An unified viewpoint for upper bounds for the number of points of curves over finite fields via Euclidean geometry and semi-definite symmetric Toeplitz matrices

Emmanuel Hallouin, Marc Perret

An unified viewpoint for upper bounds for the number of points of curves over finite fields via Euclidean geometry and semi-definite symmetric Toeplitz matrices

Emmanuel Hallouin & Marc Perret*

December 3, 2017

Abstract

We provide an infinite sequence of upper bounds for the number of rational points of absolutely irreducible smooth projective curves X over a finite field, starting from Weil classical bound, continuing to Ihara bound, passing through infinitely many *n-th order Weil bounds* and ending asymptotically to Drinfeld-Vlăduţ bound. We relate this set of bounds to Oesterlé one, proving that these are inverse functions in some sense. We explain how Riemann hypothesis for the curve X can be merely seen as an euclidean property, coming from the Toeplitz shape of some intersection matrix on the surface $X \times X$ together with the general theory of symmetric Toeplitz matrices. We also give some interpretation for the defect of asymptotically exact towers.

This is achieved by pushing further the classical Weil proof in term of euclidean relationships between classes in the euclidean part $\mathcal{F}_X$ of the numerical group $\mathrm{Num}(X \times X)$ generated by classes of graphs of iterations of the Frobenius morphism. The noteworthy Toeplitz shape of their intersection matrix takes a central place by implying a very strong cyclic structure on $\mathcal{F}_X$.

AMS classification : 11G20, 14G05, 14G15, 14H99, 15B05, 11M38.
Keywords : Curves over a finite field, Rational point, Weil bound, Toeplitz matrices, Zeta function.

Contents

*Institut de Mathématiques de Toulouse ; UMR 5219, Université de Toulouse ; CNRS, UT2J, F-31058 Toulouse, France, hallouin@univ-tlse2.fr, perret@univ-tlse2.fr. Funded by ANR grant ANR-15-CE39-0013-01 “manta”

Introduction

Let X be an absolutely irreducible smooth projective curve of genus g defined over the finite field $\mathbb{F}_q$ with q elements. Weil's [Wei48] classical proof of his bound $|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$ for the number $\sharp X(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points rests upon Castelnuovo identity, today an easy corollary of Hodge index Theorem for the smooth algebraic surface $X \times X$. The intent of this article is to push further this viewpoint by forgetting Castelnuovo Theorem. We come back to the consequence of Hodge index Theorem that the intersection pairing on the numerical space $\mathrm{Num}(X \times X)_{\mathbb{R}}$ is anti-euclidean on what can be though as its *non-trivial part*, the orthogonal complement $\mathcal{E}_X$ of the trivial plane generated by the horizontal and vertical classes. Thus, the opposite $\langle C, D\rangle = -C \cdot D$ of the intersection pairing endows $\mathcal{E}_X$ with a structure of euclidean space.

A very pleasant point is that Weil bound is nothing more than Schwartz inequality applied to the non trivial parts of the classes of the diagonal and of the graph of the

Frobenius morphism in this Euclidean space $\mathcal{E}_X$! The benefit of using Schwartz instead of Castelnuovo is the following. While we do not know what could be a Castelnuovo identity for more than two numerical classes, we do know that Schwartz for any number of vectors is the non-negativity of their Gram determinant. We are thus encouraged to investigate the consequences of the non-negativity of larger Gram determinants involving (some normalisation[1] γ^k of) the non-trivial part $p(\Gamma^k)$ of the numerical classes of the graph Γ^k of several k-th iterations of the Frobenius morphism.

Then, a very fruitful property appears: the symmetric semi-definite Gram matrix of these non-trivial parts is a Toeplitz one[2]. For instance, this mere fact entails by general properties of such symmetric semi-definite Toeplitz matrices that multiplication by the graph of the Frobenius[3] is a similarity of ratio $\sqrt{q}$ on $\mathcal{F}_X$, from which Riemann hypothesis follows by elementary spectral theory of similarities in an Euclidean space! This means actually that the subspace $\mathcal{F}_X$ of $\mathrm{Num}(X \times X)$ generated by the $p(\Gamma^k)$'s is an independant of ℓ rational realization of the part corresponding to the minimal polynomial of the Frobenius endomorphism φ_ℓ acting on the Tate module $T_\ell(\mathrm{Jac}(X))$ in the decomposition of $T_\ell(\mathrm{Jac}(X))$ in sum of cyclic sub-spaces for φ_ℓ. We then deduce integrality by the Fatou property of the rational integer ring $\mathbb{Z}$. This Toeplitz structure also yields very naturally for instance to some asymptotic bounds, such as Tsfasmann bound, so as to some relationships between the numbers of points on some extensions of scalars of the finite base field, containing as a special case the well known fact that an extremal curve over $\mathbb{F}_q$ is minimal over $\mathbb{F}_{q^2}$.

To go further, the natural arithmetic constraints $\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q)$ have to be taken into account for any $i \geq 1$ as suggested by Ihara. For the family $\gamma^0, \gamma^1, \gamma^2$, we recover the well known Ihara bound [Iha81] which improves Weil bound for curves of genus greater than $g_2 = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$, a constant appearing very naturally with this viewpoint in section 3.3 (especially looking at figure 1 therein). It follows that the classical Weil bound can be seen as a *first order Weil bound*, in that it comes from the euclidean constraints between γ^0 and γ^1, while the Ihara bound can be seen as a *second order Weil bound*, in that it comes from euclidean constraints together with an arithmetic one between γ^0, γ^1 and γ^2. This process can of course be pushed further: by considering the family $\gamma^0, \gamma^1, \gamma^2$ and γ^3, we obtain a new *third order Weil bound* (Theorem 16), which improves the Ihara bound for curves of genus greater than another constant $g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$.

We then proceed to the general n-th order Weil bound in our main Theorem 14 for any given $n \geq 1$, upper bounding the number of points of a curve of genus g by some quantity $N_n^\star(g)$ provided g is greater than a certain explicitly given genus g_n. Moreover, this upper bound $N_n^\star(g)$ is explicitly related by formula (17) below to some optimal solution $\mathbf{x}_{\mathbf{1},n}^\star(g)$ of an explicit convex optimisation problem, and these bound are sharper and sharper as n increases.

[1] This normalisation is not crucial, it serves only to obtain Toeplitz matrices below. Removing this normalisation would yield to some "skew Toeplitz" shape matrices such as in formula (6), for which standard Toeplitz theory can be easily adapted.

[2] That is, of the form (5).

[3] For the composition low $\circ$ of correspondences on $X \times X$.

Unfortunately, computing $\mathbf{x}^{\star}_{\mathbf{1},n}(g)$ explicitly requires the resolution of high degree one variable polynomial equations over $\mathbb{R}$. Indeed, item (iv) of Theorem 14 states for small values of n that the usual Weil bound requires the resolution of a degree one equation, Ihara and the third order Weil bounds require the resolution of second order equations[4], while fourth and fifth order Weil bounds require the resolution of third order equations, and so on. In any way, a simple glance at Ihara second order Weil bound and at our explicit third order Weil bound will convince the reader that they become more and more ugly as the order n increases!

To be precise, the situation is the following. For any given order $n \geq 1$, we can associate to a curve X of genus g a point $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$, where $x_0 = 2g$ and x_i is the scalar product $\langle \gamma^0, \gamma^i \rangle$. By the Toeplitz shape of the intersection matrix and the semi-definite positiveness of Gram matrices, this point should lie in some convex domain $\mathcal{W}_n$, we call the *n-th Weil domain*. This can be thought as a *geometrico-euclidean* constraint, first in that it comes from the positivity of gram determinants (an euclidean feature) itself coming from Hodge index Theorem for the surface $X \times X$ (a geometric feature), second in that the Toeplitz shape coming ultimately from projection formula (a geometric feature) entails strong euclidean properties. By the *arithmetic constraints* already described above, it should actually lie in some convex sub-domain, "under" some *Ihara line* we denote by $\mathcal{I}^g_n$. Then, Theorem 14 states that $\mathbf{x}^{\star}_{\mathbf{1},n}(g)$ is the smallest x_1 abscissa of the intersection points of the Weil domain and the Ihara line. This intersection is constraining provided $g \geq g_n$, and is then given by the zero set of an explicit one variable polynomial. It turns out that we did not succeed to prove this statement of Theorem 14 using pure convex analysis. We rely instead this optimization problem to the Oesterlé one.

Roughly speaking, given q, our optimization problem is to find the greatest number N of rational points of a genus g curve over $\mathbb{F}_q$ can have *given only* the above geometrico-euclidean and arithmetic constrains, while Oesterlé one is to find the smallest genus g a curve over $\mathbb{F}_q$ having N rational points can have *given only* some constraints we describe in the paper. We then prove that both sets of constraints entails that these optimisation problem are inverse to each other. Then, we use Oesterlé explicit solution of his problem to prove this last result on $\mathbf{x}^{\star}_{\mathbf{1},n}(g)$.

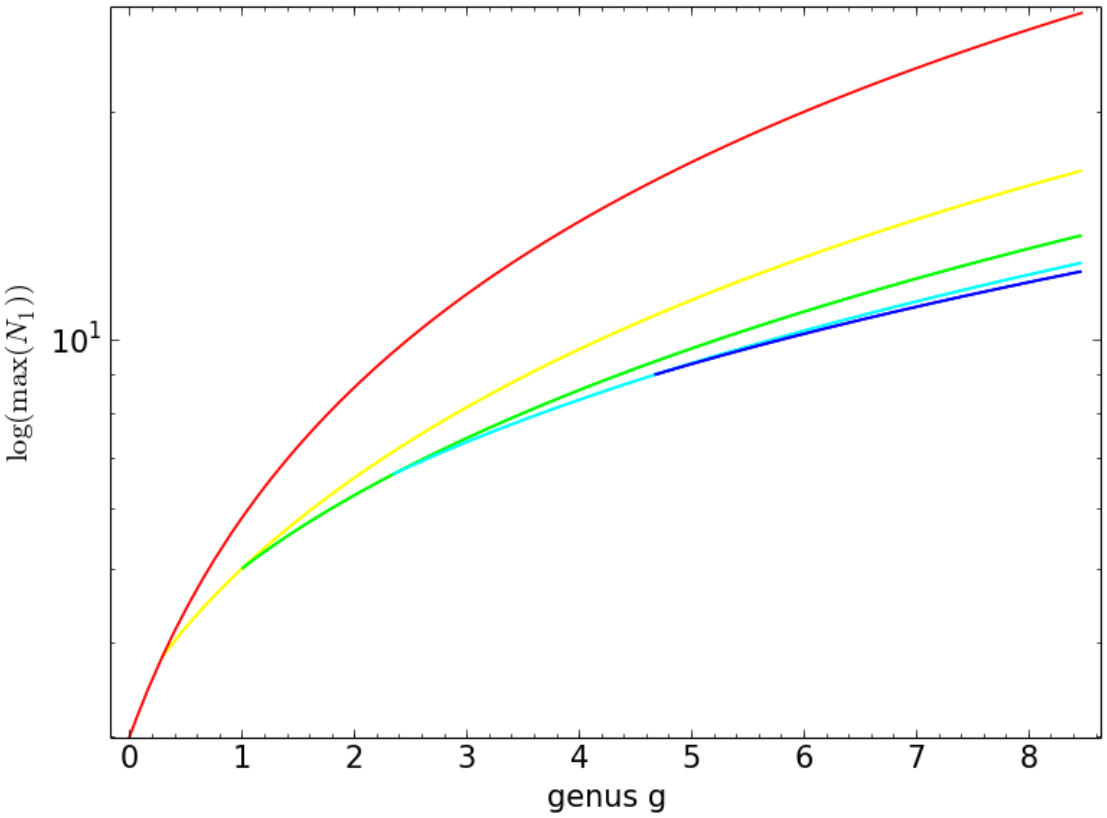
Nevertheless, note that while Oesterle have considered the infinite dimensional optimization problem taking into account the infinitely may arithmetic constraints $\sharp X(\mathbb{F}_{q^k}) \geq \sharp X(\mathbb{F}_q)$ for any $k \geq 2$, we do consider, for a given order n, a finite dimensional optimization problem by considering only these arithmetic constraints for $2 \leq k \leq n$. From this, we prove that our point of view works also for $q = 2$.

It worth to insist that we do now have for any value of q infinitely many ordered Weil bounds, starting from the usual Weil one, then to the Ihara one and so on. It is a remarkable feature that our bounds of orders n goes, as n tends to infinity, to the well known Drinfeld-Vlăduţ bound as stated in Theorem 29. Hence, it can be said that all

[4]Hence closed formulas involving only square roots can be written down.

these higher order Weil bounds fulfill the gap between the already known one — Weil and Ihara ones of order 1 and 2, to Drinfeld-Vlăduţ one of infinite order.

Once the smallest x_1-coordinate is theoretically well understood — it is the largest non-positive root of some polynomial equation in one variable, giving n-order Weil bounds for orders $n \geq 4$ is a computational one. We use an algorithm which, for a given genus g and a given field size q, returns the best upper order Weil bound for the number of $\mathbb{F}_q$-rational points of a genus g curve, together with the corresponding best order n. In the figure below illustrating some statements of Theorem 14, we represent the successive Weil bounds (in logarithmic scales) of order from 1 to 5 for $q = 2$. Note that taking into account the logarithmic scale for the y-axis, higher order Weil bounds become significantly better than usual Weil one even for small genus!



Weil bounds of order 1 to 5 for $\sharp X(\mathbb{F}_q)$ for $q = 2$. Note that the y axis is logarithmic. For small genus, red usual first order Weil bound $\mathbf{N}_1^\star(g) = q + 1 + 2g\sqrt{q}$ is the best one. Then from genus $g_2 = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$, yellow Ihara second order Weil bound $\mathbf{N}_2^\star(g)$ becomes better, up to the genus $g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ where green third order Weil bound $\mathbf{N}_3^\star(g)$ becomes better. From genus g_4, light blue fourth order Weil bound $\mathbf{N}_4^\star(g)$ is the best up to genus g_5, where dark blue fifth order Weil bound $\mathbf{N}_5^\star(g)$ becomes better, and so on. The approximate values of g_2, g_3, g_4, g_5 are particularly small, respectively about $0.3, 1, 2.35$ and 4.67. This means for instance that the best bound for $q = 2$ and $g = 3$ is the fourth order one! Continuing

with this process for larger and larger orders will lead by Theorem 29 to Drinfeld-Vlăduţ bound.

The paper is organized as follows. In Section 1 we recall some basic facts on intersection pairing on $X \times X$, we prove Proposition 5 that the intersection matrix of the non-trivial parts γ^k is Toeplitz, and we deduce Riemann hypothesis for curves in section 1.3 from general facts on Toeplitz matrices gathered in Appendix A.2.

Then, we introduce in Section 2 the n-th Weil domain resulting from the geometrico-euclidean constraint, and deduce the usual Weil bound and Proposition 12 coming from this geometrico-euclidean constraint alone.

We turn in the main Section 3 to results coming from both geometrico-euclidean and arithmetic constraints. We state the main Theorem 14 giving the general n-th order Weil bound. We study extensively the cases of orders 2 and 3, getting respectively Ihara bound and a new explicit bound in Theorem 16. Then, the relationship with Oesterlé problem is studied in subsection 3.5, from which we deduce a proof of Theorem 14.

We conclude with an asymptotic Section 4. We begin by proving Theorem 28, a stronger form of Tsfasman [Tsf92] bound in that it gives an interpretation for the *defect* of an asymptotically exact tower as a limit of nice euclidean vectors in $(\mathcal{E}, \langle \cdot, \cdot \rangle)$. We also push to the infinite-order Weil bound, proving Theorem 29 that it is exactly Drinfeld-Vlăduţ bound.

For the convenience of the reader, some results on conic programming are given in Appendix A.1, and some results on symmetric semi-definite Toeplitz matrices are given in Appendix A.2.

In the whole paper, we denote by X an absolutely irreducible smooth projective curve of genus g defined over the finite field $\mathbb{F}_q$ with q elements.

Acknowledgments. We are grateful to Yves Aubry, Christine Bachoc, Gilles Lachaud and Hugo Woerdeman for useful discussions.

1 The euclidean subspaces $\mathcal{E}_X$ and $\mathcal{F}_X$ inside $\mathrm{Num}(X \times X)$

We introduce some "non-trivial part" space $\mathcal{E}_X$ and its subspace $\mathcal{F}_X$ "generated by the Frobenius". Both are euclidean vector spaces for the opposite of the intersection pairing. We prove the very fruitful Proposition 5 that some Gram matrix in $\mathcal{F}_X$ has Toeplitz shape. From this mere fact follows for instance a rational interpretation of the whole set of Riemann Hypothesis for X.

1.1 Intersection in the surface $X \times X$

In the spirit of Weil's proof of Riemann hypothesis for curves over finite fields, we use intersection theory in the group of divisors $\mathrm{Div}(X \times X)$ of the product surface $X \times X$. There is a unique additive symmetric pairing $\mathrm{Div}(X \times X)^2 \to \mathbb{Z}$, denoted by $C \cdot D$

for any $C, D \in \mathrm{Div}(X \times X)$, such that $C \cdot D$ equals $\sharp C \cap D$ when C and D are non-singular curves meeting transversally and depending only on the linear equivalence class of divisors (cf. [Har77, Chap V, Th 1.1]).

We need for our purpose to intersect the horizontal and vertical divisors H and V, the diagonal divisor Δ and the graphs Γ of the q-Frobenius morphsim $F : X \to X$, respectively defined by:

$$H = X \times \{*\}, \quad V = \{*\} \times X, \quad \Delta = \{(P, P) \mid P \in X\}, \quad \Gamma = \{(P, F(P)) \mid P \in X\}.$$

In the following proposition, we recall some well known intersection numbers between the previous divisors. We choose to detail their computation in order to make the document self-contained.

Proposition 1. *The intersection matrix in the surface $X \times X$ of the horizontal and vertical divisors H and V, the diagonal divisor Δ, and the graph Γ of the Frobenius morphism $F : X \to X$ is given by*

$$\begin{array}{c} \\ H \\ V \\ \Delta \\ \Gamma \end{array} \begin{array}{c} \begin{array}{cccc} H & V & \Delta & \Gamma \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & q \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 2-2g & \sharp X(\mathbb{F}_q) \\ q & 1 & \sharp X(\mathbb{F}_q) & q(2-2g) \end{pmatrix} \end{array}$$

Proof — Since the intersection pairing does not depend on the linear classes of divisors, the auto-intersection H^2 is equal to $(X \times \{P\}) \cdot (X \times \{Q\})$ where P, Q are two distinct points on X. Therefore this auto-intersection must be zero. The same holds for V^2. One has $V \cdot H = 1$ since V and H meet transversally at one unique point.

The divisors Δ and Γ can be seen as the graphs of the regular morphisms Id and F, from X to X, of degree 1 and q respectively. We deduce that $\Delta \cdot H = \Delta \cdot V = 1$ and that $\Gamma \cdot H = q$, $\Gamma \cdot V = 1$.

Since Δ and Γ intersect transversally, one has $\Delta \cdot \Gamma = \sharp X(\mathbb{F}_q)$.

To compute the auto-intersection Δ^2, we use the adjunction formula (cf. [Har77, Chap V, Prop 1.5]) which states that $2g(\Delta) - 2 = \Delta^2 + \Delta \cdot K_{X \times X}$, where $g(\Delta)$ is the genus of the curve Δ, and where $K_{X \times X}$ is the canonical class of the surface $X \times X$. Since Δ is isomorphic to X, one has $g(\Delta) = g$. As for the canonical class it is known to be equal to $(2g-2)(H+V)$ (cf. [Har77, Chap II, Ex 8.3]). This leads to the value of Δ^2.

The auto-intersection Γ^2 can be computed in the same way. Note that the genus of Γ is still g since the projection morphism $(P, F(P)) \mapsto P$ defines an isomorphism from Γ to X. □

Let $\mathrm{NS}(X \times X)$ be the Neron-Severi group of $X \times X$, that is the group $\mathrm{Div}(X \times X)$ modulo algebraic equivalence. This group is known to be a finitely generated abelian

group (cf. [Har77, Chap V, Ex 1.7]). The intersection pairing on $\mathrm{Div}(X \times X)$, depending only on equivalence classes, induces a symmetric bilinear pairing on $\mathrm{NS}(X \times X)$. Let $\mathrm{Num}(X \times X)$ be the quotient of $\mathrm{NS}(X \times X)$ by the kernel of this pairing. Then $\mathrm{Num}(X \times X)$ is a free finitely generated abelian group and extending the scalars, one obtains a finite dimensional real vector space $\mathrm{Num}(X \times X)_{\mathbb{R}} = \mathrm{Num}(X \times X) \otimes_{\mathbb{Z}} \mathbb{R}$. The most important result about this space, from which we will deduce all bounds in the sequel, is the Hodge index Theorem (cf. [Har77, Chap V, Th. 1.9, Rk 1.9.1]).

