Homological error correction: Classical and quantum codes

H. Bombin, and M. A. Martin-Delgado

Citation: Journal of Mathematical Physics **48**, 052105 (2007); doi: 10.1063/1.2731356
View online: https://doi.org/10.1063/1.2731356
View Table of Contents: http://aip.scitation.org/toc/jmp/48/5
Published by the American Institute of Physics

Articles you may be interested in

Topological quantum memory
Journal of Mathematical Physics **43**, 4452 (2002); 10.1063/1.1499754

Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds
Journal of Mathematical Physics **55**, 082202 (2014); 10.1063/1.4891487

Topological quantum codes on compact surfaces with genus $g \geq 2$
Journal of Mathematical Physics **50**, 023513 (2009); 10.1063/1.3081056

Topological quantum order: Stability under local perturbations
Journal of Mathematical Physics **51**, 093512 (2010); 10.1063/1.3490195

JOURNAL OF MATHEMATICAL PHYSICS **48**, 052105 (2007)

Homological error correction: Classical and quantum codes

H. Bombin and M. A. Martin-Delgado[a)]
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain

(Received 13 February 2007; accepted 27 March 2007; published online 21 May 2007)

We prove several theorems characterizing the existence of homological error correction codes both classically and quantumly. Not every classical code is homological, but we find a family of classical homological codes saturating the Hamming bound. In the quantum case, we show that for nonorientable surfaces it is impossible to construct homological codes based on qudits of dimension $D>2$, while for orientable surfaces with boundaries it is possible to construct them for arbitrary dimension D. We give a method to obtain planar homological codes based on the construction of quantum codes on compact surfaces without boundaries. We show how the original Shor's 9-qubit code can be visualized as a homological quantum code. We study the problem of constructing quantum codes with optimal encoding rate. In the particular case of toric codes we construct an optimal family and give an explicit proof of its optimality. For homological quantum codes on surfaces of arbitrary genus we also construct a family of codes asymptotically attaining the maximum possible encoding rate. We provide the tools of homology group theory for graphs embedded on surfaces in a self-contained manner. © *2007 American Institute of Physics.* [DOI: 10.1063/1.2731356]

I. INTRODUCTION

Quantum error correction (QEC) is an important breakthrough in the theory of quantum information and computation. Without this technique, quantum communication over noisy channels would be doom to failure and quantum computation would remain in the realm of sheer ideal theoretical constructs: powerful in principle, but without any chance of being implemented in practice.

It was Landauer[1–3] who soon prompted the quantum information community to look seriously at the problem of quantum errors since they are more harmful than classical errors and Unruh pointed out the severe negative effects of decoherence.[4] In fact, quantum errors may show up from different sources: (i) decoherence due to undesired coupling of the quantum data with the surrounding environment; and (ii) imperfections in quantum logic gates during the execution of an algorithm.

The problem of correcting quantum errors seemed likely impossible in the beginning, since the classical error correcting techniques based on redundancy or repetition codes seemed to contradict the quantum no-cloning theorem. Moreover, besides bit-flip errors, there are phase errors with no classical counterpart and thus no previous theory to compare with.

Fortunately, all these doubts were dispelled by the first QEC code proposed by Shor[5] and independently by Steane[6] who showed how to get around these difficulties explicitly. Soon, more general quantum codes were constructed known as CSS codes[7,8] based on classical correcting codes. These codes are very easy to deal with since the correction of bit-flip errors is factorized out from the correction of phase-flip errors. CSS codes have found very important applications in the security proof of quantum cryptography protocols without resorting to quantum computers.[9]

[a)]Electronic mail: mardel@miranda.fis.ucm-es

 © 2007 American Institute of Physics

A more general class of codes, encompassing the CSS codes, are the stabilizer codes introduced by Gottesman.[10] In the stabilizer formalism, the construction of quantum codes can be thought of as a task in finite group theory for finding Abelian subgroups of the Pauli group, leaving invariant a certain subspace which used to encode quantum words. An alternative and independent realization was provided by Calderbank *et al.*[11] using the theory of binary vector spaces.

Despite having a general theory of QEC, explicit realization of quantum codes is also important in practical implementations. In this regard, the number of encoded qubits k, or logical qubits, with respect to the number of physical qubits $n>k$ plays an important role. The first codes discovered by Shor and Steane have a ratio of 1:9 and 1:7, respectively. It is possible to show that the best possible ratio for correcting one single error is 1:5.[12,13]

The quantum codes mentioned thus far are linear, also called additive, codes since the underlying structure is that of Abelian stabilizer codes. There are also a series of interesting extensions to nonstabilizer codes[14,15] with the aim of increasing the coding capabilities of quantum codes. For instance, a type of nonadditive codes encodes six states in five qubits and can correct the erasure of any single qubit.[16] A particularly interesting proposal for non-Abelian quantum codes is due to Ruskai[17] based on correcting (2-qubit) Pauli exchange errors besides all single qubit errors. This technique can be generalized to non-Abelian stabilizer groups based on the permutation group S_n.[18]

An alternative approach to QEC was introduced by Kitaev[19] known as topological quantum codes. The notion of topological quantum computation was also addressed independently by Freedman.[20] This technique allows us to devise topological quantum memories which are robust against local errors and capable of protecting stored quantum data.[21,22]

To understand the notion of a topological code, we first notice that a basic strategy in standard QEC is to protect logical qubits by spreading them out in a larger set of physical qubits ($n>k$). This is the reminiscent of redundancy in classical codes. In topological quantum codes, we go even farther and encode quantum words in the nonlocal degrees of freedom of topologically ordered physical systems, such as certain lattice gauge theories,[19,23–25] or condensed matter systems.[26–31] Detecting topologial order is an important issue in this regard.[32,33]

Due to this nonlocal encoding, these quantum code words are intrinsically resistant to the debilitating effects of noise, as long as it remains local. This construction is rather appealing since it relies on an intrinsic physical mechanism for the topological system to self-correcting local errors. It means that in a topological code, we do not have to check and fix quantum errors from outside the system whenever they appear like in standard (nontopological) quantum codes. It is the physical properties of the system which provide the intrinsic mechanism from protecting the encoded quantum states. This mechanism is controlled by the interactions described by Hamiltonians on certain lattices embedded in surfaces with nontrivial topology. The ground states of those Hamiltonians exhibit topological order, a type of degeneracy that is robust against local perturbations since it is protected by a gap from the rest of the spectrum and, moreover, the degeneracy depends on the topology of the lattice Hamiltonian. Due to this topological order, these states exhibit remarkable entanglement properties.[34,35]

In addition to being self-correcting, topological quantum codes exhibit more interesting properties: (i) they belong to the class of stabilizer codes, and (ii) the interaction terms in the Hamiltonian realizing these codes are local, i.e., nearest-neighbor interactions. The locality of property (ii) is very important since it facilitates the potential physical implementation of these lattice systems. In contrast, the stabilizer operators in nontopological codes are generically nonlocal.

There is another method for QEC known as decoherence free subspaces (DFSs).[36–38] In this method, quantum information is protected by using symmetry. The symmetry that protects quantum information exists naturally in the interaction of the quantum information processing system with its environment. There is a unified view of QEC strategies in which both DFSs and topological codes are instances of the algebraic notion of noiseless subsystem.[39] Kribs *et al.*[40] provided a further unification of quantum error methods by introducing the notion of operator QEC. This scheme relies on a generalized notion of noiseless subsystems that is not restricted to the commutant of the interaction algebra. Therefore, these considerations make topological quantum codes

rather interesting to study since they belong to the class of stabilizer codes and share the basic properties of quantum noiseless subsystems such as DFSs, while giving us the opportunity to have a more robust decoherence protection based on the topological properties of certain quantum systems.

Practical implementations of topological quantum codes have been proposed using optical lattices[41–43] simulating spin interactions in honeycomb lattices.[26] In this paper we shall consider only two-dimensional realizations of topological codes, but it is possible to make extensions to lattices in $3+1$ dimensions.[21,44,45]

The issue of topological quantum computation,[19,46–49] as an instance of fault-tolerance quantum computing[50–56] is closely related to quantum codes. However, this work concentrates only on topological quantum codes.

In this work we use the terminology of homological codes, both classically and quantumly, to highlight the fact that they are constructed solely on the information about the graph encoded in its homology groups, either as simple graphs or as graphs embedded on surfaces.

The paper is intended to be self-contained and is organized as follows: in Sec. II, we introduce the basic notions and definitions of classical codes and homology groups over $\mathbf{Z}_2$ for graphs. With these tools, we then proof Theorem 2 that allows us to construct classical homological codes. Not every classical code is homological, but there exists optimal families of homological codes that saturate the classical Hamming bound. In Sec. III we start recalling the definitions and characterizations of quantum codes, then we construct symplectic codes for qudits, i.e., quantum states of arbitrary dimension D. The idea is to apply the symplectic group $ESp_D(n)$ to a trivial code $\mathcal{C}_T(n,k)$ of distance 1. Symplectic codes are equivalent to stabilizer codes. We also introduce homology of 2-complexes, which are two dimensional generalizations of a graph or 1-complex. With these tools we go on to prove Theorem 4 for constructing qudit symplectic codes based on the homology and cohomology groups of graphs embedded in surfaces. Technically, these graph embeddings are called surface 2-complexes that are also introduced earlier. In particular, the celebrated Shor's original 9-qubit code can be thought of as a homological quantum code belonging to a family of codes $[[d^2,1,d]]$, with $d=3$ (see Fig. 20). Another topological realization exists for the Shor code on the projective plane.[58] In general, homological quantum codes can be degenerate codes. Next we prove a number of important results: as follows.

(i) The subgroup $\mathbf{Z}_2$ appearing in the first homology group of nonorientable surfaces is called the torsion subgroup. It plays an important role in the construction of homological quantum error correcting codes for qudits of dimension greater than 2. We show that it is impossible to construct these codes with $D>2$ on nonorientable surfaces, while it is possible to do so for codes based on qubits. For orientable surfaces with boundaries, it is possible to have homological codes of arbitrary dimension D.

(ii) We introduce the notion of topological subadditivity which is very helpful to find bounds on the efficiency (coding rates) of homological quantum codes.

(iii) For homological quantum codes on the torus, we find a family of optimal codes that outperform the original toric codes introduced in Ref. 19 and in addition, our optimal codes are extended for qudits.

(iv) We construct an explicit family of quantum homological codes for which we can show that the rate k/n of logical qubits to physical qubits approaches unity using topological graphs embedded on surfaces of arbitrary genus.

(v) It is possible to transform homological codes on compact surfaces of arbitrary genus, such as the g-torus, into homological codes embedded into planar surfaces with boundaries; this is interesting for practical purposes since constructing real torus of higher genus does not seem to be feasible.

The results concerning the quantum encoding rate were advanced without proof[57] in the particular case of qubits ($D=2$).

Section. IV is devoted to conclusions. In Appendix A we construct the generators of the sympletic group $Sp_D(n)$ for the general case of qudits, in Appendix B we give a detailed explicit

proof of the subadditivity property of quantum topological codes, and in Appendix C we prove that our homological quantum codes for qudits on the torus are optimal as far as the coding rate k/n is concern.

II. HOMOLOGICAL CODES FOR CLASSICAL ERROR CORRECTION

A. Classical error correcting codes

Classical error correction deals with the problem of transmitting messages through noisy channels.[59,60] Usually messages are composed with bits, which can take on the values 0 or 1. Such strings of bits, or *words*, can be regarded as vectors over the field $\mathbf{Z}_2$. The same idea holds for the errors introduced in a Communication, for if u and v are, respectively, the input and output words, we say that the channel has produced the error

$$e := v - u. \tag{1}$$

An important channel is the *(binary) symmetric channel*. This channel acts on each bit individually, flipping its value with certain probability $1-p$, $p>\frac{1}{2}$. Due to the symmetry between 0 and 1, it is possible to assign a probability to any given error e, since it does not depend on the input u. We introduce the *weight* of a vector $u \in \mathbf{Z}_2$, written $\mathrm{wt}(u)$, as the number of nonzero components of u. With this definition, for the symmetric channel we have that the probability for a given error e to occur is $(1-p)^{\mathrm{wt}(e)}$. Thus, errors with small weight are more probable, which is important since there is no chance to correct an arbitrary error. For words u of increasing length n, we expect $\mathrm{wt}(e) \simeq np$. If we were able to correct up to np errors, we would have a successful communication with a good probability.

Given a set of errors S, we say that two words u and v are *distinguishable* with respect to S if and only if (iff)

$$\forall e,e' \in Su + e \neq v + e'. \tag{2}$$

An *error correcting code* of length n is a subset C of $\mathbf{Z}_2^n$. Its elements are called *code words*. If $|C|=2^k$, we say that C encodes k bits. C corrects S if every pair of code words in C is distinguishable with respect to S. Let $S(t)$ consist of errors with $\mathrm{wt}(e) \leqslant t$. If C corrects $S(t)$ but not $S(t+1)$, we say that C is a *t-error correcting code*. In order to characterize this property, let us introduce the *distance* between the words u and v as $d(u,v) := \mathrm{wt}(u-v)$. Since $u+e=v+e'$ implies $d(u-v)=d(e'-e)>d(e')+d(e')$, we have that two vectors with distance d are distinguishable with respect to $S(t)$ iff $d>2t$. The distance of a code is the minimum distance between any of its code words, and C is a t-error correcting code iff $d>2t$. A code of length n, distance d, and encoding k bits is usually denoted by $[n,k,d]$.

Clearly, the values of n, k, and d cannot be arbitrary for an $[n,k,d]$ code to exist. In fact, consider a t-error correcting code C of length n and $|C|=m$. Let $S_n(t)$ contain the elements of $S(t)$ of length n. Since $|S_n(t)|=\Sigma_{i=0}^{t}\binom{n}{i}$ and $u+S_n(t) \cap v+S_n(t)=\emptyset$ for any pair of code words, we have the (upper) *Hamming bound*

$$m\sum_{i=0}^{t}\binom{n}{i} \leqslant 2^n. \tag{3}$$

Setting $m=2^k$ and taking the limit of large n, k, t,

$$\frac{k}{n} < \left(1 - H\left(\frac{t}{n}\right)\right)(1-\eta), \tag{4}$$

where $\eta \to 0$ as $n \to \infty$ and $H(x)$ is the entropy function

$$H(x) := -x\log_2 x - (1-x)\log_2(1-x). \tag{5}$$

k/n is called the *rate* of the code. A question that naturally arises here is whether this bound can

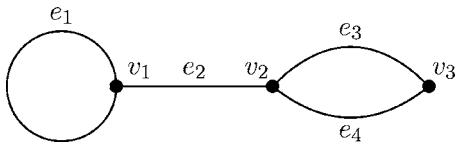

FIG. 1. A nonsimplicial graph with a self-loop e_1 and double edges e_3 and e_4.

be reached. A theorem by Shannon[61] states that this is asymptotically true, but the codes involved in the proof need not be of any practical use. For linear codes, a class of codes which we shall introduce below, there is also a lower bound known as the Gilbert-Varshamov bound: there exists a linear $[n,k,d]$ code provided

$$2^k \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n. \tag{6}$$

Again, in the limit of large numbers this becomes

$$\frac{k}{n} > \left(1 - H\left(\frac{2t}{n}\right)\right)(1-\eta), \tag{7}$$

where $\eta \to 0$ as $n \to \infty$.

