JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Emmanuel HALLOUIN et Marc PERRET

Number of points of curves over finite fields in some relative situations from an euclidean point of view

Tome 33, nº 1 (2021), p. 125-138.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_1_125_0>

Journal de Théorie des Nombres de Bordeaux **33** (2021), 125–138

Number of points of curves over finite fields in some relative situations from an euclidean point of view

par Emmanuel HALLOUIN et Marc PERRET

Résumé. Nous étudions le nombre de points rationnels d'une courbe projective lisse sur un corps fini dans certaines situations relatives et dans l'esprit d'un précédent article [4], où nous adoptions un point de vue euclidien. Nous prouvons une *borne de Weil relative*, conséquence de l'application de l'inégalité de Cauchy–Schwarz à des parties relatives de la diagonale et du graphe du Frobenius dans un sous-espace euclidien du groupe des diviseurs de la surface produit de la courbe avec elle-même, à équivalence numérique près, muni de l'opposé de la forme d'intersection.

Abstract. We study the number of rational points of smooth projective curves over finite fields in some relative situations in the spirit of a previous paper [4] from an euclidean point of view. We prove some kinds of *relative Weil bounds*, derived from Schwarz inequality for some "relative parts" of the diagonal and of the graph of the Frobenius on some euclidean sub-spaces of the numerical space of the product of the curve with itself endowed with the opposite of the intersection product.

Introduction

Several general bounds on the number $\sharp X(\mathbb{F}_q)$ of rational points on absolutely irreducible smooth projective curves X of genus g_X defined over the finite field $\mathbb{F}_q$ are known, the most famous being Weil bound [8]:

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2g_X\sqrt{q}. \tag{0.1}$$

Other bounds are known, such as asymptotic Drinfeld–Vlăduţ one [7] and Tsfasman one [6], so as a relative bound (for instance in [1])

$$|\sharp X(\mathbb{F}_q) - \sharp Y(\mathbb{F}_q)| \leq 2(g_X - g_Y)\sqrt{q} \tag{0.2}$$

holding in a covering $X \to Y$. Twisting a little bit Weil's original proof [8] of (0.1), the authors have given in a previous paper [4] proofs of Weil's,

Manuscrit reçu le 25 mai 2020, accepté le 21 septembre 2020.

2010 *Mathematics Subject Classification.* 11G20, 14G05, 14G15, 14H99.

Mots-clefs. Curves over a finite field, rational point, Weil bound, Intersection Theory.

Funded by ANR grant ANR-15-CE39-0013-01 "manta".

Drinfeld–Vlăduţ's, Tsfasman's and some other new bounds from an euclidean point of view. For instance, Weil bound (0.1) is only Schwarz inequality applied to two very natural vectors γ_X^0 and γ_X^1 in a convenient euclidean space $\mathcal{E}_X$. To be more precise, let $\mathrm{Num}(X \times X)_{\mathbb{R}}$ be the real numerical vector space of divisors of the surface $X \times X$ up to numerical equivalence. It is endowed with the intersection pairing, a non degenerate bilinear form. The space $\mathcal{E}_X$ is the orthogonal of the subspace generated by the horizontal and vertical classes H_X and V_X. By Hodge index theorem [5, Chap. V, Thm. 1.9], $\mathcal{E}_X$ endowed with the opposite of the intersection product turns to be an euclidean space. As for γ_X^0 and γ_X^1, they are respectively the orthogonal projections onto $\mathcal{E}_X$, for the intersection product on the whole space $\mathrm{Num}(X \times X)_{\mathbb{R}}$, of the class of the diagonal Δ_X and of the class of the graph Γ_{F_X} of the Frobenius morphism F_X on X.

The aim of this paper is to complete this work in some relative situations, giving for instance a similar euclidean proof for (0.2). A key point is that a covering $f : X \to Y$ induces a pull-back linear morphism $(f \times f)^*$ and a push-forward linear morphism $(f \times f)_*$ between $\mathcal{E}_X$ and $\mathcal{E}_Y$. Both morphisms behave in some very pleasant way with respect to the vectors γ_X^i and γ_Y^i for $i = 0, 1$, in such a way that it can be said that γ_X^i is the orthogonal sum, in $\mathcal{E}_X$, of the pull-back of γ_Y^i and of some "relative part" $\gamma_{Y/X}^i$. The Gram matrix between $\gamma_{Y/X}^0$ and $\gamma_{Y/X}^1$ can be computed, and (0.2) is only Schwarz inequality for this pair of vectors.

This point of view can be pushed further in a commutative diagram (3.1) below. A relative part $\gamma_{X/Y_1,Y_2/Z}^i$ of γ_X^i, denoted by γ_{12}^i, can be defined, and Schwarz inequality for $i = 0, 1$ gives the following Theorem 3.7. This leads to a new bound relating the number of rational points of the four curves involved in case the fibre product is absolutely irreducible and smooth.

Theorem. *Let X, Y_1, Y_2 and Z be absolutely irreducible smooth projective curves in a commutative diagram* (3.1) *below of finite morphisms. Suppose that the fiber product $Y_1 \times_Z Y_2$ is absolutely irreducible and smooth. Then*

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

Notice that if (0.2) can be proved using the Tate modules of the jacobians of the involved curves (see e.g. [1]), Proposition 3.2 and Theorem 3.7, up to our knowledge, cannot.

1. Known absolute results [4]

In this first section, we gather the notations and results of our previous work [4] that are needed in this paper.

