Séminaires & Congrès
11, 2005, p. 75–110

ON CURVES OVER FINITE FIELDS

by

Arnaldo Garcia

Abstract. — In these notes we present some basic results of the Theory of Curves over Finite Fields. Assuming a famous theorem of A. Weil, which bounds the number of solutions in a finite field (*i.e.*, number of rational points) in terms of the genus and the cardinality of the finite field, we then prove several other related bounds (bounds of Serre, Ihara, Stohr-Voloch, etc.). We then treat Maximal Curves (classification and genus spectrum). Maximal curves are the curves attaining the upper bound of A. Weil. If the genus of the curve is large with respect to the cardinality of the finite field, Ihara noticed that Weil's bound cannot be reached and he introduced then a quantity $A(q)$ for the study of the asymptotics of curves over a fixed finite field. This leads to towers of curves and we devote special attention to the so-called recursive towers of curves. We present several examples of recursive towers with good asymptotic behaviour, some of them attaining the Drinfeld-Vladut bound. The connection with the asymptotics of linear codes is a celebrated result of Tsfasman-Vladut-Zink, which is obtained via Goppa's construction of codes from algebraic curves over finite fields.

Résumé **(Courbes sur des corps finis).** — Nous présentons des résultats élémentaires sur les courbes sur les corps finis et leurs points rationnels. Nous avons fait un effort pour donner une présentation aussi simple que possible, la rendant accessible aux non spécialistes. Parmi ces résultats se trouvent : le théorème de Weil (l'hypothèse de Riemann dans ce contexte), son amélioration donnée par Serre, la borne de Ihara sur le genre pour les courbes maximales, genre et classification des courbes maximales, théorie de Stohr-Voloch des ordres de Frobenius pour les courbes planes, constructions de courbes sur les corps finis ayant beaucoup de points rationnels, les formules explicites de Serre, étude asymptotique des courbes sur les corps finis et des codes correcteurs d'erreurs (la connexion entre elles est un célèbre théorème de Tsfasman-Vladut-Zink), tours récursives de courbes et certaines tours particulièrement intéressantes (atteignant la borne de Drinfeld-Vladut sur des corps finis de cardinal un carré ou atteignant la borne de Zink sur des corps finis de cardinal un cube).

2000 ***Mathematics Subject Classification***. — 14H05, 11G20 , 14G05.
Key words and phrases. — Algebraic curves, finite fields, rational points, genus, linear codes, asymptotics, tower of curves.

The author was partially supported by PRONEX # 662408/1996-3 (CNPq-Brazil).

1. Introduction

These notes reflect very closely the lectures given by the author at a "European School on Algebraic Geometry and Information Theory", held at C.I.R.M. – Luminy - France in May 2003. They are intended as an invitation to the subject of curves over finite fields. At several points we have sacrificed rigorness (without mention) in favour of clarity or simplicity. Assuming to start with a very deep theorem of André Weil (equivalent to the validity of Riemann's Hypothesis for the situation of zeta functions associated to nonsingular projective curves over finite fields) we then prove several interesting related results with elementary methods (bounds of Serre, Ihara, Stöhr-Voloch, Drinfeld-Vladut, etc.), and we give also several examples illustrating those results.

These notes are organized as follows: Section 2 contains several bounds on the number of rational points of curves over finite fields (see Theorems 2.2, 2.3, 2.14 and 2.17) and examples of curves attaining those bounds. Specially interesting here are the curves attaining Weil's bound, the so-called *maximal curves*; for these curves there is a genus bound due to Ihara (see Proposition 2.8) which originated two basic problems on maximal curves: the genus spectrum problem (see Theorem 2.11) and the classification problem (see Theorems 2.10 and 2.12). For the classification problem a very important tool is the Stöhr-Voloch theory of Frobenius – orders of morphisms of curves over finite fields, and this theory is illustrated here just for projective plane curves (see Theorem 2.17). Section 3 contains two simple and related methods for the construction of curves with many rational points with respect to the genus (called *good curves*). Both constructions lead to projective curves that are Kummer covers of the projective line (or of another curve), and we also present a "recipe" due to Hasse for the genus calculation for such covers. Several examples illustrating both constructions are also presented.

Section 4 explains the basic facts on the asymptotic behaviour of curves and also of linear codes over finite fields. The relation between the two asymptotics (of curves and of codes) is a result due to Tsfasman-Vladut-Zink and this result represents an improvement on the so-called Gilbert-Varshamov bound. We also prove here an asymptotic bound due to Drinfeld-Vladut (see Proposition 4.3) which is obtained as an application of a method of Serre (see Theorem 4.1). This motivates the definition of towers of curves over finite fields which is the subject of Section 5. After introducing the concepts of ramification locus and splitting locus, we explain their significance when the tower is a tame tower (see Theorem 5.1). We then define recursive towers and we give several examples illustrating applications of Theorem 5.1. Wild towers are much harder to deal with than tame towers, and we give at the end of these notes two very interesting examples of wild towers (see Examples 5.8 and 5.9). Example 5.9 is specially interesting since it is over finite fields with cubic cardinalities, and it gives in particular a generalization of a famous lower bound, on the asymptotics of curves, due to T. Zink.

2. Bounds for the number of rational points

Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial (*i.e.*, $f(X,Y)$ is also irreducible over $\overline{\mathbb{F}}_q$ the algebraic closure of the finite field $\mathbb{F}_q$). The associated affine plane curve $\mathcal{C}$ is defined by

$$\mathcal{C} := \{(a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q \mid f(a,b) = 0\}$$

and we denote by $\mathcal{C}(\mathbb{F}_q)$ the set of rational points; *i.e.*,

$$\mathcal{C}(\mathbb{F}_q) = \{(a,b) \in \mathcal{C} \mid a,b \in \mathbb{F}_q\}.$$

Goal. — *Study the cardinality $\#\mathcal{C}(\mathbb{F}_q)$ with respect to the genus $g(\mathcal{C})$.*

The genus $g(\mathcal{C})$ of a plane curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) \leqslant (d-1)(d-2)/2,$$

where $d := \deg f(X,Y)$ is the degree of the irreducible polynomial defining the curve $\mathcal{C}$.

The next lemma gives a simple criterion for absolute irreducibility.

***Lemma 2.1* (See [27]).** — *Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be a polynomial of the following type*

$$f(X,Y) = a_0 \cdot Y^n + a_1(X) \cdot Y^{n-1} + \cdots + a_{n-1}(X) \cdot Y + a_n(X)$$

with $a_0 \in \mathbb{F}_q^*$ and with $a_1(X), \ldots, a_{n-1}(X)$, $a_n(X) \in \mathbb{F}_q[X]$.

Suppose that $\gcd(n, \deg a_n(X)) = 1$ *and that*

$$\frac{\deg a_n(X)}{n} > \frac{\deg a_i(X)}{i} \quad \textit{for each } 1 \leqslant i \leqslant n-1,$$

then the polynomial $f(X,Y)$ is absolutely irreducible.

We are going to deal with more general algebraic curves, not just an affine plane curve. Given $n-1$ polynomials $f_1(X_1,\ldots,X_n), f_2(X_1,\ldots,X_n),\ldots,f_{n-1}(X_1,\ldots,X_n)$ in the polynomial ring $\mathbb{F}_q[X_1,\ldots,X_n]$, they in general define an affine algebraic curve $\mathcal{C}$ as

$$\mathcal{C} := \{(a_1,a_2,\ldots,a_n) \in \overline{\mathbb{F}}_q^n \mid f_j(a_1,\ldots,a_n) = 0 \quad \text{for all } j = 1,2,\ldots,n-1\}$$

and its set $\mathcal{C}(\mathbb{F}_q)$ of rational points as $\mathcal{C}(\mathbb{F}_q) := \{(a_1,\ldots,a_n) \in \mathcal{C} \mid a_1,a_2,\ldots,a_n \in \mathbb{F}_q\}$.

A point P of a curve $\mathcal{C}$ is called *nonsingular* if there exists a tangent line to the curve $\mathcal{C}$ at the point P. For example if $P = (a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ is a point of the plane curve associated to the polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ (*i.e.*, if we have $f(a,b) = 0$), then the point P is called *nonsingular* when

$$f_X(a,b) \neq 0 \quad \text{or} \quad f_Y(a,b) \neq 0,$$

where f_X and f_Y denote the partial derivatives. The curve $\mathcal{C}$ is called *nonsingular* if every point $P \in \mathcal{C}$ is a nonsingular point. Also, we will deal with projective curves here rather than with affine curves. For example, if $\mathcal{C}$ is the plane curve associated to the polynomial $f(X,Y)$ in $\mathbb{F}_q[X,Y]$ with $d := \deg f(X,Y)$, then we define

$$F(X,Y,Z) = Z^d \cdot f\,(X/Z, Y/Z) \quad \text{and} \quad \widetilde{\mathcal{C}} := \{(a:b:c) \in \mathbb{P}^2(\overline{\mathbb{F}}_q) \mid F(a,b,c) = 0\}.$$

The curve $\widetilde{\mathcal{C}}$ is a projective model for the affine curve $\mathcal{C}$ associated to $f(X,Y)$. If the projective plane curve $\widetilde{\mathcal{C}}$ is nonsingular, then we have the equality $g(\widetilde{\mathcal{C}}) = (d-1)(d-2)/2$. A point $(a:b:c)$ of $\widetilde{\mathcal{C}}$ is said to be *at infinity* when $c = 0$.

The next theorem is due to A. Weil and it is the main result in this theory:

***Theorem 2.2* (See [33] and [30], Theor. V.2.3)**. — *Let $\mathcal{C}$ be a projective and nonsingular, absolutely irreducible curve defined over the finite field $\mathbb{F}_q$ with q elements. Then we have*

$$\#\mathcal{C}(\mathbb{F}_q) \leqslant 1 + q + 2\sqrt{q} \cdot g(\mathcal{C}).$$

Theorem 2.2 is a very deep result. It was proved in the particular case of elliptic curves (*i.e.*, the case $g(\mathcal{C}) = 1$) by H. Hasse and in the general case by A. Weil (see [**33**]). Theorem 2.2 says that the zeros of a certain "Congruence Zeta Function" (associated to the curve by E. Artin in analogy with Dedekind's Zeta Function for quadratic number fields) all lie on the critical line $\mathrm{Re}(s) = 1/2$. We can rewrite Theorem 2.2 as follows

***Theorem 2.3* (See [33] and [30], Cor. V.1.16)**. — *Let $\mathcal{C}$ be a projective and nonsingular, absolutely irreducible algebraic curve defined over $\mathbb{F}_q$ and let $g := g(\mathcal{C})$ denote its genus. Then there exist algebraic integers $\alpha_1, \alpha_2, \ldots, \alpha_{2g} \in \mathbb{C}$ with absolute value $|\alpha_j| = \sqrt{q}$, for $1 \leqslant j \leqslant 2g$, such that*

$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 - \sum_{j=1}^{2g} \alpha_j.$$

Clearly, the bound in Theorem 2.2 follows from the equality in Theorem 2.3 by taking $\alpha_j = -\sqrt{q}$, for all values of j with $1 \leqslant j \leqslant 2g$. We now define

Definition 2.4. — Let $q = \ell^2$ be a square. We say that the curve $\mathcal{C}$ is $\mathbb{F}_q$-*maximal* if it attains the bound in Theorem 2.2; *i.e.*, if it holds that

$$\#\mathcal{C}(\mathbb{F}_q) = \ell^2 + 1 + 2\ell \cdot g(\mathcal{C}).$$

***Example 2.5* (Hermitian curve over $\mathbb{F}_{\ell^2}$)**. — Consider the projective plane curve $\mathcal{C}$ defined over the finite field $\mathbb{F}_{\ell^2}$ by the affine equation

$$f(X,Y) = Y^\ell + Y - X^{\ell+1} \in \mathbb{F}_{\ell^2}[X,Y].$$

We have $g(\mathcal{C}) = \ell(\ell-1)/2$; indeed, the curve $\mathcal{C}$ is a nonsingular plane curve with degree d satisfying $d = \ell + 1$. The number of $\mathbb{F}_q$-rational points (with $q = \ell^2$) is given by

$$\#\mathcal{C}(\mathbb{F}_q) = 1 + \ell^3 = 1 + \ell^2 + 2\ell \cdot \frac{\ell(\ell-1)}{2};$$

i.e., the curve $\mathcal{C}$ is $\mathbb{F}_{\ell^2}$-maximal. Indeed, the associated homogeneous polynomial is

$$F(X,Y,Z) = Y^\ell Z + YZ^\ell - X^{\ell+1}$$

and the point $(0:1:0)$ is the unique point at infinity on the curve $\mathcal{C}$. The affine points are the points $(a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ such that

$$b^\ell + b = a^{\ell+1}.$$

Observing that $a^{\ell+1}$ is the norm for the extension $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$ and that $b^\ell + b$ is the trace for $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$, we conclude that

$$\#\mathcal{C}(\mathbb{F}_{\ell^2}) = 1 + \ell^3. \qquad \square$$

The next proposition, due to J.-P. Serre, enables one to construct other $\mathbb{F}_q$-maximal curves from known ones.

