Tradeoffs for reliable quantum information storage in 2D systems

Sergey Bravyi,[1] David Poulin,[2] and Barbara Terhal[1]

[1] *IBM Watson Research Center, Yorktown Heights NY 10598, USA*

[2] *Département de Physique, Université de Sherbrooke, Québec, Canada*

(Dated: September 28, 2009)

We ask whether there are fundamental limits on storing quantum information reliably in a bounded volume of space. To investigate this question, we study quantum error correcting codes specified by geometrically local commuting constraints on a 2D lattice of finite-dimensional quantum particles. For these 2D systems, we derive a tradeoff between the number of encoded qubits k, the distance of the code d, and the number of particles n. It is shown that $kd^2 = O(n)$ where the coefficient in $O(n)$ depends only on the locality of the constraints and dimension of the Hilbert spaces describing individual particles. We show that the analogous tradeoff for the classical information storage is $k\sqrt{d} = O(n)$.

PACS numbers: 03.67.Pp, 03.67.Ac, 03.65.Ud

Understanding the limits imposed on information processing by the laws of physics is a problem of fundamental and practical importance. A variety of hardware-independent limitations on the power of computers arising from thermodynamics, quantum mechanics, and relativity have been identified recently [1–3].

In this Letter we derive a fundamental upper bound on the amount of quantum information that can be stored reliably in a given volume of a 2D space. This bound stems from *geometric locality* of quantum operations used to detect and correct errors as well as peculiar features of *quantum entanglement* in 2D systems. We shall model the information storage using the framework of quantum error correcting codes [4]. Specifically, we consider a system of n finite-dimensional quantum particles (qudits) occupying sites of a 2D lattice Λ. For the sake of clarity we shall consider a regular square lattice of size $\sqrt{n}\times\sqrt{n}$ with open boundary conditions, although our results can be easily extended to more general 2D lattices and periodic boundary conditions. We shall focus on codes for which the codespace $\mathcal{C}$ spanned by encoded states can be represented as a common eigenspace of geometrically local pairwise commuting [24] projectors $\Pi_1,\ldots,\Pi_m$ such that

$$\mathcal{C} = \{|\psi\rangle \,:\, \Pi_a\,|\psi\rangle = |\psi\rangle \quad \text{for all } a\}. \tag{1}$$

The codespace $\mathcal{C}$ can be regarded as the ground-state subspace of a local gapped Hamiltonian

$$H = -\sum_{a=1}^{m} \Pi_a, \quad \Pi_a\Pi_b = \Pi_b\Pi_a. \tag{2}$$

Such a code is able to encode $k = \log_2 \dim \mathcal{C}$ logical qubits. Let d be the distance of the code [25]. Our main result in an upper bound

$$k \le \frac{c\,n}{d^2}. \tag{3}$$

Here c is a constant coefficient that depends only on locality of the projectors defining the codespace and dimension of the Hilbert space describing individual particles. The bound Eq. (3) is tight up to a constant factor since 2D surface codes [5] achieve the scaling $kd^2 \sim n$ for any given n and d [26]. The bound Eq. (3) can be put in sharp contrast with the existence of good stabilizer codes [6] for which $k/n \ge c_1$ and $d/n \ge c_2$ for some constants c_1, c_2. Our result implies that the distance of 2D quantum codes with a non-zero rate k/n is upper bounded by a constant independent of n. It also implies that the distance of any 2D quantum code is at most $O(\sqrt{n})$ extending the results of [7] beyond stabilizer codes.

The motivation for our work stems from several sources. Firstly, quantum error correcting codes provide toy models for how topological quantum order (TQO) can emerge in the ground states of 2D spin systems with short-range interactions. For example, string-net models introduced by Levin and Wen [8] are described by Hamiltonians involving a sum of commuting projectors, see [9]. The ground state of string-net models defined on a torus (or higher genus surface) has topological degeneracy and can be regarded as a codespace of a quantum code. Alternatively, the codespace can be chosen as an excited subspace corresponding to a particular configuration of excitations (anyons) — the approach adopted by Kitaev in the topological quantum computing scheme [10]. In this case the code distance is proportional to the distance between anyons while the bound Eq. (3) asserts that the number of encoded qubits is at most a constant fraction of the number of anyons.

Secondly, one can interpret Eq. (3) as a tradeoff between *degeneracy* and *stability* that must be obeyed by ground states of the code Hamiltonian H. Assuming that H is translation-invariant, one has a stable zero temperature phase in the thermodynamic limit if the degeneracy of the ground state cannot be lifted by weak local perturbations below some critical value of the perturbation parameter. It is well known that adding a weak local perturbation to H lifts the degeneracy of the ground state only in order $\Omega(d)$ of perturbation theory [10]. Thus a necessary condition for $T = 0$ stability is that the distance d must be infinite in the thermodynamic limit. Then the tradeoff Eq. (3) implies that the *amount of quantum information stored per unit volume*, $k/n \le c/d^2$ goes to zero in the thermodynamic limit. This suggests a possible connection between our results and the celebrated *holographic principle* asserting that the amount of information that can be encoded in a volume of space M scales as the area of the boundary of M.

