From Hodge Index Theorem to the number of points of curves over finite fields

Emmanuel Hallouin & Marc Perret*

July 18, 2014

Abstract

We push further the classical proof of Weil upper bound for the number of rational points of an absolutely irreducible smooth projective curve X over a finite field in term of euclidean relationships between the Neron Severi classes in $X \times X$ of the graphs of iterations of the Frobenius morphism. This allows us to recover Ihara's bound, which can be seen as a *second order* Weil upper bound, to establish a new *third order* Weil upper bound, and using `magma` to produce numerical tables for *higher order* Weil upper bounds. We also give some interpretation for the defect of exact recursive towers, and give several new bounds for points of curves in relative situation $X \to Y$.

AMS classification : 11G20, 14G05, 14G15, 14H99.
Keywords : Curves over a finite field, rational point, Weil bound.

Introduction

Let X be an absolutely irreducible smooth projective curve defined over the finite field $\mathbb{F}_q$ with q elements. The classical proof of Weil Theorem for the number of $\mathbb{F}_q$-rational points $\sharp X(\mathbb{F}_q)$ rests upon Castelnuovo identity [Wei48], a 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 Neron Severi space $\mathrm{NS}(X \times X)_{\mathbb{R}}$ is anti-euclidean on the orthogonal complement $\mathcal{E}_X$ of the trivial plane generated by the horizontal and vertical classes. Thus, the opposite $\langle \cdot, \cdot \rangle$ of the intersection pairing endows $\mathcal{E}_X$ with a structure of euclidean space. Section 1 is devoted to few useful scalar products computations.

In section 2, we begin by giving a proof of Weil inequality which is, although equivalent in principle, different in presentation than the usual one using Castelnuovo Theorem given for instance in [Har77, exercice 1.9, 1.10 p. 368] or in [Sha94, exercises 8, 9, 10 p. 251]). We prove that Weil bound follows from Cauchy-Schwartz inequality for the

[*] Institut de Mathématiques de Toulouse, UMR 5219, hallouin@univ-tlse2.fr, perret@univ-tlse2.fr

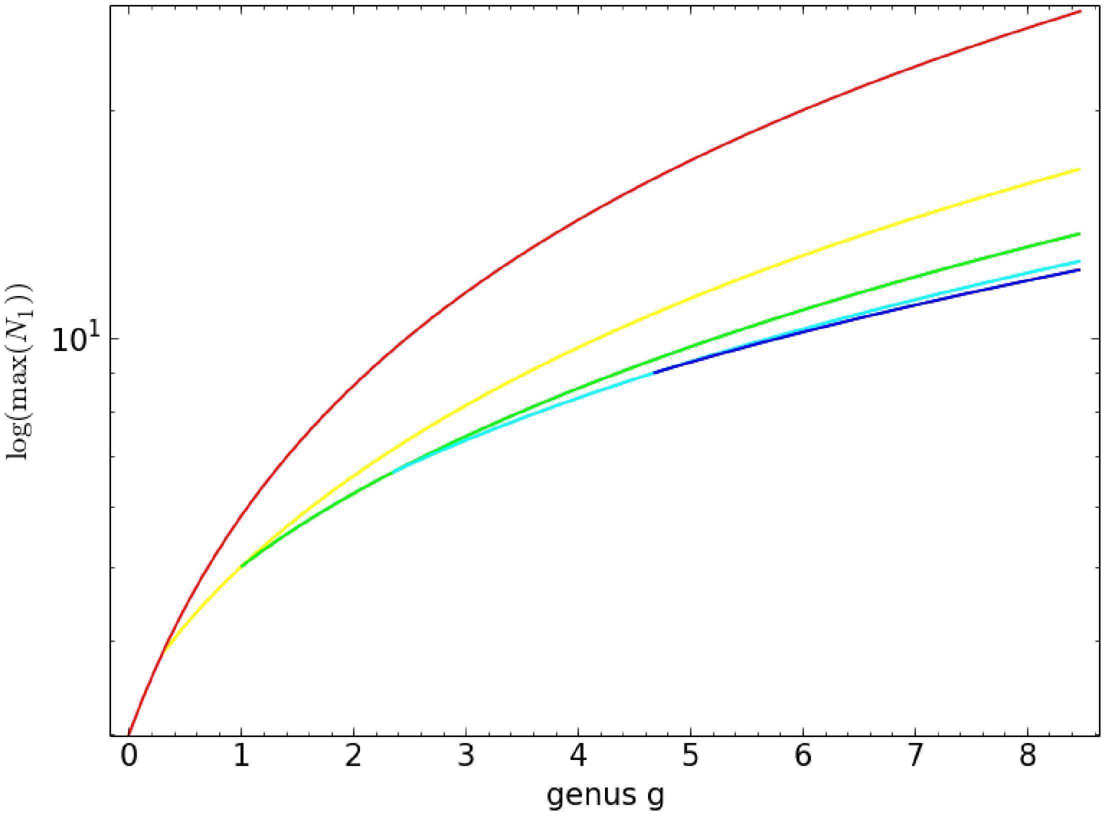
orthogonal projections onto $\mathcal{E}_X$ of the diagonal class Γ^0 and the class Γ^1 of the graph of the Frobenius morphism on X.

The benefit of using Cauchy-Schwartz instead of Castelnuovo is the following. We do not know what can be a Castelnuovo identity for more than two Neron Severi classes, while we do know what is Cauchy-Schwartz for any number of vectors. It is well-known that Cauchy-Schwartz between two vectors is the non-negativity of their 2×2 Gram determinant. Hence, we are cheered on investigating the consequences of the non-negativity of larger Gram determinants involving the Neron Severi classes Γ^k of the graphs of the k-th iterations of the Frobenius morphism.

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 2.5.2, especialy looking at figure 1 in section 2.5.2. 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 between Γ^0, Γ^1 and Γ^2. Moreover this process can 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 18), which improves the Ihara bound for curves of genus greater than another constant $g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$.

The more the genus increases, the more the Weil bound should be chosen of high order in order to be optimal. Therefore it is useful to compute higher order Weil bounds. Unfortunately, establishing them explicitely requires the resolution of high degree one variable polynomial equations over $\mathbb{R}$. For instance, 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, while fourth and fifth order Weil bounds require the resolution of third degree equations, and so on. Moreover, a 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 increase.

Hence, we give up the hope to establish explicit formulae for the Weil bounds of order from 4. We then turn to a more algorithmic point of view. 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. The validity of this algorithm requires some results proved in the second section. In the figure below, we represent the successive Weil bounds (in logarithmic scales) of order from 1 to 5. Note that taking into account the logarithmic scale for the y-axis, higher order Weil bounds become significantly better than usual Weil's one.



Weil bounds of order 1 to 5 for $\sharp X(\mathbb{F}_q)$ (here for $q = 2$). Note that the y axis is logarithmic. For small genus, red usual first order Weil bound is the best one. Then from genus $g_2 = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$, yellow Ihara's second order Weil bound becomes the best, up to the genus $g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ where green third order weil bound becomes the best. From some genus g_4, light blue fourth order Weil bound is the best up to some genus g_5, where dark blue fifth order Weil bound becomes better, and so on. Here, we have chosen $q = 2$, for which the genera 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 $g = 3, 4$ is the fourth order one!

In order to illustrate the efficiency of our algorithm, we display in section 2.6.3 a numerical table.

We acknowledge that for any pair (g, q) we have tested, a comparison of our numerical results with the table given on the website `http://www.manypoints.org/` reveals that we *always* recover the very same numerical upper bound for $N_q(g)$ than those coming from Oesterlé bounds! We were not been able to understand this experimental observation.

Nevertheless, we think that the viewpoint introduced in this article is preferable to Osterlé's one. First, our viewpoint is more conceptual in nature. Any constraints we use to obtain our bounds come in a quite pleasant way either from algebraic-geometry or from arithmetic, as explained in the introduction of section 2 in which we outline our approach. We think moreover that the graph displayed just above is very satisfying.

Second, the viewpoint introduced in this article is perfectly adapted to the study of bounds for the numbers of rational points. As the reader can see, many[1] known results can be understood with this viewpoint -even asymptotical ones, and new results can be proved. We are pretty sure that we have not extracted all potential outcomes of this viewpoint. Third, new questions can be raised from this viewpoint. We propose a few in Section 4.

To conclude Section 2, we push to the *infinite-order Weil bound* using the non-negativity of the Gram determinants of any orders, which imply that some symmetric matrix is semi-definite positive. Applied to some very simple vector, this lead us to Theorem 22, a stronger form of [Tsf92] Tsfasman bound in that it gives a new interpretation for the *defect* of an exact tower as a limit of nice euclidean vectors in $(\mathcal{E}, \langle\cdot,\cdot\rangle)$.

In Section 3, we study the relative situation. Given a finite morphism $f : X \to Y$ between two absolutely irreducible smooth projective curves defined over $\mathbb{F}_q$, the pull-back functor on divisors from the bottom algebraic surface $Y \times Y$ to the top one $X \times X$ induces a map from the Neron Severi space $\mathrm{NS}(Y \times Y)_{\mathbb{R}}$ to $\mathrm{NS}(X \times X)_{\mathbb{R}}$. Restricting this map to the subspaces $\mathcal{F}_X$ and $\mathcal{F}_Y$ generated by the classes of the graphs of iterations of the Frobenius morphisms, and after a suitable normalization (which differs from the normalization chosen in Section 2), we prove that it becomes an *isometric embedding*. We thus have an orthogonal decomposition $\mathcal{F}_X = \mathcal{F}_Y^* \oplus \mathcal{F}_{X/Y}$, involving a *relative subspace* $\mathcal{F}_{X/Y}$ of $\mathcal{F}_X$.

Now, Cauchy-Schwartz inequality applied to the orthogonal projections of Γ_X^0 and Γ_X^1 on the relative space $\mathcal{F}_{X/Y}$ is equivalent to the well known relative Weil bound that $|\sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)| \leq 2(g_X - g_Y)\sqrt{q}$.

With regard to higher orders relative Weil bounds, we encounter a difficulty since the arithmetical constraints $\sharp X(\mathbb{F}_{q^r}) - \sharp Y(\mathbb{F}_{q^r}) \geq \sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)$ for $r \geq 2$, similar to that used in Section[2] 2 does not hold true! Hence, the only constraints we are able to use are the non-negativity of Gram determinants. This lead to an inequality relating the quantities $\sharp X(\mathbb{F}_{q^r}) - \sharp Y(\mathbb{F}_{q^r})$ (corollary 29). We also prove a bound involving four curves in a cartesian diagram under some smoothness assumption (Theorem 33).

As stated above, we end this article by a very short Section 4, in which we raise a few questions.

1 The euclidean space $(\mathcal{E}, \langle\cdot,\cdot\rangle)$

Let X be an absolutely irreducible smooth projective curve defined over the finite field $\mathbb{F}_q$ with q elements. We consider the Neron-Severi space $\mathrm{NS}(X \times X)_{\mathbb{R}} = \mathrm{NS}(X \times X) \otimes_{\mathbb{Z}} \mathbb{R}$ of the smooth surface $X \times X$. It is well known that the intersection product of two divisors Γ and Γ' on $X \times X$ induces a symmetric bilinear form on $\mathrm{NS}(X \times X)_{\mathbb{R}}$, whose signature is given by the following Hodge Index Theorem (e.g. [Har77]).

[1] Other known results can be proved from this viewpoint, for instance the rationality of the Zeta function, using the vanishing of Hankel determinants. In order to save place, we have chosen to skip this.

[2] See the introduction of Section 2

Theorem 1 (Hodge index Theorem)**.** *The intersection pairing is non-degenerate on the space* $\mathrm{NS}(X \times X)_{\mathbb{R}}$*, and is definite negative on the orthogonal supplement of any ample divisor.*

Let $H = X \times \{*\}$ and $V = \{*\} \times X$ be the horizontal and vertical classes on $X \times X$. Their intersection products are given by $H \cdot H = V \cdot V = 0$ and $H \cdot V = 1$. The restriction of the intersection product to $\mathrm{Vect}(H, V)$ has thus signature $(1, -1)$. Moreover $\mathrm{Vect}(H, V) \cap \mathrm{Vect}(H, V)^{\perp} = \{0\}$. By non-degeneracy, this gives rise to an orthogonal decomposition $\mathrm{NS}(X \times X)_{\mathbb{R}} = \mathrm{Vect}(H, V) \oplus \mathrm{Vect}(H, V)^{\perp}$. Let p be the orthogonal projection onto the non-trivial part $\mathrm{Vect}(H, V)^{\perp}$, given by

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

Since $H + V$ is ample, the intersection pairing is definite negative on $\mathrm{Vect}(H, V)^{\perp}$ by Hodge index Theorem. Hence, $\mathrm{Vect}(H, V)^{\perp}$ can be turned into an euclidean space by defining a scalar product as the opposite of the intersection pairing.

Definition 2. *Let* $\mathcal{E} = \mathrm{Vect}(H, V)^{\perp}$*. We define on* $\mathcal{E}$ *a scalar product, denoted by* $\langle \cdot, \cdot \rangle$*, as*

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

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

In the sequel of this article, all the computations will take place in the euclidean space $(\mathcal{E}, \langle \cdot, \cdot \rangle)$. To begin with, let us compute this pairing between the iterates of the Frobenius morphism.

Lemma 3. *Let* $F : X \to X$ *denotes the* q*-Frobenius morphism on* X*, and* F^k *denotes the* k*-th iterate of* F *for any* $k \geq 0$*, with the usual convention that* $F^0 = \mathrm{Id}_X$*. We denote by* Γ^k *the Neron Severi class of the graph of* F^k*. Then*

$$\begin{cases} \left\langle p(\Gamma^k), p(\Gamma^k) \right\rangle = 2gq^k & \forall k \geq 0 \\ \left\langle p(\Gamma^k), p(\Gamma^{k+i}) \right\rangle = q^k \left((q^i + 1) - \sharp X(\mathbb{F}_q^i) \right) & \forall k \geq 0, \forall i \geq 1. \end{cases}$$

Proof — Since the morphism F^k is a regular map of degree q^k, one has $\Gamma^k \cdot H = q^k$ and $\Gamma^k \cdot V = 1$. Now, let $k \in \mathbb{N}$ and $i \in \mathbb{N}^*$. We consider the map $\pi = F^k \times \mathrm{Id} : X \times X \to X \times X$, which sends (P, Q) to $(F^k(P), Q)$. We have $\pi^*(\Delta) = \Gamma^k$ and $\pi_* \left(\Gamma^{k+i} \right) = q^k \Gamma^i$, so that by projection formula for the proper morphism π:

$$\begin{aligned} \Gamma^k \cdot \Gamma^{k+i} &= \pi^*(\Delta) \cdot \Gamma^{k+i} \\ &= \Delta \cdot \pi_* \left(\Gamma^{k+i} \right) \\ &= q^k \Delta \cdot \Gamma^i. \end{aligned}$$

If $i \geq 1$, then $\Delta \cdot \Gamma^i = \sharp X(\mathbb{F}_{q^i})$. If $i = 0$, then $\Gamma^0 = \Delta$ and $\Delta \cdot \Gamma^0 = \Delta^2 = -2g$. The results follow since $p(\Gamma^k) = \Gamma^k - H - q^k V$ by (1). □

Remark – Of course, $\dim \mathcal{E} \leq \dim NS(X \times X)_{\mathbb{R}} - 2 \leq 4g^2$. But as the reader can check, we are working along this article only on the subspace $\mathcal{F}$ of $\mathcal{E}$ generated by the family $p(\Gamma^k), k \geq 0$. By ([Zar95] chapter VII, appendix of Mumford), any trivial linear combination of this family is equivalent to the triviality of the same linear combination of the family $\varphi_\ell^k, k \geq 0$, of the iteration of the Frobenius endomorphism φ_ℓ on the Tate module $V_\ell(\mathrm{Jac}\ X)$ for any prime $\ell \wedge q = 1$. We deduce that for a given curve X over $\mathbb{F}_q$ of genus g, we actually are working in an euclidean space $\mathcal{F}_X$ of dimension equal to the degree of the minimal polynomial of φ_ℓ on $V_\ell(\mathrm{Jac}\ X)$.