Theorem 2 (Hodge index Theorem)**.** *The bilinear form induced by the intersection pairing on the real vector space* $\mathrm{Num}(X \times X)_{\mathbb{R}}$ *is non-degenerate, definite negative on the orthogonal supplement of any ample divisor on the surface* $X \times X$*.*

> **Remark** – In fact, this result is true for any smooth surfaces. Here only the case of a square surface is needed. This special case was known by Weil and is contained in his book on curves [Wei48].

For the ample divisor $H + V$ (for instance by Nakai-Moishezon criterion, see [Har77, Chap V, Th 1.10], or using Veronese embeding) the intersection pairing is thus definite negative on $\langle H + V \rangle^{\perp}$. Nevertheless, working in the orthogonal $\mathrm{Vect}(H, V)^{\perp}$ of the bigger subspace generated by H and V yields to better bounds. Of course, the intersection pairing is also definite negative on $\mathrm{Vect}(H, V)^{\perp}$. By non-degeneracy on $\mathrm{Num}(X \times X)_{\mathbb{R}}$, there is an orthogonal decomposition

$$\mathrm{Num}(X \times X)_{\mathbb{R}} = \mathrm{Vect}(H, V) \oplus \mathrm{Vect}(H, V)^{\perp}$$

and the orthogonal projection p onto the non-trivial part $\mathrm{Vect}(H, V)^{\perp}$ is given by

$$\begin{array}{rccl} p: & \mathrm{Num}(X \times X)_{\mathbb{R}} & \longrightarrow & \mathrm{Vect}(H, V)^{\perp} \\ & D & \longmapsto & D - (D \cdot V)H - (D \cdot H)V. \end{array} \tag{1}$$

Definition 3. *Let* $\mathcal{E} = \mathcal{E}_X = \mathrm{Vect}(H, V)^{\perp}$ *inside the real vector space* $\mathrm{Num}(X \times X)_{\mathbb{R}}$*. We define on* $\mathcal{E}$ *a scalar product, denoted by* $\langle \cdot, \cdot \rangle$*, as*

$$\langle \varepsilon, \varepsilon' \rangle = -\varepsilon \cdot \varepsilon', \qquad \forall \varepsilon, \varepsilon' \in \mathcal{E}.$$

The associated norm on $\mathcal{E}$ *is denoted by* $\| \cdot \|$*.*

From now on, all the computations will take place in this euclidean space $(\mathcal{E}, \langle \cdot, \cdot \rangle)$. In particular, all the Gram matrices so as their determinants are relative to this scalar product; they are respectively denoted by $\mathrm{Gram}(\varepsilon_1, \ldots, \varepsilon_n)$ and $\mathrm{DetGram}(\varepsilon_1, \ldots, \varepsilon_n)$ for $\varepsilon_1, \ldots, \varepsilon_n \in \mathcal{E}$.

1.2 The vector space $\mathcal{F}_X$ generated by iterations of the Frobenius morphism

In fact, all the computations will take place in a smaller subspace $\mathcal{F} \subset \mathcal{E}$ generated by the projections of the graphs of iterated Frobenius morphism. The key role will be payed by the projections $p(\Gamma^k)$ of the graph of the k-th iterations Frobenius morphism on this euclidean vector space, or more conveniently by some normalization of it.

Definition 4. *Let $\Gamma^k \in \mathrm{Num}(X \times X)$ be the class of the diagonal for $k = 0$, and the class of the graph of the k-th iterated Frobenius morphism $F^k : X \to X$ for $k \geq 1$. For any $k \geq 0$, let*

$$\gamma^k = \frac{p(\Gamma^k)}{\sqrt{q^k}} \in \mathcal{E} \tag{2}$$

be some normalization of the non-trivial part $p(\Gamma^k)$ of Γ^k in $\mathcal{E}$ and put

$$\mathcal{F} = \mathcal{F}_X = \mathrm{Vect}(\gamma^k,\ k \geq 0). \tag{3}$$

To begin with, let us compute the Gram matrix of the normalized graphs of the iterates of the Frobenius morphism.

Proposition 5. *For every $i, j, \geq 0$, one has*

$$\left\langle \gamma^i, \gamma^j \right\rangle = \begin{cases} 2g & \text{if } i = j \\ x_{|i-j|} & \text{if } i \neq j \end{cases}, \qquad \text{or} \qquad \mathrm{Gram}\left(\gamma^j, \gamma^{j+i}\right) = \begin{pmatrix} 2g & x_i \\ x_i & 2g \end{pmatrix} \quad \text{if } i \geq 1,$$

where

$$x_i = \left\langle \gamma^0, \gamma^i \right\rangle = \frac{(q^i + 1) - \sharp X(\mathbb{F}_{q^i})}{\sqrt{q}^i} \tag{4}$$

for $i \geq 1$. Hence, the Gram matrix of the whole truncated ordered family $(\gamma^0, \gamma^1, \cdots, \gamma^n)$ is a Toeplitz one

$$\mathrm{Gram}(\gamma^0, \ldots, \gamma^n) = \begin{pmatrix} 2g & x_1 & \cdots & x_{n-1} & x_n \\ x_1 & \ddots & \ddots & & x_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{n-1} & & \ddots & \ddots & x_1 \\ x_n & x_{n-1} & \cdots & x_1 & 2g \end{pmatrix}. \tag{5}$$

Remark – Note that removing the normalization factor would yield by the proof below to the "skew Toeplitz" Gram matrices

$$\mathrm{Gram}\left(p\left(\Gamma^0\right), p\left(\Gamma^1\right), \ldots, p\left(\Gamma^n\right)\right) = \begin{pmatrix} u_0 & u_1 & \cdots & u_{n-1} & u_n \\ u_1 & qu_0 & \ddots & & qu_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ u_{n-1} & & \ddots & q^{n-1}u_0 & q^{n-1}u_1 \\ u_n & qu_{n-1} & \cdots & q^{n-1}u_1 & q^n u_0 \end{pmatrix} \tag{6}$$

with

$$u_0 = 2g \in \mathbb{Z} \qquad \text{and} \qquad u_n = \left\langle p\left(\Gamma^0\right), p\left(\Gamma^n\right) \right\rangle = (q^n + 1) - \sharp X(\mathbb{F}_{q^n}) \in \mathbb{Z}.$$

Proof — Since $\langle \gamma^k, \gamma^{k+i} \rangle = -\gamma^k \cdot \gamma^{k+i}$ and $\gamma^k = \frac{1}{\sqrt{q^k}} p(\Gamma^k) = \frac{1}{\sqrt{q^k}} \left(\Gamma^k - H - q^k V\right)$, we have only by (1) and by (4) to check that we have the following intersection matrix:

$$\begin{array}{c} \\ H \\ V \\ \Gamma^k \\ \Gamma^{k+i} \end{array} \begin{array}{c} \begin{array}{cccc} H & V & \Gamma^k & \Gamma^{k+i} \end{array} \\ \begin{pmatrix} 0 & 1 & q^k & q^{k+i} \\ 1 & 0 & 1 & 1 \\ q^k & 1 & q^k(2-2g) & q^k \sharp X(\mathbb{F}_{q^i}) \\ q^{k+i} & 1 & q^k \sharp X(\mathbb{F}_{q^i}) & q^{k+i}(2-2g) \end{pmatrix} \end{array}$$

The special case $k = 0$ and $i = 1$ corresponds to the intersection matrix of Proposition 1. The self-intersections in the general case can be computed as in this special case using the adjunction formula. For the same reason why $\Gamma^0 \cdot \Gamma^1 = \Delta \cdot \Gamma = \sharp X(\mathbb{F}_q)$, one has $\Gamma^0 \cdot \Gamma^i = \Delta \cdot \Gamma^i = \sharp X(\mathbb{F}_{q^i})$ for every $i \geq 1$. The remaining intersections to be calculated are the $\Gamma^k \cdot \Gamma^{k+i}$ for $k, i \geq 1$. One can relate them to the intersections $\Gamma^0 \cdot \Gamma^i$, using the projection formula (see [Liu02, Th 2.12, p. 398]) for the morphism $\Phi^k = F^k \times \mathrm{Id}$. We have $(\Phi^k)^*(\Delta) = \Gamma^k$ and $(\Phi^k)_* \left(\Gamma^{k+i}\right) = q^k \Gamma^i$, so that

$$\Gamma^k \cdot \Gamma^{k+i} = (\Phi^k)^*(\Delta) \cdot \Gamma^{k+i} = \Delta \cdot (\Phi^k)_* \left(\Gamma^{k+i}\right) = q^k \Delta \cdot \Gamma^i.$$

Formula (5) for the Gram matrix follows. □

1.3 Toeplitz interpretation of Riemann hypothesis for curves over finite fields

In this section, we point out the close link between on the one hand the euclidean structure on the "Frobenius" space $\mathcal{F}$ (Definition 4) coming ultimately from the Toeplitz shape of the Gram matrix as described in Appendix A.2 and on the other hand the Riemann hypothesis for curves. Note that the space $\mathcal{F}$ comes from the group $\mathrm{Num}(X \times X)$ which is a $\mathbb{Z}$-module of finite type. Therefore, $\mathcal{F}$ has a natural $\mathbb{Q}$-structure. We begin with a purely "Toeplitz version" of the Riemann hypothesis for curves.

Theorem 6 (Toeplitz version of Riemann hypothesis for curves)**.** *We keep the notation of Definition 4 and we denote by d the rank of the space $\mathcal{F}$ over $\mathbb{Q}$. Let $\rho : \mathcal{F} \to \mathcal{F}$ be the linear map defined by $p(\Gamma^n) \longmapsto p(\Gamma^{n+1})$ for $0 \leq n \leq d-1$. Then ρ is a similarity on $\mathcal{F}$ of ratio $\sqrt{q}$, satisfying $p(\Gamma^n) \mapsto p(\Gamma^{n+1})$ for any $n \geq 0$, and whose eigenvalues $\omega_1, \ldots, \omega_d \in \mathbb{C}$ are algebraic integers of complex modulus $\sqrt{q}$. Moreover, there exists some non-negative integers $\lambda_1, \ldots, \lambda_d \in \mathbb{N}^*$ such that*

$$\sum_{i=1}^{d} \lambda_i = 2g$$

and for any $n \geq 1$,

$$(q^n + 1) - \sharp X(\mathbb{F}_{q^n}) = \sum_{i=1}^{d} \lambda_i \omega_i^n.$$

Proof. Thanks to Proposition 5, we know that the euclidean space $\mathcal{F}$ has a "Toeplitz structure", that is $\mathrm{Gram}(\gamma^0, \dots, \gamma^n)$ is a Toeplitz matrix for any $n \geq 0$. Using Lemma 33 in Appendix A.2, we deduce that the dimension d of $\mathcal{F}$ corresponds to the minimal integer such that $\mathrm{Gram}(\gamma^0, \dots, \gamma^d)$ is singular. Let $(a_0, \dots, a_d) \in \mathbb{Q}^{d+1}$ be a generator of the kernel of this Gram-matrix. Then $\mathcal{F} = \bigoplus_{i=0}^{d-1} \mathbb{Q}\gamma^i$ and $\gamma^d = -\frac{1}{a_d}\left(a_0\gamma^0 + \cdots + a_{d-1}\gamma^{d-1}\right)$, where $a_d \neq 0$ since the family $(\gamma^i)_{0 \leq i \leq d-1}$ is free. Besides, the map $\iota : \mathcal{F} \to \mathcal{F}$ defined by $\gamma^n \mapsto \gamma^{n+1}$ for $0 \leq n \leq d-1$ is an isometry by item (i) of Theorem 36 in Appendix A.2. Therefore its eigenvalues have modulus 1 and moreover one easily proves recursively that $\iota(\gamma^n) = \gamma^{n+1}$ for any $n \geq 0$.

Since $p(\Gamma^n) = \sqrt{q}^n\gamma^n$ by Definition 4, the map ρ of the statement is nothing else than $\sqrt{q} \times \iota$. Thus it is a similarity of ratio $\sqrt{q}$, so that all its eigenvalues have modulus $\sqrt{q}$, and $\mathcal{F}$ is also a cyclic space under ρ.

To prove that these eigenvalues are algebraic integers, note that $p\left(\Gamma^0\right), p\left(\Gamma^1\right), \dots, p\left(\Gamma^{d-1}\right)$ being a $\mathbb{Q}$-basis of $\mathcal{F}_{\mathbb{Q}}$, there exist $b_1, \dots, b_d \in \mathbb{Q}$ such that

$$p\left(\Gamma^d\right) = b_1 p\left(\Gamma^{d-1}\right) + \cdots + b_d p\left(\Gamma^0\right).$$

Hence $\rho^d = b_1\rho^{d-1} + \cdots + b_d\,\mathrm{Id}$ since $\mathcal{F}$ is cyclic under ρ. Applied to $p\left(\Gamma^i\right)$, we get that for every $i \geq 0$,

$$p\left(\Gamma^{d+i}\right) = b_1 p\left(\Gamma^{d-1+i}\right) + \cdots + b_d p\left(\Gamma^i\right).$$

Taking the scalar product with $p\left(\Gamma^0\right)$, we obtain

$$u_{d+i} = b_1 u_{d-1+i} + \cdots + b_d u_i.$$

The sequence $(u_i)_{i \geq 0}$ is thus a rationally defined recursive integer valued sequence, and Fatou Lemma below implies that $b_1, \dots, b_d$ are rational integers.

To prove the last assertion, there exist by item (iv) of Theorem 36 some non negative real numbers $\lambda_1, \dots, \lambda_d \in \mathbb{R}_+^*$ such that

$$(q^n + 1) - \sharp X(\mathbb{F}_{q^n}) = \sum_{i=1}^{d} \lambda_i \omega_i^n$$

for any $n \geq 1$. This means that the Riemann Zeta function of X equals

$$Z_X(T) = \frac{\prod_{i=1}^{d}(1 - \omega_i T)^{\lambda_i}}{(1-T)(1-qT)}.$$

But it is well known, for instance using Riemann-Roch Theorem on X as in Stichtenoth [Sti93, Theorem V.1.6, p. 161], that this Zeta function is a rational function. This implies that the λ_i's are rational integers, and the proof is complete. □

Lemma 7 (Fatou [Fat04])**.** *Let $b_1, \dots, b_d \in \mathbb{Q}$ and $(u_n)_{n \geq 0}$ be a rational sequence defined by its first terms $u_0, \dots, u_{d-1} \in \mathbb{Q}$ and the recursive relation $u_{d+i} = b_1 u_{d-1+i} + \cdots + b_d u_i$ for all $i \geq 0$. If the sequence $(u_n)_{n \geq 0}$ is an integers sequence, then the coefficients of the recursive relation $b_1, \dots, b_d$ must also be integers.*

One can now rephrase the previous statement in a more standard language. We have proved that the vector space $\mathcal{F}$ is a cyclic space under the endomorphism ρ. It can be turned into an algebra over $\mathbb{R}$ and even over $\mathbb{Q}$. One can give a more geometric flavour of this structure of algebra by means of of the *composition* $\circ$ *of correspondences*, à la Weil. In fact, there exists such a composition law on $\mathrm{Div}(X \times X)$: given two divisors $D, D' \in \mathrm{Div}(X \times X)$, Weil [Wei48, Chap 2, §1, N°5, page 37] has defined their *composition* $D \circ D' \in \mathrm{Div}(X \times X)$. One check that $\Gamma^i \circ \Gamma^j = \Gamma^{i+j}$ and that this composition low is compatible with the numerical class equivalence. The similarity ρ of the previous theorem is nothing else than the multiplication map by $p(\Gamma)$ inside the algebra $(\mathcal{F}, +, \circ)$.

Then this similarity ρ can be related to the usual Frobenius morphism acting on the Tate module as follows. The non trivial part $\mathcal{E} = \langle H, V \rangle^{\perp}$ of the group $\mathrm{Num}(X \times X)$ is known to be isomorphic to the Endomorphism group $\mathrm{Hom}(J(X))$ of the jacobian $J(X)$ of X [Zar95, App. Chap VII, p. 153]. Under this isomorphism, the projection $p(\Gamma)$ corresponds to the usual Frobenius morphism acting on $J(X)$. Then using $\mathrm{Hom}(J(X)) \hookrightarrow \mathrm{Hom}\left(T_\ell(J(X))\right)$, we do recover the usual Frobenius action. Under the decomposition of $T_\ell(J(X))$ as sum of cyclic sub-spaces for the Frobenius morphism φ_ℓ, the $\mathbb{Q}$-vector space $\mathcal{F}_X$ maps to the cyclic component corresponding to the minimal polynomial of φ_ℓ. Hence, it can be said that $\mathcal{F}$ is a rational realization of the "minimal polynomial of the Frobenius" part of the Tate module.

2 Weil domains

For any integer $n \geq 1$, one can associate to any absolutely irreducible smooth projective curve X of genus g defined over $\mathbb{F}_q$ a point $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$, where $x_0 = 2g$ and x_i is defined by formula (4) for $i \geq 1$. Thanks to Proposition 5 and standard properties of Gram and Toeplitz matrices, we prove Proposition 10 that this point is contained in a convex domain $\mathcal{W}_n^g$ we call the *n-th Weil domain* defined below. We give some properties of this Weil domain in Proposition 9 and few consequences such as classical Weil bound as a very special case, making likely that this viewpoint should have other consequences.

2.1 Description of the Weil domain of order n

Recall that a Toeplitz matrix is a square matrix whose coefficients $a_{i,j}$ depend only on the difference $i - j$. It is symmetric if $a_{i,j}$ depends only on the absolute value $|i - j|$. For $n \geq 0$ and $(x_0, \ldots, x_n) \in \mathbb{R}^{n+1}$, let $T_{n+1}(x_0, \ldots, x_n)$ denote the symmetric Toeplitz matrix of size $n + 1$ defined by

$$T_{n+1}(x_0, \ldots, x_n) = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} & x_n \\ x_1 & \ddots & \ddots & & x_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{n-1} & & \ddots & \ddots & x_1 \\ x_n & x_{n-1} & \cdots & x_1 & x_0 \end{pmatrix} \tag{7}$$

In section A.2, we collect some useful results about *positive, semi-definite* such matrices. The *Weil domain* defined below is closely related to these matrices. In the sequel, the notations $T \succ 0$ and $T \succeq 0$ mean respectively positive, definite and positive, semi-definite.

Definition 8 (The Weil domain)**.** *Let $n \geq 1$, and $g \geq 0$. The n-th Weil domain $\mathcal{W}_n$ and the n-th affine Weil domain $\mathcal{W}_n^g$ at height g, or also at genus g, are defined by*

$$\mathcal{W}_n = \left\{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} \mid T_{n+1}(x_0, x_1, \dots, x_n) \succeq 0\right\} \tag{8}$$
$$\mathcal{W}_n^g = \left\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid T_{n+1}(2g, x_1, \dots, x_n) \succeq 0\right\}. \tag{9}$$

Let $(x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1}$ be such that $T_{n+1}(x_0, x_1, \dots, x_n) \succeq 0$. As explained in subsection A.2.1 of Appendix A.2, we shall think of $T_{n+1}(x_0, x_1, \dots, x_n)$ as the matrix of a symmetric positive definite bilinear form with respect to a family $\gamma_0, \dots, \gamma_n$ which generates a finite dimensional vector space. In other words, one has $T_{n+1}(x_0, x_1, \dots, x_n) = \mathrm{Gram}(\gamma_0, \dots, \gamma_n)$. With the help of Lemmas 34 and 35, we give some properties and alternative descriptions of the Weil domain.

Proposition 9. *The Weil domains satisfy the following assertions.*

(i) Both Weil domains, $\mathcal{W}_n$ and the affine ones $\mathcal{W}_n^g$ are convex. The affine domain $\mathcal{W}_n^g$ is bounded, contained in $[-2g, 2g]^n$.

(ii) The interior of the Weil domain can be recursively defined by

$$\overset{\circ}{\mathcal{W}}_n = \left\{(x_0, \dots, x_n) \in \overset{\circ}{\mathcal{W}}_{n-1} \times \mathbb{R} \mid \mathrm{Det}(T_{n+1}(x_0, \dots, x_n)) > 0\right\}$$

(iii) There exist two functions $w_n^+, w_n^- : \overset{\circ}{\mathcal{W}}_{n-1} \to \mathbb{R}$ such that

$$(x_0, \dots, x_n) \in \overset{\circ}{\mathcal{W}}_n \iff \begin{array}{l}(x_0, \dots, x_{n-1}) \in \overset{\circ}{\mathcal{W}}_{n-1} \text{ and} \\ w_n^-(x_0, \dots, x_{n-1}) < x_n < w_n^+(x_0, \dots, x_{n-1})\end{array} \tag{10}$$

Moreover the function w_n^+ is concave while w_n^- is convex and one has

$$w_n^+(x_0, \dots, x_{n-1}) - w_n^-(x_0, \dots, x_{n-1}) = 2 \cdot \frac{\mathrm{Det}\left(T_n(x_0, \dots, x_{n-1})\right)}{\mathrm{Det}\left(T_n(x_0, \dots, x_{n-2})\right)}$$

Proof. Item (*i*). The fact that both domains are convex is easy to prove. If $T_{n+1}(g, x_1, \dots, x_n) \succeq 0$ then $\begin{pmatrix} 2g & x_i \\ x_i & 2g \end{pmatrix} \succeq 0$ and thus $\mathcal{W}_n^g \subset [-2g, 2g]^n$.