Generalizing our techniques to quantum codes defined on a D-dimensional lattice yields

$$k \le \frac{cn}{d^\alpha}, \quad \alpha = \frac{2}{D-1}. \tag{4}$$

As was shown in Ref. [7], the distance of any D-dimensional stabilizer code satisfies the bound $d \le O(n^{(D-1)/D})$. Since the upper bound Eq. (4) permits codes with $k = O(1)$ and $d \sim n^{1/\alpha} \sim n^{(D-1)/2}$, it cannot be tight for all values of n and d unless $D = 2$. Using the folded surface code construction [11] one can construct a D-dimensional stabilizer code encoding 1 qubit into n qubits with the distance $d \sim \sqrt{n}$. To the best of our knowledge there are no examples of D-dimensional codes for which the distance grows faster than $\sqrt{n}$. Therefore one cannot exclude the possibility that the bound Eq. (3) holds for any spatial dimension, although we consider this to be unlikely.

It should be emphasized that throughout this paper the geometric locality of the constraints Π_a is defined using the standard Euclidean geometry [27]. At the same time, the bound Eq. (3) can be violated for non-Euclidean geometry. For example, Ref. [12] constructed surface codes on general planar graphs with a constant rate k/n and the distance $d \sim \log n$, see also [13]. Also, it is known that stabilizer codes with $k = 1$ and $d \sim \sqrt{n}\log n$ can be constructed on triangulations of some 4D Riemannian surfaces, see Theorem 12.4 in Ref. [14].

We note that even though our results cover a large family of 2D quantum codes on qudits beyond the standard family of stabilizer codes, they do not include the important family of quantum subsystem codes [15, 16].

One can also ask about the analogue of the tradeoff Eq. (3) for classical information storage. In Appendix A we prove that any 2D classical code specified by geometrically local constraints obeys the bound

$$k \le \frac{c\,n}{\sqrt{d}} \tag{5}$$

Here c is a constant depending only on the dimension of individual particles and locality of the constraints specifying the code. Using the mapping from 1D cellular automatons to 2D classical codes we construct a family of codes with $k \sim \sqrt{n}$ and $d \sim n^{0.8}$ which is quite close to saturating the bound Eq. (5). We conjecture that for any $\epsilon > 0$ there exists a family of 2D classical codes with $k \sim \sqrt{n}$ and $d \sim n^{1-\epsilon}$ (the locality of the constraints may depend on ϵ). It would imply that the bound Eq. (5) is tight up to a factor growing slower than any power of n.

Definitions and notations. We shall assume that the locality of the projectors Π_a can be characterized by a constant interaction range w such that the support of any projector Π_a can be covered by a square block of size $w \times w$. Let

$$\Pi = \prod_{a=1}^m \Pi_a \tag{6}$$

be the projector on the codespace $\mathcal{C}$. A state ρ is called an *encoded state* iff it has support on the codespace $\mathcal{C}$, that is, $\Pi\rho = \rho\Pi = \rho$. We shall say that a region $M \subseteq \Lambda$ is *correctable* iff there exists an error correction operation (a trace preserving completely positive map) $\mathcal{R}$ that corrects the erasure of all particles in M, that is, for any encoded state ρ one has

$$\mathcal{R}(\mathrm{Tr}_M\, \rho) = \rho. \tag{7}$$

By definition of the distance any region of size smaller than d is correctable.

We shall use the notation $\bar{M} = \Lambda\backslash M$ for the complement of a region M. For any region $M \subseteq \Lambda$ and for any fixed state ρ let $S(M) = -\,\mathrm{Tr}\,\rho_M \log \rho_M$ be the von Neumann entropy of the reduced density matrix ρ_M. Using techniques from Ref. [17] one can easily show that the error correction condition Eq. (7) has the following entropic counterpart.

Fact 1. *If a region M is correctable then*

$$S(M|\bar{M}) = -S(M) \tag{8}$$

for any encoded state ρ. Here $S(M|\bar{M}) = S(M\bar{M}) - S(\bar{M})$ is the entropy of M conditioned on $\bar{M}$.

Note that the equality Eq. (8) holds automatically for any pure state of $M\bar{M}$ which would correspond to a trivial code with $k = 0$. More generally, Eq. (8) implies that there exists a (virtual) partition $\bar{M} = AB$ such that any encoded state ρ is a tensor product of some fixed pure state held by MA and some state of B depending on ρ [18].