2 Absolute bounds

We observe, as a consequence of Lemma 3, that the non-negativity

$$\begin{aligned} 0 \leq \mathrm{Gram}(p(\Gamma^0), p(\Gamma^1)) &= \begin{vmatrix} 2g & q+1-\sharp X(\mathbb{F}_q) \\ q+1-\sharp X(\mathbb{F}_q) & 2gq \end{vmatrix} \\ &= (2g\sqrt{q})^2 - (q+1-\sharp X(\mathbb{F}_q))^2 \end{aligned}$$

is nothing else than Weil inequality. In this Section, we give other bounds using larger Gram determinants. For this purpose, we need preliminary notations, normalizations and results.

Normalizations in Section 2.1 play two parts. They ease many formulae and calculations. They also make obvious that several features of the problem, such as the Gram matrix $\mathrm{Gram}(p(\Gamma^i); 0 \leq i \leq n)$, or the forthcoming n-th Weil domains $\mathcal{W}_n$, are essentially independent of q. The authors believe that these features deserve to be emphasized.

With regard to results, let $n \in \mathbb{N}^*$. To obtain the Weil bound of order n, let X be an algebraic curve of genus g defined over $\mathbb{F}_q$. We use both geometric and arithmetic facets of X as follows. We define from X in (4) a point $P_n(X) \in \mathbb{R}^n$, whose abscissa x_1 given in (3) is essentially the *opposite* of $\sharp X(\mathbb{F}_q)$, hence have to be *lower bounded*. The algebraic-geometric facet of X implies, thanks to Hodge index Theorem, that some Gram determinant involving the coordinates of $P_n(X)$ is non-negative. This is traduced on the point $P_n(X)$ in Lemma 12 in that it do lies inside some convex *n-th Weil domain* $\overline{\mathcal{W}}_n$, studied in Subsection 2.3. The arithmetic facet of X is used via *Ihara constraints*, that for any $r \geq 2$ we have $\sharp X(\mathbb{F}_{q^r}) \geq \sharp X(\mathbb{F}_q)$. We then define in Subsection 2.4 the convex *n-th Ihara domain $\mathcal{H}_n^g$ in genus g*. We state in Proposition 16 that for any curve X of genus g defined over $\mathbb{F}_q$, we have $P_n(X) \in \overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$. We are thus reduced to minimize the convex function x_1 on the convex domain $\overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$. To this end, we establish in Subsection 2.4 the optimization criteria 17, decisive for the derivations of higher order Weil bounds.

This criteria is used to prove new bounds in Subsection 2.6. Finally, we obtain in Subsection 2.7 a refined form of Tsfasman upper bound for asymptoticaly exact towers.

2.1 The Gram matrix of the normalized classes of iterated Frobenius

In this Subsection, we choose to normalize the Neron-Severi classes of the iterated Frobenius morphisms as follows. For any $n \geq 1$, and any curve X defined over $\mathbb{F}_q$ of genus

$g \neq 0$, we define a point $P_n(X) \in \mathbb{R}^n$ whose x_i-coordinates is very closely related to $\sharp X(\mathbb{F}_{q^i})$.

Definition 4. *Let X be an absolutely irreducible smooth projective curve defined over the finite field $\mathbb{F}_q$. For $k \in \mathbb{N}$, we put*

$$\gamma^k = \frac{1}{\sqrt{2gq^k}} p(\Gamma^k) \in \mathcal{E}, \tag{2}$$

so that by Lemma 3 we have $\langle \gamma^k, \gamma^k \rangle = 1$. For $i \in \mathbb{N}^*$, we put

$$x_i \overset{def.}{=} \left\langle \gamma^k, \gamma^{k+i} \right\rangle \overset{lemma\ 3}{=} \frac{(q^i+1) - \sharp X(\mathbb{F}_{q^i})}{2g\sqrt{q}^i}. \tag{3}$$

For any $n \geq 1$, we define the point

$$P_n(X) = (x_1, \ldots, x_n) \in \mathbb{R}^n. \tag{4}$$

Remark – Note first that X is Weil-maximal if and only if $x_1 = -1$, and is Weil minimal if and only if $x_1 = 1$. Second, that to give *upper* bounds for $\sharp X(\mathbb{F}_q)$ amount to give *lower* bounds for x_1.

From this Definition 4 and Lemma 3, the Gram matrix of the family $\gamma^0, \ldots, \gamma^n$ in $\mathcal{E}$ is

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

2.2 Some identities involving Toeplitz matrices

The main result of this Subsection is Lemma 5, providing the existence of the factorization in Definition 6, in which the G_n^- factor plays a fundamental part in the following of the article.

A *symmetric Toeplitz matrix* is a symmetric matrix whose entries $x_{i,j}$ depend only on $|i-j|$, that is are constant along the diagonals parallel to the main diagonal [HJ90, §0.9.7], that is

$$T_{n+1}(x_0, x_1, \ldots, x_n) = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} & x_n \\ x_1 & \ddots & \ddots & & x_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{n-1} & & \ddots & \ddots & x_1 \\ x_n & x_{n-1} & \cdots & x_1 & x_0 \end{pmatrix} \tag{6}$$

The symmetric Toeplitz matrix is said to be *normalized* if $x_0 = 1$.

An *Hankel matrix* is a matrix whose entries $x_{i,j}$ depend only on $i + j$, that is are constant along the anti-diagonals parallel to the main anti-diagonal [HJ90, §0.9.8], that is

$$H_{n+1}(x_0, x_1, \ldots, x_{2n}) = \begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_n \\ x_1 & \iddots & & \iddots & x_{n+1} \\ x_2 & & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & & x_{2n-1} \\ x_n & x_{n+1} & \cdots & x_{2n-1} & x_{2n} \end{pmatrix} \tag{7}$$

> **Remark** – It should be noticed that in this article, any matrix is indexed by its size, while this doesn't hold for determinants, for instance see formulae (9) and (10).

Lemma 5. *For any $n \geq 1$, we abbreviate $T_n(x_0, \ldots, x_{n-1})$ by T_n. The determinant of this Toeplitz matrix factorizes as*

$$\mathrm{Det}\,(T_{2n}) = \mathrm{Det}\,(T_n + H_n(x_{2n-1}, \ldots, x_1)) \times \mathrm{Det}\,(T_n - H_n(x_{2n-1}, \ldots, x_1))$$

and

$$\mathrm{Det}\,(T_{2n+1}) = \mathrm{Det}\begin{pmatrix} T_n + H_n(x_{2n}, \ldots, x_2) & {}^tX_n \\ 2X_n & x_0 \end{pmatrix} \times \mathrm{Det}\,(T_n - H_n(x_{2n}, \ldots, x_2)),$$

where $X_n = (x_n, \ldots, x_1)$.

Proof — *Even size.* The operations on the columns $C_j \leftarrow C_j + C_{2n-(j-1)}$ for $1 \leq j \leq n$, followed by the operations on the lines $L_{n+i} \leftarrow L_{n+i} - L_{n-(i-1)}$ for $1 \leq i \leq n$ lead to the determinant of a 2×2 blocks upper triangular matrix whose value is the expected product.

Odd size. The operations on the columns $C_j \leftarrow C_j + C_{2n+1-(j-1)}$ for $1 \leq j \leq n$, followed by the operations on the lines $L_{n+1+i} \leftarrow L_{n+1+i} - L_{n+1-i}$ for $1 \leq i \leq n$ lead to the result in the same manner. □

Definition 6. *For $n = 0$, we put $G_0 = G_0^- = G_0^+ = 1$, and for $n \geq 1$, we put*

$$G_n(x_1, \ldots, x_n) \overset{def.}{=} \mathrm{Det}(T_{n+1}(1, x_1, \ldots, x_n)) \overset{Lemma\ 5}{=} G_n^-(x_1, \ldots, x_n) \times G_n^+(x_1, \ldots, x_n),$$

where the last factorization is the one proved in Lemma 5 in the same order.

> **Remark** – The determinant G_n is the determinant of a matrix of size $n + 1$. Note that for $n = 2m + 1$ odd, both G_n^- and G_n^+ are polynomials of degree $m + 1$ in $x_1, \ldots, x_n$, while for $n = 2m$ even, G_n^- has degree $m + 1$, while G_n^+ have degree m. We will see later in the article that Weil bound of order n for $\sharp X(\mathbb{F}_q)$ depends heavily on the hypersurface $\{G_n^- = 0\}$.

In order to raise any ambiguity and for later purpose, let us write down these determinants for $n = 1, 2$ and 3:

$$G_1(x_1) = \begin{vmatrix} 1 & x_1 \\ x_1 & 1 \end{vmatrix} = \underbrace{(1 + x_1)}_{G_1^-(x_1)} \times \underbrace{(1 - x_1)}_{G_1^+(x_1)} \tag{8}$$

$$G_2(x_1, x_2) = \begin{vmatrix} 1 & x_1 & x_2 \\ x_1 & 1 & x_1 \\ x_2 & x_1 & 1 \end{vmatrix} = \underbrace{\begin{vmatrix} 1 + x_2 & x_1 \\ x_1 + x_1 & 1 \end{vmatrix}}_{G_2^-(x_1,x_2)} \times \underbrace{(1 - x_2)}_{G_2^+(x_1,x_2)} \tag{9}$$

$$G_3(x_1, x_2, x_3) = \begin{vmatrix} 1 & x_1 & x_2 & x_3 \\ x_1 & 1 & x_1 & x_2 \\ x_2 & x_1 & 1 & x_1 \\ x_3 & x_2 & x_1 & 1 \end{vmatrix} = \underbrace{\begin{vmatrix} 1 + x_3 & x_1 + x_2 \\ x_1 + x_2 & 1 + x_1 \end{vmatrix}}_{G_3^-(x_1,x_2,x_3)} \times \underbrace{\begin{vmatrix} 1 - x_3 & x_1 - x_2 \\ x_1 - x_2 & 1 - x_1 \end{vmatrix}}_{G_3^+(x_1,x_2,x_3)} \tag{10}$$

Lemma 7. *For any $n \geq 1$ and $\epsilon = \pm$ or nothing, we abbreviate $G_n^\epsilon(x_1, \dots, x_n)$ by G_n^ϵ. Then one has*

$$2G_n = G_{n-1}^+ \times G_{n+1}^- + G_{n-1}^- \times G_{n+1}^+.$$

Proof — Let S_{n+1}^- be the matrix obtained from T_n by adding ${}^t(x_n, \dots, x_1)$ to the first column, and S_{n+1}^+ be the matrix obtained from T_n by removing ${}^t(x_n, \dots, x_1)$ to the first column. Then by multilinearity, there exists a polynomial R_n such that:

$$\text{Det}\left(S_{n+1}^-\right) = G_n + R_n \quad \text{and} \quad \text{Det}\left(S_{n+1}^+\right) = G_n - R_n.$$

On the other hand, using the same transformations as in the proof of Lemma 5, one get

$$\text{Det}(S_{n+1}^-) = G_{n-1}^+ G_{n+1}^- \quad \text{and} \quad \text{Det}(S_{n+1}^+) = G_{n-1}^- G_{n+1}^+$$

Adding $\text{Det}(S_{n+1}^-)$ and $\text{Det}(S_{n+1}^+)$ allows us to conclude. □

2.3 The domain of positive definite normalized Toeplitz matrices

In this Subsection, we study for any $n \geq 1$ some domain $\mathcal{W}_n \subset \mathbb{R}^n$, whose closure $\overline{\mathcal{W}_n}$ also plays a fundamental part in this article.

Definition 8. *Let $n \in \mathbb{N}^*$. We denote by $\mathcal{W}_n$ the set of $(x_1, \dots, x_n) \in \mathbb{R}^n$, such that the symmetric normalized Toeplitz matrix $T_{n+1}(1, x_1, \dots, x_n)$ is positive definite.*

The domain $\mathcal{W}_n$ can be characterized in several useful ways.

Proposition 9. *For $n \geq 1$, the domain $\mathcal{W}_n$ is a convex subset of $]-1, 1[^n$, which can be written as follows.*

1. *First, one has:*

$$\mathcal{W}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid G_i(x_1, \ldots, x_i) > 0,\ \forall\, 1 \le i \le n\}\,.$$

2. *Recursively,* $\mathcal{W}_1 = \left]-1, 1\right[$ *and for any* $n \ge 2$

$$\begin{aligned}\mathcal{W}_n &= \{(x_1, \ldots, x_{n-1}, x_n) \in \mathcal{W}_{n-1} \times \mathbb{R} \mid G_n(x_1, \ldots, x_n) > 0\} \\ &= \left\{(x_1, \ldots, x_{n-1}, x_n) \in \mathcal{W}_{n-1} \times \mathbb{R} \mid G_n^-(x_1, \ldots, x_n) > 0 \text{ and } G_n^+(x_1, \ldots, x_n) > 0\right\}.\end{aligned}$$

3. $\mathcal{W}_n$ *is also the set of points between the graphs of two functions from* $\mathcal{W}_{n-1}$ *to* $\mathbb{R}$*: for* $\varepsilon = \pm$*, there exists a polynomial* $\widetilde{G}_n^\varepsilon \in \mathbb{Q}[x_1, \ldots, x_{n-1}]$*, such that* $G_n^\epsilon = -\epsilon G_{n-2}^\epsilon x_n + \epsilon \widetilde{G}_n$ *and*

$$\mathcal{W}_n = \left\{(x_1, \ldots, x_{n-1}, x_n) \in \mathcal{W}_{n-1} \times \mathbb{R} \mid \frac{\widetilde{G}_n^-(x_1, \ldots, x_{n-1})}{G_{n-2}^-(x_1, \ldots, x_{n-2})} < x_n < \frac{\widetilde{G}_n^+(x_1, \ldots, x_{n-1})}{G_{n-2}^+(x_1, \ldots, x_{n-2})}\right\}.$$

Proof — To prove the convexity, we remark that both sets of normalized symmetric Toeplitz matrices and of symmetric positive definite matrices are convex, so that $\mathcal{W}_n$ is convex. Moreover, $\mathcal{W}_n \subset \left]-1, 1\right[^n$ because if $T_{n+1}(1, x_1, \ldots, x_n)$ is positive definite, then all its principal minors are positive. In particular, for any $1 \le i \le n$, the 2×2 minors $\left|\begin{smallmatrix} 1 & x_i \\ x_i & 1 \end{smallmatrix}\right|$ is positive.

