Subsystem codes with spatially local generators

Sergey Bravyi
IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA
(Dated: August 6, 2010)

We study subsystem codes whose gauge group has local generators in the 2D geometry. It is shown that there exists a family of such codes defined on lattices of size $L \times L$ with the number of logical qubits k and the minimum distance d both proportional to L. The gauge group of these codes involves only two-qubit generators of type XX and ZZ coupling nearest neighbor qubits (and some auxiliary one-qubit generators). Our proof is not constructive as it relies on a certain version of the Gilbert-Varshamov bound for classical codes. Along the way we introduce and study properties of generalized Bacon-Shor codes which might be of independent interest. Secondly, we prove that any 2D subsystem $[n, k, d]$ code with spatially local generators obeys upper bounds $kd = O(n)$ and $d^2 = O(n)$. The analogous upper bound proved recently for 2D stabilizer codes is $kd^2 = O(n)$. Our results thus demonstrate that subsystem codes can be more powerful than stabilizer codes under the spatial locality constraint.

I. INTRODUCTION

Fault-tolerant quantum information processing based on 2D topological quantum codes has received a considerable attention lately since it can be implemented on quantum machines with a geometrically local architecture. The potential of topological codes as a viable alternative to concatenated quantum codes was first realized by Dennis et al [1]. It was shown in [1] that an active error correction in the 2D toric code permits reliable storage of a logical qubit if the error rate in the quantum hardware is below the threshold value about 1%. The threshold for storage of a qubit has been recently improved by Andrist et al [2] by using topological color codes [3, 4] instead of the toric code. The success of topological codes was extended from a storage of a qubit to the universal quantum computation by making use of the powerful technique known as code deformations [5–8]. These recent developments demonstrate that topological codes provide an attractive framework for design of new fault-tolerant protocols.

In order to better understand the potential of topological codes for storing and manipulating quantum information, it is desirable to derive fundamental bounds on the parameters of quantum codes that stem from the spatial locality constraint and find families of codes that achieve these bounds. A progress in this direction has been recently made for 2D stabilizer codes [9–12]. Such codes can be defined in a system of n physical qubits occupying sites of a regular square lattice of size $\sqrt{n} \times \sqrt{n}$. Quantum information is encoded into a codespace $\mathcal{L}$ spanned by common eigenvectors of pairwise commuting n-qubit Pauli operators $S_1, \ldots, S_m$ known as *stabilizers*, that is,

$$\mathcal{L} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, S_a |\psi\rangle = |\psi\rangle \quad \text{for all } a\}.$$

The locality condition is imposed by demanding that each stabilizer S_a acts non-trivially only on a constant number of qubits located within constant distance from each other. A code has k logical qubits if $\dim \mathcal{L} = 2^k$. It was shown in [11] that any 2D stabilizer code obeys a bound

$$kd^2 = O(n), \tag{1}$$

where d is the minimum distance of a code, i.e., the minimum weight of a Pauli operator commuting with all stabilizers and implementing a non-trivial transformation on $\mathcal{L}$. The bound Eq. (1) is tight in the sense that for any given k and d one can construct a 2D stabilizer $[n, k, d]$ code with $n = O(kd^2)$, see [11] for details.

The main conclusion of the present paper is that the bound Eq. (1) can be violated in a dramatic way for 2D *subsystem* codes. Recall that a subsystem code [13, 14] can be regarded as an ordinary stabilizer code in which only part of the logical qubits is used to store information. Accordingly, the codespace of subsystem codes can be decomposed as

$$\mathcal{L} = \mathcal{L}_{\rm logical} \otimes \mathcal{L}_{\rm gauge}, \quad \dim \mathcal{L}_{\rm logical} = 2^k,$$

where $\mathcal{L}_{\rm logical}$ is the logical subsystem used to store quantum information, while $\mathcal{L}_{\rm gauge}$ represents the unused logical qubits usually called gauge qubits. The distance d of a subsystem code is the minimum weight of a Pauli operator commuting with all stabilizers and acting non-trivially on the logical subsystem $\mathcal{L}_{\rm logical}$. The presence of the unused gauge qubits provides much more flexibility in the design of fault-tolerant gates and the error correction for subsystem codes since one does not need to worry how a particular computational operation or an error affects the gauge qubits, see for instance [15, 16]. By the same token, one should expect that spatial locality constraints lead to less severe restrictions on the parameters of subsystem codes.

One can characterize a subsystem code by its *gauge group* $\mathcal{G}$ that includes all stabilizers and all logical operators on the unused logical qubits, see Section II for more details. We shall study 2D subsystem codes for which the gauge group has spatially local generators, that is, $\mathcal{G} = \langle G_1, \ldots, G_m \rangle$ where each generator G_a acts non-trivially only on a constant number of qubits located within constant distance from each other (as for stabilizers S_a, they may or may not be spatially local). For

such codes the tradeoff between n and d was characterized in [9] by showing that

$$d = O(\sqrt{n}). \tag{2}$$

This bound is tight since the 2D Bacon-Shor code [13] has parameters $d = \sqrt{n}$ and $k = 1$. The question that remained open is whether 2D subsystem codes may have a better scaling of k compared with 2D stabilizer codes.

In the present paper we answer this question in positive by proving that there exist a family of 2D subsystem $[n, k, d]$ codes with both k and d proportional to $\sqrt{n}$. More precisely, we prove the following.

Theorem 1. *Let $\alpha > 0$ and $0 < \beta < 1/2$ be any constants such that $\alpha + H_2(\beta) < 1$, where $H_2(\beta)$ is the binary entropy. Then for all sufficiently large integers m and for all $k \leq \alpha m$ there exists a 2D subsystem $[2m^2, k, d]$ code for some $d \geq \beta m$. The gauge group of this code has two-qubit generators of type XX and ZZ coupling nearest-neighbor qubits and some one-qubit generators.*

In contrast, all previously known 2D subsystem codes with the distance proportional to $\sqrt{n}$, such as the 2D Bacon-Shor code [13] or the topological subsystem codes [17] encode only $k = O(1)$ qubits.

The proof of Theorem 1 relies on generalized Bacon-Shor codes that we introduce in Section III. One can define a generalized Bacon-Shor code for any binary matrix A by placing physical qubits at the cells of A for which $A_{i,j} = 1$ and leaving the remaining cells empty. The gauge group $\mathcal{G}$ has generators of two types: each pair of qubits c, c' located in the same row of A contributes a generator $X_c X_{c'}$ and each pair of qubits c, c' located in the same column of A contributes a generator $Z_c Z_{c'}$. We show that the code $\mathcal{G}$ has parameters $[n, k, d]$, where n is the number of non-zero matrix elements in A, k is the binary rank of A, while d is determined by the minimum distance of the classical codes spanned by columns and rows of A, see Theorem 2 in Section III. Then we employ the Gilbert-Varshamov bound to prove existence of binary matrices with the desired properties, see Theorem 3 in Section IV. Finally, we show how to transform any generalized Bacon-Shor code into the spatially local form by introducing ancillary qubits and simulating each long-range generator by a chain of nearest-neighbor couplings, see Section V.

Our second result is a new upper bound on the parameters of 2D subsystem codes whose gauge group has spatially local generators, namely,

$$kd = O(n). \tag{3}$$

It can be regarded as a generalization of Eq. (1) to subsystem codes. This bound is tight up to a constant factor since one can achieve a scaling $k \sim d \sim \sqrt{n}$, see Theorem 1. We also prove that the original bound Eq. (1) holds for any 2D subsystem code in which both stabilizer group and the gauge group have spatially local generators. The topological subsystem codes of [17, 18] provide an example of such codes.

The proof of the bound Eq. (3) presented in Sections VI,VII,VIII requires some heavy machinery that builds upon techniques developed in [9, 11, 12]. Our first tool is the identity relating the number of logical operators supported in two complementary regions of a lattice, see Lemma 2 in Section VI. It was originally proved by Yoshida and Chuang [12] for stabilizer codes. In the present paper we generalize this identity to subsystem codes using techniques of [9]. Our second tool is what we call a holographic principle for error correction, see Section VII. It asserts that a non-trivial logical operator cannot be supported in a region whose *perimeter* is smaller than the distance of the code. The analogous result was proved in [11] for 2D stabilizer codes although the proof given in [11] cannot be generalized to subsystem codes. In Section VIII we combine these technical tools to prove the upper bound Eq. (3).

In Section IX we summarize our results and discuss some open problems such as possible extensions of our constructions to 3D subsystem codes.