Proof. Let $\rho_{M\bar{M}}$ be any encoded state and $\rho_{M\bar{M}C}$ be its purification. Define an error $\mathcal{T} = \mathrm{Tr}_M \otimes \mathrm{id}_{\bar{M}C}$ erasing the region M. By assumption there exists a recovery operation $\mathcal{R}$ such that

$$\mathcal{R}\circ\mathcal{T}(\rho_{M\bar{M}C}) = \rho_{M\bar{M}C}, \quad \mathcal{R}\circ\mathcal{T}(\rho_{M\bar{M}}\otimes\rho_C) = \rho_{M\bar{M}}\otimes\rho_C.$$

Therefore

$$\mathcal{S}(\rho_{M\bar{M}C}||\rho_{M\bar{M}}\otimes\rho_C) = \mathcal{S}(\mathcal{T}(\rho_{M\bar{M}C})||\mathcal{T}(\rho_{M\bar{M}}\otimes\rho_C)) \tag{9}$$

since the relative entropy is monotone decreasing under quantum operations, see [19]. Using the definition of $\mathcal{T}$ one can rewrite Eq. (9) as

$$\mathcal{S}(\rho_{M\bar{M}C}||\rho_{M\bar{M}}\otimes\rho_C) = S(\rho_{\bar{M}C}||\rho_{\bar{M}}\otimes\rho_C). \qquad (10)$$

Taking into account that $\rho_{M\bar{M}C}$ is a pure state, one can check that Eq. (10) is equivalent to Eq. (8). $\square$

We begin by sketching the steps leading up to our main result, the bound in Eq. (3). Let R be the largest integer m such that any square block of size $m\times m$ is correctable. Note that R is at least $\sqrt{d}$ by the definition of the distance.

Consider a partition of the lattice $\Lambda = ABC$ shown in Fig. 1. The regions A and B consist of blocks of size $R\times R$, so that each individual block in A and B is correctable. The total number of blocks is roughly n/R^2. The regions A and B have small corner regions taken out which make up the region C. The purpose of the region C is to provide a sufficiently large separation between the neighboring blocks in A and between the neighboring blocks in B such that any projector Π_a overlaps with at most one block in A and with at most one block in B. It guarantees that the entire regions A and B are correctable (see Lemma 2 below). Applying Eq. (8) to regions A and B yields

$$S(A|BC) = -S(A) \quad \text{and} \quad S(B|AC) = -S(B) \qquad (11)$$

for any encoded state. Let ρ be the maximally mixed encoded state such that $k = S(\Lambda)$. Using Eq. (11) we get

$$\begin{aligned} S(\Lambda) &= S(BC) + S(A|BC) = S(BC) - S(A) \\ &\leq S(C) + S(B) - S(A). \end{aligned} \qquad (12)$$

Similarly

$$\begin{aligned} S(\Lambda) &= S(AC) + S(B|AC) = S(AC) - S(B) \\ &\leq S(C) + S(A) - S(B). \end{aligned} \qquad (13)$$

Adding together Eqs. (12,13) yields

$$k = S(\Lambda) \leq S(C) \leq |C| \sim \frac{n}{R^2}. \qquad (14)$$

The second step in the proof which may be less intuitive is to show that $R\geq cd$ for some constant c depending only on locality of the constraints. In other words, we need to prove that any block of size roughly $d\times d$ is correctable. Our main technical tool will be the *Disentangling Lemma* characterizing entanglement properties of the maximally mixed encoded state proportional to the projector on the codespace Π. We shall prove that any correctable region M can be completely disentangled from the rest of the lattice by acting only on the boundary of the region (see Lemma 1 below). The disentangling operation leaves the region M in a pure state, so that all entropy of M can be "cleaned out" by acting along the boundary of M. This result can be regarded as a generalization of the Cleaning Lemma from [7] beyond stabilizer codes. For any region M let ∂M be the boundary of M, that is, the region covered by the supports of all projectors Π_a that couple M with $\bar{M}$. The following result is a simple corollary of the Disentangling Lemma.

Corollary 1. *Let M be any correctable region. Consider any regions $B\subseteq M$ and $C\subseteq\bar{M}$ such that BC is correctable and $\partial M\subseteq BC$. Then $M\cup C$ is also correctable.*

The idea of the proof is illustrated in Fig. 2. Let us apply Corollary 1 to a square block M of size $R\times R$. Choose B and C as layers of thickness w adjacent to the surface of M such that $B\subseteq M$ and $C\subseteq\bar{M}$, see Fig. 2. Since all the projectors Π_a have size at most w, the condition $\partial M\subseteq BC$ is satisifed. Note that $|BC| = cwR$ for some constant c. If $|BC|<d$ then BC is correctable and Corollary 1 would imply that $M\cup C$ is correctable. But $M\cup C$ is a square block of size larger than R which contradicts the choice of R. Thus $|BC|\geq d$, that is, $R\geq d/(cw)\sim d$. Substituting this bound into Eq. (14) completes the proof of Eq. (3).