Proposition 2.6 **(See [26])**. — *Let $\varphi\colon \mathcal{C} \to \mathcal{C}_1$ be a surjective morphism defined over a finite field $\mathbb{F}_q$ (i.e., both curves $\mathcal{C}$ and $\mathcal{C}_1$, and also the map φ are all defined over the finite field $\mathbb{F}_q$) and suppose that the curve $\mathcal{C}$ is $\mathbb{F}_q$-maximal. Then the curve $\mathcal{C}_1$ is also $\mathbb{F}_q$-maximal.*

Example 2.7. — Let $\mathcal{C}_1$ be the curve defined over $\mathbb{F}_{\ell^2}$ by the following equation

$$f(X,Y) = Y^\ell + Y - X^m, \qquad \text{with } m \text{ a divisor of } \ell+1.$$

This curve $\mathcal{C}_1$ is $\mathbb{F}_{\ell^2}$-maximal. Indeed, this follows from Proposition 2.6 since we have the following surjective morphism (with $n := (\ell+1)/m$)

$$\begin{aligned} \varphi\colon \mathcal{C} &\longrightarrow \mathcal{C}_1 \\ (a,b) &\longmapsto (a^n, b), \end{aligned}$$

where the curve $\mathcal{C}$ is the one given in Example 2.5.

The genus of $\mathcal{C}_1$ satisfies (see Example 3.1 in Section 3)

$$g(\mathcal{C}_1) = (\ell-1)(m-1)/2.$$

One can check directly that the curve $\mathcal{C}_1$ is $\mathbb{F}_q$-maximal with $q = \ell^2$. Indeed, let us denote by H the multiplicative subgroup of $\mathbb{F}^*_{\ell^2}$ with order $|H| = (\ell-1)\cdot m$. We then have:

$$a \in H \cup \{0\} \text{ implies that } a^m \in \mathbb{F}_\ell. \tag{1}$$

Since $b^\ell + b = a^m$ for an affine point $(a,b) \in \mathcal{C}_1$ and since $b^\ell + b$ is the trace for the extension $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$, we get from the assertion in (1) that

$$\#\mathcal{C}_1(\mathbb{F}_{\ell^2}) \geqslant 1 + [1 + m(\ell-1)]\cdot \ell.$$

But we also have that

$$1+[1+m(\ell-1)]\cdot\ell = 1+\ell^2+2\ell\cdot(\ell-1)(m-1)/2. \qquad \square$$

Let $\mathcal{C}$ be an absolutely irreducible algebraic curve (projective and nonsingular) of genus g defined over the finite field $\mathbb{F}_q$ and let

$$\alpha_j \in \mathbb{C} \text{ with } |\alpha_j| = \sqrt{q} \quad \text{for } j=1,2,\ldots,2g,$$

be the algebraic integers mentioned in the statement of Theorem 2.3. Then for each $n \in \mathbb{N}$ we have (see [**30**], Cor. V.1.16)

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} \alpha_j^n. \tag{2}$$

Proposition 2.8 **(See [23])**. — *Let $\mathcal{C}$ be a projective, nonsingular and absolutely irreducible, algebraic curve defined over $\mathbb{F}_q$ with $q=\ell^2$. If $\mathcal{C}$ is a $\mathbb{F}_q$-maximal curve, then*

$$g(\mathcal{C}) \leqslant \ell(\ell-1)/2.$$

Proof. — If $\mathcal{C}$ is $\mathbb{F}_{\ell^2}$-maximal, then

$$\alpha_j = -\ell, \quad \text{for each } j=1,2,\ldots,2g.$$

Hence $\alpha_j^2 = \ell^2$, for each $j=1,2,\ldots,2g$.

Clearly we have that

$$\#\mathcal{C}(\mathbb{F}_{q^2}) \geqslant \#\mathcal{C}(\mathbb{F}_q).$$

Using now the equality in (2) for $n=1$ and $n=2$, we conclude that

$$1+\ell^4-2g\cdot\ell^2 \geqslant 1+\ell^2+2g\cdot\ell,$$

and hence that $2g(\mathcal{C}) \leqslant \ell(\ell-1)$. $\square$

Remark 2.9. — Proposition 2.8 says that the genus of a $\mathbb{F}_{\ell^2}$-maximal curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) \leqslant \ell(\ell-1)/2.$$

The bound above is sharp. The Hermitian curve given in Example 2.5 is $\mathbb{F}_{\ell^2}$-maximal with genus $g(\mathcal{C}) = \ell(\ell-1)/2$.

The following result is the starting point for the classification problem of maximal curves over finite fields.

Theorem 2.10 **(See [28])**. — *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{\ell^2}$ with genus satisfying $g(\mathcal{C}) = \ell(\ell-1)/2$. Then the curve $\mathcal{C}$ is isomorphic over the field $\mathbb{F}_{\ell^2}$ with the projetive curve given by the affine equation*

$$f(X,Y) = Y^\ell + Y - X^{\ell+1} \in \mathbb{F}_{\ell^2}[X,Y].$$

Not every natural number g with $g \leqslant \ell(\ell-1)/2$ is the genus of a $\mathbb{F}_{\ell^2}$-maximal curve. Indeed we have the following very interesting result:

***Theorem 2.11* (See [9]).** — *Let $\mathcal{C}$ be a maximal curve over the finite field $\mathbb{F}_{\ell^2}$ with genus satisfying $g(\mathcal{C}) \neq \ell(\ell-1)/2$. Then we have*

$$g(\mathcal{C}) \leqslant \frac{(\ell-1)^2}{4}.$$

According to Theorem 2.11 the second possible biggest genus g_2 of a $\mathbb{F}_{\ell^2}$-maximal curve is given by

$$g_2 = \begin{cases} \ell(\ell-2)/4 & \text{if } \ell \text{ is even} \\ (\ell-1)^2/4 & \text{if } \ell \text{ is odd.} \end{cases}$$

In case ℓ is odd we have that the equation

(3) $$Y^{\ell} + Y = X^{(\ell+1)/2} \text{ over } \mathbb{F}_{\ell^2}$$

defines a $\mathbb{F}_{\ell^2}$-maximal curve $\mathcal{C}_1$ of genus $g = (\ell-1)^2/4$. In case ℓ is even (*i.e.*, ℓ is a power of $p=2$) we have that the equation

(4) $$Y^{\ell/2} + Y^{\ell/4} + \cdots + Y^2 + Y = X^{\ell+1} \text{ over } \mathbb{F}_{\ell^2}$$

defines a $\mathbb{F}_{\ell^2}$-maximal curve $\mathcal{C}_0$ of genus $g = \ell(\ell-2)/4$. The curve $\mathcal{C}_1$ given by Eq.(3) above was already considered in Example 2.7. The curve $\mathcal{C}_0$ given by Eq.(4) above is also a quotient of the Hermitian curve $\mathcal{C}$ over $\mathbb{F}_{\ell^2}$ given in Example 2.5. In fact consider the map φ below

$$\begin{aligned} \varphi\colon \mathcal{C} &\longrightarrow \mathcal{C}_0 \\ (a,b) &\longmapsto (a, b^2+b). \end{aligned}$$

It is straighforward to check that if the point (a,b) satisfies $b^{\ell} + b = a^{\ell+1}$, then the point (a, b^2+b) satisfies Equation (4) above. It then follows from Proposition 2.6 that the curve $\mathcal{C}_0$ is also $\mathbb{F}_{\ell^2}$-maximal. Here again we have uniqueness:

***Theorem 2.12* (See [8], [1] and [25]).** — *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{\ell^2}$ with the second biggest genus $g_2 := \left[(\ell-1)^2/4\right]$. Then the curve $\mathcal{C}$ is isomorphic over $\mathbb{F}_{\ell^2}$ either to the curve $\mathcal{C}_1$ given by Eq.(3) if ℓ is odd, or to the curve $\mathcal{C}_0$ given by Eq.(4) if ℓ is even.*

***Remark 2.13*.** — Besides the action of Frobenius on the Jacobian Variety of a maximal curve (which is the main tool in proving Theorem 2.10), the other important ingredient in the proof of Theorem 2.12 is the theory due to Stöhr-Voloch of Frobenius – orders of morphisms of curves over finite fields (see [**31**]).

We are now going to explain an improvement of Theorem 2.2 due to J.-P. Serre. For an algebraic curve of genus g defined over the finite field $\mathbb{F}_q$, we denote by $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ the algebraic integers with $|\alpha_j| = \sqrt{q}$ mentioned in the statement of Theorem 2.3. It is possible to show that (see [**30**], Theor. V.1.15)

$$\prod_{j=1}^{2g}(1-\alpha_j t) \in \mathbb{Z}[t]$$

and that one can rearrange $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ so that

$$\alpha_{g+j} = \overline{\alpha}_j \quad \text{for each } j = 1, 2, \ldots, g,$$

where $\overline{\alpha}_j$ denotes the complex conjugate of $\alpha_j \in \mathbb{C}$.

***Theorem 2.14* (See [29]).** — *Let $\mathcal{C}$ be a projective, nonsingular and absolutely irreducible, algebraic curve defined over $\mathbb{F}_q$. Then we have*

$$\#\mathcal{C}(\mathbb{F}_q) \leqslant 1 + q + [2\sqrt{q}] \cdot g(\mathcal{C}),$$

where $[2\sqrt{q}]$ denotes the integer part of $2\sqrt{q}$.

Proof. — We fix an ordering of $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ satisfying

$$\alpha_{g+j} = \overline{\alpha}_j \quad \text{for each } j = 1, 2, \ldots, g.$$

Since $\alpha_j \cdot \overline{\alpha}_j = q$ we then have

$$\alpha_{g+j} = \overline{\alpha}_j = q/\alpha_j \quad \text{for } j = 1, 2, \ldots, g.$$

Setting $\beta_j = \alpha_j + \overline{\alpha}_j + [2\sqrt{q}] + 1$, for each $j = 1, 2, \ldots, g$, we see that

$$\beta_j \in \mathbb{R} \quad \text{and} \quad \beta_j > 0.$$

Since α_j is an algebraic integer, we have that β_j is also an algebraic integer, for each $j = 1, 2, \ldots, g$. Consider now the number field E generated by $\alpha_1, \ldots, \alpha_{2g}$; *i.e.*, consider

$$E := \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g}).$$

The extension $E/\mathbb{Q}$ is Galois since E is the splitting field over $\mathbb{Q}$ of the polynomial $\prod_{j=1}^{2g}(1-\alpha_j t) \in \mathbb{Z}[t]$. Hence if σ belongs to the Galois group; *i.e.*, if $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$, then σ induces a permutation of the set $\{\alpha_1, \ldots, \alpha_{2g}\}$. Suppose that $\sigma(\alpha_i) = \alpha_j$. Then

$$\sigma(\overline{\alpha}_i) = \sigma(q/\alpha_i) = \frac{\sigma(q)}{\sigma(\alpha_i)} = \frac{q}{\alpha_j} = \overline{\alpha}_j.$$