II. STABILIZER AND SUBSYSTEM CODES

The purpose of this section is to summarize the necessary facts pertaining to stabilizer and subsystem codes. The main idea of stabilizer codes is to encode k logical qubits into n physical qubits using a codespace $\mathcal{L} \subseteq (\mathbb{C}^2)^{\otimes n}$ spanned by states $|\psi\rangle$ that are invariant under the action of a *stabilizer group* $\mathcal{S}$,

$$\mathcal{L} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, P\,|\psi\rangle = |\psi\rangle \quad \forall P \in \mathcal{S}\}.$$

All stabilizers $P \in \mathcal{S}$ must be Pauli operators, that is, n-fold tensor products of the single-qubit Pauli operators

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

and the identity operators I. Such tensor products generate the Pauli group on n qubits,

$$\mathcal{P} = \{\gamma\, P_1 \otimes P_2 \otimes \cdots \otimes P_n\},$$

where $P_a \in \{I, X, Y, Z\}$ and $\gamma \in \{1, -1, i, -i\}$ is an overall phase factor that we shall often ignore. Non-trivial stabilizer codes correspond to Abelian stabilizer groups $\mathcal{S} \subset \mathcal{P}$ such that $-I \notin \mathcal{S}$.

Logical operators of a stabilizer code $\mathcal{S}$ are Pauli operators preserving the codespace $\mathcal{L}$. Equivalently, logical operators are Pauli operators commuting with every element of $\mathcal{S}$. Such operators generate the centralizer of $\mathcal{S}$ in the Pauli group,

$$\mathcal{C}(\mathcal{S}) = \{P \in \mathcal{P} \,:\, PQ = QP \quad \forall\, Q \in \mathcal{S}\}.$$

One can always decompose the centralizer as

$$\mathcal{C}(\mathcal{S}) = \langle \mathcal{S}, \overline{X}_1, \overline{Z}_1, \ldots, \overline{X}_k, \overline{Z}_k \rangle,$$

where $\overline{X}_i, \overline{Z}_i$ are the logical Pauli operators, while elements of $\mathcal{S}$ correspond to the logical identity operator. Here and below we use the notation $\langle \ldots \rangle$ for a subgroup generated by a family of operators.

For any Pauli operator $P \in \mathcal{P}$ let $\mathrm{Supp}(P) \subseteq \Lambda$ be the *support* of P, that is, the subset of qubits on which P acts non-trivially (by X, Y, or Z). We shall use the notation $|P| = |\mathrm{Supp}(P)|$ for the weight of P, that is, the number of qubits in its support.

The minimum distance d of a stabilizer code $\mathcal{S}$ is defined as the minimum weight of a non-trivial logical operator, that is,

$$d = \min_{P \in \mathcal{C}(\mathcal{S}) \setminus \mathcal{S}} |P|.$$

We shall use a notation $[n, k, d]$ for a stabilizer code encoding k logical qubits into n physical qubits with the distance d.

To define a subsystem $[n, k, d]$ code it is convenient to start from a stabilizer code $\mathcal{S}$ with $k + g$ logical qubits for some $g > 0$. Let $\overline{X}_i, \overline{Z}_i$, $i = 1, \ldots, k$ be the logical Pauli operators on the first k logical qubits that will be used to encode information. The remaining unused logical operators $\overline{X}_i, \overline{Z}_i$, $i = k+1, \ldots, k+g$, together with stabilizers $\mathcal{S}$ generate the *gauge group* [14]

$$\mathcal{G} = \langle \mathcal{S}, \overline{X}_{k+1}, \overline{Z}_{k+1}, \ldots, \overline{X}_{k+g}, \overline{Z}_{k+g} \rangle.$$

We will assume that the n physical qubits live at vertices of a regular 2D lattice Λ of size $\sqrt{n} \times \sqrt{n}$ with open or periodic boundary conditions. Given this 2D geometry we demand that the gauge group $\mathcal{G}$ must have spatially local generators, that is, $\mathcal{G} = \langle G_1, \ldots, G_m \rangle$, where the support of any generator G_m can be bounded by a square box of size $r \times r$ for some constant interaction range r. Given the gauge group $\mathcal{G}$, one can compute the stabilizer group $\mathcal{S}$ using the identity

$$\mathcal{S} = \mathcal{G} \cap \mathcal{C}(\mathcal{G}),$$

where $\mathcal{C}(\mathcal{G})$ is the centralizer of $\mathcal{G}$ in the Pauli group. Note that $\mathcal{S}$ may or may not have spatially local generators. For example, any stabilizer of the 2D Bacon-Shor code [13] has weight at least $\sqrt{n}$. On the other hand, for the topological subsystem codes [17] generators of $\mathcal{S}$ have geometry of closed loops of constant size. In general, one can think of generators of $\mathcal{G}$ as stabilizers broken into "local chunks" such that an eigenvalue of any stabilizer can be inferred by measuring eigenvalue of sufficiently many generators of $\mathcal{G}$. Subsystem codes with an Abelian gauge group are equivalent to ordinary stabilizer codes (such codes have no gauge qubits and thus $\mathcal{G} = \mathcal{S}$).

Logical operators of a subsystem codes are Pauli operators preserving the codespace $\mathcal{L}$. Equivalently, logical operators are elements of the centralizer

$$\mathcal{C}(\mathcal{S}) = \langle \mathcal{G}, \overline{X}_1, \overline{Z}_1, \ldots, \overline{X}_k, \overline{Z}_k \rangle.$$

Since the encoding is defined only modulo gauge operators, non-trivial logical operators are elements of $\mathcal{C}(\mathcal{S})$ that are not in $\mathcal{G}$. In the case of subsystem codes we shall often use the term *bare logical operators* which refers to elements of $\mathcal{C}(\mathcal{G}) \setminus \mathcal{G}$. Bare logical operators preserve the codespace $\mathcal{L}$ and act trivially on the gauge qubits. They should not be confused with *dressed logical operators* which are elements of $\mathcal{C}(\mathcal{S}) \setminus \mathcal{G}$. The identity

$$\mathcal{C}(\mathcal{S}) = \mathcal{C}(\mathcal{G}) \cdot \mathcal{G}$$

implies that any dressed logical operator can be represented as a product of a bare logical operator and a gauge operator. The minimum distance of a subsystem code is defined as the minimum weight of a non-trivial dressed logical operator,

$$d = \min_{P \in \mathcal{C}(\mathcal{S}) \setminus \mathcal{G}} |P| = \min_{P \in \mathcal{C}(\mathcal{G}) \setminus \mathcal{G}} \min_{G \in \mathcal{G}} |PG|.$$

III. GENERALIZED BACON-SHOR CODES

In this section we introduce a generalization of the 2D Bacon-Shor code [13] and describe its main properties. For the sake of clarity we shall ignore the issue of spatial locality until Section V.

Let A be an arbitrary matrix of size $m \times m$ with entries 0 and 1. We shall label cells of A by pairs of indices $c = (i, j)$. Let $n = |A|$ be the Hamming weight of A, i.e., the total number of non-zero matrix elements. To define a subsystem code associated with A let us place a physical qubit at each cell $c = (i, j)$ with $A_{i,j} = 1$. Hence there are totally n physical qubits. The remaining cells for which $A_{i,j} = 0$ are kept solely for illustrative purposes since there are no qubits located at these cells. A subsystem code associated with A has a gauge group $\mathcal{G}$ generated according to the following rules:

- Every pair of qubits c, c' located in the same row of A contributes a generator $X_c X_{c'}$
- Every pair of qubits c, c' located in the same column of A contributes a generator $Z_c Z_{c'}$

In the special case when $A_{i,j} = 1$ for all (i, j) the code $\mathcal{G}$ coincides with the standard 2D Bacon-Shor code [13]. Consider as an example a binary matrix

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

The corresponding subsystem code has $n = 6$ physical qubits. The corresponding gauge group $\mathcal{G}$ has generators

$$\mathcal{G} = \langle X_{1,1}X_{1,2},\ X_{2,2}X_{2,3},\ X_{3,1}X_{3,3},\ Z_{1,1}Z_{3,1},\ Z_{1,2}Z_{2,2},\ Z_{2,3}Z_{3,3} \rangle.$$

Let us explain how to relate the parameters of the code $\mathcal{G}$ to certain algebraic properties of the matrix A. It will be convenient to introduce a linear subspace $C_{\mathrm{col}} \subseteq \{0, 1\}^m$ spanned by the columns of A and a linear subspace

$C_{\rm row} \subseteq \{0,1\}^m$ spanned by the rows of A (throughout this section all linear subspaces are defined over the binary field $\mathbb{F}_2$). One can regard $C_{\rm col}$ and $C_{\rm row}$ as classical codes encoding $k = {\rm rank}\,(A)$ bits into m bits. Here ${\rm rank}\,(A)$ is the rank of A over the binary field $\mathbb{F}_2$. In the example of the 2D Bacon-Shor code the matrix A has rank 1 and $C_{\rm col}$, $C_{\rm row}$ are one-dimensional subspaces that include only the all-zeros and the all-ones vectors. Let $d_{\rm col}$ and $d_{\rm row}$ be the minimum Hamming weight of non-zero vectors in $C_{\rm col}$ and $C_{\rm row}$ respectively. In other words, $d_{\rm col}$ and $d_{\rm row}$ is the minimum distance of the classical code $C_{\rm col}$ and $C_{\rm row}$ respectively.

