On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction

Gilles Zémor
Institut de Mathématiques de Bordeaux,
UMR 5251, Université Bordeaux 1,
351, cours de la Libération, 33405 Talence, France
Gilles.Zemor@math.u-bordeaux1.fr

December 30, 2008

Abstract

We review constructions of quantum surface codes and give an alternative, algebraic, construction of the known classes of surface codes that have fixed rate and growing minimum distance. This construction borrows from Margulis's family of Cayley graphs with large girths, and highlights the analogy between quantum surface codes and cycle codes of graphs in the classical case. We also attempt a brief foray into the class of quantum topological codes arising from higher dimensional manifolds and find these examples to have the same constraint on the rate and minimum distance as in the 2-dimensional case.

1 Introduction

The most investigated class of quantum stabilizer codes is the CSS (Calderbank, Shor, Steane [3, 16]) class. These codes have a short classical description that highlights the parallel with classical codes and makes them amenable to investigation by classical coding theorists with little or no background in quantum physics. A CSS code of length n can be defined by a binary "parity check matrix" $\mathbf{H}$ which has n columns and two sets of rows, making up two matrices $\mathbf{H}_1$ and $\mathbf{H}_2$, such that every row of $\mathbf{H}_1$ is orthogonal to every row of $\mathbf{H}_2$. In other words the quantum code is defined by two mutually orthogonal linear subspaces V_1 and V_2 of $\mathbb{F}_2^n$, the row-spaces of $\mathbf{H}_1$ and $\mathbf{H}_2$ respectively. The parameters $[[n, k, d]]$ of the associated quantum code are its length n, its dimension k which is given by $n - \dim V_1 - \dim V_2$, and its minimum distance d, which is given by the minimum weight of a non-zero binary vector that is either orthogonal to V_1 but not in V_2, or orthogonal to V_2 but not in V_1. Why this structure is relevant to quantum error-correction has been described many times, for detailed descriptions see e.g. [12] or [14].

In this paper we will be mainly interested in the parameters n, k, d of a quantum code. While asymptotically good (having constant rate $R = k/n$ and constant relative minimum distance $\delta = d/n$) CSS codes are known to exist [3], the same cannot be said of *sparse* CSS codes, in other words LDPC (Low-Density Parity-Check) quantum codes, which are CSS codes admitting a parity-check matrix $\mathbf{H} = (\mathbf{H}_1, \mathbf{H}_2)$ with a small number of ones per row

and per column. We will be interested in asymptotics, i.e. the study of families of codes with growing length n, and a bounded, or very slowly growing row and column weight for $\mathbf{H}$. One of the motivations for the search for good quantum LDPC codes, is that they will come together with *local* decoding algorithms and that iterative methods will lead to good decoding performance. While being asymptotically good is not a prerequisite for a good (close to capacity) decoding behaviour, it is nevertheless a challenging open problem to know whether asymptotically good low density CSS codes (or more general quantum codes for that matter) exist. At present, known families of quantum LDPC codes are very far from being asymptotically good. Recent attempts from the classical coding community at devising quantum LDPC codes with non-zero rate have resulted in *constant* minimum distances (e.g. [12, 8]). In the other direction, known families of quantum LDPC codes with a minimum distance growing with n are essentially restricted to the so-called class of *surface codes* that we will present below. We note that the rate R and relative minimum distance δ functions of known constructions of surface codes are constrained by the upper bound

$$R\delta^2 \leq n^{-2+o(1)} \tag{1}$$

We shall investigate the constraints on R and δ that we obtain when we switch from surface codes to codes based on higher dimensional topological manifolds, namely the n-dimensional torus, and find exactly the same constraint (1), leading one to ask whether this constraint on the behaviour of (R, δ) is inherent to quantum codes based on algebraic topology.

Surface codes also provide the presently only known family of quantum LDPC codes with constant rate and provably growing minimum distance [7], [10]. The minimum distance for these families grows like a logarithm of the blocklength. Published accounts of these families of codes involved sophisticated arguments from hyperbolic geometry: we shall give an alternative presentation that we find to be more accessible, and that highlights the analogy between quantum surface codes and the class of cycle codes of graphs in the classical coding setting. This analogy was already remarked in [2], where cycle codes of graphs are rediscovered and named classical "homological codes". In the present paper we shall push the analogy with cycle codes of graphs further by giving an account of the algebraic constructions of quantum surface codes with fixed rate and growing minimum distance that borrows from the algebraic constructions of graphs with large girths introduced by Margulis [13] and from the work of Širáň [15].

We have tried to keep the language of algebraic topology to a minimum to be accessible to coding theorists not well-versed in the field, and to try to make the paper as self-contained as possible. The paper is organized as follows: in section 2 we give a brief review of cycle codes of graphs together with Margulis's construction of regular graphs with large girths. We then proceed to review constructions of quantum surface codes in section 3, notably Kitaev's original toric code construction which is the starting point for all surface codes. We then move on to the construction of surface codes of fixed rate and logarithmic minimum distance. Finally in section 4 we give a brief exploration of the higher dimensional case by considering quantum codes arising from n-dimensional tori.

2 Cycle codes of graphs

2.1 cycle codes

Cycle codes of graphs are codes that have a parity-check matrix with exactly two "1"s per column. They are therefore instances of Low Density Parity Check (LDPC) codes with particularly low density and are amenable to iterative decoding (e.g. message passing) techniques. Even though they are not truly practical and their performance is surpassed by other well-studied classes of LDPC codes, they are interesting because their relatively simple structure makes it possible to analyze their decoding behaviour almost completely, and they have the remarkable property that over the binary symmetric channel, the threshold probabilities (beyond which decoding fails with probabity almost 1) for maximum-likelihood decoding [4, 18] and for iterative decoding coincide.