We now focus on *linear codes*, which have certain properties that make them more convenient to use. A linear $[n,k,d]$ code is a subspace C of $\mathbf{Z}_2^n$ of dimension k for which $\min_{u \in C-\{0\}} \mathrm{wt}(u) = d$. The value for the distance follows from the fact that C is closed under substraction. A *generator matrix* G of C is any matrix with rows giving a basis for C. A *parity check matrix* H for C is any matrix with rows giving a basis for $C^\perp$, the subspace of vectors orthogonal to any vector in C. From this point on, vectors are column vectors. To understand why H is useful, first note that $Hu=0 \Leftrightarrow u \in C$. Thus, for any error e and code words u, v we have $H(u+e)=H(v+e)=He$, that is, H measures the error independently of the code word. He is called the error syndrome, and it gives enough information to distinguish among correctable errors. If this were not true, then we would have a pair of correctable errors such that $H(e-e')=0 \Rightarrow e-e' \in C$, a contradiction since $\mathrm{wt}(e-e') < \mathrm{wt}(e)+\mathrm{wt}(e') \leqslant 2t < d$. The real usefulness of linear codes comes from the fact that many codes can be constructed in such a way that the deduction of the error from the syndrome is a fast operation. As an easy example (due to Hamming), consider the following check matrix for a [7,4,3] code

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{8}$$

Notice that columns are the binary representation of numbers from one to seven, and thus in this case the error syndrome gives the position of the (single) error.

B. Homology of graphs

A *graph*, intuitively, is a collection of *vertices* and *edges*. Each edge connects two (non-necessarily distinct) vertices. Figure 1 shows how a graph can be depicted as a collection of points or nodes (vertices) linked by curves (edges). In such a representation, any intersection of edges at points which are not vertices is meaningless. The idea of a graph can be formalized in several ways. We take here a combinatorial approach, rather than topological, and we do not introduce any orientation for the edges.

A (finite) graph $\Gamma=(V,E,I)$ [or, if needed, $(V_\Gamma, E_\Gamma, I_\Gamma)$] consists of a finite set E of edges, a finite set V of vertices, and an incidence function $I: E \to \mathcal{P}(V)$ such that

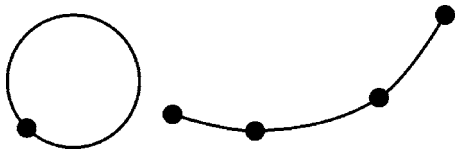

FIG. 2. The cycle C_1 and the path P_4.

$$1 \leqslant |I(e)| \leqslant 2, \quad \forall\, e \in E. \tag{9}$$

As usual, $\mathcal{P}(V)$ denotes the power set of V, that is, the set of subsets of V. The condition over I reflects the fact that an edge can only have one or two end points (in the former case, it is a *self-loop*). It is possible to arrange the information conveyed by I in a so-called *incidence matrix*. To this end, denote $V \coloneqq \{v_i\}_{i=1}^{|V|}$ and $E \coloneqq \{e_j\}_{j=1}^{|E|}$. The incidence matrix has $|V|$ rows and $|E|$ columns. The entry in row i and column j is 0 if $v_i \notin I(e_j)$, and $3-|I(e_j)|$ if $v_i \in I(e_j)$. The incidence matrix for the graph in Fig. 1 has incidence matrix

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \tag{10}$$

Whenever I is not injective we say that Γ has *multiple edges*. For example, edges e_3 and e_4 in Fig. 1 are multiple. A graph is called *simplicial* if it has no self-loops nor multiple edges. Note that this is the same as saying that the entries of the incidence matrix are 0 or 1 and there are no identical columns.

Two important families of graphs are the n-paths P_n and the n-cycles C_n ($n \in \mathbf{N}$). Formally, P_n can be defined by setting $V=1,\ldots,n$, $E=1,\ldots,n-1$, and $I(x)=\{x,x+1\}$. For C_n, set $V=E=\mathbf{Z}_n$ with the same description for I. In plain words, n paths are the combinatorial analog of a closed line segment, while n cycles are the counterpart of a circle. Pictorically, examples are shown in Fig. 2.

Let γ and Γ be graphs. γ is called a *subgraph* of Γ, denoted $\gamma \subseteq \Gamma$, if V_γ, E_γ, and I_γ are subsets, respectively, of V_Γ, E_Γ, and I_Γ. We say that two graphs Γ and Γ' are *isomorphic*, denoted $\Gamma \simeq \Gamma'$ if there exist two functions $\mu: V_\Gamma \to V_{\Gamma'}$ and $\nu: E_\Gamma \to E_{\Gamma'}$ which are one to one and onto and such that

$$I_{\Gamma'}(\nu(e)) = \{\mu(v) | v \in I_\Gamma(e)\}. \tag{11}$$

Figure 3 shows some examples of subgraphs.

A graph isomorphic to some P_n is a path, and a graph isomorphic to some C_n is a cycle. The *valence* of a vertex is the sum of the entries in its row in the incidence matrix. A path P has one or two distinguished vertices with valence distinct of 2. We shall call them the *end points* of P. Two vertices u and v of a graph Γ are said to be *connected* if there exists a path $P \subseteq \Gamma$ such that the end points of P are u and v. This defines an equivalence relation in V. The equivalence classes are called the *components* of Γ. A graph with a single component is said to be a connected graph.

A *tree* is a connected graph with no (sub)cycles. That is, a tree is a graph such that for any two vertices there exists exactly one path connecting them. Every tree which is not a point contains at

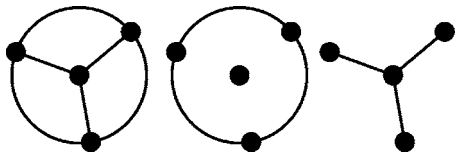

FIG. 3. The complete graph K_4 and 2 subgraphs, the second one a maximal subtree.

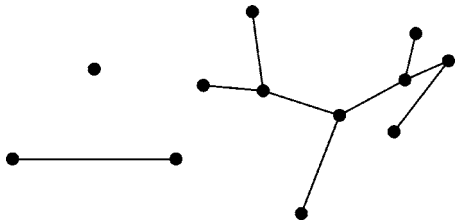

FIG. 4. Three trees with one, two, and nine vertices.

least two vertices of valence 1. Some examples of trees are shown in Fig. 4. A *maximal subtree* of a connected graph Γ is any tree $T \subseteq \Gamma$ such that $V_T = V_\Gamma$. Equivalently, a maximal subtree of Γ is any tree T such that $T \subset \Gamma' \subseteq \Gamma$ implies that Γ' is not a tree. Thus, there exists a maximal subtree for every connected graph. Moreover, given a tree $T \subseteq \Gamma$, there exists a maximal tree T' such that $T \subseteq T' \subseteq \Gamma$.

The *Euler characteristic* of a graph Γ, denoted $\chi(\Gamma)$, is defined by the formula

$$\chi(\Gamma) := |V_\Gamma| - |E_\Gamma|. \tag{12}$$

For any tree T, $\chi(T)=1$ (this can be proved by induction on $|V_T|$). Thus, if T is any maximal subtree of Γ, then $(|E_\Gamma - E_T|) = 1 - \chi(\Gamma)$. For each $e \in E_\Gamma - E_T$ we define $C_\Gamma(T,e)$ as the unique cycle of the graph $T+e$ (with the natural definition) $T+e := (V_T, E_T \cup \{e\}, I_T \cup \{(e, I_\Gamma(e))\})$. The interest of these cycles is that they form a maximal set of independent cycles, in a sense that will be made clear below. Meanwhile, Fig. 5 shows an example.

We now introduce the concept of the first homology group of a graph Γ. To this end, we start by defining 0-chains and 1-chains. Given a graph $\Gamma = (V, E, I)$, a 0-chain is a formal sum of vertices with coefficients in $\mathbf{Z}_2$,

$$\sum_{v \in V} \lambda_v v, \quad \lambda_v \in \mathbf{Z}_2. \tag{13}$$

The sum of two chains is defined in a term by term fashion

$$\sum_{v \in V} \lambda_v v + \sum_{v \in V} \lambda'_v v = \sum_{v \in V} (\lambda_v + \lambda'_v) v. \tag{14}$$

We adopt the convention that terms with zero coefficient are not written. The special element with all the coefficients equal to zero is denoted 0. Let $C_0(\Gamma)$ be de set of 0-chains of Γ; then $(C_0(\Gamma), +, 0)$ is an Abelian group isomorphic to $\mathbf{Z}_2^{|V|}$. Note that there is a natural inclusion of V in C_0 giving a basis. The definition of the space of 1-chains $C_1(\Gamma)$ runs along similar lines: just substitute V with E.

Next, we introduce a homomorphism, the boundary operator $\partial: C_1(\Gamma) \to C_0(\Gamma)$. It is enough to define its value over a set of generators,

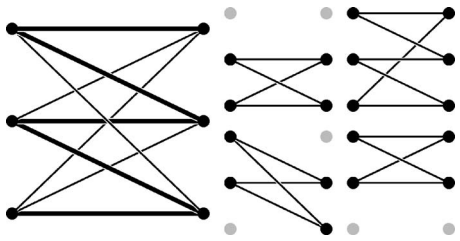

FIG. 5. The complete bipartite graph $K_{3,3}$ with a maximal subtree (thick line), and the corresponding generating set of cycles.

$$\partial(e) = \begin{cases} v_1 + v_2 & \text{if } I(e) = \{v_1, v_2\} \\ 0 & \text{if } I(e) = \{v_1\}. \end{cases} \tag{15}$$

It is possible to map naturally subgraphs onto chains; let $c_\gamma := \Sigma_{e \in E_\gamma} e$, where $\gamma \subseteq \Gamma$. Under this identification, the boundary of a path with more than one vertex are its end points, and the boundary of any cycle is 0.

The first homology group of a graph Γ is

$$H_1(\Gamma) := \ker \partial. \tag{16}$$

Its elements are always called cycles, but they do not necessarily correspond to cycles in the previous sense. To avoid confusion, we call the graphs isomorphic to some C_n simple cycles. We need a description of H_1.

Proposition 1: *Let Γ be a connected graph. Then $H_1(\Gamma) \simeq \mathbf{Z}_2^{1-\chi(\Gamma)}$. If T is a maximal subtree of Γ then the set $\{c_{C_\Gamma(T,e)} | e \in E_\Gamma - E_T\}$ forms a basis for $H_1(\Gamma)$. Moreover, if $c_1 \in H_1(\Gamma)$ has coefficients λ_e on this set of edges, then*

$$c_1 = \sum_{e \in E_\Gamma - E_T} \lambda_e c_{C_\Gamma(T,e)}. \tag{17}$$

If Γ is composed of several components Γ_i we have

$$H_1(\Gamma) \simeq \oplus_i H_1(\Gamma_i). \tag{18}$$

Let $C^0(\Gamma)$ denote the dual space of $C_0(\Gamma)$, that is, the space of homomorphisms taking $C_0(\Gamma)$ into $\mathbf{Z}_2$,

$$C^0(\Gamma) := \hom(C_0(\Gamma), \mathbf{Z}_2). \tag{19}$$

The elements of this space are called 0-cochains. It can be regarded as the additive group of functions $f: V_\Gamma \to \mathbf{Z}_2$, because a homomorphism is completely defined by giving its values on a generating set. Given $v \in V$, we define $v^* \in C^0(\Gamma)$ by

$$v^*(u) = \delta_{uv}, \tag{20}$$

where $u \in V$ and δ is the Kronecker symbol. The set $\{v^* | v \in V_\Gamma\}$ forms a basis of $C^0(\Gamma)$. For $c^0 \in C^0(\Gamma)$, $c_0 \in C_0(\Gamma)$, we define $(c^0, c_0) := c^0(c_0)$. Similarly, $C^1(\Gamma)$ denotes the dual space of $C_1(\Gamma)$ and its elements are called 1-cochains. The same comments as for C^0 are valid substituting V with E, and we use the notation e^* and (c^1, c_1) in the same way.

We define $\delta: C^0(\Gamma) \to C^1(\Gamma)$ to be the dual homomorphism of ∂, that is, for every $c^0 \in C^0(\Gamma)$ and $c_1 \in C_1(\Gamma)$ we have $(\delta c^0, c_1) := (c^0, \partial c_1)$. If we think of c^0 as a function over V, then δc^0 can be thought of as a derivative or gradient. What will be important for us is the fact that

$$\forall v \in V (\delta v^*, c_1) = 0 \Leftrightarrow c_1 \in H_1(\Gamma). \tag{21}$$

If we denote by $\text{star}(v)$ the set of edges incident *once* in v, we have

$$\delta v^* = \sum_{e \in \text{star}(v)} e^*. \tag{22}$$

Although we have maintained our discussion in the realm of combinatorics, it is interesting to comment briefly how the topological representation of a graph $\Gamma = (V, E, I)$ is constructed. One starts by giving to V the discrete topology. The points of V are called 0-cells. We also need a set $\{D_e | e \in E\}$ of closed segments or 1-cells. The boundary of each of these segments, denoted ∂D_e, consists of two points. The information contained in I is codified in functions $\phi_e: \partial D_e \to I(e) \subset V$ with the unique requirement that they must be onto. The topological space of the graph is then

constructed as the quotient space of the disjoint union $V \cup_e D_e$ under the identifications $x \sim \phi_e(x)$ for $x \in \partial D_e$. Properties such as connectedness or the first homology group are completely topological.

C. Classical homological codes

With all the machinery laid down, we are ready to introduce classical homological error correcting codes. We say that a simple cycle isomorphic to C_n has length n. Let $\mathrm{Cy}(\Gamma)$ be the set of simple subcycles of Γ. We introduce the distance of a graph Γ, denoted $\mathrm{d}(\Gamma)$, as the minimal length among the elements of $\mathrm{Cy}(\Gamma)$.

Given a graph Γ, let $E=\{e_i\}_{i=1}^{|E|}$. Consider the isomorphisms $\mathbf{h}_1 : C_1(\Gamma) \to \mathbf{Z}_D^{|E|}$ and $\mathbf{h}_2 : C^1(\Gamma) \to \mathbf{Z}_D^{|E|}$ defined by

$$\mathbf{h}_1\left(\sum_{i=1}^{|E|} \lambda_i e_i\right) := (\lambda_0, \lambda_1, \ldots, \lambda_{|E|}), \tag{23}$$

$$\mathbf{h}_2\left(\sum_{i=1}^{|E|} \lambda_i e_i^*\right) := (\lambda_0, \lambda_1, \ldots, \lambda_{|E|}). \tag{24}$$

Then

$$\mathbf{h}_2(c^1) \cdot \mathbf{h}_1(c_1) = (c^1, c_1). \tag{25}$$

Theorem 2: *Let Γ be a connected simplicial graph, not a tree. Construct a parity check matrix H by selecting a set of linearly independent rows of the incidence matrix of Γ. This gives an $[n,k,d]$ linear code C with $n=|E|$, $k=1-\chi$ and $d=\mathrm{d}(\Gamma)$.*

Proof: We claim that $\mathbf{h}_1[H_1(\Gamma)]$ is the code under consideration. Let F be the subspace generated by the elements of $B := \{\delta v^* | v \in V\}$. From Eq. (21) and (25) it follows that $\mathbf{h}_1[H_1(\Gamma)] = \mathbf{h}_2[F]^\perp$. On the other hand, since Γ is simplicial, Eq. (22) now reads

$$\delta v^* = \sum_{\{e \in E | v \in I(e)\}} e^*. \tag{26}$$

Thereby the set of vectors $\mathbf{h}_2[B]$ generates the same space as the rows of the parity check matrix H, which proofs the claim.