Item (1) follows from the well known fact that an $n \times n$ symmetric matrix is definite positive if and only if all its n leading principal minors (obtained by deleting the i last rows and columns for $0 \le i \le n-1$) are positive [HJ90, Theorem 7.2.5]. Hence, the first characterization of item (2) follows from item 1 . To prove the second characterization of item (2), we use Lemma 7 stating that $2G_{n-1} = G_{n-2}^- G_n^+ + G_{n-2}^+ G_n^-$. By induction, this allow us to prove that both factors are positive if, and only if, the product

$$G_n(x_1, \ldots, x_n) = G_n^-(x_1, \ldots, x_n) G_n^+(x_1, \ldots, x_n)$$

is positive for any $(x_1, \ldots, x_{n-1}) \in \mathcal{W}_{n-1}$.

To prove item (3), for $\epsilon = \pm$, formulae defining the polynomials G_n^ϵ in Lemma 5 and Definition 6 imply, developing along their first column and taking advantage of the very particular forms (6) and (7), that both polynomials have degree 1 in x_n, of the form

$$G_n^\epsilon = -\epsilon G_{n-2}^\epsilon x_n + \varepsilon \widetilde{G}_n^\epsilon(x_1, \ldots, x_{n-1})$$

for some $\widetilde{G}_n^\epsilon \in \mathbb{Q}[x_1, \ldots, x_{n-1}]$. Since by item 2 we have $G_{n-2}^\varepsilon > 0$, the set $\mathcal{W}_n$ is thus equal to the set of $(x_1, \ldots, x_{n-1}, x_n) \in \mathcal{W}_{n-1} \times \mathbb{R}$, such that:

$$\frac{\widetilde{G}_n^-(x_1, \ldots, x_{n-1})}{G_{n-2}^-(x_1, \ldots, x_{n-2})} < x_n < \frac{\widetilde{G}_n^+(x_1, \ldots, x_{n-1})}{G_{n-2}^+(x_1, \ldots, x_{n-2})},$$

and the proof is complete. □

The following Proposition is useful for later purpose in Section 2.6, where convexity plays a quite important part.

Proposition 10. *The locus* $\{(x_1,\dots,x_n) \in \mathcal{W}_{n-1} \times \mathbb{R} \mid G_n^-(x_1,\dots,x_n) > 0\}$ *is convex, while the locus* $\{(x_1,\dots,x_n) \in \mathcal{W}_{n-1} \times \mathbb{R} \mid G_n^+(x_1,\dots,x_n) > 0\}$ *is concave.*

Proof — By item 3 of Proposition 9, $\mathcal{W}_n$ is the set of $(x_1,\dots,x_{n-1},x_n) \in \mathcal{W}_{n-1} \times \mathbb{R}$ such that x_n is between two functions from $\mathcal{W}_{n-1}$ to $\mathbb{R}$. By convexity of $\mathcal{W}_n$ from Proposition 9, the lower function must be concave has a function on $\mathcal{W}_{n-1}$ while the upper one must be convex. The Proposition follows easily. □

The closure of $\mathcal{W}_n$ is given by the following Proposition.

Proposition 11. *The closure* $\overline{\mathcal{W}}_n$ *of* $\mathcal{W}_n$ *in* $\mathbb{R}^n$ *corresponds to the set of* $(n+1)\times(n+1)$ *normalized symmetric Toeplitz matrices which are positive semi definite. Moreover, we have*

$$\overline{\mathcal{W}}_n = \{(x_1,\dots,x_n) \in \mathbb{R}^n \mid G_{n,I}(x_1,\dots,x_i) \geq 0,\ \forall I \subset \{0,1,\dots,n\}\}\,,$$

where, for $I \subset \{0,1,\dots,n\}$*, we denote by* $G_{n,I}(x_1,\dots,x_n)$ *the principal minor of the normalized symmetric Toeplitz matrix* $T_{n+1}(1,x_1,\dots,x_n)$ *obtained by deleting the lines and columns whose indices are not in* I*.*

Proof — This is a consequence of the fact that a matrix is *positive semi definite* if and only if all the *principal minors* (the ones obtained by deleting the same subset of lines and columns) are non-negative (i.e. ≥ 0) [HJ90, last exercise after Theorem 7.2.5]. □

2.4 The curves locus

In this Subsection, we introduce Ihara's constraints and the resulting *n-Ihara domain* $\mathcal{H}_n^g$ *for genus g*. We then gather the key results for the derivation of higher order Weil bounds. The first one is Proposition 16, the second one is criteria 17.

2.4.1 The n-the Weil domain $\overline{\mathcal{W}}_n$

Lemma 12. *Let* X *be an absolutely irreducible smooth projective curve defined over* $\mathbb{F}_q$*. Then the point* $P_n(X) = (x_1,\dots,x_n)$*, as defined in* (4)*, belongs to* $\overline{\mathcal{W}}_n$*.*

Proof — By (3), we have $x_i = \langle \gamma^k, \gamma^{k+i} \rangle$ where the γ^k are defined in (2), so that it is easily seen that for any $I \subset \{0,1,\dots,n\}$, we have

$$G_{n,I}(x_1,\dots,x_n) = \mathrm{Gram}(\gamma^i,\ i \notin I),$$

for $G_{n,I}$ s defined in Proposition 11. The non-negativity of $G_{n,I}$ follows as a Gram determinant in an euclidean space, hence the Lemma by Proposition 11. □

Definition 13. *$\overline{\mathcal{W}}_n$ is called the n-th Weil domain.*

As a first illustration of the informations contained in these Weil domains, we prove the following simple result. From (9), the non-negativity of the Gram determinants G_2^- writes $x_2 \geq 2x_1^2 - 1$. Taking (3) into account, this gives immediately

Proposition 14. *For any curve X of genus $g \neq 0$, we have*

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

This Proposition means that, for a given non rational curve X, any lower bound for the deviation of $\sharp X(\mathbb{F}_q)$ to $q+1$ yields to a better upper bound than Weil's one for $\sharp X(\mathbb{F}_{q^2})$. In the same way, for any given order n, the non-negativity of the 3×3 determinant $\mathrm{Gram}(\gamma^0, \gamma^1, \gamma^n)$ gives a quite ugly upper bound of similar nature for $\sharp X(\mathbb{F}_{q^n})$ in terms of $\sharp X(\mathbb{F}_q)$ and $\sharp X(\mathbb{F}_{q^{n-1}})$.

> **Remark** – Note that this Proposition is a refinement of the following well known particular case: if X is either Weil maximal or minimal over $\mathbb{F}_q$, then $\sharp X(\mathbb{F}_q) - (q+1) = \pm 2g\sqrt{q}$, and this Proposition asserts that then $X(\mathbb{F}_{q^2}) - (q^2+1) \leq 2gq - \frac{4g^2q}{g} = -2gq$, so that X is Weil minimal over $\mathbb{F}_{q^2}$. Note also that curves such that this inequality is an equality are those curves such that the corresponding point $P_2(X) = (x_1, x_2) \in \overline{\mathcal{W}}_2$ lies on the bottom parabola $x_2 = 2x_1^2 - 1$ of the Ihara domain drawn in figure 1 below. The above particular case is that of curves corresponding to the corner points $(-1, 1)$ and $(1, 1)$.

2.4.2 Ihara constraints : the n-th Ihara domain $\mathcal{H}_n^g$ in genus g

If $(x_1, \ldots, x_n) \in \mathbb{R}^n$ comes from a curve X over $\mathbb{F}_q$ by formulae (3), then we have seen in Lemma 12 that $(x_1, \ldots, x_n)$ lies on the closure $\overline{\mathcal{W}}_n$ of $\mathcal{W}_n$. But there are also other constraints, resulting from the arithmetical inequalities $\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q)$ for any $i \geq 1$. These inequalities, by (3), write

$$\forall i \geq 2, \qquad x_i \leq \frac{x_1}{q^{\frac{i-1}{2}}} + \frac{q^{i-1}-1}{2gq^{\frac{i-2}{2}}}. \tag{11}$$

Let

$$\alpha = \frac{1}{\sqrt{q}}. \tag{12}$$

For $g \geq 0$, and $n \geq 2, i \geq 2$, we define

$$h_i^g(x_1, x_i) = x_i - \alpha^{i-1}x_1 - \frac{1}{2g\alpha}\left(\frac{1}{\alpha^{i-1}} - \alpha^{i-1}\right). \tag{13}$$

Then it is easily seen that (11) is equivalent to

$$h_i^g(x_1, x_i) \leq 0. \tag{14}$$

We now define

Definition 15. *Let $n \geq 1$ and $g \geq 0$. We define:*

1. *The n-th Ihara domain in genus g as*

$$\mathcal{H}_n^g = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid h_i^g(x_1, x_i) \leq 0, \ \forall\, 2 \leq i \leq n\} \tag{15}$$

2. *The n-th Ihara line in genus g as*

$$\mathcal{L}_n^g = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid h_i^g(x_1, x_i) = 0, \ \forall\, 2 \leq i \leq n\}\,. \tag{16}$$

Each $\mathcal{L}_n^g$ is a line which is identified with $\mathbb{R}$ using the first coordinate x_1 as a parameter. We denote by

$$P_n^g(x_1) = \left(x_1, \alpha x_1 + \frac{q-1}{2g}, \alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}, \ldots, \alpha^{n-1} x_1 + \frac{q^{n-1}-1}{2gq^{\frac{n-2}{2}}}\right) \tag{17}$$

the point of $\mathcal{L}_n^g$ with parameter x_1.

In the same way, for $g = \infty$, we define the *n-th Ihara infinite line* by

$$\mathcal{L}_n^\infty = \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_i = \alpha^{i-1} x_1, \ 2 \leq i \leq n\right\}.$$

It follows from this the following Proposition.

Proposition 16. *Let X be an absolutely irreducible smooth projective curve defined over the finite field $\mathbb{F}_q$ and $n \geq 2$. Then $P_n(X) = (x_1, \ldots, x_n) \in \overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$, where the x_i's are defined from X by (3).*

From this Proposition 16 and the remark below Definition 6, the strategy is the following.

> ***Strategy.*** — *For each $n \geq 1$, we minimize the coordinate function $x_1(P)$ for P lying inside the compact convex domain $\overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$. By Proposition 16, this leads to a lower bound for $x_1(P_n(X))$ for any curve X of genus g over $\mathbb{F}_q$, hence by (3) to an upper bound for the number $\sharp X(\mathbb{F}_q)$. It turns that for given q and genus g, this bound is better and better for larger and larger n, up to an optimal one.*

We are thus face to an optimization problem. Since the domain $\overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$ on which we have to minimize the convex function x_1 is also convex by Proposition 9, one has the following necessary and sufficient characterization of the minimum from [HU96, Théorème 2.2] where in our case the *active constraints* are $G_n^- = 0$ and $h_i^g = 0$ for $2 \leq i \leq n$, and where h_i^g are defined in (13).

Let $P_0 \in \overline{\mathcal{W}}_n \cap \mathcal{L}_n^g$. Suppose that:

- *for any $I \subset \{1, \ldots, n+1\}$ and $\varepsilon = \pm$ such that $G_{n,I}^\varepsilon(P_0) = 0$, there exists $\mu_I^\varepsilon \geq 0$,*

- *for any $2 \leq i \leq n$, there exists $\mu_i \geq 0$,*

such that

$$\nabla x_1(P_0) - \sum_{I \subset \{1,\ldots,n+1\}} \mu_I^- \nabla G_{n,I}^-(P_0) - \sum_{I \subset \{1,\ldots,n+1\}} \mu_I^+ \nabla G_{n,I}^+(P_0) + \sum_{i=2}^{n} \mu_i \nabla h_i^g(P_0) = 0. \tag{18}$$

Then, $x_1(P_0) = \min\{x_1 \mid (x_1,\ldots,x_n) \in \mathcal{W}_n \cap \mathcal{H}_n^g\}$.

We deduce from that the following criteria.

Criteria 17 (for minimizing x_1)**.** *If $P_0 = (x_1,\ldots,x_n) \in \overline{\mathcal{W}}_n \cap \mathcal{L}_n^g$ satisfies*

1. *$G_n^-(P_0) = 0$;*
2. *$\partial_i G_n^-(P_0) \geq 0$ for all $2 \leq i \leq n$;*
3. *$\sum_{i=1}^n \partial_i G_n^-(P_0)\alpha^{i-1} > 0$,*

then P_0 minimizes the first coordinate x_1 on $\overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$.

> **Remark** – Corollary 21 bellow states that the first requirement implies the third one.

Proof — Suppose that the assumptions of the criteria hold true. Then the system

$$\begin{cases} \left(\sum_{i=1}^n \partial_i G_n^-(P_0)\alpha^{i-1}\right)\mu_\emptyset^- = 1 \\ \mu_2 = \partial_2 G_n^-(P_0)\mu_\emptyset^- \\ \quad\vdots \\ \mu_n = \partial_n G_n^-(P_0)\mu_\emptyset^- \end{cases}$$

has a solution $\mu_\emptyset^- > 0, \mu_2 \geq 0, \ldots, \mu_n \geq 0$. As easily seen, this solution also satisfy

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} - \mu_\emptyset^- \begin{pmatrix} \partial_1 G_n^-(P_0) \\ \partial_2 G_n^-(P_0) \\ \vdots \\ \vdots \\ \partial_n G_n^-(P_0) \end{pmatrix} + \mu_2 \begin{pmatrix} -\alpha \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \mu_n \begin{pmatrix} -\alpha^{n-1} \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix},$$

hence (18) holds with the choice $\mu_I = 0$ for any $I \neq \emptyset$ and $\mu_\emptyset^+ = 0$, so that $x_1(P_0) = \min\{x_1 \mid (x_1,\ldots,x_n) \in \overline{\mathcal{W}}_n \cap \mathcal{H}_n^g\}$, and the criteria is proved. □

2.5 Weil bound and Ihara bound as bounds of order 1 and 2

We prove here that our viewpoint enables to deduce Weil bound and Ihara bound. We think that this Subsection is of interest since it shows on simple cases how this method works, especialy in the case of Ihara bound thanks to figure 1.