Let X be an absolutely irreducible smooth projective curve of genus g defined over the finite field $\mathbb{F}_q$ with q elements. Weil's proof of Rieman hypothesis in this context rests on intersection theory on the numerical space $\mathrm{Num}(X \times X)_{\mathbb{R}}$ of the algebraic surface $X \times X$. The key point is the Hodge Index Theorem stating that the intersection pairing is definite negative on the orthogonal complement of the class of an ample divisor [5, Chap. V, Thm. 1.9 & Rk. 1.9.1]. In particular the opposite of the intersection pairing defines a scalar product on the orthogonal complement of the plane generated by the classes of the horizontal and the vertical divisors since their sum is ample. This motivates the following definition.

Definition 1.1. *Let H_X and V_X be the horizontal and vertical classes inside* $\mathrm{Num}(X \times X)_{\mathbb{R}}$. *We put:*

$$\mathcal{E}_X = \mathrm{Vect}(H_X, V_X)^{\perp}$$

and we endow this vector space with the scalar product defined by $\langle D_1, D_2\rangle = -D_1 \cdot D_2$, the opposite of the intersection pairing $D_1 \cdot D_2$ on $X \times X$.

It is useful to introduce the orthogonal projection of $\mathrm{Num}(X \times X)_{\mathbb{R}}$ onto $\mathcal{E}_X$ for the intersection pairing bilinear form:

$$\begin{array}{rccc} p_X : & \mathrm{Num}(X \times X)_{\mathbb{R}} & \longrightarrow & \mathcal{E}_X \\ & D & \longmapsto & D - (D \cdot V_X)H_X - (D \cdot H_X)V_X. \end{array} \tag{1.1}$$

In this context, the family of (orthogonal projections of) graphs of iterates of the q-Frobenius morphism play a crucial role.

Definition 1.2. *Let $F_X : X \to X$ be the q-Frobenius morphism on the curve X. For $i \geq 0$, let $\Gamma^i_{F_X}$ be the class in* $\mathrm{Num}(X \times X)_{\mathbb{R}}$ *of the graph of the i-th iterate of F_X (the 0-th iterate being identity). We denote:*

$$\gamma^i_X = p_X(\Gamma^i_{F_X}) \in \mathcal{E}_X,$$

where $p_X : \mathrm{Num}(X \times X) \to \mathcal{E}_X$ is the orthogonal projection onto $\mathcal{E}_X$ given by (1.1).

Remark. We delete here the normalization of the vectors γ^i_X introduced in our previous work [4, Def. 4], necessary therein for some intersection matrix to be Toeplitz [4, Proposition 5]. This particular shape of the intersection matrix is irrelevant in the present work.

The computation of the norms and the scalar products of the γ^i_X's is well known and can be found in our previous work [4, Prop. 5] in which another normalization is used.

Lemma 1.3. *The norms and the scalar products of the γ^i_X's are given by*

$$\|\gamma^i_X\|_X = \sqrt{2g_X q^i} \quad \text{and} \quad \langle \gamma^i_X, \gamma^{i+j}_X \rangle_X = q^i((q^j + 1) - \sharp X(\mathbb{F}_{q^j})) \tag{1.2}$$

for any $i \geq 0$ and $j \geq 1$.

2. The relative case

We concentrate in this Section on the simplest relative situation. The data 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.

2.1. The pull-back and push-forward morphisms. All results of this Subsection hold over any field k. The morphism $f \times f$ from $X \times X$ to $Y \times Y$ induces a push forward morphism

$$(f \times f)_* : \mathrm{Num}(X \times X)_{\mathbb{R}} \longrightarrow \mathrm{Num}(Y \times Y)_{\mathbb{R}}$$

and a pull back morphism

$$(f \times f)^* : \mathrm{Num}(Y \times Y)_{\mathbb{R}} \longrightarrow \mathrm{Num}(X \times X)_{\mathbb{R}}.$$

For normalization purpose, it is convenient to define $\varphi^*_{X/Y}$ and $\varphi_{*,X/Y}$ (or φ^* and φ_* for short) by

$$\varphi_* = {\varphi_{X/Y}}_* = \frac{1}{d}(f \times f)_* \qquad \text{and} \qquad \varphi^* = \varphi^*_{X/Y} = \frac{1}{d}(f \times f)^*. \tag{2.1}$$

In the next proposition, it is shown that φ^* sends the euclidean space $\mathcal{E}_Y$ to $\mathcal{E}_X$ and that φ_* sends the euclidean space $\mathcal{E}_X$ to $\mathcal{E}_Y$ with some special features. In the sequel we denote the same way the maps φ^* and φ_* and their restrictions to either $\mathcal{E}_X$ or $\mathcal{E}_Y$.

Proposition 2.1. *The morphisms φ_* and φ^* satisfy the following.*

(1) *Vertical and horizontal divisors are preserved:*

$$\varphi^*(H_Y) = H_X, \quad \varphi_*(H_X) = H_Y, \quad \varphi^*(V_Y) = V_X, \quad \varphi_*(V_X) = V_Y, \tag{2.2}$$

so as the orthogonal complements of the horizontal and vertical parts:

$$\varphi^*(\mathcal{E}_Y) \subset \mathcal{E}_X, \qquad \varphi_*(\mathcal{E}_X) \subset \mathcal{E}_Y. \tag{2.3}$$

Moreover, the restrictions of φ^* to $\mathcal{E}_Y$ and of φ_* to $\mathcal{E}_X$ satisfy:

(2) *(projection formula) for all $\gamma \in \mathcal{E}_X$ and all $\delta \in \mathcal{E}_Y$, $\langle \gamma, \varphi^*(\delta)\rangle_X = \langle \varphi_*(\gamma), \delta\rangle_Y$;*
(3) *$\varphi_* \circ \varphi^* = \mathrm{Id}_{\mathcal{E}_Y}$, the identity map on $\mathcal{E}_Y$;*
(4) *(isometric embeding) the morphism φ^* is an isometric embedding of $\mathcal{E}_Y$ into $\mathcal{E}_X$;*
(5) *(orthogonal projection) the map $\varphi^* \circ \varphi_*$ (restricted to $\mathcal{E}_X$) is the orthogonal projection of $\mathcal{E}_X$ onto the subspace $\varphi^*(\mathcal{E}_Y)$.*

Proof. For Formulas (2.2) of item (1) and item (3), we first consider the maps $\varphi^* = \frac{1}{d}(f \times f)^*$ and $\varphi_* = \frac{1}{d}(f \times f)_*$ with their domain and co-domain equal to the total spaces $\mathrm{Num}(X \times X)_{\mathbb{R}}$ and $\mathrm{Num}(Y \times Y)_{\mathbb{R}}$. Since the morphism $f : X \to Y$ is finite, it is proper [5, Chap. II, Ex. 4.1]; since Y is a smooth curve, the morphism f is also flat [5, Chap. III, Prop. 9.7]. Then so is the morphism $f \times f$ [2, §1.10, Prop. 1.10]. Now, from the definition of the push-forward map for proper morphisms [2, §1.4, p. 11], we have $(f \times f)_*(H_X) = \deg(H_X/H_Y)H_Y = dH_Y$. From the definition of the pull-back map for flat morphism [2, §1.7, p. 18], the support of $(f \times f)^*(H_Y)$ is H_X. Since moreover $(f \times f)_* \circ (f \times f)^* = d^2\, \mathrm{Id}_{\mathrm{Num}(Y\times Y)_{\mathbb{R}}}$ [2, §1.7, Ex. 1.7.4] (from which item (3) follows), we have $(f \times f)^*(H_Y) = dH_X$. Formulas (2.2) of item (1) for horizontal parts follow, and those for vertical parts work in the same way.

Next, the projection formula [5, App. A, A4] asserts that

$$\forall\, D \in \mathrm{Num}(X \times X)_{\mathbb{R}}, \;\; \forall\, C \in \mathrm{Num}(Y \times Y)_{\mathbb{R}},$$
$$(f \times f)^*(D) \cdot C = D \cdot (f \times f)_*(C)$$

where the first (resp. second) intersection product is intersection in the surface $X \times X$ (resp. $Y \times Y$). Going back to φ, these proves that $\varphi_* \circ \varphi^* = \mathrm{Id}_{\mathrm{Num}(Y\times Y)_{\mathbb{R}}}$ and that $\varphi^*(D) \cdot C = D \cdot \varphi_*(C)$. Using formulas (2.2), we deduce that $H_X \cdot \varphi^*(D) = H_Y \cdot D$ (the same with V_X, V_Y) and thus $\varphi^*(\mathcal{E}_Y) \subset \mathcal{E}_X$. In the same way $\varphi^*(\mathcal{E}_X) \subset \mathcal{E}_Y$, so that item (1) is proved.

From now on, we restrict the maps φ^* and φ_x to the subspaces $\mathcal{E}_Y$ and $\mathcal{E}_X$ without changing the notations. Item (2) is only a restatement of the projection formula above. Item (4) is an easy consequence of items (2) and (3). Last, the morphism $\varphi^* \circ \varphi_*$ is by item (3) a projector whose image is the space $\varphi^*(\mathcal{E}_Y)$. For $\gamma \in \mathcal{E}_X$, by items (2) and (3), one has

$$\langle \varphi^* \circ \varphi_*(\gamma), \gamma - \varphi^* \circ \varphi_*(\gamma) \rangle_X$$
$$= \langle \varphi_*(\gamma), \varphi_*(\gamma) \rangle_Y - \langle \varphi_*(\gamma), \varphi_* \circ \varphi^* \circ \varphi_*(\gamma) \rangle_Y = 0$$

and thus, writing $\gamma = \varphi^* \circ \varphi_*(\gamma) + (\gamma - \varphi^* \circ \varphi_*(\gamma))$, we see that this is the sum of two orthogonal elements, the first one lying in $\varphi^*(\mathcal{E}_Y)$ and the second one in $\varphi^*(\mathcal{E}_Y)^\perp$. This proves item (5). □

Remark. Since the pull-back map $\varphi^*_{X/Y}$ is an isometry (and thus is injective), we could have identified the space $\mathcal{E}_Y$ with its embedding $\varphi^*_{X/Y}(\mathcal{E}_Y)$ inside $\mathcal{E}_X$. With this point of view, the push-forward map ${\varphi_{X/Y}}_*$ is truly the orthogonal projection of $\mathcal{E}_X$ onto $\mathcal{E}_Y$. In every proofs in the sequel, the reader may feels more comfortable by skipping all the $\varphi^*_{\_/\_}$ maps and thinking to the ${\varphi_{\_/\_}}_*$ maps as orthogonal projections.

The "bottom" space $\mathcal{E}_Y$ embeds into the "top" space $\mathcal{E}_X$ via the pull-back morphism $\varphi^*_{X/Y}$, and the orthogonal complement of this embedding $\varphi^*_{X/Y}(\mathcal{E}_Y)$ into $\mathcal{E}_X$ plays a crucial role in the whole paper.