Hence we have $\sigma(\beta_i) = \beta_j$ and the automorphism σ also induces a permutation of the set $\{\beta_1, \ldots, \beta_g\}$. The element $\left(\prod_{j=1}^{g} \beta_j\right)$ is then left fixed by all automorphisms σ of $\mathrm{Aut}(E/\mathbb{Q})$, and hence $\left(\prod_{j=1}^{g} \beta_j\right) \in \mathbb{Q}$. Since each β_j (for $j = 1, 2, \ldots, g$) is an algebraic integer, we conclude that $\left(\prod_{j=1}^{g} \beta_j\right) \in \mathbb{Z}$. Since $\beta_j > 0$, we have that $\left(\prod_{j=1}^{g} \beta_j\right) \geqslant 1$. From the inequality below relating arithmetic and geometric mean

$$\frac{1}{g} \cdot \Big(\sum_{j=1}^{g} \beta_j\Big) \geqslant \Big(\prod_{j=1}^{g} \beta_j\Big)^{1/g},$$

we then get

$$\sum_{j=1}^{g}(\alpha_j + \overline{\alpha}_j + [2\sqrt{q}] + 1) \geqslant g$$

and hence that

$$\sum_{j=1}^{2g}\alpha_j \geqslant -g\cdot[2\sqrt{q}].$$

The inequality above and Theorem 2.3 finish the proof of Theorem 2.14. □

Exercise. — Using similar arguments as in the proof of Theorem 2.14 with

$$\widetilde{\beta}_j := -(\alpha_j + \overline{\alpha}_j) + [2\sqrt{q}] + 1, \quad \text{for } j = 1, 2, \ldots, g,$$

show that the following lower bound holds:

$$\#\mathcal{C}(\mathbb{F}_q) \geqslant 1 + q - [2\sqrt{q}]\cdot g(\mathcal{C}).$$

***Example 2.15* (Klein quartic)**. — Consider the case

$$q = 8 \quad \text{and} \quad g(\mathcal{C}) = 3.$$

In this case the bound in Theorem 2.14 is

$$\#\mathcal{C}(\mathbb{F}_8) \leqslant 24.$$

Consider the projective curve $\mathcal{C}$ over $\mathbb{F}_8$ given by the affine equation

$$f(X,Y) = Y^3 + X^3Y + X \in \mathbb{F}_8[X,Y].$$

The projective plane curve $\mathcal{C}$ is nonsingular and hence

$$g(\mathcal{C}) = \frac{(d-1)(d-2)}{2} = \frac{(4-1)(4-2)}{2} = 3.$$

The points at infinity on the curve $\mathcal{C}$ are

$$Q_1 = (1:0:0) \quad \text{and} \quad Q_2 = (0:1:0),$$

and the point $Q_3 = (0:0:1)$ is the other point $(a:b:c)$ on $\mathcal{C}$ satisfying $a\cdot b\cdot c = 0$. We want to show that

$$\#\mathcal{C}(\mathbb{F}_8) = 24;$$

i.e., the curve $\mathcal{C}$ above attains Serre's bound over the finite field with 8 elements. We have the points Q_1, Q_2 and Q_3 above, and we still need to find 21 points $(a:b:1)$ on $\mathcal{C}(\mathbb{F}_8)$; *i.e.*, we still need to find 21 points $(a,b) \in \mathbb{F}_8^* \times \mathbb{F}_8^*$ such that it holds

$$b^3 + a^3b + a = 0.$$

Multiplying the equality above by a^6 we get (since $a^7 = 1$ and $a^9 = a^2$)

$$w^3 + w + 1 = 0 \quad \text{with } w = a^2b.$$

The three solutions of $w^3 + w + 1 = 0$ are elements of $\mathbb{F}_8$, and to each $a \in \mathbb{F}_8^*$ and each $w \in \mathbb{F}_8^*$ satisfying $w^3 + w + 1 = 0$, one defines $b := w/a^2$. This then gives us the 21 points (a,b) belonging to the set $\mathcal{C}(\mathbb{F}_8)$. □

Exercise. — Let $\mathcal{C}$ be a curve (projective and nonsingular) of genus g attaining Serre's bound over the finite field $\mathbb{F}_q$; *i.e.*, we have the equality

$$\#\mathcal{C}(\mathbb{F}_q) = 1 + q + [2\sqrt{q}] \cdot g.$$

(a) With notation as in the proof of Theorem 2.14, show that

$$\beta_j = 1, \quad \text{for each } j = 1, 2, \ldots, g.$$

Hint. Use that the inequality relating arithmetic and geometric mean is an equality if and only if we have that $\beta_1 = \beta_2 = \cdots = \beta_g$.

(b) Setting $\gamma := [2\sqrt{q}]$, show that

$$\alpha_i^2 + \overline{\alpha}_i^2 = \gamma^2 - 2q, \qquad \text{for each } i = 1, 2, \ldots, g.$$

(c) With similar arguments as the ones used in the proof of Proposition 2.8, show that

$$g \leqslant \frac{q^2 - q}{\gamma^2 + \gamma - 2q}.$$

(d) Show that

$$\prod_{j=1}^{2g} (1 - \alpha_j t) = (1 + \gamma t + q t^2)^g.$$

We are now going to introduce another method for counting and bounding the number of rational points on curves (projective, nonsingular and absolutely irreducible) over finite fields. This method is due to Stöhr and Voloch (see [**31**]), and it gives in particular also a proof of Theorem 2.2. This theory of Stöhr and Voloch is similar to Weierstrass Point Theory and here we are going to illustrate it just for the case of nonsingular projective plane curves. Let then $\mathcal{C}$ be a nonsingular projective plane curve with degree equal to d (*i.e.*, the genus is $g(\mathcal{C}) = (d-1)(d-2)/2$), and let $F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ be the corresponding homogeneous polynomial of degree equal to d. For a projective point $P = (a : b : c) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ belonging to the curve $\mathcal{C}$; *i.e.*, for a point $P = (a : b : c)$ such that $F(a, b, c) = 0$, we denote by $T_P(\mathcal{C})$ the tangent line to $\mathcal{C}$ at P which is the line defined by the following linear equation

$$F_X(a, b, c) \cdot X + F_Y(a, b, c) \cdot Y + F_Z(a, b, c) \cdot Z = 0,$$

where F_X, F_Y and F_Z denote the partial derivatives. For a point $P = (a : b : c) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ we denote by

$$\mathrm{Fr}(P) := (a^q : b^q : c^q).$$

Because the equation $F(X, Y, Z)$ defining the curve $\mathcal{C}$ has coefficients in the finite field $\mathbb{F}_q$, it is clear that $P \in \mathcal{C}$ implies that $\mathrm{Fr}(P) \in \mathcal{C}$.

Roughly speaking the method of Stöhr and Voloch instead of counting $\mathbb{F}_q$-rational points; *i.e.*, instead of investigating the cardinality of the set

$$\{P \in \mathcal{C} \mid \mathrm{Fr}(P) = P\},$$

it investigates the cardinality of the following possibly bigger set

$$\{P \in \mathcal{C} \mid \mathrm{Fr}(P) \in T_P(\mathcal{C})\}. \tag{5}$$

We must avoid the situation where the set given in (5) above is not a finite set; *i.e.*, we must avoid the situation where it holds that the set given in (5) is the whole curve $\mathcal{C}$.

Example 2.16. — Let $\mathcal{C}$ be the Hermitian curve over $\mathbb{F}_{\ell^2}$ introduced in Example 2.5; *i.e.*, the corresponding homogeneous polynomial $F(X, Y, Z)$ is given by

$$F(X, Y, Z) = Y^\ell Z + YZ^\ell - X^{\ell+1} \in \mathbb{F}_{\ell^2}[X, Y, Z].$$

In this case we have that the set given in (5) is the whole curve $\mathcal{C}$; *i.e.*,

$$\mathcal{C} = \{P \in \mathcal{C} \mid \mathrm{Fr}(P) \in T_P(\mathcal{C})\}.$$

Indeed at an affine point $P = (a : b : 1)$ belonging to the curve $\mathcal{C}$ we have that the tangent line $T_P(\mathcal{C})$ has the following linear equation

$$Y - a^\ell X + b^\ell Z = 0.$$

Also we have $\mathrm{Fr}(P) = (a^{\ell^2} : b^{\ell^2} : 1)$ and we have to check that the following equality holds

$$b^{\ell^2} - a^\ell \cdot a^{\ell^2} + b^\ell = 0.$$

The equality above follows from $b^\ell + b = a^{\ell+1}$ by raising it to the ℓ-th power. □

***Theorem 2.17* (See [31])**. — *Suppose that $f(X, Y) \in \mathbb{F}_q[X, Y]$ is an absolutely irreducible polynomial of degree d which defines a nonsingular projective plane curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$. Suppose moreover that*

$$(X - X^q)f_X(X, Y) + (Y - Y^q)f_Y(X, Y) \not\equiv 0 \mod f(X, Y).$$

Then

$$\#\mathcal{C}(\mathbb{F}_q) \leqslant \frac{1}{2} \cdot d \cdot (d + q - 1).$$

Remark 2.18. — The hypothesis

$$(X - X^q)f_X(X, Y) + (Y - Y^q)f_Y(X, Y) \not\equiv 0 \mod f(X, Y)$$

is equivalent to the hypothesis that the set $\{P \in \mathcal{C} \mid \mathrm{Fr}(P) \in T_P(\mathcal{C})\}$ is not the whole curve $\mathcal{C}$. Here if $P = (a : b : c)$ then $\mathrm{Fr}(P) = (a^q : b^q : c^q)$.

Proof of Theorem 2.17. — We will need some simple properties of intersection numbers of plane projective curves (see [**10**], Ch. III). For an affine point $(a, b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ and for two relatively prime polynomials $f(X, Y)$ and $h(X, Y)$, the symbol $I(P\,;\, f \cap h)$ denotes the intersection number at the point P of the curve given by $f = 0$ with the one given by the equation $h = 0$. It satisfies the following two properties:

Property a) $I(P\,;\, f \cap h) > 0$ if and only if $f(P) = h(P) = 0$.

Property b) $I(P\,;\,f\cap h)\geqslant 2$ if we have $T_P(f)=T_P(h)$; *i.e.*, if we have that the curves given by $f=0$ and $h=0$ have the same tangent line at P.

Let now $f(X,Y)\in\mathbb{F}_q[X,Y]$ be as in the statement of Theorem 2.17, and set

$$h(X,Y):=(X-X^q)f_X(X,Y)+(Y-Y^q)f_Y(X,Y).$$

Since $f(X,Y)$ is irreducible and $h\not\equiv 0 \bmod f$, we have that $f(X,Y)$ and $h(X,Y)$ are relatively prime polynomials. Also clearly

$$\deg h(X,Y)\leqslant q+d-1,\quad \text{with } d=\deg f(X,Y).$$

If $P=(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ is a rational point on the curve $\mathcal{C}$ (*i.e.*, we have $f(a,b)=0$) then we also have that $h(P)=h(a,b)=0$. We are going to show that the curves $f=0$ and $h=0$ have the same tangent line at the point P; *i.e.*, we are going to show that

$$f_X(a,b)=h_X(a,b)\quad\text{and}\quad f_Y(a,b)=h_Y(a,b).$$

From this and from Property b) above we conclude

$$I(P\,;\,f\cap h)\geqslant 2\qquad\text{for each rational point } P\in\mathcal{C}(\mathbb{F}_q).$$

Indeed we have

$$h_X(X,Y)=(X-X^q)f_{XX}+(Y-Y^q)f_{XY}+f_X$$
$$h_Y(X,Y)=(X-X^q)f_{XY}+(Y-Y^q)f_{YY}+f_Y$$

and hence for a point $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ we have

$$h_X(a,b)=f_X(a,b)\quad\text{and}\quad h_Y(a,b)=f_Y(a,b).$$

Now we conclude that

$$\#\mathcal{C}(\mathbb{F}_q)\leqslant\frac{1}{2}\sum_P I(P\,;\,f\cap h),$$

where P runs over all points of the curve $\mathcal{C}$.