Item (*ii*) follows from the well known fact that a symmetric matrix is definite positive if and only if all its leading principal minors (obtained by deleting the last rows and columns one after the other) are positive [HJ90, Theorem 7.2.5].

Item (*iii*). Let $(x_0,\dots,x_n)\in \overset{\circ}{\mathcal{W}}_n$ and let say that $T_{n+1}(x_0,\dots,x_n)=\mathrm{Gram}(\gamma_0,\dots,\gamma_n)$. Using notations of lemma 34, we have

$$\begin{array}{l}\mathrm{Gram}\left(\gamma'_0,\dots,\gamma'_{\lfloor\frac{n}{2}\rfloor}\right)\succ 0\\ \text{and }\ \mathrm{Gram}\left(\gamma'_{\lfloor\frac{n}{2}\rfloor+1},\dots,\gamma'_n\right)\succ 0\end{array}\ ,\quad \text{so that}\quad \begin{array}{l}\mathrm{DetGram}\left(\gamma'_0,\dots,\gamma'_{\lfloor\frac{n}{2}\rfloor}\right)>0\\ \text{and }\ \mathrm{DetGram}\left(\gamma'_{\lfloor\frac{n}{2}\rfloor+1},\dots,\gamma'_n\right)>0\end{array}\ .$$

Developing both determinants along their first column, one obtains two affine function in the variable x_n whose x_n-coefficient are the two positive factors $\mathrm{DetGram}\left(\gamma'_0,\dots,\gamma'_{\lfloor\frac{n}{2}-1\rfloor}\right)$ and $\mathrm{DetGram}\left(\gamma'_{\lfloor\frac{n}{2}\rfloor},\dots,\gamma'_{n-2}\right)$. This proves the existence of the two functions $w_n^{\pm}$. In order to be more explicit, one has to relate to Lemma 35. In fact, the two values $w_n^{\pm}(x_0,\dots,x_{n-1})$ must be the two scalar products denoted $x_n^{\pm}$ in this lemma. The rest of the item follows. □

Remark – Working with the closed set $\mathcal{W}_n$ instead of its interior is a little bit more subtle. The reason is that the characterization of definite positiveness used to prove item ii is not true anymore to characterize semi-definite positiveness. All diagonal minors have to be taken into account, and not only the so called *principal* ones.

Remark – When the euclidean space we deal with comes from a curve, we use exponent numbering for the datas (as for instance in Definition 4), and we use index numbering otherwise (as for instance in the previous paragraph).

2.2 The geometrico-euclidean constraint

The connection between Weil domains and our purpose is contained in the next proposition, coming from Proposition 5, positivity of Gram matrices and Definition 8.

Proposition 10 (Geometrico-euclidean[5] constraint for curves)**.** *If X is an absolutely irreducible smooth projective curve of genus g defined over the finite field $\mathbb{F}_q$, then for any $n\geq 1$, the euclidean point $(2g,x_1,\dots,x_n)$ defined by formula (4) lies in the affine Weil domain $\mathcal{W}_n^g$.*

2.2.1 Weil bound of order 1

Let us look closer at the first non-trivial geometrico-euclidean constraint given by Proposition 10, that is for $n=1$. We have $\mathrm{Gram}(\gamma^0,\gamma^1)\succeq 0$. But

$$\begin{pmatrix}2g & x_1\\ x_1 & 2g\end{pmatrix}\succeq 0 \iff \begin{vmatrix}2g & x_1\\ x_1 & 2g\end{vmatrix}\geq 0 \iff \begin{vmatrix}2g & \frac{(q+1)-\sharp X(\mathbb{F}_q)}{\sqrt{q}}\\ \frac{(q+1)-\sharp X(\mathbb{F}_q)}{\sqrt{q}} & 2g\end{vmatrix}\geq 0,$$

which is nothing else than Weil bound!

[5] *Euclidean* because of positiveness of a symmetric Gram matrix in an euclidean space, and *geometric* because the euclidean feature comes from the geometry of the algebraic surface $X\times X$ via Hodge Index Theorem.

Theorem 11 (Weil inequality)**.** *Let X be an absolutely irreducible smooth projective curve of genus g defined over $\mathbb{F}_q$, then*

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

So, Weil inequality boils down only to the Schwartz inequality for the vectors $\gamma^0, \gamma^1 \in \mathcal{E}$. Likewise, for every $i \geq 1$, the condition $\mathrm{Gram}(\gamma^0, \gamma^i) = \left(\begin{smallmatrix} 2g & x_i \\ x_i & 2g \end{smallmatrix}\right) \succeq 0$ leads to Weil inequality over $\mathbb{F}_{q^i}$.

2.2.2 Comparison between $\sharp X(\mathbb{F}_q)$ and $\sharp X(\mathbb{F}_{q^2})$

In the same spirit, from the fact that $\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^2) \succeq 0$, one can deduce that

$$\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^2) = \begin{pmatrix} 2g & x_1 & x_2 \\ x_1 & 2g & x_1 \\ x_2 & x_1 & 2g \end{pmatrix} \succeq 0, \quad \text{hence} \quad (2g - x_2)(4g^2 + 2gx_2 - 2x_1^2) \geq 0,$$
$$\text{so that} \quad 2g^2 + gx_2 - x_1^2 \geq 0.$$

From the values of x_1, x_2 in (4), we obtain the following proposition which states that for a non rational curve X, any lower bound for the deviation of $\sharp X(\mathbb{F}_q)$ from $(q+1)$ yields to a better upper bound than the Weil one for $\sharp X(\mathbb{F}_{q^2})$.

Proposition 12. *Let X be a curve of genus $g > 0$ over $\mathbb{F}_q$, then*

$$\sharp X(\mathbb{F}_{q^2}) - (q^2+1) \leq 2gq - \frac{1}{g}\Big(\sharp X(\mathbb{F}_q) - (q+1)\Big)^2.$$

In the same way, the positivity $\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^i) \succeq 0$ yields to a (quite ugly) similar upper bound for $\sharp X(\mathbb{F}_{q^i})$ in terms of $\sharp X(\mathbb{F}_q)$ and $\sharp X(\mathbb{F}_{q^{i-1}})$.

It worth to notice that Proposition 12 contains the well known fact that a Weil maximal or minimal curve over $\mathbb{F}_q$ is Weil minimal over $\mathbb{F}_{q^2}$. Just for fun, we can also easily recover this fact directly on the Gram determinant. Indeed, being Weil maximal over $\mathbb{F}_q$ means, by Theorem 11 and notation (4), that $x_1 = -2g$. Therefore

$$\mathrm{DetGram}(\gamma^0, \gamma^1, \gamma^2) = \begin{vmatrix} 2g & -2g & x_2 \\ -2g & 2g & -2g \\ x_2 & -2g & 2g \end{vmatrix} = -2g(2g - x_2)^2 \geq 0, \qquad \text{so that} \qquad x_2 = 2g,$$

that is, by Theorem 11 and notation (4), X is minimal over $\mathbb{F}_{q^2}$. Then

$$\mathrm{DetGram}(\gamma^0, \gamma^2, \gamma^3) = \begin{vmatrix} 2g & 2g & x_3 \\ 2g & 2g & -2g \\ x_3 & -2g & 2g \end{vmatrix} = -2g(2g + x_3)^2 \geq 0, \qquad \text{so that} \qquad x_3 = -2g,$$

that is X is maximal over $\mathbb{F}_{q^3}$, and so on... In the same way, if X is minimal over $\mathbb{F}_q$, that is if $x_1 = 2g$, then

$$\mathrm{DetGram}(\gamma^0, \gamma^1, \gamma^2) = \begin{vmatrix} 2g & 2g & x_2 \\ 2g & 2g & 2g \\ x_2 & 2g & 2g \end{vmatrix} = -2g(x_2 - 2g)^2 \geq 0, \qquad \text{that is} \qquad x_2 = 2g,$$

and X still minimal over $\mathbb{F}_{q^2}$. And so on again...

3 Weil bounds of higher orders

To get better bounds, we need to add some *arithmetic* constraints to the geometrico-euclidean previous one. Besides the description of the arithmetic constraints, all this section is devoted to the illustration and the proof of the main Theorem 14 of this paper below, stating that the set of constraints lead to a sequence of better and better Weil's order n upper-bounds as n increases, in accordance with the figure in the Introduction for $q = 2$.

3.1 Description of the arithmetic constraints for the generalized Weil bounds

As suggested by Ihara [Iha81], the natural arithmetic constraints $\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q)$, for every $i \geq 1$, should be fruitfully taken into account. They are easily traduced into some inequalities involving the scalar products x_i defined by equation (4):

$$\begin{aligned} x_i &= \frac{1 + q^i - \sharp X(\mathbb{F}_{q^i})}{\sqrt{q}^i} = \frac{(1 + q - \sharp X(\mathbb{F}_q)) + (q^i - q) - (\sharp X(\mathbb{F}_{q^i}) - \sharp X(\mathbb{F}_q))}{\sqrt{q}^i} \\ &= \frac{1}{\sqrt{q}^{i-1}} \frac{1 + q - \sharp X(\mathbb{F}_q)}{\sqrt{q}} + \sqrt{q}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right) - \frac{\sharp X(\mathbb{F}_{q^i}) - \sharp X(\mathbb{F}_q)}{\sqrt{q}^i} \\ &\leq \ell_i(x_1), \end{aligned}$$

where $\ell_i(x_1)$ are the affine functions[6]

$$\ell_i(x_1) = \frac{x_1}{\sqrt{q}^{i-1}} + \sqrt{q}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right). \tag{11}$$

The aim of this section is to investigate the bounds that can be derived from the conjunction of all constraints.

The **geometrico-euclidean** one:
$$\begin{array}{l} \mathrm{Gram}(\gamma^0, \ldots, \gamma^n) = T_{n+1}(2g, x_1, \ldots, x_n) \succeq 0 \\ \text{that is} \quad (2g, x_1, \cdots, x_n) \in \mathcal{W}_n^g. \end{array}, \tag{12}$$

The **arithmetic** ones:
$$x_i \leq \frac{x_1}{\sqrt{q}^{i-1}} + \sqrt{q}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right), \quad 2 \leq i \leq n. \tag{13}$$

[6] Note that $\ell_1(x_1) = 1$.

A new phenomenon arises here. Unlike in section 2.2.1, the arithmetic constraints yield to better bounds than Weil one (Theorem 11) only for large enough genus g. A nice point of this point of view is that the genus from which better bounds can be obtained appears very naturally, if not to say visually!

In order to ease the statements of the main Theorem, we need to give a name to the set of points $(x_1, \ldots, x_n)$ satisfying equalities in the arithmetic constraints, cutout by the hyperplane $x_0 = 2g$.

Definition 13 (The Ihara line)**.** *For $g \geq 0$, the Ihara line $\mathcal{I}_n^g$ is the affine line whose equations are*

$$\begin{cases} x_0 = 2g \\ x_i = \ell_i(x_1) \quad 2 \leq i \leq n \end{cases}$$

in the affine hyperplane $x_0 = 2g$ of $\mathbb{R}^{n+1}$, where

$$\ell_i(x_1) = \frac{x_1}{\sqrt{q}^{i-1}} + \sqrt{q}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right). \tag{14}$$

3.2 Statement of the main Theorem

We now state the main Theorem of this paper.

Theorem 14 (Weil bound of order n)**.** *There exist a strictly increasing sequence $(g_n)_{n\geq 1}$ of non-negative real numbers and a sequence $(\mathbf{N}_n^\star)_{n\geq 1}$ of strictly increasing functions from $[g_n, +\infty[$ to $\mathbb{R}$, such that for any $g \geq g_n$, the value $\mathbf{N}_n^\star(g)$ is an upper bound for the number of rational points of any smooth, projective and absolutely irreducible curve over $\mathbb{F}_q$ of genus g. More precisely:*

(i) For any smooth, projective and absolutely irreducible curve X over $\mathbb{F}_q$ of genus $g \geq g_n$, one has

$$\sharp X(\mathbb{F}_q) \leq \mathbf{N}_n^\star(g) \tag{15}$$

for the sequences $(g_n)_{n\geq 1}$ and $(\mathbf{N}_n^\star)_{n\geq 1}$ given by

$$g_n = \sqrt{q}^{n+1} \sum_{k=1}^{n} \frac{1}{\sqrt{q}^k} \cos\left(\frac{k\pi}{n+1}\right) \tag{16}$$

$$\mathbf{N}_n^\star(g) = (q+1) - \sqrt{q} \times \mathbf{x}_{\mathbf{1},n}^\star(g), \tag{17}$$

where $\mathbf{x}_{\mathbf{1},n}^\star(g)$ is the smallest x_1-coordinate of the intersection points of the Ihara affine line $\mathcal{I}_n^g$ with the convex affine Weil domain $\mathcal{W}_n^g$.

(ii) We have

$$N_n^\star(g_{n+1}) = N_{n+1}^\star(g_{n+1}) = 1 + \sqrt{q}^{n+2}, \tag{18}$$

and the bound $\mathbf{N}_{n+1}^\star(g)$ is sharper than $\mathbf{N}_n^\star(g)$ for $g > g_{n+1}$, that is $\mathbf{N}_{n+1}^\star(g) < \mathbf{N}_n^\star(g)$.

(iii) *The genus g_n is the genus g for witch the Ihara line $\mathcal{I}_n^g$ meets the affine Weil domain $\mathcal{W}_n^g$ at the intersection*[7] *of the two hypersurfaces $x_n = w_n^{\pm}(2g, x_1, \ldots, x_{n-1})$.*

(iv) *For $g \geq g_n$, the minimum $\mathbf{x}^\star_{\mathbf{1},n}(g)$ is reached on the intersection of the Ihara line with the hypersurface $x_n = w_n^-(x_1, \cdots, x_{n-1})$, that is is a solution of the equation*

$$w_n^-(x_1, \ell_2(x_1), \cdots, \ell_{n-1}(x_1)) = \ell_n(x_1). \tag{19}$$

Remark – Note that item (*ii*) means that the Weil bounds $\mathbf{N}_n^\star$ glue together to give a continuous global bound $\mathbf{N}^\star$ in such a way that $\mathbf{N}^\star(g) = \mathbf{N}_n^\star(g)$ for the order n such that $g \in]g_n, g_{n+1}]$.

For instance, we have $\mathbf{x}^\star_{\mathbf{1},1}(g) = -2g$ at order 1, and we will give the value for $\mathbf{x}^\star_{\mathbf{1},2}(g)$ at order 2 in formula (21). Although it is not strictly necessary, we start to study in details the cases $n = 2$ and $n = 3$ in subsections 3.3 and 3.4. This allows to explain, and especially to give "a view" of the phenomena that arises. During this way, we also recover that Ihara bound is neither that this actual second-order Weil bound, and we write down the new third-order Weil bound. We postpone the complete proof of Theorem 14 in subsection 3.5 by linking our problematic to the Oesterlé one.

3.3 Weil bound of order 2 (Ihara bound)

For $n = 2$, the geometrico-euclidean constraint is $\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^2) \succeq 0$, or more conveniently $\mathrm{Gram}\left(\frac{\gamma^0+\gamma^2}{\sqrt{2}}, \gamma^1, \frac{\gamma^0-\gamma^2}{\sqrt{2}}\right) \succeq 0$, (see Lemma 34) that is

$$\begin{pmatrix} 2g + x_2 & \sqrt{2}x_1 & 0 \\ \sqrt{2}x_1 & 2g & 0 \\ 0 & 0 & 2g - x_2 \end{pmatrix} \succeq 0, \qquad \text{meaning that} \qquad \begin{cases} -2g \leq x_1 \leq 2g \\ \frac{x_1^2}{g} - 2g \leq x_2 \leq 2g \end{cases}.$$

Note that this contains the condition $\mathrm{Gram}(\gamma^0, \gamma^1) \succeq 0$. Using the notations of Proposition 9, one has $w_2^+(2g, x_1) = 2g$ and $w_2^-(2g, x_1) = \frac{x_1^2}{g} - 2g$. As for the arithmetic constraint, this is only

$$x_2 \leq \ell_2(x_1) = \frac{x_1}{\sqrt{q}} + q - 1.$$

In other terms, inside the affine plane $x_0 = 2g$, the points $(2g, x_1, x_2)$ must lie in the convex affine Weil space $\mathcal{W}_2^g$, and *under* the Ihara line $\mathcal{I}_2^g$ whose equation is the arithmetic constraint. One can distinguish three cases depending on the genus g. A picture of each of them is drawn in figure 1. It appears that if the genus is not large enough, then the added *arithmetic* constraint does not restrict the Weil domain. On the other hand, making the genus growing, then this constraint turns to become active. This happens

[7] This can be called the *seam* of the third affine Weil domain.

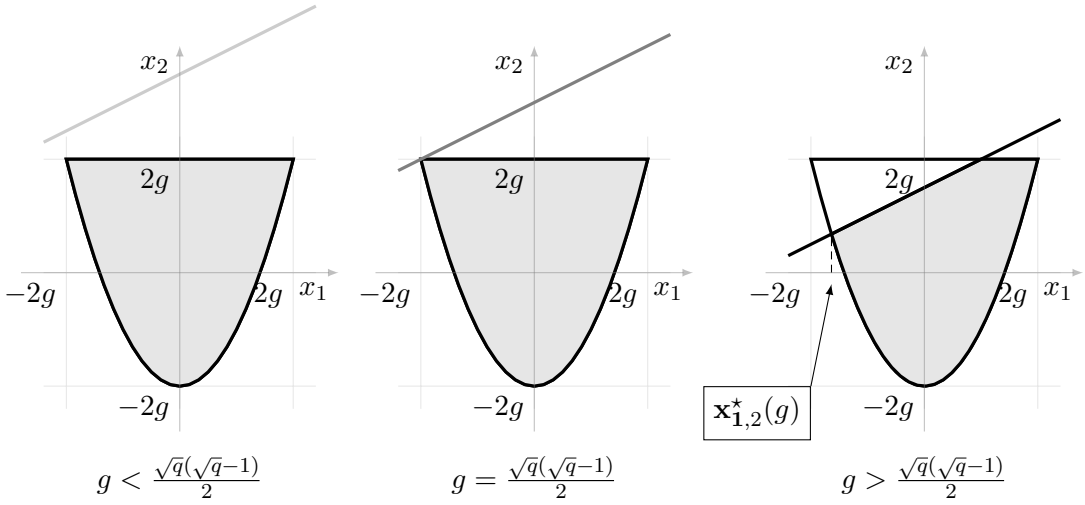


Figure 1: Three affine Weil domains $\mathcal{W}_2^g$ and Ihara lines $\mathcal{I}_2^g$ for different genus g inside the plane $x_0 = 2g$: points (x_1, x_2) coming from a curve must lie in the dashed area.

from the value of g for which in the affine plane $x_0 = 2g$, the line $x_2 = \frac{x_1}{\sqrt{q}} + q - 1$ passes through the point $(-2g, 2g)$, that is for

$$g = \frac{\sqrt{q}\left(\sqrt{q}-1\right)}{2}. \tag{20}$$

Notice that the point $(-2g, 2g)$ and $(2g, 2g)$ correspond to the locus inside $\mathcal{W}_2^g$ in the affine space $x_0 = 2g$ where the two graphs $x_2 = w_2^+(2g, x_1)$ and $x_2 = w_2^-(2g, x_1)$ do meet, in accordance with item (*iii*) of Theorem 14.

For $g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}$, the arithmetic constraint restricts the Weil domain and we get a better[8] lower bound $\mathbf{x}^\star_{\mathbf{1},2}(g)$ for the abscissa x_1. From the right part of figure 1, this bound is the x_1-coordinate of the left intersection point of the curve $x_2 = w_2^-(2g, x_1) = \frac{x_1^2}{g} - 2g$ with the affine Ihara line $\mathcal{I}_2^g$ (see Definition 13) whose equation is $x_2 = \frac{x_1}{\sqrt{q}} + q - 1$. An easy computation leads to a best abscissa

$$\mathbf{x}^\star_{\mathbf{1},2}(g) = \frac{g - \sqrt{(8q+1)g^2 + 4q(q-1)g}}{4\sqrt{q}}. \tag{21}$$

Going back to $\sharp X(\mathbb{F}_q)$ using formulas (4), we recover the well known Ihara bound.