For the above reasons cycle codes of graphs can be considered as the simplest LDPC codes. It also turns out that they also have a natural generalization to quantum LDPC codes, under the form of surface (topological) codes. Before moving on to the quantum case, we therefore review relevant facts about cycle codes.

Let $\mathbf{G}$ be a finite, undirected, connected graph without loops or multiple edges. It is defined by its *vertex set* V and its *edge set* E where an edge is a pair of vertices. Let r and n denote the number of vertices and edges respectively, and let the set of edges be numbered, so that it is identified with $\{1, \ldots, n\}$. Identify furthermore subsets of edges with their characteristic vectors in $\{0,1\}^n$. A *cycle* $\mathbf{x} \in \{0,1\}^n$ of $\mathbf{G}$ is a subset of edges with the property that any vertex of $\mathbf{G}$ is incident to an even number of edges of $\mathbf{x}$. The set of cycles of $\mathbf{G}$ is a subset of $\{0,1\}^n$ stable under addition modulo 2. It is therefore a linear code of length n called the *cycle code* of $\mathbf{G}$.

An incidence matrix $\mathbf{H} = (h_{ij})$ of $\mathbf{G}$ is an $r \times n$ matrix whose rows are indexed by the vertices of $\mathbf{G}$, whose columns are indexed by the edges, and such that $h_{ij} = 1$ whenever vertex i belongs to edge j and $h_{ij} = 0$ otherwise. The incidence matrix $\mathbf{H}$ is also a parity-check matrix of the cycle code C: it has exactly two 1's per column since any edge is incident to exactly two vertices.

It is well-known that the dimension of C is $k = n - r + 1$ when the graph is connected. For example, the cycle code of the famous Petersen graph represented on figure 1 has parameters $[15, 6, 5]$, since the smallest cycle size is 5.

2.2 bounds on the girth of a graph

The study of the minimum distance d of C, i.e. the size of the smallest cycle, or *girth*, of $\mathbf{G}$ has been of interest to graph-theorists since the 1960's, and the problem of the exact determination of the largest possible girth of a graph with a given number of vertices and of edges is still quite open. The bad news for coding theorists is that for fixed rate $R = k/n$ and growing n the minimum distance d cannot grow faster than a logarithm of n. Here is a short proof of this when $\mathbf{G}$ is a *regular* graph. A graph $\mathbf{G}$ is said to be Δ-*regular* if every vertex is incident to exactly Δ edges. Note that $R = 1 - 2/\Delta + 1/n$, so that for large n, fixing the degree fixes the rate. Let v be any given vertex of the graph and consider the set of vertices

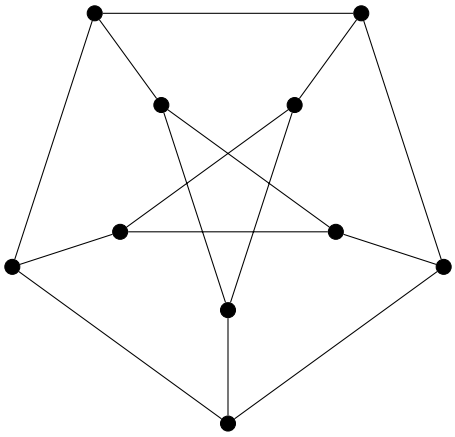

Figure 1: The Petersen graph yields a $[15, 6, 5]$ code.

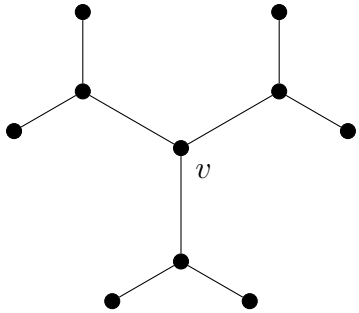

Figure 2: The neighbourhood of v in a Δ-regular graph (here $\Delta = 3$)

at distance from v less than $d/2$ in the graph, where the distance between two vertices is the length of a shortest path between the vertices. Because $\mathbf{G}$ does not contain a cycle of length smaller than d, the subgraph induced by this set of vertices must be a tree, as represented in figure 2.

The number of vertices of $\mathbf{G}$ at distance 1 from v is therefore Δ, the number of vertices at distance 2 from v is $\Delta(\Delta - 1)$, and the number of vertices at distance i from v, $i < d/2$, is $\Delta(\Delta - 1)^i$. We conclude that the total number of vertices $|V|$ in the graph has to be bigger than

$$1 + \Delta + \Delta(\Delta - 1) + \cdots + \Delta(\Delta - 1)^{\lceil d/2 \rceil}.$$

This lower bound on the number of vertices of a regular graph with given girth is known as the Moore bound. Let us mention in passing that deriving a similar bound for irregular graphs is not trivial and was achieved satisfactorily only relatively recently [1].

The resulting upper bound on the girth d (or minimum distance of the cycle code) when n is given and is large tells us that d cannot be significantly larger than

$$2 \log_{(\Delta-1)} |V|.$$

Erdös and Sachs [6] first showed with random arguments that families of Δ-regular graphs exist that satisfy $d \geq \log_{(\Delta-1)} |V|$. However, the first construction of an infinite family of Δ-regular graphs with girth d growing as a logarithm of the number of vertices is due to

Margulis [13]. We review the idea of his construction here because we will generalize it to the quantum case.