Since the length is clearly $|E|$ and $k = \dim \mathbf{h}_1[H_1(\Gamma)] = 1-\chi$, we only have to check the distance of the code. The weight function over $\mathbf{Z}_2$ can be pulled back to $C_1(\Gamma)$. For general 1-chains it gives the number of nonzero coefficients in the formal sum. Its restriction to $\mathrm{Cy}(\Gamma)$ gives the length function. Now, let $c_1 \in H_1(\Gamma)$, $c_1 \neq 0$. There exists a subgraph $\gamma \subset \Gamma$ such that $c_\gamma = c_1$. γ must contain a simple subcycle, for if not, then it is a collection of trees, and so it contains a vertex v of valence 1. But then Eq. (22) implies $(\delta v^*, \gamma) = 1$, a contradiction in view of Eq. (21). So let c be such a simple subcycle. Clearly, $\mathrm{wt}(\mathbf{h}_1(c_1)) \geqslant \mathrm{wt}(\mathbf{h}_1(c)) \geqslant \mathrm{d}(\Gamma)$, and the equality is obtained by taking γ a simple subcycle of minimal length. □

We do not let Γ be a tree just to prevent a code encoding 0 bits of information. Connectedness avoids having a code which can be decomposed into two more simple ones, but of course there is no problem at all in considering unconnected graphs. However, it is completely unnecessary to consider a set of disconnected graphs Γ_i since the wedge product of them, $\vee_i \Gamma_i$, will do the work equally well. The wedge product can be obtained by choosing one vertex from each graph and identifying them all; it does not change the first homology group. Finally, if the graph were not simplicial then the distance would be 1 or 2, something useless since $d = 2t+1$, $t \geqslant 1$.

Let us define $\nu(k,d)$ as the minimum value of n among all the possible $[n,k,d]$ homological codes. Clearly $\nu(k,d) < \nu(k+1,d)$. In addition, we note that $\nu(k+k',d) \leqslant \nu(k,d) + \nu(k',d)$, because the wedge product of two graphs leading, respectively, to $[n,k,d]$ and $[n',k,d']$ codes gives a graph associated with a $[n+n',k+k',d]$ code. The simplest example of a graph with a code

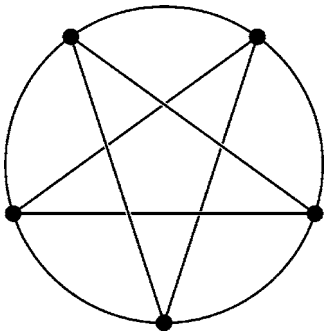

FIG. 6. The complete graph K_5.

associated is C_3. The corresponding code is the repetition code $\{(000), (111)\}$. This example can be extended to a family of codes in two ways. The easy one is the family C_d of $[d,1,d]$ repetition codes. They are clearly optimal, and thus, $\nu(1,d)=d$. More interesting is to regard C_3 as K_3. In general, the complete graph K_s is defined as a simplicial graph with s vertices and all the possible edges. As an example, K_5 is displayed in Fig. 6. The graph K_s yields an $\left[\binom{s}{2},\binom{s}{2}-s+1,3\right]$ code. These codes are clearly optimal among homological ones with $d=3$. Then we can use the family K_s to calculate the asymptotical value of $\nu(k,3)$. Clearly $\nu(k,3)>k$. Let $K(s)=\binom{s}{2}-s+1$. For $k<K(s)$, $\nu(k,3)<\binom{s}{2}=K(s)+O(\sqrt{K(s)})$. Thus

$$\lim_{k\to\infty}\frac{k}{n}=\lim_{k\to\infty}\frac{k}{\nu(k,3)}=1 \tag{27}$$

and asymptotically the point $k/n\sim 1$, $t/n\sim 0$ in the Hamming bound is reached. See Fig. 7 for a graphical representation of the rates.

A question that naturally arises is whether every linear code is homological. As we shall see, the answer is not. Note that the elements of any row of an incidence matrix always sum up to two, in $\mathbf{Z}$. So it might be the case that a subspace does not have a set of generators $\mathbf{u}_i=(u_{i1},\ldots,u_{in})$, $1\leqslant i\leqslant m$ fulfilling the condition $\Sigma_{i=1}^{m}u_{ij}=2$ (where the sum must be performed in $\mathbf{Z}$, not in $\mathbf{Z}_2$). The space generated by the rows of the H matrix in Eq. (8) is an example of this possibility. To verify this, simply check that summing one row to another one is equivalent to perform certain column permutation.

The function $\nu(k,d)$ behaves well for fixed $k=1$ and for fixed $d=3$. Is this true for other values of the parameters? We do not have a conclusive answer, but a partial one may be given. Consider the case $k=2$, the (topologically) most simple one apart from $k=1$. There are only two interesting topologies for a graph giving this value of k, see Fig. 8. For case A the inequalities $a+b\geqslant d$, $a+c\geqslant d$, and $b+c\geqslant d$ must hold. Summing up we get $2n\geqslant 3d$. The same procedure applied to case B easily yields $n\geqslant 2d$. We want n as small as possible, and so in principle the first case is the best one. This is confirmed by the (optimal) assignment $a=b=t+1$, $c=t$, where $d=2t+1$. For high

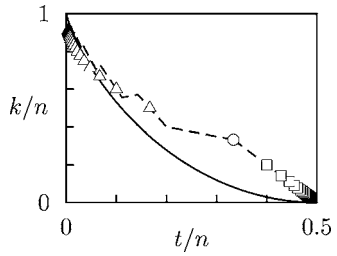

FIG. 7. The rate k/n vs t/n for the codes generated by the families C_d (□) and K_s (△), with the corresponding Hamming bound (dashed line). ○ is $C_3=K_3$. The asymptotic Hamming bound is displayed as a reference (continuous line).

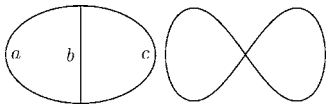

FIG. 8. The two (connected) topologies for the case $k=2$. Each curve represents a path, and the labels indicate the number of edges composing it. Other topologies are also possible, but they could be transformed in one of these by eliminating one by one any vertex of valence 1 (an operation which does not alter the homology nor the distance).

values of t, $t/n \simeq 1/3$, and there is no way to get a better result. Note how topologies with the same first homology group can somehow be classified according to their optimality for code composition. If a similar calculation is performed for $k=3$, K_4 is among the optimal ones (perhaps as expected) and gives $t/n \simeq 1/4$ for high values of t. Moreover, due to the high symmetry of K_s it is possible to construct a bound for its topology for any s. One has to consider all the C_3 cycles in K_s and proceed as above to get

$$(s-2)n \geqslant \binom{s}{3} d. \tag{28}$$

This is quite a disappointing result, since for high values of s one gets $t/n \sim 0$, even for low values of n. However, it is not conclusive as long as we do not know whether the topology of K_s is the optimal one for $k=K(s)$.

If one does not care about homology and only wants a way to visualize codes, then of course it is possible to allow "links" connecting an arbitrary number of "nodes." One can still consider chains of links, and the nodes impose the conditions of the H matrix as vertices did in the homological point of view. In such a scheme, the code (8) would look as Fig. 9. It is not clear, however, whether this could be of any use.

III. HOMOLOGICAL CODES FOR QUANTUM ERROR CORRECTION

A. Quantum error correcting codes

QEC is the quantum analog of its classical counterpart. As it usually happens, the quantum domain gives rise to difficulties not present in the classical case; the extension of techniques such as linear coding is far from being straightforward. In fact, in the early times of quantum information it was believed that QEC was impossible. As it happens quite often, the dangerous word "impossible" was soon substituted by the more encouraging "difficult."

Here we shall only consider error correction under the transmission through quantum noisy channels, which includes information storage. This means that we will suppose that the error correction stage can be performed without errors. In general this is not a realistic scenario, and the more general framework of fault-tolerant quantum computation is necessary.

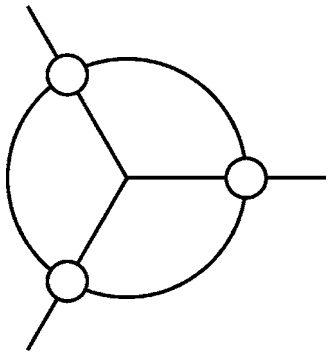

FIG. 9. A nonhomological visualization for the Hamming code [7, 4, 3]. There is one link connecting three nodes, something impossible with edges.

In the classical case we have been interested exclusively in bits. In the quantum case it would seem natural to consider only *qubits*, their quantum analog. Any quantum system with only two states can be regarded as a qubit. Its representation is a complex Hilbert space of dimension 2. We shall, however, consider higher-dimensional quantum systems, or *qudits*. Although classical computation is now far more interested in bits than in dits, it was not the case in its early times. In the quantum case it seems to be rather interesting to consider qudits,[62] and thus we will discuss them on equal footing throughout this section.

First a bit of notation. A qudit is described by a Hilbert space of dimension $D \geqslant 2$, and finite. This space will be denoted $\mathcal{D}$. The elements of a given orthogonal basis can be denoted $|x\rangle$ with $x=0,\ldots,D-1$. This set of numbers is naturally identified with the elements of the set modulus

$$\mathbf{Z}_D := \mathbf{Z}/D\mathbf{Z}. \tag{29}$$

In general, whenever an element of $\mathbf{Z}_D$ appears in an expression, any integer in that expression must be understood to be mapped to $\mathbf{Z}_D$. Messages are strings of qudits. Such a string of length n corresponds to the space $\mathcal{D}^{\otimes n}$. When expressing elements of this space, vector notation is useful. As usual, $\mathbf{v} \in \mathbf{Z}_D^n$ stands for $\mathbf{v}=(v_1,\ldots,v_n), v_i \in \mathbf{Z}_D$. With this notation, we define

$$|\mathbf{v}\rangle := \bigotimes_{i=1}^{n} |v_i\rangle. \tag{30}$$

The usual scalar product $\mathbf{u}\cdot\mathbf{v}$ will be employed. It is worth noting that, whenever D is not prime, $\mathbf{Z}_D$ is not a field and $\mathbf{Z}_D^n$ is not a vector space. This is not seriously dangerous and we will use the word vector in this wider sense.[62] For fixed dimension D, we also introduce the symbol

$$\varphi(k) := \mathrm{e}^{(2\pi \mathrm{i}/D)k}, \tag{31}$$

where $k \in \mathbf{Z}_D$.

The essence of QEC is what follows. We consider a system S and its environment E. The environment cannot be controlled, and it interacts with the system producing *noise*. The system is not initially entangled with the environment, but entanglement grows with the unavoidable interaction between E and S. Omitting the tensor product symbol, this interaction can be described as follows:[65]

$$|e\rangle|s\rangle \to \sum_k |e_k\rangle M_k |s\rangle, \tag{32}$$

where $|e\rangle$ and $|s\rangle$ are, respectively, the initial state of the environment and the system; the final states of the environment $|e_k\rangle$ are not necessarily orthogonal or normalized and the operators M_k acting on the system are unitary. In order to perform error correction we need to disentangle system and environment. This can be achieved by enlarging the system S with an ancilla system A and whenever it is possible to perform a unitary operation R over $S' = A \otimes S$ such that

$$R(|a\rangle M_k |s\rangle) = |a_k\rangle|s\rangle, \tag{33}$$

where $|a\rangle$ is the initial state of the ancilla. If this is the case, then we have

$$\sum_k |e_k\rangle R(|a\rangle M_k |s\rangle) = \left(\sum_k |e_k\rangle|a_k\rangle\right)|s\rangle, \tag{34}$$

and the errors are gone. Of course, the state $|s\rangle$ is unknown. This means that our strategy should work (with the same R) for certain subspace of S. Then we could use this subspace for information transmission or storage without errors. In general, however, we will not be able to correct every error and thus we will have to consider only errors M_k that happen with high probability, just as in the classical case.

Let us explain under which conditions there exists a recovery operation R as in Eq. (33). A *quantum error correcting code of length n* is a subspace $\mathcal{C}$ of $\mathcal{D}^{\otimes n}$ such that recovery is possible

after noise consisting of any combination of error operators from some set $\mathcal{E}$ of operators over $\mathcal{D}^{\otimes n}$. The set $\mathcal{E}$ is the set of *correctable errors*, and we say that $\mathcal{C}$ *corrects* $\mathcal{E}$. Note that any linear combination of correctable errors is also correctable. A requirement for correction to be possible that looks pretty intuitive is the following. For every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ such that $\langle\xi|\eta\rangle = 0$ and for every $M, N \in \mathcal{E}$

$$\langle\xi|N^\dagger M|\eta\rangle = 0. \tag{35}$$

This only says that errors do not mix up orthogonal states of the code. In what follows we show that, in fact, this condition is enough and sufficient for Eq. (33) to be possible.

Condition (35) can be rewritten in an equivalent form: For every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ and for every $N, M \in \mathcal{E}$

$$\langle\xi|N^\dagger M|\eta\rangle = c(N^\dagger M)\langle\xi|\eta\rangle, \tag{36}$$

where $c(N^\dagger M) \in \mathbf{C}$. Clearly this implies Eq. (35). For the converse, note that for every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ such that $\langle\xi|\eta\rangle = 0$ condition (35) implies

$$0 = \langle\xi - \eta|N^\dagger M|\xi + \eta\rangle = \langle\xi|N^\dagger M|\xi\rangle - \langle\eta|N^\dagger M|\eta\rangle, \tag{37}$$

from which Eq. (36) follows by considering any orthogonal basis of $\mathcal{C}$ and evaluating $N^\dagger M$ on it.

We now observe that the existence of an ancilla system A and a recovery operation R as in Eq. (33) implies Eq. (36). This is because

$$\langle\xi|M_i^\dagger M_j|\eta\rangle = \langle\xi|M_i^\dagger\langle a|R^\dagger R|a\rangle M_j|\eta\rangle = \langle\xi|\eta\rangle\langle a_i|a_j\rangle. \tag{38}$$

The converse is also true; it is enough to take $\mathcal{D}^{\otimes n}$ as the ancilla system and set

$$R(|a\rangle M|\xi\rangle) = M|a\rangle|\xi\rangle \tag{39}$$

for every $\xi \in \mathcal{C}$ and $M \in \mathcal{E}$ and for some $|a\rangle \in \mathcal{C}$ chosen as the initial state of the ancilla system. This does not define R completely, but it is enough to check that it can be extended to a unitary operator over $\mathcal{D}^{\otimes n} \otimes \mathcal{D}^{\otimes n}$. This in turn holds true if

$$\langle\eta|N^\dagger M|\xi\rangle\langle a|a\rangle = \langle a|N^\dagger M|a\rangle\langle\eta|\xi\rangle, \tag{40}$$

but this follows from Eq. (36).

Our next goal is to introduce a notion of code *distance*, just as in the classical case. A quantum code $\mathcal{C}$ is said to *detect* an error N if for every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$

$$\langle\xi|N|\eta\rangle = c(N)\langle\xi|\eta\rangle \tag{41}$$

for some $c(N) \in \mathbf{C}$. From the above discussion follows that a code $\mathcal{C}$ corrects error from $\mathcal{E}$ iff it detects errors from the space

$$\mathcal{E}^\dagger\mathcal{E} := \left\{ \sum_l N_l^\dagger M_l | M_l, N_l \in \mathcal{E} \right\}. \tag{42}$$

For codes of length n, let $\mathcal{E}(n,k)$ be the set of operators acting on at most k qudits. We define the distance of the code $\mathcal{C}$, denoted $d(\mathcal{C})$, as the smallest number d for which the code does not detect $\mathcal{E}(n,d)$. Since $\mathcal{E}(n,t)^\dagger\mathcal{E}(n,t) = \mathcal{E}(n,2t)$, a code $\mathcal{C}$ corrects $\mathcal{E}(n,t)$ iff $d(\mathcal{C}) > 2k$. In this case we say that $\mathcal{C}$ corrects t errors. As in the classical case, we can talk about $[[n,k,d]]$ codes when referring to codes of length n, dimension D^k, and distance d. Such a code is said to encode k qudits. We use double brackets to distinguishing them from classical codes.