Theorem 15 (Ihara bound [Iha81])**.** *Let X be a curve of genus g over $\mathbb{F}_q$ then*

$$\sharp X(\mathbb{F}_q) - (q+1) \leq \frac{\sqrt{(8q+1)g^2 + 4q(q-1)g} - g}{2}$$

[8] Than the usual Weil bound $x_1 \geq -2g$.

and this bound is better than the Weil one as soon as $g \geq \frac{\sqrt{q}(\sqrt{q}-1)}{2}$.

Of course, the values given by formula (21) and $g_2 = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$ meet those given respectively by equations (16) and (17) in the main Theorem 14.

Remark – One may wonder whether one can also optimize in this way the usual Weil *lower* bound $\sharp X(\mathbb{F}_q) \geq (q+1) - 2g\sqrt{q}$, that is $x_1 \leq 2g$. For g large enough[9], one indeed obtain a best upper bound for x_1, that is a lower bound for $\sharp X(\mathbb{F}_q)$, seemingly optimizing Weil lower bound. Unfortunately, this works only for so large genus that this "new" lower bound is negative!

3.4 Weil bound of order 3 (new bound)

For $n = 3$, the geometrico-euclidean constraint is $\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^2, \gamma^3) \succeq 0$, or more conveniently as in Lemma 34

$$\mathrm{Gram}\left(\frac{\gamma^0+\gamma^3}{\sqrt{2}}, \frac{\gamma^1+\gamma^2}{\sqrt{2}}, \frac{\gamma^0-\gamma^3}{\sqrt{2}}, \frac{\gamma^1-\gamma^2}{\sqrt{2}}\right)$$
$$= \begin{pmatrix} 2g+x_3 & x_1+x_2 & 0 & 0 \\ x_1+x_2 & 2g+x_1 & 0 & 0 \\ 0 & 0 & 2g-x_3 & x_1-x_2 \\ 0 & 0 & x_1-x_2 & 2g-x_1 \end{pmatrix} \succeq 0.$$

It is equivalent to $(2g, x_1, x_2) \in \mathcal{W}_2$ together with the two inequalities coming from the semi-positiveness of the the preceding sub-Gram determinants:

$$\underbrace{-2g + \frac{(x_1+x_2)^2}{2g+x_1}}_{w_3^-(2g,x_1,x_2)} \leq x_3 \leq \underbrace{2g - \frac{(x_1-x_2)^2}{2g-x_1}}_{w_3^+(2g,x_1,x_2)}$$

As for the arithmetic constraints, they are

$$x_2 \leq \ell_2(x_1) = \frac{x_1}{\sqrt{q}} + q - 1 \qquad \text{and} \qquad x_3 \leq \ell_3(x_1) = \frac{x_1}{q} + \frac{q^2-1}{\sqrt{q}}.$$

By item (*iii*) of Theorem 14, the genus from which the last constraint becomes active is the one for which the Ihara line $\mathcal{I}_3^g$ meets the affine Weil domain $\mathcal{W}_3^g$ at the intersection of the two affine surfaces $x_3 = w_3^-(2g, x_1, x_2)$ and $x_3 = w_3^+(2g, x_1, x_2)$.

Let us begin by computing this intersection. The two last equalities correspond to the nullity of both $\mathrm{DetGram}\left(\frac{\gamma^0+\gamma^3}{\sqrt{2}}, \frac{\gamma^1+\gamma^2}{\sqrt{2}}\right)$ and $\mathrm{DetGram}\left(\frac{\gamma^0-\gamma^3}{\sqrt{2}}, \frac{\gamma^1-\gamma^2}{\sqrt{2}}\right)$, that is to

$$(x_3+2g)(x_1+2g) = (x_1+x_2)^2 \qquad \text{and} \qquad (x_3-2g)(x_1-2g) = (x_1-x_2)^2.$$

[9] To be precise, from the genus $g = \frac{\sqrt{q}(\sqrt{q}+1)}{2}$ for which the Ihara line passes through the upper right point $(2g, 2g)$ of the Weil domain.

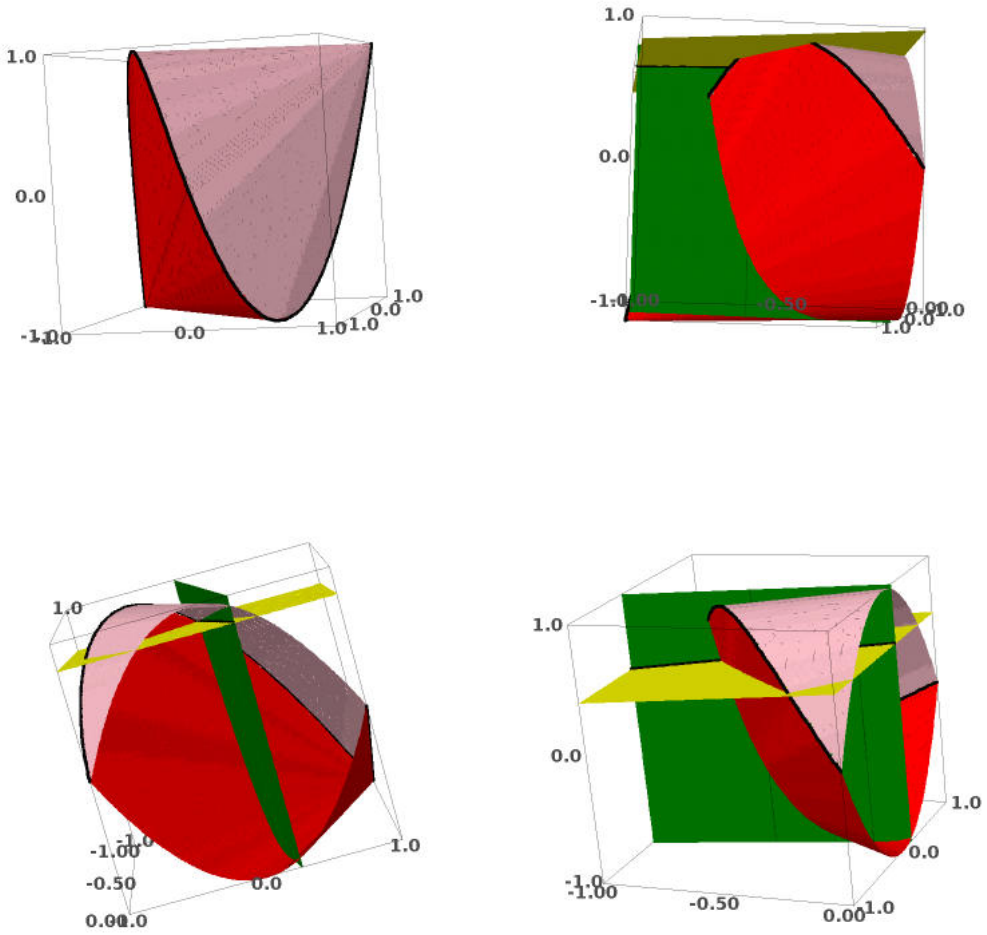


Figure 2: The affine Weil domains $\mathcal{W}_3^g$ for $g \geq 0$ are all homothetic to the domain drawn in the top-left figure. In the other three figures, we add the affine Ihara line (intersection of the green and yellow affine hyperplane). Top-right: the genus is too small and the new constraint is not active. Bottom-left: the genus $g = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ and the Ihara line meet the Weil domain at its seam. Bottom-right: the new constraint becomes active.

This also implies that $\mathrm{DetGram}(\gamma^0,\gamma^1,\gamma^2)=0$, or more conveniently

$$\mathrm{DetGram}\left(\frac{\gamma^0+\gamma^2}{\sqrt{2}},\gamma^1,\frac{\gamma^0-\gamma^2}{\sqrt{2}}\right)=\begin{vmatrix}2g+x_2 & \sqrt{2}x_1 & 0\\ \sqrt{2}x_1 & 2g & 0\\ 0 & 0 & 2g-x_2\end{vmatrix}=0.$$

Therefore, either $x_2=2g$, in which case $x_1=x_3$. Or $gx_2=x_1^2-2g^2$, and we deduce that

$$g(x_2+x_1)=(x_1-g)(x_1+2g),\qquad\qquad g(x_2-x_1)=(x_1+g)(x_1-2g),$$

and thus $x_3=\frac{x_1^3}{g^2}-3x_1$. In conclusion, inside the affine space $x_0=2g$, the two surfaces $x_3=w_3^{\pm}(2g,x_1,x_2)$ meet along the union of the two segments of parametric curves

$$\{(x_1,2g,x_1)\,,\ -2g\le x_1\le 2g\}\cup\left\{\left(x_1,\frac{x_1^2}{g}-2g,\frac{x_1^3}{g^2}-3x_1\right),\ -2g\le x_1\le 2g\right\}\quad(22)$$

Remark – For the second segment and for $i=1,2,3$, if we put $y_i=\frac{x_i}{g}$, then one has $y_i=C_i(y_1)$, where C_1,C_2,C_3 denote the first three Chebychev polynomials.

Now, the genus from which the second constraint $x_3=\frac{x_1}{q}+\frac{q^2-1}{\sqrt{q}}$ becomes active is thus the one for which the curve given by formula (22) above meets the Ihara line, which is parametrized by

$$\left(x_1,\frac{x_1}{\sqrt{q}}+q-1,\frac{x_1}{q}+\frac{q^2-1}{\sqrt{q}}\right),\qquad\qquad x_1\in\mathbb{R}$$

To find such a genus it suffices to eliminate x_1 in the system of equation

$$\begin{cases}\frac{x_1^2}{g}-2g=\frac{x_1}{\sqrt{q}}+q-1\\ \frac{x_1^3}{g^2}-3x_1=\frac{x_1}{q}+\frac{q^2-1}{\sqrt{q}}.\end{cases}$$

Using `magma`, we compute the resultant in x_1 of the two polynomials obtained by difference in the preceding system; up to a power of g factor, the result is

$$(g-1)\left(g-\frac{\sqrt{q}(q-1)}{\sqrt{2}}\right)\left(g-\frac{\sqrt{q}(1-q)}{\sqrt{2}}\right)$$

After taking off unadmissible solutions, it only remains the value

$$g=\frac{\sqrt{q}(q-1)}{\sqrt{2}}\qquad(23)$$

which of course meets the value of g_3 given by equation (16) of Theorem 14. For $g\ge g_3=\frac{\sqrt{q}(q-1)}{\sqrt{2}}$, the last arithmetic constraint become active and the minimum $\mathbf{x}^{\star}_{\mathbf{1},3}(g)$ of the abscissa x_1 is attained by item (*iv*) of Theorem 14 on the intersection of the

surface $x_3 = w_3^-(x_1, x_2)$ with the Ihara line. In order to calculate this intersection, we have to solve the system of equations

$$\begin{cases} (x_1+x_2)^2 - (g+x_1)(g+x_3) = 0 \\ x_2 = \ell_2(x_1) = \frac{x_1}{\sqrt{q}} + \frac{q-1}{2} \\ x_3 = \ell_3(x_1) = \frac{x_1}{q} + \frac{q^2-1}{2\sqrt{q}} \end{cases}$$

This leads to some quadratic equation in x_1 whose discriminant and roots, althought really ugly, are easily computed. Skipping these calculations, we only give the final result which is nothing else than the case $n = 3$ of Theorem 14.

Theorem 16. *Let X be a smooth, projective, absolutely irreducible curve defined over $\mathbb{F}_q$, of genus $g \geq g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$. Then*

$$\sharp X(\mathbb{F}_q) - (q+1) \leq \left(\frac{\sqrt{a(q) + \frac{b(q)}{g} + \frac{c(q)}{g^2}} - \frac{q+1}{q} - \frac{d(q)}{g}}{\sqrt{q}+2} \right) g\sqrt{q},$$

where

$$\begin{cases} a(q) = \frac{(5q-2\sqrt{q}+1)(\sqrt{q}+1)^2}{q^2} \\ b(q) = \frac{(q-1)(q+1)(3\sqrt{q}-1)(\sqrt{q}+1)}{q\sqrt{q}} \\ c(q) = \frac{(q-1)^2(q^2-4q\sqrt{q}-2q-4\sqrt{q}+1)}{4q} \\ d(q) = \frac{(q-1)(q-2\sqrt{q}-1)}{2\sqrt{q}} \end{cases}$$

The formula becomes nicer if we let g going to infinity. We obtain the following third order asymptotic bound for Ihara constant $A(q)$ (see [Iha81]).

Corollary 17. *The Ihara constant $A(q)$ is bounded above by:*

$$A(q) \leq \frac{\sqrt{5 + \frac{8}{\sqrt{q}} + \frac{2}{q} + \frac{1}{q^2}} - \left(1 + \frac{1}{q}\right)}{1 + \frac{2}{\sqrt{q}}} \sqrt{q}.$$

Remark – For q large the preceding upper bound is equivalent to $(\sqrt{5}-1)\sqrt{q} \simeq 1,236\sqrt{q}$. This is better than the upper bound of $A(q)$ following from Ihara bound

$$A(q) \leq \frac{\sqrt{8q+1}-1}{2},$$

which is equivalent to $\sqrt{2q} \simeq 1,414\sqrt{q}$ for q large. Later, in Theorem 29, we prove that the upper bounds for $A(q)$ that are deduced from the Weil bounds of growing orders, asymptotically tend to the Drinfeld-Vlăduţ bound, $A(q) \leq \sqrt{q} - 1$.

3.5 Oesterlé bounds and proof of Theorem 14

In order to prove the main Theorem 14, it is convenient to turn the generalized Weil bound optimization problem into a conic optimization one. We relate then this optimization problem to the one formulated and solved by Oesterlé for his own bounds. The reader is referred to Appendix A.1 for details on conic programming.

3.5.1 Two optimization problems

Depending on whether we choose to fix a genus or a number of points, one can express two optimization problems.

Weil primal optimization problem. — In the spirit of the preceding sections, we fix a genus g and we intend to give an upper bound for the number of points N over $\mathbb{F}_q$ that can have a curve of genus less than g from some constraints. Since $x_1 = \frac{1+q-N}{\sqrt{q}}$ by (4), maximizing the number of points N is equivalent to minimizing the scalar product x_1. The geometrico-euclidean and arithmetic constraints (12) and (13) lead to what we call the **generalized Weil optimization problem**.

Definition 18 (generalized Weil optimization problem)**.** *Put*

$$\alpha = \frac{1}{\sqrt{q}}, \qquad \beta_i = \sqrt{q}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right), \tag{24}$$

and let $g \geq 0$ be a constant (thought as a genus). The associated generalized Weil optimization problem of order $n \geq 1$ consists in computing the minimum

$$\mathbf{x}^{\star}_{\mathbf{1},n}(g) \stackrel{def.}{=} \min\left\{ x_1 \;\middle|\; \begin{array}{l} T_{n+1}(x_0, x_1, \ldots, x_n) \succeq 0 \\ x_0 \leq 2g \\ x_i - \alpha^{i-1} x_1 \leq \beta_i, 2 \leq i \leq n \end{array} \right\}. \tag{W_n}$$

We denote by

$$\mathbf{N}^{\star}_n(g) = 1 + q - \sqrt{q} \times \mathbf{x}^{\star}_{\mathbf{1},n}(g) \tag{25}$$

the corresponding value for the maximum of the number N.

Oesterlé primal optimization problem. — On the other hand, one can fix after Oesterlé a number of points N and intend to give a lower bound on the genus of a curve X over $\mathbb{F}_q$ that has at least N rational points over $\mathbb{F}_q$, i.e. $\sharp X(\mathbb{F}_q) \geq N$. For every $i \geq 1$, one imposes the arithmetic constraint $\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q) \geq N$, which turn be

$$\begin{aligned} x_i &= \frac{1 + q^i - \sharp X(\mathbb{F}_{q^i})}{\sqrt{q^i}} = \frac{1 + q^i - N}{\sqrt{q^i}} - \frac{\sharp X(\mathbb{F}_{q^i}) - N}{\sqrt{q^i}} \\ &\leq \frac{1 + q^i - N}{\sqrt{q^i}}. \end{aligned}$$

Taking into account the geometrico-euclidean constraint $(x_0, x_1, \ldots, x_n) \in \mathcal{W}_n$ leads to the following optimization problem.

Definition 19 (Oesterlé optimization problem)**.** *Let $N \geq 1$ be a constant (thought as a number) and put*

$$\forall i \geq 1, \qquad \delta_i(N) = \frac{1 + q^i - N}{\sqrt{q^i}}. \tag{26}$$

The Oesterlé optimization problem of order $n \geq 1$ consists in computing the minimum

$$\mathbf{g}_n^\star(N) \overset{def.}{=} \frac{1}{2} \min \left\{ x_0 \;\middle|\; \begin{array}{l} T_{n+1}(x_0, x_1, \ldots, x_n) \succeq 0 \\ x_i \leq \delta_i(N), 1 \leq i \leq n \end{array} \right\}. \tag{O_n}$$

Both optimization problems enter the class of *semi-definite* optimizations problems because they involve a condition where a symmetric matrix must be *positive semi definite*. One can also turn these problems into what is called a *conic program*, making easier the formulation of the corresponding dual problem and leading to the proof of the fact that these two problems are equivalent in some sense.

3.5.2 Conic reformulation of (W_n) and (O_n) with their dual problems

The optimization problems (W_n) and (O_n) can be turned into conic optimization problems using trigonometric polynomials.

Let $\mathbb{T} = \{z \in \mathbb{C},\ |z| = 1\}$ be the complex unit circle and let $\mathrm{Pol}\mathbb{T}_n$ denote the real vector space of trigonometric polynomials of degree less than n, with real coefficients, and having real values on the unit circle:

$$\mathrm{Pol}\mathbb{T}_n = \left\{ P(z) = \sum_{i=-n}^{n} a_i z^i \mid a_i \in \mathbb{R},\ \text{and } P(\mathbb{T}) \subset \mathbb{R} \right\}.$$

The latter condition is equivalent to $a_{-i} = a_i$ for all $i \geq 1$, so that $\mathrm{Pol}\mathbb{T}_n$ has dimension $n+1$ with basis

$$\mathrm{Pol}\mathbb{T}_n = \bigoplus_{i=0}^{n} \mathbb{R} P_i,$$

with

$$P_0 = 1, \quad \text{and} \quad P_i = z^i + \frac{1}{z^i}, \quad 1 \leq i \leq n.$$

This space is endowed with a structure of $(n+1)$-dimensional euclidean space for the usual scalar product defined by

$$\left\langle \sum_{i=0}^{n} a_i P_i, \sum_{i=0}^{n} b_i P_i \right\rangle = a_0 b_0 + 2 \sum_{i=1}^{n} a_i b_i.$$

Note that the basis $(P_0, \ldots, P_n)$ is orthogonal but not orthonormal since $\langle P_i, P_i \rangle = 2$ for $i \geq 1$. It follows that one has $P = \langle P, P_0 \rangle + \sum_{i=1}^{n} \frac{\langle P, P_i \rangle}{2} P_i$ for every $P \in \mathrm{Pol}\mathbb{T}_n$. Last, we need to introduce two very important subsets of $\mathrm{Pol}\mathbb{T}_n$.

Definition 20. *Let $n \geq 1$.*

(i) We denote by $\mathrm{Pol}\mathbb{T}_n^{\geq 0}$ the subset of ***non-negative*** *trigonometric polynomials:*

$$\mathrm{Pol}\mathbb{T}_n^{\geq 0} = \{ P \in \mathrm{Pol}\mathbb{T}_n \mid P(\mathbb{T}) \subset \mathbb{R}_+ \}.$$

(ii) To each trigonometric polynomial $P = \sum_{i=0}^{n} a_i P_i$, *we associate the symmetric Toeplitz matrix* $T(P) \overset{def.}{=} T_{n+1}(a_0, \ldots, a_n)$ *given by (7), and we put*[10]

$$\mathrm{Pol}\mathbb{T}_n^{\succeq 0} = \{P \in \mathrm{Pol}\mathbb{T}_n \mid T(P) \succeq 0\}.$$

We have ([BW11, Lemma 1.1.6]):

Proposition 21. *Both subsets* $\mathrm{Pol}\mathbb{T}_n^{\geq 0}$ *and* $\mathrm{Pol}\mathbb{T}_n^{\succeq 0}$ *are cones in* $\mathrm{Pol}\mathbb{T}_n$, *dual to each other.*

We can now reformulate both optimization problems (W_n) and (O_n) and their associated dual problems in a conic way.

Definition 22 (Conic versions of the optimization problems)**.** *Let* $n \geq 1$.

