A study of quantum error-correcting codes derived from platonic tilings

Gabriele SPINI

Advised by Prof. Gilles ZÉMOR

ALGANT Master Thesis - 8 July 2013

Università degli Studi di Milano and Université Bordeaux 1

A study of quantum error-correcting codes derived from platonic tilings

Gabriele Spini

8 July 2013

Contents

Abstract

This thesis concerns the study of a family of quantum-error correcting codes that present low-density parity-check matrices. These codes are of CSS-type and are obtained from a family of tilings called *platonic surfaces*; the possibility of using this family of surfaces for quantum coding theory has been introduced by Reina Riemann in her PhD thesis in 2011.

Our work is devoted to revisiting and expanding this study; we first present an overview of platonic surfaces, using a combinatorial approach based on graph theory, and study their remarkable properties without restricting us to those related to the derived codes. Computations regarding symmetry and spectrum of these graphs are presented, as well as an alternative contruction.

The main new result we introduce is the computation of an upper bound on the minimal distance of these codes, equal to the homology systole of platonic surfaces; this yields a relative minimum distance that tends to zero as the block length goes to infinity.

Finally, we present some computer simulations that are necessary to compute the above bound for some of the platonic surfaces, and that could be useful for further investigation of the properties of these codes.

Introduction

It is known that tilings of surfaces yield quantum error-correcting codes with efficient decoding algorithms; in the present paper, we study a family of codes obtained in this way. Properties of these codes can be obtained directly in terms of the underlying surface structure, hence we shall mostly work on the tilings themselves to investigate the quality of the codes; graph theory will be our fundamental tool. No knowledge of quantum (or classical) coding theory is assumed, and we try to make this paper as self-contained as possible to make it accessible for the readers that are not familiar with the subject.

The aim of this work is to compute the homology systole of a family of combinatorial surfaces: namely, we will define these to be a special type of 2-complexes, constructed via a combinatorial approach based on graph theory, which is the most natural language for our study. Although these surfaces can be given a Riemann-manifold structure, we stick to the topological/combinatorial approach; the homology systole of such a family is the smallest possible length of a cycle whose class is non-zero in a homology quotient that will be defined.

Our main object of study is a family of combinatorial surfaces called *platonic tilings*, which gives rise to a family of quantum error-correcting codes of CSS (Calderbank, Shor and Steane) type that have low-density parity-check matrices.

The possibility of using this family of surfaces for quantum error-correction was introduced by R. Riemann in her doctorate thesis in 2011 [15]; the present dissertation is essentially devoted to revisiting and expanding the work of Riemann, as well as to collecting various properties of platonic tilings.

The first chapter will present some background information and motivation for our study, with a short introduction to quantum surface codes; this will be introducted by a small paragraph on cycle codes of graphs, as this is a very quick and intuitive way to approach quantum surface codes.

The second chapter provides an overview of the family of platonic graphs $\{\pi_n : n \in \mathbb{N}_{\geq 3}\}$, whose remarkable properties have been studied (among others) by Biggs [3], Brooks [5],[4], Gunnells [10], and Lanphier & Rosenhouse [12].

We show the high symmetry of these graphs, and discuss their regularity, the length of their diameter and their eigenvalues; moreover, we stress that platonic graphs are actually endowed with the structure of a (combinatorial) surface, so that they can give rise to quantum topological codes. General properties of the dual surfaces π'_n are also presented.

In the third chapter we compute the homology systole of π_n and of the dual surface π'_n, i.e. the length of the shortest cycle that is not a sum of faces; the smallest of these parameters coincides with the minimal distance of the derived code, and hence the computation of their values (or at least of some bounds on them) is critical to understand the effectiveness of the code.

This is the section where our work significantly expands Riemann's one: exploiting the structure of $\mathbb{F}_2$-vector space of the cycles of π_n to use dimensional arguments, we show that the homology systole of platonic graphs is indeed not bigger than 6 (for $n = p$ a prime); this result was not present in Riemann's work.

We also report the covering argument that allows one to prove a logarithmic lower bound on the girth of the dual graphs π'_n, and discuss how close this is to Moore's bound.

In the fourth chapter we discuss the properties of the error-correcting codes derived from platonic graphs, providing computations regarding their rate, sparsity and minimal distance.

Finally, the appendix presents the computer simulations that have been useful to formulate the result on the homological systole of π_n; some of the included programs have been necessary to compute this parameter for some values of n, and will certainly be useful for further analysis on the sharpness of the provided bound.

Chapter 1

Backgound and motivation

We shall first briefly present the main mathematical concepts we will deal with, i.e. quantum CSS-codes of topological type, and combinatorial surfaces; we will only cover those aspects more relevant for our purposes (see [8], [16] and [13] for a more specific study).

1.1 A brief review of classical cycle codes

Among all quantum error-correcting codes, topological codes share several similarities with classical cycle codes; we shall emphasize these analogies and present them in a way accessible to readers that are not familiar with quantum coding theory.

Definition 1.1.1. *A* (classical) binary linear code *is the kernel of a matrix* $H \in \mathcal{M}_{\mathbb{F}_2}(r \times n)$*, called a* parity-check matrix *of the code. An element of a code is called a* codeword.

The parameters of a code $C = \ker(H)$ are $[n, k, d]$, where:

- n is called the *block length*, equal to the number of columns of H;
- k is called the *dimension* of the code, and it is indeed its dimension as an $\mathbb{F}_2$-vector space;
- d is called the *minimum distance* of the code, equal to the minimum weight (=number of non-zero coordinates) of a non-zero codeword.

One of the objectives of coding theory is, for a fixed block length n, to find a code with dimension and minimum distance as large as possible.

A classical family of codes is given by the *cycle code* of any given graph: let G be a finite, undirected graph, i.e. $G := (V, E)$ where V is a finite set (called the vertex set) and $E \subseteq \binom{V}{2}$ is a family of pairs of vertices, called edges; fix an ordering of the vertex and edge set, say $V : \{v_1, \cdots, v_{|V|}\}$ and $E : \{l_1, \cdots, l_{|E|}\}$. Then we can define the incidence matrix of the graph $H \in \mathcal{M}_{\mathbb{F}_2}(|V| \times |E|)$ to be such that $H_{ij} = 1$ if the vertex v_i belongs to l_j, and $H_{ij} = 0$ for all other couples.

Codewords of cycle codes have an intuitive geometric picture: notice that elements of $\mathbb{F}_2^E$ can be seen as characteristic vectors of a set of the edges; now let us study the orthogonality conditions that define codewords: given $W \in \mathbb{F}_2^E$ (that we will thus also view as a subset of E), we have that W is a codeword if and only if $H \cdot W^t$ is the zero vector. But this holds if and only if for every line H_i of H, the scalar product $H_i \cdot W^t$ is equal to zero, which in turn happens if and only if $\#\{j : H_{ij} = W_j = 1\}$ is even. Now recall that $H_{ij} = 1$ only when the edge l_j is incident to the vertex v_i: this means that $H \cdot W^t = \underline{0}$ if and only if for every vertex v of the graph, the number of edges belonging to W that are incident to v is even. We will call *cycles* the subsets of E with this property; notice that with this definition, cycles don't need to be connected.

The parameters of a code derived from a graph $G = (V, E)$ are the following:

- the block length is equal to the number of edges of the graph (trivial by definition);
- the dimension of the code is equal $|E| - |V| +$ the number of connected components of the graph. This is a standard result from graph theory, not difficult to prove by induction (see [2], for instance);
- the minimum distance is the *girth* of the graph, i.e. the length of the shortest non-zero cycle (this is obvious by the above characterization of codewords).

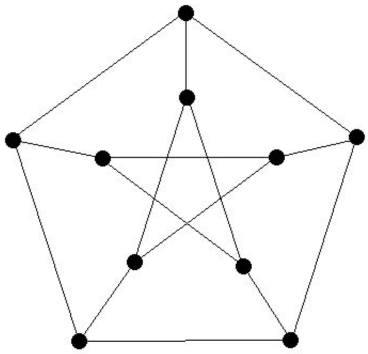


Figure 1.1: Petersen's graph; the derived code has parameters [15,6,5].

The minimum distance of cycle codes of graphs is far from being optimal: for instance, consider a Δ-regular graph G (i.e, such that every vertex is incident to Δ edges) with N vertices, and let d be the girth of the graph; then for every fixed vertex v, and for any $r < \left\lfloor \frac{d}{2} \right\rfloor$, the ball centered at v and of radius r does not contain cycles (since the distance between to vertices is the length of the shortest path joining them). Thanks to the absence of cycles, computing the cardinality of such a ball is rather easy: the number of elements at distance 1 from v is Δ; the number of element at distance 2 is $\Delta \cdot (\Delta - 1)$, and that of elements at distance i is $\Delta \cdot (\Delta - 1)^{i-1}$. Thus

$$\#B(v,r) = 1 + \Delta + \cdots + \Delta(\Delta - 1)^{r-1},$$

and therefore by setting $r := \left\lfloor \frac{d}{2} \right\rfloor - 1$ we get

$$1 + \Delta(\Delta - 1) + \Delta(\Delta - 1)^2 + \cdots + \Delta(\Delta - 1)^{\left\lfloor \frac{d}{2} \right\rfloor - 2} < N.$$

This inequality is known as *Moore's bound*; now if we keep Δ fixed and we let N go to infinity, we get

$$d \leq 2 \cdot \log_{\Delta-1} N + O(1) \approx 2 \cdot \log_{\Delta-1}(\text{block length}) + O(1)$$

which means that the minimum distance of cycle codes is at most logarithmic in the block length.

Cycle codes of graphs, however, are very simple to decode: namely, there exist algorithms that for any given vector of $\mathbb{F}_2^n$ always find the closest codeword in time polynomial in the block length, which is remarkable in coding theory.

1.2 Topological quantum codes

Let us first introduce the family of CSS (Calderbank, Shore and Steane) codes:

Definition 1.2.1. *A* (quantum) CSS-code *is described in term of two binary matrices* $\mathbf{H}_X$ *and* $\mathbf{H}_Z$*, having the same number of columns and enjoying the property that all rows of* $\mathbf{H}_X$ *are orthogonal to all rows of* $\mathbf{H}_Z$*.*

The parameters of the code are $[[n, k, d]]$ where:

- n is called the *block length*, and is equal to the number of columns of $\mathbf{H}_X$ (or of $\mathbf{H}_Z$);
- k is called the *dimension* of the code, and is equal to $n - \mathrm{rk}\mathbf{H}_X - \mathrm{rk}\mathbf{H}_Z$;
- d is called the *minimum distance* of the code; it is equal to the minimum between d_X and d_Z, where:
    - d_X is the minimum weight of a vector lying in $\mathbb{F}_2^n$, which is orthogonal to the space generated by the rows of $\mathbf{H}_Z$ and does not belong to the linear span of the rows of $\mathbf{H}_X$;
    - d_Z is defined in a similar way, with X and Z swapped.

Now, topological CSS-codes can be constructed in a similar way as cycle codes of graphs: let $\mathbf{H}_X$ be the incidence matrix of a graph; then $\mathbf{H}_Z$ must be a matrix whose rows are characteristic vectors of cycles, because of the orthogonality condition between rows of the two matrices.

In other words, a CSS code can de defined from any 2-complex, a topological space obtained from three steps: first, select a (finite) set of points V; then glue a set $E = \{l_1, \cdots, l_{|E|}\}$ of segments (copies of the interval $[0, 1]$) to the vertex set V via maps $\varphi_i : \partial l_i \to V$. By "glueing", we mean that our topological space at this step is a disjoint union of vertices and edges with identifications provided by the glueing maps (i.e. $x = \varphi_i(x)$ for any x in the boundary of an edge l_i); this way we get a graph structure G. Now to complete the construction, we just need to glue a set of discs $F = \{f_1, \cdots, f_{|F|}\}$ (copies of the open ball in $\mathbb{R}^2$) to the graph via maps $\psi_j : \partial f_j \to G$; the final space will be the disjoint union of the graph and of the discs with identifications given by these new glueing maps.

Among all possible 2-complexes, the following surfaces are somewhat natural candidates for the construction of a CSS code:

define a *(combinatorial) surface* to be a graph, together with a favoured set of elementary cycles (i.e., that are not union of other non-zero cycles) called *faces*, satisfying the following properties:

(i) two arbitrary faces are either disjoint or share a unique edge, and every edge belongs to exactly two faces;

(ii) for any vertex v of the graph, if F_v denotes the set of faces incident to v, then any edge common to two faces of F_v contains v; moreover if γ_v denotes the graph whose vertices are elements of F_v, joined by an edge whenever the two corresponding faces share an edge, then γ_v is an elementary cycle.

This allows us to define the *dual surface*, whose vertices are faces of the original surface, such that two vertices are joined by an edge whenever the corresponding faces share an edge; faces are given by the elementary cycles γ_v of the above definition.

Given a combinatorial surface, we then have a natural way to define its associated topological quantum code: the matrix $\mathbf{H}_X$ will be, as previoulsy stated, the incidence matrix of the underlying graph; the matrix $\mathbf{H}_Z$ will be the matrix whose rows are characteristic vectors of faces.

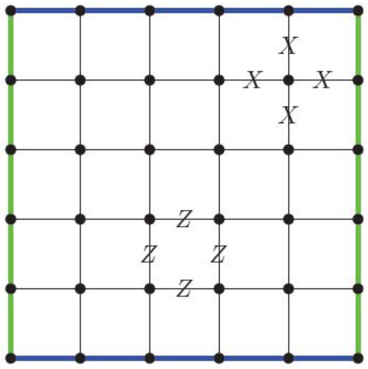
As one might expect, parameters of a topological code can be expressed in term of of the associated surface:

- the block length will be equal to the number of edges of the surface;
- the dimension will be equal to twice the number of connected components of the surface minus its Euler characteristic;
- the minimum distance will be equal to the shortest non-zero cycle of the surface or of its dual that cannot be written as sum of faces.

Topological codes have similar drawbacks as classical cycle codes: it has been recently proved by Delfosse [7] that if the rate k/n of such a code is non-vanishing, then the minimum distance is at most logarithmic in the block length; however, topological codes have highly remarkable decoding permformances.

It will be useful to present an example: we shall discuss Toric codes, introduced by Kitaev [11]; this is actually the first family of topological quantum codes ever proposed.

View the torus T as a square with opposite sides identified; then divide it into a square grid of size $m \times m$. This gives us a surface in the sense that has been discussed above: the graph structure is given by the one-dimensional grid, and the faces are the squares. This way, lines of $\mathbf{H}_X$ are vectors of weight 4 representing the four edges incident to each vertex, and lines of $\mathbf{H}_Z$ represent squares.



The parameters of this code are $[[n, k, d]] = [[2m^2, 2, m]]$: indeed, n is the number of edges of the graph, and k can be computed by the above formula in terms of the parameters of the tiling. Finally, an example of a cycle that is not sum of faces is given by a vertical or horizontal line in the grid, i.e. a shortest non-contractible cycle: this is of length m, and it is immediately seen to be outside the linear span of the faces; since this toric graph is self-dual, it will suffice to show that cycles of legnth less than m are always sum of faces to prove that $d = m$. This can be showed rather quickly by noticing that such cycles can be embedded in a planar portion of the graph, and that all cycles are sum of faces in planar graphs.