From Bezout's Theorem (see [**10**], Ch. V) we know

$$\sum_P I(P\,;\,f\cap h)=\deg f\cdot\deg h\leqslant d\cdot(q+d-1).$$

This finishes the proof of Theorem 2.17. □

Example 2.19. — Consider the projective curve $\mathcal{C}$ over $\mathbb{F}_5$ given by the affine equation

$$f(X,Y)=X^4+Y^4-2\in\mathbb{F}_5[X,Y].$$

The projective curve $\mathcal{C}$ is nonsingular and hence $g(\mathcal{C})=3$. Any point $(a,b)\in\mathbb{F}_5^*\times\mathbb{F}_5^*$ belongs to the curve $\mathcal{C}$ and it is easy to check that

$$\#\mathcal{C}(\mathbb{F}_5)=4\cdot 4=16=\frac{1}{2}\cdot 4\cdot(4+5-1);$$

i.e., the curve $\mathcal{C}$ attains the bound in Theorem 2.17. We leave to the reader to check that the hypothesis of Theorem 2.17 are satisfied in our case. □

Example 2.20. — Consider the projective curve $\mathcal{C}$ over $\mathbb{F}_{13}$ given by the affine equation

$$f(X,Y) = w^2X^4 + Y^4 + w \in \mathbb{F}_{13}[X,Y],$$

where $w \in \mathbb{F}_{13}$ satisfies $w^2 + w + 1 = 0$. The set of rational points over $\mathbb{F}_{13}$ on the affine part of the curve $\mathcal{C}$ is the union of the following two sets:

$$\{(a,b) \mid a^4 = b^4 = 1\} \quad \text{and} \quad \{(a,b) \mid a^4 = w \text{ and } b^4 = w^2\}.$$

Hence we have

$$\#\mathcal{C}(\mathbb{F}_{13}) = 16 + 16 = \frac{1}{2} \cdot 4 \cdot (4 + 13 - 1);$$

i.e., the curve $\mathcal{C}$ attains the bound in Theorem 2.17. We leave again to the reader to check that the hypothesis of Theorem 2.17 are satisfied also in this case. □

The following proposition substitutes the hypothesis in Theorem 2.17

$$h(X,Y) := (X - X^q)f_X(X,Y) + (Y - Y^q)f_Y(X,Y) \not\equiv 0 \mod f(X,Y),$$

by the more natural hypothesis below:

$$f_{XX} \cdot f_Y^2 - 2f_{XY} \cdot f_X \cdot f_Y + f_{YY} \cdot f_X^2 \not\equiv 0 \mod f.$$

Proposition 2.21. — *Let $h(X,Y)$ be the polynomial defined above. If $h(X,Y) \equiv 0 \mod f(X,Y)$, then we also have that*

$$f_{XX} \cdot f_Y^2 - 2f_{XY} \cdot f_X \cdot f_Y + f_{YY} \cdot f_X^2 \equiv 0 \mod f.$$

Proof. — For two polynomials $g_1(X,Y)$ and $g_2(X,Y)$ we will write $g_1 \equiv g_2$ if we have that the polynomial $f(X,Y)$ divides the difference $(g_2 - g_1)$.

The hypothesis $h \equiv 0$ means that

$$(X - X^q)f_X \equiv -(Y - Y^q)f_Y.$$

We then have also

$$\begin{aligned}(X - X^q)^2 &\cdot (f_{XX} \cdot f_Y^2 - 2f_{XY} \cdot f_X \cdot f_Y + f_{YY} \cdot f_X^2) \\ &\equiv f_Y^2 \cdot [(X - X^q)^2 \cdot f_{XX} + 2(X - X^q)(Y - Y^q) \cdot f_{XY} + (Y - Y^q)^2 \cdot f_{YY}].\end{aligned}$$

Hence it is enough to show that

$$(X - X^q)^2 \cdot f_{XX} + 2(X - X^q)(Y - Y^q) \cdot f_{XY} + (Y - Y^q)^2 \cdot f_{YY} \equiv 0.$$

Again from the hypothesis $h \equiv 0$ we have that

$$(X - X^q)f_X + (Y - Y^q)f_Y = f \cdot g, \quad \text{for some polynomial } g.$$

Taking partial derivative with respect to the variable X of the equality above and multiplying afterwards by $(X - X^q)$, we get

$$(X - X^q)^2 \cdot f_{XX} + (X - X^q)(Y - Y^q) \cdot f_{XY} \equiv (X - X^q)(g - 1) \cdot f_X.$$

Similarly taking partial derivative with respect to the variable Y and multiplying afterwards by $(Y - Y^q)$, we get

$$(Y - Y^q)^2 \cdot f_{YY} + (X - X^q)(Y - Y^q) \cdot f_{XY} \equiv (Y - Y^q)(g - 1) \cdot f_Y.$$

Summing up the last two congruences we then get

$$(X - X^q)^2 \cdot f_{XX} + 2(X - X^q)(Y - Y^q) \cdot f_{XY} + (Y - Y^q)^2 \cdot f_{YY} \equiv 0,$$

since we have that $h(X, Y) = (X - X^q)f_X + (Y - Y^q)f_Y \equiv 0$ by the hypothesis. □

We return now to maximal curves over $\mathbb{F}_{\ell^2}$. The results already presented here (specially Prop. 2.8 and Theorem 2.10) lead to two natural problems on maximal curves:

Genus Spectrum. — *Asks for the determination of the set of genus of maximal curves over $\mathbb{F}_{\ell^2}$; i.e., the determination of the set*

$$\Lambda(\ell^2) = \{g(\mathcal{C}) \mid \mathcal{C} \text{ is } \mathbb{F}_{\ell^2}\text{-maximal}\}.$$

Classification. — *For an element $g \in \Lambda(\ell^2)$ one asks for the determination of all maximal curves $\mathcal{C}$ over $\mathbb{F}_{\ell^2}$ (up to isomorphisms) with genus $g(\mathcal{C}) = g$.*

The main tool for the genus spectrum problem is Proposition 2.6 (see [**17**] and also [**6**]). The main tool for the classification problem is Stöhr-Voloch theory of Frobenius-orders of morphisms of curves over finite fields (see [**31**]). A very particular case of this general theory is given here in Theorem 2.17. Another interesting question on maximal curves is the following (compare with Prop. 2.6):

Question. — *Let $\mathcal{C}_1$ be a $\mathbb{F}_{\ell^2}$-maximal curve. Does there exist a surjective morphism defined over the finite field $\mathbb{F}_{\ell^2}$*

$$\varphi \colon \mathcal{C} \longrightarrow \mathcal{C}_1,$$

where the curve $\mathcal{C}$ is the Hermitian curve over $\mathbb{F}_{\ell^2}$ presented in Example 2.5?

An interesting result connected to the question above is that every maximal curve over $\mathbb{F}_{\ell^2}$ is contained in a Hermitian Variety of degree $(\ell+1)$ (see [**24**]). Another very interesting paper, leading to the construction of many maximal curves, is due to van der Geer and van der Vlugt (see [**19**]).

3. Some constructions of good curves

The constructions we are going to present here lead to Kummer covers of the projective line (or fibre products of such covers) and we are going to need the following recipe due to Hasse for the determination of the genus (see [**22**] or [**30**], Section III.7):

Recipe. — Let $\mathcal{C}$ be the nonsingular projective model of the curve given by the equation below

$$Y^m = f(X) \quad \text{with } f(X) \in \mathbb{F}_q(X),$$

where $m \in \mathbb{N}$ satisfies $\gcd(m, q) = 1$. Write the rational function $f(X)$ as

$$f(X) = \frac{g(X)}{h(X)} \quad \text{with } g(X),\ h(X) \in \mathbb{F}_q[X]$$

and with $g(X)$ and $h(X)$ relatively prime polynomials. For an element $\alpha \in \overline{\mathbb{F}}_q$ define

$$m(\alpha) := \ \mathrm{mult}(\alpha \mid g \cdot h) \quad \text{and} \quad d(\alpha) := \gcd(m, m(\alpha)),$$

where $\mathrm{mult}(\alpha \mid g \cdot h)$ means the multiplicity of the element α as a root of the product polynomial $g(X) \cdot h(X)$. For $\alpha = \infty$ we also define

$$m(\infty) := |\deg g - \deg h| \quad \text{and} \quad d(\infty) := \gcd(m, m(\infty)).$$

Then the genus $g(\mathcal{C})$ of the curve $\mathcal{C}$ is given by

$$2g(\mathcal{C}) - 2 = -2m + \sum_{\alpha} (m - d(\alpha)),$$

where the sum is over the elements $\alpha \in \overline{\mathbb{F}}_q \cup \{\infty\}$. The sum above is actually a finite sum: either $\alpha = \infty$ or the element $\alpha \in \overline{\mathbb{F}}_q$ is a root of the product $g(X) \cdot h(X)$.

Example 3.1. — We show here that the genus $g(\mathcal{C}_1)$ of the curve $\mathcal{C}_1$ in Example 2.7 satisfies

$$g(\mathcal{C}_1) = (\ell - 1)(m - 1)/2.$$

Interchanging the variables X and Y, the curve $\mathcal{C}_1$ is then given by (here m divides $\ell + 1$ and hence $\gcd(m, \ell) = 1$) :

$$Y^m = X^\ell + X \text{ over } \mathbb{F}_{\ell^2}.$$

At the elements $\alpha \in \overline{\mathbb{F}}_\ell$ such that $\alpha^\ell + \alpha = 0$, we have $m(\alpha) = 1$ and $d(\alpha) = 1$. For the element $\alpha = \infty$, we have $m(\infty) = \ell$ and $d(\infty) = \gcd(m, \ell) = 1$. Using the recipe above we then get

$$2g(\mathcal{C}_1) - 2 = -2m + (\ell + 1)(m - 1), \quad \text{and hence} \quad g(\mathcal{C}_1) = (\ell - 1)(m - 1)/2. \qquad \square$$

Exercise. — Show that the genus of the curve $\mathcal{C}_0$ given by (see Eq.(4)):

$$Y^{\ell+1} = X^{\ell/2} + X^{\ell/4} + \cdots + X^2 + X, \text{ with } \ell \text{ a power of } 2,$$

satisfies $g(\mathcal{C}_0) = (\ell - 2)\ell/4$.

Exercise. — Consider the projective plane curve $\widetilde{\mathcal{C}}$ over $\mathbb{F}_{\ell^2}$ given by the following affine equation (here ℓ is an odd prime power):

$$f(X, Y) = X^{(\ell+1)/2} + Y^{(\ell+1)/2} - 1 \in \mathbb{F}_{\ell^2}[X, Y].$$

One can check that the curve $\widetilde{\mathcal{C}}$ is nonsingular and hence that

$$g(\widetilde{\mathcal{C}}) = \frac{(d-1)(d-2)}{2} = \frac{(\frac{\ell+1}{2}-1)(\frac{\ell+1}{2}-2)}{2} = \frac{(\ell-1)(\ell-3)}{8}.$$

Prove the genus formula above using the recipe given in the beggining of Section 3.

Remark. — The curve $\widetilde{\mathcal{C}}$ in the above exercise is a maximal curve over $\mathbb{F}_{\ell^2}$. It can be shown (see [**5**]) that it is the unique maximal curve over $\mathbb{F}_{\ell^2}$ having genus $g = (\ell-1)(\ell-3)/8$ that possesses a nonsingular projective plane model over the finite field $\mathbb{F}_{\ell^2}$.

Exercise. — Consider the projective plane curve $\mathcal{C}$ given by the following affine equation

$$f(X,Y) = X^{\ell+1} + Y^{\ell+1} - 1 \in \mathbb{F}_{\ell^2}[X,Y].$$

Prove that the curve $\mathcal{C}$ is $\mathbb{F}_{\ell^2}$-maximal with genus $g(\mathcal{C}) = \ell(\ell-1)/2$.

Remark. — It follows from Theorem 2.10 that the projective plane curve $\mathcal{C}$ in the exercise above is $\mathbb{F}_{\ell^2}$-isomorphic to the Hermitian curve of Example 2.5. Indeed choose two elements $\alpha, \beta \in \mathbb{F}_{\ell^2}$ such that

$$\alpha^\ell + \alpha = \beta^{\ell+1} = -1.$$

Set

$$X_1 := \frac{1}{Y - \beta X} \quad \text{and} \quad Y_1 := \beta X X_1 - \alpha.$$

One can show easily that if the variables X and Y satisfy

$$X^{\ell+1} + Y^{\ell+1} - 1 = 0,$$

then the functions X_1 and Y_1 defined above satisfy

$$Y_1^\ell + Y_1 - X_1^{\ell+1} = 0. \qquad \square$$

Method of Construction. — We are going to consider Kummer covers of the projective line over the finite field $\mathbb{F}_q$; *i.e.*, projective curves given by an affine equation of the type:

$$Y^m = f(X) \in \mathbb{F}_q(X), \quad \text{with } m \text{ a divisor of } (q-1).$$

The idea behind the method is to construct suitable rational functions $f(X)$ with "few zeros and poles" such that $f(\alpha) = 1$ for "many elements" α in $\mathbb{F}_q$.