• *For* $g \geq 0$, *the generalized Weil optimization problem of order* n *and its dual consist in the following minimizing/maximizing optimization problems: find*

$$\min \left\{ \langle P, P_1 \rangle \;\middle|\; \begin{array}{l} P \in \mathrm{Pol}\mathbb{T}_n^{\succeq 0} \\ \langle P, P_0 \rangle \leq 2g \\ \langle P, P_i - \alpha^{i-1} P_1 \rangle \leq 2\beta_i \; 2 \leq i \leq n \end{array} \right\}$$

and

$$\max \left\{ -\left\langle \begin{pmatrix} y_0 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \begin{pmatrix} \beta_0 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} \right\rangle_{\mathbb{R}^n} \;\middle|\; \begin{array}{l} P_1 + y_0 + \sum_{i=2}^{n} y_i \left(P_i - \alpha^{i-1} P_1\right) \in \mathrm{Pol}\mathbb{T}_n^{\geq 0}, \\ y_0 \geq 0, \; y_i \geq 0, \; 2 \leq i \leq n \end{array} \right\}.$$

• *For* $N \geq 0$, *the Oesterlé optimization problem of order* n *and its dual consist in the following minimizing/maximizing optimization problems: find*

$$\min \left\{ \langle P_0, P \rangle \;\middle|\; \begin{array}{l} P \in \mathrm{Pol}\mathbb{T}_n^{\succeq 0} \\ \langle P, P_i \rangle \leq 2\delta_i(N), \; 1 \leq i \leq n \end{array} \right\}$$

and

$$\max \left\{ -\left\langle \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}, \begin{pmatrix} \delta_1 \\ \vdots \\ \delta_n \end{pmatrix} \right\rangle_{\mathbb{R}^n} \;\middle|\; \begin{array}{l} P_0 + \sum_{i=1}^{n} z_i P_i \in \mathrm{Pol}\mathbb{T}_n^{\geq 0}, \\ z_i \geq 0, \; 1 \leq i \leq n \end{array} \right\}.$$

Note that both primal programs do have a solution. In the Weil program, a polynomial $P = \sum_{i=0}^{n} x_i P_i$ must satisfies $0 \leq x_0 \leq 2g$ and $\left(\begin{smallmatrix} x_0 & x_i \\ x_i & x_0 \end{smallmatrix}\right) \succeq 0$, thus the domain of feasibility of the Weil program is a compact one contained in $[-2g, 2g]^{n+1}$. Anyway, the continuous function $\langle P, P_1 \rangle$ attains its minimum on this domain. The Oesterlé program has a solution because the first coordinate function $P \mapsto \langle P, P_0 \rangle$ to be minimized is bounded below by zero.

[10] Notice the difference between notations $\geq$ and $\succeq$.

3.5.3 Explicit Oesterlé solution for the Oesterlé conic program

Oesterlé has computed an explicit trigonometric polynomial $P \in \mathrm{Pol}\mathbb{T}_n^{\succeq 0}$ satisfying all the constraints of the primal problem with equalities instead of inequalities, i.e. an element of the so-called "strict border", together with a second trigonometric polynomial $Q \in \mathrm{Pol}\mathbb{T}_n^{\geq 0}$ satisfying all the constrains of the dual problem, which is orthogonal to P. More precisely, such trigonometric polynomials P and Q must be of the form:

$$P(z) = x_0 + \sum_{i=1}^{n} \delta_i(N) \left(z^i + \frac{1}{z^i} \right) \in \mathrm{Pol}\mathbb{T}_n^{\succeq 0}$$

$$Q(z) = 1 + \sum_{i=1}^{n} y_i \left(z^i + \frac{1}{z^i} \right) \in \mathrm{Pol}\mathbb{T}_n^{\geq 0}, \qquad \text{and} \qquad y_i \geq 0$$

and they have to be orthogonal. Thanks to Proposition 31, this proves that the polynomial P is a minimizing element for the Oesterlé optimization problem. With the terminology of Definition 32, one can say that the polynomial Q is a certificate for P being a minimizing element of this problem.

Before describing the Oesterlé construction, in the spirit of sections 3.3 and 3.4, let us give an informal vision of what is going on. Let us see the polynomial P inside $\mathbb{R}^{n+1}$. It must be inside the Weil domain $\mathcal{W}_n$, but also on the line defined by the equations $x_i = \delta_i(N)$ for $1 \leq i \leq n$, where $\delta_i(N)$ are given by formula (26). By convexity, the minimizing polynomial for the first coordinate function should be on the border $\partial\mathcal{W}_n$ of $\mathcal{W}_n$. So one can understand the constant coefficient x_0 of the minimizing polynomial P as follows. Having cases $n = 2, 3$ in mind, one can easily convince ourselves that $\mathbb{R}^{n+1} = \bigcup_{x_0 \geq 0} \partial\mathcal{W}_n^{x_0}$ and this union is disjoint. The minimizing polynomial P corresponds to the one having its constant term $x_0 \geq 0$ in such a way that $(x_0, \delta_1(N), \ldots, \delta_n(N)) \in \partial\mathcal{W}_n$. This ends our informal paragraph.

The little bit intricate description of the explicit solution becomes more natural working with the Toeplitz matrix $T(P)$ instead of the polynomial P itself. Indeed, this matrix should satisfies

$$T_{n+1}(x_0, \delta_1(N), \ldots, \delta_n(N)) \succeq 0 \qquad \text{and} \qquad \mathrm{rk}\left(T_{n+1}(x_0, \delta_1(N), \ldots, \delta_n(N))\right) = n,$$

the rank condition coming from the fact that P must be an element of the boundary of $\mathcal{W}_n$. Such a matrix is known to have a very specific structure by Theorem 36 in Appendix A.2): there exist $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{T}$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_+^*$ such that

$$T(P) = \begin{pmatrix} \sum \lambda_i & \sum \lambda_i \varepsilon_i & \cdots & \sum \lambda_i \varepsilon_i^{n-1} & \sum \lambda_i \varepsilon_i^n \\ \sum \lambda_i \varepsilon_i & \ddots & \ddots & & \sum \lambda_i \varepsilon_i^{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \sum \lambda_i \varepsilon_i^{n-1} & & \ddots & \ddots & \sum \lambda_i \varepsilon_i \\ \sum \lambda_i \varepsilon_i^n & \sum \lambda_i \varepsilon_i^{n-1} & \cdots & \sum \lambda_i \varepsilon_i & \sum \lambda_i \end{pmatrix}, \tag{27}$$

where all sums are from 1 to n. Instead of computing directly the coefficient x_0, the method of Oesterlé consists in constructing first the ε_i's, then the λ_i's, then the constant coefficient x_0, and last the certificate polynomial Q. This construction works only for $N > 1 + \sqrt{q}^{n+1}$.

A key observation made by Oesterlé is that the special shape of the coefficients $\delta_i(N)$ implies strong conditions on the set of eigenvalues $\varepsilon_1, \dots, \varepsilon_n$.

Lemma 23 (Oesterlé)**.** *If the matrix $T_{n+1}(x_0, \delta_1(N), \dots, \delta_n(N))$ is positive semi definite of rank n, then the eigenvalues $\varepsilon_1, \dots, \varepsilon_n$ are roots of the polynomial*

$$R_0(z) = z^{n+2} + t(z^{n+1} + z) + 1 \in \mathbb{R}[z], \qquad \textit{where} \qquad t = \frac{1 + \sqrt{q}^{n+2} - N}{\sqrt{q}\left(N - 1 - \sqrt{q}^n\right)}. \tag{28}$$

Proof. Since $T_{n+1}(x_0, \delta_1(N) \dots, \delta_n(N))$ is positive semi-definite of rank n, it is the Gram matrix of the family of all iterations of an element by an isometry in a cyclic euclidean space (see section A.2). More precisely, let $(a_0, \dots, a_n) \in \mathbb{R}^{n+1}$ be a non-zero element of the kernel of T_{n+1} and let us consider the finite $\mathbb{R}$-vector space $\mathbb{R}[X]/\langle P\rangle = \bigoplus_{i=0}^{n-1} \mathbb{R}x^i$ where $x = X \bmod P$. Then the identity

$$\mathrm{Gram}(1, x, \dots, x^n) = T_{n+1}(x_0, \delta_1(N) \dots, \delta_n(N))$$

defines a scalar product on $\mathbb{R}[X]/\langle P\rangle$, in such a way that the multiplication by x is an isometry. This isometry has P as minimal polynomial and can be diagonalized over $\mathbb{C}$. Let $\mathcal{R}$ be the set of roots of P. Being the spectrum of an isometry, we have $\mathcal{R} \subset \mathbb{T}$. From elementary linear algebra, we have

$$\mathbb{C}[X]/\langle P\rangle = \bigoplus_{\varepsilon \in \mathcal{R}} \mathbb{C}P_\varepsilon(x) \qquad \text{where} \qquad P_\varepsilon(x) = \prod_{\varepsilon' \in \mathcal{R}\setminus\{\varepsilon\}} \frac{x - \varepsilon'}{\varepsilon - \varepsilon'} = \frac{P(x)}{P'(\varepsilon)(x - \varepsilon)}$$

is the interpolation polynomial taking value 1 on ε, and value 0 on all other $\varepsilon' \in \mathcal{R}$. One also have $xP_\varepsilon(x) = \varepsilon P_\varepsilon(x)$, $P_\varepsilon(x) \perp P_{\varepsilon'}(x)$ for $\varepsilon' \neq \varepsilon$, and with $\sum_{\varepsilon\in\mathcal{R}} P_\varepsilon(x) = 1$.

We now prove that each $\varepsilon \in \mathcal{R}$ is a root of the polynomial R_0. The key point is that the coefficients $\delta_i(N)$ can be written as follows:

$$\delta_i(N) = \frac{1 + q^i - N}{\sqrt{q}^i} = \sqrt{q}^i - (N - 1) \times \frac{1}{\sqrt{q}^i}.$$

Setting $a = \sqrt{q}$ and $b = N - 1$ for simplicity, this means that

$$\langle 1, xQ(x)\rangle = aQ(a) - \frac{b}{a}Q(1/a) \tag{29}$$

for any polynomial Q of degree $\leq n - 1$. Let us compute the square norm λ_ε of each

eigenvector $P_\varepsilon(x)$:

$$\begin{aligned}
\lambda_\varepsilon &= \langle P_\varepsilon(x), P_\varepsilon(x)\rangle = \langle 1, P_\varepsilon(x)\rangle && \text{since } P_\varepsilon(x) \perp 1 - P_\varepsilon(x)\\
&= \frac{1}{\varepsilon}\langle 1, \varepsilon P_\varepsilon(x)\rangle = \frac{1}{\varepsilon}\langle 1, xP_\varepsilon(x)\rangle && \text{since } xP_\varepsilon(x) = \varepsilon P_\varepsilon(x)\\
&= \frac{1}{\varepsilon}\left(aP_\varepsilon(a) - \frac{b}{a}P_\varepsilon(1/a)\right) && \text{by (29)}\\
&= \frac{1}{\varepsilon}\left(\frac{aP(a)}{P'(\varepsilon)(a-\varepsilon)} - \frac{b}{a}\times\frac{P(1/a)}{P'(\varepsilon)(1/a-\varepsilon)}\right)\\
&= \frac{1}{\varepsilon}\left(\frac{aP(a)}{P'(\varepsilon)(a-\varepsilon)} - b\frac{P(a)a^{-(n+1)}}{P'(\varepsilon)(1/a-\varepsilon)}\right) && \text{since } P(1/a) = P(a)a^{-n}\\
&= \frac{P(a)}{\varepsilon P'(\varepsilon)}\times\frac{1 - ba^{-n} + \left(ba^{-(n+1)} - a\right)\varepsilon}{\varepsilon^2 - (a+1/a)\,\varepsilon + 1}.
\end{aligned}$$

In the same way

$$\begin{aligned}
\lambda_{1/\varepsilon} &= \frac{P(a)}{P'(1/\varepsilon)/\varepsilon}\times\frac{1 - ba^{-n} + \left(ba^{-(n+1)} - a\right)/\varepsilon}{\left(\varepsilon^2 - (a+1/a)\,\varepsilon + 1\right)/\varepsilon^2}\\
&= \frac{P(a)}{\varepsilon P'(\varepsilon)}\times\frac{-\varepsilon^{n+1}\left(\left(1 - ba^{-n}\right)\varepsilon + \left(ba^{-(n+1)} - a\right)\right)}{\left(\varepsilon^2 - (a+1/a)\,\varepsilon + 1\right)} \quad \text{since } P'(1/\varepsilon) = -P'(\varepsilon)/\varepsilon^{n-2}.
\end{aligned}$$

To conclude, we take into account the fact that the starting point matrix has real coefficients. Therefore one must have $\lambda_\varepsilon = \lambda_{1/\varepsilon}$ and thus

$$\left(1 - ba^{-n}\right)\varepsilon^{n+2} + \left(ba^{-(n+1)} - a\right)\left(\varepsilon^{n+1} + \varepsilon\right) + 1 - ba^{-n} = 0$$

or

$$\varepsilon^{n+2} + \frac{b - a^{n+2}}{a\left(a^n - b\right)}\left(\varepsilon^{n+1} + \varepsilon\right) + 1 = 0.$$

The result follows. □

The Lemma 23 is a key step of the explicit construction of the solution of the Oesterlé optimization problem. The complete construction is given in the theorem below. As far as we know, no complete proof of the validity of this construction has been published so far. Oesterlé himself, for sure, has never published his result and we never have in hand a copy of his original notes. The two published sources that we know are the Serre's Harvard course notes titled "rational points on curves over finite fields" [Ser] and a survey of Hansen [Han95], but both references only contain partial proof. In fact, we know only one (unpublished) source containing a complete proof: the chapters 4 and 5 of the thesis of A. Edouard (whose advisor was G. Lachaud) are devoted to a twenty pages long complete proof of the Oesterlé bound. Since we do not succeed in substantially simplifying this proof, we refer to this thesis for the two skipped tedious calculations below.

Theorem 24 (The Oesterlé solution)**.** *Let $n \geq 1$, $N > 1 + \sqrt{q}^{n+1}$, and let $R_0 \in \mathbb{R}[z]$ be the polynomial defined in Lemma 23. It has all its roots in the unit circle $\mathbb{T}$; we denote by $e^{i\varphi_0}$ the root of R_0 having the smallest positive argument, by $Q_0 \in \mathbb{R}[z]$ the quotient of the polynomial R_0 by the quadratic polynomial $\left(z - e^{i\varphi_0}\right)\left(z - e^{-i\varphi_0}\right)$, and by $y_0, \ldots, y_n \in \mathbb{R}$ the coefficients of the trigonometric polynomial $Q_0(z)Q_0(1/z) = y_0 + \sum_{i=1}^{n} y_i \left(z^i + \frac{1}{z^i}\right)$. Then the trigonometric polynomials*

$$P(z) = 2\left(1 + \frac{N\left(\sqrt{q}\cos(\varphi_0) - 1\right)}{q - 2\sqrt{q}\cos(\varphi_0) + 1}\right) + \sum_{i=1}^{n} \frac{1 + q^i - N}{\sqrt{q}^i}\left(z^i + \frac{1}{z^i}\right) \tag{30}$$

$$Q(z) = 1 + \frac{y_1}{y_0}\left(z + \frac{1}{z}\right) + \cdots + \frac{y_n}{y_0}\left(z^n + \frac{1}{z^n}\right) \tag{31}$$

are such that:

(i) the polynomial P is in $\mathrm{Pol}\mathbb{T}_n^{\succeq 0}$, is a feasible solution for the Oesterlé conic program, and $T(P)$ is of rank n;

(ii) the polynomial Q is in $\mathrm{Pol}\mathbb{T}_n^{\succeq 0}$ and is a feasible solution for the Oesterlé dual conic program;

(iii) the polynomials P and Q are orthogonal.

Proof with two skipped tedious calculations — We give the main steps of the proof and skip the most tedious computations with trigonometric polynomials.

• Proving the fact that if $N \geq 1 + \sqrt{q}^{n+1}$, then the polynomial R_0 has all its roots in the unit circle $\mathbb{T}$ is a first course calculus exercise. The elements $e^{\pm i\varphi_0} \in \mathbb{T}$ are the two roots of R_0 having the smallest argument in absolute value; we denote by $\varepsilon_j = e^{i\varphi_j}$, $1 \leq j \leq n$, the others. Note that if n is odd then -1 is one these ε_j's.

• To prove that this choice of the ε_i's is the good one, it is worth to notice that taking into account the matrix equality (27), the scalars $\lambda_1, \ldots, \lambda_n$ can be uniquely expressed in terms of the ε_i's and the $\delta_i(N)$'s. Indeed equality (27) leads to the following invertible linear system

$$\begin{pmatrix} \varepsilon_1 & \cdots & \varepsilon_1^n \\ \vdots & & \vdots \\ \varepsilon_n & \cdots & \varepsilon_n^n \end{pmatrix} \times \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \delta_1(N) \\ \vdots \\ \delta_n(N) \end{pmatrix}$$

It remains to prove that such λ_i's are all positive. It can be done by explicitly compute them. A (skipped) tedious calculation leads to

$$\lambda_i = \frac{N\sin(\varphi_i)}{\sin\left((n+1)\varphi_i\right) + (n+1)\sin(\varphi_i)}\left(\frac{q-1}{q - 2\sqrt{q}\cos(\varphi_0) + 1} - \frac{q-1}{q - 2\sqrt{q}\cos(\varphi_i) + 1}\right)$$

if $\varepsilon_i \neq -1$, or

$$\lambda_i = \frac{N(1-t)}{(n+2) - nt}\left(\frac{q-1}{q - 2\sqrt{q}\cos(\varphi_0) + 1} - \frac{q-1}{q - 2\sqrt{q}\cos(\pi) + 1}\right)$$

if $\varepsilon_i = -1$. In any cases, one has $\lambda_i > 0$, since the function $\varphi \mapsto \sin(n\varphi) + n\sin(\varphi)$ is positive for every $n \in \mathbb{N}^*$ and every $\varphi \in]0, \pi[$ (easy first course calculus exercise). This shows that $T(P) \succeq 0$, that $\mathrm{rk}(T(P)) = n$ and that P is a feasible solution for the Oesterlé conic program.

• The computation of the λ_i also permits to give the value of the coefficient x_0 since $x_0 = \sum_{i=1}^{n} \lambda_i$.

• By construction, $Q \in \mathrm{Pol}\mathbb{T}_n^{\geq 0}$ and $\langle P, Q \rangle = 0$. The only thing that remains to be proved is that Q is a feasible solution for the Oesterlé dual conic program. For this, it suffices to show that the coefficients y_i are all positive. This can be done by explicitly computing the coefficients of the trigonometric polynomial Q. A (skipped) tedious calculation leads to:

$$\frac{y_k}{y_0} = \frac{\sum_{j=0}^{n-k} \cos\left(\left(\frac{n}{2} - (j+k)\right)\varphi_0\right) \cos\left(\left(\frac{n}{2} - j\right)\varphi_0\right)}{\sum_{j=0}^{n} \cos^2\left(\left(\frac{n}{2} - j\right)\varphi_0\right)}$$

and the positiveness of this coefficient comes from the fact that $0 < \varphi_0 < \frac{\pi}{n+1}$. □

Going back to the number of points, using the preceding theorem together with Proposition 31, we recover the well known Oesterlé bounds.

Theorem 25 (Oesterlé bounds)**.** *Let $n \geq 1$, and $N \geq 1 + \sqrt{q}^{n+1}$. The minimizing function of the Oesterlé optimization problem (O_n) is given by the function*

$$\mathbf{g}_n^\star : \left[1 + \sqrt{q}^{n+1}, +\infty\right[\longrightarrow [g_n, +\infty[$$

defined by

$$\mathbf{g}_n^\star(N) = 1 + \Re\left(\frac{N}{\sqrt{q}e^{i\varphi_0} - 1}\right) = 1 + \frac{N\left(\sqrt{q}\cos(\varphi_0) - 1\right)}{q - 2\sqrt{q}\cos(\varphi_0) + 1}$$

where φ_0, depending on n and N, is defined as in Theorem 24. Moreover, the value g_n is given by:

$$g_n = \mathbf{g}_n^\star\left(1 + \sqrt{q}^{n+1}\right) = \frac{\left(\sqrt{q}^{n+1} - 1\right)\sqrt{q}\cos\left(\frac{\pi}{n+1}\right) + q - \sqrt{q}^{n+1}}{q - 2\sqrt{q}\cos\left(\frac{\pi}{n+1}\right) + 1} \tag{32}$$

$$= \sqrt{q}^{n+1} \sum_{k=1}^{n} \frac{1}{\sqrt{q}^k} \cos\left(\frac{k\pi}{n+1}\right). \tag{33}$$

Strictly speaking, the construction of Oesterl'e works for $N > 1 + \sqrt{q}^{n+1}$ but it can be easily continuously extended. The expression of the value $g_n = \mathbf{g}_n^\star\left(1 + \sqrt{q}^{n+1}\right)$ comes from the fact that, at the order n, the polynomial R_0 is very simple:

$$\begin{array}{lll} N = 1 + \sqrt{q}^{n+1} & \Longrightarrow & R_0(z) = \left(z^{n+1} + 1\right)(z+1) \quad \text{by Lemma 23} \\ & \Longrightarrow & \varphi_0 = \dfrac{\pi}{n+1} \quad \text{by Theorem 24,} \end{array}$$

and the given value of g_n follows.