2.5.1 Weil bound as a bound of order 1

With this viewpoint, the usual Weil bound comes from Cauchy-Schwartz inequality applied to γ^0 and γ^1. Indeed, one have by (8)

$$\mathrm{Gram}(\gamma^0,\gamma^1)=\begin{vmatrix}1 & x_1\\ x_1 & 1\end{vmatrix}\geq 0, \qquad \text{that is} \qquad |x_1|\leq 1.$$

By (3), we have just recovered the Weil bound

$$\boxed{|\sharp X(\mathbb{F}_q)-(q+1)|\leq 2g\sqrt{q}} \qquad\qquad \textbf{(Weil ``first order'' bound)}$$

Just for fun, we can also easily recover the fact that a curve which is maximal over $\mathbb{F}_q$ must be minimal over the $\mathbb{F}_{q^{2i}}$ and maximal of the $\mathbb{F}_{q^{2i+1}}$. Indeed, being maximal over $\mathbb{F}_q$ means by (3) that $x_1=-1$, therefore

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

that is by (3) that X is minimal over $\mathbb{F}_{q^2}$. Then

$$\mathrm{Gram}(\gamma^0,\gamma^2,\gamma^3)=\begin{vmatrix}1 & 1 & x_3\\ 1 & 1 & -1\\ x_3 & -1 & 1\end{vmatrix}=-(1+x_3)^2\geq 0, \qquad \text{so that} \qquad x_3=-1,$$

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 $x_1=1$, then

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

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

2.5.2 Ihara bound as a bound of order 2

For $n=2$, the domain $\mathcal{W}_2$ recursively corresponds by item 2 of Proposition 9 and (9) to the set of $(x_1,x_2)\in\mathbb{R}^2$ satisfying:

$$\begin{cases}G_1(x_1)=1-x_1^2>0\\ G_2^+(x_1,x_2)=1-x_2>0\\ G_2^-(x_1,x_2)=1+x_2-2x_1^2>0\end{cases}, \qquad \text{that is} \qquad \begin{cases}-1<x_1<1\\ 2x_1^2-1<x_2<1\end{cases}.$$

We represent the second Weil domain $\overline{\mathcal{W}_2}$ on figure 1.

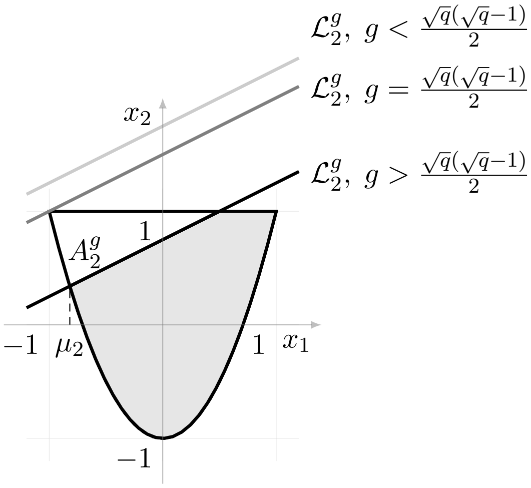

$\mathcal{L}_2^g,\ g < \frac{\sqrt{q}(\sqrt{q}-1)}{2}$
$\mathcal{L}_2^g,\ g = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$
$\mathcal{L}_2^g,\ g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}$
x_2
A_2^g
1
-1
μ_2
1
x_1
-1

Figure 1: The Weil domain $\overline{\mathcal{W}}_2$. If X is a curve over $\mathbb{F}_q$ of genus $g \geq \frac{\sqrt{q}(\sqrt{q}-1)}{2}$, then $P_2(X) = (x_1, x_2)$ as defined by (3) lies on the grey domain $\overline{\mathcal{W}}_2 \cap \mathcal{H}_2^g$, so that x_1 is lower bounded by some constant $\mu_2 = \min\{x_1(P), P \in \mathcal{W}_2 \cap \mathcal{H}_2^g\} > -1$, improving Weil bound by Proposition 16.

The second Ihara line $\mathcal{L}_2^g$ with positive slope $\alpha = \frac{1}{\sqrt{q}}$ meets the domain $\overline{\mathcal{W}}_2$ if and only if the genus is greater than the genus g_2 for which $\mathcal{L}_2^{g_2}$ contains the point $(-1, 1)$ (see figure 1), that is

$$1 = \alpha \times (-1) + \frac{1}{2g_2\alpha}\left(\frac{1}{\alpha} - \alpha\right) \qquad \Longleftrightarrow \qquad g_2 = \frac{\sqrt{q}\left(\sqrt{q}-1\right)}{2}.$$

For $g > g_2$, the constraint $h_2^g(x_1, x_2) \leq 0$ restricts the domain $\overline{\mathcal{W}}_2$ to the grey domain $\overline{\mathcal{W}}_2 \cap \mathcal{H}_n^g$, as can be seen on figure 1. The point A_2^g such that $[A_2^g, B_2^g] = \overline{\mathcal{W}}_2 \cap \mathcal{L}_2^g$ lies on the curve $G_2^- = 0$, and minimizes[3] the first coordinate x_1 on $\overline{\mathcal{W}}_2 \cap \mathcal{H}_2^g$.

μ_2 is thus the solution in $[-1, 0]$ of the quadratic equation $G_2^-(x_1, \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}) = 0$. Solving it, we find

$$\mu_2 = \frac{\alpha^2 - \sqrt{\alpha^2 + 8\left(\frac{q-1}{2g} - 1\right)}}{4},$$

so that using (3), we recover the well known Ihara bound

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

(Ihara "second order Weil" bound)

[3] It can also be trivially proved using criteria 17 since $\nabla G_2^- = \binom{-4x_1}{1}$ and $x_1(A_2^g) < 0$.

2.6 Weil bounds of higher finite orders

Following the same line, one can study Weil bounds *of order* n for $n \geq 3$. We compute in Section 2.6.1 the exact formulae for the Weil bound of order 3 and for the genus bound g_3 from which this new bound is better than the Weil bound of order 2.

For $n \geq 4$, computations to obtain explicit formula for the n-order Weil bound becomes intractable. Therefore we choose to develop an algorithm which, given a genus g and a size field q, computes the best upper order bound for the number of $\mathbb{F}_q$-rational points of a curve of genus g, together with the corresponding order n. We need to prove in Section 2.6.2 some preliminary results to justify this algorithm.

To illustrate the efficiency of the algorithm we display in Section 2.6.3 a table of numerical results for orders $n \geq 4$ and few given q, g.

2.6.1 Weil bound of order 3

For $n = 3$, we have by (10) that

$$\begin{aligned} G_3^+(x_1,x_2,x_3) &= \begin{vmatrix} 1-x_3 & x_1-x_2 \\ x_1-x_2 & 1-x_1 \end{vmatrix} && = -(1-x_1)x_3 + 1 - x_1 - (x_1-x_2)^2, \\ G_3^-(x_1,x_2,x_3) &= \begin{vmatrix} 1+x_3 & x_1+x_2 \\ x_1+x_2 & 1+x_1 \end{vmatrix} && = (1+x_1)x_3 + (1+x_1) - (x_1+x_2)^2, \end{aligned}$$

where by (8) we have $G_1^- = 1 + x_1$ and $G_1^+ = 1 - x_1$. Hence, by item 3 of Proposition 9, we have

$$\begin{aligned} \widetilde{G}_3^- &= -\left(1 + x_1 - (x_1+x_2)^2\right), \\ \widetilde{G}_3^+ &= 1 - x_1 - (x_1-x_2)^2, \end{aligned}$$

so that by item 3 of Proposition 9, we have

$$\mathcal{W}_3 = \left\{(x_1,x_2,x_3) \mid (x_1,x_2) \in \mathcal{W}_2 \quad \text{and} \quad -1 + \frac{(x_1+x_2)^2}{1+x_1} < x_3 < 1 - \frac{(x_1-x_2)^2}{1-x_1}\right\}.$$

The boundary $\partial\mathcal{W}_3 = \overline{\mathcal{W}}_3 \setminus \mathcal{W}_3$ is by item 3 of Proposition 9 the part of the 2-dimensional graphs $G_3^{\pm} = 0$ above $\overline{\mathcal{W}}_2$, and both graphs meet by Lemma 7 along a curve above the plane curve $\{(x_1,x_2) \in]-1,+1[^2; G_2(x_1,x_2) = 0\}$, where G_2 is given by (9). More precisely, above the part $G_2^+ = 0$, that is above the locus $x_2 = 1$, the two surfaces $G_3^- = 0$ and $G_3^+ = 0$ meet along the segment $(x_1, 1, x_1)$ for $-1 \leq x_1 \leq 1$. Above the curve $G_2^- = 0$, i.e. above the locus $x_2 = 2x_1^2 - 1$, one has $x_2 + x_1 = (x_1+1)(2x_1-1)$ and $x_2 - x_1 = (x_1-1)(2x_1+1)$. Therefore, $\{G_3^+ = 0\}$ and $\{G_3^- = 0\}$ above $x_2 = 2x_1^2 - 1$ are respectively

$$\begin{aligned} x_3 + 1 &= \frac{(x_1+x_2)^2}{x_1+1} = (x_1+1)(2x_1-1)^2 = 4x_1^3 - 3x_1 + 1 \text{ and } x_2 = 2x_1^2 - 1 \\ x_3 - 1 &= \frac{(x_1-x_2)^2}{x_1-1} = (x_1-1)(2x_1+1)^2 = 4x_1^3 - 3x_1 - 1 \text{ and } x_2 = 2x_1^2 - 1, \end{aligned}$$

so that their intersection above $x_2 = 2x_1^2 - 1$ is the curve $(x_1, 2x_1^2 - 1, 4x_1^3 - 3x_1)$ for $-1 \leq x_1 \leq 1$.

- Looking at figure 2, for g small the line $\mathcal{L}_3^g$ does not meet the third Weil domain $\overline{\mathcal{W}}_3$.
- As g increase, it intersects the domain inside the $G_3^+ = 0$ part, and increasing again inside the $G_3^- = 0$ part. This happens for g greater than the value g_3 such that the line $\mathcal{L}_3^{g_3}$ crosses the boundary $\partial\mathcal{W}_3$ where the two graphs $G_3^{\pm} = 0$ above $\overline{\mathcal{W}}_2$ meet. In other terms, the value g_3 is such that there exist a point

  $$P_3^g(x_1) \in \mathcal{L}_3^{g_3} \cap \overline{\mathcal{W}}_3 \cap \{G_3^- = 0\} \cap \{G_3^+ = 0\}. \tag{19}$$

  We now compute this value g_3, and the corresponding point $P_3^{g_3}(x_1) \in \mathcal{L}_3^{g_3} \cap \overline{\mathcal{W}}_3 \cap \{G_3^- = 0\} \cap \{G_3^+ = 0\}$. Using (13) and (16), there exists some $x_1 \in \mathbb{R}$, such that $(x_1, \frac{1}{g_3})$ is a solution of the two polynomials in $(x_1, \frac{1}{g})$

  $$G_3^-\left(x_1, \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}, \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}}\right) = 0 \quad \text{and} \quad G_3^+\left(x_1, \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}, \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}}\right) = 0. \tag{20}$$

  Eliminating x_1 in these equations, $\frac{1}{g_3}$ is a solution of their resultant in x_1. We have avoided calculations and factorization by hand: with the help of `magma`, we obtain that g_3 is a root of

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

  Of course, $g = -\frac{\sqrt{q}(q-1)}{\sqrt{2}} < 0$ cannot be a solution coming from a curve X. If $g = 1$ or q, substituting these values for g in (20), we find that $x_1 = \frac{q+1}{2\sqrt{q}}$ is the only corresponding solution (for both values $g = 1$ and $g = q$), which is not contained in $[-1, +1]$, so that these two values for the genus cannot come from a curve over a finite field by Weil bound (of order 1). Therefore

  $$g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}},$$

  and substituting again this value in (20), we find (using `magma`) that $x_1 = -\frac{\sqrt{2}}{2}$ is the only corresponding solution, so that, as seen above, $x_2 = 2x_1^2 - 1 = 0$ and $x_3 = 4x_1^3 - 3x_1 = \frac{\sqrt{2}}{2}$. Finally, $g = g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ is the only solution, corresponding to the point $P_3(-\frac{\sqrt{2}}{2}) = (-\frac{\sqrt{2}}{2}, 0, \frac{\sqrt{2}}{2})$, for which (19) holds.
- For $g > g_3$, the intersection of the line $\mathcal{L}_3^g$ with the domain $\overline{\mathcal{W}}_3$ is a segment $[A_3^g, B_3^g]$, where the point A_3^g lies on $G_3^- = 0$.

The point of the proof of the next Theorem is to check that, for $g > g_3$, the point $P_0 = A_3^g$ satisfies the requirements of criteria 17, showing that this point minimizes x_1 on the domain $\overline{\mathcal{W}}_3 \cap \mathcal{H}_3^g$, which contains all points coming from curves by Proposition 16.