Construction 1 (see [**20**]*).* — Let $R(X) \in \mathbb{F}_q[X]$ be a polynomial having all roots in the finite field $\mathbb{F}_q$, and split it as below

$$R(X) = g(X) - h(X) \quad \text{with } g(X), h(X) \in \mathbb{F}_q[X].$$

For a divisor m of $(q-1)$ one considers the projective curve $\mathcal{C}$ given by the affine equation

$$Y^m = \frac{g(X)}{h(X)}.$$

– If $\alpha \in \mathbb{F}_q$ is such that $R(\alpha) = 0$ and $g(\alpha) \neq 0$, then $g(\alpha)/h(\alpha) = 1$ and hence we have

$$\#\mathcal{C}(\mathbb{F}_q) \geqslant m \cdot \#\{\alpha \mid R(\alpha) = 0 \text{ and } g(\alpha) \neq 0\}.$$

– The genus $g(\mathcal{C})$ is obtained with the recipe given in the beggining of this section. In order to obtain a curve $\mathcal{C}$ of small genus one needs the following property :

Desired property. — The product $g(X) \cdot h(X)$ is highly inseparable.

In other words, in order to get a curve $\mathcal{C}$ of small genus one needs that the product polynomial $g(X) \cdot h(X)$ has just a few number of distinct roots. This assertion follows directly from the recipe for the genus of Kummer covers.

Example 3.2. — Consider the polynomial $R(X) = X^{16} + X \in \mathbb{F}_{16}[X]$. We split it as

$$R(X) = g(X) - h(X) \quad \text{with } g(X) = X^{16} + X^2 \text{ and } h(X) = X^2 + X,$$

and we then consider the projective curve $\mathcal{C}$ given by

$$Y^{15} = \frac{(X^8 + X)^2}{(X^2 + X)}.$$

The rational function $g(X)/h(X)$ has a simple zero at the elements $\alpha \in \mathbb{F}_2$, it has a double zero at the elements $\alpha \in \mathbb{F}_8 \smallsetminus \mathbb{F}_2$ and it has a pole of order 14 at $\alpha = \infty$. In any case we have that

$$d(\alpha) = \gcd(15, m(\alpha)) = 1.$$

Hence the recipe for the genus gives

$$2g(\mathcal{C}) - 2 = 15(-2) + 9 \cdot (15 - 1) \text{ and hence that } g(\mathcal{C}) = 49.$$

For the $\mathbb{F}_{16}$-rational points we have

$$\#\mathcal{C}(\mathbb{F}_{16}) \geqslant 15 \cdot (16 - 2) = 210.$$

Adding the points $(0, 0)$ and $(1, 0)$, and also the point at infinity, we get

$$\#\mathcal{C}(\mathbb{F}_{16}) = 213.$$

□

Remark. — To check that the curve constructed is a *good curve* (*i.e.*, it has many rational points with respect to its genus) one should look at the tables of curves over finite fields in [**18**]. For a fixed pair q and g the information on this table is given as

$$A \leqslant N \leqslant B.$$

This means that B is the best upper bound known for the number N of $\mathbb{F}_q$-rational points on curves over $\mathbb{F}_q$ having genus $= g$, and that one knows the existence of a curve $\mathcal{C}$ over $\mathbb{F}_q$ of genus g with $\#\mathcal{C}(\mathbb{F}_q) \geqslant A$. For example looking at the table in [**18**] for $q = 16$ and $g = 49$, one finds there the information $A = 213$. This information is provided by the projective curve $\mathcal{C}$ considered in Example 3.2 above.

Construction 2 (see [**12**] *and* [**11**]*).* — This construction is a variant of Construction 1. We start again with a polynomial $R(X) \in \mathbb{F}_q[X]$ having all roots in the finite field $\mathbb{F}_q$. For a polynomial $g(X) \in \mathbb{F}_q[X]$ which is not a multiple of $R(X)$, we perform the euclidean algorithm; *i.e.*, we have

$$g(X) = t(X) \cdot R(X) + h(X)$$

where $t(X), h(X) \in \mathbb{F}_q[X]$ and $\deg h(X) < \deg R(X)$.

We then consider the curve $\mathcal{C}$ (projective and nonsingular) having the following affine plane equation :

$$Y^m = \frac{g(X)}{h(X)} \quad \text{with } m \text{ a divisor of } (q-1).$$

If $\alpha \in \mathbb{F}_q$ is such that $R(\alpha) = 0$ and $g(\alpha) \neq 0$, then we have $g(\alpha)/h(\alpha) = 1$ and hence

$$\#\mathcal{C}(\mathbb{F}_q) \geqslant m \cdot \#\{\alpha \mid R(\alpha) = 0 \text{ and } g(\alpha) \neq 0\}.$$

One difficulty here is to choose the pair of polynomials $R(X)$ and $g(X)$ in $\mathbb{F}_q[X]$ leading to a product $g(X) \cdot h(X)$ which is "highly inseparable".

Example 3.3. — Consider the polynomial $R(X)$ below

$$R(X) = \frac{X^{16} + X}{X^4 + X} = X^{12} + X^9 + X^6 + X^3 + 1 \in \mathbb{F}_{16}[X].$$

The roots of $R(X)$ are the elements $\alpha \in \mathbb{F}_{16} \smallsetminus \mathbb{F}_4$. For the polynomial $g(X) = (X^3 + X^2 + 1)^4$ we get from the euclidean algorithm

$$g(X) = R(X) + X^3(X+1)^3(X^3 + X + 1).$$

Note that the remainder $h(X) = X^3(X+1)^3(X^3 + X + 1)$ is highly inseparable. We then consider the projective curve $\mathcal{C}$ over $\mathbb{F}_{16}$ given by the affine equation

$$Y^3 = \frac{(X^3 + X^2 + 1)^4}{X^3(X+1)^3(X^3 + X + 1)}.$$

This curve $\mathcal{C}$ defined over $\mathbb{F}_{16}$ satisfies the equalities $g(\mathcal{C}) = 4$ and $\#\mathcal{C}(\mathbb{F}_{16}) = 45$.

Indeed, we have in our situation

$$\#\{\alpha \mid R(\alpha) = 0 \text{ and } g(\alpha) \neq 0\} = 12, \text{ and hence } \#\mathcal{C}(\mathbb{F}_{16}) \geqslant 3.12 = 36.$$

We still need to find 9 rational points on $\mathcal{C}(\mathbb{F}_{16})$ and they should have first coordinate $\alpha \in \mathbb{F}_4$ or $\alpha = \infty$. If $\alpha \in \mathbb{F}_4 \smallsetminus \mathbb{F}_2$ (*i.e.*, if $\alpha^2 + \alpha + 1 = 0$) then $\alpha^3 = 1$ and

$$\frac{(X^3 + X^2 + 1)^4}{X^3(X+1)^3(X^3 + X + 1)}(\alpha) = \alpha.$$

Since the equation $Y^3 = \alpha$ has no solution in the finite field $\mathbb{F}_{16}$ if $\alpha \in \mathbb{F}_4 \smallsetminus \mathbb{F}_2$, we have to look for rational points on $\mathcal{C}(\mathbb{F}_{16})$ with first coordinate $\alpha \in \mathbb{F}_2$ or $\alpha = \infty$.

One can show that in each case ($\alpha = 0$, 1 or ∞) there are 3 rational points on $\mathcal{C}(\mathbb{F}_{16})$ with first coordinate equal to the element α. Hence

$$\#\mathcal{C}(\mathbb{F}_{16}) = 36 + 3.3 = 45.$$

Substituting $Z := XY(X+1)/(X^3 + X^2 + 1)$ we see easily that the curve $\mathcal{C}$ can also be given by the affine equation in X and Z below

$$Z^3 = \frac{X^3 + X^2 + 1}{X^3 + X + 1}.$$

The zeros of the product $(X^3 + X^2 + 1) \cdot (X^3 + X + 1)$ are exactly the elements $\alpha \in \mathbb{F}_8 \setminus \mathbb{F}_2$ and they are simple zeros. The recipe then gives

$$2g(\mathcal{C}) - 2 = 3 \cdot (-2) + 6 \cdot (3-1) \text{ and hence that } g(\mathcal{C}) = 4. \qquad \square$$

Example 3.4. — Consider the curve $\mathcal{C}$ over $\mathbb{F}_{25}$ given by the following equation

$$Y^8 = X(X-1)^3(X+2).$$

This curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) = 7 \quad \text{and} \quad \#\mathcal{C}(\mathbb{F}_{25}) = 84.$$

The point here is to explain that the equation for the curve $\mathcal{C}$ above is obtained from our method. Let $R(X) = (X^2+2) \cdot (X^2-2) \cdot (X^2+2X-2) \cdot (X^2-2X-2)$ in the polynomial ring $\mathbb{F}_{25}[X]$. Note that $R(X)$ is a product of four irreducible polynomials of degree 2 over the finite field $\mathbb{F}_5$. Considering $g(X) = X^3(X+2)^3(X-1)^9$ we then get

$$g(X) = t(X) \cdot R(X) + 1, \quad \text{with } t(X) = (X+1)(X-2)^2(X^4 + 2X^2 - 2).$$

So we are lead by our construction to consider the equation $Y^{24} = X^3(X+2)^3(X-1)^9$ and, taking the 3^{rd} root of it,we arrive at the equation in the beggining of Example 3.4. $\square$

In order to produce other examples of curves with many rational points, one should also consider fibre products of curves obtained from the constructions above (see Section 6 in [**11**]). Let again $R(X) \in \mathbb{F}_q[X]$ be a polynomial having all roots in the finite field $\mathbb{F}_q$. For two polynomials $g_1(X)$ and $g_2(X)$ in $\mathbb{F}_q[X]$, each one of them not divisible by $R(X)$, we perform the euclidean algorithm:

$$g_1(X) = t_1(X) \cdot R(X) + h_1(X) \quad \text{with } \deg h_1 < \deg R,$$
$$g_2(X) = t_2(X) \cdot R(X) + h_2(X) \quad \text{with } \deg h_2 < \deg R.$$

We then get a curve $\mathcal{C}_1$ over $\mathbb{F}_q$ given by

$$Y_1^{m_1} = \frac{g_1(X)}{h_1(X)} \quad \text{with } m_1 \text{ a divisor of } (q-1),$$

and a curve $\mathcal{C}_2$ over $\mathbb{F}_q$ given by

$$Y_2^{m_2} = \frac{g_2(X)}{h_2(X)} \quad \text{with } m_2 \text{ a divisor of } (q-1).$$

We denote by $\mathcal{C}$ the curve which is the fibre product of the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ above. Similarly we get here that the set $\mathcal{C}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$ satisfies:

$$\#\mathcal{C}(\mathbb{F}_q) \geqslant m_1 \cdot m_2 \cdot \#\{\alpha \mid R(\alpha) = 0 \text{ and } (g_1 \cdot g_2)(\alpha) \neq 0\}.$$

The genus $g(\mathcal{C})$ is obtained by generalizing the recipe given in the beggining of this section.

Example 3.5. — Let $\mathcal{C}$ be the fibre product of the curves over $\mathbb{F}_{16}$ given by

$$Y_1^5 = (X^4 + X)^3 \text{ and by } Y_2^3 = \frac{(X^2 + X + 1)^3 \cdot (X^3 + X + 1)^2}{X(X+1) \cdot (X^3 + X^2 + 1)^3}.$$

This curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) = 34 \quad \text{and} \quad \#\mathcal{C}(\mathbb{F}_{16}) = 183.$$

The two equations defining the fibre product curve $\mathcal{C}$ are obtained by considering $R(X) = (X^{16} + X)/(X^4 + X)$, $g_1(X) = (X^4 + X)^3$ and $g_2(X) = (X^2 + X + 1)^3 \cdot (X^3 + X + 1)^2$. In our case we have

$$\#\{\alpha \mid R(\alpha) = 0 \text{ and } (g_1 \cdot g_2)(\alpha) \neq 0\} = 12$$

and hence $\#\mathcal{C}(\mathbb{F}_q) \geqslant m_1 \cdot m_2 \cdot 12 = 5 \cdot 3 \cdot 12 = 180$.

We have 3 other rational points corresponding to $X = \alpha$ with $\alpha = 0$, 1 or ∞. □

Remark. — The best result for the pair $q = 16$ and $g = 34$ (before the curve given in Example 3.5) was a curve with 161 rational points over $\mathbb{F}_{16}$ with genus 34.