2.3 Margulis's construction of graphs with large girths

Margulis's construction uses Cayley graphs. A *Cayley graph* is defined by a group G together with a generating set S of group elements such that $s \in S$ implies $s^{-1} \in S$. The vertex set is the set of group elements, $V = G$, and we draw an edge between vertices x and y whenever $y = xs$ for some $s \in S$. Margulis takes for G the groups $G = \mathrm{SL}_2(\mathbb{F}_\mathrm{p})$ of 2×2 matrices of determinant 1 with elements in the field on p elements, for a prime p. The set S is the set $S = \{A, B, A^{-1}, B^{-1}\}$ where

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \quad B^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}.$$

We obtain therefore an infinite family of 4-regular graphs with $|V| = |G| = p(p^2 - 1)$. We see furthermore that a cycle of $\mathbf{G}$ is given by a sequence $s_1, \ldots, s_\ell$ of elements of S such that

$$s_1 s_2 \cdots s_\ell = 1 \quad \text{and} \quad s_{i+1} \neq s_i^{-1}, i = 1 \ldots \ell - 1. \tag{2}$$

Now Margulis's girth argument is as follows. Consider the set S viewed as matrices with elements in $\mathbb{Z}$, i.e. matrices of $\mathrm{SL}_2(\mathbb{Z})$. It is known that S generates a *free* subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. In other words (2) never occurs in Γ, and the Cayley graph (Γ, S) is a 4-regular *tree*. Therefore, a product of the form in (2) can only equal the identity matrix if it is reduced modulo p. But for this to happen, at least one of the matrix elements in the product $s_1 s_2 \cdots s_\ell$ must be larger than $p - 1$ in absolute value. But the largest term (in absolute value) of any matrix Ms is clearly not more than 3 times the largest term of the matrix M, for any $s \in S$. Therefore the length ℓ of any cycle (2) is at least $\log_3(p - 1)$, and the girth of the family of graphs $\mathbf{G}$ has at least logarithmic growth in the vertex (and edge) size.

Actually Margulis's original proof is slightly more involved and gives a better multiplicative constant in the lower bound on the girth, but this simple argument will suffice for our purposes. We remark also that this method can be clearly extended to yield Δ-regular graphs with large girths for different values of Δ.

Finally, we conclude this section with the following consideration. At the cost of letting the rate R of the cycle code go to zero, we can let the minimum distance (or girth) grow faster than $\log n$ where n is the block length (or number of edges). Start for example with the case when the graph consists of a single cycle, then the dimension is 1 and the minimum distance is n (we have the repetition code). But the Moore bound will constrain us with the upper bound

$$R\delta \leq n^{-1+o(1)} \tag{3}$$

where $\delta = d/n$ is the relative minimum distance. We are far away from the Gilbert-Varshamov bound which tells us that we have linear codes with constant $R\delta$.

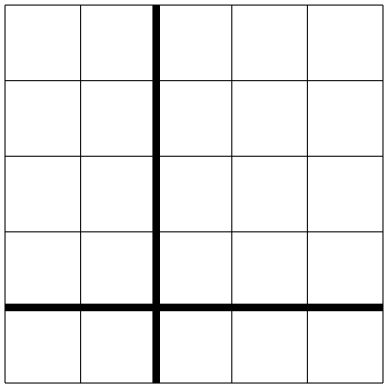

Figure 3: a two-dimensional torus: identify opposing edges.

3 Kitaev's toric code and surface codes

3.1 The toric code

To construct a quantum LDPC code we now need two low-density matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ such that every row of $\mathbf{H}_1$ is orthogonal to every row of $\mathbf{H}_2$. A relatively natural strategy is to try and adapt cycle codes to the quantum case. We can take for $\mathbf{H}_1$ the parity-check matrix of a cycle code of a graph that we defined in the preceding section and put some cycles as the rows of $\mathbf{H}_2$. For the quantum code to be non-empty we need the row-space V_2 of $\mathbf{H}_2$ to be not equal to the whole cycle code, and we would like both the rows of $\mathbf{H}_2$ to be of bounded weight (so that we have a genuine LDPC code) and the surviving cycles not in V_2 to be as large as possible. Furthermore, we would also like to control the weight of the vectors orthogonal to V_2 and not in the row-space V_1 of $\mathbf{H}_1$. Obviously some machinery will be required to achieve all these objectives.

One idea due to Kitaev [11] is to take the graph $\mathbf{G}$ equal to a tiling of a two-dimensional torus by squares. Specifically, take the graph with vertex set $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and connect every (x, y) to $(x, y-1), (x, y+1), (x-1, y), (x+1, y)$. The graph has m^2 vertices and $2m^2$ edges (figure 3). We remark that this graph is the Cayley graph over the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with generator set $S = \{(0, 1), (0, -1), (1, 0), (-1, 0)\}$.

Take for $\mathbf{H}_1$ the vertex-edge incidence matrix of the graph $\mathbf{G}$. For the rows of $\mathbf{H}_2$ take all elementary squares, i.e. cycles of the form $(x, y)-(x, y+1)-(x+1, y+1)-(x+1, y)-(x, y)$, or *faces* of the tiling. It is relatively easy to see that the quotient space $V_1^{\perp}/V_2$ has dimension 2, and that lowest-weight representatives are given by cycles that keep one coordinate constant, e.g. $(x, 0), (x, 1), \ldots (x, m-1), (x, 0)$ represented by thick lines on figure 3.