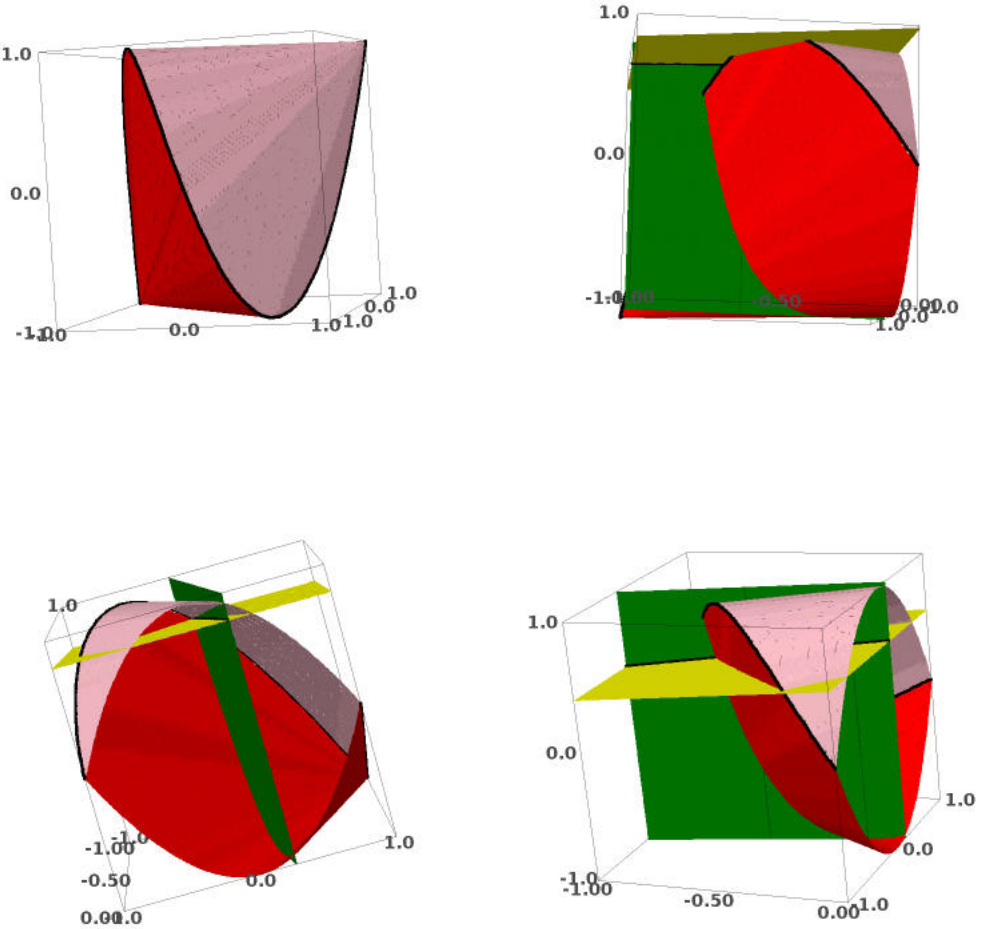


Figure 2: a complete view of the third Weil domain $\overline{\mathcal{W}}_3$ (upper left) and three partial views of $\overline{\mathcal{W}}_3 \cap \mathcal{L}_3^g$ (for $-1 \leq x_1 \leq 0$): one for $g < g_3$ (upper right), one for $g = g_3$ (bottom left) and one for $g > g_3$ (bottom right). The red (resp. pink) surface is the locus $\{G_3^- = 0\}$ (resp. $\{G_3^+ = 0\}$) above $\overline{\mathcal{W}}_2$. The dark green almost vertical plane is $x_2 = \alpha x_1 + \frac{q-1}{2g}$, the light green almost horizontal plane is $x_3 = \alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}$. Their intersection is the black third Ihara line $\mathcal{L}_3^g$ in genus g, which cuts the red surface only for $g \geq g_3$.

Theorem 18. *Let X be a smooth projective absolutely irreducible curve over $\mathbb{F}_q$ of genus g such that $g > g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}}$. Then, we have*

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

where

$$\begin{cases} a(q) &= 5 + \frac{8}{\sqrt{q}} - \frac{1}{q^2} \\ b(q) &= \frac{q-1}{q\sqrt{q}}\left(q^2 - 4q\sqrt{q} + 2q + 4\sqrt{q} - 1\right) \\ c(q) &= \frac{q-1}{4q}\left(q^3 - 5q^2 - 8q\sqrt{q} - 5q - 8\sqrt{q} + 1\right) \\ d(q) &= \frac{2\sqrt{q}(q-1)^2}{q}. \end{cases}$$

Proof — Let $g > g_3$. Referring to the last item in the discussion above the statement of the Theorem, we begin to prove that the unique $-1 < \mu_3 < 0$, such that $A_3^g = P_3(\mu_3) \in \overline{\mathcal{W}}_3 \cap \mathcal{L}_3^g \cap \{G_3^- = 0\}$, satisfies criteria 17. Then, we compute the exact value of μ_3, which is, by criteria 17 together with Proposition 16, a lower bound for x_1's coming from curve over $\mathbb{F}_q$. We deduce the Theorem using (3).

Let us prove that $P_0 = P_3(\mu_3))$ satisfies the requirements of criteria 17. The first requirement holds true: $A_3^g \in \{G_3^- = 0\}$. We prove later in corollary 21 that the third one also holds true for any $n \geq 1$. we have only to check the second requirement, that $\partial_i G_3^-(P_3^g(\mu_3)) \geq 0$ for $i = 2, 3$. Since by (10) we have

$$G_3^-(x_1, x_2, x_3) = \begin{vmatrix} 1 + x_3 & x_1 + x_2 \\ x_1 + x_2 & 1 + x_1 \end{vmatrix},$$

we deduce that for any $(x_1, x_2, x_3) \in \mathbb{R}^3$,

$$\begin{cases} \partial_2 G_3^-(P_3(x_1)) &= -2(x_1 + x_2) \\ \partial_3 G_3^-(P_3(x_1)) &= 1 + x_3. \end{cases}$$

If $x_1 = \mu_3$, then $P_0 = A_3^g = P_3(\mu_3) \in \overline{\mathcal{W}}_3 \subset]-1, +1[^3$, hence

$$\partial_3 G_3^-(P_3(\mu_3)) = 1 + x_3(P_0) > 0,$$

so that it remains to prove that $x_1(P_0) + x_2(P_0) \leq 0$.

Since $P_3(\mu_3) = A_3^g \in \{G_3^- = 0\} \cap \mathcal{L}_3^g$, we have

$$\begin{cases} (x_1 + x_2)^2 &= (1 + x_1)(1 + x_3) \\ x_3 &= \alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}. \end{cases}$$

We deduce that $P_3(\mu_3)$ lies on on the plane parabola

$$x_1 + x_2 = \pm\sqrt{(1 + x_1)\left(1 + \alpha^2 x_1 + \frac{q^2 - 1}{2g\sqrt{q}}\right)},$$

and are reduced to check that $P_3(\mu_3)$ lies on on the lower branch

$$x_1 + x_2 = -\sqrt{(1+x_1)\left(1+\alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}\right)}.$$

The point is that $(x_1, x_2) = (-1, 1)$ lies on on both branches of this parabola, and that the tangent line to the parabola at this point is the vertical one. Hence, the upper branch defines a concave subset

$$\left\{(x_1, x_2) \mid x_1 \geq -1, \quad x_2 \geq 1 \quad \text{and} \quad x_1 + x_2 \leq \sqrt{(1+x_1)\left(1+\alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}\right)}\right\}$$

of $\mathbb{R}^2$, containing $(-1, 1)$ and $(0, \sqrt{1+\frac{q^2-1}{2g\sqrt{q}}})$ with $\sqrt{1+\frac{q^2-1}{2g\sqrt{q}}} > 1$. It follows that for any $-1 < x_1 < 0$, a point (x_1, x_2) lying on the upper parabolic branch lies also on the locus $x_2 > 1$, which cannot hold for $P_0 = P_3(\mu_3)) \in \overline{\mathcal{W}}_3 \subset [-1, -1]^3$.

It follows that all requirements of criteria 17 hold true for the point $P_3(\mu_3)$, which lies on the branch $x_1 + x_2 = -\sqrt{(1+x_1)(1+\alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}})$, so that μ_3 is a lower bound on $\overline{\mathcal{W}}_3 \cap \mathcal{H}_3^g$ for $g > g_3$.

Since $P_3(\mu_3)$ lies on $\mathcal{L}_3^g$, it lies in particular on $x_2 = \alpha x_1 + \frac{q-1}{2g}$, so that μ_3 is a solution of the quadratic equation

$$(x_1 + \alpha x_1 + \frac{q-1}{2g})^2 = (1+x_1)(1+\alpha^2 x_1 + \frac{q^2-1}{2g\sqrt{q}}),$$

where we recall that $\alpha = \frac{1}{\sqrt{q}}$. Solving this equation proves that the only solution in $[-1, 0]$ is

$$\mu_3 = \frac{\frac{q-1}{q} - \frac{2\sqrt{q}(q-1)^2}{gq} - \sqrt{a(q) + \frac{b(q)}{g} + \frac{c(q)}{g^2}}}{2},$$

hence the Theorem using (3). □

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

Corollary 19. *The Ihara constant $A(q)$ is bounded above by:*

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

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. We prove later in Theorem 22 that we can also recover Dinfeld-Vlăduţ and Tsfasman bounds with this viewpoint.

2.6.2 General features

The idea of the algorithm producing numerical values for higher order Weil bounds for given g, q is the following. It computes numerically in a first step an approximation of the unique $-1 \leq x_1 < 0$ for which $P_n(x_1)$ lies on the intersection of $\mathcal{L}_n^g$ with $G_n^- = 0$, and it checks numerically in a second step that this point satisfies criteria 17. This algorithm is valid thanks to Proposition 20 that such an x_1 as in the first step do exists, at least for g large enough.

Proposition 20. *There exists a sequence $(g_n)_{n\geq 2}$ such that $g > g_n$ if, and only if, the intersection of the n-th Ihara line $\mathcal{L}_n^g$ in genus g with the interior of the n-the Weil domain $\mathcal{W}_n$ is a non-empty x_1-segment $]A_n^g, B_n^g[$, with A_n^g lies on on the hypersurface of $\overline{\mathcal{W}}_{n-1} \times \mathbb{R}$ having equation $G_n^- = 0$, and with $-1 \leq x_1 < 0$.*

Proof — We keep notations of Section 2.4 and we begin by studying the infinite line $\mathcal{L}_n^\infty = \{(x_1, \alpha x_1, \ldots, \alpha^{n-1}x_1),\ x_1 \in \mathbb{R}\}$, whose points are the $P_n^\infty(x_1)$ for $x_1 \in \mathbb{R}$. This line $\mathcal{L}_n^\infty$ and the domain $\mathcal{W}_n$ have a non empty intersection since the origin of $\mathbb{R}^n$ belongs to $\mathcal{W}_n \cap \mathcal{L}_n^\infty$. Since $\mathcal{W}_n$ is convex and open, $\mathcal{W}_n \cap \mathcal{L}_n^\infty$ must be a non empty segment $]P_n^\infty(\mu_n^\infty), P_n^\infty(\nu_n^\infty)[$ for some $-1 \leq \mu_n^\infty < \nu_n^\infty \leq 1$. Necessarily $\mu_n^\infty < 0$ and[4] $\overline{\mathcal{W}}_n \cap \mathcal{L}_n^\infty = [P_n^\infty(\mu_n^\infty), P_n^\infty(\nu_n^\infty)]$.

Next, we prove that the point $P_n^\infty(\mu_n^\infty)$ lies on the hypersurface of $\mathcal{W}_{n-1} \times \mathbb{R}$ having equation $G_n^- = 0$. To relieve the notations, for $\epsilon = \pm$ or nothing, we put $L_n^\epsilon(x_1) = G_n^\epsilon(x_1, \alpha x_1, \ldots, \alpha^{n-1}x_1)$. Let us prove by induction that the abscissa μ_n^∞ satisfy

$$\forall n \geq 1, \qquad L_n^-(\mu_n^\infty) = 0 \text{ and } L_m(\mu_n^\infty) > 0,\ \forall m < n. \tag{21}$$

For $n = 1$ this is true from (8): $\mu_1 = -1$ is the only root of $L_1(x_1) = 1 + x_1$ and satisfies $L_0(-1) > 0$ since $L_0 = 1$. Suppose that assertion (21) holds true for some $n \geq 1$. By Lemma 7, one has

$$2\,\underbrace{L_n(\mu_n^\infty)}_{=0} = \underbrace{L_{n-1}^+(\mu_n^\infty)}_{>0}\, L_{n+1}^-(\mu_n^\infty) + \underbrace{L_{n-1}^-(\mu_n^\infty)}_{>0}\, L_{n+1}^+(\mu_n^\infty),$$

where the underbrace (in)equalities come from the induction hypotheses. We first establish that $L_{n+1}^+(\mu_n^\infty) > 0$. To this end, let m be the quotient of $n+2$ by 2. By Lemma 5, one has $G_{n+1}^+ = \mathrm{Det}(T_m - H_m)$, where T_m is a Toeplitz given by (6), while H_m is Hankel given by (7). Specializing to the point $(\mu_n^\infty, \alpha\mu_n^\infty, \ldots, \alpha^n\mu_n^\infty)$, the Hankel part becomes a rank one matrix:

$$-H_m = \alpha^{\frac{(-1)^{n+1}+1}{2}} \times (-\mu_n^\infty) \times {}^t(\alpha^{m-1}, \ldots, \alpha, 1) \times (\alpha^{m-1}, \ldots, \alpha, 1).$$

This matrix is clearly symmetric positive semi definite. But, for general A and B positive semi-definite symmetric matrices, one has $\det(A + B) \geq \det(A)$ (easy consequence of

[4] If $\mathcal{O}$ is a convex open subspace of $\mathbb{R}^n$, for any $x \in \mathcal{O}$ and any $y \in \overline{\mathcal{O}}$, the segment $]x, y[$ is included in $\mathcal{O}$.

[HJ90, Corollary 4.3.3]). We deduce by induction hypothesis that, for some $z \in \mathbb{R}^{2n}$,

$$\begin{aligned} L^+_{n+1}(\mu_n^\infty) &= \mathrm{Det}\left(T_m(1, \mu_n^\infty, \dots, \alpha^{m-2}\mu_n^\infty) + H_m(z)\right) \\ &\geq \mathrm{Det}(T_m(1, \mu_n^\infty, \dots, \alpha^{m-2}\mu_n^\infty)) = G_{m-1}(\mu_n^\infty, \dots, \alpha^{m-2}\mu_n^\infty) = L_{m-1}(\mu_n^\infty) > 0 \end{aligned}$$

holds true. It then follows by (2.6.2) that $L^-_{n+1}(\mu_n^\infty) < 0$. Since $L_{n+1}(0) = 1$, there exists $\mu \in]\mu_n^\infty, 0[$ such that $L_{n+1}(\mu) = 0$. Since the points $P_n^\infty(x_1)$ with $x_1 \in]\mu_n^\infty, 0[$ of the line $\mathcal{L}_n^\infty$ belong to $\mathcal{W}_n$, this is the case for the point $P_n^\infty(\mu)$. Hence one must have $L_m(\mu) > 0$ for all $m \leq n$ and $L_{n+1}(\mu) = 0$. This proves that point $P_{n+1}^\infty(\mu)$ belongs to $\overline{\mathcal{W}}_{n+1}$ and that $\mu = \mu_{n+1}$. This concludes the induction, hence in particular $G_n^-(P_n^\infty(\mu_n^\infty)) = L_n^-(P_n^\infty(\mu_n^\infty)) = 0$ as asserted, with moreover $-1 \leq \mu_n^\infty < 0$.