Remark. — The constructions presented here give rise to curves of Kummer type, in particular each ramification is tame. One can also give constructions leading to curves of Artin-Schreier type, and here each ramification is wild. One has also a recipe due to Hasse for the determination of the genus of Artin-Schreier covers of the projective line (see [**22**] and [**30**], Section III.7). A very interesting construction of curves of Artin-Schreier type is given in [**19**], where many new interesting examples of maximal curves are presented.

4. Asymptotic results on curves and on codes

In this section we are going to explain the asymptotics on curves over a fixed finite field and also the asymptotics on codes over a fixed finite field, and relate them to each other.

Asymptotics on curves. — Let $\mathbb{F}_q$ be a fixed finite field. We denote by

$$N_q(g) = \max_{\mathcal{C}} \#\mathcal{C}(\mathbb{F}_q),$$

where $\mathcal{C}$ runs over the curves defined over $\mathbb{F}_q$ whose genus satisfies $g(\mathcal{C}) = g$. The asymptotics of curves over the fixed field $\mathbb{F}_q$ with q elements, with genus g tending to infinity, is described by the quantity $A(q)$ below

$$A(q) = \lim\sup_{g\to\infty} N_q(g)/g.$$

It follows from Theorem 2.2 that

$$A(q) \leqslant 2\sqrt{q}.$$

Ihara was the first one to observe that the bound above for the quantity $A(q)$ can be improved significantly. He showed that $A(q) \leqslant \sqrt{2q}$. Based on Ihara's ideas, Drinfeld and Vladut (see [**7**]) proved the following bound (see Proposition 4.3 here):

$$A(q) \leqslant \sqrt{q} - 1, \text{ for any prime power } q.$$

The bound of Drinfeld-Vladut above is sharp since it is attained whenever q is a square; *i.e.*, we have the following equality

$$A(\ell^2) = \ell - 1, \text{ for any prime power } \ell.$$

The equality above was proved firstly by Ihara in [**23**] (see also [**32**]) and his proof involves the consideration of the theory of modular curves. A more elementary proof of this equality can be seen in [**13**] (see also Example 5.2 here).

As for lower bounds on the quantity $A(q)$ we mention a result of T. Zink (see [**35**]):

$$A(p^3) \geqslant \frac{2(p^2-1)}{p+2}, \text{ with } p \text{ any prime number.}$$

The proof of T. Zink involves degeneration of modular surfaces (à la Shimura), and a much more elementary proof can be seen in [**4**]. In [**4**] we have also a generalization of the result of Zink; *i.e.*, we have the lower bound

$$A(q^3) \geqslant \frac{2(q^2-1)}{q+2}, \text{ with } q \text{ any prime power.}$$

The advantage of the proofs in [**13**] and in [**4**] is that the infinite sequence of curves, respectively their genera and their rational points, are all explicitely given by equations, respectively by their formulas and by their coordinates. This makes them more suitable for applications in Coding Theory and Cryptography.

Asymptotics on codes. — A linear code C over the finite field $\mathbb{F}_q$ is just a linear subspace of $\mathbb{F}_q^n$. Given a vector $v = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$ we define its *weight* $wt(v)$ as below

$$wt(v) := \#\{i \mid 1 \leqslant i \leqslant n \text{ and } v_i \neq 0\}.$$

For a linear code C in $\mathbb{F}_q^n$ we have 3 basic parameters:

– $n = n(C)$ is called the *length* of C; it is the dimension of the ambient space $\mathbb{F}_q^n$ of the linear code C.

– $k = k(C)$ is called the *dimension* of C; it is the dimension of the linear code C as a $\mathbb{F}_q$-vector space, that is, we have $k(C) := \dim_{\mathbb{F}_q}(C)$.

– $d = d(C)$ is called the *mimimum distance* of C; it is the minimal weight of a nonzero codeword, that is, we have $d(C) := \min\{wt(v) \mid v \in C \smallsetminus \{0\}\}$.

We have also two relative parameters:

– $R = R(C)$ is called the *transmission rate* of C; it is given by $R(C) := k(C)/n(C)$.

– $\delta = \delta(C)$ is called the *relative distance* of C; it is given by $\delta(C) := d(C)/n(C)$.

We then consider the map φ below

$$\begin{aligned}\varphi\colon \{\mathbb{F}_q\text{-linear codes}\} &\longrightarrow [0,1]\times[0,1]\\ C &\longmapsto (\delta(C), R(C)).\end{aligned}$$

We are interested in the accumulation points of the image $\operatorname{Im}\varphi$ of the map φ above. We define, for a fixed value of δ with $0 \leqslant \delta \leqslant 1$:

$$\alpha_q(\delta) := \max\{R \mid (\delta, R) \text{ is an accumulation point of } \operatorname{Im}\varphi\}.$$

The function $\alpha_q\colon [0,1] \to [0,1]$ defined above controls the asymptotics of linear codes over the finite field $\mathbb{F}_q$. It satisfies the following bound:

***Gilbert-Varshamov bound* (See [30], Prop. VII.2.3).** — *Let $0 \leqslant \delta \leqslant 1 - q^{-1}$, then*

$$\alpha_q(\delta) \geqslant 1 - H_q(\delta),$$

where $H_q(\delta) = \delta\log_q(q-1) - \delta\log_q\delta - (1-\delta)\log_q(1-\delta)$ is the so-called entropy function.

Relation between the asymptotics. — This relation was established by Tsfasman-Vladut-Zink via Goppa's construction of linear codes from algebraic curves over finite fields (see [**32**]). If $\mathbb{F}_q$ is a finite field such that $A(q) > 1$, then for each real number δ satisfying $0 \leqslant \delta \leqslant 1 - A(q)^{-1}$, we have the inequality

$$\alpha_q(\delta) \geqslant 1 - A(q)^{-1} - \delta.$$

The lower bound above on the function $\alpha_q(\delta)$ caused a big sensation among the coding theorists, since it represents (for q a square with $q \geqslant 49$) an improvement on the Gilbert-Varshamov bound for values of δ in a certain small interval.

Our aim now is to present a proof of the Drinfeld-Vladut bound:

$$A(q) \leqslant \sqrt{q} - 1, \text{ for any prime power } q.$$

This bound will be obtained here using a method due to Serre (the so-called Explicit Formulas). It will be convenient to introduce the following notation:

$$N_r := \#\mathcal{C}(\mathbb{F}_{q^r}),$$

where $\mathcal{C}$ is a curve (projective and nonsingular) defined over the finite field $\mathbb{F}_q$ and $r \in \mathbb{N}$.

In the proof of Proposition 2.8 we have used the simple fact that $N_2 \geqslant N_1$; the method of Serre below uses that $N_r \geqslant N_1$ for any $r \in \mathbb{N}$.

We will consider nonzero polynomials $\Psi(t)$ with positive real coefficients. We write

$$\Psi(t) = \sum_{r=1}^{m} c_r \cdot t^r \in \mathbb{R}[t]$$

where $c_r \in \mathbb{R}$ and $c_r \geqslant 0$. Since $\Psi(t)$ is nonzero we have $c_r > 0$ for some index r.

To such a polynomial $\Psi(t) \in \mathbb{R}[t]$ we associate the rational function $f(t) \in \mathbb{R}(t)$

$$f(t) := 1 + \Psi(t) + \Psi(t^{-1}).$$

Clearly we have

$$f(\gamma) \in \mathbb{R}, \quad \text{for each } \gamma \in \mathbb{C} \text{ with } |\gamma| = 1.$$

***Theorem 4.1* (Explicit Formulas).** — *Let $\Psi(t) \in \mathbb{R}[t]$ be a nonzero polynomial with positive coefficients, and let $f(t) = 1 + \Psi(t) + \Psi(t^{-1}) \in \mathbb{R}(t)$ be the associated rational function. Suppose that*

$$f(\gamma) \geqslant 0 \quad \textit{for each } \gamma \in \mathbb{C} \textit{ with } |\gamma| = 1.$$

Then for a curve $\mathcal{C}$ defined over $\mathbb{F}_q$ we have

$$\#\mathcal{C}(\mathbb{F}_q) \leqslant \frac{g(\mathcal{C})}{\Psi(q^{-1/2})} + \frac{\Psi(q^{1/2})}{\Psi(q^{-1/2})} + 1.$$

Proof. — We denote by (see Theorem 2.3)

$$\alpha_1, \alpha_2, \dots, \alpha_g, \alpha_{g+1}, \dots, \alpha_{2g}$$

the algebraic integers with $|\alpha_j| = \sqrt{q}$, and we again order them so that

$$\alpha_{g+j} = \overline{\alpha}_j, \text{ for each } j = 1, 2, \dots, g.$$

For $r \in \mathbb{N}$, we have the equality (see Eq.(2))

$$N_r = 1 + q^r - \sum_{j=1}^{g} (\alpha_j^r + \overline{\alpha}_j^r).$$

Multiplying this equality by $q^{-r/2}$, we obtain

$$N_r \cdot q^{-r/2} = q^{-r/2} + q^{r/2} - \sum_{j=1}^{g} (\alpha_j \cdot q^{-1/2})^r + (\overline{\alpha}_j \cdot q^{-1/2})^r.$$

If we denote $\gamma_j := \alpha_j \cdot q^{-1/2}$, we have $|\gamma_j| = 1$ and $\overline{\gamma}_j = \gamma_j^{-1}$; hence we have

$$N_r \cdot q^{-r/2} = q^{-r/2} + q^{r/2} - \sum_{j=1}^{g} (\gamma_j^r + \gamma_j^{-r}).$$

Denoting $\Psi(t) = \sum_{r=1}^{m} c_r \cdot t^r$ and multiplying the equality above by the coefficient c_r, and summing up for $r = 1, 2, \ldots, m$, we get

$$\sum_{r=1}^{m} N_r \cdot c_r \cdot q^{-r/2} = \Psi(q^{-1/2}) + \Psi(q^{1/2}) + g - \sum_{j=1}^{g} f(\gamma_j),$$

where $f(t)$ is the associated rational function.

Adding $N_1 \cdot \Psi(q^{-1/2})$ to both sides of the last equality, we can rewrite it as follows

$$N_1 \cdot \Psi(q^{-1/2}) = \Psi(q^{-1/2}) + \Psi(q^{1/2}) + g - R,$$

where R is defined as below

$$R := \sum_{j=1}^{g} f(\gamma_j) + \sum_{r=1}^{m} (N_r - N_1) c_r \cdot q^{-r/2}.$$

Since we have $c_r \geqslant 0$, $N_r \geqslant N_1$ and also $f(\gamma_j) \geqslant 0$ for each $j = 1, 2, \ldots, g$, we have that $R \geqslant 0$ and hence that

$$N_1 = \#\mathcal{C}(\mathbb{F}_q) \leqslant \frac{g}{\Psi(q^{-1/2})} + \frac{\Psi(q^{1/2})}{\Psi(q^{-1/2})} + 1. \qquad \square$$

Example 4.2. — For a natural number $e \in \mathbb{N}$ define

$$q_0 := 2^e \quad \text{and} \quad q := 2^{2e+1}.$$

Consider the projective curve $\mathcal{C}$ over $\mathbb{F}_q$ associated to the polynomial $f(X, Y)$ below

$$f(X, Y) := Y^q - Y - X^{q_0} \cdot (X^q - X) \in \mathbb{F}_q[X, Y].$$

It can be easily seen that the curve $\mathcal{C}$ has just one point at infinity, and moreover

$$\#\mathcal{C}(\mathbb{F}_q) = 1 + q^2.$$

The genus of this curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) = q_0 \cdot (q - 1) = \frac{q^{1/2}}{\sqrt{2}} \cdot (q - 1).$$

Let us denote by $g_0 := q_0 \cdot (q - 1)$. It follows from Theorem 4.1 that

$$\#\mathcal{C}_0(\mathbb{F}_q) \leqslant 1 + q^2,$$

for any curve $\mathcal{C}_0$ over $\mathbb{F}_q$ with genus g_0. Indeed, consider the polynomial

$$\Psi_0(t) = \frac{1}{\sqrt{2}} \cdot t + \frac{1}{4} \cdot t^2.$$

For a complex number $\gamma = e^{i\theta} = \cos\theta + i \sin\theta$ with $|\gamma| = 1$, and using the following cosine equality $\cos 2\theta = 2\cos^2\theta - 1$, we have

$$f(\gamma) = \left(\frac{1}{\sqrt{2}} + \cos\theta\right)^2 \geqslant 0,$$

where $f(t) := 1 + \Psi_0(t) + \Psi_0(t^{-1})$ is the associated rational function.