It remains to bound from below the weight of representatives from the other quotient space $V_2^{\perp}/V_1$. A convenient way to achieve this is to use *Poincaré duality*. The *dual graph* $\mathbf{G}^*$ of $\mathbf{G}$ is obtained from $\mathbf{G}$ by declaring the vertices of $\mathbf{G}^*$ to be the faces of $\mathbf{G}$ and by drawing an edge between two vertices of $\mathbf{G}^*$ if they have a common edge in $\mathbf{G}$. Now we see that the dual graph of $\mathbf{G}^*$ is isomorphic to $\mathbf{G}$, and that the rows of $\mathbf{H}_1$ are exactly the characteristic vectors of the cycles of $\mathbf{G}^*$. Therefore the minimum weight of representatives of $V_2^{\perp}/V_1$ is

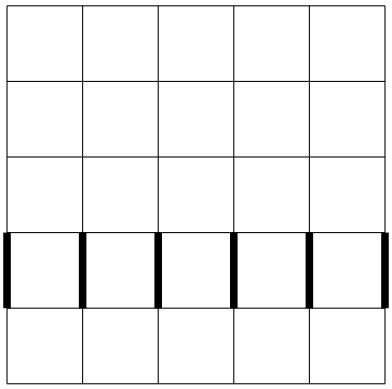

Figure 4: A minimum weight representative of $V_2^{\perp}/V_1$.

again m and the parameters of the associated quantum code are:

$$[[2m^2, 2, m]].$$

On the original graph G a minimum-weight representative of $V_2^{\perp}/V_1$ looks like a ladder and is represented on figure 4.

3.2 Surface codes

From a classical coding theorist's point of view, the dimension of the toric code is dreadfully small and one would like to generalize it to larger dimensions. For this the natural thing to do is to take tilings of other surfaces, i.e. graphs that generalize the 2-dimensional torus. Some definitions from algebraic topology are in order.

We adopt the combinatorial point of view, for which there is essentially no difference between a surface and a tiling of the surface. A cycle is said to be elementary if it is not the union of two non-empty cycles. A 2-*complex* is a connected graph $\mathbf{G}$ together with a collection of privileged elementary cycles called *faces*. For precise definitions of a surface in algebraic topology see for example [9]. For our purposes it will suffice to say that a 2-complex defines a *surface* (without boundary) when it satisfies the two following properties :

1. any two faces meet in at most one edge and every edge belongs to exactly two faces.
2. For any given vertex v, if F is the set of faces incident to v, then any edge common to two faces of F is an edge incident to v and furthermore, if we define a graph on F by declaring two elements of F to be adjacent if they have a common edge in $\mathbf{G}$, then we obtain an elementary cycle.

We see that the second condition enables us precisely to define the dual graph $\mathbf{G}^*$ and the associated dual 2-complex in a way that generalizes duality for the toric tiling of the preceding section. The faces of $\mathbf{G}$ define the vertices of $\mathbf{G}^*$. Two vertices of $\mathbf{G}^*$ are adjacent in $\mathbf{G}^*$ if the corresponding faces of $\mathbf{G}$ have a common edge in $\mathbf{G}$. The faces of $\mathbf{G}^*$ are the cycles of $\mathbf{G}^*$ that arise from the sets of faces of $\mathbf{G}$ incident to a vertex of $\mathbf{G}$, as in condition 2 above.

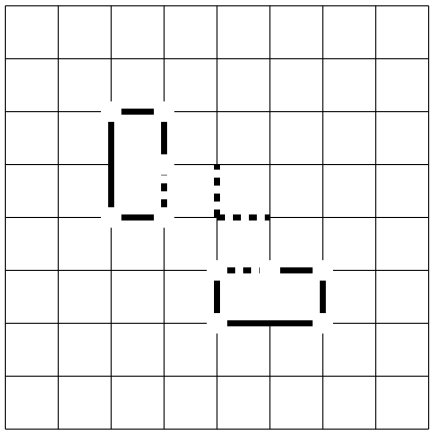

Figure 5: A grid with holes (thick lines). Dashed edges are a word of $V_2^{\perp}/V_1$.

Finally, the $(\mathbb{Z}/2\mathbb{Z})$ *homology* group $H_1(\mathbf{G})$ is the quotient of the cycle code of $\mathbf{G}$ by the $\mathbb{F}_2$-linear subspace generated by the faces of $\mathbf{G}$. The *cohomology* group $H^1(\mathbf{G})$ is the homology group $H_1(\mathbf{G})$ of the dual 2-complex $\mathbf{G}^*$.

Now, switching to the construction of the associated quantum code, we take the matrix $\mathbf{H}_1$ to be again the point-edge incidence matrix of the graph $\mathbf{G}$, and the matrix $\mathbf{H}_2$ is now the set of characteristic vectors of the faces of $\mathbf{G}$. Alternatively, $\mathbf{H}_1$ can be seen as the set of characteristic vectors of the faces of $\mathbf{G}^*$ and $\mathbf{H}_2$ as the point-edge incidence matrix of the dual graph $\mathbf{G}^*$. The homology and cohomology groups of $\mathbf{G}$ are exactly the coset spaces $V_1^{\perp}/V_2$ and $V_2^{\perp}/V_1$ whose dimension is the dimension of the quantum code and whose minimum weight representatives give the quantum minimum distance.