As an example, let us introduce the trivial code of length n encoding k qudits,

$$\mathcal{C}_T(n,k) := \{|\mathbf{0}\rangle \otimes |\xi\rangle | \xi \in \mathcal{D}^{\otimes k}\}, \tag{43}$$

where $|\mathbf{0}\rangle = |0\rangle^{\otimes n-k}$. Since it has distance 1, the trivial code is quite useless. However, its structure can give rise to a rich family of codes. To this end, let $U: \mathcal{D}^{\otimes n} \to \mathcal{D}^{\otimes n}$ be any unitary operator. Clearly

$$U\mathcal{C}_T(n,k) := \{U|c\rangle | c \in \mathcal{C}_T(n,k)\} \tag{44}$$

is also an error correcting code. In fact, it is clear that for any $[[n,k,d]]$ quantum error correcting code $\mathcal{C}$ for which k is an integer there exists a unitary operator U such that $U\mathcal{C}_T(n,k) = \mathcal{C}$. These kinds of codes are the most usual ones. Since

$$\langle \xi | N | \eta \rangle = \langle \xi | U^\dagger U N U^\dagger U | \eta \rangle, \tag{45}$$

the errors detected by $\mathcal{C}_T$ and $U\mathcal{C}_T$ are in a one to one correspondence through conjugation $U \cdot U^\dagger$. Exploiting this idea we could try to find a family of U operators for which the calculation of the distance of the code $U\mathcal{C}_T(n,k)$ is easy. This is the subject of the next section.

B. Symplectic codes

As a generalization of the usual X and Z Pauli matrices for qubits, we define for qudits of fixed dimension D the operators (31)

$$X := \sum_{k \in \mathbf{Z}_D} |k+1\rangle\langle k|, \tag{46}$$

$$Z := \sum_{k \in \mathbf{Z}_D} \varphi(k) |k\rangle\langle k|. \tag{47}$$

Note that $X^D = Z^D = 1$ and $XZ = \varphi(1) ZX$. With these operators a basis for the linear operators over $\mathcal{D}$ can be defined,

$$\sigma_{xz} := f(xz) X^x Z^z, \tag{48}$$

where $x, z \in \mathbf{Z}_D$ and $f: \mathbf{Z}_D \to \mathbf{C}$ is there to guarantee $\sigma_{xz}^D = 1$. Thus we have to define f by demanding $f(x)^D = \varphi(x)^{D(D-1)/2} = (-1)^{x(D+1)}$, and then we take

$$f(x) := \begin{cases} e^{\pi i/D} & \text{if } D \text{ is even and } x \text{ is odd} \\ 1 & \text{if } D \text{ is odd or } x \text{ is even.} \end{cases} \tag{49}$$

The set of σ operators is a basis because

$$|k\rangle\langle l| = \frac{1}{D} \sum_{m \in \mathbf{Z}_D} \varphi(-lm) X^{k-l} Z^m. \tag{50}$$

As an example, note that for qubits we recover the usual Pauli matrices: $\sigma_{00} = I$, $\sigma_{10} = X$, $\sigma_{01} = Z$, and $\sigma_{11} = Y$.

We consider strings of qudits. For $\mathbf{v} \in \mathbf{Z}_D^{2n}$ and $\mathbf{x}, \mathbf{z} \in \mathbf{Z}_D^n$ let us introduce the notation $\mathbf{v} = (\mathbf{xz})$ meaning

$$\mathbf{v} = (x_1, \ldots, x_n, z_1, \ldots, z_n). \tag{51}$$

We can extend our family of operators to act on $\mathcal{D}^{\otimes n}$,

$$\sigma_{\mathbf{v}} := \sigma_{\mathbf{xz}} := \bigotimes_{i=1}^{n} \sigma_{x_i z_i}, \tag{52}$$

where $\mathbf{v} = (\mathbf{xz})$. We have

$$\sigma_{\mathbf{x}0}|\mathbf{v}\rangle := |\mathbf{v}+\mathbf{x}\rangle, \tag{53}$$

$$\sigma_{0\mathbf{z}}|\mathbf{v}\rangle := \varphi(\mathbf{z}\cdot\mathbf{v})|\mathbf{v}\rangle. \tag{54}$$

An important commutation relation is[62]

$$\sigma_{\mathbf{u}}\sigma_{\mathbf{v}} = \varphi(\mathbf{u}^t\Omega\mathbf{v})\sigma_{\mathbf{v}}\sigma_{\mathbf{u}}, \tag{55}$$

where

$$\Omega := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{56}$$

is a $2n\times 2n$ matrix over $\mathbf{Z}_D$. The group of all the operators generated by the set of σ operators is the Pauli group $\mathbf{P}_D(n)$. Note that there is a natural homomorphism from this group onto $\mathbf{Z}_D^{2n}$ since $\sigma_{\mathbf{u}}\sigma_{\mathbf{v}} \propto \sigma_{\mathbf{u}+\mathbf{v}}$.

Let us now consider operators $U\cdot U^\dagger$ with U unitary such that they are closed over $\mathbf{P}_D(n)$, that is,

$$U\sigma_{\mathbf{v}}U^\dagger = \psi(\mathbf{v})\sigma_{\omega(\mathbf{v})}, \tag{57}$$

where $\psi:\mathbf{Z}_D^{2n}\to\mathbf{C}$ and $\omega:\mathbf{Z}_D^{2n}\to\mathbf{Z}_D^{2n}$ are functions depending on U. We call this group the extended symplectic group $ESp_D(n)$. It might look that this condition is not enough to guarantee that $U\cdot U^\dagger$ is closed over $\mathbf{P}_D(n)$, but since it implies $\psi(\mathbf{v})^D=1$, we have $\psi(\mathbf{v})=\varphi(g(\mathbf{v}))$ for some $g:\mathbf{Z}_D^{2n}\to\mathbf{Z}_D$. Thus, there is no problem at all. It is can be easily derived that

$$\sigma_{\omega(\mathbf{u}+\mathbf{v})} \propto \sigma_{\omega(\mathbf{u})}\sigma_{\omega(\mathbf{v})} \propto \sigma_{\omega(\mathbf{u})+\omega(\mathbf{v})}. \tag{58}$$

From it this follows that $\omega(\mathbf{u})=M\mathbf{u}$ where M is a $2n\times 2n$ matrix over $\mathbf{Z}_D$. From Eq. (55) we obtain the following condition on M:

$$M^t\Omega M = \Omega. \tag{59}$$

The matrix group described by this condition is the symplectic group $Sp_D(n)$. There is thus a natural group homomorphism

$$h:ESp_D(n)\to Sp_D(n). \tag{60}$$

But h is onto, see Appendix A, and so it induces the isomorphism

$$ESp_D(n)/\ker h \cong Sp_D(n). \tag{61}$$

It is interesting to study the kernel of h. For any of its elements we have

$$U\sigma_{\mathbf{v}}U^\dagger = \varphi(g(\mathbf{v}))\sigma_{\mathbf{v}}. \tag{62}$$

But this easily implies that $g(\mathbf{v})=\mathbf{w}\cdot\mathbf{v}$ for some $\mathbf{w}\in\mathbf{Z}_D^{2n}$. On the other hand,

$$\sigma_{\mathbf{u}}\sigma_{\mathbf{v}}\sigma_{\mathbf{u}}^\dagger = \varphi(\mathbf{u}^t\Omega\mathbf{v})\sigma_{\mathbf{v}}. \tag{63}$$

As a result, $\ker h\cong\mathbf{Z}_D^{2n}$.

Now that we have characterized $ESp_D(n)$, it is time to return to our initial purpose of constructing quantum error correcting codes. The idea is to apply the symplectic group $ESp_D(n)$ to $\mathcal{C}_T(n,k)$ and obtain the codes which are called symplectic. A first result is that $\ker h$ does not help a lot; it only generates codes of the form

$$\{|\mathbf{u}\rangle \otimes |\xi\rangle | \xi \in \mathcal{D}^{\otimes k}\}, \tag{64}$$

where $\mathbf{u} \in \mathbf{Z}_D^{n-k}$. This is an example of conjugated codes. More generally, for each symplectic $[[n,k,d]]$ code $\mathcal{C}$ there exists a family of D^{n-k} conjugated $[[n,k,d]]$ codes obtained from $\mathcal{C}$ by application of σ operators. This will become clear shortly. As a result, we only have to focus on $Sp_D(n)$ when looking for better codes.

For any subspace $V \subset \mathbf{Z}_D^{2n}$ we define the subspace

$$\hat{V} := \{\mathbf{u} \in \mathbf{Z}_D^{2n} | \forall\, \mathbf{v} \in V \mathbf{u}^t \Omega \mathbf{v} = 0\}. \tag{65}$$

If V has a basis which is a linearly independent set and $V \subset \hat{V}$ we say that V is *isotropic*. Now let $V_{\mathcal{C}_T} \subset \mathbf{Z}_D^{2n}$ be the isotropic subspace containing the elements of the form $(\mathbf{0}\mathbf{z})$, where $\mathbf{z} \in \mathbf{Z}_D^n$ must have its last k elements equal to zero. It is not difficult to verify that $\mathcal{C}_T(n,k)$ detects $\sigma_\mathbf{v}$ iff

$$\mathbf{v} \notin \hat{V}_{\mathcal{C}_T} - V_{\mathcal{C}_T}. \tag{66}$$

Consider any symplectic code $\mathcal{C} = U\mathcal{C}_T(n,k)$ with $h(U) = M$. We can define $V_\mathcal{C} := MV_{\mathcal{C}_T}$, giving $\hat{V}_\mathcal{C} = \widehat{MV}_{\mathcal{C}_T} = M\hat{V}_{\mathcal{C}_T}$. Then $\mathcal{C}$ detects $\sigma_\mathbf{v}$ iff $\mathbf{v} \notin \hat{V}_\mathcal{C} - V_\mathcal{C}$. In analogy with the weight function for classical codes, for any $\mathbf{v} = (\mathbf{x}\mathbf{z}) \in \mathbf{Z}_D^{2n}$, let

$$|\mathbf{v}| := |\{i = 1, \ldots, n | x_i \neq 0 \text{ or } z_i \neq 0\}|. \tag{67}$$

Recall that σ operators over one qudit form a basis. This, the fact that the space of operators detected by a code is a linear subspace, and the previous discussion imply altogether

$$d(\mathcal{C}) = \min_{\mathbf{v} \in \hat{V}_\mathcal{C} - V_\mathcal{C}} |\mathbf{v}|. \tag{68}$$

This equation shows that the distance of the code depends only upon $V_\mathcal{C}$. On the other hand, given two isotropic subspaces $V_1, V_2 \subset \mathbf{Z}_D^{2n}$ of the same dimension it is possible to find a matrix $M \in Sp_D(n)$ such that $MV_1 = V_2$.[62] Therefore, for any isotropic subspace of dimension $n-k$ such that $V \subset \hat{V}$ there exists an $[[n,k,d]]$ symplectic code $\mathcal{C}$ with $V_\mathcal{C} = V$. This way, the problem of finding good codes is reduced to the problem of finding good isotropic subspaces $V \subset \mathbf{Z}_D^{2n}$. This is analogous to the classical situation with linear codes.

It is worth revisiting the trivial code on a new light. Consider the following Abelian subgroup of $\mathbf{P}_D(n)$:

$$\mathcal{S}_T(n,k) := \{\sigma_\mathbf{v} | \mathbf{v} \in V_{\mathcal{C}_T}\}. \tag{69}$$

The trivial code can be defined just in terms of this group,

$$\mathcal{C}_T(n,k) = \{|\xi\rangle \in \mathcal{D}^{\otimes n} | \forall\, \sigma \in \mathcal{S}_T(n,k) \sigma |\xi\rangle = |\xi\rangle\}. \tag{70}$$

$\mathcal{S}_T(n,k)$ is called the *stabilizer* of $\mathcal{C}_T(n,k)$. The stabilizer of any code $\mathcal{C} = U\mathcal{C}_T(n,k)$ is the Abelian group $\mathcal{S}_\mathcal{C} := U\mathcal{S}_T(n,k)U^\dagger$, and $\mathcal{C}$ can be defined by its stabilizer just as we did for $\mathcal{C}_T(n,k)$. It is because of this point of view that symplectic codes are also called stabilizer codes. A question that naturally arises here is under which conditions an Abelian subgroup $\mathcal{S} \subset \mathbf{P}_D(n)$ is the stabilizer of a symplectic code. Clearly $\mathcal{S}$ must fulfill the condition

$$\forall\, \sigma_1, \sigma_2 \in \mathcal{S}, \quad \sigma_1 \propto \sigma_2 \Rightarrow \sigma_1 = \sigma_2. \tag{71}$$

For D prime this is the end of the story, but in other case a bit of care is necessary, as we shall show now. Because of condition (71), $\mathcal{S}$ is isomorphically mapped to a subgroup $V_\mathcal{S} \subset \mathbf{Z}_D^{2n}$. We claim that $\mathcal{S}$ is the stabilizer of a symplectic code iff $V_\mathcal{S}$ is a subspace of $\mathbf{Z}_D^{2n}$ with a basis that is a linearly independent set. We only have to check the if direction. First, the elements of $\mathcal{S}$ can be labeled with the elements of $V_\mathcal{S}$. We denote them $\sigma_\mathcal{S}(\mathbf{v})$, $\mathbf{v} \in V_\mathcal{S}$. $V_\mathcal{S}$ is isotropic, and so we can find

a symplectic code $\mathcal{C}$ such that $V_{\mathcal{C}}=V_{\mathcal{S}}$. Let us denote the elements of its stabilizer $\sigma_{\mathcal{C}}(\mathbf{v})$, but in such a way that

$$\sigma_{\mathcal{C}}(\mathbf{v}) = \varphi(g(\mathbf{v}))\sigma_{\mathcal{S}}(\mathbf{v}), \tag{72}$$

where $g:\mathbf{Z}_D^{2n}\to\mathbf{C}$ and $\mathbf{v}\in V_{\mathcal{C}}=V_{\mathcal{S}}$. This is always possible since $\sigma_{\mathcal{S}}(\mathbf{v})^D=\sigma_{\mathcal{C}}(\mathbf{v})^D=1$. It is easily verified that g is linear, but then $g(\mathbf{v})=\mathbf{w}\cdot\mathbf{v}$ for some $\mathbf{w}\in\mathbf{Z}_D^{2n}$. Due to Eq. (63), there is a conjugate code of $\mathcal{C}$ such that $\mathcal{S}$ is its stabilizer.