Now for finite genus, formula (13) shows that the union $\mathcal{P}_n = \cup_{g \in]0,+\infty]}\mathcal{L}_n$ is a closed half linear 2-dimensional plane with parameters $\left(x_1 \in \mathbb{R}, \frac{1}{g} \in [0, +\infty[\right)$. Hence the intersection $\mathcal{P}_n \cap \mathcal{W}_n$ is a 2-dimensional convex subset in the closed half plane $\mathcal{P}_n$. Moreover, we have just seen above that the cut out with the line having parameter $\frac{1}{g} = 0$ meet it on an non-empty segment with an end $A_n^\infty = P_n(\mu_n^\infty) \in \{G_n^- = 0\}$ with $-1\|eq\mu_n^\infty < 0$. Since by Proposition 10 the locus $\{(x_1, \dots, x_n) \in \mathcal{W}_{n-1} \mid G_n^-(x_1, \dots, x_n) > 0\}$ is convex, this segment is non empty and meet $G_n^- = 0$ for at least one point with $x_1 < 0$ for a connected subset of the parameter $0 \leq \frac{1}{g} < +\infty$ containing 0, hence have the form $0 \leq \frac{1}{g} < \frac{1}{g_n}$ for some $0 < g_n < +\infty$. for such a g, the cut out with $\mathcal{L}_n^g$ is a segment $[A_n^g, B_n^g]$, with $A_n^g \neq B_n^g$ since $g > g_n$, with $A_n^g \in \{G_3^- = 0\}$ and with $-1 \leq x_1(A_n^g) < 0$. The Proposition is proved. □

It turns out that under the assumption that a point on $\mathcal{L}_n^g$ lies on the locus $\overline{\mathcal{W}}_n \cap \{G_n^- = 0\}$ always satisfy the last requirement of criteria 17:

Corollary 21. *Let $n \in \mathbb{N}$, $g > g_n$ and $\mu_n \in]-1, 0[$ such that $P_n^g(\mu_n)$ is the point A_n^g of Proposition 20. Then $\sum_{i=1}^n \partial_i G_n^-(P_n^g(\mu_n))\alpha^{i-1} > 0$.*

Proof — Denote by $\varphi(x_1) = G_n^-(P_n^g(x_1))$ for $x_1 \in \mathbb{R}$. This is a $\mathcal{C}^\infty$ function of the real variable x_1.

By assumption, $P_n^g(\mu_n) \in \{G_n^- = 0\} \cap \mathcal{L}_n^g$ and $g > g_n$, hence by Proposition 9 and Proposition 20 we have $P_n^g(\mu_n) = A_n^g$ and $]P_n^g(\mu_n), B_n^g[\subset \mathcal{W}_n \subset \{G_n^- > 0\}$, and there exists some $\varepsilon > 0$, such that

$$\forall x_1 \in \mathbb{R}, \quad \mu_n < x_1 < \mu_n + \varepsilon \Longrightarrow P_n^g(x_1) \in \{G_n^- > 0\}. \tag{22}$$

Hence by item 2 of Proposition 9, we have $P_n^g(x_1) \in \{G_n^- > 0\}$ for $\mu_n < x_1 < \mu_n + \varepsilon$, so that $\varphi(x_1) > 0$ for such x_1. Since by assumption $\varphi(\mu_n) = 0$, we deduce that

$$0 \leq \frac{\mathrm{d}\varphi}{\mathrm{d}t}(\mu_n) = \frac{\mathrm{d}G_n^-(P_n^g(\mu_n))}{\mathrm{d}t} = \sum_{i=1}^n \partial_i G_n^-(P_n^g(\mu_n))\alpha^{i-1} = \left\langle \nabla G_n^-(\mu_n), \vec{u} \right\rangle,$$

where $\vec{u} = (1, \alpha, \dots, \alpha^{n-1})$ is a director vector of $\mathcal{L}_n^g$. Now, suppose by contradiction that $\frac{\mathrm{d}\varphi}{\mathrm{d}t}(\mu_n) = 0$. Then by (2.6.2) the line $\mathcal{L}_n^g$ would be perpendicular to $\nabla G_n^-(\mu_n^\infty)$, hence tangent to $\{G_n^- = 0\}$ at $P_n^g(\mu_n) = A_n^g$ by Proposition 20. But $\{G_n^- \geq 0\} \cap \overline{\mathcal{W}}_{n-1}$ is convex by Proposition 10, so that $\mathcal{L}_n^g$ would never meet the interior $\{G_n^- = 0\}$, a contradiction with (22). □

It turns out that proving that this points is also always a minimum of the coordinate function x_1 seems to be difficult for $N \geq 4$. But this is an easy task numerically using criteria 17: this will be done in our `magma` routine in Section 2.6.3.

2.6.3 Numerical results for $n \geq 4$

We have implemented a routine in `magma` and leading to the following results.

In the following tabular we give, for genus g such that $1 \leq g \leq 52$, and for $q \in \{2, 3\}$, the best generalized Weil bound for the number of points on a curve of genus g over $\mathbb{F}_q$. The number in brackets corresponds to the *optimal* order Weil bound. For instance, if this number is 2, this means that the bound is the well known Ihara bound and that bounds of other orders are not better.

g	$q=2$	$q=3$	g	$q=2$	$q=3$	g	$q=2$	$q=3$	g	$q=2$	$q=3$
1	5(3)	7(2)	14	16(6)	26(4)	27	25(8)	42(5)	40	34(9)	57(6)
2	6(3)	9(2)	15	17(7)	28(4)	28	26(8)	43(5)	41	35(9)	58(6)
3	7(4)	10(3)	16	18(7)	29(5)	29	27(8)	44(5)	42	35(9)	59(6)
4	8(4)	12(3)	17	18(7)	30(5)	30	27(8)	46(5)	43	36(9)	60(6)
5	9(5)	14(3)	18	19(7)	31(5)	31	28(8)	47(5)	44	37(9)	61(6)
6	10(5)	15(3)	19	20(7)	32(5)	32	29(8)	48(6)	45	37(9)	62(6)
7	11(5)	17(4)	20	21(7)	34(5)	33	29(8)	49(6)	46	38(9)	63(6)
8	11(5)	18(4)	21	21(7)	35(5)	34	30(8)	50(6)	47	38(9)	65(6)
9	12(6)	19(4)	22	22(7)	36(5)	35	31(8)	51(6)	48	39(9)	66(6)
10	13(6)	21(4)	23	23(7)	37(5)	36	31(8)	52(6)	49	40(9)	67(6)
11	14(6)	22(4)	24	23(8)	38(5)	37	32(8)	54(6)	50	40(9)	68(6)
12	15(6)	24(4)	25	24(8)	40(5)	38	33(9)	55(6)	51	41(9)	69(6)
13	15(6)	25(4)	26	25(8)	41(5)	39	33(9)	56(6)	52	42(9)	70(6)

Comparing with the results available on the web site `http://www.manypoints.org/`, we unfortunately observe that we do not beat any record, and that we reach the records exactly in those cases were it is held by Osterlé bounds! . So we are pretty sure that there is a link between Osterle bound and the one in this Section, even if we do not know how to relate the two approaches.

2.7 Drinfeld-Vlăduţ and Tsfasman bounds as a bound of infinite order

In this Section, we recover the Drinfeld-Vlăduţ and Tsfasman bounds for the asymptotic of the number of points on curves over $\mathbb{F}_q$, giving a new meaning for the defect δ defined in [Tsf92]. With our point of view, these bounds can be considered as Weil bounds of infinite order.

We consider a sequence $(X_n)_{n\geq 1}$ of absolutely irreducible smooth projective curves over $\mathbb{F}_q$. Let $(g_n)_{n\geq 1}$ be the genus sequence and for $r \geq 1$ and let $B_r(X_n)$ be the number of points of degree r on X_n:

$$B_r(X_n) = \sharp \left\{ P \in X_n(\overline{\mathbb{F}}_q) \mid \deg(P) = r \right\}.$$

Following Tsfasman, we assume this sequence to be *asymptotically exact*: this means that $\lim_{n\to+\infty} g_n = +\infty$ and that for any $r \geq 1$, the sequence $\left(\frac{B_r(X_n)}{g_n}\right)_{n\geq 1}$ admits a limit. Then, as usual, we put

$$\forall r \geq 1, \qquad \beta_r \overset{\text{def}}{=} \lim_{n\to+\infty} \frac{B_r(X_n)}{g_n}.$$

In the following Theorem, the notations and the normalizations are the same as in Definitions 2 and 4.

Theorem 22. *Let $(X_n)_{n\geq 1}$ be a sequence of absolutely irreducible smooth projective curves over $\mathbb{F}_q$. If this sequence is asymptotically exact, then its* defect δ, *defined as $\delta = 1 - \sum_{r=1}^{\infty} \frac{r\beta_r}{\sqrt{q^r}-1}$, satisfy*

$$\delta = \lim_{m\to+\infty} \lim_{n\to+\infty} \frac{\left\|\gamma_{X_n}^0 + \gamma_{X_n}^1 + \cdots + \gamma_{X_n}^{m-1}\right\|_{X_n}^2}{m}.$$

Proof — Thanks to the Gram matrix following Definition 4, we compute

$$\begin{aligned}
\frac{1}{m}\left\|\sum_{i=0}^{m-1}\gamma_{X_n}^i\right\|_{X_n}^2 &= \frac{1}{m}\begin{pmatrix}1 & \cdots & 1\end{pmatrix} \times \operatorname{Gram}\left(\gamma_{X_n}^0, \ldots, \gamma_{X_n}^{m-1}\right) \times \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}\\
&= \frac{1}{m}\left[m + 2\sum_{i=1}^{m-1}(m-i)x_i\right]\\
&= 1 + \frac{1}{m}\sum_{i=1}^{m-1}(m-i)\frac{(q^i+1) - \sharp X_n(\mathbb{F}_{q^i})}{g_n q^{\frac{i}{2}}}\\
&= 1 + \frac{1}{g_n}\sum_{i=1}^{m-1}(m-i)\left(q^{\frac{i}{2}} + q^{-\frac{i}{2}}\right) - \sum_{i=1}^{m-1}\left(1 - \frac{i}{m}\right)\sum_{r|i}\frac{r}{q^{\frac{i}{2}}} \times \frac{B_r(X_n)}{g_n}.
\end{aligned}$$

Letting n tends to $+\infty$ leads to

$$\lim_{n\to+\infty}\frac{1}{m}\left\|\sum_{i=0}^{m-1}\gamma_{X_n}^i\right\|_{X_n}^2 = 1 - \sum_{rs\leq m-1}\left(1 - \frac{rs}{m}\right)\frac{r\beta_r}{q^{\frac{rs}{2}}} = 1 - \sum_{r=1}^{m-1}\left(\sum_{s=1}^{\lfloor\frac{m-1}{r}\rfloor}\left(1 - \frac{rs}{m}\right)\frac{1}{q^{\frac{rs}{2}}}\right)r\beta_r. \tag{23}$$

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 converging serie, the first term of the last expression tends to zero when $m \to +\infty$; as for the second term it also tends to zero by Cesaro. 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 (23). □

Just pointing out that a norm is non-negative, Theorem 22 leads to the well-known bound:

$$\boxed{\sum_{r=1}^{\infty} \frac{r\beta_r}{\sqrt{q^r}-1} \leq 1.} \qquad \textbf{(Tsfasman)}$$

As is well known, Tsfasman bound is itself a refinement of

$$\boxed{\limsup_{n \to +\infty} \frac{\sharp X_n(\mathbb{F}_q)}{g_n} \leq \sqrt{q} - 1.} \qquad \textbf{(Drinfeld-Vlăduţ)}$$

3 Relative bounds

From now on, we concentrate on the relative situation. Our starting point is a finite morphism $f : X \to Y$ of degree d, where X and Y are absolutely irreducible smooth projective curves defined over $\mathbb{F}_q$, whose genus are denoted by g_X and g_Y.

3.1 The relative Neron-Severi subspace

The morphism $f \times f$ from $X \times X$ to $Y \times Y$ induces two morphisms

$$(f \times f)_* : \mathrm{NS}(X \times X)_{\mathbb{R}} \longrightarrow \mathrm{NS}(Y \times Y)_{\mathbb{R}} \quad \text{and} \quad (f \times f)^* : \mathrm{NS}(Y \times Y)_{\mathbb{R}} \longrightarrow \mathrm{NS}(X \times X)_{\mathbb{R}}$$

satisfying $(f \times f)_* \circ (f \times f)^* = d^2 \,\mathrm{Id}_{Y \times Y}$. We put:

$$\varphi = \frac{1}{d}(f \times f)_* \qquad \text{and} \qquad \psi = \frac{1}{d}(f \times f)^*. \tag{24}$$

Each of these morphisms can be restricted to the euclidean spaces $(\mathcal{E}_X, \langle\cdot,\cdot\rangle_X)$ and $(\mathcal{E}_Y, \langle\cdot,\cdot\rangle_Y)$ associated to the curves X and Y as in Section 1. Recall that both are the image of the orthogonal projections given by (1):

$$p_X : \mathrm{NS}(X \times X)_{\mathbb{R}} \longrightarrow \mathcal{E}_X \qquad \text{and} \qquad p_Y : \mathrm{NS}(Y \times Y)_{\mathbb{R}} \longrightarrow \mathcal{E}_Y.$$

In fact, we still restrict a little bit more the morphisms φ and ψ. Let $F_X : X \to X$ and $F_Y : Y \to Y$ be the q-Frobenius on X and Y. As usual, for $k \geq 0$, we denote by $\Gamma^k_{F_X}$ the class in $\mathrm{NS}(X \times X)_{\mathbb{R}}$ of the k-th iterated of F_X. We do the same for $\Gamma^k_{F_Y}$ inside $\mathrm{NS}(Y \times Y)_{\mathbb{R}}$.

Definition 23. *For $i \geq 0$, we put:*

$$\gamma^i_X = \frac{1}{\sqrt{2q^i}} p_X\left(\Gamma^i_{F_X}\right) \in \mathcal{E}_X, \qquad \gamma^i_Y = \frac{1}{\sqrt{2q^i}} p_Y\left(\Gamma^i_{F_Y}\right) \in \mathcal{E}_Y,$$

and we denote by $\mathcal{F}_X$ and $\mathcal{F}_Y$ the two subspaces of $\mathcal{E}_X$ and $\mathcal{E}_Y$ defined by

$$\mathcal{F}_X = \mathrm{Vect}\left(\gamma^i_X,\ i \geq 0\right) \subset \mathcal{E}_X, \qquad \mathcal{F}_Y = \mathrm{Vect}\left(\gamma^i_Y,\ i \geq 0\right) \subset \mathcal{E}_Y.$$

> **Remark** – Note that the normalization in this Section differs from the one chosen in Definition 3 by a factor $\frac{1}{\sqrt{g}}$. The nice feature of this new normalization is that with this choice, the pull-back of divisor classes between some subspaces of the Neron Severi spaces is isometric, see the next Proposition 24.

For $i \geq 0$ and $j \geq 1$, one has by Lemma 3, with this new normalization for γ^i,

$$\left\|\gamma^i_X\right\|_X = \sqrt{g_X}, \qquad \left\langle \gamma^i_X, \gamma^{i+j}_X \right\rangle_X = \frac{(q^j+1) - \sharp X(\mathbb{F}_{q^j})}{2\sqrt{q^j}}, \tag{25}$$

$$\left\|\gamma^i_Y\right\|_Y = \sqrt{g_Y}, \qquad \left\langle \gamma^i_Y, \gamma^{i+j}_Y \right\rangle_Y = \frac{(q^j+1) - \sharp Y(\mathbb{F}_{q^j})}{2\sqrt{q^j}}. \tag{26}$$

In other words, the vectors γ^i_X for $i \geq 0$ lie on in the euclidean sphere of radius $\sqrt{g_X}$ in the finite dimensional euclidean vector space $\mathcal{E}_X$, and the data of the scalar products is equivalent to the datas of the numbers of rational points of X on the finite extensions of $\mathbb{F}_q$.