Our work will be devoted to the study of the family of topological quantum codes derived from platonic surfaces, a generalization of the five platonic solids.

Chapter 2

An overview of Platonic surfaces

In this chapter, we shall focus on the properties of platonic tilings, that are remarkable even aside from their effects on the construction of quantum codes. Platonic graphs have been studied by several authors: Brooks [4], [5] mainly focuses on an approach based on modular curves, while we will rather use graph theory; we shall first discuss the good symmetry properties of platonic tilings and of their dual, then compute their spectrum, following the work of Gunnells [10] and of DeDeo, Lanphier and Minei [6]. We shall see that the eigenvalues are optimal with respect to expansion properties. We will see that platonic graphs have a very small diameter, which is equal to the number of distinct eigenvalues minus 1; we will also see that platonic graphs are distance-regular.

Finally, we will present an alternative construction by Biggs [3].

2.1 Platonic graphs: first definitions and properties

Definition 2.1.1. Let $n \in \mathbb{N}_{\geq 3}$; we define the *platonic n-th graph* to be $\pi_n := (V_n, E_n)$ where:

- the vertex set V_n is defined by

$$V_n := \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,:\, gcd(a,b,n) = 1 \right\} \Big/ \sim$$

where

$$\binom{a}{b} \sim \binom{a'}{b'} \iff \begin{cases} a = a' \\ b = b' \end{cases} \text{or} \begin{cases} a = -a' \\ b = -b' \end{cases};$$

- the edge set E_n is defined by

$$\binom{a}{b}\binom{c}{d} \in E_n \iff \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \equiv \pm 1 \mod n.$$

Notice that the condition "$gcd(a, b, n) = 1$" is equivalent to "$ka = kb = 0 \Rightarrow k = 0 \in \mathbb{Z}/n\mathbb{Z}$", and that in the case $n = p$ a prime, we have that

$$V_p = \left\{ \binom{a}{b} \in (\mathbb{F}_p)^2 \setminus \{\underline{0}\} \right\} \Big/ \sim;$$

moreover, $\#V_p = \frac{p^2-1}{2}$(= half the number of non-zero elements of $\mathbb{F}_p$).

Also notice that when n is not a prime, the definition of V_n is not universally accepted: for instance for $n = p^m$ a prime power, DeDeo, Lanphier and Minei [6] define $V_n := \left\{ \binom{a}{b} \in (\mathbb{F}_n \times \mathbb{F}_n) \setminus \{\underline{0}\} \right\} / \sim$.

From now on, the notation $\binom{a}{b}$ shall both denote elements of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and of V_n (that is to say, their classes modulo ±1); what we mean should be clear from the context.

We have the following properties:

Proposition 2.1.1. *For every couple of vertices* $\binom{a}{b}, \binom{c}{d} \in V_n$ *such that* $\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in (\mathbb{Z}/n\mathbb{Z})^\times$, *we have that* $\#\left(N\binom{a}{b} \cap N\binom{c}{d}\right) = 2$ *(where $N(X)$ denotes the neighbourhood of X, i.e. all the vertices connected to X).*

In particular, for any edge in π_n there are exactly two paths of length 2 joining the first and the last vertex of the edge; we will refer to this as the two-step property*.*

Proof. We have that a given $\binom{x}{y}$ belongs to $N\binom{a}{b} \cap N\binom{c}{d}$ if and only if

$$\begin{cases} \det \begin{bmatrix} a & x \\ b & y \end{bmatrix} = \pm 1 \\ \det \begin{bmatrix} c & x \\ d & y \end{bmatrix} = \pm 1 \end{cases}$$

Notice that up to exchanging a solution $\binom{x}{y}$ with its opposite $\binom{-x}{-y}$, we may assume that $\det \begin{bmatrix} a & x \\ b & y \end{bmatrix} = 1$.

Now the matrix $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is invertible, since its determinant belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$; thus the equation $\binom{x}{y} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \binom{r}{s}$ always admits a solution, namely $\forall \binom{x}{y} \in V_n \quad \exists\, r, s \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\begin{pmatrix} x \\ y \end{pmatrix} = r \begin{pmatrix} a \\ b \end{pmatrix} + s \begin{pmatrix} c \\ d \end{pmatrix}.$$

Let $D := \det \begin{bmatrix} a & c \\ b & d \end{bmatrix}$; the above equations become

$$\begin{cases} 1 & = r \cdot \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \\ \pm 1 & = s \cdot \det \begin{bmatrix} c & a \\ d & b \end{bmatrix} \end{cases}$$

i.e.

$$\begin{cases} r & = D^{-1} \\ s & = \pm D^{-1} \end{cases}$$

Thus $S := N\binom{a}{b} \cap N\binom{c}{d} = \left\{ D^{-1} \cdot \left[\binom{a}{b} \pm \binom{c}{d} \right] \right\}$

We can easily see that $\#S = 2$: indeed, if by contradiction $D^{-1} \cdot \left[\binom{a}{b} + \binom{c}{d}\right] = \pm D^{-1} \cdot \left[\binom{a}{b} - \binom{c}{d}\right]$, then either $2 \cdot \binom{c}{d} = \binom{0}{0}$ or $2 \cdot \binom{a}{b} = \binom{0}{0}$, which would imply $2 = 0 \in \mathbb{Z}/n\mathbb{Z}$ by definition of V_n, impossible since $n \geq 3$. □

Proposition 2.1.2. *For every $X = \binom{a}{b} \in V_n$, we have that $N(X)$ is a (connected) cycle of length n; in particular, π_n is regular of degree n.*

Proof. We first prove that $N(X) \neq \emptyset$, i.e. that the equation $1 = \det \begin{bmatrix} a & x \\ b & y \end{bmatrix} = ya - xb$ has solutions mod n; notice that if this is the case, then this equality automatically implies $gcd(x, y, n) = 1$, i.e. $\binom{x}{y} \in V_n$.

If we set $k := gcd(a, b)$, then by definition of V_n, we have that $gcd(k, n) = 1$, i.e. k is invertible mod n; now write k as a linear combination of a and b, say $k = y'a - x'b$: by reducing the equation mod n and by multiplying by k^{-1}, we get

$$1 = (k^{-1}y')a - (k^{-1}x')b =: ya - xb\,(\in \mathbb{Z}/n\mathbb{Z}).$$

Thus $N(X) \neq \emptyset$; as noticed in the above proposition, every $\binom{x}{y}$ in V_n can be written as a linear combination of X and of any of its neighbours, i.e. $\binom{x}{y} = r\binom{a}{b} + s\binom{c}{d}$ for a fixed $\binom{c}{d} \in N(X)$.

If $\binom{x}{y} \in N(X)$, then we may assume without loss of generality that $1 = \det \begin{bmatrix} a & x \\ b & y \end{bmatrix} (= s)$, and thus

$$N(X) = \left\{ X_s := \begin{pmatrix} c \\ d \end{pmatrix} + s \cdot \begin{pmatrix} a \\ b \end{pmatrix} \;:\; s \in \mathbb{Z}/n\mathbb{Z} \right\} / \sim .$$

Notice that every X_s is connected to X_{s+1}, and thus $N(X)$ is a cycle; to prove that it has cardinality n, it suffices to show that $X_s \nsim X_{s'}\, \forall s \neq s'$:

- if $X_s = X_{s'}$, then $\binom{c}{d} + s\binom{a}{b} = \binom{c}{d} + s'\binom{a}{b}$, i.e. $(s - s')\binom{a}{b} = \binom{0}{0}$, which implies $s = s'$ by definition of V_n;
- if $X_s = -X_{s'}$, then $\binom{c}{d} + s\binom{a}{b} = -\binom{c}{d} - s'\binom{a}{b}$, i.e. $2\binom{c}{d} = -(s + s')\binom{a}{b}$; thus

  $$2 = \det \begin{bmatrix} a & 2c \\ b & 2d \end{bmatrix} = \det \begin{bmatrix} a & -(s+s')a \\ b & -(s+s')b \end{bmatrix} = 0,$$

  a contradiction since $n \geq 3$.

□

2.2 From graphs to surfaces

Proposition 2.1.2, together with the two-step property, allows us to define a tiling of a surface from these graphs:

Definition 2.2.1. A *(combinatorial) surface* is a triplet $S := (V, E, F)$ where

- V is a set of vertices and E is a set of edges of V, i.e. (V, E) is a graph;
- F is a collection of cycles called *faces* satisfying the following properties:
  (i) every element of F is an *elementary* cycle, i.e. it cannot be written as the union of two non-empty cycles;
  (ii) two arbitrary faces are either disjoint or share a unique edge, and every edge belongs to exactly two faces;
  (iii) for any vertex $v \in V$, if F_v denotes the set of faces incident to v, then any edge common to two faces of F_v contains v; moreover if γ_v denotes the graph whose vertices are elements of F_v, joined by an edge whenever the two corresponding faces share an edge, then γ_v is an elementary cycle.

Definition 2.2.2. For every $n \geq 3$, we define the *platonic n-th surface* to be $S_n := (V_n, E_n, F_n)$ where $F_n := \{\text{cycles of length 3 in } \pi_n\}$; we will often denote the surface S_n simply by π_n.

Recall that given two graphs $G = (V, E)$ and $G' = (V', E')$, a morphism of graphs between G and G' is a map $\Phi : V \to V'$ that sends edges to edges; an isomorphism of graphs is a morphism that is bijective on vertices and edges.

Proposition 2.2.1. *We have that S_n is indeed a surface in the sense of the above definition.*

Proof. (i) Triangles are obviously elementary since cycles cannot have length 1 nor 2 by definition of a graph.

(ii) The fact that two distinct faces are either disjoint or share a unique edge is a general property of all cycles of length 3: indeed, if C_1 and C_2 are two such cycles, then $\#(C_1 \cap C_2)$ cannot be equal to 2, since an edge of a cycle of length 3 is uniquely determined by the other two edges; thus $\#(C_1 \cap C_2)$ can only be either 0 or 1, as requested.

The fact that every edge belongs to exactly two faces has been proved by Prop. 2.1.1 - it is nothing but the two-step property.

(iii) A length-3 cycle incident to $X \in V_n$ must be of the form $(XX', X'X'', X''X)$ for some $X', X'' \in N(X)$, with $X'X'' \in E_n$; but as seen in the proof of the above proposition, $N(X)$ is an elementary cycle, i.e. we may lebel its elements as $N(X) = \{X_m : m \in \mathbb{Z}/n\mathbb{Z}\}$ where $X_m \neq X_{m'} \, \forall \, m \neq m'$ and $X_m X_{m+1} \in E_n \, \forall \, m \in \mathbb{Z}/n\mathbb{Z}$.

Thus a face incident to X is of the form $F_m := (XX_m, X_m X_{m+1}, X_{m+1}X)$ for some $m \in \mathbb{Z}/n\mathbb{Z}$, and hence any edge common to two faces must necessarily be of the form XX_k for some $k \in \mathbb{Z}/n\mathbb{Z}$. Moreover the map

$$\begin{aligned} N(X) &\to F_X \\ X_m &\mapsto F_m \end{aligned}$$

is an isomorphism of graphs, so that the property is proved.

□

Notice that $\#E_n = \frac{n}{2} \cdot \#V_n$ (since π_n is n-regular) and $\#F_n = \frac{2}{3} \cdot \#E$ (every edge is common to two faces, every face has three edges). This allows us to compute easily these parameters when n is a prime, since we have a simple formula to express the cardinality of the set of vertices:

Remark 2.2.1. For any prime $p \geq 3$, the parameters of the platonic tiling π_p are

$$\#V_p = \frac{p^2-1}{2}, \quad \#E_p = \frac{p \cdot (p^2-1)}{4}, \quad \#F_p = \frac{p \cdot (p^2-1)}{6}.$$

We can define the dual surface $\pi'_n := (V'_n = F_n, E'_n = E_n, F'_n = V_n)$; for $n = 3, 4, 5$, it can be easily proved that via this contruction, we find the platonic solids (hence the name of "platonic graphs"): $\pi_3 \equiv \pi'_3$ is the tetrahedron, π_4 is the octahedron, π'_4 is the cube, π_5 is the icosahedron and π'_5 is the dodecahedron.

2.3 Further properties of platonic surfaces and of their duals

We shall now present some remarkable properties of π_n and of π'_n.

Theorem 2.3.1. *For all $n \geq 3$, we have that π_n is arc-transitive: that is to say, for every four vertices $X, Y, Z, W \in V_n$ such that $XY \in E_n$, $ZW \in E_n$, there exists an isomorphism of graphs $\varphi : \pi_n \to \pi_n$ such that $\varphi(X) = Z$ and $\varphi(Y) = W$.*

In particular, π_n is also vertex-transitive for every $n \geq 3$.

Proof. Let $G := \{M \in \mathcal{M}_{\mathbb{Z}/n\mathbb{Z}}(2 \times 2) \,:\, \det(M) = 1\}/\langle \pm \mathrm{Id} \rangle$ $(= PSL_2(\mathbb{F}_p)$ for $n = p$ a prime); then G acts on V_n via left multiplication: for $[M] \in G$, define

$$\begin{aligned} \varphi_{[M]} : V_n &\to V_n \\ \begin{pmatrix} a \\ b \end{pmatrix} &\mapsto M \cdot \begin{pmatrix} a \\ b \end{pmatrix} \end{aligned}$$

We have that $\varphi_{[M]}$ is well-defined, i.e. it just depends on the class of M in G thanks to the definition of V_n; it is obviously a bijection since the matrices we are considering are invertible. Moreover $\varphi_{[M]}$ is a morphism of graphs: indeed, let $\left(\binom{a}{b}, \binom{c}{d}\right) \in E_n$; we may assume without loss of generality that $\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = 1$. Then we have that

$$\det \left[M\begin{pmatrix} a \\ b \end{pmatrix} \; M\begin{pmatrix} c \\ d \end{pmatrix} \right] = \det(M) \cdot \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = 1$$

$$\Rightarrow \left(\varphi_{[M]}\begin{pmatrix} a \\ b \end{pmatrix}, \varphi_{[M]}\begin{pmatrix} c \\ d \end{pmatrix} \right) = \left(M\begin{pmatrix} a \\ b \end{pmatrix}, M\begin{pmatrix} c \\ d \end{pmatrix} \right) \in E_n.$$

We thus get an isomorphism of graphs $\varphi_{[M]} : \pi_n \to \pi_n$ for every $[M] \in G$; we are thus left to prove that for every couple of edges $l, l' \in E_n$ there exists a $\varphi_{[M]}$ sending l to l':
let $l = \left(\binom{a}{b}, \binom{c}{d}\right)$, $l' = \left(\binom{x}{y}, \binom{z}{w}\right)$; again, we may assume without loss of generality that $\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \det \begin{bmatrix} x & z \\ y & w \end{bmatrix} = 1$.