Although condition (35) guarantees that recovery is possible, it is worth giving a more concrete recipe for symplectic codes. So let $\mathcal{C}$ be a code of distance d, $\{\mathbf{v}_i\}$ a basis of $V_{\mathcal{C}}$, and $G:=\{\varphi(f_i)\sigma_{\mathbf{v}_i}\}$ a generating set for its stabilizer, where $f_i\in\mathbf{Z}_D$. Suppose that an encoded state $|\xi\rangle$ has been subject to correctable noise as in Eq. (32),

$$|e\rangle|\xi\rangle \to \sum_k |e_k\rangle\sigma_{\mathbf{u}_k}|\xi\rangle, \tag{73}$$

where $\mathbf{u}_k\in\mathbf{Z}_D^{2n}$ and $|\mathbf{u}_k|<d/2$. We first measure the *syndrome* of the error. This amounts to project the system to any of the eigenstates of each operator in G. For each of the eigenstates there is a corresponding eigenvalue $\varphi(g_i)$, $g_i\in\mathbf{Z}_D$. The final state then is proportional to

$$\sum_{k:\forall i v_i^t\Omega u_k=g_i} |e_k\rangle\sigma_{\mathbf{u}_k}|\xi\rangle. \tag{74}$$

Let $\sigma_{\mathbf{u}}$ and $\sigma_{\mathbf{u}'}$ be any of the error operators in this sum. Note that $\mathbf{u}-\mathbf{u}'\in\hat{V}_{\mathcal{C}}$. Also, $\sigma_{\mathbf{u}'}^{\dagger}\sigma_{\mathbf{u}}\propto\sigma_{\mathbf{u}-\mathbf{u}'}$ is detectable, and so, in fact, $\mathbf{u}-\mathbf{u}'\in V_{\mathcal{C}}$. With the information from the error syndrome, we can choose any $\mathbf{w}$ such that $\mathbf{u}_i'\Omega\mathbf{w}=g_i$ and $\sigma_{\mathbf{w}}$ is correctable. Then any of the error operators in the sum is of the form $\sigma_{\mathbf{u}_k}\propto\sigma_{\mathbf{w}}\sigma_{\mathbf{u}_k'}$ with $\mathbf{u}_k'\in V_{\mathcal{C}}$. In other words, Eq. (74) can be rewritten as

$$\left(\sum_{k:\forall i v_i^t\Omega u_k=g_i} |e_k'\rangle\right)\sigma_{\mathbf{w}}|\xi\rangle, \tag{75}$$

where $|e_k'\rangle\propto|e_k\rangle$. This means that the measurement by itself is enough to disentangle system and environment, and we only have to perform $\sigma_{\mathbf{w}}^{\dagger}$ to recover the original encoded state.

Due to the essential role of $V_{\mathcal{C}}$, symplectic codes are usually given in the form of a $2n\times(n-k)$ matrix whose rows form a basis for it. As an example, there is a [[5,1,3]] symplectic code[12,13] of the form

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{76}$$

An important class of codes is that of the so-called CSS codes. Initially, CSS codes were introduced as a tool to obtain quantum codes from classical ones.[7,8] Given a classical $[n,k,d]$ code $\mathcal{C}$ with $\mathcal{C}\subset\mathcal{C}^{\perp}$ and check matrix H, the quantum code with check matrix

$$\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}$$

is a $[[n,2k-n,d]]$ code. More generally, any code for which the matrix can be put in the form

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

in such a way that X and Z operators are not mixed up, is called CSS. Following Steane[63] and Preskill,[64] we adopt here this terminology to designate CSS codes in general, A good example of

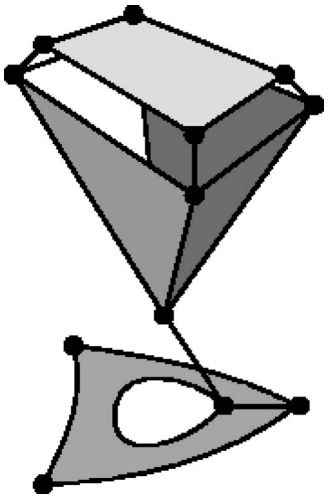

FIG. 10. A 2-complex composed of 9 vertices, 21 edges, and 4 faces.

these generalized CSS codes are the homological quantum codes, as we will see.

Returning to general codes, it is possible to derive a quantum analog of the Hamming bound for certain quantum codes. Let

$$\mathcal{E}_\sigma(n,t) := \{\sigma_{\mathbf{v}} || \mathbf{v}| \leqslant t\}. \tag{77}$$

It is clear that a code that corrects $\mathcal{E}_\sigma(n,t)$ corrects t errors. Let $\mathcal{C}$ be a code of length n and dimension m that corrects t errors and satisfies the condition that for every normalized $|\xi\rangle \in \mathcal{C}$ and for every $\mathbf{u},\mathbf{v} \in \mathbf{Z}_D^{2n}$ such that $|\mathbf{u}|, |\mathbf{v}| \leqslant t$

$$\langle \xi | \sigma_{\mathbf{u}}^\dagger \sigma_{\mathbf{v}} | \xi \rangle = \delta_{\mathbf{uv}}. \tag{78}$$

Such codes are called orthogonal or nondegenerate. Notice that for $\mathcal{D}^{\otimes n}$ there are $(D^2-1)^t\binom{n}{t}\sigma$ operators of weight t. This and condition (78) give the quantum Hamming bound[66]

$$m\sum_{i=0}^{t}(D^2-1)^i\binom{n}{i} \leqslant D^n. \tag{79}$$

C. Homology of 2-complexes

A 2-complex is the two-dimensional generalization of a graph or 1-complex. In general one can speak of cell complexes of arbitrary dimension, but we will keep things simple and restrict our attention to these low-dimensional cases. Recall that graphs were obtained by attaching 1-cells (arcs) to a set of 0-cells (points). We can continue the process by attaching 2-cells (disks) to the graph. Here attaching means "identify points in the boundary through continuous maps;" recall the end of Sec. II B. Indeed, we will not consider such general 2-complexes. We are interested in the combinatorial point of view, and our definition will reflect this fact. Figure 10 shows an example of the kind of objects we shall consider. The goal is to study the first homology group H_1 of these objects. Although our study of graphs only included $\mathbf{Z}_2$ homology, now we will discuss $\mathbf{Z}$ homology. In fact, when we talk about qudits we will be interested in $\mathbf{Z}_D$ homology, but this is constructed substituting $\mathbf{Z}$ for $\mathbf{Z}_D$ in the definitions.

Moving from $\mathbf{Z}_2$ homology to $\mathbf{Z}$ homology requires the introduction of orientation. An *oriented finite graph* $\Gamma=(V,E,I_s,I_t)$ consists of a finite set V of vertices, a finite set E of edges, and two incidence functions $I_s,I_t: E \to V$. The subindices stand for "source" and "target." We say that an edge $e \in E$ goes or points from $I_s(e)$ to $I_t(e)$. Let us introduce the set of inverse edges E^{-1}

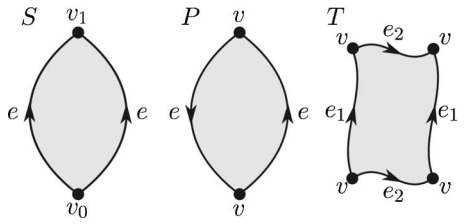

FIG. 11. Planar representations of several 2-complexes. They have the topology of the sphere S, the projective plane P, and the torus T. The identifiers for vertices and edges are the same as in the text.

$:=\{e^{-1}\,|\,e\in E\}$, where e^{-1} is just a symbol and we set $(e^{-1})^{-1}:=e$. We will use the notation $\bar{E}:=E\cup E^{-1}$. The incidence functions can be extended to $\bar{E}$ setting $I_s(e)=I_t(e^{-1})$ for any $e\in\bar{E}$.

In order to give a combinatorial meaning to the attachment of disks to graphs described above, we introduce the idea of walks on graphs. Given an n-tuple $(a,b,c,\ldots)$, let $[a,b,c,\ldots]$ denote the class of n-tuples equal to it up to cyclic permutations. We call such objects cyclic n-tuples, and its elements are naturally indexed by $\mathbf{Z}_n$. A *closed walk of length n* on a graph Γ is a cyclic n-tuple of oriented edges

$$w=[e_0,\ldots,e_{n-1}],\quad e_i\in\bar{E}, \tag{80}$$

such that $I_t(e_i)=I_s(e_{i+1})$ for every $i\in\mathbf{Z}_n$. The idea is that, given a graph, we can attach to it n-gons along closed walks. Note that the attachment can have two orientations, since given a closed walk w one could take the inverse walk $w^{-1}:=[e_{n-1}^{-1},\ldots,e_1^{-1}]$ to describe the same attachment. Our definition of walks excludes the possibility of attaching the boundary of a disk along a walk consisting of a single vertex, something very useful in other contexts but not for our purposes.

Let W_Γ denote the set of closed walks on the oriented graph Γ. An *oriented 2-complex* $\Sigma=(V,E,F,I_s,I_t,B)$ has the structure of a graph $\Gamma=(V,E,I_s,I_t)$ plus a finite set F of faces and a boundary function $B:F\to W_\Gamma$. Just as we did for edges, we can consider the set F^{-1} of inverse faces setting $B(f^{-1})=B(f)^{-1}$. We also set $\bar{F}:=F\cup F^{-1}$. The discussion above explains how a topological space M is related to this combinatorial structure Σ, and we will say that Σ represents M and use them almost indistinguishably. In any case, our application to quantum error correcting codes only depends on the combinatorial point of view. Some examples will illustrate the concept of 2-complex (see Figs. 11 and 12).

- The sphere S. Take two vertices v_0 and v_1, an edge e pointing from v_0 to v_1, and a face f with the boundary $[e,e^{-1}]$.
- The projective plane P. Only a single vertex v, a single edge e, and a single face f with boundary $[e,e]$ are needed.
- The torus T. This can be constructed with a vertex v, two edges e_1 and e_2, and a face f with boundary $[e_1,e_2,e_1^{-1},e_2^{-1}]$.

For any 2-complex Σ the Euler characteristic is

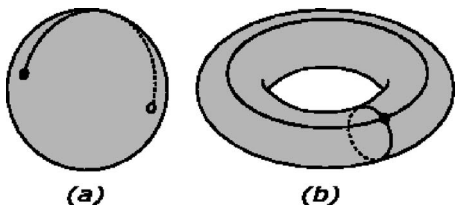

FIG. 12. A pair of 2-complexes embedded in $\mathbf{R}^3$. They represent (a) the sphere S and (b) the torus T.

$$\chi(\Sigma) := |V| - |E| + |F|. \tag{81}$$

Σ is said to be connected if its graph Γ is connected. $\Sigma' = (V', E', F', I'_s, I'_t, B')$ is said to be a subcomplex of Σ if $V' \subset V$, $E' \subset E$, $F' \subset F$, $I'_s \subset I_s$, $I'_t \subset I_t$ and $B' \subset B$. As usual, we call components the maximal connected subcomplexes of Σ. Although we have defined χ and connectedness in terms of Σ, they only depend upon the underlying topology. The same is true for H_1; its definition is our next goal.

Consider a 2-complex Σ. For the sake of simplicity, let us introduce the notation $\Delta_0 := V$, $\Delta_1 := E$, $\Delta_2 := F$. Let also the sets of 0-, 1-, and 2-chains be denoted $C_i(\Sigma)$ with $i = 0, 1, 2$. They contain formal sums of elements of Δ_i with integer coefficients. We adopt the same conventions as for 0- and 1-chains for graphs. As in that case, $C_i(\Sigma) \simeq \mathbf{Z}^{|\Delta_i|}$ and Δ_i is a natural basis of $C_i(\Sigma)$.

We introduce the boundary homomorphisms $\partial_i : \Delta_i \to \Delta_{i-1}$ for $i = 1, 2$. It is enough to give their value on a set of generators. We have

$$\forall e \in E, \quad \partial_1(e) = I_t(e) - I_s(e); \tag{82}$$

$$\forall f \in F, \quad \partial_2(f) = c_{B(f)}; \tag{83}$$

where for any $w = [e_1^{\sigma_1}, \ldots, e_n^{\sigma_n}] \in W_\Gamma$, $e_i \in E$, $\sigma_i = \pm 1$, we define

$$c_w := \sum_{i=1}^{n} \sigma_i e_i. \tag{84}$$

Whenever the index i in ∂_i can be inferred from the context, we will omit it. A simple but fundamental property is

$$\partial^2 = 0. \tag{85}$$

Let $Z_1(\Sigma) := \ker \partial_1$, $B_1(\Sigma) := \operatorname{ran} \partial_2$. The elements of Z_1 are called cycles and the elements of B_1 boundaries. We already encountered cycles in our study of the homology of a graph. Note that $B_1 \subset Z_1$. Thus we can define

$$H_1(\Sigma) := Z_1(\Sigma)/B_1(\Sigma). \tag{86}$$

Two cycles which represent the same element of the homology group are said to be homologous. Boundaries are homologous to zero. If Σ consists of several components Σ_i, we have

$$H_1(\Sigma) \simeq \oplus_i H_1(\Sigma_i). \tag{87}$$

Our next goal is the definition of the first cohomology group $H^1(\Sigma)$. For $i = 0, 1, 2$, let $C^i(\Sigma)$ denote the dual space of $C_i(\Sigma)$, that is,

$$C^i(\Sigma) := \hom(C_i(\Sigma), \mathbf{Z}). \tag{88}$$

The elements of these spaces are called i-cochains. They can be regarded as the additive group of functions $f : \Delta_i \to \mathbf{Z}$. Given $\sigma \in \Delta_i$, we define $\sigma^* \in C^i(\Sigma)$ by

$$\sigma^*(\sigma') = \delta_{\sigma\sigma'}, \tag{89}$$

where $\sigma' \in \Delta_i$. The set $\{\sigma^* \,|\, \sigma \in \Delta_i\}$ is a basis of $C^i(\Sigma)$. For $c^i \in C^i(\Sigma)$, $c_i \in C_i(\Sigma)$, we let $(c^i, c_i) := c^i(c_i)$.

For $i = 1, 2$, we define the coboundary maps $\delta_i : C^{i-1}(\Sigma) \to C^i(\Sigma)$ to be the dual homomorphism of ∂_i, that is, for every $c^{i-1} \in C^{i-1}(\Sigma)$ and $c_i \in C_i(\Sigma)$ we have $(\delta c^{i-1}, c_i) := (c^{i-1}, \partial c_i)$. Clearly, again omitting indices,

$$\delta^2 = 0. \tag{90}$$

The set of cocycles and coboundaries are, respectively, $Z^1(\Sigma) := \ker \delta_2$ and $B^1(\Sigma) := \mathrm{ran}\, \delta_1$. The first cohomology group is

$$H^1(\Sigma) := Z^1(\Sigma)/B^1(\Sigma). \tag{91}$$

Since they will be of interest when studying homological quantum error correcting codes, we collect here the following dual pair of properties. For any $c_1 \in C_1$ and $c^1 \in C^1$,

$$\forall v \in V(\delta v^*, c_1) = 0 \Leftrightarrow c_1 \in Z_1, \tag{92}$$

$$\forall f \in F(c^1, \partial f) = 0 \Leftrightarrow c^1 \in Z^1. \tag{93}$$

Also

$$\forall v \in V, \forall f \in F \quad (\delta v^*, \partial f) = 0. \tag{94}$$

We say that $(\delta v^*, \cdot)$ is a *star operator* and that $(\cdot, \partial f)$ is a *boundary operator*, reflecting their geometrical nature. The name of the boundary operator is clear enough, but perhaps the star operator deserves some explanation. Let the star of a vertex v be the set

$$\mathrm{star}(v) := \{(e,\sigma) \in E \times \{1,-1\} | I_i(e^\sigma) = v\}. \tag{95}$$

Then we have

$$\delta v^* = \sum_{(e,\sigma) \in \mathrm{star}(v)} \sigma e^*. \tag{96}$$

D. Surfaces

For a *surface* we understand a compact connected two-dimensional manifold. We already encountered several examples of surfaces constructed with 2-complexes, namely, S, T, and P. It is a fundamental result of surface topology that every other surface can be obtained by combination of these three; let us explain what is meant here by combination.

Consider two surfaces, M_1 and M_2. Let D_i, $i=1,2$, be a subset of M_i homeomorphic to a closed disk and let its boundary be ∂D_i. Let $h: \partial D_1 \to \partial D_2$ be a homeomorphism. The *connected sum* of M_1 and M_2, denoted $M_1 \sharp M_2$, is defined as the quotient space of the disjoint union $(M_1 - \mathring{D}_1) \cup (M_2 - \mathring{D}_2)$ under the identifications $x \sim h(x)$ for $x \in \partial D_1$. Here $\mathring{D}_i$ denotes the interior of D_i. $M_1 \sharp M_2$ is a surface, and its homeomorphism class depends only upon the homeomorphism classes of M_1 and M_2. To gain intuition, Fig. 13 shows a connected sum of two tori to give a 2-torus.