Definition 2.2. *The orthogonal complement $\varphi^*_{X/Y}(\mathcal{E}_Y)^\perp$ of $\varphi^*_{X/Y}(\mathcal{E}_Y)$ inside $\mathcal{E}_X$ is denoted by $\mathcal{E}_{X/Y}$ and is called the relative space for the covering $X \to Y$.*

We emphasize for future need the fact that this space $\mathcal{E}_{X/Y}$ is contained in the kernel of the push-forward morphism.

Lemma 2.3. *The push-forward morphism ${\varphi_{X/Y}}_*$ is zero on the relative space $\mathcal{E}_{X/Y}$ for $X \to Y$.*

Proof. Let $\gamma \in \mathcal{E}_{X/Y} = \varphi^*(\mathcal{E}_Y)^\perp$. Then, $\varphi^* \circ \varphi_*(\gamma) = 0$ by Proposition 2.1 item (5), so that $\varphi^*(\gamma) = 0$ by item (4). □

2.2. The relative part of the γ_X^i's in a covering. In this section, we look at the image of the iterated Frobenius graphs and their orthogonal projection into the spaces $\mathcal{E}_X$ and $\mathcal{E}_Y$ (see Definition 1.2) under the maps φ^* and φ_*.

We begin by stating a Lemma.

Lemma 2.4. *For any $i \geq 0$, one has ${\varphi_{X/Y}}_*(\gamma_X^i) = \gamma_Y^i$.*

Proof. From Definition 1.2 together with Formula (1.1), we have

$$\gamma_X^i = p_X(\Gamma_X^i) = \Gamma_X^i - H_X - q^i V_X$$

and

$$\gamma_Y^i = p_Y(\Gamma_Y^i) = \Gamma_Y^i - H_Y - q^i V_Y.$$

Since $(f \times f)(\Gamma_X^i) = \Gamma_Y^i$ and $\deg(\Gamma_X^i/\Gamma_Y^i) = d$ for any $i \leq 0$, we get from the definition of the push-forward map [2, §1.4, p. 11] that $(f \times f)_*(\Gamma_X^i) = d\Gamma_Y^i$. The Lemma follows using item (1) of Proposition 2.1. □

In the other direction, it turns out that we do not have equality $\varphi^*_{X/Y}(\gamma_Y^i) = \gamma_X^i$, but rather the very fruitful following orthogonal decomposition. In view of definition 2.2, we have the orthogonal sum

$$\mathcal{E}_X = \varphi^*(\mathcal{E}_Y) \oplus \mathcal{E}_{X/Y}. \tag{2.4}$$

For $i \geq 0$, the corresponding decomposition of γ_X^i is

$$\gamma_X^i = \underbrace{\varphi^*(\gamma_Y^i)}_{\in \varphi^*(\mathcal{E}_Y)} + \underbrace{(\gamma_X^i - \varphi^*(\gamma_Y^i))}_{\in \varphi^*(\mathcal{E}_Y)^\perp}, \tag{2.5}$$

since by Proposition 2.1 item (2) together with Lemma (2.4), the orthogonal projection of γ_X^i is $\varphi^*(\gamma_Y^i)$. The orthogonal components $\gamma_X^i - \varphi^*(\gamma_Y^i)$ inside $\mathcal{E}_{X/Y} = \varphi^*(\mathcal{E}_Y)^\perp$ turning to be of greatest importance in the sequel, we give them a name in the following Definition.

Definition 2.5. *For $i \geq 0$, the component*

$$\gamma^i_{X/Y} = \gamma^i_X - \varphi^*(\gamma^i_Y) \in \mathcal{E}_{X/Y},$$

of γ^i_X inside $\mathcal{E}_{X/Y}$ is called the i-th relative part of the Frobenius.

We can relate in the following Lemma the scalar products between the relative parts of γ^i_X and γ^{i+j}_X, for any $i, j \geq 0$, to standard geometrical and arithmetical invariants of both curves X and Y.

Lemma 2.6. *For any $i \geq 0$ and $j > 0$, we have*

$$\|\gamma^i_{X/Y}\|_X = \sqrt{2(g_X - g_Y)q^i}$$

and

$$\langle \gamma^i_{X/Y}, \gamma^{i+j}_{X/Y} \rangle_X = q^i(\sharp Y(\mathbb{F}_{q^j}) - \sharp X(\mathbb{F}_{q^j})).$$

Proof. Since $\gamma^i_{X/Y} \perp \varphi^*(\gamma^i_Y)$, the first norm calculation is just Pythagorean Theorem. Indeed, we have for any $i \geq 0$

$$\begin{aligned} \|\gamma^i_X\|^2_X &= \|\varphi^*(\gamma^i_Y)\|^2_X + \|\gamma^i_{X/Y}\|^2_X && \text{by Def. 2.5 and Pythagore} \\ &= \|\gamma^i_Y\|^2_Y + \|\gamma^i_{X/Y}\|^2_X, && \text{since } \varphi^* \text{ isometric (Prop. 2.1, item (4))} \end{aligned}$$

from which we deduce using (1.2) that $2g_X q^i = 2g_Y q^i + \|\gamma^i_{X/Y}\|^2_X$.