A natural way to obtain sequences of quantum surface codes with growing dimension is to take tori with a growing number of handles. This approach is discussed in [5] and more recently and at some length in [2]. We do not dwell upon this, instead we will be content to give a very short description of an alternative method, also discussed in [5, 2], which is topologically quite close, is quite visual, and gives essentially the same asymptotic parameters.

Take for the graph $\mathbf{G}$ an $m \times m$ grid with *holes* as in figure 5.

Again $\mathbf{H}_1$ is the point-edge incidence matrix of the graph $\mathbf{G}$. The matrix $\mathbf{H}_2$ has rows corresponding to the elementary squares of the grid with the inside of the holes missing. A close look at the situation convinces one that the dimension of the quantum code is equal to the number of holes. The minimum distance is the minimum of the perimeter of the holes, and the smallest "ladder distance" between holes or between a hole and the outside boundary. See [5, 2] for details.

By multiplying the number of holes in the grid, one can push the dimension of the quantum code all the way to a quantity linear in the blocklength. The price to pay for this however will be a constant minimum distance. In between we have the relation between the quantum rate $R = k/n$ and the relative quantum minimum distance $\delta = d/n$

$$R\delta^2 \leq cn^{-2} \tag{4}$$

for a constant c. The same compromise is obtained with the natural tilings of tori with a growing number of handles.

The above bound seems to be inherent to the nature of surface codes. By taking more sophisticated surfaces however, one can obtain a slight improvement in the behaviour of the minimum distance. In particular one can obtain quantum LDPC codes of constant rate and non-constant, slowly growing minimum distance, proportional to $\log n$ for blocklength n. This result is implicit in [7], where sophisticated topological methods are used. See also [10]. We shall give a different account of this result by appealing to a method which is very much reminiscent of Margulis's construction of graphs with large girth of section 2.3.

3.3 Surface quantum codes with constant rate and logarithmic minimum distance

Our purpose is to construct a family of quantum surface codes with constant rate and growing minimum distance.

Recall that Margulis's Cayley graph construction consists of realizing an infinite tree as the Cayley graph of a free group and then projects this infinite tree on a finite graph by taking a suitable quotient of the infinite free group. We will adopt a similar approach, but we will start with an infinite Cayley graph that is not a tree so as to have cycles that will define the faces of the surface that we shall obtain.

Specifically, consider the group on two generators a and b defined by the presentation

$$a^2 = 1, b^\ell = 1, (ab)^m = 1$$

where m, ℓ are positive integers such that $1/2 + 1/\ell + 1/m < 1$. This group, denoted by $T = T(2, m, \ell)$, is called a triangular group of type $(2, m, \ell)$ and has numerous applications, in particular to hyperbolic geometry.

Consider now the Cayley graph $\mathcal{T}$ on T with generating set $S = \{a, b, b^{-1}\}$. We associate to $\mathcal{T}$ a 2-complex by declaring its faces to be the length ℓ cycles

$$\{x, xb, xb2, \ldots, xb^{\ell-1}, xb^\ell = x\} \tag{5}$$

and the length $2m$ cycles

$$\{x, xa, xab, xaba, x(ab)^2, \ldots, x(ab)^{m-1}a, x(ab)^m = x\} \tag{6}$$

for every vertex x of $\mathcal{T}$. One easily checks that this 2-complex satisfies conditions 1 and 2 that define a surface, and furthermore the subgraph induced by the set of vertices at fixed distance r from the identity element is a planar graph, as is illustrated on figure 6.

Now suppose that we can find a finite quotient group G of the group T such that no product of the elements a, b, b^{-1} of length r or less collapses to the identity in G if it doesn't collapse to the identity in the infinite group T. Consider the corresponding finite graph $\mathbf{G}$ defined as the Cayley graph on the group G with generator set $S = \{a, b, b^{-1}\}$ and consider the associated quantum surface code. We note that the row weight of $\mathbf{H}_1$ is 3 and the row weight of $\mathbf{H}_2$ is ℓ or $2m$ (the face lengths), so that $(\mathbf{H}_1, \mathbf{H}_2)$ define a genuine quantum LDPC code.

First, let us estimate the dimension of the quantum code. The number of rows of the matrix $\mathbf{H}_1$ is simply equal to number of vertices $|V|$ of the graph which equals, since the graph is of degree 3,