Proposition 24. *Restricted respectively to $\mathcal{F}_X$ and $\mathcal{F}_Y$, the morphisms φ and ψ satisfy the followings.*

1. *One has $\varphi \circ \psi = \mathrm{Id}_{\mathcal{F}_Y}$, the identity map on $\mathcal{F}_Y$.*
2. *For all $i \geq 0$, $\varphi(\gamma^i_X) = \gamma^i_Y$.*
3. *For all $\gamma \in \mathcal{F}_X$ and all $\delta \in \mathcal{F}_Y$, $\langle \gamma, \psi(\delta) \rangle_X = \langle \varphi(\gamma), \delta \rangle_Y$.*
4. *For all $i, j \geq 0$, $\left\langle \psi(\gamma^i_Y), \psi(\gamma^j_Y) \right\rangle_X = \left\langle \gamma^i_Y, \gamma^j_Y \right\rangle_Y$.*
5. *The morphism ψ is an isometric embedding $(\mathcal{F}_Y, \langle \cdot, \cdot \rangle_Y) \hookrightarrow (\mathcal{F}_X, \langle \cdot, \cdot \rangle_X)$ and $\psi \circ \varphi$ is the orthogonal projection of $\mathcal{F}_X$ on its subspace $\psi(\mathcal{F}_Y)$.*

Proof — Item (1) follows from the identity $(f \times f)_* \circ (f \times f)^* = d^2\, \mathrm{Id}_{Y \times Y}$. Item (2) follows from the identity $(f \times f)_* \Gamma_{F^i_X} = d\Gamma_{F^i_Y}$. Item (3) follows from the projection formula for the proper morphism $f \times f : X \times X \to Y \times Y$. Item (4) follows then from items (1) and (3). Finally, item (5) follow from the preceding ones together with the following Lemma. □

Lemma 25. *Let $(E, \langle ., . \rangle_E)$ and $(F, \langle ., . \rangle_F)$ be two finite dimensional euclidean vector spaces. Suppose that E is generated by a family $\{u_i, i \geq 0\}$ and F is generated by a family $\{v_j, j \geq 0\}$. Let $\varphi : E \to F$ and $\psi : F \to E$ be linear maps satisfying $\varphi \circ \psi = \mathrm{Id}_F$ and such that*

$$\langle \psi(v_i), \psi(v_j) \rangle_E = \langle v_i, v_j \rangle_F, \qquad \forall i, j \geq 0, \tag{27}$$

$$\langle v, \varphi(u) \rangle_F = \langle \psi(v), u \rangle_E, \qquad \forall u \in E, \forall v \in F. \tag{28}$$

Then, ψ is an isometric embedding from F to E and $\psi \circ \varphi$ is the orthogonal projection from E to $\psi(F)$.

Proof — By (27), the morphism ψ must be an isometric embedding. Let us prove that $\psi \circ \varphi$ is the orthogonal projection on $\psi(F)$. Since $\varphi \circ \psi = \mathrm{Id}_F$, we have $(\psi \circ \varphi)^2 = \psi \circ \varphi \circ \psi \circ \varphi = \psi \circ \varphi$; therefore $\psi \circ \varphi$ is a projector. For $v \in F$, one has $\psi \circ \varphi(\psi(v)) = \psi(v)$, again by $\varphi \circ \psi = \mathrm{Id}_F$; in other terms $\psi(F)$ is stabilized by $\psi \circ \varphi$. Last, for $u \in E$, one has $u - \psi \circ \varphi(u) \in \psi(F)^\perp$. Indeed, for $v \in F$, one has:

$$\begin{aligned}
\langle u - \psi \circ \varphi(u), \psi(v) \rangle_E &= \langle u, \psi(v) \rangle_E - \langle \psi \circ \varphi(u), \psi(v) \rangle_E \\
&= \langle \varphi(u), v \rangle_F - \langle \varphi(u), v \rangle_F \qquad \text{by (28)} \\
&= 0.
\end{aligned}$$

This concludes the proof. □

Definition 26. *Let $\mathcal{F}_{X/Y}$ be the subspace $\psi(\mathcal{F}_Y)$, called the* relative subspace *for the morphism $X \to Y$.*

Then we have just proved that

$$\begin{array}{ccccc}
\mathcal{F}_X & = & \mathcal{F}_{X/Y} & \oplus & \mathcal{F}_{X/Y}^\perp \\
\Cup & & \Cup & & \Cup \\
u & = & \psi \circ \varphi(u) & + & (u - \psi \circ \varphi(u))
\end{array}$$

Remark – The absolute case of Section 2 enters in this relative case by choosing any non-constant rational function $X \to \mathbb{P}^1$; in this case, the relative space $\mathcal{F}_{X/\mathbb{P}^1}$ is the sub-space of $\mathcal{E}_X$ generated by the projections of the classes of iterations of the Frobenius morphism.

We are now able to easily compute some norms and scalar products.

Lemma 27. *For any $i \geq 0$, the following decomposition holds true:*

$$\gamma_X^i = \underbrace{\psi(\gamma_Y^i)}_{\in \mathcal{F}_{X/Y}} + \underbrace{\left(\gamma_X^i - \psi(\gamma_Y^i)\right)}_{\in \mathcal{F}_{X/Y}^\perp} \in \mathcal{F}_X$$

and one has:

$$\forall i, j \geq 0, \qquad \psi(\gamma_Y^i) \perp \gamma_X^j - \psi(\gamma_Y^j) \tag{29}$$

$$\forall i \geq 0, \qquad \left\| \gamma_X^i - \psi(\gamma_Y^i) \right\|_X = \sqrt{g_X - g_Y} \tag{30}$$

$$\forall i \geq 0, \forall j \geq 1, \qquad \left\langle \gamma_X^i - \psi(\gamma_Y^i), \gamma_X^{i+j} - \psi(\gamma_Y^{i+j}) \right\rangle_X = \frac{\sharp Y(\mathbb{F}_{q^j}) - \sharp X(\mathbb{F}_{q^j})}{2\sqrt{q^j}}. \tag{31}$$

Proof — The first norm calculation is just a consequence of Pythagore Theorem:

$$\begin{aligned} \left\|\gamma_X^i\right\|_X^2 &= \left\|\psi(\gamma_Y^i)\right\|_X^2 + \left\|\gamma_X^i - \psi\left(\gamma_Y^i\right)\right\|_X^2 && \text{by Pythagore} \\ &= \left\|\gamma_Y^i\right\|_Y^2 + \left\|\gamma_X^i - \psi\left(\gamma_Y^i\right)\right\|_X^2 && \text{since } \psi \text{ isometric} \end{aligned}$$

and thus by (25) and (26)

$$g_X = g_Y + \left\|\gamma_X^i - \psi\left(\gamma_Y^i\right)\right\|_X^2 .$$

Taking intby o account orthogonality, we also easily compute the scalar product:

$$\begin{aligned} \left\langle \gamma_X^i - \psi(\gamma_Y^i), \gamma_X^{i+j} - \psi(\gamma_Y^{i+j}) \right\rangle_X &= \left\langle \gamma_X^i, \gamma_X^{i+j} \right\rangle_X - \left\langle \psi\left(\gamma_Y^i\right), \psi\left(\gamma_Y^{i+j}\right) \right\rangle_X && \text{by orthogonality} \\ &= \left\langle \gamma_X^i, \gamma_X^{i+j} \right\rangle_X - \left\langle \gamma_Y^i, \gamma_Y^{i+j} \right\rangle_Y && \text{since } \psi \text{ isometric} \\ &= \frac{(q^j+1) - \sharp X(\mathbb{F}_{q^j})}{2\sqrt{q^j}} - \frac{(q^j+1) - \sharp Y(\mathbb{F}_{q^j})}{2\sqrt{q^j}} && \text{by (25) and (26).} \end{aligned}$$

The result follows. □

3.2 Number of points in coverings

As applications of this Proposition, we prove in the very same spirit than in Section 2 the following three results. The first one is well known, the others are new. It worth to notice that the first one can be proved using Tate modules of the jacobians of the involved curves (see e.g. [AP95]), whereas up to our knowledge, the others cannot.

Proposition 28. *Suppose that there exists a finite morphism $X \to Y$. Then we have*

$$|\sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)| \leq 2(g_X - g_Y)\sqrt{q}.$$

Proof — We apply Cauchy-Schwartz inequality to the vectors $\gamma_X^0 - \psi(\gamma_Y^0)$ and $\gamma_X^1 - \psi(\gamma_Y^1)$. Thanks to Lemma 27 specialized to $j = 1$ and $i = 0, 1$, we obtain

$$\begin{aligned} \left|\frac{\sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)}{2\sqrt{q}}\right|^2 &= \left|\langle \gamma_X^0 - \psi(\gamma_Y^0), \gamma_X^1 - \psi(\gamma_Y^1)\rangle_X\right|^2 \\ &\leq \|\gamma_X^0 - \psi(\gamma_Y^0)\|_X^2 \times \|\gamma_X^1 - \psi(\gamma_Y^1)\|_X^2 \\ &= (g_X - g_Y)^2, \end{aligned}$$

hence the Proposition. □

The following Proposition is the relative form of Proposition 14. Of course, although less nice, such upper bounds can be given for any n.

Proposition 29. *For any finite morphism $X \to Y$ with $g_X \neq g_Y$, we have*

$$\sharp X(\mathbb{F}_{q^2}) - \sharp Y(\mathbb{F}_{q^2}) \leq 2(g_X - g_Y)q - \frac{\left(\sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)\right)^2}{g_X - g_Y}.$$

Proof — After computating the 3×3 Gram determinant

$$G_3(X/Y) = \mathrm{Gram}(\gamma_X^0 - \psi(\gamma_Y^0), \gamma_X^1 - \psi(\gamma_Y^1), \gamma_X^2 - \psi(\gamma_Y^2))$$

using Lemma 27, it is readily seen, with the very same proof, that factorization in Lemma 5 holds also in this relative case, so that there exists two (explicitly given as determinants) factors $G_n^+(X/Y)$ and $G_n^-(X/Y)$ ($n = 2$ is sufficient here) as in Definition 6, such that $G_n(X/Y) = G_n^+(X/Y) \times G_n^-(X/Y)$ also holds. Moreover, Proposition 9 also continue to hold, hence for $n = 2$, the result follows from $G_2^-(X/Y) \geq 0$. □

3.3 Number of points in a fiber product

Let

$$\begin{tikzcd}
 & Y_1 \arrow[dr, "f_1"] & \\
X \arrow[ur, "p_1"] \arrow[dr, "p_2"'] & & Z \\
 & Y_2 \arrow[ur, "f_2"'] &
\end{tikzcd} \tag{32}$$

be a commutative diagram of finite covers of absolutely irreducible smooth projective curves defined over $\mathbb{F}_q$. Applying the results of the beginning of this Section to the four morphisms involved in this diagram leads to another diagram between Euclidean spaces

$$\begin{tikzcd}
 & \mathcal{F}_{Y_1} \arrow[dl, dashed, bend right, "\varphi_{Y_1/Z}"'] \arrow[dr, hook, "\psi_{X/Y_1}"] & \\
\mathcal{F}_Z \arrow[ur, hook, "\psi_{Y_1/Z}"] \arrow[dr, hook, "\psi_{Y_2/Z}"'] & & \mathcal{F}_X \arrow[ul, dashed, bend right, "\varphi_{X/Y_1}"'] \arrow[dl, dashed, bend left, "\varphi_{X/Y_2}"] \\
 & \mathcal{F}_{Y_2} \arrow[ul, dashed, bend left, "\varphi_{Y_2/Z}"] \arrow[ur, hook, "\psi_{X/Y_2}"'] &
\end{tikzcd}$$

Let us introduce the following hypothesis:

(H) *The fiber product $Y_1 \times_Z Y_2$ is abolutely irreducible and smooth.*

Proposition 30. *Suppose that (H) holds, and that $X = Y_1 \times_Z Y_2$ in diagram (32). Then*

$$\varphi_{X/Y_2} \circ \psi_{X/Y_1} = \psi_{Y_2/Z} \circ \varphi_{Y_1/Z}$$

on $\mathcal{F}_{Y_1}$.

Proof — The proof of formula (30) is mainly set theoretic. We write:

$$\begin{aligned}(p_2\times p_2)_*\circ(p_1\times p_1)^*\left(\Gamma_{F_{Y_1}}\right) &= (p_2\times p_2)_*\left(\{[(y_1,y_2),(y_1',y_2')]\in (Y_1\times_Z Y_2)^2; y_1'=F_{Y_1}(y_1)\}\right)\\ &= \{(y_2,y_2')\in Y_2\times Y_2; \exists y_1\in Y_1; f_1(y_1)=f_2(y_2); f_2(y_2')=F_{Y_2}(f_1(y_1))\}\\ &= \deg f_1\times\{(y_2,y_2')\in Y_2\times Y_2; f_2(y_2')=F_{Y_2}(f_2(y_2))\}\\ &= \deg f_1\times(f_2\times f_2)^*(\Gamma_{F_Z}).\end{aligned}$$

Now, since $Y_1\times_X Y_2$ is assumed to be absolutely irreducible, we have $\deg f_1=\deg p_2$ and $\deg f_2=\deg p_1$ in a fiber product setting. Taking into account the normalization (24), and projecting onto $\mathcal{E}_{Y_2}$ as in Section 4, allow us to conclude. □

This allow us us to compute some other norms and scalar products.