Theorem 2. *Let A be an arbitrary binary matrix and $\mathcal{G}$ be the subsystem code associated with A as described above. Then $\mathcal{G}$ encodes $k = {\rm rank}\,(A)$ qubits into $n = |A|$ qubits with the minimum distance $d = \min(d_{\rm row}, d_{\rm col})$.*

Before we proceed with the proof of the theorem let us make several remarks concerning the definition of $\mathcal{G}$. Firstly, the set of generators of $\mathcal{G}$ introduced above might be overcomplete. For example, suppose c, c', c'' is a triple of consecutive qubits that belong to the same row of A. Then clearly $X_c X_{c''} = (X_c X_{c'})(X_{c'} X_{c''})$, that is, it suffices to retain only the generators $X_c X_{c'}$ and $X_{c'} X_{c''}$. In general, it suffices to retain generators $X_c X_{c'}$ and $Z_c Z_{c'}$ for consecutive pairs of qubits c, c' that belong to the same row and the same column of A respectively. Secondly, the generators of $\mathcal{G}$ are not necessarily spatially local. For example, if some row of A contains an isolated '1' separated by a long string of zeros on the left and on the right, there is no choice of spatially local generators for $\mathcal{G}$. We shall explain how to circumvent with difficulty in Section V by placing two ancillary qubits into each cell of A with $A_{i,j} = 0$ and splitting each long-range generator into a chain of short-range generators. Finally, let us point out that a similar but technically different construction of subsystem codes was described by Bacon and Casaccino in [19]. The construction of [19] starts from a pair of classical linear codes $C_1 = [n_1, k_1, d_1]$ and $C_2 = [n_2, k_2, d_2]$. A quantum subsystem code is then defined by placing a physical qubit at *every* cell of a matrix A of size $n_1 \times n_2$. The X-part of the gauge group is defined by replicating the parity checks of C_1 in every column of A (in the X-basis). Similarly, the Z-part of the gauge group is defined by replicating the parity checks of C_2 in every row of A (in the Z-basis). The resulting subsystem code has parameters $[n_1 n_2, k_1 k_2, \min(d_1, d_2)]$. The main difference between our construction and the one of [19] is that we allow to use different classical codes in different rows and columns of A (although each of these codes is simply the repetition code on some subset of qubits). Also, as one can see from Theorem 2, the two constructions result in quantum codes with different parameters.

Using Theorem 2 one can easily get upper bounds on the number of logical qubits k and the distance d of generalized Bacon-Shor codes. Firstly, we claim that for any binary matrix A one has $d_{\rm row} d_{\rm col} \le n$. Indeed, since any column of A has weight at least $d_{\rm col}$, the matrix A must contain at least $d_{\rm col}$ non-zero rows. Each of these rows must have weight at least $d_{\rm row}$. Hence the number of non-zero matrix elements in A is at least $d_{\rm row} d_{\rm col}$. Applying Theorem 2 one arrives at

$$d^2 \le d_{\rm row} d_{\rm col} \le n. \tag{4}$$

Although it is not necessary, let us point out that the bound Eq. (4) is not as good as it could be. In Appendix A we shall prove a slightly stronger bound

$$2 d_{\rm row} d_{\rm col} (1 - 2^{-k}) \le n \tag{5}$$

and construct a family of binary matrices that achieves this bound.

Furthermore, since A must contain at least k non-zero rows and at least k non-zero columns, we conclude that $k d_{\rm row} \le n$ and $k d_{\rm col} \le n$. Theorem 2 then implies that

$$k d \le n. \tag{6}$$

In Section IV we shall use Gilbert-Varshamov bound to prove that there exists a family of codes that achieves the bounds Eqs. (4,6) up to a constant factor asymptotically in the limit $n \to \infty$. The corresponding binary $m \times m$ matrices A are defined for all sufficiently large m and obey the scaling ${\rm rank}\,(A) \ge \alpha m$, and $d_{\rm col}, d_{\rm row} \ge \beta m$ for some constants $\alpha, \beta > 0$. It leads to the scaling $k \ge \alpha m$, $d \ge \beta m$, and $\beta^2 m^2 \le n \le m^2$.

Proof of Theorem 2. We shall use notations $X_{i,j}$ and $Z_{i,j}$ for the Pauli operators acting on a qubit located at a cell (i,j). Let us begin by describing the centralizer $\mathcal{C}(\mathcal{G})$. For any row i define a row operator R_i acting by Z on every qubit located in the i-th row:

$$R_i = \prod_{j\,:\,A_{i,j}=1} Z_{i,j}.$$

Similarly, for any column j define a column operator C_j acting by X on every qubit located in the j-th column:

$$C_j = \prod_{i\,:\,A_{i,j}=1} X_{i,j}.$$

Proposition 1. *The centralizer $\mathcal{C}(\mathcal{G})$ is generated by the row and column operators,*

$$\mathcal{C}(\mathcal{G}) = \langle R_1, \ldots, R_m, C_1, \ldots, C_m \rangle. \tag{7}$$

Proof. Indeed, let us check that $R_i \in \mathcal{C}(\mathcal{G})$ for any row i. A generator $X_c X_{c'}$ located at the row i anti-commutes with R_i at both cells c and c'. Thus $X_c X_{c'}$ commutes with R_i. In addition, R_i commutes with generators $X_c X_{c'}$ located at rows $i' \ne i$ since their supports do not overlap. It also commutes with generators $Z_c Z_{c'}$ since they are both operators of Z-type. Hence $R_i \in \mathcal{C}(\mathcal{G})$. The same reasoning shows that $C_j \in \mathcal{C}(\mathcal{G})$. Conversely, let $P^Z \in \mathcal{C}(\mathcal{G})$ be a Pauli operator of Z-type. If P^Z acts

by Z on some qubit c, it must act by Z on every other qubit c' located in the same row since P^Z has to commute with all generators $X_c X_{c'}$ in this row. It shows that P^Z is a product of the row operators over some subset of rows. Similarly, any operator $P^X \in \mathcal{C}(\mathcal{G})$ of X-type is a product of the column operators over some subset of columns. It proves Eq. (7). □

Note that the supports of R_i and C_j overlap on exactly one qubit if $A_{i,j} = 1$ and do not overlap if $A_{i,j} = 0$. It follows that the matrix A controls the commutation rules between the row and column operators, namely,

$$R_i C_j = (-1)^{A_{i,j}} C_j R_i \tag{8}$$

for all pairs i, j. Using Proposition 1 we can parameterize any X-type operator $P^X \in \mathcal{C}(\mathcal{G})$ by a binary string $x \in \{0,1\}^m$ such that

$$P^X = \prod_{j=1}^{m} C_j^{x_j} = \prod_{i,j\,:\,A_{i,j}x_j=1} X_{i,j}. \tag{9}$$

Similarly, any Z-type operator $P^Z \in \mathcal{C}(\mathcal{G})$ can be parameterized by a binary string $z \in \{0,1\}^m$ such that

$$P^Z = \prod_{i=1}^{m} R_i^{z_i} = \prod_{i,j\,:\,z_i A_{i,j}=1} Z_{i,j}. \tag{10}$$

The commutation rules Eq. (8) then imply that

$$P^X P^Z = (-1)^{z^T A x} P^Z P^X, \quad z^T A x \equiv \sum_{i,j} A_{i,j} z_i x_j. \tag{11}$$

Recall that the stabilizer group $\mathcal{S}$ of a subsystem code is defined as $\mathcal{S} = \mathcal{G} \cap \mathcal{C}(\mathcal{G})$. From Eq. (11) we infer that P^X commutes with all elements of $\mathcal{C}(\mathcal{G})$ iff $x \in \mathrm{Ker}(A)$. In this case one has $P^X \in \mathcal{C}(\mathcal{C}(\mathcal{G})) = \mathcal{G}$, that is, $P^X \in \mathcal{S}$. The same argument shows that $P^Z \in \mathcal{S}$ iff $z \in \mathrm{Ker}(A^T)$. Thus stabilizers of X-type and Z-type can be identified with right and left zero-vectors of A respectively. Using the standard Gram-Schmidt orthogonalization one can choose $k = \mathrm{rank}\,(A)$ pairs of operators $P_a^X, P_a^Z \in \mathcal{C}(\mathcal{G})$, $a = 1, \ldots, k$, such that P_a^X are linear combinations of the column operators, P_a^Z are linear combinations of the row operators,

$$P_a^X P_b^Z = (-1)^{\delta_{a,b}} P_b^Z P_a^X,$$

and

$$\mathcal{C}(\mathcal{G}) = \langle \mathcal{S}, P_1^X, \ldots, P_k^X, P_1^Z, \ldots, P_k^Z \rangle.$$

It shows that P_a^X, P_a^Z are the bare logical Pauli operators and the code $\mathcal{G}$ has k logical qubits.