$$|V| = \frac{2}{3}|E|$$

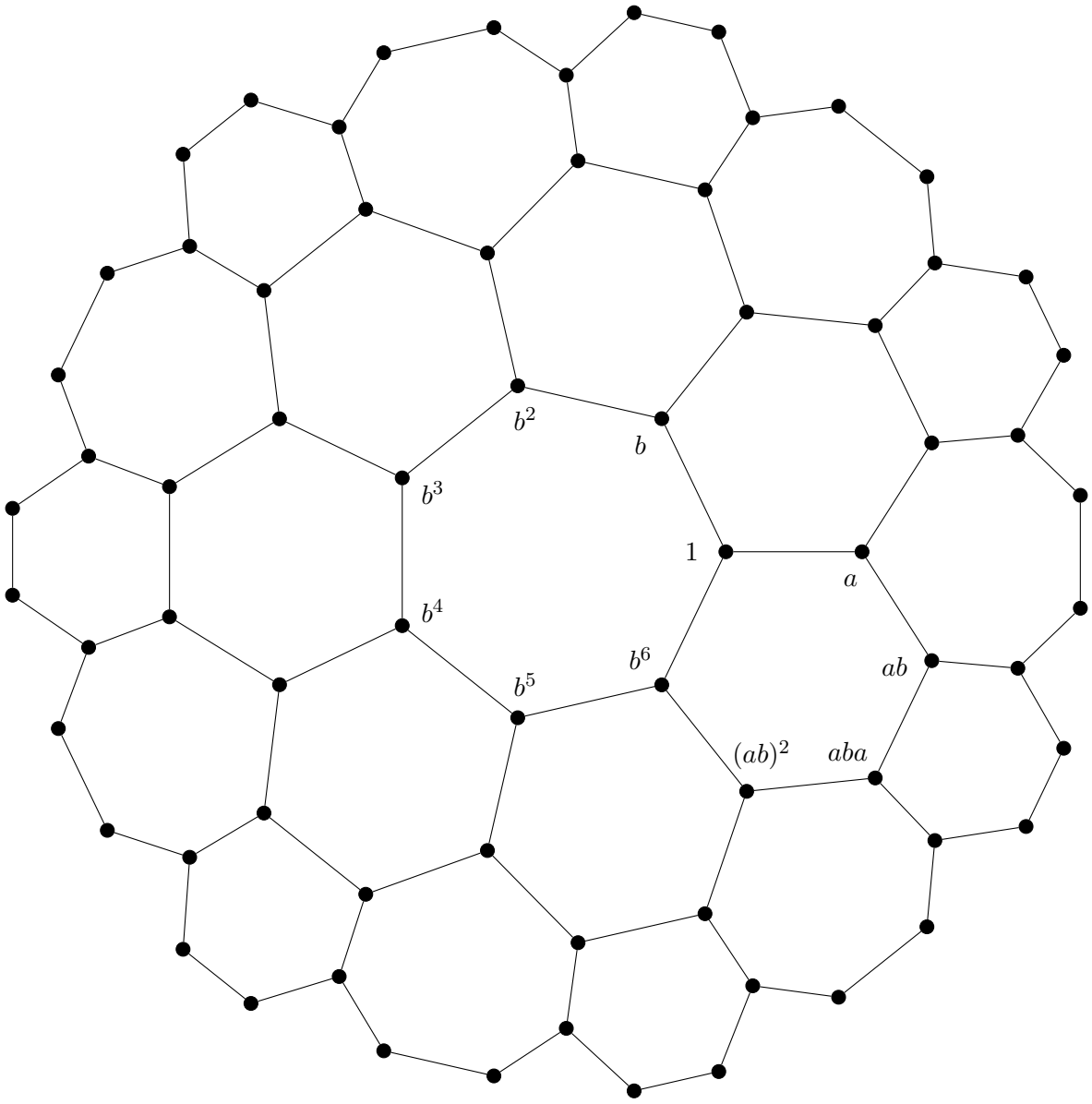

Figure 6: a local view of the Cayley graph $\mathcal{T}$ in the case $m = 3$ and $\ell = 7$.

where $|E|$ is the number of edges. We proceed to count the number of rows of $\mathbf{H}_2$, i.e. the number of faces of the graph $\mathbf{G}$. We remark that every vertex x is incident to two edges $\{x, xb\}$ and $\{x, xb^{-1}\}$ that belong to the same ℓ-face (5) and is incident to one edge $\{x, xa\}$ that belongs to two $2m$-faces of type (6). Hence, denoting by $|F_\ell|$ and $|F_{2m}|$ the number of ℓ-faces and of $2m$-faces respectively, we have :

$$\ell|F_\ell| = |V| \qquad \text{and} \qquad 2m|F_{2m}| = 2|V|$$

from which the total number of faces equals

$$\left(\frac{1}{\ell} + \frac{1}{m}\right)|V| = \frac{2}{3}\left(\frac{1}{\ell} + \frac{1}{m}\right)|E|.$$

Therefore the dimension k of the quantum code satisfies

$$\begin{aligned} \frac{k}{|E|} &\geq 1 - \frac{2}{3} - \frac{2}{3}\left(\frac{1}{\ell} + \frac{1}{m}\right) \\ k &\geq |E|\frac{1}{3}\left(1 - 2\left(\frac{1}{\ell} + \frac{1}{m}\right)\right) \end{aligned}$$

so that the dimension k is a positive fraction of the blocklength $n = |E|$ for any m, ℓ such that $1/m + 1/\ell > 1/2$. For example, when $m = 3$ and $\ell = 7$ we obtain $k \geq n/63$.

We now address the estimation of the quantum minimum distance. Consider any elementary cycle of length r or less in the finite Cayley graph $\mathbf{G}$. Now if x is any vertex lying on this cycle, the cycle is included in the distance r-neighbourhood of x. But since we have supposed that any word formed with the letters a, b, b^{-1} collapses to the identity in G only if it collapses to the identity in T, the subgraph of $\mathbf{G}$ induced by the distance r-neighbourhood of x is exactly the same as the corresponding distance r-induced subgraph of the infinite Cayley graph $\mathcal{T}$. Since this graph is planar, all of its cycles are sums of its faces, and the initial cycle is a sum of faces of $\mathbf{G}$. Similarly, if a vector is orthogonal to all the faces of $\mathbf{G}$, i.e. is a cycle of the dual graph $\mathbf{G}^*$, and if its weight is sufficiently small, then everyone of its connected components $\mathbf{x}$ must belong to a bounded distance neighbourhood of $\mathbf{G}^*$, which is planar and coincides with a bounded distance neighbourhood of of $\mathcal{T}^*$, hence $\mathbf{x}$ must equal a sum of faces of $\mathbf{G}^*$. We obtain in this way a quantum code with minimum distance proportional to r.

