.0928. II D, 2, III B, IV A, IV E, IV E, 3, IV G

[35] K. Feng and Z. Ma, Information Theory, IEEE Transactions on **50**, 3323 (2004). III A

[36] A. A. Kovalev, I. Dumer, and L. P. Pryadko, Phys. Rev. A **84**, 062319 (2011). III B, III B, 3

[37] J. Haah, Phys. Rev. A **83**, 042330 (2011), URL `http://link.aps.org/doi/10.1103/PhysRevA.83.042330`. III C, III C, V

[38] S. Litsyn and V. Shevelev, Information Theory, IEEE Transactions on **48**, 887 (2002). IV D

[39] I. Andriyanova, D. Maurice, and J. Tillich, in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on* (2012), pp. 343 –347. V

[40] A. De and L. P. Pryadko, Phys. Rev. Lett. **110**, 070503 (2013), URL `http://link.aps.org/doi/10.1103/PhysRevLett.110.070503`. V