Let us now determine the distance of $\mathcal{G}$. Consider some bare logical operator P^X defined in Eq. (9). Let us analyze how one can reduce the weight of P^X by multiplying it with the gauge operators. Obviously, if P^X has even weight in some row i, that is, $\sum_j A_{i,j} x_j = 0 \pmod 2$, one can completely cancel P^X in this row by multiplying it with the generators $X_c X_{c'}$ located in this row. On the other hand, if P^X has odd weight in some row i, that is, $\sum_j A_{i,j} x_j = 1 \pmod 2$, the best one can do is to reduce the weight of P^X in this row down to 1. Also it is clear that multiplying P^X with gauge operators of Z-type cannot decrease its weight. It shows that the minimum weight of a dressed logical operator corresponding to P^X is equal to the number of rows i for which $\sum_j A_{i,j} x_j = 1 \pmod 2$. The number of such rows is nothing but the Hamming weight of the vector Ax. Note that $Ax \neq 0$ whenever P^X is a non-trivial logical operator since $Ax = 0$ implies that $P^X \in \mathcal{S}$, see above. We conclude that the minimum weight of X-type dressed operators coincides with the minimum Hamming weight of a vector Ax where $x \notin \mathrm{Ker}(A)$. Since such vectors span the subspace C_{col}, their minimum weight coincides with the distance d_{col}. Similar arguments show that the minimum weight of Z-type dressed operators coincides with d_{row}. □

IV. GILBERT-VARSHAMOV BOUND FOR BINARY MATRICES

Let $\mathcal{B}(m,k)$ be the set of all $m \times m$ binary matrices with the rank k over the binary field $\mathbb{F}_2$. Given any matrix $A \in \mathcal{B}(m,k)$ let $C_{\mathrm{col}}(A) \subseteq \{0,1\}^m$ be the linear subspace spanned by the columns of A. Similarly, let $C_{\mathrm{row}}(A) \subseteq \{0,1\}^m$ be the linear subspace spanned by the rows of A. Let $d_{\mathrm{col}}(A)$ and $d_{\mathrm{row}}(A)$ be the minimum distance of the classical code $C_{\mathrm{col}}(A)$ and $C_{\mathrm{row}}(A)$ respectively. We shall use the notation $H_2(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ for the binary entropy. The main result of this section is the following theorem.

Theorem 3 (Gilbert-Varshamov bound). *Let $\alpha > 0$ and $0 < \beta < 1/2$ be any constants such that $\alpha < 1 - H_2(\beta)$. Then for all sufficiently large m and for all $k \leq \alpha m$ there exists a matrix $A \in \mathcal{B}(m,k)$ such that $d_{\mathrm{col}}(A) \geq \beta m$ and $d_{\mathrm{row}}(A) \geq \beta m$.*

Proof. Our arguments will rely Gilbert-Varshamov bound for classical codes as presented in [20].

For any non-zero vector $x \in \{0,1\}^m$ let $W(x)$ be the number of matrices $A \in \mathcal{B}(m,k)$ such that $x \in C_{\mathrm{col}}(A)$. We claim that $W(x)$ does not depend on x as long as x is a non-zero vector. Indeed, let $e_1 = (10\ldots0)$ be the first basis vector of $\{0,1\}^m$. Let W be the number of matrices $A \in \mathcal{B}(m,k)$ such that $e_1 \in C_{\mathrm{col}}(A)$. Any non-zero $x \in \{0,1\}^m$ can be written as $x = Re_1$ for some $R \in \mathcal{B}(m,m)$. By definition of the column space we have $x \in C_{\mathrm{col}}(A)$ iff $x = Ay$ for some $y \in \{0,1\}^m$. Hence

$$x \in C_{\mathrm{col}}(A) \quad \text{iff} \quad e_1 \in C_{\mathrm{col}}(R^{-1}A).$$

Since the map $A \to RA$ defines a bijection from the set $\mathcal{B}(m,k)$ to itself, we conclude that $W(x) = W$. Since the rank of a matrix is invariant under transpositions, we

conclude that for any non-zero $x \in \{0,1\}^m$ the number of matrices $A \in \mathcal{B}(m,k)$ such that $x \in C_{\rm row}(A)$ also equals W.

Define a matrix $\Gamma_{x,A}$ labeled by non-zero $x \in \{0,1\}^m$ and $A \in \mathcal{B}(m,k)$ such that

$$\Gamma_{x,A} = \begin{cases} 1 & \text{if } x \in C_{\rm col}(A), \\ 0 & \text{otherwise.} \end{cases}$$

For any $A \in \mathcal{B}(m,k)$ one has $\sum_{x \neq 0} \Gamma_{x,A} = 2^k - 1$ since $C_{\rm col}(A)$ has dimension k. Also for any $x \neq 0$ one has $\sum_{A \in \mathcal{B}(m,k)} \Gamma_{x,A} = W$. Hence we arrive at

$$(2^k - 1)|\mathcal{B}(m,k)| = (2^m - 1)W. \tag{12}$$

Let $d = \lceil \beta m \rceil$ and N be the number of matrices $A \in \mathcal{B}(m,k)$ such that $C_{\rm col}(A)$ or $C_{\rm row}(A)$ contains a non-zero vector with weight smaller than d. It suffices to check that for the chosen d and any $k \leq \alpha m$ one has $N < |\mathcal{B}(m,k)|$. Applying the union bound one gets

$$N \leq 2W \sum_{i=1}^{d-1} \binom{m}{i} \leq 2W \cdot 2^{mH_2((d-1)/m)} \leq 2W 2^{mH_2(\beta)}.$$

Here we used the assumption $\beta \leq 1/2$. Using Eq. (12) and a bound $(2^m - 1)^{-1} \leq 2^{1-m}$ we arrive at

$$N \leq 4 \cdot 2^{k-m+mH_2(\beta)} \cdot |\mathcal{B}(m,k)|.$$

We conclude that $N < |\mathcal{B}(m,k)|$ whenever

$$m(\alpha - 1 + H_2(\beta)) < -2.$$

Since we assumed that $\alpha < 1 - H_2(\beta)$, it holds for all sufficiently large m. □

V. BREAKING UP THE LONG-RANGE GENERATORS

Let A be an arbitrary $m \times m$ binary matrix and $\mathcal{G}$ be the subsystem $[n,k,d]$ code associated with A. As was pointed out in Section III, one can choose an independent set of generators of $\mathcal{G}$ that includes operators $X_c X_{c'}$ for consecutive pairs of qubits c, c' that belong to the same row, and operators $Z_c Z_{c'}$ for consecutive pairs of qubits c, c' that belong to the same column. We shall consider the 2D geometry in which cells of the matrix A are identified with sites of a two-dimensional lattice of size $m \times m$.

Consider a pair of consecutive qubits c, c' in some row i and the corresponding generator $X_c X_{c'}$. In general the cells c and c' are not nearest neighbors, so there might be one or several empty cells in the i-th row (those with $A_{i,j} = 0$) between c and c'. Let these empty cells be $c_1, \ldots, c_p$, see Fig. 1.

Our strategy will be to simulate the long-range generator $X_c X_{c'}$ by adding an ancillary qubit at every cell

	1	0	0	0	0	0	1	
	c	c_1	c_2	c_3	c_4	c_5	c'	

FIG. 1. The cells c and c' represent a pair of consecutive qubits in some row of A that are not nearest neighbors. The cells $c_1, \ldots, c_p$ are empty.

$c_1, \ldots, c_p$ and connecting c, c' by a chain of short-range generators,

$$X_c X_{c'} = (X_c X_{c_1}) \cdot (X_{c_1} X_{c_2}) \cdots (X_{c_p} X_{c'}). \tag{13}$$

More formally, we shall define a new subsystem code $\mathcal{G}'$ obtained from $\mathcal{G}$ by taking out the long-range generator $X_c X_{c'}$ and adding all the short-range generators that appear in the right-hand side of Eq. (13). In addition, $\mathcal{G}'$ will contain one-qubit generators $Z_{c_1}, \ldots, Z_{c_p}$ on every added ancillary qubit. We have to verify that the codes $\mathcal{G}$ and $\mathcal{G}'$ have the same parameters k and d. It follows from the following lemma.

Lemma 1. *Let $\mathcal{G}$ be any subsystem $[n,k,d]$ code. Let q be one of the physical qubits of $\mathcal{G}$ and a be an extra ancillary qubit. Define a new subsystem code*

$$\mathcal{G}' = \langle \mathcal{G}, X_q X_a, Z_a \rangle, \tag{14}$$

where all elements of $\mathcal{G}$ act trivially on the ancillary qubit. Then $\mathcal{G}'$ has parameters $[n+1,k,d]$.