Let the Moëbius band B be the topological space obtained as the quotient space of $[0,1] \times [0,1]$ under the identifications $[0,x] \sim [1,1-x]$. For a picture, see Fig. 14. A surface is said to be *orientable* if it does not contain a subset homeomorphic to B. A surface is embeddable without self-intersections in $\mathbf{R}^3$ iff it is orientable. S and T are orientable, but P is not. Define recursively $gP := (g-1)P \sharp P$ for $g > 1$ and $1P := P$. Let also $gT := (g-1)T \sharp T$ for $g > 0$ and $0T := S$. No two of them are homeomorphic. gP is the sphere with n crosscaps and gT is the sphere with g handles or g-torus. gT and gP are said to have *genus* g.

Proposition 3. *Any orientable surface is homeomorphic to* gT *for some integer* $n \geq 0$. *Any nonorientable surface is homeomorphic to* gP *for some integer* $n \geq 1$.

See, for example, Ref. 67 for a proof. We already presented above the standard 2-complexes representing P and T. gP can be represented by the 2-complex consisting of a vertex v, n edges $\{a_1, \ldots, a_n\}$, and a face f with $B(f) = [a_1, a_1, \ldots, a_n, a_n]$. gT can be constructed with a vertex v, $2n$ edges $\{a_1, b_1, \ldots, a_n, b_n\}$, and a face f with $B(f) = [a_1, b_1, a_1^{-1}, b_1^{-1}, \ldots, a_n, b_n, a_n^{-1}, b_n^{-1}]$. Note that $\chi(gT) = 2(1-g)$ and $\chi(gP) = 2-g$. The corresponding homology and cohomology groups are

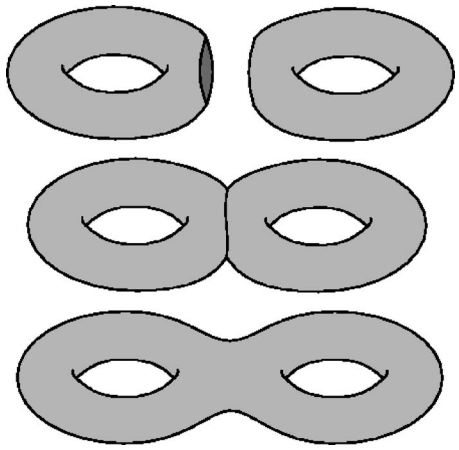

FIG. 13. The connected sum of two tori to give a 2-torus in three steps: cutting, gluing, and smoothing out.

$H_1(gT) \simeq H^1(gT) \simeq \mathbf{Z}^{2g}$ and $H_1(gP) \simeq H^1(gP) \simeq \mathbf{Z}^{g-1} \oplus \mathbf{Z}_2$. The subgroup $\mathbf{Z}_2$ appearing in the first homology group of nonorientable surfaces is called the torsion subgroup. It will play an important role when homological quantum error correcting codes for qudits of dimension greater than 2 are considered.

Consider a topological graph Γ embedded in a surface M, that is, a homeomorphism between Γ and a subset of M. When $M-\Gamma$ is a union of disks, we say that the embedding is a cell embedding. Clearly, such an embedding leads to a 2-complex whose faces are the mentioned disks. This raises the question of how to characterize combinatorially whether a 2-complex Σ represents a surface or not. It is enough to give a condition such that for each vertex the corresponding point for the represented topological space has a neighborhood isomorphic to a disk. Let us first define the index of face $f \in F$ on the "corner" described by the ordered pair (e,e'), where $e,e' \in \bar{E}$ and $I_t(e)=I_s(e')$. In plain words, the index counts the number of times that the walk $B(f)$ goes across the corner (e_1,e_2). Formally, let $B(f)=[e_0,\ldots,e_{k-1}]$ and

$$s_{e,e'} := |\{i \in \mathbf{Z}_k | e = e_i \text{ and } e' = e_{i+1}\}|; \tag{97}$$

(98)

then the index of f in (e,e') is

$$\text{index}(f,e,e') = \begin{cases} s_{e,e'} + s_{e'^{-1},e^{-1}} & \text{if } e^{-1} \neq e' \\ s_{e,e'} & \text{if } e^{-1} = e'. \end{cases} \tag{99}$$

So let $v \in V$ be a vertex and let $k := |\text{star}(v)|$. We say that v is a surface vertex if there exists a cyclic k-tuple $S(v)=[e_0^{\sigma_0},\ldots,e_{k-1}^{\sigma_{k-1}}]$ such that $\text{star}(v)=\{(e_i,\sigma_i)\}_{i=0}^{k-1}$ and

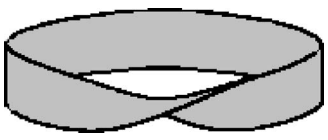

FIG. 14. The Moëbius band.

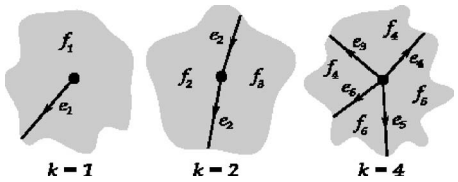

FIG. 15. An illustration of the definition of surface vertex and the expressions (99) and (100). We have, for example, $\mathrm{index}(f_1,e_1,e_1^{-1})=1$, $\mathrm{index}(f_2,e_2,e_2)=1$, and $\mathrm{index}(f_4,e_3^{-1},e_4)=1$.

$$\sum_{f\in F}\mathrm{index}(f,e_i^{\sigma_i},e_j^{-\sigma_j})=\begin{cases}1 & \text{if } k=1\\ 2 & \text{if } k=2, j-i\equiv 1\\ 1 & \text{if } k>2, j-i\equiv \pm 1\\ 0 & \text{in other case,}\end{cases} \tag{100}$$

where $\equiv$ is equality modulo k. Figure 15 illustrates the concept. Then, as a definition, a surface 2-complex is a connected 2-complex such that all its vertices are surface vertices. We also need a way to distinguish orientability. We say that a surface 2-complex is oriented if

$$\sum_{f\in F}\partial f=0. \tag{101}$$

A surface 2-complex for which there is a suitable sign selection for faces so that it is oriented is said to be orientable. Figure 16 clarifies this definition.

An interesting notion that emerges when considering the cell embedding of a graph in a surface is that of duality. The germ of this idea can be traced back to the five regular platonic solids. Each of these polyhedra has a dual polyhedron whose vertices are the center points of the given one. For example, the tetrahedron is self-dual and the cube and the octahedron are dual of each other. The idea can be generalized. Given a cell embedding of a graph Γ in the surface M, the dual embedded graph Γ^* is constructed as follows. For each face f a point f^* is chosen to serve as a vertex for the new graph. For each edge e lying on the boundary of the faces f_1 and f_2, the edge e^* connects f_1^* and f_2^* crossing e once but no other edge or dual edge. Figure 17 shows a pair of examples.

We now work out duality in the context of surface 2-complexes. Consider an oriented surface 2-complex $\Sigma=(V,E,F,I_s,I_t,B)$. We construct the dual 2-complex $\Sigma^*=(V'=F^*,E'=E^*,F'=V^*,I_s',I_t',B')$ where $V^*:=\{v^*|v\in V\}$ and so on. There is a unique $f\in F$ such that $(e^*,\partial f)=1$ (respectively -1) and we set $I_s'(e)=f^*$ [respectively $I_t'(e)=f^*$]. For each $v\in V$, let $S(v)=[e_0^{\sigma_0},\ldots,e_{k-1}^{\sigma_{k-1}}]$ be the cyclic k-tuple from the definition of surface 2-complexes. Then $B'(v^*)=[e_0^{*\sigma_0},\ldots,e_{k-1}^{*\sigma_{k-1}}]$. Now let the operator d take v to v^*, e to e^*, and f to f^*. Extend d linearly to act on any chain. Now, if we denote ∂^* and δ^* the ∂ and δ operators for Σ^*, we have

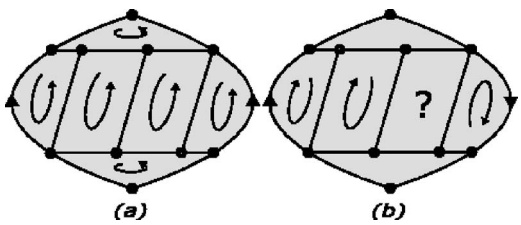

FIG. 16. Two planar representations of 2-complexes for (a) the sphere S and (b) the projective plane P. The identified vertices and edges are the same as in Fig. 11. S is shown with its faces oriented. On the other hand, P is not orientable. The picture shows an attempt to give a coherent orientation and the failure. Note that the impossibility comes from the presence of a Moëbius band. It consists of the faces already oriented and the one with the interrogation sign.

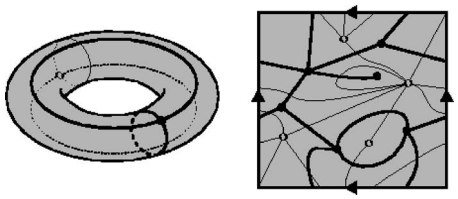

FIG. 17. (a) The standard cell embedding in the torus. The thin lines represent the dual graph. Notice self-duality. (b) A more complicated graph embedded in the torus and its dual. The torus is recovered from the plane model by identification of opposite edges.

$$\delta^* d = d\partial, \quad d\partial^* = \delta d, \tag{102}$$

where the domains must be defined in the apparent way so that the composed function is well defined. Finally, we observe that Σ^* is oriented and $\Sigma^{**} \simeq \Sigma$. If one wants to extend the notion of duality to nonorientable surface 2-complexes, $\mathbf{Z}_2$ homology must be considered in order to eliminate orientation-related problems. We shall not dwell upon this here, however.

Let us enlarge a bit the concept of surface. Take a surface M and a finite collection of disjoint sets $\{D_i\}$ such that each of them is homeomorphic to a disk. We say that $M - \cup_i \mathring{D}_i$ is a *surface with boundary*. We already encountered an important example of such an object, namely, the Moëbius band B. If one attaches to B a disk identifying homeomorphically its boundary with the rim of B, the projective plane P is obtained. We again need a combinatorial definition. Let Σ be a surface 2-complex and $F' \subset F$ a collection of faces with no edge or vertex in common along the boundary walk. We say that $\Sigma' := (V, E, F - F', I_s, I_t, B)$ is a surface with boundary 2-complex. It is quite tempting to atempt an extension of duality to this broader class of 2-complexes. As the dual of a face is a vertex, it is apparent that the dual of a surface with boundary would be a "surface with missing points." Such an object is not a 2-complex, however. To overcome this difficulty, relative homology can be considered. The relative homology of a complex with respect to certain subcomplex is a topic in which we shall not enter, but it is worth mentioning that it would be perfectly suited to the error correcting code construction. Another possibility is to construct the dual of a surface with boundary by identifying the correspondending vertices instead of deleting them. This construction leads us to what is called a pseudosurface, a "surface" which fails to be such a thing only in a finite set of points. From a homological point of view, the result is equivalent. See Fig. 18.

For us the most important example of surface with boundary will be the h-holed disk D_h, $h \geqslant 1$. As a 2-complex, D_h can be constructed with $h+1$ vertices, $2h+1$ edges, and 1 face. Instead of giving explicitly the construction, we prefer to illustrate it with an example in Fig. 19. We have $H_1(D_h) \simeq H^1(D_h) \simeq \mathbf{Z}^h$ and $\chi(D_h) = 1 - h$. The point of these perforated disks is that they have a nontrivial homology while still being a subset of the plane, something that we will find useful when physics come into play.

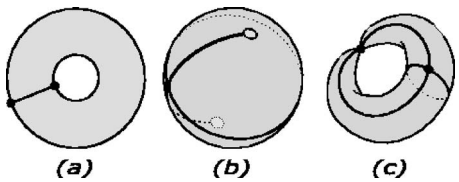

FIG. 18. (a) A 2-complex representing the disk with a hole, D_1. (b) The dual of D_1 in the form of a sphere with two vertices missing. (c) Another possibility for the dual of D_1, obtained by identifying the missing vertices of the previous sphere.

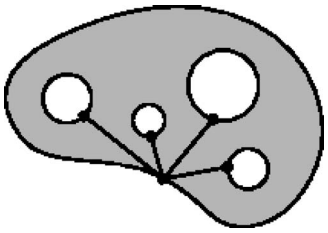

FIG. 19. A 2-complex representing the disk with four holes.

E. Quantum homological codes

From this point on we will be working with qudits of fixed dimension D. Unless otherwise stated, the homology considered will be always homology with coefficients in $\mathbf{Z}_D$.

Before introducing homological quantum error correcting codes we still need a pair of definitions. Given a 2-complex Σ, let $E=\{e_i\}_{i=1}^{|E|}$. Consider the isomorphisms $\mathbf{h}_1: C_1(\Sigma)\to\mathbf{Z}_D^{|E|}$ and $\mathbf{h}_2: C^1(\Sigma)\to\mathbf{Z}_D^{|E|}$ defined by

$$\mathbf{h}_1\left(\sum_{i=1}^{|E|}\lambda_i e_i\right) := (\lambda_0,\lambda_1,\ldots,\lambda_{|E|}), \tag{103}$$

$$\mathbf{h}_2\left(\sum_{i=1}^{|E|}\lambda_i e_i^*\right) := (\lambda_0,\lambda_1,\ldots,\lambda_{|E|}). \tag{104}$$

Let $\mathbf{h}: C_1(\Sigma)\cup C^1(\Sigma)\to\mathbf{Z}_D^{2|E|}$ be

$$\forall c_1 \in C_1(\Sigma), \quad \mathbf{h}(c_1) := (\mathbf{0}\mathbf{h}_1(c_1)), \tag{105}$$

$$\forall c^1 \in C^1(\Sigma), \quad \mathbf{h}(c^1) := (\mathbf{h}_2(c^1)\mathbf{0}). \tag{106}$$

Then

$$\mathbf{h}_2(c^1)\cdot\mathbf{h}_1(c_1) = \mathbf{h}(c^1)^t\Omega\mathbf{h}(c_1) = (c^1,c_1). \tag{107}$$

It is natural to use the notation $\sigma_{c_1} := \sigma_{\mathbf{h}(c_1)}$ and $\sigma_{c^1} := \sigma_{\mathbf{h}(c^1)}$ so that

$$\sigma_{c^1}\sigma_{c_1} = \varphi((c^1,c_1))\sigma_{c_1}\sigma_{c^1}. \tag{108}$$

As we did for graphs, we can pull back the weight function through $\mathbf{h}_1$ and $\mathbf{h}_2$. Then we let the distance $d(\Sigma)$ be the minimal weight among the representatives of nontrivial elements of H_1 and H^1.

Theorem 4: *Let Σ be a connected 2-complex. If*

$$V := \mathbf{h}[B^1(\Sigma)]\oplus\mathbf{h}[B_1(\Sigma)] \tag{109}$$

is generated by a linearly independent set, then setting $V_C=V$ a symplectic $[[n,k,d]]$ quantum error correcting code $\mathcal{C}$ is obtained with $n=|E|$, $H_1(\Sigma)\simeq H^1(\Sigma)\simeq\mathbf{Z}_D^k$, and $d=\mathrm{d}(\Sigma)$.