Lemma 31. *Suppose that* (*H*) *holds, and that* $X=Y_1\times_Z Y_2$ *in diagram* (32). *Then we have in* $\mathcal{F}_X$

$$\begin{aligned}&\psi_{X/Y_1}(\gamma^i_{Y_1}),\psi_{X/Y_2}(\gamma^i_{Y_2}),\psi_{X/Z}(\gamma^i_Z)\\ &\qquad\in \mathrm{Vect}\left(\psi_{X/Y_1}\left(\gamma^i_{Y_1}-\psi_{Y_1/Z}(\gamma^i_Z)\right),\psi_{X/Y_2}\left(\gamma_{Y_2^i}-\psi_{Y_2/Z}(\gamma^i_Z)\right),\gamma^i_X-\psi_{X/Z}(\gamma^i_Z)\right)^\perp\end{aligned}$$

and

$$\forall i,j\in\mathbb{N},\qquad \psi_{X/Y_1}\left(\gamma^i_{Y_1}-\psi_{Y_1/Z}(\gamma^i_Z)\right)\perp\psi_{X/Y_2}\left(\gamma^j_{Y_2}-\psi_{Y_2/Z}(\gamma^j_Z)\right).$$

Proof — First, we compute scalar products with $\psi_{X/Y_1}(\gamma^i_{Y_1})$. We have

$$\begin{aligned}\left\langle\psi_{X/Y_1}(\gamma^i_{Y_1}),\psi_{X/Y_1}\left(\gamma^i_{Y_1}-\psi_{Y_1/Z}(\gamma^i_Z)\right)\right\rangle_X &= \left\langle\gamma^i_{Y_1},\gamma^i_{Y_1}-\psi_{Y_1/Z}(\gamma^i_Z)\right\rangle_{Y_1} && \text{since } \psi_{X/Y_1} \text{ is isometric}\\ &=0, && \text{by Lemma 27}\end{aligned}$$

$$\begin{aligned}\left\langle\psi_{X/Y_1}(\gamma^i_{Y_1}),\psi_{X/Y_2}\left(\gamma_{Y_2^i}-\psi_{Y_2/Z}(\gamma^i_Z)\right)\right\rangle_X &= \left\langle\varphi_{X/Y_2}\circ\psi_{X/Y_1}(\gamma^i_{Y_1}),\gamma_{Y_2^i}-\psi_{Y_2/Z}(\gamma^i_Z)\right\rangle_{Y_2} && \text{by prop. 24}\\ &= \left\langle\psi_{Y_2/Z}\circ\varphi_{Y_1/Z}(\gamma^i_{Y_1}),\gamma_{Y_2^i}-\psi_{Y_2/Z}(\gamma^i_Z)\right\rangle_{Y_2} && \text{by prop. 30}\\ &= \left\langle\psi_{Y_2/Z}(\gamma^i_Z),\gamma_{Y_2^i}-\psi_{Y_2/Z}(\gamma^i_Z)\right\rangle_{Y_2} && \text{by prop. 24}\\ &=0, && \text{by Lemma 27}\end{aligned}$$

and

$$\begin{aligned}\left\langle\psi_{X/Y_1}(\gamma^i_{Y_1}),\gamma^i_X-\psi_{X/Z}(\gamma^i_Z)\right\rangle_X &= \left\langle\psi_{X/Y_1}(\gamma^i_{Y_1}),\gamma^i_X-\psi_{X/Y_1}(\gamma^i_{Y_1})+\psi_{X/Y_1}\left(\gamma^i_{Y_1}-\psi_{Y_1/Z}(\gamma^i_Z)\right)\right\rangle_X\\ &=0.\end{aligned}$$

The same holds for $\psi_{X/Y_2}(\gamma^i_{Y_2})$.

Secondly, we compute scalar products with $\psi_{X/Z}(\gamma_Z^i) = \psi_{X/Y_\epsilon} \circ \psi_{Y_\epsilon/Z}(\gamma_Z^i)$, for $\epsilon = 1, 2$. We have:

$$\begin{aligned}
\left\langle \psi_{X/Z}(\gamma_Z^i), \psi_{X/Y_\epsilon}\left(\gamma_{Y_\epsilon}^i - \psi_{Y_\epsilon/Z}(\gamma_Z^i)\right)\right\rangle_X &= \left\langle \psi_{X/Y_\epsilon} \circ \psi_{Y_\epsilon/Z}(\gamma_Z^i), \psi_{X/Y_\epsilon}\left(\gamma_{Y_\epsilon}^i - \psi_{Y_\epsilon/Z}(\gamma_Z^i)\right)\right\rangle_X \\
&= \left\langle \psi_{Y_\epsilon/Z}(\gamma_Z^i), \gamma_{Y_\epsilon}^i - \psi_{Y_\epsilon/Z}(\gamma_Z^i)\right\rangle_{Y_\epsilon} && \psi_{X/Y_\epsilon} \text{ isometric} \\
&= 0. && \text{by Lemma 27}
\end{aligned}$$

Last, $\left\langle \psi_{X/Z}(\gamma_Z^i), \gamma_X^i - \psi_{X/Z}(\gamma_Z^i)\right\rangle_X = 0$ by Lemma 27. □

In the same way than the use of the orthogonal projections associated to $\mathcal{F}_{X/Y} \subset \mathcal{F}_X$ in the preceding Section, we do the same here with $\mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2} \subset \mathcal{F}_X$.

Lemma 32. *Suppose that (H) holds, and that $X = Y_1 \times_Z Y_2$ in diagram (32). For $i \geq 0$, let γ_{12}^i be the orthogonal projection of γ_X^i onto $\left(\mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2}\right)^\perp$ inside $\mathcal{F}_X$. Then*

$$\gamma_{12}^i = \gamma_X^i - \psi_{X/Y_1}(\gamma_{Y_1}^i) - \psi_{X/Y_2}(\gamma_{Y_2}^i) + \psi_{X/Z}(\gamma_Z^i),$$

and one has:

$$\begin{aligned}
\|\gamma_{12}^i\|_X &= \sqrt{g_X - g_{Y_1} - g_{Y_2} + g_Z} \\
\left\langle \gamma_{12}^i, \gamma_{12}^{i+j}\right\rangle_X &= \frac{\sharp Y_1(\mathbb{F}_{q^j}) + \sharp Y_2(\mathbb{F}_{q^j}) - \sharp X(\mathbb{F}_{q^j}) - \sharp Z(\mathbb{F}_{q^j})}{2\sqrt{q^j}}.
\end{aligned}$$

Proof — Clearly $\gamma_X^i - \gamma_{12}^i \in \mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2}$. Thanks to orthogonality relations of Lemma 31 and rewriting γ_{12}^i a little bit like

$$\gamma_{12}^i = \left(\gamma_X^i - \psi_{X/Z}(\gamma_Z^i)\right) - \psi_{X/Y_1}\left(\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right) - \psi_{X/Y_2}\left(\gamma_{Y_2}^i) - \psi_{Y_2/Z}(\gamma_Z^i)\right),$$

we prove that $\gamma_{12}^i \in \left(\mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2}\right)^\perp$.

To compute the norm let us note that in the decomposition

$$\gamma_X^i - \psi_{X/Z}(\gamma_Z^i) = \left[\psi_{X/Y_1}\left(\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right) + \psi_{X/Y_2}\left(\gamma_{Y_2}^i) - \psi_{Y_2/Z}(\gamma_Z^i)\right)\right] + \left[\gamma_{12}^i\right].$$

The first bracket lies on in $\mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2}$, while the second one lies on in $\left(\mathcal{F}_{X/Y_1} + \mathcal{F}_{X/Y_2}\right)^\perp$. Applying Pythagore again, we deduce that

$$\begin{aligned}
\left\|\gamma_X^i - \psi_{X/Z}(\gamma_Z^i)\right\|_X^2 &= \left\|\psi_{X/Y_1}\left(\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right) + \psi_{X/Y_2}\left(\gamma_{Y_2}^i - \psi_{Y_2/Z}(\gamma_Z^i)\right)\right\|_X^2 + \left\|\gamma_{12}^i\right\|_X^2 \\
&= \left\|\psi_{X/Y_1}\left(\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right)\right\|_X^2 + \left\|\psi_{X/Y_2}\left(\gamma_{Y_2}^i) - \psi_{Y_2/Z}(\gamma_Z^i)\right)\right\|_X^2 + \left\|\gamma_{12}^i\right\|_X^2 \\
&= \left\|\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right\|_{Y_1}^2 + \left\|\gamma_{Y_2}^i - \psi_{Y_2/Z}(\gamma_Z^i)\right\|_{Y_2}^2 + \left\|\gamma_{12}^i\right\|_X^2.
\end{aligned}$$

Lemma 27 allows us to conclude since

$$\begin{aligned}
\left\|\gamma_{12}^i\right\|_X^2 &= \left\|\gamma_X^i - \psi_{X/Z}(\gamma_Z^i)\right\|_X^2 - \left\|\gamma_{Y_1}^i - \psi_{Y_1/Z}(\gamma_Z^i)\right\|_{Y_1}^2 - \left\|\gamma_{Y_2}^i - \psi_{Y_2/Z}(\gamma_Z^i)\right\|_{Y_2}^2 \\
&= (g_X - g_Z) - (g_{Y_1} - g_Z) - (g_{Y_2} - g_Z).
\end{aligned}$$

In the same way, the calculation of $\left\langle \gamma_{12}^i, \gamma_{12}^{i+j}\right\rangle$ is a consequence of the computation of the scalar product $\left\langle \gamma_X^i - \psi_{X/Z}(\gamma_Z^i), \gamma_X^{i+j} - \psi_{X/Z}(\gamma_Z^{i+j})\right\rangle$. □

Last we can prove the following results.

Theorem 33. *Let X, Y_1, Y_2 and Z be absolutely irreducible smooth projective curves in a cartesian diagram* (32) *of finite morphisms. Suppose that the fiber product $Y_1 \times_Z Y_2$ is also absolutely irreducible and smooth. Then*

$$|\sharp X(\mathbb{F}_q) - \sharp Y_1(\mathbb{F}_q) - \sharp Y_2(\mathbb{F}_q) + \sharp Z(\mathbb{F}_q)| \leq 2(g_X - g_{Y_1} - g_{Y_2} + g_Z)\sqrt{q}.$$

Proof — First, for $X = Y_1 \times_Z Y_2$ the result is a direct consequence of Cauchy-Schwartz inequality applied to γ_{12}^0 and γ_{12}^1 thanks to Lemma 31 since (H) holds by assumption.

Now, for general X satisfying the assumptions of the Theorem, we have by the universal property of the fibered product a finite morphism $X \to Y_1 \times_Z Y_2$. By triangular inequality, and using Proposition 28 together with the result for X, we have

$$\begin{aligned} |\sharp X(\mathbb{F}_q) - \sharp Y_1(\mathbb{F}_q) - \sharp Y_2(\mathbb{F}_q) + \sharp Z(\mathbb{F}_q)| &\leq |\sharp X(\mathbb{F}_q) - \sharp Y_1 \times_Z Y_2(\mathbb{F}_q)| \\ &\quad + |\sharp Y_1 \times_Z Y_2(\mathbb{F}_q) - \sharp Y_1(\mathbb{F}_q) - \sharp Y_2(\mathbb{F}_q) + \sharp Z(\mathbb{F}_q)| \\ &\leq 2(g_X - g_{Y_1 \times_Z Y_2})\sqrt{q} + 2(g_{Y_1 \times_Z Y_2} - g_{Y_1} - g_{Y_2} + g_Z)\sqrt{q} \\ &= 2(g_X - g_{Y_1} - g_{Y_2} + g_Z)\sqrt{q} \end{aligned}$$

and the Theorem is proved. □

It worth to notice that Theorem 33 cannot holds without any hypothesis. For instance, if $X = Y_1 = Y_2$ and the morphisms $Y_i \to Z$ are equal, then the right hand side equals $2(g_X - 2g_X + g_Z)\sqrt{q} = -2(g_X - g_Z)\sqrt{q}$, a negative number! In this case, the Theorem doesn't apply since $Y_1 \times_Z Y_2$ is not irreducible.

Remark – For $Y_1 \times_Z Y_2$ to be absolutely irreducible, it suffices that the tensor product of function fields $\mathbb{F}_q(Y_1) \otimes_{\mathbb{F}_q(Z)} \mathbb{F}_q(Y_2)$ to be an integral domain. For $(Q_1, Q_2) \in Y_1 \times_Z Y_2$ to be smooth it is necessary and sufficient that at least one of the morphism $Y_i \to Z$ is unramified at Q_i.

4 Questions

In this Section, we suggest a few questions raised by the viewpoint of this article.

1. Numerical calculations using our algorithm make it possible that the genus sequence $(g_n, n \in \mathbb{N})$ whose existence is asserted in Proposition 20 has, at least asymptotically, a quite nice behaviour. It seems that for fixed $n \geq 1$, there do exists a constant $0 < c_n < 1$, such that for q large,

$$g_n \sim c_n \sqrt{q}^n,$$

with moreover $\lim_{n \to +\infty} c_n = 1$. Of course, we have proved that $c_2 = \frac{1}{2}$ and $c_3 = \frac{1}{\sqrt{2}}$.

It numerically also seems that for any $n \geq 1$ and any q,

$$g_n < \frac{\sqrt{q}^{n+1}}{\sqrt{q} - 1}.$$

2. Is it true that the first requirement of criteria 17 implies the second one, in the same way that it do implies the third one as proved in corollary 21 ? It turns out that numerically, our algorithm shows that this holds true for all pairs (g, q) we have tested. We gave up this question when we became aware that our bounds seems to be equivalent to Oesterlé's.

3. Why do the upper bounds obtained in this article always coincide numerically with Osterlé's one ?

4. In view of the hope to write down explicitly Weil bounds of order $n \geq 4$, it is necessary to solve a one variable polynomial equation on x_1 of degree $\lceil \frac{n+1}{2} \rceil$, which is greater than 5 for $n \geq 8$. This polynomial equation is, eliminating $\frac{1}{g}$, the resultant
$$\mathrm{Res}_{\frac{1}{g}}\left(G_n^-(P_n^g(x_1)), G_n^+(P_n^g(x_1))\right) \in \mathbb{Q}\left(\frac{1}{\sqrt{q}}\right)[x_1].$$
Do this polynomial have solvable Galois group over the rational function field $\mathbb{Q}\left(\frac{1}{\sqrt{q}}\right)$?

5. Is there a nice interpretation in this framework for the number of rational points of the Jacobian $\mathrm{Jac}(X)$ of a curve X ? In the affirmative, same question for the Prym variety associated to an unramified double cover $X \to Y$?

6. Do the viewpoint of this article can be extended to higher dimensional varieties ?

7. As explained in the article, the geometry and the arithmetic of X are traduced via Hodge Index Theorem to an euclidean property throught Gram determinants by $P_n(X) \in \overline{\mathcal{W}}_n$, and its arithmetic by $P_n(X) \in \mathcal{H}_n^g$ through Ihara's constraints, so that upper bounds for $\sharp X(\mathbb{F}_q)$ are derived from the lower bound for x_1 on $\overline{\mathcal{W}}_n \cap \mathcal{H}_n^g$.

   Any other constraint coming either from the geometry or the arithmetic of X is likely to reduce the domain $\mathcal{W}_n \cap \mathcal{H}_n^g$, making possible that the x_1 function on the new domain as greater lower bound. For instance, do the records obtained in the table `http://www.manypoints.org/`, better than Osterlé bound, can be understood in this way ?

References

[AP95] Yves Aubry and Marc Perret, *Coverings of singular curves over finite fields*, Manuscripta Math. **88** (1995), no. 4, 467–478. MR 1362932 (97g:14022)

[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.

[HU96] Jean-Baptiste Hiriart-Urruty, *L'optimisation*, Que sais-je ?, PUF, 1996.

[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)

[Sha94] Igor R. Shafarevich, *Basic algebraic geometry 1*, Springer-Verlag, 1994, — **N° 31**.

[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)

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), 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)