Taking again into account orthogonality, we also easily compute the scalar product

$$\begin{aligned} &\langle \gamma^i_{X/Y}, \gamma^{i+j}_{X/Y} \rangle_X \\ &= \langle \gamma^i_X, \gamma^{i+j}_X \rangle_X - \langle \varphi^*\left(\gamma^i_Y\right), \varphi^*\left(\gamma^{i+j}_Y\right) \rangle_X && \text{by Def. 2.5 and orthogonality} \\ &= \langle \gamma^i_X, \gamma^{i+j}_X \rangle_X - \langle \gamma^i_Y, \gamma^{i+j}_Y \rangle_Y && \text{since } \varphi^* \text{ isometric} \\ &= q^i\left((q^j+1) - \sharp X(\mathbb{F}_{q^j})\right) - q^i\left((q^j+1) - \sharp Y(\mathbb{F}_{q^j})\right), && \text{by (1.2)} \end{aligned}$$

as requested. □

We end this Section with a Lemma giving a useful result on the push-forward of the relative part of the γ^i's.

Lemma 2.7. *In a tower $X \to Y \to Z$, we have for any $i \geq 0$*

$$\varphi_{X/Y_*}(\gamma^i_{X/Z}) = \gamma^i_{Y/Z}.$$

Proof. Applying φ_{X/Y_*} to the identity $\gamma^i_X = \varphi^*_{X/Z}(\gamma^i_Z) + \gamma^i_{X/Z}$, we obtain thanks to Lemma (2.4)

$$\gamma^i_Y = \varphi_{X/Y_*} \circ \varphi^*_{X/Y} \circ \varphi^*_{Y/Z}(\gamma^i_Z) + \varphi_{X/Y_*}(\gamma^i_{X/Z}),$$

that is $\gamma_Y^i = \varphi_{Y/Z}^*(\gamma_Z^i) + {\varphi_{X/Y}}_*(\gamma_{X/Z}^i)$ by Proposition 2.1 item (3), proving the Lemma using Definition 2.5. □

3. Applications to relative bounds on numbers of rational points of curves

We prove Propositions 3.1 and 3.2 in the first Subsection, so as Theorem 3.7 in the second one, in the very same spirit as in our previous work [4, Thm. 11 and Prop. 12, pp. 5420-5421].

3.1. First application: number of points in a covering $X \to Y$.

As told in the introduction, Propositions 3.1 below is well known. We think it is interesting to show how it is neat using the euclidean framework.

Proposition 3.1. *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 Schwarz inequality to the relative vectors $\gamma_{X/Y}^0$ and $\gamma_{X/Y}^1$. We obtain from Lemma 2.6

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

hence the Proposition. □

The following Proposition 3.2 is the relative form of a previous absolute bound [4, Prop. 12]. Of course, although less nice, such upper bounds can be given for $\sharp X(\mathbb{F}_{q^n}) - \sharp Y(\mathbb{F}_{q^n})$, for any $n \geq 2$.

Proposition 3.2. *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. The idea is to write down the matrix $\operatorname{Gram}(\gamma_{X/Y}^0, \gamma_{X/Y}^1, \gamma_{X/Y}^2)$ using Lemma 2.6, and then to use that it has a non-negative determinant. In fact, as noted in our previous work [4], it is more convenient to write down

$$\operatorname{Gram}\left(q\gamma_{X/Y}^0 + \gamma_{X/Y}^2, \gamma_{X/Y}^1\right) = \begin{pmatrix} 4(g_X - g_Y)q^2 + 2q\delta_2 & 2q\delta_1 \\ 2q\delta_1 & 2(g_X - g_Y)q \end{pmatrix}$$

where we put $\delta_i = \sharp Y(\mathbb{F}_{q^i}) - \sharp X(\mathbb{F}_{q^i})$, $i = 1, 2$ for short. The result to be proved is just the fact that this matrix has a non-negative determinant. □

3.2. Second application: number of points in some commutative diagram (3.1). We focus in this Subection on the situation of a commutative diagram

(3.1)
$$\begin{tikzcd}
 & X \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & \\
Y_1 \arrow[dr, "f_1"'] & & Y_2 \arrow[dl, "f_2"] \\
 & Z &
\end{tikzcd}$$

of finite covers of absolutely irreducible smooth projective curves defined over $\mathbb{F}_q$. In order to give a relationship between the number of rational points of the involved curves, we need a decomposition of γ^i_X, for $i = 1, 2$, much sharper than the one given by (2.5), taking into account the whole diagram.

3.2.1. ***Pull-back and push-forward morphisms in a commutative diagram.*** Applying results of §2, we have ten relative linear maps that fit into a diagram of four Euclidean spaces:

(3.2)
$$\begin{tikzcd}
 & \mathcal{E}_X \arrow[dl, dashed, bend right, "\varphi_{X/Y_1*}"'] \arrow[dr, dashed, bend left, "\varphi_{X/Y_2*}"] \arrow[dd, dashed, bend right, "\varphi_{X/Z*}"'] & \\
\mathcal{E}_{Y_1} \arrow[ur, hook, "\varphi^*_{X/Y_1}"] \arrow[dr, dashed, bend right, "\varphi_{Y_1/Z*}"'] & & \mathcal{E}_{Y_2} \arrow[ul, hook', "\varphi^*_{X/Y_2}"'] \arrow[dl, dashed, bend left, "\varphi_{Y_2/Z*}"] \\
 & \mathcal{E}_Z \arrow[ul, hook', "\varphi^*_{Y_1/Z}"] \arrow[ur, hook, "\varphi^*_{Y_2/Z}"'] \arrow[uu, hook, bend right, "\varphi^*_{X/Z}"'] &
\end{tikzcd}$$

As noted in the proof of Proposition 2.1, all the involved morphisms $f_i \times f_i$ and $p_i \times p_i$ from a square surface to another are proper and flat. As a consequence, the push-forward and pull-back operations are functorial [2, §1.4, p 11 & §1.7, p 18], that is we have ${\varphi_{X/Z}}_* = {\varphi_{Y_i/Z}}_* \circ {\varphi_{X/Y_i}}_*$ and $\varphi^*_{X/Z} = \varphi^*_{X/Y_i} \circ \varphi^*_{Y_i/Z}$ for $i = 1, 2$. We also recall that all the $\varphi^*_{\_/\_}$ maps are isometric embeddings by Proposition 2.1.