There is another simple value of the function $\mathbf{g}_n^\star$ coming from another simple polynomial R_0:

$$\begin{aligned} N = 1+\sqrt{q}^{n+2} \quad &\Longrightarrow \quad R_0(z) = z^{n+2}+1 && \text{by Lemma 23} \\ &\Longrightarrow \quad \varphi_0 = \frac{\pi}{n+2} && \text{by Theorem 24} \\ &\Longrightarrow \quad \mathbf{g}_n^\star\left(1+\sqrt{q}^{n+2}\right) = g_{n+1}. \end{aligned}$$

We deduce the the two functions $\mathbf{g}_n^\star$ and $\mathbf{g}_{n+1}^\star$ coincide at $1+\sqrt{q}^{n+2}$ with:

$$g_{n+1} = \mathbf{g}_n^\star\left(1+\sqrt{q}^{n+2}\right) = \mathbf{g}_{n+1}^\star\left(1+\sqrt{q}^{n+2}\right). \tag{34}$$

3.5.4 Proof of the main Theorem 14

The strategy to prove our main Theorem is to show that the minimizing polynomial constructed by Oesterlé to solve his optimization program is also a minimizing polynomial for the Weil optimization problem.

Proposition 26. *Let $n \geq 1$, $N > 1+\sqrt{q}^{n+1}$, and let P, Q be the trigonometric polynomials given in Theorem 24. Then the minimum of the Weil optimization problem of order n associated to the genus $\mathbf{g}_n^\star(N)$ is attained at P and the functions*

$$\mathbf{N}_n^\star : [g_n, +\infty[\longrightarrow \left[1+\sqrt{q}^{n+1}, +\infty\right[\quad \text{and} \quad \mathbf{g}_n^\star : \left[1+\sqrt{q}^{n+1}, +\infty\right[\longrightarrow [g_n, +\infty[$$

are strictly increasing inverse functions, where $\mathbf{N}_n^\star$ is defined by equation (25).

Proof. By construction, one has

$$P = 2\mathbf{g}_n^\star(N) + \sum_{i=1}^{n} \delta_i(N) P_i, \qquad \begin{array}{l} P \in \mathrm{Pol}\mathbb{T}_n^{\succeq 0}, \\ \langle P, P_0\rangle = 2\mathbf{g}_n^\star(N), \\ \langle P, P_i\rangle = 2\delta_i(N),\ 1 \leq i \leq n. \end{array}$$

For $i \geq 2$, we deduce that

$$\left\langle P, P_i - \alpha^{i-1} P_1 \right\rangle = \langle P, P_i\rangle - \alpha^{i-1}\langle P, P_1\rangle = 2\delta_i(N) - \alpha^{i-1} 2\delta_1(N) = 2\beta_i.$$

Therefore, P is an element of the "strict border" of the domain corresponding to the Weil program of order n associated to the genus $\mathbf{g}_n^\star(N)$.

As for the polynomial Q, it can be rewritten as follows:

$$Q = 1 + \sum_{i=1}^{n} c_i P_i = 1 + \left(\sum_{i=1}^{n} \alpha^{i-1} c_i\right) P_1 + \sum_{i=2}^{n} c_i \left(P_i - \alpha^{i-1} P_1\right).$$

Put $c = \sum_{i=1}^{n} \alpha^{i-1} c_i$, then the polynomial $\frac{1}{c}Q = P_1 + \frac{1}{c} + \sum_{i=2}^{n} \frac{c_i}{c}\left(P_i - \alpha^{i-1} P_1\right)$ belongs to $\mathrm{Pol}\mathbb{T}_n^{\geq 0}$ and has non negative coefficients. Since $\left\langle P, \frac{1}{c}Q\right\rangle = 0$, the polynomial $\frac{1}{c}Q$ can

be used to certify that the polynomial P is a minimizing element for the Weil program (see Proposition 31). We deduce that $\mathbf{x}^\star_{\mathbf{1},n}(\mathbf{g}^\star_n(N)) = \langle P, P_1\rangle = \delta_1(N)$, which means that $\mathbf{N}^\star_n(\mathbf{g}^\star_n(N)) = N$.

Now, the functions $\mathbf{g}^\star_n$ and $\mathbf{N}^\star_n$ have to be increasing from their definition. Being inverse to each other, they are in fact strictly increasing and the proposition follows. □

We are now ready to prove the main Theorem 14.

Proof of Theorem 14, item (*i*) — We consider the sequence g_n given for $n \geq 1$ by Theorem 25. First note that since $g_n = \mathbf{g}^\star_n\left(1+\sqrt{q}^{n+1}\right)$ and $g_{n+1} = \mathbf{g}^\star_n\left(1+\sqrt{q}^{n+2}\right)$ by formula (34), we can deduce from Proposition 26 that the sequence $(g_n)_{n\geq 1}$ is strictly increasing. We also consider the sequence of functions $\mathbf{N}^\star_n(g)$ given by formula (25). The functions $\mathbf{N}^\star_n(g)$ are strictly increasing and defined for $g \geq g_n$ by Theorem 25 for any $n \geq 1$.

Thanks to Proposition 26, the minimizing element for the n-th Weil optimization problem for g is attained at the polynomial $P = 2g+\sum_{i=1}^n \delta_i(N)P_i \in \mathrm{Pol}\mathbb{T}^{\succeq 0}_n$, where $N \geq 1+\sqrt{q}^{n+1}$ is the value such that $g = \mathbf{g}^\star_n(N)$. Going back to $\mathbb{R}^{n+1}$, the minimum is attained at the point $(2g, \delta_1(N), \ldots, \delta_n(N)) \in \mathcal{W}^g_n$. More precisely, this point lies on the border of $\mathcal{W}^g_n$, since by Theorem 24, the matrix $T(P)$ given by equation (26) has rank n and size $n+1$. Last, we observe that $\delta_i(N) = \frac{1}{\sqrt{q}^{i-1}}\delta_1(N) + \beta_i$ from equation (24) which means that the point $(2g, \delta_1(N), \ldots, \delta_n(N))$ is also an element of the Ihara line $\mathcal{I}^g_n$. Thus the "strict border" for the Oesterlé optimization problem corresponds to the Ihara line for the Weil optimization problem. Hence $\mathbf{x}^\star_{\mathbf{1},n}(g) = \delta_1(N)$ is the smallest x_1-coordinate of the points of $\mathcal{W}^g_n \cap \mathcal{I}^g_n$. □

Proof of Theorem 14, item (*ii*) — Applying both functions $\mathbf{N}^\star_n$ and $\mathbf{N}^\star_{n+1}$ to equality (34) and taking into account Proposition 26 leads to the first equalities of item (*ii*)

$$\mathbf{N}^\star_n(g_n) = 1+\sqrt{q}^{n+1} \quad \text{and} \quad \mathbf{N}^\star_n(g_{n+1}) = \mathbf{N}^\star_{n+1}(g_{n+1}).$$

The application $\pi : \mathcal{W}^g_{n+1} \to \mathcal{W}^g_n$ defined by $(x_0, \ldots, x_{n+1}) \mapsto (x_0, \ldots, x_n)$ is surjective. This implies that $\mathbf{N}^\star_{n+1}(g) \leq \mathbf{N}^\star_n(g)$. Suppose that equality holds and let us denote by N their common value. Then minimizing tuples/polynomials for the n-th and $(n+1)$-th order Weil problems are respectively

$$P_n = (2g, \delta_1(N), \ldots, \delta_n(N)) \in \mathcal{W}^g_n \quad \text{and} \quad P_{n+1} = (2g, \delta_1(N), \ldots, \delta_{n+1}(N)) \in \mathcal{W}^g_{n+1}$$

with $\mathrm{rk}(T(P_n)) = n$ and $\mathrm{rk}(T(P_{n+1})) = n+1$ (cf. Theorem 24). But the Toeplitz matrix $T(P_n)$ being a sub-matrix of the Toeplitz matrix $T(P_{n+1})$, by Lemma 33, necessarily $\mathrm{rk}(T(P_{n+1})) = \mathrm{rk}(T(P_n))$. This is thus contradictory and therefore equality does not hold. □

Proof of Theorem 14, item (*iii*) — Let $n \geq 2$, $g > g_n$ and put $\mathbf{x}^\star_{\mathbf{i},n} = \alpha^{n-1}\mathbf{x}^\star_{\mathbf{1},n}(g) + \beta_n$ for $i \geq 1$. Then the point minimizing the n-th Weil optimization problem is

$$\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \ldots, \mathbf{x}^\star_{\mathbf{n},n}(g)\right) \in \mathcal{W}^g_n \cap \mathcal{I}^g_n$$

It even lies inside the border of $\mathcal{W}_n^g$ and thus is such that

$$w_n^-\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) \leq \mathbf{x}^\star_{\mathbf{n},n}(g) \leq w_n^+\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) \tag{35}$$

and

$$\begin{aligned} w_n^+\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) - w_n^-\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) \\ = 2 \cdot \frac{\mathrm{Det}\left(T_n\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right)\right)}{\mathrm{Det}\left(T_{n-1}\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-2},n}(g)\right)\right)} \end{aligned} \tag{36}$$

Since $\mathbf{x}^\star_{\mathbf{1},n}(g_n) = \mathbf{x}^\star_{\mathbf{1},n-1}(g_n)$, one has $\mathbf{x}^\star_{\mathbf{i},n-1}(g_n) = \mathbf{x}^\star_{\mathbf{i},n}(g_n)$ for each $1 \leq i \leq n-1$ and the point

$$\left(2g_n, \mathbf{x}^\star_{\mathbf{1},n}(g_n), \dots, \mathbf{x}^\star_{\mathbf{n},n-1}(g_n)\right)$$

is the minimizing element of the $(n-1)$-th Weil optimization problem. Therefore

$$\begin{aligned} \mathrm{Det}\left(T_n\left(2g_n, \mathbf{x}^\star_{\mathbf{1},n}(g_n), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g_n)\right)\right) = 0 \\ \mathrm{Det}\left(T_{n-1}\left(2g_n, \mathbf{x}^\star_{\mathbf{1},n}(g_n), \dots, \mathbf{x}^\star_{\mathbf{n-2},n}(g_n)\right)\right) \neq 0 \end{aligned}$$

This permits us to let g tends to g_n in (36) and by (35), we obtain

$$\mathbf{x}^\star_{\mathbf{n},n}(g) = w_n^-\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) = w_n^+\left(2g, \mathbf{x}^\star_{\mathbf{1},n}(g), \dots, \mathbf{x}^\star_{\mathbf{n-1},n}(g)\right) \tag{37}$$

so that this item is proved. □

Proof of Theorem 14, item (*iv*) — Since the minimal value $\mathbf{x}^\star_{\mathbf{1},n}(g)$ is reached on the line segment $\mathcal{W}_n^g \cap \mathcal{I}_n^g$ by item (*i*), it is also reached on any subset of the Weil domain $\mathcal{W}_n^g$ containing this segment. This is the case of the Weil domain cut-out by the two dimensional plane $(x_1, \ell_2(x_1), \cdots, \ell_{n-1}(x_1), x_n)$ parallel to the-x_n-axis over the $(n-1)$-th Ihara line $\mathcal{I}_{n-1}^g$. By Proposition 9, this means that $\mathbf{x}^\star_{\mathbf{1},n}(g)$ is the minimum of the set

$$\left\{ x_1 \mid \begin{array}{c} (x_1, \cdots, x_{n-1}) \in \mathcal{W}_{n-1}^g; \\ x_i = \ell_i(x_1), 2 \leq i \leq n-1; \\ x_n \leq \ell_n(x_1); \\ w_n^-(x_1, \cdots, x_{n-1}) \leq x_n \leq w_n^+(x_1, \cdots, x_{n-1}) \end{array} \right\}.$$

This can also be written as

$$\mathbf{x}^\star_{\mathbf{1},n}(g) = \min\{x_1 \mid \mathbf{x}^\star_{\mathbf{1},n-1}(g) \leq x_1 \leq b_{n-1}(g), x_n \leq \ell_n(x_1) \text{ and } f_n(x_1) \leq x_n \leq g_n(x_1)\} \tag{38}$$

for the value $b_{n-1}(g)$ such that the $(n-1)$-th Ihara line cuts the $(n-1)$-th affine Weil domain on the x_1 parameter set $[\mathbf{x}^\star_{\mathbf{1},n-1}(g), b_{n-1}(g)]$, and where

$$\begin{cases} f_n(x_1) &= w_n^-(x_1, \ell_2(x_1), \cdots, \ell_{n-1}(x_1)), \\ g_n(x_1) &= w_n^+(x_1, \ell_2(x_1), \cdots, \ell_{n-1}(x_1)). \end{cases}$$

Since w_n^- is convex by item (*iii*) of Proposition 9 and the ℓ_i-th are affine, the univariate function f_n is convex; in the same way g_n is concave. Now by item (*ii*), we have $\mathbf{x}^\star_{\mathbf{1},n}(g) > \mathbf{x}^\star_{\mathbf{1},n-1}(g)$ since g is assumed to be greater than g_n. It follows from (38) by elementary convexity task for univariate functions that the minimum is reached at the point satisfying $x_n = \ell_n(x_1) = f_n(x_1)$, which concludes the proof of the theorem. □

4 Asymptotic bounds

In this section, we show that our point of view also leads to the known general asymptotic bounds. Let $(X_k)_{k\geq 1}$ be an *asymptotically exact* sequence of absolutely irreducible smooth projective curves defined over $\mathbb{F}_q$, of genus $g(X_k)$. This means that the genus sequence $(g(X_k))_{k\geq 1}$ tends to infinity and that for any $r \geq 1$, the limit ℓ_r of the *relative*[11] number of points of exact degree r sequences do exist:

$$\ell_r = \lim_{k\to+\infty} \frac{\frac{1}{r}\sharp\left\{P \in X_k(\overline{\mathbb{F}}_q) \mid \deg_{\mathbb{F}_q}(P) = r\right\}}{g(X_k)} \in \mathbb{R}^+, \qquad \forall r \geq 1. \tag{39}$$

Last, we introduce after Tsfasman and Vlăduţ the *defect* δ (see [TV02]) of the asymptotically exact sequence

$$\delta = 1 - \sum_{r=1}^{+\infty} \frac{r\ell_r}{\sqrt{q^r}-1}. \tag{40}$$

The known result is the following Tsfasman theorem, stating that the defect is always non-negative.

Theorem 27 (Tsfasman [Tsf92])**.** *Let $(X_k)_{k\geq 1}$ be a asymptotically exact sequence of absolutely irreducible smooth projective curves over $\mathbb{F}_q$. Then*

$$\sum_{r=1}^{\infty} \frac{r\ell_r}{\sqrt{q^r}-1} \leq 1,$$

where the sequence $(\ell_r)_{r\geq 1}$ is defined as in (39).

As in section 1, one can associate to each curve X_k an euclidean space $(\mathcal{E}(X_k), \langle\cdot,\cdot\rangle_{X_k})$ with norm $\|\cdot\|_{X_k}$ and a subspace $\mathcal{F}(X_k)$ generated by the projections $\gamma^i_{X_k}$ of the iterations of the Frobenius morphism. The quantity to be studied being the ratio $\frac{\sharp X_k(\mathbb{F}_q)}{g(X_k)}$, it is convenient to change the normalization, putting

$$\eta^i_{X_k} = \frac{\gamma^i_{X_k}}{\sqrt{g(X_k)}}. \tag{41}$$

Then $\|\eta^i_{X_k}\|_{X_k} = 2$ and for any $n \geq 1$,

$$\mathrm{Gram}(\eta^0_{X_k}, \ldots, \eta^n_{X_k}) = \begin{pmatrix} 2 & y_1 & \cdots & y_{n-1} & y_n \\ y_1 & \ddots & \ddots & & y_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ y_{n-1} & & \ddots & \ddots & y_1 \\ y_n & y_{n-1} & \cdots & y_1 & 2 \end{pmatrix} \quad \text{with} \quad y_i = \frac{1+q^i-\sharp X_k(\mathbb{F}_{q^i})}{g(X_k)\sqrt{q}^i}. \tag{42}$$

[11] Relative to the genus.

Note that omitting reference to X_k, the x_i's defined in (4) and the y_i's are related by $y_i = \frac{x_i}{g}$.

Just as for the finite order case, one can first wonder about the consequences of the geometrico-euclidean constraint alone, second about both geometrico-euclidean and arithmetic constraints consequences. The bound derived in this last way can be considered as the *Weil bound of infinite order*.

4.1 Weil domain and asymptotic (Tsfasman bound)

Let us first look at the geometrico-euclidean constraint alone. Just expressing non-negativity of the norm of a well-chosen vector in the euclidean spaces $\mathcal{E}(X_k)$ yields to an interpretation for the defect of the sequence. Note that Tsfasman bound follows just pointing out that a norm is non-negative.

Theorem 28. *Let $(X_k)_{k\geq 1}$ be an asymptotically exact sequence of absolutely irreducible smooth projective curves over $\mathbb{F}_q$. Then its* defect *δ, defined as in (40) satisfies*

$$\delta = \lim_{m\to+\infty} \lim_{k\to+\infty} \frac{\left\|\eta^0_{X_k} + \eta^1_{X_k} + \cdots + \eta^{m-1}_{X_k}\right\|^2_{X_k}}{2m}.$$

Note that this can also be written as

$$\delta = \lim_{m\to+\infty} \lim_{k\to+\infty} \frac{\left\|\eta^0_{X_k} + \eta^1_{X_k} + \cdots + \eta^{m-1}_{X_k}\right\|^2_{X_k}}{\left\|\eta^0_{X_k}\right\|^2_{X_k} + \left\|\eta^1_{X_k}\right\|^2_{X_k} + \cdots + \left\|\eta^{m-1}_{X_k}\right\|^2_{X_k}}.$$

Proof. Inside the euclidean space $\mathcal{E}(X_k)$, one can compute the norm:

$$\begin{aligned}
\frac{1}{2m}\left\|\sum_{i=0}^{m-1}\eta^i_{X_k}\right\|^2_{X_k} &= \frac{1}{2m}\begin{pmatrix}1 & \cdots & 1\end{pmatrix} \times \mathrm{Gram}\left(\eta^0_{X_k},\ldots,\eta^{m-1}_{X_k}\right) \times \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} \\
&= \frac{1}{m}\left[m + \sum_{i=1}^{m-1}(m-i)y_i\right] \\
&= 1 + \frac{1}{m}\sum_{i=1}^{m-1}(m-i)\frac{(q^i+1) - \sharp X_k(\mathbb{F}_{q^i})}{g(X_k)q^{\frac{i}{2}}} \\
&= 1 + \frac{1}{g(X_k)}\sum_{i=1}^{m-1}(1-\frac{i}{m})\left(q^{\frac{i}{2}} + q^{-\frac{i}{2}}\right) \\
&\quad - \sum_{i=1}^{m-1}\left((1-\frac{i}{m})\sum_{r|i}\frac{1}{q^{\frac{i}{2}}} \times \frac{\sharp\left\{P \in X_k(\overline{\mathbb{F}}_q) \mid \deg_{\mathbb{F}_q}(P) = r\right\}}{g(X_k)}\right).
\end{aligned}$$

Letting k growing to $+\infty$ leads, for any $m \geq 1$, to

$$\lim_{k\to+\infty} \frac{1}{2m} \left\| \sum_{i=0}^{m-1} \eta^i_{X_k} \right\|^2_{X_k} = 1 - \sum_{r=1}^{m-1} \left(\sum_{s=1}^{\lfloor \frac{m-1}{r} \rfloor} \left(1 - \frac{rs}{m}\right) \frac{1}{q^{\frac{rs}{2}}} \right) r\ell_r. \tag{43}$$

To conclude, for any $r, m \geq 1$,we remark that

$$\frac{1}{q^{\frac{r}{2}}-1} - \sum_{s=1}^{\lfloor \frac{m-1}{r} \rfloor} \left(1 - \frac{rs}{m}\right) \frac{1}{q^{\frac{rs}{2}}} = \sum_{s=1}^{+\infty} \frac{1}{q^{\frac{rs}{2}}} - \sum_{s=1}^{\lfloor \frac{m-1}{r} \rfloor} \left(1 - \frac{rs}{m}\right) \frac{1}{q^{\frac{rs}{2}}} = \sum_{s=\frac{m-1}{r}}^{+\infty} \frac{1}{q^{\frac{rs}{2}}} + \frac{1}{m} \sum_{s=1}^{\lfloor \frac{m-1}{r} \rfloor} \frac{rs}{q^{\frac{rs}{2}}}.$$

Being the remainder of a convergent series, the first term of the right hand side goes to zero when m grows to infinity. The second term also goes to zero by Cesaro Theorem. Therefore

$$\lim_{m\to+\infty} \sum_{s=1}^{\lfloor \frac{m-1}{r} \rfloor} \left(1 - \frac{rs}{m}\right) \frac{1}{q^{\frac{rs}{2}}} = \frac{1}{q^{\frac{r}{2}}-1},$$

and the Theorem follows letting m tends to $+\infty$ in (43). □

4.2 Generalized Weil bound of infinite order (Drinfeld-Vlăduţ bound)

Let us now take also into account the arithmetic constraints. As a result of the normalization (41) $\eta^i = \frac{\gamma^i}{\sqrt{g}}$ at the beginning of this section, the picture changes a little bit compared to what was going on in section 3. Using the γ^i's, the affine Weil domain $\mathcal{W}_n^g$ in the $(x_1, \ldots, x_n)$ system of coordinates depends on g, while the Ihara constraints do not. Normalizing by $\sqrt{g}$ turns things around. The Weil domain $\mathcal{W}_n^g$ in the $(y_1, \ldots, y_n)$ system of coordinates, with $y_i = \frac{x_i}{g}$ by (42), does not depends on g anymore and is a fixed bounded convex domain, which looks like the affine Weil domain $\mathcal{W}_n^1$ in the $(x_1, \ldots, x_n)$ system of coordinates. The Ihara constraints in the $(y_1, \ldots, y_n)$ system of coordinates become

$$y_i \leq \alpha^{i-1} y_1 + \frac{\beta_i}{2g} \qquad \forall 2 \leq i \leq n, \tag{44}$$

and the Ihara line becomes

$$\mathcal{J}_n^g = \left\{ (y_1, \ldots, y_n) \in \mathbb{R}^n \mid y_i = \alpha^{i-1} y_1 + \frac{\beta_i}{2g}, \ \ 2 \leq i \leq n \right\}.$$

With these notations, our main Theorem 14 can be reformulated in its $\mathbf{y}$-form: for any $n \geq 1$ and for $g \geq g_n$, a curve X of genus g has a number of rational points satisfying

$$\frac{\sharp X(\mathbb{F}_q)}{g} - \frac{q+1}{g} \leq -2\sqrt{q} \times \mathbf{y}_n^\star(g) \tag{45}$$

where $\mathbf{y}_n^\star(g)$ denotes the y_1-coordinate the intersection point of the convex domain $\mathcal{W}_n^1$ with the Ihara line $\mathcal{J}_n^g$ having the smallest y_1 coordinate.