Indeed, applying the lemma with $q = c$ and $a = c_1$ we obtain a new code $\mathcal{G}'$ with the same parameters k and d, with an extra short-range generator $X_c X_{c_1}$, and an extra one-qubit generator Z_{c_1}. Although $\mathcal{G}'$ inherits the long-range generator $X_c X_{c'} \in \mathcal{G}$, we can now replace this generator by $X_{c_1} X_{c'} = (X_c X_{c_1}) \cdot (X_c X_{c'})$. Note that $X_{c_1} X_{c'}$ has a shorter length. Now we can apply the lemma again with $q = c_1$ and $a = c_2$ which breaks the generator $X_{c_1} X_{c'}$ into a pair $X_{c_1} X_{c_2}$, $X_{c_2} X_{c'}$ and an extra generator Z_{c_2}. We can continue this process until all cells $c_1, \ldots, c_p$ are occupied by ancillary qubits and the long-range generator $X_c X_{c'}$ is replaced by a chain of short-range generators, see Eq. (13), and one-qubit generators $Z_{c_1}, \ldots, Z_{c_p}$.

Similar arguments can be applied to break up all long-range Z-type generators. The resulting code $\mathcal{G}''$ has at most two qubits at every cell of A. It has two-qubit generators $X_c X_{c'}$, $Z_c Z_{c'}$ coupling only horizontal and vertical nearest neighbor cells respectively. In addition, $\mathcal{G}''$ has one-qubit generators Z_c and X_c for some cells c. Lemma 1 implies that the code $\mathcal{G}''$ has the same parameters k and d.

Now we can easily prove Theorem 1. Let m be any sufficiently large integer. Theorem 3 implies that for any $k \leq \alpha m$ there exists a matrix $A \in \mathcal{B}(m,k)$ such that $d_{\rm col}(A) \geq \beta m$ and $d_{\rm row}(A) \geq \beta m$. By Theorem 2, the corresponding subsystem code $\mathcal{G}$ has parameters $[n,k,d]$, where $n \leq m^2$ and $d = \min(d_{\rm col}, d_{\rm row}) \geq \beta m$, see Theorem 2. Transforming $\mathcal{G}$ into a local form as explained

above increases the number of physical qubits due to the addition of ancillas. Since each cell of A contains at most two qubits, we can get a $[2m^2, k, d]$ code. (Some cells of A may contain only one qubit or no qubits at all. We can add extra unused gauge qubits to each of those cells thus making the total number of qubits $2m^2$.) In the rest of this section we prove Lemma 1.

Proof. Consider an auxiliary subsystem code with a gauge group $\tilde{\mathcal{G}} = \langle \mathcal{G}, X_a, Z_a \rangle$, where all elements of $\mathcal{G}$ act trivially on the ancillary qubit. Clearly $\tilde{\mathcal{G}}$ is obtained from $\mathcal{G}$ by adding one gauge qubit and thus $\tilde{\mathcal{G}}$ has parameters $[n+1, k, d]$. Let U be the CNOT gate with the control qubit a and a target qubit q, see Fig. 2. One can easily check that U maps $\tilde{\mathcal{G}}$ to $\mathcal{G}'$, that is,

$$\mathcal{G}' = \{P' = U\tilde{P}U^\dagger, \quad \tilde{P} \in \tilde{\mathcal{G}}\}. \tag{15}$$

It follows that $\mathcal{G}'$ and $\tilde{\mathcal{G}}$ have the same number of logical

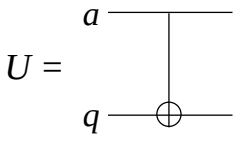

FIG. 2. The conjugation by U maps generators of $\tilde{G}$ to generators of $\mathcal{G}'$ since $UX_aU^\dagger = X_qX_a$ and $UZ_aU^\dagger = Z_a$.

qubits, that is, $\mathcal{G}'$ has parameters $[n+1, k, d']$ for some distance d'. Let us show that $d' = d$. Indeed, Eq. (15) implies that $\tilde{P}$ is a dressed logical operator for $\tilde{\mathcal{G}}$ iff $P' \equiv U\tilde{P}U^\dagger$ is a dressed logical operator for $\mathcal{G}'$. Let $\tilde{P}$ be a dressed logical operator of $\tilde{\mathcal{G}}$ with the minimum weight, that is, $|\tilde{P}| = d$. Since $X_a, Z_a \in \tilde{\mathcal{G}}$, minimality of the weight implies that $\tilde{P}$ acts trivially on the qubit a. Then $P' = U\tilde{P}U^\dagger$ is a dressed logical operator for $\mathcal{G}'$ and P' acts on the qubit a either by identity or by Z. More specifically, $P' = \tilde{P}Z_a^\alpha$ where $\alpha = 0$ iff $\tilde{P}$ acts on q by I or X, and $\alpha = 1$ iff $\tilde{P}$ acts on q by Z or Y. Since $Z_a \in \mathcal{G}'$ we conclude that $\tilde{P}$ is also a dressed logical operator for $\mathcal{G}'$ and thus $d' \le |\tilde{P}| = d$.

Conversely, let P' be a dressed logical operator of $\mathcal{G}'$ with the minimum weight, that is, $|P'| = d'$. Using the gauge operators X_qX_a and Z_a we can cancel the action of P' on the qubit a without increasing its total weight, so we can additionally assume that P' acts trivially on a. Then $\tilde{P} = U^\dagger P'U$ is a dressed logical operator for $\tilde{\mathcal{G}}$ and $\tilde{P} = P'Z_a^\alpha$ for some $\alpha \in \{0, 1\}$. Since $Z_a \in \tilde{\mathcal{G}}$ we conclude that P' is also a dressed logical operator for $\tilde{\mathcal{G}}$ and thus $d \le |P'| = d'$. We have shown that $d' = d$. □

VI. THE UPPER BOUND: TECHNICAL TOOLS

Let us begin by introducing some more notations. We shall assume that the n physical qubits occupy sites of a 2D lattice Λ of size $\sqrt{n} \times \sqrt{n}$. For any subgroup $\mathcal{G} \subseteq \mathcal{P}$ and any subset of qubits $M \subseteq \Lambda$ introduce a group

$$\mathcal{G}(M) = \{P \in \mathcal{G} \,:\, \mathrm{Supp}(P) \subseteq M\}$$

which includes all elements of $\mathcal{G}$ whose support is contained in M. In particular, $\mathcal{P}(M)$ is a group of all Pauli operators whose support is contained in M. For any subset $M \subseteq \Lambda$ let $\overline{M} = \Lambda \backslash M$ be the complement of M. Introduce also a group

$$\mathcal{G}_M = \{P \in \mathcal{P}(M) \,:\, PQ \in \mathcal{G} \quad \text{for some } Q \in \mathcal{P}(\overline{M})\}$$

which includes all Pauli operators $P \in \mathcal{P}(M)$ that can be extended to some element of $\mathcal{G}$. In other words $\mathcal{G}_M$ is a group obtained by restricting elements in $\mathcal{G}$ to M. By definition $\mathcal{G}(M) \subseteq \mathcal{G}_M \subseteq \mathcal{P}(M) \subseteq \mathcal{P}$.

Throughout this paper we shall ignore overall phase factors of Pauli operators. Then the Pauli group $\mathcal{P}$ can be regarded as the $2n$-dimensional binary space [21] such that multiplication of the Pauli operators corresponds to addition of the binary strings modulo two. For any subgroup $\mathcal{G} \subseteq \mathcal{P}$ define its dimension $\dim \mathcal{G}$ as the smallest number of Pauli operators generating $\mathcal{G}$. In particular, $\dim \mathcal{P} = 2n$ and $\dim \mathcal{P}(M) = 2|M|$. The standard stabilizer formalism [21] implies that

$$\mathcal{C}(\mathcal{C}(\mathcal{G})) = \mathcal{G}$$

and

$$\dim \mathcal{C}(\mathcal{G}) + \dim \mathcal{G} = 2n$$

for any subgroup $\mathcal{G}$. We shall need the following simple fact.

Fact 1. *Let $\mathcal{G} \subseteq \mathcal{P}$ be any subgroup and $M \subseteq \Lambda$ be any subset of qubits. Suppose $2|M| < \dim \mathcal{G}$. Then $\mathcal{G}$ contains at least one non-identity operator acting trivially on M.*

Proof. Indeed, the constraint that P acts trivially on M leads to a system $2|M|$ binary linear equations which has a non-trivial solution whenever $2|M| < \dim \mathcal{G}$. □

Consider a subsystem code with a gauge group $\mathcal{G}$ and a stabilizer group $\mathcal{S} = \mathcal{G} \cap \mathcal{C}(\mathcal{G})$. For any subset of qubits $M \subseteq \Lambda$ let $l(M)$ be the number of independent dressed logical operators supported inside M, that is,

$$l(M) = \dim \mathcal{C}(\mathcal{S}_M) \cap \mathcal{P}(M) - \dim \mathcal{G}(M).$$

Let $l_{\mathrm{bare}}(M)$ be the number of independent bare logical operators supported inside M,

$$l_{\mathrm{bare}}(M) = \dim \mathcal{C}(\mathcal{G}_M) \cap \mathcal{P}(M) - \dim \mathcal{S}(M).$$

Our first technical tool will be the following lemma which was originally proved for stabilizer codes by Yoshida and Chuang [12].