It remains to find such a quotient group G. Similarly to Margulis's construction, we again appeal to a representation of the infinite group T by a subgroup of a matrix group, though a somewhat more complicated one. A construction that does exactly what we need, though for different reasons, was found by Širáň [15] and we sketch it below.

Let

$$P_k(X) = 2\cos(k \arccos(X/2))$$

be the normalized kth Chebychev polynomial and let $\xi = 2\cos(\pi/m\ell)$. Let B and C be the matrices of $\mathrm{SL}_3(\mathbb{Z}[\xi])$:

$$B = \begin{bmatrix} -1 & -P_\ell(\xi) & 0 \\ P_\ell(\xi) & P_\ell(\xi)^2 - 1 & 0 \\ P_m(\xi) & P_m(\xi)P_\ell(\xi) & 1 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} P_m(\xi)^2 - 1 & 0 & P_m(\xi) \\ P_\ell(\xi) & 1 & 0 \\ -P_m(\xi) & 0 & -1 \end{bmatrix}.$$

Širáň proved that the subgroup of $\mathrm{SL}_3(\mathbb{Z}[\xi])$ generated by B and C has presentation: $B^\ell = 1$, $C^m = 1$ and $(CB)^2 = 1$. Equivalently, if we set $a = CB$ and $b = B$, then the subgroup of $\mathrm{SL}_3(\mathbb{Z}[\xi])$ generated by a and b has presentation $a^2 = 1$, $b^\ell = 1$ and $(ab)^m = 1$. Therefore, the subgroup of $\mathrm{SL}_3(\mathbb{Z}[\xi])$ generated by a and b is exactly the triangular group T.

Now to take a quotient, proceed like Margulis and reduce the matrix entries of $SL_3(\mathbb{Z}[\xi])$ modulo p for some prime p. Some care must be taken for this reduction to make sense and to behave properly. Širáň argues that ξ is a root of the polynomial $h(X) = P_{2m\ell}(X) - 2$ that has integer coefficients and leading coefficient equal to 1. There is therefore a ring homomorphism

$$\mathbb{Z}[\xi] \to \mathbb{Z}[X]/(h(X))$$

defined by $\xi \mapsto X$, and by reducing coefficients of polynomials in $\mathbb{Z}[X]/(h(X))$ modulo p we obtain a ring homorphism

$$\mathbb{Z}[\xi] \to \mathbb{F}_p[X]/(h(X)).$$

this homorphism has the property that an integer polynomial expression in ξ of degree $< \deg h$ that is non-zero in $\mathbb{Z}[\xi]$ maps to zero only if not all the absolute values of its coefficients belong to $\{0, 1, \ldots, p-1\}$. Therefore, if we define the finite group G to be the subgroup of $\mathrm{SL}_3[\mathbb{F}_\mathrm{p}[\mathrm{X}]/(\mathrm{h}(\mathrm{X}))]$ generated by a and b, we obtain that a word in $a, b, b^{-1} = b^{\ell-1}$ collapses to the identity in G but not in T, only if one the polynomial coefficients of its matrix entries is larger than $p-1$. But we see that these coefficients grow exponentially (but not faster) in the length of the word. We obtain therefore that the shortest word that collapses to the identity in G but not in T behaves like a logarithm of p and hence like a logarithm of the size of the group G. See [15] for numerical estimations of constants.

4 The n-dimensional toric code

In this section we make a short incursion into the realm of topological codes built on manifolds of dimension greater than 2. Another way to raise the dimension of Kitaev's torus code is to consider tilings of tori in dimensions greater than 2. The case of dimension 4 was already considered in [5] and in [17] with the hope that local decoding strategies will work better than in dimension 2. Let us consider the general case.

In this section the length of the quantum codes will be denoted by N rather than n, and n will denote the dimension of the torus. Consider the Cayley graph $\mathbf{G}$ on the group $G = (\mathbb{Z}/m\mathbb{Z})^n$ with generator set made up of all n-tuples of G of weight one and with their non-zero coordinate equal to either 1 or -1. The graph $\mathbf{G}$ is made into an n-complex, by associating to $\mathbf{G}$ faces of dimension $2, 3 \ldots, n$, where an i-dimensional face is obtained by fixing $n-i$ coordinates and letting the i remaining coordinates describe an elementary cube of dimension i.

Now instead of indexing coordinates of $\{0,1\}^N$ by edges of the graph, as in the cycle code and surface code case, we index coordinates by the i-faces of $\mathbf{G}$ for some i. The number of i-dimensional faces is easily seen to be

$$N_i = m^n \binom{n}{i} \tag{7}$$

and the codelength is therefore $N = N_i$. Now a vector $\mathbf{x} \in \{0,1\}^N$, equivalently a collection of i-faces, is called an *i-cycle* if every $(i-1)$-face is incident to (is included in) an even number of i-faces of $\mathbf{x}$. We now define the matrix $\mathbf{H}_1 = (h_{ab})$ as the matrix whose rows are indexed by the $(i-1)$-faces and whose columns are indexed by the i-faces, with a $h_{ab} = 1$ if $(i-1)$-face a belongs to i-face b, and $h_{ab} = 0$ otherwise.

Now every $(i+1)$-face, viewed as a collection of i-faces is an i-cycle. In other words, an $(i+1)$-face, viewed as a vector of $\mathbb{F}_2^N$, is orthogonal to all the rows of $\mathbf{H}_1$. We therefore take for $\mathbf{H}_2$ the matrix whose rows are all the characteristic vectors of the $(i+1)$-faces of $\mathbf{G}$.