Let us comment on how to extend this proof technique to D-dimensional lattices. The partition $\Lambda = ABC$ of Fig. 1 should be chosen such that A and B consist of D-dimensional cubes of linear size R. Adjacent cubes in A or B overlap along $(D-2)$-dimensional faces. Accordingly, the region C is a union of all $(D-2)$-dimensional faces (with a thickness of order w) over all blocks in A and B. Note that $|C|\sim n/R^2$, so we arrive at Eq. (14). Repeating the same arguments as above shows that a cubic-shaped block $M\subseteq\Lambda$ is correctable if $|\partial M|<d$, that is, $R^{D-1}\sim d$. Substituting it into Eq. (14) leads to Eq. (4).

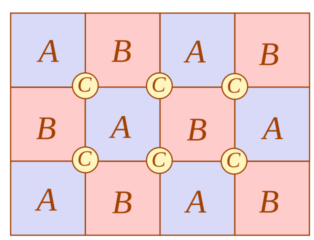

FIG. 1: The partition of the lattice $\Lambda = ABC$. Each individual block in A and B must be correctable. The region C provides separation between adjacent blocks in A and adjacent blocks in B. It guarantees that the entire regions A and B are correctable. The entropic error correction condition implies that $S(A|BC) = -S(A)$ and $S(B|AC) = -S(B)$ for the maximally mixed encoded state. It yields $k = S(ABC)\leq S(C)$.

In the rest of the paper we state and prove the Disentangling Lemma and another technical Lemma which have been used above.

Definition 1. *Let $M \subseteq \Lambda$ be any region. Define the external boundary $\partial_+ M$ as a set of all sites $u \in \bar{M}$ such that there is at least one projector Π_a acting on both u and M. Define the internal boundary as $\partial_- M = \partial_+ \bar{M}$. Finally, define $\partial M = \partial_- M \cup \partial_+ M$.*

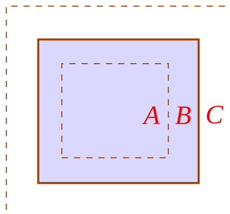

FIG. 2: Extending the correctability from a region AB to a larger region ABC. The Disentangling Lemma implies that any encoded state ρ can be represented as $\rho = U_{BC}(\eta_{AB} \otimes \eta_{CD})U_{BC}^\dagger$, where η_{AB} is a pure state independent of ρ. It implies $\mathrm{Tr}_C\, \eta_{CD} = \rho_D$ and thus $\eta_A \otimes \rho_D = \mathcal{E}(\rho)$, where $\mathcal{E}$ is an 'error' erasing the region BC. If BC is correctable, one must be able to reconstruct ρ starting from $\mathcal{E}(\rho)$. Since η_{AB} is known, it means that one can reconstruct ρ starting from ρ_D. Therefore ABC is correctable.

Lemma 1 (Disentangling). *Let $M \subseteq \Lambda$ be any correctable region. Suppose the external boundary $\partial_+ M$ is also a correctable region. Then there exists a unitary operator $U_{\partial M}$ acting only on the boundary ∂M such that*

$$U_{\partial M} \Pi U_{\partial M}^\dagger = |\phi_M\rangle\langle\phi_M| \otimes \Pi_{\bar{M}}. \tag{15}$$

for some pure state $|\phi_M\rangle$ and some projector $\Pi_{\bar{M}}$.

It follows from Eq. (15) that $U_{\partial M}$ disentangles any encoded state $|\psi\rangle \in \mathcal{C}$, that is, $U_{\partial M}|\psi\rangle = |\psi_{in}\rangle \otimes |\psi_{out}\rangle$ where $|\psi_{in}\rangle = |\phi_M\rangle$ is the same for all encoded states $|\psi\rangle$. In particular, any encoded state ρ obeys the entanglement area law, that is, $S(M) \le |\partial M|$ for any correctable region M. In the case of trivial codes ($k=0$) the codespace is one-dimensional and thus any region is correctable. It reproduces the entanglement area law proved for ground states of local Hamiltonians with commuting interactions in Ref. [20]. Note that the boundary ∂M_+ is correctable whenever the size of the boundary is smaller than the distance d. One can easily check that this is the case for all applications of the lemma used above.

Finally, it is worth mentioning that $\Pi_{\bar{M}}$ might not be representable as a product of geometrically local projectors because the unitary operator $U_{\partial M}$ might not be locality preserving. Similarly, the state $|\phi_M\rangle$ might lack a representation in terms of local commuting projectors.

The proof of the Disentangling Lemma is based on the following well-known result [21].

Proposition 1. *Consider a tripartite system ABC and let $\Pi = \Pi_{AB}\Pi_{BC} = \Pi_{BC}\Pi_{AB}$ be a product of two commuting projectors acting on AB and BC respectively. Then the Hilbert space of B can be decomposed as*

$$\mathcal{H}_B = \bigoplus_x \mathcal{H}_{B'_x} \otimes \mathcal{H}_{B''_x} \tag{16}$$

such that

$$\Pi = \bigoplus_x \Pi_{AB'_x} \otimes \Pi_{B''_x C} \tag{17}$$

for some projectors $\Pi_{AB'_x}$ and $\Pi_{B''_x C}$.