Lemma 2. *Suppose a subsystem code $\mathcal{G}$ has k logical qubits. Then*

$$l_{\mathrm{bare}}(M) + l(\overline{M}) = 2k$$

for any subset of qubits $M \subseteq \Lambda$.

It can also be regarded as a generalization of the "Cleaning Lemma" proved for subsystem codes in [9]. The Cleaning Lemma of [9] dealt only with a special case $l_{\rm bare}(M)=0$ or $l(M)=0$. Specializing Lemma 2 to stabilizer codes ($\mathcal{G}=\mathcal{S}$) one gets a simpler statement $l(M)+l(\overline{M})=2k$ which coincides with the result proved in [12]. Note that Lemma 2 does not need any spatial locality properties.

Proof. Let $m\equiv l_{\rm bare}(M)$ and let $P_1,\ldots,P_m$ be m independent bare logical operators supported inside M, that is,

$$P_a\in\mathcal{C}(\mathcal{G})\backslash\mathcal{G}\quad\text{and}\quad \mathrm{Supp}(P_a)\subseteq M \tag{16}$$

for all $a=1,\ldots,m$. Since the code has k logical qubits, one can choose $t=2k-m$ independent bare logical operators $Q_1,\ldots,Q_t\in\mathcal{C}(\mathcal{G})\backslash\mathcal{G}$ commuting with $P_1,\ldots,P_m$. Then we have

$$\mathcal{C}(\mathcal{G}_M)\cap\mathcal{P}(M)=\langle\mathcal{S}(M),P_1,\ldots,P_m\rangle. \tag{17}$$

and

$$P_aQ_b=Q_bP_a,\quad\forall\, a,b. \tag{18}$$

Taking the centralizer of both parts of Eq. (17) one arrives at

$$\mathcal{G}_M=\mathcal{P}(M)\cap\mathcal{C}(\mathcal{S}(M))\cap\mathcal{C}(P_1)\cap\ldots\cap\mathcal{C}(P_m). \tag{19}$$

Represent $Q_a=Q_a^{\rm in}Q_a^{\rm out}$, where $Q_a^{\rm in}$ and $Q_a^{\rm out}$ are the restrictions of Q_a onto M and $\overline{M}$ respectively. Combining Eqs. (16,18,19) and taking into account that $P_1,\ldots,P_m$ have support only on M one gets

$$Q_a^{\rm in}\in\mathcal{G}_M\quad\text{for all } a=1,\ldots,t.$$

By definition of $\mathcal{G}_M$, there must exist gauge operators $G_a\in\mathcal{G}$ extending $Q_a^{\rm in}$, that is, $Q'_a\equiv Q_aG_a\in\mathcal{P}(\overline{M})$ for all $a=1,\ldots,t$. It follows that $Q'_1,\ldots,Q'_t$ are independent dressed logical operators supported on $\overline{M}$, that is, $l(\overline{M})\geq t$. On the other hand, any dressed logical operator supported on $\overline{M}$ must commute with $P_1,\ldots,P_m$, and thus $l(\overline{M})\leq t$. We have proved that $l(\overline{M})=t$. □

Our second technical tool is the "Restriction Lemma" proved in [9] which relates the distance of a subsystem code $\mathcal{G}$ defined on the entire lattice Λ to the distance of a code $\mathcal{G}_M$ obtained by restricting $\mathcal{G}$ onto some subset of qubits $M\subseteq\Lambda$. Note a generators of $\mathcal{G}_M$ can be chosen as generators of $\mathcal{G}$ restricted to M. Assuming that $\mathcal{G}$ has spatially local generators with some interaction range r, the same is true for $\mathcal{G}_M$.

Definition 1. *Given an interaction range r and a subset $M\subseteq\Lambda$ let $\partial M\subseteq\overline{M}$ be the set of all sites in $\overline{M}$ that lie within distance r from M.*

Lemma 3 (Restriction Lemma)**.** *Suppose a gauge group $\mathcal{G}$ has spatially local generators with an interaction range r. Choose any subset $M\subseteq\Lambda$ and consider the subsystem code with the gauge group $\mathcal{G}_M$. Then one of the following is true:*
(1) The code $\mathcal{G}_M$ has no logical qubits,
(2) The code $\mathcal{G}_M$ has distance at least $d-|\partial M|$ where d is the distance of $\mathcal{G}$.

VII. HOLOGRAPHIC PRINCIPLE FOR ERROR CORRECTION

Let $\mathcal{G}$ be the gauge group of some subsystem $[n,k,d]$ code. We shall fix some choice of spatially local generators of $\mathcal{G}$ such that each generator has support in a box of size $r\times r$ for some interaction range $r=O(1)$. By definition of the distance d, no subset $M\subseteq\Lambda$ of less than d qubits can support a dressed logical operator, that is, $l(M)=0$ whenever $|M|<d$. Accordingly, one can choose R proportional to $\sqrt{d}$ such that no square box of size $R\times R$ supports a dressed logical operator. In this section we derive a much stronger condition which can be regarded as an analogue of the famous holographic principle.

Lemma 4. *One can choose $R=\Omega(d)$ such that no square box of size $R\times R$ supports a dressed logical operator.*

Loosely speaking, the lemma asserts that a non-trivial dressed logical operator cannot be supported on a region whose *perimeter* is smaller than the distance d (with some constant coefficient depending on r) even if the number of qubits in the interior of the region is much larger than d. A similar result was obtained in [11] for 2D stabilizer codes. We shall begin by proving an auxiliary lemma.

Lemma 5. *Let A,B be any disjoint subsets of qubits such that $l(A)=0$ and $|B|+|\partial\overline{A}|<d$. Then $l(AB)=0$.*

Proof. Let C be the complement of AB such that $\Lambda=ABC$. Applying Lemma 2 to the subset A we conclude that $l_{\rm bare}(BC)=2k$. Hence we can choose a complete set of $2k$ bare logical operators $\overline{X}_1,\overline{Z}_1,\ldots,\overline{X}_k,\overline{Z}_k\in\mathcal{C}(\mathcal{G})\backslash\mathcal{G}$ supported inside BC. Consider a subsystem code specified by the gauge group $\mathcal{G}_{BC}$ that involves only qubits of BC. We claim that $\mathcal{G}_{BC}$ has k logical qubits and $\overline{X}_a,\overline{Z}_a$ are the bare logical operators of $\mathcal{G}_{BC}$. Indeed, since $\overline{X}_a,\overline{Z}_a$ have support on BC and commute with $\mathcal{G}$ we infer that $\overline{X}_a,\overline{Z}_a\in\mathcal{C}(\mathcal{G}_{BC})$ for all a. Accordingly, $\overline{X}_a,\overline{Z}_a\notin\mathcal{G}_{BC}$ since $\overline{X}_a\overline{Z}_a=-\overline{Z}_a\overline{X}_a$ for all a. It shows that $\mathcal{G}_{BC}$ has at least k logical qubits. Conversely, let $\overline{P}\in\mathcal{C}(\mathcal{G}_{BC})\backslash\mathcal{G}_{BC}$ be any bare logical operator of $\mathcal{G}_{BC}$. By definition of $\mathcal{G}_{BC}$ it implies that $\overline{P}\in\mathcal{C}(\mathcal{G})$ and $\overline{P}\notin\mathcal{G}$, that is, $\overline{P}$ must be a bare logical operator of the original code $\mathcal{G}$ in which case it can be expressed in terms of $\overline{X}_a,\overline{Z}_a$. We have shown that $\mathcal{G}_{BC}$ has k logical qubits and $\overline{X}_a,\overline{Z}_a$ are the bare logical operators of $\mathcal{G}_{BC}$. Applying the Restriction Lemma to the code $\mathcal{G}_{BC}$ we conclude

that $\mathcal{G}_{BC}$ has distance $d' \geq d - |\partial(BC)| = d - |\partial\overline{A}|$. The assumptions of the lemma then imply $d' > |B|$. Thus the code $\mathcal{G}_{BC}$ has no dressed logical operators supported inside B, that is, $l'(B) = 0$ (here and in the rest of the proof all quantities labeled by a prime refer to the code $\mathcal{G}_{BC}$). Applying Lemma 2 to the code $\mathcal{G}_{BC}$ and the subset B we infer that $l'_{\rm bare}(C) = 2k$. Hence we can choose a complete set of bare logical operators $\overline{X}'_a, \overline{Z}'_a \in \mathcal{C}(\mathcal{G}_{BC})\backslash\mathcal{G}_{BC}$ supported on C. But then $\overline{X}'_a, \overline{Z}'_a$ are also bare logical operators of the original code $\mathcal{G}$ which implies $l_{\rm bare}(C) = 2k$ for the code $\mathcal{G}$. Applying Lemma 2 to the code $\mathcal{G}$ and the subset C we arrive at $l(AB) = 0$. □

Now we are ready to prove Lemma 4.