In order to understand better the relationships between these euclidean vector spaces and linear maps, we need a new hypothesis in the following Lemma.

Lemma 3.3. *Consider a commutative diagram of curves like in* (3.1). *Suppose that the fiber product $Y_1 \times_Z Y_2$ is absolutely irreducible and smooth. Then, we have:*

(1) ${\varphi_{X/Y_2}}_* \circ \varphi^*_{X/Y_1} = \varphi^*_{Y_2/Z} \circ {\varphi_{Y_1/Z}}_*$ *on* $\mathcal{E}_{Y_1}$*;*

(2) *inside* $\mathcal{E}_X$*, the subspaces* $\varphi^*_{X/Y_1}(\mathcal{E}_{Y_1/Z})$ *and* $\varphi^*_{X/Y_2}(\mathcal{E}_{Y_2/Z})$ *are orthogonal, and lie into* $\varphi^*_{X/Z}(\mathcal{E}_Z)^\perp = \mathcal{E}_{X/Z}$.

Proof. Let us prove the first item. By the universal property of the fiber product, the two top morphisms in the commutative starting diagram (3.1) factor through

$$\begin{array}{rccc} g: & X & \longrightarrow & Y_1 \times_Z Y_2 \subset Y_1 \times Y_2 \\ & x & \longmapsto & (p_1(x), p_2(x)), \end{array}$$

yielding to the diagram

$$\begin{tikzcd}
 & X \arrow[d, "g"] \arrow[ddl, bend right, "p_1"'] \arrow[ddr, bend left, "p_2"] & \\
 & Y_1 \times_Z Y_2 \arrow[dl, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
Y_1 \arrow[dr, "f_1"'] & & Y_2 \arrow[dl, "f_2"] \\
 & Z &
\end{tikzcd},$$

where π_i is the projection of the fiber product $Y_1 \times_Z Y_2 \subset Y_1 \times Y_2$ on the i-th factor Y_i and $p_i = \pi_i \circ g$. This last diagram induces a similar one between the five squared curves, related by the seven squared morphisms. As already noted, all these squared morphisms are proper and flat, the flatness of $g \times g$ following from the smoothness assumption on $Y_1 \times_Z Y_2$.

Since the bottom square involving the nodes $(Y_1 \times_Z Y_2)^2$, Y_i^2 $i = 1, 2$, and Z^2 is itself a fiber square, we know that [2, Prop. 1.7 p. 18],

$$(\pi_2 \times \pi_2)_* \circ (\pi_1 \times \pi_1)^* = (f_2 \times f_2)^* \circ (f_1 \times f_1)_* \tag{3.3}$$

on $\mathrm{Num}(Y_1 \times Y_1)_\mathbb{R}$. Since $g \times g$ is also finite and flat, we also know that $(g \times g)_* \circ (g \times g)^* = (\deg g)^2 \,\mathrm{Id}_{\mathrm{Num}(Y_1 \times Y_1)_\mathbb{R}}$ [2, Ex 1.7.4 p. 20]. Taking into account normalizations (2.1), item (1) follows now by direct calculation from (3.3) and the multiplicativity of the degree in towers of finite morphisms.

For the second item, we first prove that

$$\varphi^*_{X/Y_i}(\mathcal{E}_{Y_i/Z}) \subset \mathcal{E}_{X/Z} = \left(\varphi^*_{X/Z}(\mathcal{E}_Z)\right)^\perp.$$

Let $\gamma_Z \in \mathcal{E}_Z$ and $\gamma_i \in \mathcal{E}_{Y_i/Z}$ for $i = 1$ or 2. We have

$$\begin{aligned}
&\langle \varphi^*_{X/Z}(\gamma_Z), \varphi^*_{X/Y_i}(\gamma_i)\rangle_X \\
&= \langle \varphi^*_{X/Y_i} \circ \varphi^*_{Y_i/Z}(\gamma_Z), \varphi^*_{X/Y_i}(\gamma_i)\rangle_X \\
&= \langle \varphi^*_{Y_i/Z}(\gamma_Z), \gamma_i\rangle_{Y_i} && \text{since } \varphi^*_{X/Y_i} \text{ is an isometry} \\
&= 0 && \begin{array}{l}\text{since } \varphi^*_{Y_i/Z}(\gamma_Z) \in \varphi^*_{Y_i/Z}(\mathcal{E}_Z) \\ \text{and } \gamma_i \in \mathcal{E}_{Y_i/Z} = (\varphi^*_{Y_i/Z}(\mathcal{E}_Z))^\perp.\end{array}
\end{aligned}$$

Last, let $\gamma_1 \in \mathcal{E}_{Y_1/Z}$. Then, we have by item (1) together with Lemma 2.3

$$\varphi_{X/Y_2 *} \circ \varphi^*_{X/Y_1}(\gamma_1) = \varphi^*_{Y_2/Z} \circ \varphi_{Y_1/Z *}(\gamma_1) = 0.$$