Note that some of the projectors in the above decomposition might be zero.

Proof of the Disentangling Lemma. Consider a partition $\Lambda = ABCD$, where

$$A = M \backslash \partial_- M, \quad B = \partial_- M, \quad C = \partial_+ M, \quad D = \bar{M} \backslash \partial_+ M.$$

By definition, $M = AB$ and $\bar{M} = CD$, see Fig. 2. Using Eq. (6) one can represent Π as a product of commuting projectors acting on MC and CD. Then Proposition 1 implies that the Hilbert space of C can be decomposed as

$$\mathcal{H}_C = \bigoplus_x \mathcal{H}_{C'_x} \otimes \mathcal{H}_{C''_x} \tag{18}$$

such that

$$\Pi = \bigoplus_x \Pi^{(x)}_{MC'_x} \otimes \Pi^{(x)}_{C''_x D}, \tag{19}$$

where $\Pi^{(x)}_{MC'_x}$ and $\Pi^{(x)}_{C''_x D}$ are projectors. Since C is correctable, the direct sum over x contains exactly one term — otherwise it would be possible to distinguish some orthogonal encoded states by measuring x which can be done locally in C, see Eq. (18). Thus one can subdivide C into two subsystems $C = C'C''$ such that

$$\Pi = U_C \left(\Pi_{MC'} \otimes \Pi_{C''D}\right) U_C^\dagger. \tag{20}$$

Using Eq. (6) again one can represent Π as a product of commuting projectors acting on AB and $B\bar{M}$. Applying the same arguments as above one arrives at

$$\Pi = U_B \left(\Pi_{AB'} \otimes \Pi_{B''\bar{M}}\right) U_B^\dagger \tag{21}$$

where $B = B'B''$ is a partition of B into two subsystems and $\Pi_{AB'}$, $\Pi_{B''\bar{M}}$ are some projectors. Define a new projector

$$\Pi' = U_B^\dagger U_C^\dagger \Pi U_B U_C. \tag{22}$$

Combining Eqs. (20,21) one concludes that Π' has a product structure with respect to the partition $(AB')(B''C')(C''D)$, that is,

$$\Pi' = \Pi_{AB'} \otimes \Theta_{B''C'} \otimes \Pi_{C''D} \tag{23}$$

for some projector $\Theta_{B''C'}$. The error correction condition Eq. (7) for M implies that $\Pi_{AB'}$ must be one-dimensional, since otherwise one would be able to find a pair of orthogonal codestates which can be distinguished by acting only on M. Thus

$$\Pi' = |\phi_{AB'}\rangle\langle\phi_{AB'}| \otimes \Theta_{B''C'} \otimes \Pi_{C''D} \tag{24}$$

for some pure state $|\phi_{AB'}\rangle$. As for the projector $\Theta_{B''C'}$, the error correction condition Eq. (7) for M and C (separately) implies that $\Theta_{B''C'}$ can be regarded as a codespace of an error correcting code that corrects all errors on B'' and all errors on C'. The no-cloning principle implies that $\Theta_{B''C'}$ must be one-dimensional, that is,

$$\Pi' = |\phi_{AB'}\rangle\langle\phi_{AB'}| \otimes |\phi_{B''C'}\rangle\langle\phi_{B''C'}| \otimes \Pi_{C''D} \tag{25}$$

for some pure state $|\phi_{B''C'}\rangle$. Thus the desired unitary operator $U_{\partial M}$ can be chosen as

$$U_{\partial M} = W_{B''C'} U_B^\dagger U_C^\dagger \tag{26}$$

where $W_{B''C'}$ is an arbitrary unitary operator disentangling the state $|\phi_{B''C'}\rangle$. □

Proof of Corollary 1. Applying the Disentangling Lemma to the region $M = AB$ we conclude that there exists a unitary operator U_{BC} and a pure state η_{AB} such that for any encoded state ρ one has

$$\rho = U_{BC}(\eta_{AB} \otimes \eta_{CD})U_{BC}^\dagger, \tag{27}$$

where η_{CD} is some (mixed) state depending on ρ. Taking the partial trace of Eq. (27) over ABC we conclude that $\mathrm{Tr}_C\, \eta_{CD} = \rho_D$. Therefore

$$\eta_A \otimes \rho_D = \mathcal{E}(\rho), \tag{28}$$

where we introduced an 'error' $\mathcal{E}$ that takes the partial trace over BC. If BC is correctable, there exists a recovery operation $\mathcal{R}$ such that $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$ for any encoded state ρ. Therefore

$$\rho = \mathcal{R}(\eta_A \otimes \rho_D). \tag{29}$$

Since η_A is a known state independent of ρ, it means that one can reconstruct ρ starting from ρ_D. Therefore ABC is a correctable region. □

Our final lemma asserts that the union of two correctable regions M_1 and M_2 that are sufficiently far apart is also correctable. Note that this statement would be obvious if the error correction would amount to the "syndrome measurement", that is, measuring eigenvalues of the constraints Π_a and guessing the error based on the measured syndrome. Indeed, an error acting on a region M_i creates non-trivial syndrome only in a small neighborhood of M_i, so the error corrections at M_1 and M_2 do not interfere with each other. Unfortunately, this intuition does not lead to a formal proof, so we need to use different arguments similar to the ones used in the proof of Lemma 1.