The assertion now follows from the equality

$$\frac{g_0}{\Psi_0(q^{-1/2})} + \frac{\Psi_0(q^{1/2})}{\Psi_0(q^{-1/2})} + 1 = 1 + q^2. \qquad \square$$

Exercise. — Let $\mathcal{C}$ be the curve over the finite field $\mathbb{F}_q$ given in Example 4.2 above. With notations as in the proof of Theorem 4.1, show that:

(a) $N_2 = N_1$ and $f(\gamma_j) = 0$ for each $j = 1, 2, \ldots, g$.

(b) Using that $f(\gamma_j) = \left(\frac{1}{\sqrt{2}} + \cos\theta_j\right)^2$, conclude that

$$\gamma_j = -\frac{1}{\sqrt{2}} \pm i \cdot \frac{1}{\sqrt{2}}, \quad \text{for each } j = 1, 2, \ldots, g.$$

(c) Conclude then that

$$\prod_{j=1}^{2g}(1 - \alpha_j t) = (1 + 2q_0 t + qt^2)^g.$$

We are now going to use Theorem 4.1 to derive the following bound (due to Drinfeld and Vladut) on the asymptotics of curves over a fixed finite field $\mathbb{F}_q$ with q elements:

***Proposition 4.3* (See [7])**. — *The quantity $A(q)$ satisfies the so-called Drinfeld-Vladut bound; i.e., we have*

$$A(q) \leqslant \sqrt{q} - 1.$$

Proof. — For each $m \in \mathbb{N}$ we consider the polynomial

$$\Psi_m(t) = \sum_{r=1}^{m}\left(1 - \frac{r}{m}\right) \cdot t^r \in \mathbb{R}[t].$$

Note that $\deg \Psi_m(t) = m - 1$, and also that for $t \neq 1$ we have

$$\Psi_m(t) = \frac{t}{(t-1)^2} \cdot \left(\frac{t^m - 1}{m} + 1 - t\right).$$

Indeed the equality above is equivalent to the validity of the equality below (and this validity can be checked by comparing the coefficients of terms with the same degrees):

$$(t-1)^2 \cdot \sum_{r=1}^{m}\left(1 - \frac{r}{m}\right) \cdot t^{r-1} = \frac{1}{m} \cdot t^m - t + \left(1 - \frac{1}{m}\right).$$

Then we have for the associated rational function $f_m(t) \in \mathbb{R}(t)$:

$$\begin{aligned}
f_m(t) &= 1 + \Psi_m(t) + \Psi_m(t^{-1}) \\
&= 1 + \frac{t}{(t-1)^2} \cdot \left(\frac{t^m - 1}{m} + 1 - t \right) \\
&\quad + \frac{t^{-1}}{(t^{-1}-1)^2} \cdot \left(\frac{t^{-m} - 1}{m} + 1 - t^{-1} \right) \\
&= \frac{t}{(t-1)^2} \cdot \frac{t^m - 1}{m} + \frac{t^{-1}}{(t^{-1}-1)^2} \cdot \frac{t^{-m} - 1}{m}.
\end{aligned}$$

We have clearly the equalities below

$$\frac{t}{(t-1)^2} = \frac{t^{-1}}{(t^{-1}-1)^2} = \frac{-1}{(t-1)(t^{-1}-1)}$$

and hence we conclude that

$$f_m(t) = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1}-1)}.$$

If $\gamma \in \mathbb{C}$ with $\gamma \neq 1$ and $|\gamma| = 1$, then $(\gamma - 1)(\gamma^{-1} - 1)$ is a positive real number. Also

$$|\gamma^m + \gamma^{-m}| \leqslant |\gamma^m| + |\gamma^{-m}| = 1 + 1 = 2,$$

and this shows that $f_m(\gamma) \geqslant 0$ for each $\gamma \in \mathbb{C}$ with $|\gamma| = 1$. We then conclude from Theorem 4.1 that (for each $m \in \mathbb{N}$):

$$\frac{N_q(g)}{g} \leqslant \frac{1}{\Psi_m(q^{-1/2})} + \frac{1}{g} \left(\frac{\Psi_m(q^{1/2})}{\Psi_m(q^{-1/2})} + 1 \right).$$

From the following equality

$$\Psi_m(t) = \frac{t}{(t-1)^2} \cdot \left(\frac{t^m - 1}{m} + 1 - t \right),$$

we get that the limit below holds true

$$\lim_{m \to \infty} \Psi_m(q^{-1/2}) = \frac{1}{\sqrt{q} - 1}.$$

Given a real number $\varepsilon > 0$, we then fix a natural number $n = n(\varepsilon)$ such that

$$\Psi_n(q^{-1/2})^{-1} < \sqrt{q} - 1 + \varepsilon/2.$$

For each $\varepsilon > 0$, having fixed $n = n(\varepsilon)$ as above, we can choose $g_0 = g_0(\varepsilon)$ such that

$$\frac{1}{g} \cdot \left(\frac{\Psi_n(q^{1/2})}{\Psi_n(q^{-1/2})} + 1 \right) < \frac{\varepsilon}{2} \quad \text{if } g \geqslant g_0.$$

Hence for each real number $\varepsilon > 0$, there exists $g_0 = g_0(\varepsilon)$ such that

$$\frac{N_q(g)}{g} < \left(\sqrt{q} - 1 + \frac{\varepsilon}{2} \right) + \frac{\varepsilon}{2} = \sqrt{q} - 1 + \varepsilon$$

holds for every choice of g satisfying $g \geqslant g_0$. This then implies that

$$\limsup_{g\to\infty} \frac{N_q(g)}{g} \leqslant \sqrt{q} - 1. \qquad \square$$

5. Towers of curves over finite fields

As we have done already, we will use simply the word curve to mean an algebraic curve, projective and nonsingular, defined and absolutely irreducible over a finite field $\mathbb{F}_q$ with q elements. A *tower* $\mathcal{F}$ over $\mathbb{F}_q$ is just an infinite sequence

$$\mathcal{F} = \Big(\dots \mathcal{C}_n \xrightarrow{\varphi_{n-1}} \mathcal{C}_{n-1} \twoheadrightarrow \cdots \xrightarrow{\varphi_2} \mathcal{C}_2 \xrightarrow{\varphi_1} \mathcal{C}_1\Big)$$

of curves $\mathcal{C}_n$ and surjective maps $\varphi_n\colon \mathcal{C}_{n+1} \to \mathcal{C}_n$, both the curves and the maps are all defined over $\mathbb{F}_q$, such that $g(\mathcal{C}_n) \to \infty$ as $n \to \infty$. We will always assume that all the maps $\varphi_n\colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ are separable. Then the assumption that $g(\mathcal{C}_n) \to \infty$ can be replaced by the assumption that there exists $n \in \mathbb{N}$ with $g(\mathcal{C}_n) \geqslant 2$.

The *limit* $\lambda(\mathcal{F})$ of the tower exists; *i.e.*, the following limit does exist (see [**14**]):

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \#\mathcal{C}_n(\mathbb{F}_q)/g(\mathcal{C}_n).$$

We have clearly

$$\lambda(\mathcal{F}) \leqslant A(q), \text{ for any tower } \mathcal{F} \text{ over } \mathbb{F}_q.$$

Let $\pi\colon \mathcal{C} \to \mathcal{C}_1$ be a surjective and separable map of curves $\mathcal{C}$ and $\mathcal{C}_1$ defined over an algebraically closed field k (in what follows the field k will be taken as $\overline{\mathbb{F}}_q$ the algebraic closure of the finite field $\mathbb{F}_q$). For a point $P \in \mathcal{C}_1(k)$ on the curve $\mathcal{C}_1$ we denote by

$$\pi^{-1}(P) = \{Q_1, Q_2, \dots, Q_r\} \subseteq \mathcal{C}(k)$$

the set of points of $\mathcal{C}$ having image under the map π equal to P. For each $j = 1, 2, \dots, r$, we have natural numbers $e(Q_j|P)$, called the *ramification index* of Q_j over P, such that

$$\sum_{j=1}^{r} e(Q_j|P) = \deg \pi.$$

The point P is called *unramified* for the map π if we have $r = \deg \pi$; *i.e.*, P is unramified if $\pi^{-1}(P)$ has exactly $\deg \pi$ elements. The points P on the curve $\mathcal{C}_1$ such that

$$\#\pi^{-1}(P) < \deg \pi$$

are called *ramified points* for the morphism π. The number of ramified points for the morphism π is always finite. We denote by $V(\pi)$ the *ramification locus* for the map π; *i.e.*,

$$V(\pi) := \{P \in \mathcal{C}_1(k) \mid \#\pi^{-1}(P) < \deg \pi\}.$$

For a tower $\mathcal{F} = (\ldots \mathcal{C}_n \overset{\varphi_{n-1}}{\twoheadrightarrow} \mathcal{C}_{n-1} \twoheadrightarrow \cdots \overset{\varphi_2}{\twoheadrightarrow} \mathcal{C}_2 \overset{\varphi_1}{\twoheadrightarrow} \mathcal{C}_1)$ of curves over the finite field $\mathbb{F}_q$, and denoting for each $n \in \mathbb{N}$

$$\pi_n := \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_{n-1} \colon \mathcal{C}_n \longrightarrow\!\!\!\!\rightarrow \mathcal{C}_1$$

the composite morphism, we define the *ramification locus* $V(\mathcal{F})$ of the tower by

$$V(\mathcal{F}) := \bigcup_{n=2}^{\infty} V(\pi_n).$$

In other words, a point $P \in \mathcal{C}_1(k)$ with $k = \overline{\mathbb{F}}_q$ belongs to $V(\mathcal{F})$ if and only if there exists $n \in \mathbb{N}$ and a point $\widetilde{P}$ belonging to the curve $\mathcal{C}_n$ such that

$$\pi_n(\widetilde{P}) = P \quad \text{and} \quad \#\varphi_n^{-1}(\widetilde{P}) < \deg \varphi_n,$$

where $\varphi_n \colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ is the map appearing in the definition of the tower $\mathcal{F}$.

For a morphism $\pi \colon \mathcal{C} \twoheadrightarrow \mathcal{C}_1$ and a point $P \in V(\pi)$, the point P is said to be *tame* if the characteristic $p = \mathrm{char}(\mathbb{F}_q)$ does not divide the ramification index $e(Q_j|P)$, for each $j = 1, 2, \ldots, r$. The point P is said to be *wild*, otherwise. The morphism $\pi \colon \mathcal{C} \twoheadrightarrow \mathcal{C}_1$ is called *tame* if every point $P \in V(\pi)$ is a tame point. A tower $\mathcal{F}$ of curves over the finite field $\mathbb{F}_q$ is called *tame* if each morphism (for $n \in \mathbb{N}$) $\varphi_n \colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ in the definition of the tower $\mathcal{F}$ is a tame morphism.

For a tower of curves $\mathcal{F}$ over $\mathbb{F}_q$ we let again $\pi_n \colon \mathcal{C}_n \twoheadrightarrow \mathcal{C}_1$ denote the composite morphism as before. For a point $P \in \mathcal{C}_1(\mathbb{F}_q)$, which is $\mathbb{F}_q$-rational and which does not belong to $V(\pi_n)$, we have $\#\pi_n^{-1}(P) = \deg \pi_n$. The rational point P on the first curve $\mathcal{C}_1$ is said to be π_n-*split* if $P \notin V(\pi_n)$ and if $\pi_n^{-1}(P)$ consists of $\mathbb{F}_q$-rational points on $\mathcal{C}_n$; *i.e.*, the point P is π_n-*split* if we have

$$P \notin V(\pi_n) \quad \text{and} \quad \pi_n^{-1}(P) \subseteq \mathcal{C}_n(\mathbb{F}_q).$$

For a tower $\mathcal{F}$ over $\mathbb{F}_q$ we define the *splitting locus* $S(\mathcal{F})$ as below

$$S(\mathcal{F}) := \{P \in \mathcal{C}_1(\mathbb{F}_q) \mid P \text{ is } \pi_n\text{-split}, \forall\, n \in \mathbb{N}\}.$$

The ramification locus $V(\mathcal{F})$ and the splitting locus $S(\mathcal{F})$ of a tower $\mathcal{F}$ of curves over a finite field are specially interesting for tame towers.