Proof. Choose any R such that $rR \ll d$. For any square box M of size $R \times R$ consider a sequence of square boxes $A_1 \subset A_2 \subset \ldots \subset A_p = M$ such that A_1 has cardinality $|A_1| < d$ and A_{i+1} is the smallest box that contains A_i and the boundary of A_i. Let $B_i = A_{i+1}\backslash A_i$. Then $|B_i| + |\partial\overline{A_i}| \leq O(1)rR < d$ for all $i = 1, \ldots, p$. Since $|A_1| < d$ we have $l(A_1) = 0$. Applying Lemma 5 inductively with $A \equiv A_i$ and $B \equiv B_i$ we arrive at $l(A_p) = l(M) = 0$. □

VIII. PROOF OF THE UPPER BOUND

Now we are ready to prove the upper bound Eq. (3). By assumption, the support of any generator of the gauge group $\mathcal{G}$ can be covered by a square block of size $r \times r$ for some interaction range $r = O(1)$. Consider a partition of the lattice $\Lambda = AB$ shown on Fig. 3. The region A consists of square blocks $A_1, \ldots, A_m$ of size $R \times R$ with $R = \Omega(d)$ such that $l(A_i) = 0$, see Lemma 4. We choose the separation between adjacent blocks in A at least r such that any generator of $\mathcal{G}$ overlaps with at most block in A. We claim that

$$l_{\rm bare}(A) = 0. \tag{20}$$

Indeed, suppose $P \in \mathcal{C}(\mathcal{G})\backslash\mathcal{G}$ is a bare logical operator supported on A. Let P_i be the restriction of P onto a block A_i such that $P = P_1 P_2 \cdots P_m$. Since any generator of $\mathcal{G}$ overlaps with at most one block in A, we have $P_i \in \mathcal{C}(\mathcal{G})$ for all i. However there must exist at least one block A_i such that $P_i \notin \mathcal{G}$ since otherwise $P \in \mathcal{G}$. Then for such a block we have $P_i \in \mathcal{C}(\mathcal{G})\backslash\mathcal{G}$, that is, P_i is a bare logical operator supported inside A_i. But this implies $l(A_i) \geq l_{\rm bare}(A_i) > 0$ which is a contradiction. It proves Eq. (20). Applying Lemma 2 we get

$$l(B) = 2k.$$

However, a subset B can support at most $2|B|$ independent Pauli operators which implies $2|B| \geq l(B)$, that is, $|B| \geq k$. Simple algebra shows that $|B| = O(n/R) = O(n/d)$ and thus $kd = O(n)$.

Let us now prove the stronger bound Eq. (1) assuming that both $\mathcal{G}$ and $\mathcal{S}$ have spatially local generators with a constant interaction range r and r_s respectively. Consider a partition of the lattice $\Lambda = ABC$ shown on Fig. 4. The regions A, B consist of blocks $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ respectively of size $R \times R$ with $R = \Omega(d)$ such that $l(A_i) = 0$ and $l(B_i) = 0$, see Lemma 4. The region C consists of disks of radius $\max\{r, r_s\}$ so that adjacent blocks in A and adjacent blocks in B are separated from each other by distance $\max\{r, r_s\}$. Then we can choose generators in $\mathcal{G}$ and $\mathcal{S}$ such that any generator overlaps with at most one block in A and with at most one block in B. Applying the same arguments as above we get $l_{\rm bare}(A) = 0$ and thus Lemma 2 implies

$$l(BC) = 2k.$$

Let us assume that

$$|C| < k \tag{21}$$

and show that it leads to a contradiction. Indeed, choose any set of $2k$ independent dressed logical operators $P_1, \ldots, P_{2k} \in \mathcal{C}(\mathcal{S})\backslash\mathcal{G}$ supported inside BC and let $\mathcal{Q} = \langle P_1, \ldots, P_{2k}\rangle$. Applying Fact 1 to region C and the group $\mathcal{Q}$ we conclude that there exists at least one non-trivial dressed logical operator $P \in \mathcal{C}(\mathcal{S})\backslash\mathcal{G}$ supported only inside B. Let P_i be the restriction of P onto a block B_i such that $P = P_1 P_2 \cdots P_m$. Since any generator of $\mathcal{S}$ overlaps with at most one block in B we conclude that $P_i \in \mathcal{C}(\mathcal{S})$. However, there must exist at least one block B_i such that $P_i \notin \mathcal{G}$ since otherwise $P \in \mathcal{G}$. Then P_i is a non-trivial dressed logical operator, that is, $l(B_i) > 0$ which is a contradiction. Hence Eq. (21) is impossible and we have $|C| \geq k$. Simple algebra shows that $|C| = O(n/R^2) = O(n/d^2)$ which yields $kd^2 = O(n)$.

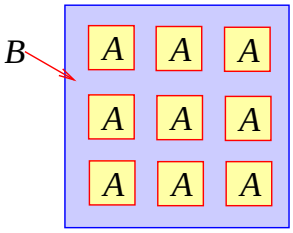

FIG. 3. The partition of the lattice $\Lambda = AB$ used to prove the bound $kd = O(n)$. The region A consists of square blocks $A_1, \ldots, A_m$ of size $R \times R$ with $R = \Omega(d)$ such that $l(A_i) = 0$. Adjacent blocks are separated from each other by distance $r = O(1)$. It implies $l_{\rm bare}(A) = 0$ and thus $l(B) = 2k$. This is possible only if $|B| \geq k$ which yields $kd = O(n)$.

IX. CONCLUSIONS AND OPEN PROBLEMS

In this paper we have studied subsystem codes for which the gauge group has spatially local generators in the 2D geometry. It was shown that the parameters $[n, k, d]$ of such codes must obey an upper bound $kd = O(n)$. We have also introduced a family of codes, the

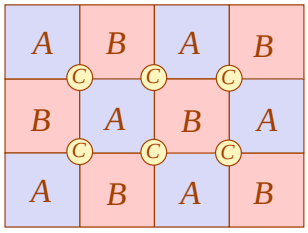

FIG. 4. The partition of the lattice $\Lambda = ABC$ used to prove the bound $kd^2 = O(n)$. The regions A, B consist of blocks $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ respectively of size $R \times R$ with $R = \Omega(d)$ such that $l(A_i) = 0$ and $l(B_i) = 0$. The region C consists of disks of radius $\max\{r, r_s\}$ so that adjacent blocks in A and adjacent blocks in B are separated from each other by distance $\max\{r, r_s\}$. It implies $l_{\rm bare}(A) = 0$ and thus $l(BC) = 2k$. If k violates the upper bound one would have $l(B) \geq l(BC) - 2|C| > 0$. Assuming that $\mathcal{S}$ has spatially local generators this is possible only if $l(B_i) > 0$ for some block B_i which is a contradiction.

generalized Bacon-Shor codes, that achieves this bound with both k and d proportional to $\sqrt{n}$. The gauge group of the generalized Bacon-Shor codes involves only two-qubit generators of type XX and ZZ coupling nearest-neighbor qubits (and some one-qubit generators). It follows that the syndrome measurement for these codes requires only eigenvalue measurements for operators XX and ZZ on nearest-neighbor qubits. Our proof of existence presented in Sections III,IV is not constructive since it requires binary matrices achieving the Gilbert-Varshamov bound stated in Theorem 3. On the other hand, one can easily show that a random $m \times m$ binary matrix A with a fixed rank k achieves the Gilbert-Varshamov bound of Theorem 3 with probability approaching one in the limit $m \to \infty$. Therefore for finite sufficiently small lattice sizes one can simply choose the desired binary matrix A randomly (with a fixed rank), compute the minimum distances $d_{\rm col}$, $d_{\rm row}$ and check whether the Gilbert-Varshamov bound is satisfied.

A serious drawback of the standard 2D Bacon-Shor code [13] that precludes it from being used in the topological quantum computation schemes is the lack of a constant error threshold in the limit of large lattice size [16, 22]. We expect that the same drawback is shared by the generalized Bacon-Shor codes introduced in the paper. It is therefore an interesting open problem whether it is possible to construct 2D subsystem codes with both k and d proportional to $\sqrt{n}$ which would have a good behavior under random uncorrelated errors.

Finally, let us point out that our construction of the generalized Bacon-Shor codes naturally extends to 3D Bacon-Shor codes [13]. In the 3D case the binary matrix A should be replaced by a three-dimensional binary array with qubits occupying cells with $A_{i,j,k} = 1$. The corresponding gauge group $\mathcal{G}$ is generated by operators XX, YY, and ZZ coupling pairs of qubits that differ only in x, y, and z-coordinate respectively. For any choice of the array A the resulting subsystem code can be transformed into the spatially local form by introducing ancillary qubits and simulating every long-range generator by a chain of short-range generators as described in Section V. Finding the optimal scaling of d and k for such generalized 3D Bacon-Shor codes is an interesting open problem.

ACKNOWLEDGMENTS

The author would like to thank Graeme Smith and Barbara Terhal for useful discussions. This work was partially supported by DARPA QUEST program under contract number HR0011-09-C-0047.

APPENDIX A

The purpose of this section is to prove the upper bound Eq. (5). We shall also construct a family of codes that achieves this bound.