Lemma 2. *Let $M_1, M_2 \subseteq \Lambda$ be any correctable regions such that any projector Π_a overlaps with at most one of M_1, M_2. Suppose that $\partial_+ M_1$ is also correctable. Then the region $M_1 \cup M_2$ is correctable.*

Proof. It suffices to prove that

$$\Pi\, O_{M_1} \otimes O_{M_2}\, \Pi \sim \Pi \tag{30}$$

for any operators O_{M_1}, O_{M_2} acting on M_1, M_2 respectively. Indeed, since any projector Π_a overlaps with at most one of M_1, M_2 the regions $M_1 \cup \partial_+ M_1$ and M_2 are disjoint. Let us apply the decomposition described by Eqs. (22-25) to the region M_1. It yields

$$\Pi\, O_{M_1} \otimes O_{M_2}\, \Pi = f(O_{M_1})\, \Pi O_{M_2} \Pi, \tag{31}$$

where

$$f(O_{M_1}) = \langle\phi_{AB'} \otimes \phi_{B''C'}|O_{AB'B''}|\phi_{AB'} \otimes \phi_{B''C'}\rangle \tag{32}$$

and $O_{AB'B''} = U_B^\dagger\, O_{M_1} U_B$. Since M_2 is correctable, Eq. (31) implies Eq. (30). □

ACKNOWLEDGMENTS

We thank Frank Verstraete for useful discussions. Part of this work was done while the authors were visiting the Erwin Schrödinger International Institute for Mathematical Physics at Vienna. SB and BMT were partially supported by the DARPA QUEST program under contract number HR0011-09-C-0047. DP is supported in part by NSERC and FQRNT.

APPENDIX A

In this section we prove the bound Eq. (5) for 2D classical codes and demonstrate that this bound might be tight by inspecting properties of 2D classical codes associated with 1D cellular automatons.

In the classical case each site of the lattice $u \in \Lambda$ is occupied by a classical variable x_u that can take a constant number of values. The codespace $\mathcal{C}$ is a set of all assignments $x = \{x_u\}_{u \in \Lambda}$ that obey geometrically local constraints $\Pi_1(x) = 1, \ldots, \Pi_m(x) = 1$. A code encodes k bits with the distance d iff $|\mathcal{C}| = 2^k$ and any pair of distinct codewords differ at d or more sites. Consider a partition $\Lambda = AB$, where $B = B_1 \ldots B_m$ consists of square-shaped blocks of size roughly $\sqrt{d} \times \sqrt{d}$ such that the number of sites in any block B_i is smaller than d, see Fig. 3. We assume that the separation between the blocks in B is of order w, so that any constraint Π_a overlaps with at most one block B_i. Let $x, y \in \mathcal{C}$ be any pair of codewords such that $x|_A = y|_A$. We claim that $x = y$. Indeed, suppose x and y differ at some block B_i. Then there exists a codeword $z \in \mathcal{C}$ that coincides with x inside B_i and coincides with y in the complement of B_i. It means that z and y are distinct codewords that differ at less than d sites which is a contradiction.

Let ρ be the uniform distribution on $\mathcal{C}$. We have $S(B|A) = 0$ since there is a unique way to extend a codeword from A to B. Therefore

$$k = S(\rho) = S(A) + S(B|A) = S(A) \le |A| \sim \frac{n}{d^{1/2}}.$$

It proves Eq. (5).

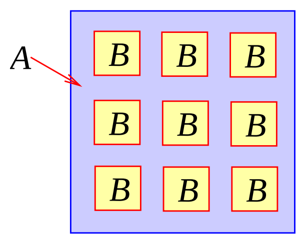

FIG. 3: The partition $\Lambda = AB$.

In the rest of the section we describe a family of 2D linear codes associated with 1D cellular automatons (CA) that are quite close to saturating the bound Eq. (5). To the best of our knowledge the idea of CA-based codes was originally introduced in Ref. [22]. A very similar construction has also been used in Ref. [23] as an exactly solvable model of a 2D spin glass.