We need to find an $M \in \mathcal{M}_{\mathbb{Z}/n\mathbb{Z}}(2 \times 2)$ with determinant equal to 1 such that

$$\begin{cases} M\binom{a}{b} &= \binom{x}{y} \\ M\binom{c}{d} &= \binom{z}{w} \end{cases};$$

this happens $\iff M\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} x & z \\ y & w \end{bmatrix} \iff M = \begin{bmatrix} x & z \\ y & w \end{bmatrix}\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1}$. Such an M clearly has determinant 1, and thus the theorem is proved.

Also notice that the matrix $M' := \begin{bmatrix} x & -z \\ y & -w \end{bmatrix}\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1}$ would also have worked, which means that we can decide whether to send the vertex $\binom{a+c}{b+d}$ to $\binom{x+z}{y+w}$ or to $\binom{x-z}{y-w}$. □

Corollary 2.3.1. *π'_n is arc-transitive in the sense of the above proposition, and thus also vertex transitive, $\forall n \geq 3$.*

Proof. Let l_1, l_2 be two arbitrary edges of π'_n, say

$$l_1 = \left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix}\begin{pmatrix} e' \\ f' \end{pmatrix}\right),$$

$$l_2 = \left(\begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}\begin{pmatrix} h \\ k \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix}\begin{pmatrix} h' \\ k' \end{pmatrix}\right).$$

Then as seen in the proof of the above theorem, we may find a matrix $M \in \mathcal{M}_{\mathbb{Z}/n\mathbb{Z}}(2 \times 2)$ having determinant 1 such that

$$M\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}, M\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} z \\ w \end{pmatrix},$$
$$M\begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} h \\ k \end{pmatrix}, M\begin{pmatrix} e' \\ f' \end{pmatrix} = \begin{pmatrix} h' \\ k' \end{pmatrix}.$$

Indeed, the first two equations are straightforward from the proof; the third and fourth ones come from the remark at the end of the proof, since $\binom{e}{f} = \binom{a\pm c}{b\pm d}$ and $\binom{e'}{f'} = \binom{a\mp c}{b\mp d}$, and similarly for $\binom{h}{k}$ and $\binom{h'}{k'}$. Thus if we define

$$\begin{aligned} &\varphi'_{[M]} : V'_n \to V'_n \\ &\{\alpha, \beta, \gamma\} \mapsto \{M\alpha, M\beta, M\gamma\} \end{aligned}$$

we get a map that is well-defined (since multiplication by M preserves incidence, and thus sends triangles to triangles), and that sends the (oriented) edge l_1 to l_2; moreover it is clearly a morphism of graphs (since if two faces share an edge $\alpha\beta$, then their images will share $M\alpha M\beta$) and it is bijective since the matrix M is invertible.

We have therefore constructed the requested isomorphism of graphs. □

Proposition 2.3.1. *For every prime $p \geq 5$, we have that the diameter of π_p is equal to 3.*

Proof. Let $= diam(\pi_p) = dist(x, y)$ for $x, y \in V_p$. Since π_p is vertex-transitive, we may assume that $x = \binom{0}{1}$; we then have two cases:

- $y = \binom{\alpha}{\beta}$ with $\alpha \neq 0$: thus $\alpha \in \mathbb{F}_p^\times$, and we have that $\binom{0}{1}\binom{1}{\alpha^{-1}(1+\beta)} \in E_p$ and $\binom{1}{\alpha^{-1}(1+\beta)}\binom{\alpha}{\beta} \in E_p$: thus $dist(x, y) \leq 2$.
- $y = \binom{0}{\beta}$: then necessarily $\beta \in \mathbb{F}_p^\times$, and thus we get $\binom{0}{1}\binom{1}{1} \in E_p$, $\binom{1}{1}\binom{\beta^{-1}}{1+\beta^{-1}} \in E_p$, $\binom{\beta^{-1}}{1+\beta^{-1}}\binom{0}{\beta} \in E_p$;

  thus $dist(x, y) \leq 3$.

Now notice that $N\binom{0}{1} = \left\{\binom{1}{k} \ : \ k \in \mathbb{F}_p\right\}$ and $N\binom{0}{\beta} = \left\{\binom{\beta^{-1}}{h} \ : \ h \in \mathbb{F}_p\right\}$; thus if $\beta \neq 0, \pm 1$ (and such a β exists if $p \geq 5$), we have that

$$N\begin{pmatrix}0\\1\end{pmatrix} \cap N\begin{pmatrix}0\\\beta\end{pmatrix} = \emptyset,$$

i.e. $dist\left(\binom{0}{1}, \binom{0}{\beta}\right) \geq 3$.

Thus $diam(\pi_p) = 3$ for $p \geq 5$. □

Remark 2.3.1. We shall see that the number of distinct eigenvalues of π_p is 4 for every prime $p \geq 5$, so that

$$diam(\pi_p) + 1 = \#\{\text{distinct eigenvalues of } \pi_p\}.$$

Remark 2.3.2. *It can be easily seen that $diam(\pi_3) = 1$, i.e. π_3 is the complete graph on 4 vertices (we had actually already noticed that it is a tetrahedron).*

Corollary 2.3.2. *π_p (and thus also π'_p) is connected for every prime $p \geq 3$.*

Now this actually allows us to prove that all platonic graphs are distance-regular for every p prime: first recall the following

Definition 2.3.1. A graph $G = (V, E)$ of diameter D is said to be *distance-regular* if for every $i = 0, \cdots, D$ there are integeres $a_i, b_i, c_i \in \mathbb{N}_{\geq 0}$ such that for every couple of vertices $v, w \in V$ with $dist(v, w) = i$ we have that

$$\#\left(\partial B_i(v) \cap N(w)\right) = a_i, \quad \#\left(\partial B_{i+1}(v) \cap N(w)\right) = b_i,$$

$$\#\left(\partial B_{i-1}(v) \cap N(w)\right) = c_i.$$

(where $\partial B_j(x)$ denotes the elements of V at distance j from x, $N(y)$ denotes the neighbours of y).

Notice that in particular any such graph is regular of degree $k = a_i + b_i + c_i$ (for any i); the vector

$$(b_0, \cdots, b_{d-1}; c_1, \cdots, c_d)$$

is called the *intersection vector* of G, and its elements are called *intersection numbers*; also notice that we always have

$$b_0 = \#\left(\partial B_1(v) \cap N(v)\right) = k, \quad c_0 = b_D = 0, \quad k = a_i + b_i + c_i \,\forall\, i.$$

Proposition 2.3.2. *The platonic graphs π_p are distance-regular for every prime $p \geq 5$, with intersection vector*

$$(b_0,\, b_1,\, b_2;\, c_1,\, c_2,\, c_3) = (p,\, p-3,\, 1;\, 1,\, 2,\, p)\,.$$

Proof. Let $v, w \in V_p$ be at distance i; thanks to the vertex-transitivity of the graph, we may assume $v = \binom{0}{1}$. Let $w = \binom{\alpha}{\beta}$; since the diameter of π_p is equal to 3, we only have three cases to discuss:

i=1: since $vw \in E_p$, $N(w) = (N(w) \cap \{v\}) \sqcup (N(w) \cap N(v)) \sqcup (N(w) \cap \partial B_2(v))$; but $N(w) \cap \{v\} = \{v\}$ and $\#(N(w) \cap N(v)) = 2$ thanks to the two-step property, so that

$$b_1 = \#(\partial B_2(v) \cap N(w)) = \#N(w) - \#(N(w) \cap \{v\}) - \#(N(w) \cap N(v)) =$$

$$p - 1 - 2 = p - 3.$$

We also have $c_1 = \#(\partial B_0(v) \cap N(w)) = 1$.

i=2: recall that from the proof of proposition 2.3.1, since $d\left(\binom{0}{1}, \binom{\alpha}{\beta}\right) = 2$, we have that $\alpha \in \mathbb{F}_p^\times \setminus \{\pm 1\}$; moreover, thanks again to the proof of the proposition,

$$\partial B_3\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \left\{ \begin{pmatrix} 0 \\ \gamma \end{pmatrix} \,:\, \gamma \in \mathbb{F}_p^\times \setminus \{\pm 1\} \right\}$$

and thus

$$\partial B_3\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \cap N\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha^{-1} \end{pmatrix}$$

which implies $b_2 = \#(\partial B_3(v) \cap N(w)) = 1$; moreover, since

$$\det \begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix} = -\alpha \in \mathbb{F}_p^\times,$$

we have by proposition 2.1.1 that $2 = \#(N(v) \cap N(w)) = c_2$.

i=3: again by proposition 2.3.1, we have $\alpha = 0$, $\beta \neq 0, \pm 1$, and thus

$$\partial B_3\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \cap N\begin{pmatrix} 0 \\ \beta \end{pmatrix} = \left\{\begin{pmatrix} 0 \\ \gamma \end{pmatrix} \,:\, \gamma \in \mathbb{F}_p^\times \setminus \{\pm 1\}\right\} \cap \left\{\begin{pmatrix} \beta^{-1} \\ \delta \end{pmatrix} \,:\, \delta \in \mathbb{F}_p\right\}$$
$$= \emptyset.$$

Thus $N(w) = N(w) \cap \partial B_2(v)$, so that $c_3 = \#(N(w) \cap \partial B_2(v)) = p$.

□

Remark 2.3.3. The tetrahedron π_3 is well-known to be distance-regular (it is actually distance-transitive) with intersection vector $(3; 1)$; thus all platonic graphs π_p are distance-regular for p (odd) prime.

2.4 The spectrum of π_p

Recall that given any graph $G = (V, E)$, we can define its *adjacency matrix* to be $A_G \in \mathcal{M}_{\mathbb{C}}(|V| \times |V|)$ where $A_{ij} = 1$ if the vertex v_i is connected to v_j, $A_{ij} = 0$ for all other pairs of vertices. The *spectrum* of the graph G is defined to be the set of eigenvalues of A_G; equivalently, if we set $\mathbb{C}^V := \{\text{functions } f : V \to \mathbb{C}\}$, the spectrum of G can be defined to be the set of eigenvalues of the adjacency operator $\mathrm{Ad} : \mathbb{C}^V \to \mathbb{C}^V$ where $\mathrm{Ad}(f)(v) := \sum_{w \in N(v)} f(w)$. Notice that since all adjancency matrices are symmetric, the spectrum of any graph is real.

In this section we will compute the spectrum of the platonic graphs π_p for any odd prime p; the knowledge of the spectrum of a graph is relevant to understand if it has good *expansion properties*, i.e. if any subset of the vertex set that is not too big is connected to a huge number of vertices in its complement. Graphs with good expansion properties are useful in many areas, particularly in computer sciences (e.g., to build efficient networks) and cryptography; the difference between the largest and second largest eigenvalues of a graph yields a lower bound on the expansion ratio of the graph, a parameter that express the quality of its expansion properties. Therefore, a graph is more interesting from this point of view if it has a large *spectral gap*, i.e. a large difference between the first and second largest eigenvalues; we shall see that platonic graphs are asymptotically optimal in this sense.

Fix an odd prime p; to discuss the spectrum of the platonic p-th graph, we will need a decomposition of π_p:

Definition 2.4.1. *We shall define the following group action:*

$$\begin{array}{rcl} \mathbb{F}_p^\times \times V_p & \to & V_p \\ \left(k, \binom{a}{b}\right) & \mapsto & k \cdot \binom{a}{b} := \binom{ka}{kb}. \end{array}$$

We say that two vertices in the same orbit are associates*; notice that this is* not *an action of graphs, since it does not preserve edges.*

Now fix a vertex $v \in V_p$; the orbit of v has cardinality $\frac{p-1}{2}$ (since $-w = w$ for every $w \in V_p$). Also notice that if $w \in V_p$ is a vertex that is not associate to v, then it is adjacent to a unique associate of v: indeed, write

$$v = \begin{pmatrix} a \\ b \end{pmatrix}, \quad w = \begin{pmatrix} c \\ d \end{pmatrix}.$$

Since w is not an associate of v, we have that $D := \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \neq 0$, and thus w is only adjacent to $D^{-1} \cdot v = -D^{-1} \cdot v$.

Now for every associate $k \cdot v$ of v, consider the "cap" $C_{kv} := \{kv\} \cup N(kv)$, which is a "wheel" having center kv connected to the vertices of the p-gon $N(kv)$. Notice that caps of different associates are disjoint, since if $kv \neq k'v$, then $kv \notin N(k'v)$, $k'v \notin N(kv)$ and $N(kv) \cap N(k'v) = \emptyset$.

Thus the cardinality of the union of all caps is

$$\#\left(\bigsqcup_{w \text{ associates to } v} C_w \right) = \sum_{w \text{ associates to } v} \#C_w = \frac{p-1}{2} \cdot (p+1) = \frac{p^2-1}{2} = \#V_p.$$

This means that the (disjoint) union of all caps exhausts the vertex set of π_p. Moreover, we have that if a vertex w is not associate to v, then it is connected to exactly two vertices on the p-gon of each cap, and to one associate of v.

Indeed, we have already seen that every such a w is adjacent to exactly one associate of v; now thanks to the transitivity of π_p, we may assume that $v = \binom{0}{1}$; thus $w = \binom{c}{d}$ with $c \neq 0$, since w is not associate to v. For every $k \in \mathbb{F}_p^\times$, the p-gon of the cap C_{kv} is equal to $\left\{\binom{k^{-1}}{x} : x \in \mathbb{F}_p\right\}$; thus in order to look for elements of this form adjacent to w, we have to solve the equation

$$\pm 1 = \det \begin{bmatrix} c & k^{-1} \\ d & x \end{bmatrix} = cx - dk^{-1},$$

which has exactly two solutions since $c \neq 0$.

This construction will allow us to build the eigenvectors of the adjacency matrix A_p of π_p:

Definition 2.4.2. Fix a vertex $v \in V_p$; we then define the following vectors of $\mathbb{C}^{V_p}$:

(1) $S_v : V_p \to \mathbb{C}$ is such that

$$S_v(w) := \begin{cases} p & \text{if } w = k \cdot v \text{ for some } k \in \mathbb{F}_p^\times, \text{ i.e. if } w \text{ is associate to } v; \\ -1 & \text{otherwise.} \end{cases}$$

(2) Let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a non-trivial character with $\chi(-1) = 1$; then we set $P^+_{\chi,v} : V_p \to \mathbb{C}$ to be such that

   (a) $P^+_{\chi,v}(k \cdot v) := \chi(k)\sqrt{p}$ for all $k \in \mathbb{F}_p^\times$;

   (b) $P^+_{\chi,v}(w) := \chi(k)$, if w is not associate to v and $k \cdot v$ is the (unique) associate to v adjacent to w.

(3) Let χ be as in (2); we then define $P^-_{\chi,v}$ in a similar way to $P^+_{\chi,v}$, simply by putting $-\sqrt{p}$ instead of $\sqrt{p}$ in point (a).