Denoting as before V_1 to be the row-space of $\mathbf{H}_1$ and V_2 to be the row-space of $\mathbf{H}_2$, the quotient $V_1^\perp/V_2$ is exactly the i-th homology group $H_i(\mathbf{G})$ of the n-complex and it is known (see e.g. [9]) to have dimension

$$k = \binom{n}{i} \tag{8}$$

which is the dimension of the quantum code.

Now we have a straightforward upper bound on the minimum weight of an i-cycle that is not a sum of $(i+1)$-faces. To obtain one, simply consider the set of all i-faces that fix some given $n-i$ coordinates. This defines a set of i-faces that is isomorphic to a tiling of an i-dimensional torus, whose weight is, by (7), m^i. Hence the quantum minimum distance satisfies

$$d \leq m^i. \tag{9}$$

What about the minimum weight of representatives of $V_2^\perp/V_1$? As in the 2-dimensional case, we can again appeal to Poincaré duality by considering the dual n-complex $\mathbf{G}^*$, that transforms i-faces of $\mathbf{G}$ into $(n-i)$-faces of $\mathbf{G}^*$. Since the dual complex $\mathbf{G}^*$ is again isomorphic to $\mathbf{G}$, the quotient space $V_2^\perp/V_1$ is exactly the homology group $H_{n-i}(\mathbf{G}^*)$ so that (9) turns into

$$d \leq m^{n-i}.$$

Given these upper bounds on d together with the code dimension, we see that we shall obtain the best results by choosing n to be even and $i = n/2$, in which case we have :

$$N = m^n \binom{n}{n/2}, \quad k = \binom{n}{n/2}, \quad d \leq m^{n/2}.$$

Somewhat surprisingly, these values give:

$$kd^2 \leq N$$

so that the quantum codes based on n-dimensional tori are, as in the dimension 2 case, constrained by the inequality (4).

5 Concluding remarks

Our brief exploration of quantum codes arising from higher dimensional topological manifolds barely scratches the surface (so to speak !) of the subject. It is intriguing however that one encounters the same constraint (1) that seems to be associated with surface codes. Bearing

in mind the constraint (3) that is known to hold for cycle codes from the Moore bound, could it be that there is a 2-dimensional (or even higher-dimensional !) equivalent of the Moore bound that would constrain topological quantum codes to (1) ?

Acknowledgement. We are grateful to Jean-Pierre Tillich for involving us in the subject and for numerous inspiring discussions.

References

[1] N. Alon, S. Hoory and N. Linial, The Moore bound for irregular graphs, *Graphs Combin.*, Vol. 18, pp. 53–57.

[2] H. Bombin and M. A. Martin-Delgado, Homological Error Correction: Classical and Quantum Codes, *J. Math. Phys.* 48, 052105 (2007).

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

[4] L. Decreusefond and G. Zémor, On the error-correcting capabilities of cycle codes of graphs, *Combinatorics, Probability and Computing*, Vol. 6 (1997) pp. 27–38.

[5] E. Dennis, A. Kitaev, A. Landahl, J. Preskill, Topological quantum memory, *J. Math. Phys.* Vol. 43 (2002) pp. 4452–4505.

[6] P. Erdös and H. Sachs, Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl, *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg, Math.-Naturwiss.* Reihe 12, 251-258 (1963).

[7] M. H. Freedman, D. A. Meyer, F. Luo, $\mathbb{Z}_2$-systolic freedom and quantum codes, in *Mathematics of quantum computation*, 287320, Comput. Math. Ser., Chapman & Hall/CRC, Boca Raton, FL, 2002.

[8] M. Hagiwara and H. Imai, Quantum Quasi-Cyclic LDPC Codes, in *Proc. IEEE International Symposium Information Theory (ISIT)*, Nice 2007 pp. 806-810.

[9] A. Hatcher, *Algebraic Topology*, Cambridge University Press, 2002.

[10] I. H. Kim, Quantum codes on Hurwitz surfaces, S. B. Thesis, MIT, 2007. `http://dspace.mit.edu/handle/1721.1/40917`

[11] A. Kitaev, Quantum error correction with imperfect gates, in *Proc. 3rd nt. Conf. of Quantum Communication and Measurement*, 1997.

[12] D. J. C. Mackay, G. Mitchison, P. L. Mcfadden, Sparse Graph Codes for Quantum Error-Correction, *IEEE Trans. Inform. Theory*, Vol. 50, No 10, (2004) pp. 2315–2330.

[13] G. A. Margulis, Explicit constructions of graphs without short cycles and low density codes, *Combinatorica*, Vol. 2 No 1, (1982) pp. 71–78.

[14] J. Preskill, Quantum computation,
`http://www.theory.caltech.edu/ preskill/ph219`

[15] J. Širáň, Triangle group representations and constructions of regular maps, *Proc. London Math. Soc.*, Vol. 82, No 3 (2001) pp. 513–532.

[16] A. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. Lond. A*, 452:2551, 1996.

[17] K. Takeda and H. Nishimori, Self-dual random-plaquette gauge model and the quantum toric code, *Nuclear Physics B*, Vol. 686, No 3, (2004) pp. 377–396.

[18] J-P. Tillich and G. Zémor, Optimal cycle codes constructed from Ramanujan graphs, *Siam J. on Discrete Math.*, Vol. 10, No 3 (1997) pp. 447–459.