We will show that a tuple $[n, k, d_{\rm row}, d_{\rm col}]$ can be realized by some binary matrix A only if the following quadratic optimization problem has feasible solutions:

$$r_x \geq 0 \qquad \forall x \in \Sigma^k \tag{22}$$

$$c_x \geq 0 \qquad \forall x \in \Sigma^k \tag{23}$$

$$\sum_{x\,:\,x\cdot y=1} r_x \geq d_{\rm row} \qquad \forall y \in \Sigma^k \backslash 0, \tag{24}$$

$$\sum_{x\,:\,x\cdot y=1} c_x \geq d_{\rm col} \qquad \forall y \in \Sigma^k \backslash 0, \tag{25}$$

$$\sum_{x,y\,:\,x\cdot y=1} r_x c_y = n. \tag{26}$$

Here r_x and c_x are integer-valued variables labeled by binary strings $x \in \Sigma^k \equiv \{0,1\}^k$. We used the notation $x \cdot y \equiv \sum_{i=1}^k x_i y_i \pmod 2$ for the binary inner product. Hence we can get a lower bound on n by minimizing the quadratic function of r_x, c_y defined in Eq. (26) subject to constraints Eqs. (22-25).

Let us begin by deriving analogous optimization problem corresponding to ordinary classical codes. Let G be the generating matrix of some classical $[n, k, d]$ code, such that G has size $k \times n$ and the rows of G form the basis of the codespace. For any binary string $x = [x_1, \ldots, x_k] \in \Sigma^k$ let n_x be the number of columns $[x_1, \ldots, x_k]^T$ in the matrix G. Any codeword can be represented as yG for some binary string $y \in \Sigma^k$. One can easily check that the Hamming weight of yG can be expressed as

$$|yG| = \sum_{x\,:\,x\cdot y=1} n_x,$$

where the summation is over binary strings $x \in \Sigma^k$. Hence a tuple $[n, k, d]$ can be realized by some code iff the

following optimization problem has feasible solutions:

$$n_x \geq 0 \qquad \forall x \in \Sigma^k \tag{27}$$

$$\sum_{x\,:\,x\cdot y=1} n_x \geq d \qquad \forall y \in \Sigma^k \backslash 0, \tag{28}$$

$$\sum_{x\in\Sigma^k} n_x = n. \tag{29}$$

Here we treat n_x as integer-valued variables. Indeed, any solution $\{n_x\}$ can be transformed into a generating matrix G (defined uniquely up to permutation of columns) of size $k \times n$. Then Eq. (29) implies that G represents a $[n, k, d]$ classical code.

Now consider an arbitrary binary matrix A of rank k. Without loss of generality the first k rows and the first k columns of A are linearly independent (otherwise permute rows or columns). Let $G_{\rm row}$ be the generating matrix of a classical code spanned by the first k rows of A. Similarly, let $G_{\rm col}$ be the generating matrix of a classical code spanned by the first k rows of A^T. (Note that $G_{\rm row}$ and $G_{\rm col}$ may have different length if A is not a square matrix.) Let c_x be the number of columns $x = [x_1, \ldots, x_k]^T$ in $G_{\rm col}$. Let r_x be the number of columns $x = [x_1, \ldots, x_k]^T$ in $G_{\rm row}$. The variables c_x, r_x must obey inequalities analogous to Eq. (27,28) since we assumed that $G_{\rm col}$ and $G_{\rm row}$ have distance $d_{\rm col}$ and $d_{\rm row}$ respectively. It yields Eqs. (22-25). It remains to derive Eq. (26). Consider any row of A that starts with $x = [x_1, \ldots, x_k]$. It can be represented as $zG_{\rm row}$ for some $z = z(x) \in \Sigma^k$ since by assumption any row of A is a linear combination of the first k rows. Moreover, the function $z(x)$ must be linear and invertible, that is, $z(x) = xM$ for some $k \times k$ invertible matrix M. As before, the Hamming weight of $zG_{\rm row}$ can be expressed as

$$|zG_{\rm row}| = \sum_{y\,:\,y\cdot z=1} r_y,$$

where the summation is over binary strings $y \in \Sigma^k$. Since the number of rows in A that start from $x = [x_1, \ldots, x_k]$ is equal to c_x we arrive at

$$n = |A| = \sum_{x\in\Sigma^k} c_x\, |z(x)G_{\rm row}| = \sum_{x,y\,:\,xM\cdot y=1} c_x r_y.$$

Here $xM \cdot y$ is the inner product between binary strings xM and y. Since Eqs. (22-25) are invariant under a change of variables $c_x \to c_{xM}$ for any invertible matrix M, we get Eq. (26).

Now we can easily prove Eq. (5). Let $r = \sum_{x\neq 0} r_x$. Adding up Eq. (24) for all $y \neq 0$ we count each r_x exactly 2^{k-1} times, that is, we get

$$r \geq d_{\rm row}(2^k - 1)2^{1-k} = d_{\rm row}(2 - 2^{1-k}).$$

Then combining Eqs. (25,26) we get $n \geq d_{\rm col} r$ which is equivalent to Eq. (5).

Let us show that Eq. (5) is tight. Choose any integer $k \geq 1$ and define a matrix A of size $(2^k - 1) \times (2^k - 1)$ as a binary version of the Hadamard matrix,

$$A_{x,y} = x \cdot y$$

with $x, y \in \Sigma^k \backslash 0$. Obviously, A is a symmetric matrix. Its row-space and its column-space coincide with the Hamming code $[2^k - 1, k, 2^{k-1}]$. In particular, any row and any column of A have weight 2^{k-1}. Thus we get $d_{\rm row} = d_{\rm col} = 2^{k-1}$ and $n = (2^k - 1)2^{k-1}$. It achieves the bound Eq. (5).

[1] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452–4505, 2002.

[2] R. S. Andrist, H. G. Katzgraber, H. Bombin, and M. A. Martin-Delgado. Tricolored Lattice Gauge Theory with Randomness: Fault-Tolerance in Topological Color Codes. 2010, arXiv:1005.0777.

[3] H. Bombin and M. A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97, 2006.

[4] H. G. Katzgraber, H. Bombin, R. S. Andrist, and M. A. Martin-Delgado. Topological color codes on union jack lattices: A stable implementation of the whole clifford group. *Phys. Rev. A*, 81:012319, 2010.

[5] R. Raussendorf and J. Harrington. Fault-Tolerant Quantum Computation with High Threshold in Two Dimensions. *Phys. Rev. Lett.*, 98(19):190504, 2007.

[6] R. Raussendorf, J. Harrington, and K. Goyal. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.*, 9:199, 2007.

[7] H. Bombin and M. A. Martin-Delgado. Quantum Measurements and Gates by Code Deformation. *Jour. of Phys. A.*, 42:095302, 2009.

[8] D. P. DiVincenzo. Fault-tolerant architectures for superconducting qubits. *Physica Scripta Volume T*, 137(1):014020, 2009.

[9] S. Bravyi and B. M. Terhal. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New J. Phys.*, 11:043029, 2009.

[10] A. Kay and R. Colbeck. Quantum Self-Correcting Stabilizer Codes. 2008, arXiv:0810.3557.

[11] S. Bravyi, D. Poulin, and B. M. Terhal. Tradeoffs for reliable quantum information storage in 2D systems. *Phys. Rev. Lett.*, 104:050503, 2010.

[12] B. Yoshida and I. L. Chuang. Framework for classifying logical operators in stabilizer codes. *Phys. Rev. A*, 81(5):052302, 2010.

[13] D. Bacon. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Phys. Rev. A*, 73(1):012340, 2006.

[14] D. Poulin. Stabilizer Formalism for Operator Quantum Error Correction. *Phys. Rev. Lett.*, 95(23):230504, 2005.

[15] P. Aliferis and A. W. Cross. Subsystem Fault Tol-

erance with the Bacon-Shor Code. *Phys. Rev. Lett.*, 98(22):220502, 2007.

[16] A. W. Cross, D. P. DiVincenzo, and B. M. Terhal. A comparative code study for quantum fault-tolerance. 2007, arXiv:0711.1556.

[17] H. Bombin. Topological subsystem codes. *Phys. Rev. A*, 81(3):032301, 2010.

[18] H. Bombin. Clifford gates by code deformation. *arXiv:1006.5260*, 2010.

[19] D. Bacon and A. Casaccino. Quantum Error Correcting Subsystem Codes From Two Classical Linear Codes. 2006, arXiv:quant-ph/0610088.

[20] A. Calderbank and P. Shor. Good Quantum Error-Correcting Codes Exist. *Phys. Rev. A*, 54(2):1098, 1996.

[21] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum Error Correction and Orthogonal Geometry. *Phys. Rev. Lett.*, 78:405, 1997.

[22] F. Pastawski, A. Kay, N. Schuch, and I. Cirac. Limitations of Passive Protection of Quantum Information. 2009, arXiv:0911.3843.