Remark 2.4.1. The definitions of $P^+_{\chi,v}$ and of $P^-_{\chi,v}$ are well-posed since $\chi(-1) = 1$: indeed, this implies that $\chi(-k) = \chi(-1) \cdot \chi(k) = \chi(k)$.

Proposition 2.4.1. *We have that S_v, $P^+_{\chi,v}$ and $P^-_{\chi,v}$ are eigenvectors for the adjacency operator A_p of π_p with eigenvalues -1, $\sqrt{p}$ and $-\sqrt{p}$, respectively.*

Proof. We shall first study S_v: consider the cap decomposition of V_p with centers the associates of v; if kv is an associate of v, then none of its neighbours can be associate to v since associates are never adjacent: thus

$$A_p(S_v)(kv) = \sum_{x \in N(kv)} S_v(x) = \sum_{x \in N(kv)} (-1) = -p = -S_v(kv).$$

If w is not associate to v, then it has been showed that it is adjacent to a unique associate of v, say kv; hence

$$\begin{aligned} A_p(S_v)(w) = \sum_{x \in N(w)} S_v(x) = S_v(kv) + \sum_{x \in N(w),\, x \neq kv} S_v(x) = p + (p-1)(-1) \\ = 1 = -S_v(w) \end{aligned}$$

which means that S_v is an eigenvector with eigenvalue -1.

Now let us focus on $P^+_{\chi,v}$: consider the same cap decomposition, and let kv be an associate of v; then every neighbour x of kv is not associate to v, and thus we have

$$\begin{aligned} A_p(P^+_{\chi,v})(kv) = \sum_{x \in N(kv)} P^+_{\chi,v}(x) = \sum_{x \in N(kv)} \chi(k) = p \cdot \chi(k) \\ = \sqrt{p} \cdot \chi(k)\sqrt{p} = \sqrt{p} \cdot P^+_{\chi,v}(kv). \end{aligned}$$

Now let w be a vertex that is not associate to v; then it has been showed that it is adjacent to exactly one associate of v, say kv, and to two elements on the p-gon of each associate of v; now if we list the associates of v as $\left\{h \cdot v \,:\, h = 1, \cdots \frac{p-1}{2}\right\}$, we then have

$$\begin{aligned} A_p(P^+_{\chi,v})(w) = \sum_{x \in N(w)} P^+_{\chi,v}(x) = P^+_{\chi,v}(kv) + \sum_{x \in N(w),\, x \neq kv} P^+_{\chi,v}(x) \\ = \chi(k)\sqrt{p} + \sum_{h=0}^{\frac{p-1}{2}} 2 \cdot \chi(h). \end{aligned}$$

But now, since $\chi(-1) = 1$ we have that $\chi(h) = \chi(-h)$ for every $h \in \mathbb{F}_p^\times$, and thus

$$\sum_{h=0}^{\frac{p-1}{2}} 2 \cdot \chi(h) = \sum_{h=0}^{\frac{p-1}{2}} \chi(h) + \sum_{h=0}^{\frac{p-1}{2}} \chi(h) = \sum_{h=0}^{\frac{p-1}{2}} \chi(h) + \sum_{h=0}^{\frac{p-1}{2}} \chi(-h) = \sum_{h \in \mathbb{F}_p^\times} \chi(h) = \langle \chi, 1 \rangle$$

where 1 is the trivial character, $1(h) = 1$ for every $h \in \mathbb{F}_p^\times$; but the character χ is different from 1 by assumption, and thus it is orthogonal to it, i.e. the above expression is equal to zero: this implies that

$$A_p(P^+_{\chi,v})(w) = \chi(k)\sqrt{p} = \sqrt{p} \cdot P^+_{\chi,v}(w).$$

Thus $P^+_{\chi,v}$ is an eigenvector with eigenvalue $\sqrt{p}$; a similar computation shows that $P^-_{\chi,v}$ is an eigenvector with eigenvalue $-\sqrt{p}$. □

Definition 2.4.3. *We define the eigenspaces* $S := \langle S_v \, : \, v \in V_p \rangle$ *(with eigenvalue* -1*),* $P^+ := \langle P^+_{\chi,v} \, : \, \chi \in \widehat{\mathbb{F}_p^\times}, \, \chi \neq 1, \, \chi(-1) = 1, \, v \in V_p \rangle$ *(with eigenvalue* $\sqrt{p}$*) and* $P^- := \langle P^-_{\chi,v} \, : \, \chi \in \widehat{\mathbb{F}_p^\times}, \, \chi \neq 1, \, \chi(-1) = 1, \, v \in V_p \rangle$ *(with eigenvalue* $-\sqrt{p}$*).*

Now we have that these are actually all the possible eigenvectors of A_p that are associated to eigenvalues different from the regularity p: we will just sketch the proof of this fact in the following definition; a formal proof can be found in the article by Gunnells [10]. In [6], DeDeo, Lanphier and Minei extend this computations to the platonic graph π_q for q a prime power, although with the alternative definition that was given at the beginning of this chapter.

Proposition 2.4.2. *We have that* $\dim(S) = p$ *and* $\dim(P^\pm) = \frac{(p+1)(p-3)}{4}$.

Proof. Sketch. The proof follows from representation theory: first notice that the group $\Gamma_p := PSL_2(\mathbb{F}_p)$ acts on the graph π_p via left multiplication, as it was seen in the proof of the edge-transitivity of π_p. This implies that $\mathbb{C}^{V_p}$ is a Γ_p-module: simply define, for $f \in \mathbb{C}^{V_p}$ and $M \in \Gamma_p$, $M \cdot f(v) := f(M \cdot v)$ for every $v \in V_p$.

Thus $\mathbb{C}^{V_p}$ can be seen as a linear representation of Γ_p: it is then natural to look for isomorphisms between its eigenspaces and some irreducible representations of Γ_p, that are well-known (see [1] or [14], for instance). Via this procedure, one can find that S is isomorphic as an Γ_p-module to the Steinberg representation St of degree p; the computation for $P^\pm$ is more complicated, and follows these steps: first fix a character χ with the properties discussed above, and define the subspaces $P^\pm_\chi := \langle P^\pm_{\chi,v} \, : \, v \in V_p \rangle$. Then these Γ_p-modules can be isomorphic either to the principal series representation PS_χ or to the split principal series $SPS_{\pm}$, depending on the character χ; the dimensions of the spaces $P^{\pm}$ turn out to be as stated. □

Corollary 2.4.1. *The eigenvalues of A_p are p with multiplicity 1, -1 with multiplicity p and $\pm\sqrt{p}$ with multiplicity $\frac{(p+1)(p-3)}{4}$ each.*

Proof. Since π_p is p-regular and connected, p is an eigenvalue with multiplicity 1; the multiplicities of the eigenvalues -1 and $\pm\sqrt{p}$ have been computed above. Now

$$1 + p + 2 \cdot \frac{(p+1)(p-3)}{4} = \frac{p^2-1}{2} = \dim(\mathbb{C}^{V_p})$$

which proves that these are the only eigenvalues. □

Remark 2.4.2. The number of distinct eigenvalues of π_p is thus 4, which is equal to the diameter of π_p plus one (see the previous section); this means that the bound $\mathrm{diam}(\pi_p) + 1 \leq \#\{\text{distinct eigenvalues of } \pi_p\}$ is tight.

Also notice that $\lambda := \max\{|\lambda_i| \ : \ \lambda_i \text{ eigenvalue of } \pi_p, \lambda_i \neq p\} = \sqrt{p}$; we shall now prove that this value is optimal, i.e. it cannot be asymptotically smaller.

Indeed, for every d-regular graph with n vertices, we have that $\lambda \geq d \cdot \frac{n-d}{n-1}$; to see this, consider the adjacency matrix A of the graph, then construct a lower and an upper bound on the trace of A^2:

- every element on the diagonal of A^2 is the number of closed walks of length 2 beginning (and ending) at the corresponding vertex, and thus it is exactly equal to d (the number of walks given by moving back and forth along any edge incident to the vertex); thus $\mathrm{Tr}(A^2) = nd$.
- on the other hand, if $\{\lambda_i \ : \ i = 1, \cdots, n\}$ denotes the spectrum of A, then $\mathrm{Tr}(A^2) = \sum \lambda_i^2 \leq d^2 + (n-1)\lambda^2$.

We thus find

$$nd \leq d^2 + (n-1)\lambda^2 \Rightarrow \lambda^2 \geq d \cdot \frac{n-d}{n-1}.$$

Now in our case, $n = \frac{p^2-1}{2}$, $d = p$, so that $\frac{n-d}{n-1}$ goes to 1 as p tends to infinity, i.e.

$$\lambda \geq \sqrt{p} \cdot (1 - o(1)) \text{ as } p \to \infty.$$

2.5 An alternative construction

We shall now present the family $\{T(p) \; : \; p \text{ odd prime}\}$ of 3-regular graphs discussed by Norman Biggs in [3]; as we shall see, they coincide with π'_p for some values of p.

Definition 2.5.1. *Let p be an odd prime, and let $\mathbb{P}^1(p)$ be the projective line over $\mathbb{F}_p$; we will view it as $\mathbb{F}_p \sqcup \{\infty\}$. For every set of four (distinct) points x_1, x_2, x_3, x_4 of $\mathbb{P}^1(p)$, we define their* cross-ratio *to be*

$$(x_1, x_2; x_3, x_4) := \frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)} \in \mathbb{F}_p$$

when one of these points is equal to ∞, we simply neglect the corresponding factors: e.g. $(x_1, x_2; x_3, \infty) := \frac{(x_1 - x_3)}{(x_2 - x_3)}$.

Notice that when we swap two points in the first and/or second couple, the cross-ratio is either unchanged or becomes the inverse: more precisely,

$$(x_2, x_1; x_3, x_4) = (x_1, x_2; x_4, x_3) = (x_1, x_2; x_3, x_4)^{-1}$$

$$(x_2, x_1; x_4, x_3) = (x_1, x_2; x_3, x_4).$$

Thus the following definition is well-posed:

Definition 2.5.2. *Two unordered couples $\{x_1, x_2\}$, $\{x_3, x_4\}$ of points of $\mathbb{P}^1(p)$ are said to be* harmonic conjugated *if and only if $(x_1, x_2; x_3, x_4) = -1$.*

Now this allows us to define a graph $T(p)$: the vertex set $V(T(p))$ will consist of all unordered triplets $\{x, y, z\}$ of $\mathbb{P}^1(p)$, and each triplet $\{x, y, z\}$ will be adjacent to the three triplets

$$\{x', y, z\}, \quad \{x, y', z\}, \quad \{x, y, z'\}$$

where x', y' and z' are chosen in such a way that the couples $\{x, x'\}$ and $\{y, z\}$ are harmonic conjugated, as well as $\{y, y'\}$ and $\{x, z\}$, and as $\{z, z'\}$ and $\{x, y\}$.

Remark 2.5.1. Notice that given any three distinct points α, β, γ of $\mathbb{P}^1(p)$, it is always possible to find a $t \in \mathbb{P}^1(p)$ which is solution of the equation

$$\frac{(\alpha - \beta)(t - \gamma)}{(\alpha - \gamma)(t - \beta)} = -1.$$

Moreover, such a t must clearly be different from α, β and γ; this means that every vertex of $T(p)$ has indeed 3 neighbours, i.e. $T(p)$ is 3-regular.

Also notice that the cardinality of the vertex set of $T(p)$ is equal to the number of unordered triplets of $\mathbb{P}^1(p)$, i.e.

$$\#V(T(p)) = \binom{\#\mathbb{P}^1(p)}{3} = \binom{p+1}{3} = \frac{p\cdot(p^2-1)}{6}$$

which is the cardinality of π'_p.

We have the following

Proposition 2.5.1. *When $p \equiv 1 \mod (4)$, we have that $T(p)$ has two (isomorphic) connected components; when $p \equiv 3 \mod (4)$, it is connected.*

When $p \equiv 1 \mod (4)$, Biggs actually denotes with $T(p)$ one of the two connected components of the graph; we shall adopt the same notation.

Theorem 2.5.1. *The map*

$$\Phi : \pi'_p \to T(p)$$
$$\left\{\begin{pmatrix}a\\b\end{pmatrix}, \begin{pmatrix}c\\d\end{pmatrix}, \begin{pmatrix}e\\f\end{pmatrix}\right\} \mapsto \left\{\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right\},$$

where $\frac{x}{0} := \infty$, is a covering of graphs for every $p \geq 3$, i.e. for every vertex v of π'_n, the restriction map $\Phi_{|N(v)} : N(v) \to T(p)$ is a bijection between $N(v)$ and $N(\Phi(v))$.

Proof. sketch: first notice that the map is well defined, i.e. the quotients $\frac{a}{b}$, $\frac{c}{d}$ and $\frac{e}{f}$ are pairwise different: this is because the three vectors they are obtained from cannot be proportional, since they are adjacent in π_p.

Φ is a morphism of graphs: by proposition 2.1.1, we may assume that $\binom{e}{f} = \binom{a+c}{b+d}$, up to change the order of the couples; now this will allow us to determine explicitely the three neighbours of $\left\{\binom{a}{b}, \binom{c}{d}, \binom{e}{f}\right\}$ in terms of a, b, c and d. An immediate computation will then show that their image are adjacent to the image of the original vertex.

We have to prove that for any vertex v' of V'_p, the induced map from neighbours of v' to neighbours of $\Phi(v')$ is a bijection; since we have already showed that both graphs are 3-regular, it will suffice to show that these induced maps are injective.

Finally, it can be proved that Φ is surjective on vertices, so that the theorem is proved. □

Corollary 2.5.1. *For $p \equiv 1 \mod (4)$, the map $\Phi : \pi'_p \to T(p)$ is a two-folded covering; for $p \equiv 3 \mod (4)$, it is an isomorphism of graphs.*

Proof. The result is immediate since $\#(T(p)) = \#(\pi'_p)/2$ when $p \equiv 1 \mod (4)$ (recall that all fibers have the same cardinality), and $\#(T(p)) = \#(\pi'_p)$ when $p \equiv 3 \mod (4)$. □

Chapter 3

Homological systole of platonic surfaces and of their duals

Recall that given any graph $G = (V, E)$, the set of union of edges $\mathcal{P}(E)$ has a natural structure of $\mathbb{F}_2$-vector space: for instance, by viewing a subset of E as a characteristic vector in $\{0, 1\}^E$, we may view $\mathcal{P}(E)$ as $\{0, 1\}^E = \mathbb{F}_2^E$; we can also explicitely define $A + B := A \cup B \setminus (A \cap B)$, for $A, B \subseteq E$.