Proof: The isotropy of $V_{\mathcal{C}}$ follows from Eqs. (94) and (107). Also, from Eq. (92) we get $\mathbf{h}_1[Z_1(\Sigma)]=\mathbf{h}_2[B^1(\Sigma)]^\perp$ and $\mathbf{h}_2[Z^1(\Sigma)]=\mathbf{h}_1[B_1(\Sigma)]^\perp$, that is,

$$\hat{V}_{\mathcal{C}} = \mathbf{h}[Z^1(\Sigma)]\oplus\mathbf{h}[Z_1(\Sigma)]. \tag{110}$$

But $\dim\hat{V}_{\mathcal{C}}-\dim V_{\mathcal{C}}=2k$, and since $\dim\mathbf{h}_1[Z_1(\Sigma)]+\dim\mathbf{h}_2[B^1(\Sigma)]=\dim\mathbf{h}_1[B_1(\Sigma)]+\dim\mathbf{h}_2[Z^1(\Sigma)]$ we get as desired $H_1(\Sigma)\simeq H^1(\Sigma)\simeq\mathbf{Z}_D^k$. As for the distance, we recall the expres-

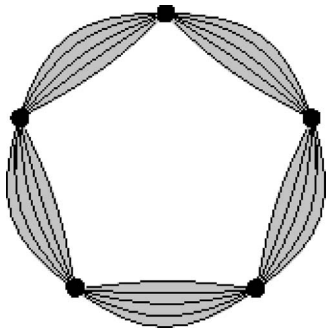

FIG. 20. A 2-complex giving rise to a [[25,1,5]] code.

sion for the code distance given in Eq. (68) and observe that a vector in $\hat{V}_C$ and not in V_C is of the form $\mathbf{h}(c_1)+\mathbf{h}(c^1)$ with c_1 or c^1 homologically nontrivial.

□

The condition that Σ be connected is just to avoid having a code which can be decomposed into two more simple ones. As for graphs, there is no point at all in considering disconnected 2-complexes; given such a disconnected 2-complex with components Σ_i one can consider the wedge product of them, $\vee_i\Sigma_i$, giving raise to the same code. The wedge product is obtained by choosing one vertex from each component and identifying them all.

Because of the condition stating that the subspace (109) must be a linear subspace with a basis which is a linearly independent set in $\mathbf{Z}_D^{2n}$, not every 2-complex can be used to produce codes for general qudits. For example, consider the case $D=4$ in P, the projective plane. In this case $H_1 \simeq \mathbf{Z}_2$ and thus a code cannot be constructed. The origin of the problem is in the torsion subgroup appearing in nonorientable surfaces. However, we can get rid of it if we only consider the case $D=2$ in this surfaces, as we shall do. Under this assumption and restricting attention to surface 2-complexes, we can give a more geometrical definition for the distance. Let Σ be a surface 2-complex, and let Γ be its graph. Let also $\mathrm{Cy}'(\Gamma)$ be the set of simple subcycles of Γ not homologous to a point, and $\mathrm{d}'(\Sigma)$ the minimal length among the elements of $\mathrm{Cy}'(\Gamma)$. Then

$$d(\Sigma) = \min\{d'(\Sigma), d'(\Sigma^*)\}. \tag{111}$$

To gain intuition on the construction of the codes, consider the special case of a graph as a 2-complex. In this case we obtain a pseudoclassical code, capable of correcting errors of the form $\sigma_{\mathbf{x}0}$ whenever $\mathbf{x}$ is correctable in the corresponding classical code.

It is possible to construct homological quantum codes inspired by classical ones. Consider for example, the graphs C_d, related to $[d,1,d]$ classical linear codes. Joining d copies of C_d along vertices and attaching $d(d-1)$ faces, as shown in Fig. 20, gives a $[[d^2,1,d]]$ code. In particular, for $d=3$ we get Shor's original [[9, 1, 3]] code. Unfortunately, $\lim_{d\to\infty} d/n=0$, which is very different to the classical case. This first example already shows that the length of quantum homological codes does not seem to behave very well when the distance grows. However, below we show that this is not the case when k grows.

In general, homological quantum codes can be degenerate. It is enough to have a vertex lying in less than $d/2$ edges or a boundary with less than $d/2$ edges to have degeneracy. Such examples of degenerate codes will show up in the next section.

F. Surface codes

In this section we study homological quantum codes derived from 2-complexes representing surfaces. Such 2-complexes are usually regarded as cell embeddings of graphs on surfaces, and so we will tend to use the language of topological graph theory. Note that the genus is directly related to the number of encoded qudits; codes derived from gT encode $k=2g$ qudits, and codes derived

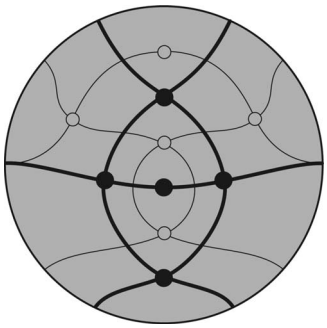

FIG. 21. A self-dual cell embedding in P. The projective plane is recovered by identifying opposite edges of the circumference. This embedding leads to a [[9,1,3]] code for qubits.

from gP encode $k=g$ *qubits*. This can be put altogether using the Euler characteristic; cell embeddings of graphs on a surface M will give codes with

$$k = 2 - \chi(M). \tag{112}$$

As a first example of a surface code, Fig. 21 shows a self-dual embedding on P giving a [[9, 1, 3]] code.

The whole problem of constructing good codes related to a certain surface relies on finding embeddings of graphs in such a way that both the embedded graph *and* its dual have a big distance whereas the number of edges keeps as small as possible. But let us be more accurate.

Definition 5: *Given a surface M and a positive integer d we let the quantity $\mu(M,d)$ be the minimum number of edges among the embeddings of graphs in M giving a code of distance d.*

Since we do not know how to calculate the value of the function μ, we shall investigate some properties of this function. The problem of locality suggests also the introduction of a refinement of μ; the quantity $\mu_l(M,d)$ is defined as $\mu(M,d)$ but with the restriction that the graphs can have faces with at most l edges and vertices lying on at most l edges. Locality here means that we want that the vertex $\sigma_{\delta v}$ and face $\sigma_{\partial f}$ operators act on at most l qudits. Having operators as local as possible simplifies the error correction stage. We shall return on this issue below.

We stress that in the case of nonorientable surfaces we *only* consider $\mathbf{Z}_2$ homology. Keeping this in mind, we can state the following.

Theorem 6: *The function $\mu(M,d)$ is subadditive in its first argument, in the sense that given two surfaces M_1 and M_2*

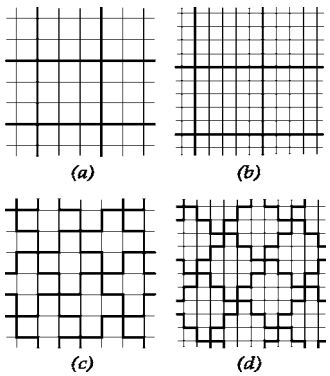

FIG. 22. A graphical comparison between the original toric codes and their optimized versions. The thick lines are the border of tesserae and the torus is recovered as a quotient of the plane and its tessellation. [(a) and (b)] The toric codes introduced in Ref. 19, for $d=3$ and $d=5$. [(c) and (d)] The optimal regular toric codes for $d=3$ and $d=5$.

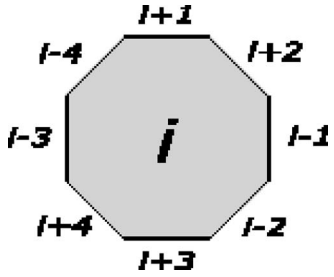

FIG. 23. The self-dual embedding of K_9 in the 10-torus can be described using addition in $\mathbf{Z}_9$. It is enough to label the eight-sided faces with $i=0,\ldots,8$ and glue them altogether as the picture indicates.

$$\mu(M_1 \sharp M_2, d) \leqslant \mu(M_1, d) + \mu(M_2, d). \tag{113}$$

The proof is given in Appendix B.

The most simple orientable surface with nontrivial first homology group is the torus. In Ref. 19, a family of so-called toric codes was presented, in the form of self-dual regular lattices on the torus. An investigation on other regular lattices on the torus led us to another system of lattices that demand half the number of qudits whereas it keeps the same good properties as the the first one; in particular, vertex and face operators act on four qudits. In fact, in Ref. 19 only qubits were considered. Examples of both systems of lattices are depicted in Fig. 22, where the torus is represented as a quotient of the plane through a tessellation. In Appendix C we show the optimality of our system. The original toric codes lead to a family of $[[2d^2, 2, d]]$ codes. Our lattices give $[[d^2+1, 2, d]]$ codes. This already shows that

$$\mu(T, d) \leqslant \mu_4(T, d) \leqslant d^2 + 1. \tag{114}$$

Invoking subadditivity, we learn that $\mu(gT, d)$ is $O(x^2)$ in its second argument, that is, it grows at most cuadratically with d.

A closer examination of Fig. 22 reveals that the lattice giving a [10,2,3] code is a self-dual embedding of K_5. This suggests considering self-dual embeddings of K_s, since such an embedding would give a $\left[\left[\binom{s}{2}, \binom{s}{2} - 2(s-1), 3\right]\right]$ code, see Fig. 23. In fact, these embeddings are possible in orientable surfaces with the suitable genus as long as $s \equiv 1 (\mathrm{mod}\ 4)$,[68] and this family of codes with self-dual embeddings of complete graphs is enough to show that the coding rate k/n behaves as

$$\lim_{k\to\infty} \frac{k}{n} = \lim_{g\to\infty} \frac{2g}{\mu(gT, 3)} = 1. \tag{115}$$

In order to verify this, note first that $\mu(gT, d) \geqslant \mu(gT, 1) = 2g$. Let $K(s) = \binom{s}{2} - 2(s-1)$. Due to subadditivity, for $K(s)/2 \leqslant g < K(s+1)/2$ we have $\mu(gT, 3) \leqslant \mu((K(s)/2)T, 3) + (g - (K(s)/2))\mu(T, 3) = \binom{s}{2} + O(s)$.

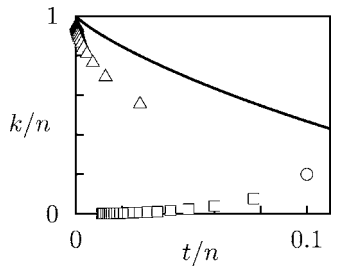

FIG. 24. The rate k/n vs t/n for the codes derived from self-dual embeddings of the complete graphs K_{4l+1} (△) and for the optimized toric codes (□); ○ corresponds to the embedding of K_5 in the torus. The quantum Hamming bound is displayed as a reference (solid line).

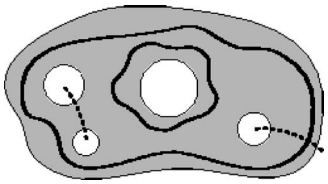

FIG. 25. Examples of noncorrectable errors in D_4. For clarity, the embedded graph is not shown. The thick lines represent typical elements of H_1, that is, cycles in the direct graph not homologous to zero. The dashed lines are elements of H^1, in the form of cycles in the dual graph.

The limit (115) shows that the ratio k/n is asymptotically 1, and thus good codes can be constructed using surfaces. Figure 24 displays the rates for this family of codes and also for the optimized toric codes. The differences with Fig. 7 are apparent.

G. Planar codes

We now focus on homological quantum codes derived from 2-complexes representing surfaces with boundary. The situation is similar to the previous section and again we talk about cell embeddings of graphs. Note that for such a cell embedding of a graph on a surface with boundary, the boundaries are a subset of the graph.

Surfaces with boundary offer more possible topologies to encode the same amount of qudits. If we remove from a g-torus l nonadjacent faces, H_1 is enlarged with $l-1$ dimensions; removing a single face is useless since its boundary is a linear combination of the boundaries of the remaining faces. The nonorientable case is similar, because we only consider $\mathbf{Z}_2$ homology. The results can again be collected using the Euler characteristic; given a surface with boundary M, not a surface, cell embeddings of graphs on it will give codes with

$$k = 1 - \chi(M). \tag{116}$$

It is time to return on the issue of locality. Although topological codes are local, one has to face the problem of constructing a physical system with the shape of the surface on which the code lyes. At this point, the problem of nonplanarity arises; surfaces with nontrivial first homology group are not a subset of the plane, and so are difficult to realize experimentally. Among surfaces with boundary, however, there *is* such a planar family: the disks with h holes, D_h, which encode h qudits. Figure 25 displays the shape of noncorrectable errors in D_h.

An interesting point is that cell embeddings in gT giving codes of distance d can be transformed to obtain cell embeddings in D_{2g-1}. The idea is to cut each of the handles of the torus, as shown in Fig. 26. The cut must be performed along a simple cycle of the graph, and so the edges of the cycle are duplicated in the process. This means that each cut introduces at least d new edges in the graph. On the other hand, the whole procedure produces the lost of a single encoded qudit. A fundamental drawback of this method is that cocycles of length less than d could appear, thus diminishing the distance of the code. In such a case some additional edges could be added. However, it is also very possible that some edges become unnecessary after the cut: Fig. 27 shows an example.

FIG. 26. How to cut a torus of genus 2 to obtain a surface with boundary homeomorphic to a disk with three holes.

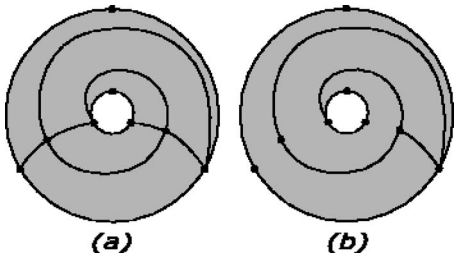

FIG. 27. (a) The result of cutting the self-dual embedding of K_5 in T. (b) Some of the edges of the previous embedding can be deleted and still obtain a code of distance 3.

Another possible drawback of the cutting procedure is that the resulting embedding could be quite odd shaped, and thus perhaps not very useful when true locality is necessary. In any case, one can always switch to more regular embeddings if the number of edges is unimportant. Figure 28 displays such an embedding.

It is possible to remove the condition that all faces must be homeomorphic to disks. In that case we are not dealing anymore with homology, but errors can still be visualized in a similar fashion. For example, Shor's [9,1,3] is displayed in Fig. 29.

IV. CONCLUSIONS

Quantum topology holds the promise of providing a mechanism for self-correcting errors without having to resort to constantly monitoring a quantum memory for error syndrome and error fixing. In this fashion, the functioning of a quantum memory would very much resemble the robustness of its classical counterpart. This is the main reason why it is very important to study quantum error correcting codes from a quantum topological point of view. In this paper we have acomplished this task by developing theorems characterizing homological quantum codes for qudits of arbitrary dimension D based on graphs embedded in surfaces of arbitrary topology, either with or without boundaries, orientable or nonorientable. Orientability becomes an issue when trying to construct homological quantum codes using qudits of dimension $D \geqslant 3$, due to the existence of a nontrivial torsion subgroup in the homology group.

In doing so, we have realized that homological codes can also be well defined in the classical case. This is interesting since not every classical code is of homological type. Nevertheless, we find that there exists a family of classical homological codes saturating the classical Hamming bound.

As a result of our work, we have found that the problem of constructing good quantum homological codes on arbitrary surfaces relies on finding embeddings of graphs in such a way that both the embedded graph and its dual graph have a big distance whereas the number of edges

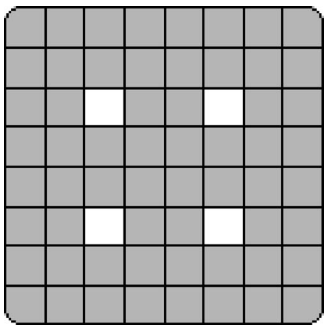

FIG. 28. An example of an embedding in D_4. The corresponding code has distance 3 and encodes four qudits. It is not difficult to generalize this embedding for general d and k; asymptotically the resulting code has $n \propto kd^2$. As usual, the growth is quadratic in d and linear in k.