It follows by adjunction that, for any $\gamma_2 \in \mathcal{E}_{Y_2}$, we have

$$\begin{aligned}
\langle \varphi^*_{X/Y_1}(\gamma_1), \varphi^*_{X/Y_2}(\gamma_2)\rangle_X &= \langle \varphi_{X/Y_2 *} \circ \varphi^*_{X/Y_1}(\gamma_1), \gamma_2\rangle_{Y_2} \\
&= \langle 0, \gamma_2\rangle_{Y_2} \\
&= 0,
\end{aligned}$$

so that $\varphi^*_{X/Y_1}(\mathcal{E}_{Y_1/Z}) \subset (\varphi^*_{X/Y_2}(\mathcal{E}_{Y_2}))^\perp \subset (\varphi^*_{X/Y2}(\mathcal{E}_{Y_2/Z}))^\perp$, and the proof is complete. □

3.2.2. ***The relative part of the γ^i_X's in a commutative diagram.*** We are now ready to introduce some orthogonal decompositions of the γ^i_X's inside $\mathcal{E}_X$ sharper than the one

$$\gamma^i_X = \underbrace{\varphi^*_{X/Z}(\gamma^i_Z)}_{\in \varphi^*_{X/Z}(\mathcal{E}_Z)} + \underbrace{\gamma^i_{X/Z}}_{\in \mathcal{E}_{X/Z}} \tag{3.4}$$

given in Section 2 for the covering $X \to Z$, that takes into account the whole diagram (3.1) below X.

There is, from item (2) of Lemma 3.3, an orthogonal decomposition of $\mathcal{E}_{X/Z}$ of the form

$$\mathcal{E}_{X/Z} = \varphi^*_{X/Y_1}(\mathcal{E}_{Y_1/Z}) \oplus \varphi^*_{X/Y_2}(\mathcal{E}_{Y_2/Z}) \oplus \mathcal{E}_{12} \tag{3.5}$$

for some uniquely defined subspace $\mathcal{E}_{X/Y_1,Y_2/Z} = \mathcal{E}_{12}$ for simplicity. To study the corresponding decomposition of the relative vectors $\gamma^i_{X/Z} \in \mathcal{E}_{X/Z}$ for $X \to Z$, we need another definition.

Definition 3.4. *For $i \geq 0$, denote*

$$\gamma^i_{12} = \gamma^i_{X/Z} - \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z}) - \varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z}), \tag{3.6}$$

and we call it the i-th "square diagram" part of the Frobenius.

Lemma 3.5. *Consider the situation of diagram* (3.1) *in which* $Y_1 \times_Z Y_2$ *is assumed to be absolutely irreduible and smooth. Let* $i \geq 0$*. Then the decomposition of* $\gamma^i_{X/Z}$ *as an orthogonal sum accordingly to* (3.5) *is given by*

$$\gamma^i_{X/Z} = \underbrace{\varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})}_{\in\varphi^*_{X/Y_1}(\mathcal{E}_{Y_1/Z})} + \underbrace{\varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z})}_{\in\varphi^*_{X/Y_2}(\mathcal{E}_{Y_2/Z})} + \underbrace{\gamma^i_{12}}_{\in\mathcal{E}_{12}}. \tag{3.7}$$

Proof. Given Definition 3.4, formula (3.7) clearly holds true. Since the vectors $\varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})$ and $\varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z})$ are orthogonal thanks to Lemma 3.3, item (2), it suffices to prove that $\gamma^i_{12} \perp \varphi^*_{X/Y_k}(\gamma^i_{Y_k/Z})$ for $k = 1, 2$. Let for instance take $k = 1$. Then, we have

$$\begin{aligned}
&\langle \gamma^i_{12}, \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})\rangle_X \\
&\quad = \langle \gamma^i_{X/Z}, \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})\rangle_X \\
&\qquad - \langle \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z}), \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})\rangle_X \\
&\qquad - \langle \varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z}), \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})\rangle_X \\
&\quad = \langle \varphi_{X/Y_1 *}(\gamma^i_{X/Z}), \gamma^i_{Y_1/Z}\rangle_X && \text{by adjunction} \\
&\qquad - \langle \gamma^i_{Y_1/Z}, \gamma^i_{Y_1/Z}\rangle_X && \text{since } \varphi^*_{X/Y_1} \text{ is isometric} \\
&\qquad - 0 && \text{by Lemma 3.3, item (2)} \\
&\quad = \langle \gamma^i_{Y_1/Z}, \gamma^i_{Y_1/Z}\rangle_X && \text{by Lemma 2.7} \\
&\qquad - \langle \gamma^i_{Y_1/Z}, \gamma^i_{Y_1/Z}\rangle_X \\
&\quad = 0,
\end{aligned}$$

and the proof is complete. □

Next, we can compute the norms and scalar products of the γ^i_{12}'s.

Lemma 3.6. *Consider a commutative diagram of curves like in* (3.1)*. Suppose that* $Y_1 \times_Z Y_2$ *is absolutely irreducible and smooth. Then for any* $i \geq 0$*,* $j > 0$*, we have*

$$\|\gamma^i_{12}\|_X = \sqrt{2(g_X - g_{Y_1} - g_{Y_2} + g_Z)q^i}$$

and

$$\langle \gamma^i_{12}, \gamma^{i+j}_{12}\rangle_X = q^i(\sharp Y_1(\mathbb{F}_{q^j}) + \sharp Y_2(\mathbb{F}_{q^j}) - \sharp X(\mathbb{F}_{q^j}) - \sharp Z(\mathbb{F}_{q^j})).$$