Thanks to this structure, one can define the *homological* or *homology systole* of a surface $S = (V, E, F)$ to be the length of its shortest cycle that is not sum of faces; from another point of view, we can define the spaces of formal sums with binary coefficients of vertices, edges and faces, i.e.

$$C_0(S) := \left\{ \sum_{v \in V} \lambda_v v \ : \ \lambda_v \in \mathbb{F}_2 \right\},$$

$$C_1(S) := \left\{ \sum_{l \in E} \lambda_l l \ : \ \lambda_l \in \mathbb{F}_2 \right\},$$

$$C_2(S) := \left\{ \sum_{f \in F} \lambda_f f \ : \ \lambda_f \in \mathbb{F}_2 \right\}.$$

We then have two boundary maps $\partial_2 : C_2(S) \to C_1(S)$ and $\partial_1 : C_1(S) \to C_0(S)$ that send every face f to the sum of its edges $\sum_{l \in f} l$ and every edge l to the sum of its 2 vertices $\sum_{v \in l} v$, extended by $\mathbb{F}_2$-linearity.

It can be easily seen that the composition of the two maps is equal to zero (thus giving a complex); moreover, the kernel of ∂_1 is the set of cycles of the graph and the image of ∂_2 is the set of sum of faces of S, both with the sum operation defined above. The homology systole of S is therefore equal to the length of the shortest element of $\mathrm{Ker}\partial_1$ whose homology class is non-trivial in $\mathrm{Ker}\partial_1/\mathrm{Im}\partial_2$.

In the present chapter we study the homology systole of π_p and of π'_p; we shall see that it is constant for π_p, and at least logarithmic in p for π'_p.

3.1 The platonic surface π_p

We shall begin with π_p for p prime: this computation and its consequences were not present in Riemann's work, and it will provide the minimum distance of the error-correcting codes issued from π_p; our strategy to compute the homology systole will be to exploit the vector space structure of the set of cycles of π_p to use dimension theory:

Proposition 3.1.1. *Let $F := F_p$ denote, as usual, the set of faces of π_p; then*

$$\dim\langle F\rangle = \#F - 1 \left(= \frac{p(p^2-1)}{6} - 1\right).$$

Proof. This is actually a property that is common to all faces set of any connected graph: we need to show that $rank(F) = \#F - 1$.

First notice that any face x is the sum of all other faces: indeed,

$$\sum_{y\in F\setminus\{x\}} y = \sum_{y\in F\setminus\{x\}}\sum_{e\in y} e = \sum_{e\in E_p}\sum_{y\in F\setminus\{x\}\,:\,e\in y} e = \sum_{e\in E_p} \#\{y \in F\setminus\{x\} \;:\; e\in y\}e.$$

But now, $\#\{y \in F\setminus\{x\} \;:\; e \in y\} = \begin{cases} 2 & \text{if } e\notin x \\ 1 & \text{if } e \in x\end{cases}$
by the definition of faces; since we are in characteristic 2, we thus get

$$\sum_{y\in F\setminus\{x\}} y = \sum_{e\in x} e = x \quad \Rightarrow rank(F) \leq \#F - 1.$$

Now to see that equality holds, it suffices to show that any face $x \in F$ cannot be written as a sum of less than $\#F - 1$ faces: let $x \in F \setminus F'$, $F' \subset F$ being an arbitrary subset with $\#F' \leq \#F - 2$.

Then there exists a face $z \in F \setminus (F' \cup \{x\})$; moreover since the graph (and hence its dual) is connected, we may assume that z share an edge e with an element of $F' \cup \{x\}$: if by contradiction all elements of $F \setminus (F' \cup \{x\})$ did not share edges with the complementary set $F' \cup \{x\}$, then they would share edges only with themselves, thus being a connected component strictly contained in the graph, which is a contradiction.

Now such an edge e cannot belong to x (since all of its edges belongs to exactly two faces, one being x and the other belonging to F' by assumption) $\Rightarrow e \in F'$; but then $\#\{y \in F' \,:\, e \in y\} = 1$, since e also belongs to $z \notin F'$, and thus

$$e \notin x, \quad e \in \sum_{y \in F'} y \quad \Rightarrow \quad x \neq \sum_{y \in F'} y$$
$$\Rightarrow dim\langle F\rangle = rank(F) = \#F - 1.$$

□

Theorem 3.1.1. *For $p \gg 0$ a prime, let $d_p :=$ length of the shortest cycle of π_p that is not sum of faces; then $d_p \leq 6$.*

Proof. Let $F := F_p$ denote the set of faces of π_p; it will suffice to find a family H of cycles of length at most 6 such that $dim\langle H\rangle \geq dim\langle F\rangle$ (this would imply $H \nsubseteq \langle F\rangle \Rightarrow$ there exists a cycle $c \in H \setminus \langle F\rangle$, that is to say of length at most 6 and that is not sum of faces).

We will define H to be derived from the family of all cycles of length 6 having extremal points $\binom{0}{\alpha}$ and $\binom{0}{\beta}$: first, let A denote the family of all subsets of V_p of cardinality 2, containing only vertices with first coordinate equal to zero:

$$A := \left\{ \left\{ \begin{pmatrix} 0 \\ \alpha \end{pmatrix} \neq \begin{pmatrix} 0 \\ \beta \end{pmatrix} \right\} \,:\, \alpha, \beta \in \mathbb{F}_p^\times \right\} \in \binom{\mathbb{F}_p^\times}{2}.$$

A will be the set of "extremal points" of H; now to shorten the notation, let $\overline{\alpha} := \binom{0}{\alpha} \in V_p$; we define, for $\{\overline{\alpha}, \overline{\beta}\} \in A$,

$$E_{\{\overline{\alpha},\overline{\beta}\}} := \left\{ \text{paths of the form } \begin{pmatrix} 0 \\ \alpha \end{pmatrix} — \begin{pmatrix} \alpha^{-1} \\ \gamma \end{pmatrix} — \begin{pmatrix} \beta^{-1} \\ \alpha(\gamma\beta^{-1} + (-1)^\varepsilon) \end{pmatrix} — \begin{pmatrix} 0 \\ \beta \end{pmatrix} \right.$$
$$\left. : \gamma \in \mathbb{F}_p,\, \varepsilon \in \{0,1\} \right\}.$$

Now these are clearly (open) paths in π_p, of length 3 since $\overline{\alpha} \neq \overline{\beta} \Rightarrow \alpha^{-1} \neq \pm\beta^{-1}$(it is actually rather easy to show that these are *all* the paths of length 3 between $\overline{\alpha}$ and $\overline{\beta}$).

Now our cycles will be union of two elements of $E_{\{\overline{\alpha},\overline{\beta}\}}$:

$$C_{\{\overline{\alpha},\overline{\beta}\}} := \left\{ x + y \ : \ x \neq y \in E_{\{\overline{\alpha},\overline{\beta}\}} \right\}.$$

We have that $C_{\{\overline{\alpha},\overline{\beta}\}}$ only contains elements of length 4 or 6: let $x \neq y \in E_{\{\overline{\alpha},\overline{\beta}\}}$; then

$$x \leftrightarrow \left\{ \begin{pmatrix} \alpha^{-1} \\ \gamma \end{pmatrix}, \begin{pmatrix} \beta^{-1} \\ \alpha(\gamma\beta^{-1} + (-1)^{\varepsilon_1}) \end{pmatrix} \right\} =: \{x_1, x_2\}$$
$$y \leftrightarrow \left\{ \begin{pmatrix} \alpha^{-1} \\ \delta \end{pmatrix}, \begin{pmatrix} \beta^{-1} \\ \alpha(\delta\beta^{-1} + (-1)^{\varepsilon_2}) \end{pmatrix} \right\} =: \{y_1, y_2\}$$

Now since $\overline{\alpha} \neq \overline{\beta}$, we have that $\alpha^{-1} \neq \pm\beta^{-1}$, and thus $x_1 \neq y_2$, $x_2 \neq y_1$; therefore if $x \neq y$, we can only have 3 cases:

-$x_1 = y_1$: then necessarily $x_2 \neq y_2$, and thus $x + y$ is a cycle of length 4 with starting point $\binom{0}{\beta}$;

-$x_2 = y_2$: then necessarily $x_1 \neq y_1$, and thus $x + y$ is a cycle of length 4 with starting point $\binom{0}{\alpha}$;

-$x_1 \neq y_1$ and $x_2 \neq y_2$: we then get a cycle of length 6.

Our family H will clearly be given by the set of all these cycles, i.e.

$$H := \bigcup_{\{\overline{\alpha},\overline{\beta}\} \in A} C_{\{\overline{\alpha},\overline{\beta}\}}.$$

We will now compute the dimension of $\langle H \rangle$: first notice that

$$dim\langle H \rangle = dim\langle \bigcup_{\{\overline{\alpha},\overline{\beta}\} \in A} C_{\{\overline{\alpha},\overline{\beta}\}} \rangle = dim \sum_{\{\overline{\alpha},\overline{\beta}\} \in A} \langle C_{\{\overline{\alpha},\overline{\beta}\}} \rangle.$$

We shall now prove that $dim \sum_{\{\overline{\alpha},\overline{\beta}\} \in A} \langle C_{\{\overline{\alpha},\overline{\beta}\}} \rangle = \sum_{\{\overline{\alpha},\overline{\beta}\} \in A} dim \langle C_{\{\overline{\alpha},\overline{\beta}\}} \rangle$: notice that $\leq$ always holds; thus to prove the claim we just have to show that any non-trivial sum of the form $\sum_{\{\overline{\alpha},\overline{\beta}\} \in A} X_{\{\overline{\alpha},\overline{\beta}\}}$ with $X_{\{\overline{\alpha},\overline{\beta}\}} \in \langle C_{\{\overline{\alpha},\overline{\beta}\}} \rangle$ is never zero.

But this can be easily seen: indeed, given any $\{\overline{\alpha},\overline{\beta}\}$ in A and any $X_{\{\overline{\alpha},\overline{\beta}\}} \in \langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle$, we have that $X_{\{\overline{\alpha},\overline{\beta}\}}$ contains edges of the form $\binom{\alpha^{-1}}{\gamma}$—$\binom{\beta^{-1}}{\alpha(\gamma\beta^{-1}+(-1)^{\varepsilon})}$, since edges of these kind belong to *one* single element of $E_{\{}\overline{\alpha},\overline{\beta}\}$ (since $\alpha \neq \pm\beta$ and $\binom{\alpha^{-1}}{\gamma} = \binom{\alpha^{-1}}{\delta} \iff \gamma=\delta$, and similarly for ε), and thus cannot erase each other when the corresponding elements of $E_{\{}\overline{\alpha},\overline{\beta}\}$ are summed.

But edges of this kind cannot belong to any element of $\langle C_{\{\overline{\alpha}',\overline{\beta}'\}}\rangle$ for any $\{\overline{\alpha}',\overline{\beta}'\} \neq \{\overline{\alpha},\overline{\beta}\}$ (since either $\alpha \neq \pm\alpha', \pm\beta'$ or $\beta \neq \pm\alpha', \pm\beta'$); this implies that when we consider a non-trivial sum $\sum_{\{\overline{\alpha},\overline{\beta}\}\in A} X_{\{\overline{\alpha},\overline{\beta}\}}$ with $X_{\{\overline{\alpha},\overline{\beta}\}} \in \langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle$, edges of the form $\binom{\alpha^{-1}}{\gamma}$—$\binom{\beta^{-1}}{\alpha(\gamma\beta^{-1}+(-1)^{\varepsilon})}$ cannot erase each other, so that the sum is different from zero and the claim is proved.

Therefore $dim\langle H\rangle = \sum_{\{\overline{\alpha},\overline{\beta}\}\in A} dim\langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle$; now we only have to compute these dimensions.

We claim that $dim\langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle = \#E_{\{\overline{\alpha},\overline{\beta}\}}-1$: indeed, fix an element $z \in E_{\{\overline{\alpha},\overline{\beta}\}}$; then

$$C_{\{\overline{\alpha},\overline{\beta}\}} = \Big\{x+y \,:\, x\neq y \in E_{\{\overline{\alpha},\overline{\beta}\}}\Big\} \supseteq \Big\{z+w \,:\, w \in E_{\{\overline{\alpha},\overline{\beta}\}} \setminus \{z\}\Big\} =: K.$$

Now if $x \neq y$ are two elements different from z, then $x+y = (z+x)+(z+y)$ with $x, y \in E_{\{\overline{\alpha},\overline{\beta}\}} \setminus \{z\}$, and thus

$$\Big\{x+y \,:\, x\neq y \in E_{\{\overline{\alpha},\overline{\beta}\}}\Big\} \subseteq \langle\Big\{z+w \,:\, w \in E_{\{\overline{\alpha},\overline{\beta}\}} \setminus \{z\}\Big\}\rangle$$

$$\Rightarrow \langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle = \langle K\rangle.$$

Now the elements of $E_{\{\overline{\alpha},\overline{\beta}\}}$ are linearly independent (we have shown above that every "central edge" $\binom{\alpha^{-1}}{\gamma}$—$\binom{\beta^{-1}}{\alpha(\gamma\beta^{-1}+(-1)^{\varepsilon})}$ of an element cannot belong to any other element of $E_{\{\overline{\alpha},\overline{\beta}\}}$), and hence also the elements of K are linearly independent; therefore

$$dim\langle C_{\{\overline{\alpha},\overline{\beta}\}}\rangle = rank(K) = \#K = \#E_{\{\overline{\alpha},\overline{\beta}\}} - 1.$$

But this quantity can be easily computed: indeed, it is immediately seen that if $(\gamma,\varepsilon) \neq (\gamma',\varepsilon')$, then the corresponding elements of $E_{\{\overline{\alpha},\overline{\beta}\}}$ are different, and hence

$$\#E_{\{\overline{\alpha},\overline{\beta}\}} = \#(\mathbb{F}_p \times \mathbb{F}_2) = 2p.$$

We then have

$$dim\langle H\rangle = \sum_{\{\overline{\alpha},\overline{\beta}\}\in A} \#E_{\{\overline{\alpha},\overline{\beta}\}} - 1 = \sum_{\{\overline{\alpha},\overline{\beta}\}\in A} (2p-1) = (2p-1)\cdot \#A.$$

Now computing the cardinality of A is very easy: we have $p-1$ choices for an $\alpha \neq 0$, and thus $\frac{p-1}{2}$ choices for $\overline{\binom{0}{\alpha}}$ since $\overline{\binom{0}{\alpha}} = \overline{\binom{0}{-\alpha}}$; we then have $p-3$ choices for $\beta \neq 0, \pm\alpha$, and thus $\frac{p-3}{2}$ choices for $\overline{\binom{0}{\beta}}$. Finally, this number must be divided by two since we are considering unordered couples, and hence $\#A = \frac{p-1}{2}\cdot\frac{p-3}{2}\cdot\frac{1}{2} = \frac{(p-1)(p-3)}{8}$

$$\Rightarrow dim\langle H\rangle = \frac{(p-1)(p-3)(2p-1)}{8} \underset{p\to\infty}{\sim} \frac{p^3}{4}$$

$$\text{and } dim\langle F\rangle = \frac{p\cdot(p^2-1)}{6} - 1 \underset{p\to\infty}{\sim} \frac{p^3}{6}$$

$$\Rightarrow \text{for } p \gg 0, \text{ we have } dim\langle H\rangle > dim\langle F\rangle.$$

□

Remark 3.1.1. To study the case of p small, notice that with the above notation we have

$$dim\langle H\rangle - dim\langle F\rangle = \left(\frac{(p-1)(p-3)(2p-1)}{8}\right) - \left(\frac{p(p^2-1)}{6} - 1\right)$$
$$= \frac{1}{24}(2p^3 - 27p^2 + 34p + 15).$$

Now if we define $P(x) := 2x^3 - 27x^2 + 34x + 15$, we have that $P(13) = 288 > 0$; moreover,

$$P'(x) = 6x^2 - 54x + 34 \geq 0 \iff \begin{array}{r} x \leq \dfrac{27-\sqrt{525}}{6} \approx 0.681 \\ \text{or } x \geq \dfrac{27+\sqrt{525}}{6} \approx 8.319 \end{array}$$

$\Rightarrow P(x) \geq P(13) > 0 \quad \forall x \geq 13$, i.e. $d_p \leq 6$ for all $p \geq 13$.