Let us start from considering a semi-infinite lattice $\Lambda = \mathbb{Z} \times [0, L-1]$. Let $x_i^t \in \{0,1\}$ be a classical bit living at a site $(i,t) \in \Lambda$. We shall refer to the coordinates i and t as *space* and *time* respectively. Let $\{0,1\}^\Lambda$ be the set of all bit assignments $\{x_i^t\}_{(i,t)\in\Lambda}$ with a finite Hamming weight. Define a code

$$\begin{aligned} \mathcal{C}_\infty^L &= \{x \in \{0,1\}^\Lambda \, : \, x_i^{t+1} = x_{i-1}^t \oplus x_{i+1}^t \\ &\quad \forall i \in \mathbb{Z}, \quad \forall t \in [0, L-2]\} \end{aligned} \tag{33}$$

Note that all constraints are linear and involve a triple of bits located close to each other. Clearly there is a one-to-one correspondence between the codewords of $\mathcal{C}_\infty^L$ and computational histories of a 1D linear cellular automaton (CA) with transition rules $x_i \to x_{i-1} \oplus x_{i+1}$. Accordingly, any codeword $x \in \mathcal{C}_\infty^L$ is uniquely determined by the restriction of x onto the first row of the lattice which determines the initial conditions for the CA at $t=0$. It means that the code $\mathcal{C}_\infty^L$ has 1 encoded bit per unit of length along the space axis. Since the code $\mathcal{C}_\infty^L$ is linear, its distance d is just the minimum Hamming weight of a non-zero codeword $x \in \mathcal{C}_\infty^L$.

Lemma 3. *Let $d(p)$ be the distance of the code $\mathcal{C}_\infty^L$ defined on a lattice of height L, where $L = 2^p$ for some integer p. Then $d(p) = 3^p$.*

Proof. Clearly $\mathcal{C}_\infty^L$ consists of two independent codes defined on the even and odd sublattices of Λ. Let Λ_0 be the even sublattice, i.e., a set of all sites $(i,t) \in \Lambda$ such that $i+t$ is even. It suffices to bound the distance of the code $\mathcal{C}_\infty^L$ restricted to Λ_0. Consider a partition $\Lambda_0 = ABCD$ where

$$\begin{aligned} A &= \{(i,t) \, : \, i+t = 0 \bmod 4, \quad t = 0 \bmod 2\} \\ B &= \{(i,t) \, : \, i+t = 2 \bmod 4, \quad t = 0 \bmod 2\} \\ C &= \{(i,t) \, : \, i+t = 0 \bmod 4, \quad t = 1 \bmod 2\} \\ D &= \{(i,t) \, : \, i+t = 2 \bmod 4, \quad t = 1 \bmod 2\} \end{aligned}$$

Note that each of the above sublattices is isomorphic to the original lattice Λ_0 of height 2^{p-1}. Using the transition rules $x_i^{t+1} = x_{i-1}^t \oplus x_{i+1}^t$ one easily gets $x_i^{t+2} = x_{i-2}^t \oplus x_{i+2}^t$, that is, the code $\mathcal{C}_\infty^L$ reproduces itself on each of the sublattices A, B, C, D. We conclude that

$$d(p) \ge \Gamma \, d(p-1) \tag{34}$$

where Γ is the minimum number of sublattices A, B, C, D that can be occupied by a non-zero codeword. Simple combinatorial analysis shows that $\Gamma \ge 3$, that is, $d(p) \ge 3^p$.

To get the matching upper bound on $d(p)$ consider a codeword $x \in \mathcal{C}_\infty^L$ generated starting from a state with a single active cell, i.e., a codeword corresponding to the initial conditions $x_i^0 = \delta_{i,1}$. One can easily check that the support of x is the Sierpinski triangle fractal which has Hamming weight 3^p. Thus $d(p) = 3^p$. □

Consider now a finite lattice $\Lambda = \mathbb{Z}_L \times [0, L-1]$ with periodic boundary conditions along the space axis and open boundary conditions along the time axis. Define a finite version of the code $\mathcal{C}_\infty^L$ by the constraints

$$x_i^{t+1} = x_{i-1}^t \oplus x_{i+1}^t, \quad x_0^0 = 0, \tag{35}$$

which must hold for all $i \in \mathbb{Z}_L$ and for all $t \in [0, L-2]$. Let us denote the corresponding code $\mathcal{C}_L^L$. We shall restrict ourselves only to odd values of L. One can easily check that for odd L the transition rule $x_i \to x_{i-1} \oplus x_{i+1}$ is essentially reversible: a pair of distinct initial states $\{x_i^0\}_{i\in\mathbb{Z}_L}$ and $\{y_i^0\}_{i\in\mathbb{Z}_L}$ can evolve into the same state after a finite number of steps iff $x_i^0 = y_i^0 \oplus 1$ for all $i \in \mathbb{Z}_L$. The additional constraint $x_0^0 = 0$ thus guarantees that distinct codewords of $\mathcal{C}_L^L$ have distinct restrictions on every time slice of the lattice. By construction, the modified code $\mathcal{C}_L^L$ encodes $k = L-1$ bits into $n = L^2$ bits. We have computed the distance d of the code $\mathcal{C}_L^L$ numerically using the exhaustive search optimization for odd values of L in the interval $5 \le L \le 23$, see Fig. 4. It was checked that for all considered values of L one has $d = d'$, where d' is the Hamming weight of a codeword generated starting from a state with a single active cell, that is, with the initial conditions $x_i^0 = \delta_{i,1}$. Since we have also shown that $d = d'$ for the semi-infinite lattice, see the proof of Lemma 3, it is natural to conjecture that $d = d'$ for all odd values of L. Computing d' numerically for lattice sizes up to $L \sim 10^4$ we have found $d' \sim L^{1.584}$ which agrees perfectly with the scaling