Proof. From the orthogonal sum

$$\gamma^i_{X/Z} = \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z}) + \varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z}) + \gamma^i_{12},$$

we get using Pythagorean theorem

$$\|\gamma^i_{X/Z}\|^2_X = \|\varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z})|^2_X + \|\varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z})\|^2_X + \|\gamma^i_{12}\|^2_X,$$

and also

$$\begin{aligned}\langle \gamma^i_{X/Z}, \gamma^{i+j}_{X/Z}\rangle_X &= \langle \varphi^*_{X/Y_1}(\gamma^i_{Y_1/Z}), \varphi^*_{X/Y_1}(\gamma^{i+j}_{Y_1/Z})\rangle_X \\ &\quad + \langle \varphi^*_{X/Y_2}(\gamma^i_{Y_2/Z}), \varphi^*_{X/Y_2}(\gamma^{i+j}_{Y_2/Z})\rangle_X \\ &\quad + \langle \gamma^i_{12}, \gamma^{i+j}_{12}\rangle_X.\end{aligned}$$

This allows to conclude using Lemma 2.6 and the fact that all the maps $\varphi^*_{\_/\_}$ are isometries. □

3.2.3. ***Number of rational points in a commutative diagram.*** We can now prove the following result.

Theorem 3.7. *Let X, Y_1, Y_2 and Z be absolutely irreducible smooth projective curves in a commutative diagram* (3.1) *of finite morphisms. Suppose that the fiber product $Y_1 \times_Z Y_2$ is 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. In the same way than for the proof of Proposition 3.1, this is Schwarz inequality for γ^0_{12} and γ^1_{12} together with Lemma 3.6. □

For $Y_1 \times_Z Y_2$ to be irreducible, it suffices that the two function fields $\mathbb{F}_q(Y_1)$ and $\mathbb{F}_q(Y_2)$ are linearly disjoint over $\mathbb{F}_q(Z)$ inside $\mathbb{F}_q(X)$; it is moreover absolutely irreducible if $\mathbb{F}_q$ is algebraically closed inside the compositum of $\mathbb{F}_q(Y_1)$ and $\mathbb{F}_q(Y_2)$. For $Y_1 \times_Z Y_2$ to be smooth at a point (Q_1, Q_2), it is necessary and sufficient that at least one of the morphisms $Y_i \to Z$ is unramified at Q_i. Thus it is smooth if and only if the “branch loci” of the covers $Y_i \to Z$ are disjoint.

It worth noticing that Theorem 3.7 cannot hold without any hypothesis. For instance, if $g_Z \geq 2$ and if $X = Y_1 = Y_2$ and if the (non constant) morphisms $Y_i \to Z$ are the same, 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 3.7 does not apply since $Y_1 \times_Z Y_2$ is not irreducible.

Theorem 3.7 is a refinement of Proposition 3.1 since one can recover the latter by taking $Z = Y_1 = Y_2$. In the special case where $X = Y_1 \times_Z Y_2$, one can compute its genus using intersection theory:

$$g_X = d_1 g_{Y_2} + d_2 g_{Y_1} + (d_1 - 1)(d_2 - 1) - d_1 d_2 g_Z$$

or

$$g_X - 1 = d_1 (g_{Y_2} - 1) + d_2 (g_{Y_1} - 1) - d_1 d_2 (g_Z - 1)$$

where we put $d_i = \deg(Y_i \to Z)$ (see [3, Lem. 3]). Hence

$$\begin{aligned}&|\sharp Y_1 \times_Z Y_2(\mathbb{F}_q) - \sharp Y_1(\mathbb{F}_q) - \sharp Y_2(\mathbb{F}_q) + \sharp Z(\mathbb{F}_q)| \\ &\quad \leq 2\left[(d_1 - 1)(g_{Y_2} - 1) + (d_2 - 1)(g_{Y_1} - 1) - (d_1 d_2 - 1)(g_Z - 1)\right]\sqrt{q}.\end{aligned}$$

References

[1] Y. AUBRY & M. PERRET, "Coverings of singular curves over finite fields", *Manuscr. Math.* **88** (1995), no. 4, p. 467-478.

[2] W. FULTON, *Intersection Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 2, Springer, 1998.

[3] E. HALLOUIN & M. PERRET, "Recursive towers of curves over finite fields using graph theory", *Mosc. Math. J.* **14** (2014), no. 4, p. 773-806.

[4] ———, "An unified viewpoint for upper bounds for the number of points of curves over finite fields via euclidean geometry and semi-definite symmetric toeplitz matrices", *Trans. Am. Math. Soc.* **312** (2019), p. 5409-5451.

[5] R. HARTSHORNE, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, 1977.

[6] M. A. TSFASMAN, "Some remarks on the asymptotic number of points", in *Coding theory and algebraic geometry (Luminy, 1991)*, Lecture Notes in Mathematics, vol. 1518, Springer, 1991, p. 178-192.

[7] S. G. VLĂDUŢ & V. DRINFELD, "Number of points of an algebraic curve", *Funct. Anal. Appl.* **17** (1983), p. 53-54.

[8] A. WEIL, *Courbes algébriques et variétés abéliennes*, Actualités Scientifiques et Industrielles, vol. 1064, Hermann, 1948.

Emmanuel HALLOUIN
Institut de Mathématiques de Toulouse ;
UMR 5219, Université de Toulouse ;
CNRS, UT2J
F-31058 Toulouse, France
E-mail: hallouin@univ-tlse2.fr
URL: http://www.math.univ-toulouse.fr/~hallouin/

Marc PERRET
Institut de Mathématiques de Toulouse ;
UMR 5219, Université de Toulouse ;
CNRS, UT2J
F-31058 Toulouse, France
E-mail: perret@univ-tlse2.fr
URL: http://www.math.univ-toulouse.fr/~perret/