Moreover, it can be easily proved, via computer simulations, that the cycle of figure 3.1 is not sum of faces for $p = 7, 11$; see the following chapter on Sage simulations for more details.

Finally, for $p = 3, 5$, the graph π_p is planar, and hence all cycles are sum of faces, i.e. $d_3 = d_5 = 0$. We have thus proved that

$$d_p \leq 6 \quad \forall p \text{ prime}.$$

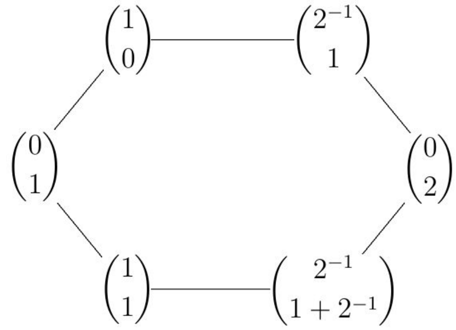


Figure 3.1: A cycle which is not sum of faces for $p = 7, 11$.

3.2 The dual surface π'_n

We shall now discuss the case of π'_n, the dual surface; as we will see, its systole is considerably bigger - we will be able to prove a logarithmic lower bound for the girth of the graph.

This result is proved by providing a covering of our graph by the infinite, 3-regular tree (recall that π'_n is 3-regular for every n, since the faces of π_n are triangles).

We define inductively the infinite graph T_3, whose vertex set V is contained in $(\mathbb{Z}\times\mathbb{Z})^3$; it will be proved that this is nothing but a labelling of the infinite, 3-regular tree.

Definition 3.2.1. Define the three functions "*left child*", "*right child*" and "*parent*" to be

$$\begin{array}{rccc} LC: & (\mathbb{Z}\times\mathbb{Z})^3 & \to & (\mathbb{Z}\times\mathbb{Z})^3 \\ & \binom{a}{b}\binom{c}{d}\binom{e}{f} & \mapsto & \binom{a}{b}\binom{a+c}{b+d}\binom{c}{d} \end{array}$$

$$\begin{array}{rccc} RC: & (\mathbb{Z}\times\mathbb{Z})^3 & \to & (\mathbb{Z}\times\mathbb{Z})^3 \\ & \binom{a}{b}\binom{c}{d}\binom{e}{f} & \mapsto & \binom{c}{d}\binom{c+e}{d+f}\binom{e}{f} \end{array}$$

$$\begin{array}{rccc} P: & (\mathbb{Z}\times\mathbb{Z})^3 & \to & (\mathbb{Z}\times\mathbb{Z})^3 \\ & \binom{a}{b}\binom{c}{d}\binom{e}{f} & \mapsto & \begin{cases} \binom{a-e}{b-f}\binom{a}{b}\binom{e}{f} & \text{if } b-f>0 \text{ or } (b-f=0 \text{ and } a-e>0) \\ \binom{a}{b}\binom{e}{f}\binom{e-a}{f-b} & \text{otherwise.} \end{cases} \end{array}$$

Definition 3.2.2. We define the *Farey tree* T_3 recursively: its root is $R := \binom{0}{1}\binom{1}{1}\binom{1}{0} \in (\mathbb{Z}\times\mathbb{Z})^3$, and the neighbours of an element X already present are $LC(X), RC(X), P(X)$.

Remark 3.2.1. The definition is well-posed, i.e. if $X \in N(Y)$, then $Y \in N(X)$.

To see this, first notice that every element of T_3 is of the form $\binom{x}{y}\binom{x+z}{y+w}\binom{z}{w}$, simply because R is of this form and all "left children", "right children" and "parents" have this property.

Also notice for every element X of T_3 we have that its couples $\binom{\alpha}{\beta}$ are all distinct and are such that either $\beta > 0$ or ($\beta = 0$ and $\alpha > 0$): indeed, the root R satisfies this property, and if an element $X \in (\mathbb{Z}\times\mathbb{Z})^3$ satisfies this property, then so do $LC(X)$, $RC(X)$ and $P(X)$ (simply look at the definitions).

This implies that for every element X of T_3, $P(LC(X)) = X$, $P(RC(X)) = X$ and either $LC(P(X)) = X$ or $RC(P(X)) = X$: for instance, if $X = \binom{a}{b}\binom{c}{d}\binom{e}{f}$, then $\binom{c}{d} = \binom{a+e}{b+f}$, and thus $P(LC(X)) = \binom{a}{b}\binom{c}{d}\binom{c-a}{d-b} \left(= \binom{a}{b}\binom{c}{d}\binom{e}{f}\right)$ since either $f = d - b > 0$ or $f = 0$ and $e = c - a > 0$; the other cases are similar.

Therefore, $Y \in N(X) \iff X \in N(Y) \quad \forall X, Y \in T_3$.

Now this construction can be re-expressed in the following terms, which will be useful for our purposes: define a sequence of roots

$$\left\{R_m := \begin{pmatrix} m \\ 1 \end{pmatrix}\begin{pmatrix} m+1 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\}_{m\in\mathbb{Z}}$$

such that R_m is connected to R_{m-1} and R_{m+1} for every $m \in \mathbb{Z}$, and a sequence of "subroots"

$$\{R'_m := LC(R_m)\}_{m\in\mathbb{Z}}$$

such that R'_m is connected to R_m for all m; then attach to every subroot its two "children", then their "children" and so on.

It is immediately seen that we get again the Farey tree: the sequence $\{R_m\}$ is nothing but the root $R = R_0$ together with all of its "ancestors" and all of its "right descendants" (proof is very easy by induction). We will denote by B_m the rooted tree consisting of R_m and of all of its descendants; B_0 is generally called the *Stern-Brocot tree*, but it is not unusual to find it under the name of Farey tree (that in our work designates T_3).

These two equivalent definitions will allow us to prove the following

Proposition 3.2.1. *T_3 is indeed a tree, i.e. it has no cycles.*

Proof. Since T_3 is connected and 3-regular, the claim amounts to prove that T_3 is actually *the* 3-regular tree; to prove this, we will view the construction of T_3 as a labelling $\Phi : T \to (\mathbb{Z} \times \mathbb{Z})^3$ of the 3-regular tree T, and prove that two different vertices of T are never given the same label.

To be more precise, we may construct T as follows: start with a sequence $\{r_n\}_{n\in\mathbb{Z}}$ of roots, such that r_n is connected to r_{n-1} and r_{n+1} for every n, then attach to every root r_n a copy B_n of the binary rooted tree. It is immediately seen that we actually obtain the infinite, 3-regular tree; we get T_3 as the labelling

$$\Phi : T \to (\mathbb{Z} \times \mathbb{Z})^3$$

that sends every root r_n to R_n, and all "descendants" of a root to the corresponding "descendants" defined via the left and right "children" functions.

Now by contradiction, assume that there exist two distinct vertices $x \neq y$ of T having same label, i.e. such that $\Phi(x) = \Phi(y)$; denote by B_n the binary rooted tree that x belongs to (here we actualy denote by B_j a binary rooted tree together with its root r_j), and by B_m that of y.

We will now study the labelling of the "fathers" of x and y: if $x \neq r_n$, define x_1 to be the only neighbour of x that is closer to the root r_n; if $x = r_n$, set $x_1 := r_{n-1}$, and define in a similar way y_1.

Then iterate this procedure recursively: if x_k is not a root, define x_{k+1} as the only neighbour of x_k that is closer to the root of x_k; if x_k is a root, then define x_{k+1} to be the previous one, and similarly for y_k.

We have only two possible cases:

(i) $x_k = y_k =: z$ for some $k \in \mathbb{N}$: assume that k is the smallest possible integer with this property, i.e. $x_{k-1} \neq y_{k-1}$, where we set $x_0 := x$ and $y_0 := y$; notice that since $x \neq y$, we cannot have $x_l = y_l$ for every $l \geq 0$, which means that such a k exists.

Then by using the first definition of our labelling, $\Phi(x_{k-1}) = P^{(k-1)}(\Phi(x)) = P^{(k-1)}(\Phi(y)) = \Phi(y_{k-1})$; but at the same time, $\Phi(x_{k-1}) = LC(\Phi(x_k)) = LC(\Phi(z))$ and $\Phi(y_{k-1}) = RC(\Phi(x_k)) = RC(\Phi(z))$ (we may assume this without loss of generality, up to exchanging x and y).

Now $LC(\alpha) \neq RC(\alpha)$ for every $\alpha \in T_3$, hence leading to a contradiction.

(ii) $x_k \neq y_k$ for every $k \geq 0$: then by taking $k \gg 0$, we have that both x_k and y_k are roots, say $x_k = r_{n_x}$ and $y_k = r_{n_y}$.

We then get $R_{n_x} = \Phi(x_k) = P^{(k)}(\Phi(x)) = P^{(k)}(\Phi(y)) = \Phi(y_k) = R_{n_y}$, a contradiction since all roots have different labels by definition.

□

In order to define a covering $T_3 \to \pi'_n$, we will need to prove some further properties concerning T_3:

Lemma 3.2.1. *For any vertex $X := \binom{a}{b}\binom{c}{d}\binom{e}{f}$ of T_3, we have that*

$$b \cdot e - a \cdot f = b \cdot c - a \cdot d = d \cdot e - c \cdot f = 1$$

i.e., the determinants of the matrices obtained by joining two columns of X are all equal to -1.

Proof. The root R clearly satisfies this property; it is then immediately seen that if X satisfies this property, then so do $LC(X)$, $RC(X)$ and $P(X)$ (by linearity on the columns of the determinant). □

Corollary 3.2.1. *Every couple $\binom{\alpha}{\beta}$ of every element of T_3 is such that*

$$gcd(\alpha, \beta) = 1.$$

Proof. Trivial since the above equations are Bézout's identities. □

We can now define the coverings $T_3 \to \pi'_n$:

Definition 3.2.3. For every $n \geq 3$, define

$$\Psi_n : V(T_3) \to \binom{V_n}{3}$$

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix}\right) \mapsto \left\{ \begin{pmatrix} a \mod n \\ b \mod n \end{pmatrix}_{\langle \pm 1 \rangle} \begin{pmatrix} c \mod n \\ d \mod n \end{pmatrix}_{\langle \pm 1 \rangle} \begin{pmatrix} e \mod n \\ f \mod n \end{pmatrix}_{\langle \pm 1 \rangle} \right\}.$$

Notice that element in the codomain are ordered triplets, whereas the codomain contains unordered elements.

From now on, we shall fix n and denote Ψ_n simply by Ψ.

Remark 3.2.2. The definition is well-posed: indeed, given any couple $\binom{x}{y}$ belonging to a vertex of T_3, by corollary 3.2.1 we have that $gcd(x, y) = 1$, so that in particular $gcd(x, y, n) = 1$ for every $n \geq 3$.

Also notice given any $\left(\binom{a}{b}\binom{c}{d}\binom{e}{f}\right) \in V(T_3)$, by lemma 3.2.1 the three vertices corresponding to $\binom{a}{b}$, $\binom{c}{d}$ and $\binom{e}{f}$ are adjacent in π_n, so that they form a triangle; therefore, the map Ψ has codomain the faces of π_n, i.e.

$$\Psi : V(T_3) \to F_n = V_n'.$$

As said before, we have the following

Theorem 3.2.1. *The map $\Psi : T_3 \to \pi_n'$ is a covering of graphs.*

To prove this result, we shall proceed through several steps:

Lemma 3.2.2. *$\Psi : V(T_3) \to V_n'$ is a morphism of graphs, i.e. it sends edges to edges.*

Proof. Let $X = \binom{a}{b}\binom{c}{d}\binom{e}{f}$ be a vertex of T_3; then $N(X) = (LC(X), RC(X), P(X))$ and each of these three elements shares two couples with X by definition. Thus the three corresponding faces of π_n' share an edge with $\Psi(X)$, i.e. they are adjacent to it. □

Lemma 3.2.3. *For every $X \in V(T_3)$, the restriction map*
$\Psi_{\big|N(X)} : N(X) \to N(\Psi(X))$ is bijective.

Proof. Since both T_3 and π_n' are regular of degree 3, it will suffice to show that $\Psi_{\big|N(X)}$ is injective. Now, let $X = \binom{a}{b}\binom{c}{d}\binom{e}{f}$, and recall that $N(X) = (LC(X), RC(X), P(X))$; therefore, $\Psi(LC(X))$ contains the edge $\binom{a}{b}\binom{c}{d}$ (here we mean their classes modulo n and ± 1), $\Psi(RC(X))$ contains $\binom{c}{d}\binom{e}{f}$ and $\Psi(P(X))$ contains $\binom{a}{b}\binom{e}{f}$.

Thus if by contradiction two elements of $\{\Psi(LC(X)), \Psi(RC(X)), \Psi((X))\}$ would coincide, then they would share two edges with $\Psi(X)$, and would hence coincide with it; we will then get $\Psi(X) \in N(\Psi(X))$, a contradiction. □

Proposition 3.2.2. *The morphism of graphs $\Psi : T_3 \to \pi_n'$ is surjective on vertices.*

Proof. We shall actually prove a stronger result, i.e. that the restriction map $\Psi_{\big|B_0} : B_0 \to \pi'_n$ is surjective on vertices.