$$d \sim L^{\log_2 3} \approx L^{1.585} \approx n^{0.793} \qquad (36)$$

that was derived in Lemma 3 for the semi-infinite lattice. Summarizing, the code $\mathcal{C}_L^L$ encodes $k = \sqrt{n} - 1$ bits into n bits with the distance $d \approx n^{0.793}$. Note that $k\sqrt{d} \sim n^{0.897}$ which is quite close to saturating the bound Eq. (5).

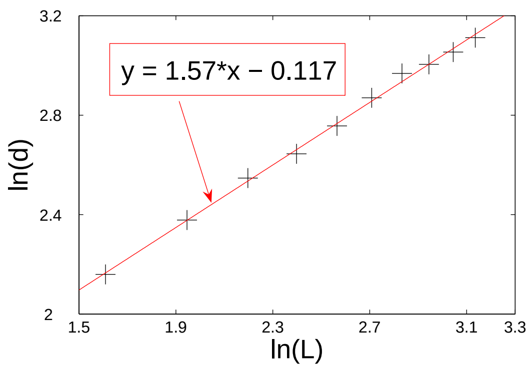

FIG. 4: The distance of the code $\mathcal{C}_L^L$ defined on a lattice $\mathbb{Z}_L \times [0, L-1]$ computed numerically using the exhaustive search for $L = 5, 7, \ldots, 23$.

[1] R. Landauer, Nature **335**, 779 (1988).
[2] C. H. Bennett and R. Landauer, Scientific American **253**, 48 (1985).
[3] S. Lloyd, Nature **406**, 1047 (2000).
[4] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] S. Bravyi and A. Kitaev, *Quantum codes on a lattice with boundary*, arXiv:quant-ph/9811052.
[6] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1995), http://arxiv.org/abs/quant-ph/9512032.
[7] S. Bravyi and B. Terhal, New J. Phys. **11**, 043029 (2009).
[8] M. A. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[9] R. Koenig, B. Reichardt, and G. Vidal, Phys. Rev. B **79**, 195123 (2009).
[10] A. Kitaev, Annals Phys. **303**, 2 (2003).
[11] A. Kitaev, private communication (2009).
[12] G. Zemor, in *Coding and Cryptography, Lect. Notes in Computer Science Vol. 5557* (Springer-Verlang, Berlin, Germany, 2009), pp. 259–273, http://www.math.u-bordeaux.fr/~zemor/surface.pdf.
[13] H. Bombin and M. A. Martin-Delgado, Physical Review A **73**, 062303 (2006), URL doi:10.1103/PhysRevA.73.062303.
[14] M. Freedman, D. Meyer, and F. Luo, in *Mathematics of Computation* (Chapman & Hall/CRC, Boca Raton, FL, 2002), pp. 287–320, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA414975&Location=U2&doc=GetTRDoc.pdf.
[15] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).
[16] D. Bacon, Phys. Rev. A **73**, 012340 (2006).
[17] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[18] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Comm. Math. Phys. **246**, 359 (2004).
[19] A. Uhlmann, Comm. Math. Phys. **54**, 21 (1977).
[20] M. Wolf, F. Verstraete, M. Hastings, and J. I. Cirac, Phys. Rev. Lett. **100**, 070502 (2008).
[21] S. Bravyi and M. Vyalyi, Quantum Inf. and Comp. **5**, 187 (2005).
[22] D. Roy Chowdhury, S. Basu, I. Sen Gupta, and P. Pal Chaudhuri, IEEE Trans. Comput. **43**, 759 (1994).
[23] M. E. J. Newman and C. Moore, Phys. Rev. E **60**, 5068 (1999).
[24] The commutativity of the constraints specifying a code is a highly desirable property since it allows one to use error correction algorithms based on the syndrom measurement.
[25] Recall that a code has distance d iff any measurement performed on any subset of less than d particles reveals no information about an encoded state. Such a code protects encoded information against $\lfloor (d-1)/2 \rfloor$ single-particle errors in the worst-case scenario.
[26] Note that a 2D surface code defined on a lattice with two smooth and two rough boundary regions encodes one qubit into approximately d^2 physical qubits, see [5]. In order to encode k qubits one can use k independent copies of the surface code placed next to each other on a plane. It requires roughly kd^2 physical qubits.
[27] More strictly, our analysis applies to the regular D-dimensional cubic lattice with open or periodic boundary conditions.