The goal of this section is to investigate the asymptotic behaviour of the bound (45) when both n and the genus g of X grow to infinity. Roughly speaking, the situation is very nice. For $g = \infty$, the Ihara affine line given by (44) becomes the vectorial line $\mathcal{J}_n^\infty$ whose equations are simply $y_i = \alpha^{i-1} y_1$, for $2 \leq i \leq n$. This line intersects the bounded convex Weil domain at a segment whose "left point" for the y_1-coordinate's order has y_1 coordinate $\mathbf{y}_n^\star(\infty)$ and (45) becomes

$$\lim_{g\to\infty} \frac{\sharp X(\mathbb{F}_q)}{g} \leq -2\sqrt{q} \times \mathbf{y}_n^\star(\infty). \tag{46}$$

The limit $\mathbf{y}_n^\star(\infty)$ being the largest negative solution of some explicit determinantal equation, $\mathbf{y}_n^\star(\infty)$ turns to be related to the spectral radius of some very simple non-negative[12] matrix of size n.

Let us turn this idea into a complete proof.

Theorem 29. *We have*

$$\lim_{n\to\infty} \limsup_{g\geq g_n, g\to\infty} \frac{\mathbf{N}_n^\star(g)}{g} = \sqrt{q} - 1. \tag{47}$$

This means of course that the infinite order Weil bound is exactly Drinfeld-Vlăduţ Theorem [VD83] stating that $A(q) \leq \sqrt{q} - 1$.

Proof. Let us begin by writing down Theorem 14 for some given order $n \geq 1$ using the new normalization (41). For any $g \geq g_n$, the intersection of the Weil domain with the Ihara line $\mathcal{J}_n^g$ is a segment whose left end for the y_1-coordinate order has a y_1 coordinate $\mathbf{y}_n^\star(g)$, and we have

$$\frac{\mathbf{N}_n^\star(g)}{g} - \frac{q+1}{g} = -2\sqrt{q} \times \mathbf{y}_n^\star(g). \tag{48}$$

Still by Theorem 14 and by formulas (9) and (7), $\mathbf{y}_n^\star(g)$ is the largest non positive root of the polynomial

$$D_{n,g}(Y) = \mathrm{Det}\left(T_{n+1}\left(1, Y, \alpha Y + \frac{\beta_2}{2g}, \ldots, \alpha^{n-1} Y + \frac{\beta_n}{2g}\right)\right).$$

The family $(D_{n,g}(Y))_{g\geq g_n}$ of polynomials of degree $\leq n$ converges when g goes to infinity to the polynomial $D_{n,\infty}$ defined by

$$D_{n,\infty}(Y) = \mathrm{Det}\left(T_{n+1}\left(1, Y, \alpha Y, \ldots, \alpha^{n-1} Y\right)\right)$$

Since $\mathbf{y}_n^\star(g) \in [-2, 2]$ for any $n, g \geq g_n$, one can assume by compacity that $(\mathbf{y}_n^\star(g))_{g\geq g_n}$ converges, say to $\mathbf{y}_n^\star(\infty)$. Then $D_{n,\infty}(\mathbf{y}_n^\star(\infty)) = 0$ and $\mathbf{y}_{n,\infty}^\star$ is the non-positive y_1-coordinate of the intersection point of the Ihara line $\mathcal{J}_n^\infty$ with the Weil domain. Since the origin of the space $\mathbb{R}^n$ is a common element of the Weil domain and of $\mathcal{J}_n^\infty$, one must

[12] In the sense that its entries are non-negative.

have $\mathbf{y}_n^\star(\infty) \leq 0$, and $\mathbf{y}_n^\star(\infty)$ is the greatest negative root of the polynomial $D_{n,\infty}(Y)$. Letting g going to infinity, we deduce from (48) that

$$\forall n \geq 1, \qquad \limsup_{g\to\infty} \frac{\mathbf{N}_n^\star(g)}{g} = -2\sqrt{q} \times \mathbf{y}_n^\star(\infty). \tag{49}$$

We are then reduced to prove that $\lim_{n\to+\infty} \mathbf{y}_n^\star(\infty) = \frac{1-\sqrt{q}}{2\sqrt{q}}$. To this end, we relate this limit to the asymptotic spectral radius of some specific Toeplitz matrix. One has

$$\begin{aligned} T_{n+1}(1, Y, \alpha Y, \ldots, \alpha^{n-1}Y) &= I_{n+1} + Y T_{n+1}(0, 1, \ldots, \alpha^{n-1}) \\ &= I_{n+1} + Y \times \frac{1}{\alpha}\left[T_{n+1}(1, \alpha, \ldots, \alpha^n) - I_{n+1}\right] \\ &= -\frac{Y}{\alpha}\left[\left(\frac{Y-\alpha}{Y}\right) I_{n+1} - T_{n+1}(1, \alpha, \ldots, \alpha^n)\right]. \end{aligned}$$

Therefore the map $\lambda \longmapsto \frac{\lambda-\alpha}{\lambda}$ defines a one-to-one correspondence from the roots of the polynomial $\mathrm{Det}\left(T_{n+1}\left(1, Y, \alpha Y, \ldots, \alpha^{n-1}Y\right)\right)$ to the set of eigenvalues of the matrix $T_{n+1}\left(1, \alpha, \ldots, \alpha^n\right)$. This bijection maps the largest negative root $\mathbf{y}_n^\star(\infty)$ to the largest non negative real eigenvalue. Since the matrix $T_{n+1}\left(1, \alpha, \ldots, \alpha^n\right)$ is non negative (i.e. all its coefficients are non negative), this eigenvalue turns to be its spectral radius ([HJ90, Chap 8, Th. 8.3.1]) which we denote by $\rho_n(\alpha)$. Thus

$$\frac{\mathbf{y}_n^\star(\infty) - \alpha}{\mathbf{y}_n^\star(\infty)} = \rho_n(\alpha), \qquad \text{that is} \qquad \mathbf{y}_n^\star(\infty) = \frac{\alpha}{1-\rho_n(\alpha)}.$$

But the spectral radius $\rho_n(\alpha)$ is asymptotically known, see Lemma 30 below. This leads to

$$\lim_{n\to+\infty} \mathbf{y}_n^\star(\infty) = \frac{\alpha}{1-\frac{1+\alpha}{1-\alpha}} = \frac{\alpha-1}{2} = \frac{1-\sqrt{q}}{2\sqrt{q}}$$

which completes the proof together with formula (49). □

We would like to thank Hugo Woerdeman for letting us aware of Lemma 30 and for giving us the reference to Nikolski [Nik01, Corollary 4.1.7, p. 246].

Lemma 30. *Let $\alpha \in [0, 1[$ and let $\rho_n(\alpha)$ denote the spectral radius of the symmetric Toeplitz matrix $T_{n+1}(1, \alpha, \ldots, \alpha^n)$. Then $\lim_{n\to+\infty} \rho_n(\alpha) = \frac{1+\alpha}{1-\alpha}$.*

A Appendix

A.1 Conic programming

We recall here some very usual results on conic programming. Most of the times, the optimization problems, such as the description of the dual problem, are presented "with equalities". For our applications, we need to deal with problems with inequalities. There

is a folklore technique to transform a problem with inequalities into another one with equalities. We recall this trick and formulate suited statements for our applications.

Let $(E, \langle \cdot, \cdot \rangle_E)$ be an euclidean space and let $\mathcal{C}$ be a cone inside E. Let $p_0, p_1, \ldots, p_n \in E$ and $\delta_1, \ldots, \delta_n \in \mathbb{R}$. The *primal conic program* (with inequalities) associated to these data is the problem of minimizing the *objective function* $x \mapsto \langle p_0, x \rangle_E$ subject to the convex constraint $x \in \mathcal{C}$ and $\langle p_i, x \rangle_E \leq \delta_i$ for $1 \leq i \leq n$. That is, to find

$$\rho \stackrel{\text{def.}}{=} \min \left\{ \langle p_0, x \rangle_E \;\middle|\; \begin{array}{l} x \in \mathcal{C} \\ \langle x, p_i \rangle_E \leq \delta_i,\ 1 \leq i \leq n \end{array} \right\} \tag{50}$$

An element $x \in E$ is said to be a *feasible solution* of this primal program if it satisfies all the constraints. It is said to be a *strictly feasible solution* if in addition it lies in the interior of the cone $\mathcal{C}$.

Some *dual program* can be associated to this primal program. To this end, one can reformulate the primal conic program with inequalities to another conic program (in a bigger euclidean space) with equalities only as follows. Consider the space $\mathbb{R}^n$ with its canonical basis $(e_1, \ldots, e_n)$ and its usual scalar product $\langle \cdot, \cdot \rangle_{\mathbb{R}^n}$, and let $F = E \times \mathbb{R}^n$ endowed with the scalar product defined by $\langle (x, v), (y, w) \rangle_F = \langle x, y \rangle_E + \langle v, w \rangle_{\mathbb{R}^n}$. The initial cone $\mathcal{C}$ is replaced by a new one $\mathcal{D} = \mathcal{C} \times \mathbb{R}^n_+$, and finding a solution for the initial primal conic program (with inequalities) is equivalent to finding:

$$\rho = \min \left\{ \langle (p_0, 0), (x, d) \rangle_F \;\middle|\; \begin{array}{l} (x, d) \in \mathcal{D} \\ \langle (x, d), (p_i, e_i) \rangle_F = \delta_i,\ 1 \leq i \leq n \end{array} \right\}$$

Note that the added variables play the role of the differences $\delta_i - \langle x, p_i \rangle_E$ whose positiveness are now part of the conic conditions.

We now formulate the *dual program*. It involves the dual cones $\mathcal{C}^*$ and $\mathcal{D}^* = \mathcal{C}^* \times \mathbb{R}^n_+$ (recall that $\mathbb{R}^n_+$ is auto-dual in $\mathbb{R}^n$). Put $\delta = (\delta_1, \ldots, \delta_n) \in \mathbb{R}^n$. The *dual program* is the following maximization problem:

$$\begin{aligned} \rho^* &\stackrel{\text{def.}}{=} \max \left\{ -\langle \delta, y \rangle_{\mathbb{R}^n} \;\middle|\; \begin{array}{l} y = (y_1, \ldots, y_n) \in \mathbb{R}^n \\ (p_0, 0) + \sum_{i=1}^n y_i (p_i, e_i) \in \mathcal{D}^* \end{array} \right\} \\ &= \max \left\{ -\langle \delta, y \rangle_{\mathbb{R}^n} \;\middle|\; \begin{array}{l} y = (y_1, \ldots, y_n) \in \mathbb{R}^n_+ \\ p_0 + \sum_{i=1}^n y_i p_i \in \mathcal{C}^* \end{array} \right\}. \end{aligned}$$

As in the primal program, an element $y \in \mathbb{R}^n$ that satisfies all the constraints of the dual program is called a *feasible solution* of the dual program.

The relevance of duality to optimization is contained in the following key remark. Let $x \in \mathcal{C}$ and $y = (y_1, \ldots, y_n) \in \mathbb{R}^n_+$ be any pair of feasible solutions of the primal and dual programs respectively. Then, by duality, $\langle x, p_0 + \sum_{i=1}^n y_i p_i \rangle \geq 0$ and thus

$$\langle x, p_0 \rangle \geq -\sum_{i=1}^n y_i \langle x, p_i \rangle \geq -\sum_{i=1}^n y_i \delta_i$$

since $y_i \geq 0$ and $\langle x, p_i \rangle \leq \delta_i$. Therefore, one has

$$\langle x, p_0 \rangle \geq \rho \geq \rho^* \geq -\sum_{i=1}^{n} y_i \delta_i.$$

Suppose now that $x^\star$ and $y^\star$ is a pair of feasible solutions such that equality $\langle x^\star, p_0 \rangle = -\sum_{i=1}^{n} y_i^\star \delta_i$ holds. Then both optimization problems are solved, and their solutions satisfy

$$\rho = \langle p_0, x^\star \rangle = \rho^* = -\langle \delta, y^\star \rangle .$$

Thank to this observation, one can give a criterion for an element contained in the "strict border" of the convex domain (i.e. an element where all scalar product inequalities are equalities) to be a minimizing element.

Proposition 31. *Let $x^\star \in \mathcal{C}$ be a feasible solution of the primal program such that $\langle x^\star, p_i \rangle = \delta_i$ for $1 \leq i \leq n$ (equalities instead of inequalities). If there exists $y^\star = p_0 + \sum_{i=1}^{n} y_i^\star p_i \in \mathcal{C}^*$ a feasible solution of the dual program (i.e. $y_i^\star \geq 0$ for $1 \leq i \leq n$) which is orthogonal to $x^\star$, then the minimum (resp. maximum) of the primal (resp. dual) program is attained at $x^\star$ (resp. $y^\star$) and one has $\rho = \rho^* = \langle p_0, x^\star \rangle$.*

Proof. The facts that $\langle x^\star, y^\star \rangle = 0$ and that $\langle x^\star, p_i \rangle = \delta_i$ for $1 \leq i \leq n$ imply that

$$\langle x^\star, p_0 \rangle = \sum_{i=1}^{n} -y_i^\star \langle x^\star, p_i \rangle = \sum_{i=1}^{n} -y_i^\star \delta_i,$$

so that one can conclude using the remark preceding the Proposition. □

To sum up, an element $x^\star$ of the "strict border" of the domain is a minimizing element provided that there exists an element $y^\star$ in the dual of the domain which is orthogonal to $x^\star$. In this situation, we choose to give a name to $y^\star$:

Definition 32. *If $(x^\star, y^\star) \in \mathcal{C} \times \mathcal{C}^*$ satisfies the hypotheses of the preceding proposition we say call $y^\star$ a **certificate** for $x^\star$ being a minimizing element of the primal problem.*

A.2 Real symmetric positive semi definite Toeplitz matrices

In this section, we gather some known results on the euclidean structure hiden behind a *real symmetric positive semi-definite Toeplitz matrices* $T_n(x_0, \ldots, x_{n-1})$ of rank r. Our main reference is Bakonyi and Woerdeman's book [BW11]. More precisely, this section can be seen as answers to Exercises 15 and 20 of Chapter 1.

As usual, for a symmetric real matrix S, the notation $S \succ 0$ (respectively $S \succeq 0$) means that S is definite positive (respectively semi-definite positive). Recall that any matrix $S \succeq 0$ of size n and rank r is the Gram matrix of the column vectors $v_1, \ldots, v_n$ of its square root $S^{\frac{1}{2}}$ ([HJ90, Cor 7.2.11]). In particular, there exists an euclidean space $(E, \langle \cdot, \cdot \rangle)$ of dimension r and a family of vectors $\gamma_1, \ldots, \gamma_n \in E$ such

that $\mathrm{Gram}(\gamma_1, \ldots, \gamma_n) = S$. If $r = n$, that is if $S \succ 0$, then S is nothing else than the matrix of the scalar product in the basis $(\gamma_i)_{1 \leq i \leq n}$.

In order to shorten the statements, we need to introduce some notations for some specific matrices, where the index is the size of the matrix.

Toeplitz	$T_n(x_0, \ldots, x_{n-1}) = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & x_1 \\ x_{n-1} & \cdots & x_1 & x_0 \end{pmatrix}$
Diagonal anti-diagonal	$D_n(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}, \quad J_n = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$
Vandermonde	$V_{n,m}(\varepsilon_1, \ldots, \varepsilon_n) = \begin{pmatrix} 1 & \varepsilon_1 & \cdots & \varepsilon_1^{m-1} \\ \vdots & \vdots & & \vdots \\ 1 & \varepsilon_n & \cdots & \varepsilon_n^{m-1} \end{pmatrix}$ $V_n(\varepsilon_1, \ldots, \varepsilon_n) = V_{n,n}(\varepsilon_1, \ldots, \varepsilon_n)$

A.2.1 Rank of real symmetric, positive semi-definite, Toeplitz matrices

The rank of a symmetric semi-definite positive Toeplitz matrix can be characterized as follows.

Lemma 33. *Let $T_n(x_0, \ldots, x_{n-1})$ be a (non zero) real symmetric, positive, semi-definite Toeplitz matrix. Then its rank is equal to the size of largest non-zero leading minor (obtained by keeping the first lines an columns), that is*

$$\mathrm{rk}\,(T_n(x_0, \ldots, x_{n-1})) = \max_{1 \leq m \leq n} \{\mathrm{Det}(T_m(x_0, \ldots, x_{m-1})) \neq 0\}$$

Proof. As already noted, one can consider an euclidean space $(E, \langle \cdot, \cdot \rangle)$ of dimension r and $\gamma_1, \ldots, \gamma_n \in E$ such that

$$\mathrm{Gram}(\gamma_1, \ldots, \gamma_n) = T_n(x_0, \ldots, x_{n-1}).$$

Necessarily $x_0 \neq 0$ since otherwise we would have $\langle \gamma_i, \gamma_i \rangle = 0$, that is $\gamma_i = 0$, for every i, hence $T_n(x_0, \ldots, x_{n-1})$ should be zero, in contradiction with the assumption. The max in the lemma is thus well defined, say equals s. By definition, one has

$$\mathrm{Gram}(\gamma_1, \ldots, \gamma_s) \neq 0 \qquad \text{and} \qquad \mathrm{Gram}(\gamma_1, \ldots, \gamma_{s+1}) = 0$$

in such a way that the family $\gamma_1, \dots, \gamma_s$ is free while the family $\gamma_1, \dots, \gamma_{s+1}$ is not. It follows that $\gamma_{s+1} \in \bigoplus_{i=1}^{s} \mathbb{R}\gamma_i$. Using the Toeplitz structure, we know that

$$\mathrm{Gram}(\gamma_2, \dots, \gamma_{s+1}) = \mathrm{Gram}(\gamma_1, \dots, \gamma_s) \neq 0,$$

so that the family $\gamma_2, \dots, \gamma_{s+1}$ is free and that $\bigoplus_{i=1}^{s} \mathbb{R}\gamma_i = \bigoplus_{i=2}^{s+1} \mathbb{R}\gamma_i$. Step by step, we deduce that the full family $\gamma_1, \dots, \gamma_n$ has rank s and that $T_n(x_0, \dots, x_n)$ has also rank s. □

A.2.2 A first isometry: the switch

Let $T_n(x_0, \dots, x_{n-1})$ be a real symmetric Toeplitz matrix. An easy calculation shows that

$$J_n T_n J_n = T_n. \tag{51}$$

Suppose that $T_n(x_0, \dots, x_{n-1}) \succ 0$ and that it is the defining matrix of a scalar product in the basis $(\gamma_i)_{0 \leq i \leq n-1}$ on the vector space $E = \bigoplus_{i=0}^{n-1} \mathbb{R}\gamma_i$. Then formulae (51) means that the so called *switch* linear map defined by

$$\gamma_i \mapsto \gamma_{n-1-i}$$

is an involutive isometry of E. Let us denote it by s_E or by s. Since $s^2 = \mathrm{Id}$, the space E decomposes into a direct sum $E = E[1] \oplus E[-1]$ of the two orthogonal subspaces $E[\pm 1]$, the two eigenspaces corresponding to the eigenvalues ± 1. This decomposition is made explicit in the next lemma. We choose to state this lemma in the little more general context of semi-definite Toeplitz matrices.