Recall that $B := B_0$ is defined as the tree having root $R = \binom{0}{1}\binom{1}{1}\binom{1}{0}$, with child $R' = \binom{0}{1}\binom{1}{2}\binom{1}{1}$ and with all left and right descendants of R'; now a very well-known property of this "Stern-Brocot tree" (see [9], for instance) affirmes that the "middle couples" $\binom{\cdots}{\cdots}\binom{x}{y}\binom{\cdots}{\cdots}$ of vertices of B exhaust the set

$$A := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{N} \times \mathbb{N} \,:\, 0 < x < y,\, gcd(x,y) = 1 \right\}.$$

Now let $F := \left\{ \binom{a}{b}\binom{c}{d}\binom{e}{f} \right\}$ be a face of π_n; to find a preimage in $V(B)$, we shall focus on the first vertex $\binom{a}{b}$:

choose representatives $a, b \in \mathbb{N}$ such that $0 < a < b$ (possible up to adding multiples of n); now by definition of V_n, we have that $gcd(a,b,n) = 1$, and this allows us to choose *coprime* representatives:

let $k := gcd(a,b) > 0$; then we may factor a and b as

$$\begin{cases} a = a' \cdot k \\ b = b' \cdot k \end{cases} \quad \text{with } a', b' > 0;$$

we have that $gcd(k,n) = 1$; thus if we set

$$h := \prod_{\text{primes } p | a',\, p \nmid k} p$$

and we choose representatives $\binom{\tilde{a} := a}{\tilde{b} := b + h \cdot n}$, we still have $0 < \tilde{a} < \tilde{b}$, and moreover $gcd(\tilde{a}, \tilde{b}) = 1$: indeed, if p is a prime dividing $\tilde{a} = a$, then we have two cases:

- either p divides k, and so it divides b but not n nor h, and hence cannot divide $b + h \cdot n$;

- or p does not divide k, and thus it necessarily divides a' and h but does not divide b, and thus does not divide $b + h \cdot n$ either.

Thus there exists a vertex $\binom{\cdots}{\cdots}\binom{a}{b}\binom{\cdots}{\cdots} \in B$; now its right child will be of the form $\binom{a}{b}\binom{a+c}{b+d}\binom{c}{d}$ (since all middle couples are sum of the two external couples). The left descendants up to distance $n-1$ of this elements are

$$\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} a+c \\ b+d \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} 2a+c \\ 2b+d \end{pmatrix}\begin{pmatrix} a+c \\ b+d \end{pmatrix}, \ldots, \begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} na+c \\ nb+d \end{pmatrix}\begin{pmatrix} (n-1)a+c \\ (n-1)b+d \end{pmatrix}.$$

But now, $\binom{a}{b}\binom{c}{d}$ represents an edge of π_n by corollary 3.2.1, and thus by proposition 2.1.1 these triplets represents *all* faces adjacent to $\binom{a}{b}$ (see chapter 1 for more details); hence necessarily one of these elements must be sent to F via Ψ, which proves the proposition. □

The theorem is thus completely proved: $\Psi_n : T_3 \to \pi'_n$ is a covering for all $n \in \mathbb{N}_{\geq 3}$.

Remark 3.2.3. Notice that this also implies that π'_n is connected (and thus π_n too) for every $n \in \mathbb{N}_{\geq 3}$, since T_3 is obviously connected; we had proved this result in Chapter 1 only for $n = p$ a prime.

One final lemma will allow us to prove a logarithmic lower bound on the girth of π'_n:

Lemma 3.2.4. *Let $V = \binom{a_1}{b_1}\binom{a_2}{b_2}\binom{a_3}{b_3}$ be a vertex of T_3 having distance m from the root $R = \binom{0}{1}\binom{1}{1}\binom{1}{0}$; then $|a_j|, |b_j| \leq Fib(m+2)$ for every $j = 1, 2, 3$, where $Fib(k)$ denotes the k-th Fibonacci number (the Fibonacci sequence begins at $Fib(0) = 0$).*

Proof. We shall prove a sligthly stronger result, namely that there exists an $i \in \{1, 2, 3\}$ such that:

- $|a_i|, |b_i| \leq \text{Fib}(m+2)$;
- $|a_j|, |b_j| \leq \text{Fib}(m+1)\, \forall\, j \neq i$.

Indeed, by induction on m:

- $m = 0$: the claim is trivial since $\text{Fib}(1) = \text{Fib}(2) = 1$ and $|a_j|, |b_j| \in \{0, 1\}$ for $V = R$.
- $m \rightsquigarrow m+1$: let $W = \binom{c_1}{d_1}\binom{c_2}{d_2}\binom{c_3}{d_3}$ be the neighbour of V that is closest to R, i.e. $d(R, W) = m$, $d(W, V) = 1$. Hence by inductive hypothesis, there exists an $i \in \{1, 2, 3\}$ such that $|c_i|, |d_i| \leq \text{Fib}(m+2) = \text{Fib}((m+1)+1)$ and $|c_j|, |d_j| \leq \text{Fib}(m+1)$ for all the other j.

  Now we have that V is either a "child" of W or its "parent"; in any case, by definition of these functions it will share two elements with W, say

$\binom{c_k}{d_k}$ and $\binom{c_l}{d_l}$. Hence elements in these couples have modulus at most $\mathrm{Fib}(m+1)+1$); thus to conclude, it suffices to show that the elements of the remaining couple $\binom{a_j}{b_j}$ have modulus not greater than $\mathrm{Fib}((m+1)+2)$.

But the remaining couple is either the sum or the difference of the other two couples, so the moduli of its elements satisfy the relation

$$\begin{cases} |a_j| \leq |c_k| + |c_l| \\ |b_j| \leq |d_k| + |d_l|. \end{cases}$$

Now, at most one element between $|c_k|$ and $|c_l|$ is $\leq \mathrm{Fib}((m+1)+1)$, and the other one is $\leq \mathrm{Fib}(m+1)$: hence $|a_j| \leq \mathrm{Fib}((m+1)+1) + \mathrm{Fib}(m+1) = \mathrm{Fib}((m+1)+2)$, and the same clearly holds for $|b_j|$.

The lemma is thus proved. □

Theorem 3.2.2. *Let $g(n)$ denote the* girth *of π'_n, i.e. the length of its shortest non-zero cycle; then $g(n) \geq c \cdot \log n + O(1)$ where $c = 2/\log(\varphi) \approx 4.156$, $\varphi = \frac{1+\sqrt{5}}{2}$ being the golden ratio.*

As an immediate consequence, the same bound holds for the homological systole d'_n of π'_n.

Proof. Fix $n \geq 3$, and set $\Psi := \Psi_n$; first notice that given any (connected) path $l = (v_0v_1, v_1v_2, \cdots, v_{m-1}v_m)$ of π'_n, we may find a path
$l' = (w_0w_1, w_1w_2, \cdots, w_{m-1}w_m)$ in T_3 (still connected) such that $\Psi(l') = l$:

indeed, first select any set of m edges $w_0w'_1, w_1w'_2, \cdots, w_{m-1}w'_m$ such that $\Psi(w_jw'_{j+1}) = v_jv_{j+1}$ for every $j = 0, \cdots m-1$; this is possible since Ψ is a covering of graphs, and thus in particular it is surjective on edges.

Let us focus on the first two edges $w_0w'_1$ and $w_1w'_2$: we have that $\Psi(w'_1) = v_1 = \Psi(w_1)$, and hence $\Psi(LC(w'_1)) = \Psi(LC(w_1))$ since the "left child" map LC only involves algebraic operations, and similarly for RC and P. Now $w'_2 \in N(w_1)$, and thus w'_2 is either a "child" or the "parent" of w_1; but then $v_2 = \Psi(w'_2) = \Psi(w''_2)$ for some $w''_2 \in N(w'_1)$, i.e. $\Psi(w'_1w''_2) = v_1v_2$.

Now it suffices to replace $w_1w'_2$ with $w'_1w''_2$ and to iterate this procedure on the following edges to get the claim.

Now let C be a cycle of π'_n that realizes the girth; thanks to the above procedure, we may find a connected path C' in T_3 such that length(C') =length$(C) = g(n)$ and such that $\Psi(C') = C$. Denote by V_{start} and V_{end} the starting and ending point of C'; thanks to the transitivity of T_3 and of π'_n, we may assume that $R = \binom{0}{1}\binom{1}{1}\binom{1}{0}$ is the "middle point" of C', i.e. $R \in C'$ and

$$d(R, V_{\text{start}}) = \left\lfloor \frac{g(n)}{2} \right\rfloor, \quad d(R, V_{\text{end}}) = \left\lceil \frac{g(n)}{2} \right\rceil.$$

Now since $\Psi(V_{\text{start}}) = \Psi(V_{\text{end}})$, necessarily at least one element of a couple belonging to V_{start} or to V_{end} must have modulus greater then $(n-1)/2$:

indeed, for any two distinct vertices $\alpha = \binom{a_1}{b_1}\binom{a_2}{b_2}\binom{a_3}{b_3}$, $\beta = \binom{x_1}{y_1}\binom{x_2}{y_2}\binom{x_3}{y_3}$ of T_3, we have that $|a_j|, |b_j|, |x_j|, |y_j| \leq \frac{n-1}{2}$ for every j implies $\Psi(\alpha) \neq \Psi(\beta)$: by contradiction, let $\Psi(\alpha) = \Psi(\beta)$; then

$$\left\{ \begin{pmatrix} a_1 & \bmod n \\ b_1 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} a_2 & \bmod n \\ b_2 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} a_3 & \bmod n \\ b_3 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle} \right\}$$
$$= \left\{ \begin{pmatrix} x_1 & \bmod n \\ y_1 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} x_2 & \bmod n \\ y_2 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} x_3 & \bmod n \\ y_3 & \bmod n \end{pmatrix}_{\langle \pm 1 \rangle} \right\}$$
$$\Rightarrow \left\{ \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} a_3 \\ b_3 \end{pmatrix}_{\langle \pm 1 \rangle} \right\} = \left\{ \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}_{\langle \pm 1 \rangle}, \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}_{\langle \pm 1 \rangle} \right\}$$

But then necessarily

$$\left\{ \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}, \begin{pmatrix} a_3 \\ b_3 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} \right\}$$

since we have showed in remark 3.2.1 that all couples $\binom{z}{w}$ belonging to elements of T_3 are such that either $w > 0$ or ($w = 0$ and $z > 0$): this implies that the couple $\binom{-z}{-w}$ cannot belong to any element of T_3.

This means that the two vertices are just two (different) permutation of the same three couples; now to conclude, it suffices to notice that $\binom{a_2}{b_2} = \binom{a_1+a_3}{b_1+b_3}$ and $\binom{x_2}{y_2} = \binom{x_1+x_3}{y_1+y_3}$: hence since none of the involved couples can be zero, necessarily $\binom{a_2}{b_2} = \binom{x_2}{y_2}$.

But then we must have $\binom{a_1}{b_1} = \binom{x_3}{y_3}$ and $\binom{a_3}{b_3} = \binom{x_1}{y_1}$ (since $\alpha \neq \beta$); but this is a contradiction, since by lemma 3.2.1, we will then have

$$-1 = \det \begin{pmatrix} a_1 & a_3 \\ b_1 & b_3 \end{pmatrix} = -\det \begin{pmatrix} x_1 & x_3 \\ y_1 & y_3 \end{pmatrix} = 1.$$

This proves the claim: at least one element x belonging to a couple of V_{start} or of V_{end} has modulus greater then $(n-1)/2$. Now, thanks to lemma 3.2.4, we have that

$$\frac{n-1}{2} < |x| \leq \text{Fib}\left(\left\lceil \frac{g(n)}{2} \right\rceil + 2\right) = \left[\frac{\varphi^{\left\lceil \frac{g(n)}{2} \right\rceil + 2}}{\sqrt{5}} \right]$$

where the braces symbol denotes the nearest integer function, and $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio; by expliciting $g(n)$ we thus find

$$g(n) \geq \frac{2}{\log \varphi} \cdot \log n + O(1).$$

□

Remark 3.2.4. This theorem allows us to compare the girth of π'_n with the value provided by Moore's bound: namely for a d-regular graph G with N vertices, the girth $g(G)$ of G satisfies the inequality

$$g(G) \leq 2 \cdot \log_{d-1} N + O(1)$$

as $N \to \infty$; for the dual platonic surface π'_p (p being an odd prime), the regularity is $d = 3$ and the number of vertices is equal to the number of faces of the graph π_p, i.e. $\frac{p(p^2-1)}{6}$. Now by the above theorem we have that

$$g(\pi'_p) \geq \frac{2}{\log \varphi} \cdot \log p + O(1) = \frac{2}{3 \log \varphi} \cdot \log p^3 + O(1) = \frac{2 \log 2}{3 \log \varphi} \cdot \log_2 p^3 + O(1);$$

now let $k := \frac{2 \log 2}{3 \log \varphi}$, and notice that $\log_2 p^3 = \log_2 \frac{p^2(p-1)}{6} + o\left(\log_2 \frac{p^2(p-1)}{6}\right)$, which implies that

$$g(\pi'_p) \geq (k + o(1)) \cdot \log_{d-1} N$$

where $k \approx 0.9603$.

Chapter 4

The quantum error-correcting codes issued by platonic tilings

4.1 Definition and basic parameters

We shall now study the quantum codes derived from previous constructions and results. As many several properties were obtained only for platonic surfaces π_p for p odd prime, we will stick to this case also in the present chapter. Fix $p \geq 3$ a prime; our stabilizer group S_p will be the subgroup of the Pauli group generated by the rows of the matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$, where

- $\mathbf{H}_X \in \mathcal{M}_{|V_p|,|E_p|}(\mathbb{F}_2)$ is the incidence matrix of π_p, or equivalently the matrix whose rows are characteristic vectors of faces of π'_p;
- $\mathbf{H}_Z \in \mathcal{M}_{|F_p|,|E_p|}(\mathbb{F}_2)$ is the incidence matrix of π'_p, or equivalently the matrix whose rows are characteristic vectors of faces of π_p.

where, of course, zeroes of $\mathbf{H}_X$ and of $\mathbf{H}_Z$ are replaced by I (the identity matrix), ones of $\mathbf{H}_X$ are replaced by $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and ones of $\mathbf{H}_Z$ are replaced by $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Here are the parameters of the code $\mathcal{C}_p := C(S_p)$:
- the block length is

$$N = N_p = |E_p| = \frac{p \cdot (p^2 - 1)}{4}.$$

- Since π_p is connected, the dimension is 2^k with

$$k = k_p = 2 - |V_p| + |E_p| - |F_p| = 2 - \frac{p^2 - 1}{2} + \frac{p \cdot (p^2 - 1)}{4} - \frac{p \cdot (p^2 - 1)}{6}$$
$$= \frac{1}{12} \left(p^3 - 6p^2 - p + 10 \right).$$

- The minimum distance $d = d_p$ of the code is the length of the shortest cycle of π_p or of π'_p which is not sum of faces; therefore from the discussion in chapter 2, for $p \geq 7$ we have

$$d \in \{4, 5, 6\}.$$

We may also compute the asymptotic rate of the code:

$$\lim_{p \to \infty} \frac{k_p}{N_p} = \lim_{p \to \infty} \frac{\frac{p^3}{12} - \frac{p^2}{2} - \frac{p}{12} + \frac{5}{2}}{\frac{p^3}{4} - \frac{p}{4}} = \frac{1}{3}.$$

4.2 Sparsity analysis of $\mathcal{C}_p$

We shall now prove that the family of quantum error-correcting codes $\{\mathcal{C}_p\}_{p \geq 3}$ has sparse parity-check matrices, hence proving that these are LDPC codes:

- first start with the matrix $\mathbf{H}_X$, the incidence matrix of π_p. Every row represents a vertex, and its weight is the number of edges incident to the vertex; the length of every row is equal to the number of edges of π_p, and thus we find for the row corresponding to the vertex $v \in V_p$:

$$\frac{\text{weight of a row}}{\text{cardinality of a row}} = \frac{\#\{N(v)\}}{\# E_p} = \frac{p}{\frac{p^3 - p}{4}} \sim_{p \to \infty} 4 \cdot p^{-2} \to 0.$$

- for the matrix $\mathbf{H}_Z$, every row is the characteristic vector of a face f: hence

$$\frac{\text{weight of a row}}{\text{cardinality of a row}} = \frac{\# f}{\# E_p} = \frac{3}{\frac{p^3 - p}{4}} \sim_{p \to \infty} 12 \cdot p^{-3} \to 0.$$

Conclusions

The study of platonic surfaces has revealed remarkable properties of regularity and symmetry of these objects; the quantum error-correcting codes derived from them present good qualities such as sparse sparity-check matrices and constant rate, but are also seriously affected by the small value of their minimum distance, which is at most 6 for all prime-index codes.