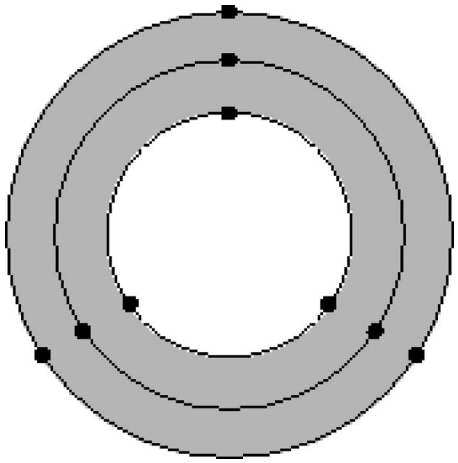

FIG. 29. A visualization of Shor's[9,1,3] code. It can also be considered as an embedding in the torus, since one face can be added for free.

keeps as small as possible. This provides a connection between the theory of quantum topological codes and topological graph theory.[68] More specifically, the problem of finding topological quantum codes is an instance of extremal graph theory which deals with the problem of finding maxima/minima of certain quantities defined on graphs. In our case, it is the distance of a quantum code which has to be maximal on both the embedded graph and its dual. We have given an asymptotically optimal family of codes for the case of distance $d=3$. We leave open the challenge of giving such optimal constructions for higher d.

Finally, we want to point out that our results on quantum homological error correction have further consequences in other areas of quantum information such as quantum channel capacities. In particular, our optimality results may have implications for finding bounds on those capacities. This application is possible, thanks to the result that it is possible to send a nonvanishing amount of quantum data undisturbed through a noisy quantum channel, provided the errors produced by this channel are small enough.[69]

ACKNOWLEDGEMENTS

We acknowledge financial support from a PFI fellowship of the EJ-GV [to one of the authors (H.B.)], DGS grant under Contract No. BFM 2003-05316-C02-01 [to the other author (M.A.M.D.)] and CAM-UCM grant under Ref. No. 910758.

APPENDIX A: GENERATORS OF $Sp_D(n)$

In order to proof that the homomorphism h introduced in Eq. (60) is onto, it is enough to exhibit a subset $S \subset ESp_D(n)$ such that $h[S]$ generates $Sp_D(n)$. We consider the following.

- The Fourier operator on one qudit

$$\mathcal{F} := \sum_{k,l \in \mathbf{Z}_D} \varphi(kl)|k\rangle\langle l|, \tag{A1}$$

$$\mathcal{F}X\mathcal{F}^\dagger = Z, \quad \mathcal{F}Z\mathcal{F}^\dagger = X^{-1}. \tag{A2}$$

- The operator on one qudit

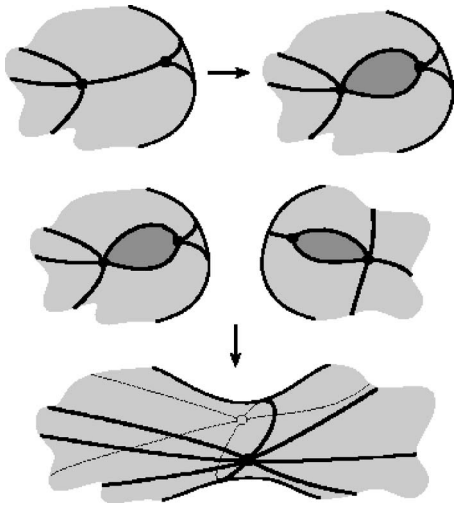

FIG. 30. The construction used to proof the subadditivity of μ. The first step is to perform a cut along a selected edge in each of the embeddings to be added. Then the resulting boundaries must be identified.

$$K := \sum_{k \in \mathbf{Z}_D} f(1)^k \varphi\left(\frac{k(k+1)}{2}\right) |k\rangle\langle k|, \tag{A3}$$

where the argument of φ must be evaluated in $\mathbf{Z}$;

$$KXK^\dagger = f(1)XZ, \quad KZK^\dagger = Z. \tag{A4}$$

- The controlled NOT operator on two qudits

$$U_{\mathrm{CNot}} := \sum_{k,l \in \mathbf{Z}_D} |k,l\rangle\langle k,k+l|; \tag{A5}$$

$$U_{\mathrm{CNot}} X^i \otimes X^j U_{\mathrm{CNot}}^\dagger = X^i \otimes X^{i+j}, \tag{A6}$$

$$U_{\mathrm{CNot}} Z^i \otimes Z^j U_{\mathrm{CNot}}^\dagger = Z^{i-j} \otimes Z^j. \tag{A7}$$

The images under h of these operator on the first qudit(s) plus any qudit permutation generate $Sp_D(n)$.[62]

APPENDIX B: TOPOLOGICAL SUBADDITIVITY OF μ

We proof Theorem 6. The assertion is quite trivial in the case $d=1$. In order to proof it for $d \geqslant 2$, it is enough to construct an embedding of distance d in $M_1 \sharp M_2$ starting with two embeddings of distance d in M_1 and M_2 in such a way that the number of edges does not increase; see Fig. 30. So let Σ_1 and Σ_2 be 2-complexes of distance d representing, respectively, M_1 and M_2. We can suppose that neither of them is a sphere. Since $d \geqslant 2$, there exists an edge e_1 in E_{Σ_1} which is not a self-loop. Let f_1 be a face such that $B_{\Sigma_1}(f)=[\sigma e_1, a, b, \ldots]$, $\sigma \in \{1,-1\}$. We construct a new 2-complex Σ_1' introducing in Σ_1 a new edge e_1' with the same source and target as e_1 and changing the boundary of f_1 so that $B_{\Sigma_1'}(f_1)=[\sigma e_1', a, b, \ldots]$. We proceed in the same manner with Σ_2. Up to this point, we have performed the cutting step of Fig. 13 and constructed two surfaces with boundary, Σ_1' and Σ_2'. Then we construct Σ as a union of Σ_1' and Σ_2' but identifying e_1 and e_2 in a single edge e, and similarly for their primed versions. Of course, the end points of e_1 and e_2 must be properly identified also, but the construction is clear enough so as to be self-explanatory. The resulting 2-complex is a surface, and that it represents the expected one follows from the two

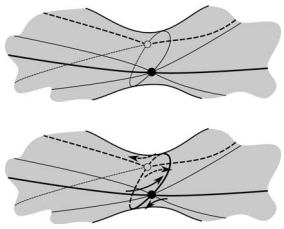

FIG. 31. A simple cycle over the connected sum is divided into two, with each new simple cycle in one of the initial surfaces.

facts: it is orientable iff both Σ_1 and Σ_2 are orientable and $\chi(\Sigma)=\chi(\Sigma_1)+\chi(\Sigma_2)-2$. We still have to check that its distance is d. The key observation is that $e-e'$ is a boundary, in particular, the boundary of the sum of all the faces in Σ_1', properly oriented in the orientable case. Consider, for example, a simple cycle not homologous to zero that contains edges both from $E_{\Sigma_1'}-\{e,e'\}$ and $E_{\Sigma_1'}-\{e,e'\}$; see Fig. 31. It must pass through each end point $\{v_1,v_2\}$ of e exactly once. Then we can construct two simple cycles γ_1 and γ_2 contained, respectively, in Γ_1' and Γ_2'. To this end we "cut" γ in v_1 and v_2 and glue again one of the pieces with e and the other with e'. At least one of the new simple cycles, say γ_1, is not homologous to zero in Σ, and thus in Σ_1'. Then its length is at least d, and the same is then true for the length of γ. Other possible simple cycles, including those in the dual graph, can be similarly worked out.

APPENDIX C: OPTIMAL SELF-DUAL REGULAR TORIC CODES

Let a cell embedding of a simplicial graph on a surface be a (v,f) regular cell embedding if the star of any vertex comprises v edges and the boundary of any face consists of f edges. On the torus, only the combinations (4,4), (3,6), and (6,3) are possible, since Euler's characteristic must be zero. We shall investigate here the self-dual case, (4,4). In particular, given a distance $d=2t+1$, we want to know which is the minimum number of edges in a (4,4) regular cell embedding on the torus such that its distance is d.

We shall answer the question using homotopy. We say that an n-tuple $w=(e_1,\ldots,e_n)$, $e_i\in\bar{E}$, is a walk of length n if $I_t(e_i)=I_s(e_{i+1})$, $i=1,\ldots,n-1$. Its inverse is $w^{-1}=(e_n^{-1},\ldots e_1^{-1})$. The empty walk is also a walk. If $w=(\ldots,e_n)$ and $w'=(e_1',\ldots)$ are such that $I_t(e_n)=I_s(e_1)$, then the composed walk is $w+w'=(\ldots,e_n,e_1',\ldots)$. If a walk is of the form $w=w_1+w_2+w_3$, and the boundary of a face (or its inverse) can be expressed as a walk as $b=w_2+w_4$, then we say that w and $w'=w_1+w_4^{-1}$

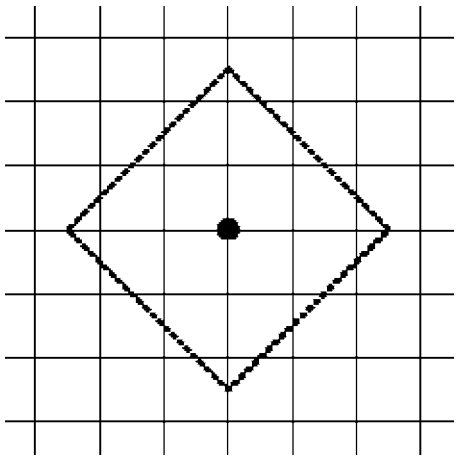

FIG. 32. An infinite square lattice on the plane. The vertices inside the dashed square are at most at distance 2 from the distinguished one.

$+w_3$ are homotopic and write $w \sim w'$. On a given embedding of a graph, we can choose any vertex v as a base point and consider the walks starting at v under the equivalence just stated. The resulting equivalence classes are the vertices of a new graph, naturally embedded in the universal cover of the surface under consideration.

In the case of (4,4) regular cell embeddings in the torus, the resulting graph is an infinite square lattice on the plane, as in Fig. 32. Let Γ be the original graph on the torus and Γ' the obtained graph on the plane. There is a natural projector $p:\Gamma' \to \Gamma$ taking vertices to vertices and edges to edges. Let v be the distinguished vertex in Γ' representing the class of walks homotopic to a point. As in Fig. 32, we can consider the set of vertices at a distance at most t from v. If two of them have equal projections, say $p(v_1)=p(v_2)$, then there exists a walk going from v_1 to v_2 of length less or equal to $2t$ such that its projection in Γ is not homotopic to a point. On a torus, this also means that it is not homologous to zero. Therefore, if Γ has distance $d=2t+1$, no such two vertices can exist. This means that Γ must have at least $(d^2+1)/2$ vertices, and thus at least d^2+1 edges. As this minimal size is attained by the embeddings of Sec. III F, we have the desired result.

[1] R. Landauer, Philos. Trans. R. Soc. London, Ser. A **353**, 367 (1995).
[2] R. Landauer, Phys. Lett. A **217**, 188 (1996).
[3] R. Landauer, in *Proceedings of Drexel-4 Symposium on Quantum Nonintegrability-Quantum-Classical Correspondence, Philadelphia, PA, 8 September 1994*, edited by D. H. Feng and B.-L. Hu (International Press, Boston, MA, 1997).
[4] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).
[5] P. Shor, Phys. Rev. A **52**, 2493 (1995).
[6] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[7] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[8] A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[11] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[12] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996).
[13] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[14] E. Knill, e-print arXiv:quant-ph/9608049.
[15] A. Klappenecker and M. Roetteler, e-print arXiv:quant-ph/0010082.
[16] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).
[17] M. B. Ruskai, Phys. Rev. Lett. **85**, 194 (2000).
[18] H. Pollatsek and M. B. Ruskai, Linear Algebr. Appl. **392**, 255 (2004).
[19] A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003); e-print arXiv:quant-ph/9707021.
[20] M. H. Freedman, Proc. Natl. Acad. Sci. U.S.A. **95**, 98 (1998).
[21] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[22] S. B. Bravyi and A. Yu. Kitaev, e-print arXiv:quant-ph/9811052.
[23] M. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[24] M. Freedman, C. Nayak, and K. Shtengel, Phys. Rev. Lett. **94**, 147205 (2005).
[25] P. Fendley and E. Fradkin, Phys. Rev. B **72**, 024412 (2005).
[26] A. Kitaev, Ann. Phys. **321**, 2–111 (2003).
[27] M. Freedman, C. Nayak, and K. Shtengel, Phys. Rev. Lett. **94**, 066401 (2005).
[28] S. H. Simon, N. E. Bonesteel, M. H. Freedman, N. Petrovic, and L. Hormozi, Phys. Rev. Lett. **96**, 070503 (2006).
[29] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).
[30] M. Freedman, C. Nayak, and K. Walker, Phys. Rev. B **73**, 245307 (2006).
[31] S. Das Sarma, M. Freedman, and C. Nayak, Phys. Rev. Lett. **94**, 166802 (2005).
[32] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006).
[33] M. Levin and X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).
[34] F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
[35] J. J. Garcia-Ripoll, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **93**, 250405 (2004).
[36] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
[37] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[38] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[39] P. Zanardi and S. Lloyd, Phys. Rev. Lett. **90**, 067902 (2003).
[40] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[41] L.-M. Duan, E. Demler, and M. D. Lukin, Phys. Rev. Lett. **91**, 090402 (2003); e-print arXiv:cond-mat/0210564.
[42] A. Micheli, G. K. Brennen, and P. Zoller, Nat. Phys. **2**, 341–347 (2007).
[43] J. K. Pachos, e-print arXiv:quant-ph/0511273.
[44] C. Wang, J. Harrington, and J. Preskill, Ann. Phys. (N.Y.) **303**, 31 (2003).
[45] K. Takeda and H. Nishimori, Nucl. Phys. B **686**, 377 (2004).
[46] R. W. Ogburn and J. Preskill, Lect. Notes Comput. Sci. **1509**, 341 (1999).

[47] M. H. Freedman, A. Kitaev, and Z. Wang, Commun. Math. Phys. **227**, 587 (2002).
[48] M. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
[49] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Bull. Am. Math. Soc. **40**, 31 (2003); e-print arXiv:quant-ph/0101025.
[50] P. W. Shor, IEEE Symposium on Foundations of Computer Science, 1996 (unpublished).
[51] E. Knill, R. Laflamme, and W. Zurek, e-print arXiv:quant-ph/9610011.
[52] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[53] D. Aharonov and M. Ben-Or, in Proceedings of the 29th Annual ACM Symposium on Theory of Computing, El Paso, TX, May 1997 (unpublished), pp. 176–188.
[54] C. Zalka, e-print arXiv:quant-ph/9612028.
[55] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).
[56] P. Aliferis, D. Gottesman, and J. Preskill, Quantum Inf. Comput. **6**, 97 (2006).
[57] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **73**, 062303 (2006).
[58] M. H. Freedman and D. A. Meyer, e-print arXiv:quant-ph/9810055.
[59] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, New York, 1977).
[60] D. Welsh, *Codes and Cryptography* (Oxford University Press, Oxford, 1988).
[61] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[62] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **72**, 032313 (2005).
[63] A. Steane, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, T. Spiller, and S. Popescu (World Scientific, Singapore, 1998).
[64] J. Preskill, *Lecture Notes on Quantum Computation*; http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.ps
[65] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[66] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[67] P. J. Giblin, *Graphs, Surfaces, and Homology: An Introduction to Algebraic Topology* (Chapman and Hall, London, 1981).
[68] J. L. Gross and T. W. Tucker, *Topological Graph Theory* (Wiley, New York, 1987).
[69] M. Keyl and R. F. Werner, Lect. Notes Phys. **611**, 263 (2002) and references therein.