Lemma 34. *Let $T_{n+1}(x_0, \dots, x_n) = \mathrm{Gram}(\gamma_0, \dots, \gamma_n)$ be a symmetric Toeplitz semi-definite positive matrix. Then the family $(\gamma'_i)_{0 \leq i \leq n}$ defined by*

$$\left(\gamma'_0, \dots, \gamma'_n\right) = \begin{cases} \left(\frac{\gamma_0+\gamma_n}{\sqrt{2}}, \dots, \frac{\gamma_{\frac{n-1}{2}}+\gamma_{\frac{n+1}{2}}}{\sqrt{2}}, \frac{\gamma_0-\gamma_n}{\sqrt{2}}, \dots, \frac{\gamma_{\frac{n-1}{2}}-\gamma_{\frac{n+1}{2}}}{\sqrt{2}} \right) & \text{if } n \text{ is odd} \\ \left(\frac{\gamma_0+\gamma_n}{\sqrt{2}}, \dots, \frac{\gamma_{\frac{n}{2}-1}+\gamma_{\frac{n}{2}+1}}{\sqrt{2}}, \gamma_{\frac{n}{2}}, \frac{\gamma_0-\gamma_n}{\sqrt{2}}, \dots, \frac{\gamma_{\frac{n}{2}-1}-\gamma_{\frac{n}{2}+1}}{\sqrt{2}} \right) & \text{if } n \text{ is even} \end{cases}$$

is such that the two sub-spaces $\mathrm{Vect}(\gamma'_0, \dots, \gamma'_{\lfloor \frac{n}{2} \rfloor})$ *and* $\mathrm{Vect}(\gamma'_{\lfloor \frac{n}{2} \rfloor + 1}, \dots, \gamma'_n)$ *are orthogonal and thus*

$$\mathrm{Gram}\left(\gamma'_0, \dots, \gamma'_n\right) = \begin{pmatrix} \mathrm{Gram}\left(\gamma'_0, \dots, \gamma'_{\lfloor \frac{n}{2} \rfloor}\right) & 0 \\ 0 & \mathrm{Gram}\left(\gamma'_{\lfloor \frac{n}{2} \rfloor + 1}, \dots, \gamma'_n\right) \end{pmatrix}$$

Moreover, one has

$$\begin{aligned} \mathrm{DetGram}\left(\gamma_0, \dots, \gamma_n\right) &= \mathrm{DetGram}\left(\gamma'_0, \dots, \gamma'_n\right) \\ &= \mathrm{DetGram}\left(\gamma'_0, \dots, \gamma'_{\lfloor \frac{n}{2} \rfloor}\right) \times \mathrm{Det\,Gram}\left(\gamma'_{\lfloor \frac{n}{2} \rfloor + 1}, \dots, \gamma'_n\right). \end{aligned}$$

Proof. One way to rephrase the fact that the symmetric matrix is Toeplitz is to say that for every $0 \leq i, j \leq n$, $\langle \gamma_i, \gamma_j \rangle = x_{|i-j|}$. Therefore, if $0 \leq i, j \leq \frac{n}{2}$, one has

$$\begin{aligned}\langle \gamma_i + \gamma_{n-i}, \gamma_j - \gamma_{n-j} \rangle &= x_{|i-j|} - x_{|i-(n-j)|} + x_{|(n-i)-j|} - x_{|(n-i)-(n-j)|} \\ &= x_{|i-j|} - x_{|n-(i+j)|} + x_{|n-(i+j)|} - x_{|i-j|} \\ &= 0\end{aligned}$$

If moreover n is even then $\left\langle \gamma_{\frac{n}{2}}, \gamma_j - \gamma_{n-j} \right\rangle = 0$ for all $0 \leq j \leq \frac{n}{2}$. The form of $\mathrm{Gram}\,(\gamma'_0, \ldots, \gamma'_n)$ follows.

The equality between the determinants of the two Gram matrices is due to the fact that the change of bases matrix from the family $(\gamma_i)_{0 \leq i \leq n}$ to the family $(\gamma'_i)_{0 \leq i \leq n}$, is an unitary one. □

A.2.3 Singular bordered Toeplitz matrix

Let $T_n(x_0, \ldots, x_{n-1}) \succ 0$ be a real, symmetric, positive definite Toeplitz matrix of size n. First, we prove that there exists only two values $x_n^{\pm} \in \mathbb{R}$ such that the bordered Toeplitz matrix $T_{n+1}(x_0, \ldots, x_{n-1}, x_n^{\pm})$ is positive semi-definite of size $n+1$ and of rank n.

Lemma 35. *Let $T_n(x_0, \ldots, x_{n-1}) = \mathrm{Gram}(\gamma_0, \ldots, \gamma_{n-1})$ be a real, symmetric, positive definite, Toeplitz matrix where $(E, \langle \cdot, \cdot \rangle)$ is an euclidean space with base $(\gamma_i)_{0 \leq i \leq n-1}$. There exist two (eventually equal) $\gamma_n^{\pm} \in E$ such that*

$$\mathrm{Gram}(\gamma_0, \ldots, \gamma_{n-1}, \gamma_n^{\pm}) = T_{n+1}(x_0, \ldots, x_{n-1}, x_n^{\pm})$$

is still a Toeplitz matrix of same rank n. Moreover, the two possible upper-right and lower-left coefficients $x_n^{\pm} = \langle \gamma_0, \gamma_n^{\pm} \rangle$ are related by

$$x_n^+ - x_n^- = 2 \cdot \frac{\mathrm{DetGram}\,(\gamma_0, \ldots, \gamma_{n-1})}{\mathrm{DetGram}\,(\gamma_0, \ldots, \gamma_{n-2})}$$

In this situation, $T_{n+1}(x_0, \ldots, x_n)$ is called a *singular bordered Toeplitz matrix.*

Proof. The elements $\gamma \in E$ satisfying the conclusion of the lemma are characterized by

$$\langle \gamma, \gamma_i \rangle = x_{n-i}, \qquad 1 \leq i \leq n-1, \qquad\qquad \langle \gamma, \gamma \rangle = x_0,$$

and the new coefficient is then $x_n = \langle \gamma, \gamma_0 \rangle$. Certainly, there exists a unique element of the hyperplane $F = \bigoplus_{i=1}^{n-1} \mathbb{R}\gamma_i$, satisfying the $(n-1)$ first conditions. We denote by $\pi_F : E \to E$ the orthogonal projection onto F and by $s_F : F \to F$ the "switch" isometry defined on the subspace F. Then $s_F(\pi_F(\gamma_0))$ is this unique element of F, since for every $1 \leq i \leq n-1$, one has

$$\begin{aligned}\langle s_F(\pi_F(\gamma_0)), \gamma_i \rangle &= \langle \pi_F(\gamma_0), s_F(\gamma_i) \rangle && \text{(since } s_F \text{ auto-dual)} \\ &= \langle \pi_F(\gamma_0), \gamma_{n-i} \rangle && \text{(by definition of } s_F) \\ &= \langle \gamma_0, \gamma_{n-i} \rangle && \text{(since } \gamma_0 - \pi_F(\gamma_0) \in F^{\perp} \text{ and } \gamma_{n-i} \in F) \\ &= x_{n-i}\end{aligned}$$

The orthogonal line $F^\perp$ is generated by $\gamma_0 - \pi_F(\gamma_0)$ and any element γ of the whole space E such that $\langle \gamma, \gamma_i \rangle = x_{n-i}$ for every $1 \leq i \leq n-1$, must be of the form $\gamma = s_F(\pi_F(\gamma_0)) + \lambda(\gamma_0 - \pi_F(\gamma_0))$ for some $\lambda \in \mathbb{R}$. Adding the last condition $\langle \gamma, \gamma \rangle = x_0$ leads to

$$\begin{aligned} x_0 &= \|s_F(\pi_F(\gamma_0)) + \lambda(\gamma_0 - \pi_F(\gamma_0))\|^2 = \|\pi_F(\gamma_0)\|^2 + \lambda^2 \|\gamma_0 - \pi_F(\gamma_0)\|^2 \\ &= \|\pi_F(\gamma_0)\|^2 + \|\gamma_0 - \pi_F(\gamma_0)\|^2 \end{aligned}$$

and thus $\lambda = \pm 1$. The two choices are thus $\gamma_n^\pm = s_F(\pi_F(\gamma_0)) \pm (\gamma_0 - \pi_F(\gamma_0))$, and

$$\begin{aligned} x_n^\pm &= \left\langle \gamma_n^\pm, \gamma_0 \right\rangle = \langle s_F(\pi_F(\gamma_0)) \pm (\gamma_0 - \pi_F(\gamma_0)), \gamma_0 \rangle \\ &= \langle \pi_F(\gamma_0), s_F(\pi_F(\gamma_0)) \rangle \pm \|\gamma_0 - \pi_F(\gamma_0)\|^2 . \end{aligned}$$

By difference, $x_n^+ - x_n^-$ is related to the norm $\|\gamma_0 - \pi_F(\gamma_0)\|$ which is nothing else than the distance of $\gamma_0 \in E$ to the subspace F. This distance is known to be equal to the ratio of the two Gram determinants:

$$\begin{aligned} x_n^+ - x_n^- &= 2\|\gamma_0 - \pi_F(\gamma_0)\|^2 = 2 \cdot \frac{\mathrm{DetGram}(\gamma_0, \ldots, \gamma_{n-1})}{\mathrm{DetGram}(\gamma_1, \ldots, \gamma_{n-1})} \\ &= 2 \cdot \frac{\mathrm{DetGram}(\gamma_0, \ldots, \gamma_{n-1})}{\mathrm{DetGram}(\gamma_0, \ldots, \gamma_{n-2})}, \end{aligned}$$

the last equality coming from the Toeplitz structure of the family $(\gamma_0, \ldots, \gamma_{n-1})$. □

A.2.4 A second isometry

In this section, we study the resulting Toeplitz matrix of the previous lemma, that is a semi-definite Toeplitz matrix having a kernel of dimension 1.

Theorem 36. *Let $T_{n+1}(x_0, \ldots, x_n) = \mathrm{Gram}(\gamma_0, \ldots, \gamma_n)$ be a real, symmetric, positive semi-definite Toeplitz matrix of size $(n+1)$ and of rank n, where $(E, \langle \cdot, \cdot \rangle)$ is an euclidean space with basis $(\gamma_i)_{0 \leq i \leq n-1}$. Let $(a_0, \ldots, a_n) \in \mathbb{R}^{n+1}$ be non-zero element of its kernel and let $P = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$. Then:*

(i) The coefficient a_n is non zero, $\gamma_n = -\frac{1}{a_n}(a_{n-1}\gamma_{n-1} + \cdots + a_0\gamma_0)$, and the linear map defined by

$$\gamma_i \mapsto \gamma_{i+1}, \quad 0 \leq i \leq n-1$$

is an isometry which has P as minimal and characteristic polynomial.

(ii) The polynomial $P(X)$ has n distinct complex roots $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{C}$ all of norm 1.

(iii) Let $P_1, \ldots, P_n \in \mathbb{C}[X]$ the unique interpolation polynomials of degree $\leq n$ satisfying $P_i(\varepsilon_j) = \delta_{i,j}$. The family $(P_i(u)(\gamma_0))_{1 \leq i \leq n}$ is an orthogonal basis of the hermitian space $E \otimes_{\mathbb{R}} \mathbb{C}$.

(iv) The Toeplitz matrices factorizes as

$$\begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & x_1 \\ x_{n-1} & \cdots & x_1 & x_0 \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 1 \\ \overline{\varepsilon}_1 & \cdots & \overline{\varepsilon}_n \\ \vdots & & \vdots \\ \overline{\varepsilon}_1^{n-1} & \cdots & \overline{\varepsilon}_n^{n-1} \end{pmatrix} \times \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \times \begin{pmatrix} 1 & \varepsilon_1 & \cdots & \varepsilon_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \varepsilon_n & \cdots & \varepsilon_n^{n-1} \end{pmatrix},$$

where $\lambda_i = \|P_i(u)(\gamma_0)\|^2 \in \mathbb{R}_+^*$. *For any* $0 \leq k \leq n$, *one has* $x_k = \langle \gamma_0, \gamma_k \rangle = \sum_{i=1}^n \lambda_i \varepsilon_i^k$ *and more generally,*

$$\langle A(u)(\gamma_0), B(u)(\gamma_0) \rangle = \sum_{i=1}^n \lambda_i \overline{A(\varepsilon_i)} B(\varepsilon_i)$$

for all $A, B \in \mathbb{C}[X]$.

Proof. By lemma 33, the matrix $T_n(x_0, \ldots, x_{n-1})$ is non-singular and thus $a_n \neq 0$. Moreover, one has $a_0\gamma_0 + \cdots a_n\gamma_n = 0$. The fact that $\mathrm{Gram}(\gamma_0, \ldots, \gamma_n) = T_{n+1}(x_0, \ldots, x_n)$ implies that $\langle \gamma_i, \gamma_j \rangle = x_{|i-j|}$ for all $0 \leq i, j \leq n$. By definition of the map u, one has

$$\langle u(\gamma_i), u(\gamma_j) \rangle = \langle \gamma_{i+1}, \gamma_{j+1} \rangle = x_{|(i+1)-(j+1)|} = x_{|i-j|} = \langle \gamma_i, \gamma_j \rangle$$

for all $0 \leq i, j \leq n-1$. Therefore u is an isometry. Moreover,

$$\begin{aligned} a_0\gamma_0 + \cdots + a_n\gamma_n = 0 &\Rightarrow a_0\gamma_0 + a_1 u(\gamma_0) + \cdots + a_n u^n(\gamma_0) = 0 \\ &\Rightarrow (a_0 \operatorname{Id} + a_1 u + \cdots + a_n u^n)(\gamma_0) = 0 \\ &\Rightarrow (a_0 \operatorname{Id} + a_1 u + \cdots + a_n u^n)(\gamma_i) = 0 \quad \forall i \geq 0 \quad \text{(apply } u^i\text{)}. \end{aligned}$$

We deduce that $P(u) = a_0 \operatorname{Id} + a_1 u + \cdots + a_n u^n = 0$, and P must be the minimal polynomial of u otherwise the family $(\gamma_i)_{0 \leq i \leq n-1}$ would not be free. This means that the vector space E is a cyclic space under u, that is $E \simeq \mathbb{R}[X]/\langle P(X) \rangle$, the isomorphism being defined by $X \bmod P \mapsto \gamma_0$. Under this isomorphism, the multiplication by $X \bmod P$ acting on the right space corresponds to u acting on E, from which item (*i*) follows.

Since P is the minimal polynomial of an euclidean isometry, all its complex roots must be simple and of norm 1, so that item (*ii*) holds true.

As an euclidean isometry, u is diagonalizable over $\mathbb{C}$. So let us extend the scalar to $\mathbb{C}$ and work in $E \otimes_{\mathbb{R}} \mathbb{C}$ with the hermitian form defined by the matrix $T_n(x_0, \ldots, x_{n-1})$ in the basis $(\gamma_i)_{0 \leq i \leq n-1}$. The interpolation polynomials $P_1, \ldots, P_n \in \mathbb{C}[X]$ are explicitly given by

$$P_i(X) = \prod_{j \neq i} \frac{X - \varepsilon_j}{\varepsilon_i - \varepsilon_j},$$

and thus P divides $(X - \varepsilon_i) \times P_i$. We deduce that $(u - \varepsilon_i \operatorname{Id}) \circ P_i(u) = 0$. Applying the left endomorphism to γ_0 leads to $u(P_i(u)(\gamma_0)) = \varepsilon_i P_i(u)(\gamma_0)$. The family $(P_i(u)(\gamma_0))_{1 \leq i \leq n}$

is thus a family of eigenvectors of u associated to the eigenvalues $(\varepsilon_i)_{1\leq i\leq n}$. This must be an orthogonal basis, as stated by item (*iii*):

$$E\otimes_{\mathbb{R}}\mathbb{C}=\bigoplus_{i=1}^{n}\mathbb{C}P_i(u)(\gamma_0)\qquad\text{with}\qquad\langle P_i(u)(\gamma_0),P_j(u)(\gamma_0)\rangle=0,\quad\forall i\neq j.$$

It follows that the matrix of the hermitian product in this basis is diagonal

$$\mathrm{Mat}\left(\langle\cdot,\cdot\rangle,(P_i(u)(\gamma_0))_{1\leq i\leq n}\right)=\begin{pmatrix}\lambda_1&&\\&\ddots&\\&&\lambda_n\end{pmatrix}\qquad\begin{array}{l}\lambda_i=\|P_i(u)(\gamma_0)\|^2>0\\1\leq i\leq n\end{array}.$$

Now, it is well known that the inverse of the Vandermonde matrix $V_n(\varepsilon_1,\ldots,\varepsilon_n)$ is the matrix whose columns are made of the coefficients of the polynomials $P_1,\ldots,P_n$, the bases-change formula for sesquilinear hermitian forms gives item (*iv*):

$$T_n(x_0,\ldots,x_{n-1})={}^tV_n(\overline{\varepsilon}_1,\ldots,\overline{\varepsilon}_n)\times D_n(\lambda_1,\ldots,\lambda_n)\times V_n(\varepsilon_1,\ldots,\varepsilon_n).$$

This can be re-written $x_k=\sum_{i=1}^{n}\lambda_i\varepsilon_i^k$ for every $0\leq k\leq n-1$. More generally for every polynomials $A,B\in\mathbb{C}[X]$ of any degree, one has:

$$\begin{aligned}\langle A(u)(\gamma_0),B(u)(\gamma_0)\rangle&=\langle(A\bmod P)(u)(\gamma_0),(B\bmod P)(u)(\gamma_0)\rangle\\&=\sum_{i=1}^{n}\lambda_i\overline{(A\bmod P)(\varepsilon_i)}(B\bmod P)(\varepsilon_i)=\sum_{i=1}^{n}\lambda_i\overline{A(\varepsilon_i)}B(\varepsilon_i)\end{aligned}$$

since $(A\bmod P)(\varepsilon_i)=A(\varepsilon_i)$ for every $1\leq i\leq n$. This completes the proof of Theorem 36. □

References

[BW11] Mihaly Bakonyi and Hugo J. Woerdeman, *Matrix completions, moments, and sums of hermitian squares*, Princeton University Press, 2011.

[Fat04] Pierre Fatou, *Sur les séries entières à coefficients entiers*, C. R. Acad. Sci. Paris Sér. A **138** (1904), 342–344.

[Han95] Soren Have Hansen, *Rational points on curves over finite fields*, Lect. Notes Ser. Aarhus Univ. Math. Institute (1995), no. 64.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer, 1977.

[HJ90] Roger A. Horn and Charles R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 1990, Corrected reprint of the 1985 original.

[Iha81] Yasutaka Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724 (1982). MR 656048 (84c:14016)

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford, 2002.

[Nik01] Nikolai K. Nikolski, *Operators, functions and systems: An easy reading vol i: Hardy, hankel, and toeplitz*, Mathematical Surveys and Monographs, vol. 92, American Mathematical Society, 2001.

[Ser] Jean-Pierre Serre, *Rational points on curves over finite fields*, Lectures given at Harvard University (notes by F.Q. Gouvea).

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext (1993), Springer, 1993.

[Tsf92] Michael A. Tsfasman, *Some remarks on the asymptotic number of points*, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 178–192. MR 1186424 (93h:11064)

[TV02] M. A. Tsfasman and S. G. Vlăduţ, *Infinite global fields and the generalized Brauer-Siegel theorem*, Mosc. Math. J. **2** (2002), no. 2, 329–402, Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR 1944510 (2004f:11132)

[VD83] Sergei G. Vlăduţ and Vladimir Drinfeld, *Number of points of an algebraic curve*, Funksional Anal i Prilozhen **17** (1983), 53–54.

[Wei48] André Weil, *Courbes algébriques et variétés abéliennes*, Hermann et Cie., Paris, 1948.

[Zar95] Oscar Zariski, *Algebraic surfaces*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, With appendices by S. S. Abhyankar, J. Lipman and D. Mumford, Preface to the appendices by Mumford, Reprint of the second (1971) edition. MR 1336146 (96c:14024)