This bound is obtained from the homology systole of the platonic surface π_p, while dual surfaces present far better parameters (their girth being equal to almost one half of the maximal asymptotical value given by Moore's bound). The latter computation, concerning dual surfaces π'_n, hold for all values of n, while the previous one was obtained only for n prime; thus the distance of the code could be increasing for the values of n that we have not investigated, although as shown by Delfosse [7] the overall distance cannot significantly exceed a logarithm of the length.

Further analysis of the given results for n not prime may also need a different approach, since many of the computations that we have presented strongly rely on properties of $\mathbb{F}_p$: for instance, neighbours of a given vertex of π_p can be easily computed thanks to the existence of multiplicative inverses in $\mathbb{F}_p^\times$, while for arbitrary integers we can just know their number and some properties they enjoy; moreover, our computation of the homology systole of platonic graphs deeply relied on dimension counting, which again may be difficult to perform in the non-prime case.

Different tools might therefore be needed to carry on further investigation on the quality of quantum codes obtained from platonic tilings.

Appendix A

Computer simulations

The present chapter will be devoted to present simulations regarding platonic surfaces; the program we have used is Sage (www.sagemath.org), version 5.7.

The goal of these simulations is essentially to investigate some properties of the platonic surfaces π_n; we will just deal with the case $n = p$ an odd prime. These programs have been used, among the other things, to compute the upper bound on the homological systole provided in chapter 2 for $p = 7, 11$.

A.1 Construction of π_p

We shall present some first programs to build objects related to the graph π_p: first of all, a simple command to construct vertices of the graph. Recall that these are nothing but classes of $\mathbb{F}_p^2 \setminus \left\{ \binom{0}{0} \right\}$ modulo ± 1; now elements of $\mathbb{F}_p^2$ will be built as 2-by-1 matrices with coefficients in $\mathbb{F}_p$, and for each class $\left[\binom{\alpha}{\beta} \right]_{\langle \pm 1 \rangle}$ we will choose the only representative $\binom{\alpha}{\beta}$ with $0 < \alpha \leq \frac{p-1}{2}$ or with $\alpha = 0$ and $0 < \beta \leq \frac{p-1}{1}$: namely,

```
def pl_class(x,p):
    if 0<float(x[0][0])<=float((p-1)/2)
    or (x[0][0]==0 and 0<float(x[1][0])<=float((p-1)/2)):
        return(x)
    else:
        return(-x)
```

pl_class will be the function that associates to every element the representative of its class with the above property; this will be used to define the vertex set in the following way:

```
def pl_vertices(p):
    l=list(MatrixSpace(GF(p),2,1))
    #first create the vector with all elements of F_p^2
    V=[]
    for i in range(1,len(l)): #the first element of l, l[0], will
                              #be the zero couple, which must not
                              #be considered
        if pl_class(l[i],p)==l[i]:
            V.append(l[i])
    return(V)
```

We then create the list of all edges of π_p:

```
def pl_edges(l):
    l=pl_vertices(p)
    L=[]
    for i in range(len(l)):
        for j in range(i+1,len(l)):
            if det(matrix( [ [ l[i][0][0] , l[j][0][0] ] ,
            [ l[i][1][0] , l[j][1][0] ] ] ))^2 == 1:
                L.append([l[i],l[j]])
                #for every vertex v, we look for all other adjacent
                #vertices; to avoid repetitions, we look for them
                #only in the positions of the list following v.
    return(L)
```

We can also build the adjacency matrix of π_p, which can be useful if one wants to use the "graph" class functions of Sage:

```
def pl_adj(p):
    M=zero_matrix(GF(2),len(l),sparse=true) #first define
    #a zero matrix with desired dimensions.
    l=pl_vertices(p)
    for i in range(len(l)):
        for j in range(i+1,len(l)):
         #then use the same procedure as the "edge" command:
            if det(matrix( [ [ l[i][0][0] , l[j][0][0] ] ,
            [ l[i][1][0] , l[j][1][0] ] ] ))^2 == 1:
                M[i,j]=M[j,i]=1
                #exploit symmetry of the matrix to speed up
                #construction.
    return(M)
```

The list of all faces shall now be contructed:

```
def pl_faces(p):
    e=pl_edges(p)
    L=[]
    c=0 #a tool variable
    for x in e:
        z=[x[0],x[1],pl_class(x[0]+x[1],p)]
        #this builds one of the two faces containing the edge;
        #via this procedure, we can construct all faces (see
        #chapter 1), but we may get doubles.
        for y in L:
            if all(t in y for t in z):
                c=1
                break
                #a simple, brute force-method to avoid doubles:
                #just check that the face is different from all
                #previously constructed ones.
        if c==0:
            L.append(z)
        c=0
    return(L)
```

A.2 Cycles testing

Throughout this section, we present a simple method to understand if a cycle is or not sum of faces: first, we need to construct the incidence matrix of the dual surface π_p', i.e. the matrix whose rows are characteristic vectors of faces of π_p.

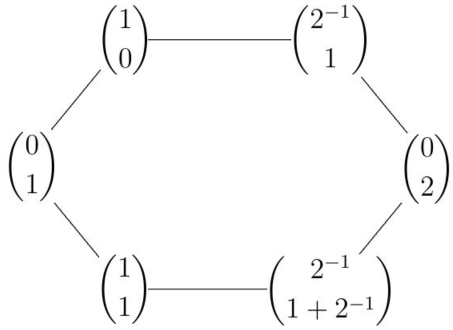
```
def dual_inc(p):
    e=pl_edges(p)
    f=pl_faces(p)
    M=zero_matrix(GF(2),len(f),len(e),sparse=true)
    #first construct a zero matrix of the desired dimensions.
    for i in range(len(f)):
        for j in range(len(e)):
            if all(x in f[i] for x in e[j]):
                M[i,j]=1
                #simple brute force: for each edge, look
                #for all the faces containing it.
    return(M)
```

Now to decide whether a cycle C is sum of faces or not, first write it as a characteristic vector l_C of length $\#E$; then compute the rank of the incidence matrix of the dual graph π_p', and see if it changes after adding l_C: it will change if and only if l_C is not sum of faces (since this will happen if and only if l_C is not contained in the linear span of the faces).

Therefore the following function will return 1 if and only if the input cycle is not sum of faces:

```
def faces_test(l,p):
    #l will be the desired vector.
    M=dual_inc(p)
    L=list(M)
    L.append(l)
    N=matrix(L)
    return( rank(N)-(p*(p^2-1)/6-1) )
    #recall that the rank of the dual incidence matrix has been
    #computed in chapter 2.
```

The following lines will contruct our ”test cycle”: simply two different paths joining the vertices $\binom{0}{1}$ and $\binom{0}{2}$, namely


$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}2^{-1}\\1\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}0\\2\end{pmatrix}$
$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}2^{-1}\\1+2^{-1}\end{pmatrix}$

```
def test_vector(p):
    e=pl_edges(p)
    w=[column_matrix(GF(p),[0,1])]
    w.append(column_matrix(GF(p),[1,0]))
    w.append(pl_class(column_matrix(GF(p),[2^(-1),1])),p)
    w.append(column_matrix(GF(p),[0,2]))
    w.append(pl_class(column_matrix(GF(p),[2^(-1),1+2^(-1)])),p)
    w.append(column_matrix(GF(p),[1,1]))
    #first construct the cycle as a list of edges,
    #then build the associated characteristic vector:
    r=[0]*len(e)
    #initialize it as a zero vector;
    for k in range(6):
        for i in [i for i,x in enumerate(e) if
        all(t in x for t in [w[k],w[(k+1)%6]]) ]:
            r[i]=1
            #then find the positions of the edges and mark them
            #with 1.
    return(r)
```

This "test cycle" is not sum of faces for $p = 7, 11, 13, 17, 19$; since an upper bound on the homological systole d_p of π_p was computed only for $p \geq 13$ (or $p = 3, 5$), this proves that $d_p \leq 6$ for every $p \geq 3$.

The command line to verify this is simply:

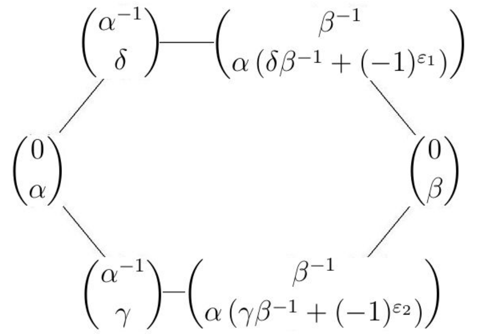
```
faces_test(test_vector(p),p)
```

Remark A.2.1. Notice that the efficiency of these programs can be easily increased, since each of them compute the vertex set of π_p or its edge set, and thus the relative instructions are carried out several times when we test our cycle: the actual version we used was modified so that these quantitities are computed just once.

A.3 Further rank analysis

Throughout this section, we will provide a program to compute the rank of the family of cycles presented in chapter 2; although such a computation was carried out without simulations, this tool may still be useful for further analysis on π_p. For instance, one could try to compute exactly the homology systole d_p of these graphs by adapting the same method to other families of cycles (recall that our computation only proves $d_p \in \{4, 5, 6\}$ for $p \geq 7$).

The following program will return the matrix whose lines are characteristic vecors of cycles of the form


$\begin{pmatrix}\alpha^{-1}\\ \delta\end{pmatrix}$
$\begin{pmatrix}\beta^{-1}\\ \alpha\left(\delta\beta^{-1} + (-1)^{\varepsilon_1}\right)\end{pmatrix}$
$\begin{pmatrix}0\\ \alpha\end{pmatrix}$
$\begin{pmatrix}0\\ \beta\end{pmatrix}$
$\begin{pmatrix}\alpha^{-1}\\ \gamma\end{pmatrix}$
$\begin{pmatrix}\beta^{-1}\\ \alpha\left(\gamma\beta^{-1} + (-1)^{\varepsilon_2}\right)\end{pmatrix}$

```
def rank_test(p):
    l=pl_edges(p)
    w=[]
    for delta in GF(p):
        for gamma in GF(p):
            if float(delta)<float(gamma):
                for beta in GF(p):
                    if 0<float(beta)<=(p-1)/2:
                        for alpha in GF(p):
                            if float(beta)<float(alpha)<=(p-1)/2:
                                for epsilon1 in range(2):
                                    for epsilon2 in range(2):
if delta/beta+(-1)^epsilon1<>gamma/beta+(-1)^epsilon2:
w.append(column_matrix(GF(p),[0,alpha]))
w.append(pl_class(column_matrix(GF(p),[alpha^(-1),delta]),p))
w.append(pl_class(column_matrix(GF(p),
[beta^(-1),alpha*(delta/beta+(-1)^epsilon1)]),p))
w.append(column_matrix(GF(p),[0,beta]))
w.append(pl_class(column_matrix(GF(p),
[beta^(-1),alpha*(gamma/beta+(-1)^epsilon2)]),p))
w.append(pl_class(column_matrix(GF(p),[alpha^(-1),gamma]),p))

    M=zero_matrix(GF(2),len(w)/6,len(l),sparse=true)
    for j in range(len(w)/6):
        for k in range(6):
            for i in [i for i,x in enumerate(l)
            if all(t in x for t in [w[j*6+k],w[j*6+(k+1)%6]]) ]:
                M[j,i]=1
    return(M)
```

The rank of this matrix will be equal to $\frac{(p-1)(p-3)(2p-1)}{8}$.

Bibliography

[1] Luisa Aburto, Roberto Johnson, and José Pantoja. The complex linear representations of $\mathrm{GL}(2, k)$, k a finite field. *Proyecciones*, 25(3):307–329, 2006.

[2] Claude Berge. *Graphs*, volume 6 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1985. Second revised edition of part 1 of the 1973 English version.

[3] Norman Biggs. Constructions for cubic graphs with large girth. *Electron. J. Combin.*, 5:Article 1, 25 pp. (electronic), 1998.

[4] Robert Brooks. Platonic surfaces. *Comment. Math. Helv.*, 74(1):156–170, 1999.

[5] Robert Brooks, Hershel M. Farkas, and Irwin Kra. Number theory, theta identities, and modular curves. In *Extremal Riemann surfaces (San Francisco, CA, 1995)*, volume 201 of *Contemp. Math.*, pages 125–154. Amer. Math. Soc., Providence, RI, 1997.

[6] Michelle DeDeo, Dominic Lanphier, and Marvin Minei. The spectrum of Platonic graphs over finite fields. *Discrete Math.*, 307(9-10):1074–1081, 2007.

[7] Nicolas Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. *arXiv:1301.6588 [quant-ph]*, 2013.

[8] Daniel Gottesman. An introduction to quantum error correction. In *Quantum computation: a grand mathematical challenge for the twenty-first century and the millennium (Washington, DC, 2000)*, volume 58 of

Proc. Sympos. Appl. Math., pages 221–235. Amer. Math. Soc., Providence, RI, 2002.

[9] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[10] Paul E. Gunnells. Some elementary Ramanujan graphs. *Geom. Dedicata*, 112:51–63, 2005.

[11] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Physics*, 303(1):2–30, 2003.

[12] Dominic Lanphier and Jason Rosenhouse. Cheeger constants of Platonic graphs. *Discrete Math.*, 277(1-3):101–113, 2004.

[13] David J. C. MacKay, Graeme Mitchison, and Paul L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. Inform. Theory*, 50(10):2315–2330, 2004.

[14] Ilya Piatetski-Shapiro. *Complex representations of* GL(2, K) *for finite fields* K, volume 16 of *Contemporary Mathematics*. American Mathematical Society, Providence, R.I., 1983.

[15] Reina Riemann. *Good Families of Quantum Low-Density Parity-Check Codes and a Geometric Framework for the Amplitude-Damping Channel*. ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–Massachusetts Institute of Technology.

[16] Gilles Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Coding and cryptology*, volume 5557 of *Lecture Notes in Comput. Sci.*, pages 259–273. Springer, Berlin, 2009.