Theorem 5.1. — *Let $\mathcal{F}$ be a tame tower of curves over $\mathbb{F}_q$. Suppose that*

(a) *The ramification locus $V(\mathcal{F})$ is a finite set.*

(b) *The splitting locus $S(\mathcal{F})$ is a nonempty set.*

Then the limit $\lambda(\mathcal{F})$ satisfies

$$\lambda(\mathcal{F}) \geqslant \frac{2 \cdot \#S(\mathcal{F})}{2g(\mathcal{C}_1) - 2 + \#V(\mathcal{F})}.$$

Proof. — The result follows easily from Hurwitz genus formula (see [**16**]). ☐

In order to give some examples illustrating Theorem 5.1 we will introduce now the concept of *recursive towers*. Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial with coefficients in the finite field $\mathbb{F}_q$ (*i.e.*, the polynomial $f(X,Y)$ remains irreducible over the algebraic closure $\overline{\mathbb{F}}_q$). We say that the tower $\mathcal{F}$ is *recursively defined* by the polynomial $f(X,Y)$ if:

– The first curve $\mathcal{C}_1$ is the projective line $\mathbb{P}^1$ with affine coordinate X_1.

– The second curve $\mathcal{C}_2$ is the nonsingular projective model for the affine plane curve given by $f(X_1, X_2) = 0$.

– The third curve $\mathcal{C}_3$ is the nonsingular projective model for the affine space curve given by $f(X_1, X_2) = f(X_2, X_3) = 0$.

– The fourth curve $\mathcal{C}_4$ is the nonsingular projective model for the curve in the 4-dimensional affine space given by $f(X_1, X_2) = f(X_2, X_3) = f(X_3, X_4) = 0$.

– and so on...

Example 5.2. — Consider the tower $\mathcal{F}$ over the finite field $\mathbb{F}_q$ with $q = \ell^2$, defined recursively by the equation

$$f(X,Y) = Y^\ell + Y - \frac{X^\ell}{1 + X^{\ell-1}}.$$

One can show (see [**14**]) that its limit over $\mathbb{F}_{\ell^2}$ satisfies

$$\lambda(\mathcal{F}) = \ell - 1;$$

i.e., the tower $\mathcal{F}$ attains the Drinfeld-Vladut bound over the finite field with ℓ^2 elements. This gives a more elementary proof of the equality

$$A(\ell^2) = \ell - 1, \text{ for any prime power } \ell.$$

The determination of the limit

$$\lambda(\mathcal{F}) = \ell - 1$$

in Example 5.2 is quite involved. One cannot use here Theorem 5.1, since each ramification occuring in the tower in Example 5.2 is wild. □

One has the following result due to J.-P. Serre (proved using Class Field Theory):

$$A(q) > 0, \quad \text{for any prime power } q.$$

The next example gives an elementary proof (for q nonprime) of this result.

***Example 5.3* (See [16])**. — Let q be a power of a prime number p and suppose that $q \neq p$. Consider the tower $\mathcal{F}$ over the finite field $\mathbb{F}_q$ given recursively by

$$f(X,Y) = Y^m - (X+1)^m + 1, \text{ with } m = \frac{q-1}{p-1}.$$

The limit of this tower satisfies

$$\lambda(\mathcal{F}) \geqslant \frac{2}{q-2} > 0.$$

Proof. — It follows from the theory of Kummer extensions (see [**30**], Section III.7) that the point at infinity on $\mathcal{C}_1 = \mathbb{P}^1$ is splitting in the tower $\mathcal{F}$; *i.e.*, the set $S(\mathcal{F})$ is nonempty and hence $\#S(\mathcal{F}) \geqslant 1$. The ramification locus satisfies

$$V(\mathcal{F}) \subseteq \{P \in \mathcal{C}_1(\mathbb{F}_q) \mid X_1(P) \in \mathbb{F}_q\}$$

and hence $\#V(\mathcal{F}) \leqslant q$. It then follows from Theorem 5.1 that

$$\lambda(\mathcal{F}) \geqslant \frac{2\#S(\mathcal{F})}{\#V(\mathcal{F}) - 2} \geqslant \frac{2}{q-2}.$$

The particular case where $q = 4$ is very interesting. In this particular case the tower $\mathcal{F}$ is recursively given over $\mathbb{F}_4$ by the equation

$$f(X,Y) = Y^3 - (X+1)^3 + 1 \in \mathbb{F}_4[X,Y],$$

and its limit satisfies $\lambda(\mathcal{F}) \geqslant 2/(4-2) = 1$. We also have $A(4) \leqslant \sqrt{4} - 1 = 1$, and hence the tower in Example 5.3 with $q = 4$ attains the Drinfeld-Vladut bound over $\mathbb{F}_4$. □

Example 5.4. — Let p be an odd prime number and let $q = p^2$. Consider the tower $\mathcal{F}$ of curves over $\mathbb{F}_q$ given recursively by the equation

$$f(X,Y) = Y^2 - \frac{X^2+1}{2X}.$$

The limit of this tower satisfies

$$\lambda(\mathcal{F}) = p - 1;$$

i.e., the tower $\mathcal{F}$ attains the Drinfeld-Vladut bound over the finite field with p^2 elements.

Proof. — It is easy to see that the ramification locus $V(\mathcal{F})$ of the tower is

$$V(\mathcal{F}) = \{P \in \mathcal{C}_1 \mid X_1(P) = 0, \infty, \pm 1 \text{ or } \pm i\}$$

where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Hence

$$\#V(\mathcal{F}) = 6.$$

Because p is an odd prime number, the tower $\mathcal{F}$ is a tame tower. If we can show that

$$\#S(\mathcal{F}) = 2(p-1),$$

then it follows from Theorem 5.1 that

$$\lambda(\mathcal{F}) \geqslant \frac{2 \cdot 2(p-1)}{6-2} = p - 1;$$

i.e., the tower $\mathcal{F}$ attains the Drinfeld-Vladut bound. The hard part here is to show

$$\#S(\mathcal{F}) = 2(p-1).$$

The determination of the splitting locus $S(\mathcal{F})$ involves the investigation of the rationality in the finite field $\mathbb{F}_{p^2}$ of the roots of the following polynomial $H(X)$, the so-called *Deuring polynomial* (see [**15**]):

$$H(X) := \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot X^j \in \mathbb{F}_p[X]. \qquad \square$$

***Example 5.5* (See [16]).** — For $q = \ell^2$ consider the tower $\mathcal{F}$ over $\mathbb{F}_q$ given recursively by

$$f(X,Y) = Y^{\ell-1} + (X+1)^{\ell-1} - 1.$$

Similarly to Example 5.3 we have here that the point at infinity of $\mathcal{C}_1 = \mathbb{P}^1$ is splitting over $\mathbb{F}_{\ell^2}$ in the tower $\mathcal{F}$, and hence the splitting locus satisfies

$$\#S(\mathcal{F}) \geqslant 1;$$

we also have here that $\#V(\mathcal{F}) \leqslant \ell$ and, more concretely, the ramification locus satisfies

$$V(\mathcal{F}) \subseteq \{P \in \mathcal{C}_1 \mid X_1(P) \in \mathbb{F}_\ell\}.$$

It now follows from Theorem 5.1 that the limit of $\mathcal{F}$ over the finite field $\mathbb{F}_{\ell^2}$ satisfies:

$$\lambda(\mathcal{F}) \geqslant \frac{2 \cdot \#S(\mathcal{F})}{\#V(\mathcal{F}) - 1} \geqslant \frac{2}{\ell - 2}.$$

The case when $\ell = 3$ is particularly interesting. In this case we get a tower $\mathcal{F}$ of curves over the finite field $\mathbb{F}_9$ given by $f(X,Y) = Y^2 + (X+1)^2 - 1 \in \mathbb{F}_9[X,Y]$, which attains the Drinfeld-Vladut bound. $\square$

***Remark*.** — Not every polynomial $g(X,Y) \in \mathbb{F}_q[X,Y]$ defines recursively a tower $\mathcal{F}$ of curves over the finite field $\mathbb{F}_q$. For example, let m be a divisor of $(q-1)$ and consider the polynomial

$$g(X,Y) = Y^m - X^m - 1 \in \mathbb{F}_q[X,Y].$$

One starts to go upwards in the "possible tower" defined by the polynomial $g(X,Y)$ above (where p denotes the characteristic):

$$X_2^m = X_1^m + 1; \quad X_3^m = X_2^m + 1 = X_1^m + 2;$$
$$X_4^m = X_3^m + 1 = X_1^m + 3 \text{ and } X_{p+1}^m = X_p^m + 1 = X_1^m + p = X_1^m.$$

The equality $X_{p+1}^m = X_1^m$ shows that the polynomial $g(X,Y) = Y^m - X^m - 1$ does not define recursively a tower of curves. One can show that (see [**34**]) the polynomial

$$f(X,Y) = Y^m + a(X+b)^m + c \in \mathbb{F}_q[X,Y],$$

with m and q relatively prime, defines a tower of curves over $\mathbb{F}_q$ if and only if $a \cdot b \cdot c \neq 0$. If we have the condition that $a, b, c \in \mathbb{F}_q^*$ satisfy the equality

$$a \cdot b^m + c = 0,$$

then it is very easy to see that the polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ as above defines indeed a tower of curves over $\mathbb{F}_q$. This is so since the point $X_1 = 0$ of the first curve $\mathcal{C}_1 = \mathbb{P}^1$ is totally ramified in the tower.

***Example 5.6* (See [15]).** — Let q be a power of a prime number p and suppose that p is odd. Let $\beta \in \mathbb{F}_q$ with $\beta^2 \neq 1$. Consider the tower $\mathcal{F}$ over the finite field $\mathbb{F}_q$ given by

$$f(X,Y) = Y^2 - \frac{X(X+\beta^2)}{X+1}.$$

The two points P of $\mathcal{C}_1 = \mathbb{P}^1$ with $X_1(P) = \pm\beta$ are splitting in the tower over $\mathbb{F}_q$. Indeed we have the equalities below

$$\frac{\beta(\beta+\beta^2)}{\beta+1} = \beta^2 = \frac{-\beta(-\beta+\beta^2)}{-\beta+1}.$$

Since p is assumed to be an odd prime number, then the tower $\mathcal{F}$ here is a tame tower. If the finite field $\mathbb{F}_q$ is chosen so that the ramification locus $V(\mathcal{F})$ is a finite set, then it follows from Theorem 5.1 that the limit over $\mathbb{F}_q$ satisfies

$$\lambda(\mathcal{F}) \geqslant \frac{2 \cdot \#S(\mathcal{F})}{\#V(\mathcal{F}) - 2} \geqslant \frac{4}{\#V(\mathcal{F}) - 2}.$$

This is the case if we choose $q = 9$. In this case we get $\#V(\mathcal{F}) = 8$ and hence we also get that its limit satisfies $\lambda(\mathcal{F}) \geqslant 4/(8-2) = 2/3$. □

Tame towers are easier since we have at least the criteria in Theorem 5.1 ensuring that the limit $\lambda(\mathcal{F})$ is a positive number. Wild towers $\mathcal{F}$ with $S(\mathcal{F})$ nonempty and with $V(\mathcal{F})$ finite, can have limit $\lambda(\mathcal{F})$ equal to zero.

For example consider the tower $\mathcal{F}_0$ over $\mathbb{F}_q$, with $q = p^p$ and p a prime number, given by

$$f(X,Y) = Y^p - Y - \frac{(X+1)(X^{p-1}-1)}{X^{p-1}}.$$

There are at least p points of $\mathcal{C}_1 = \mathbb{P}^1$ which are splitting in the tower over $\mathbb{F}_{p^p}$; we have

$$S(\mathcal{F}_0) \supseteq \{P \in \mathcal{C}_1 \mid (X_1^p - X_1 - 1)(P) = 0\} \quad \text{and hence } \#S(\mathcal{F}_0) \geqslant p.$$

One can check that the ramification locus $V(\mathcal{F}_0)$ is a finite set; indeed we have

$$V(\mathcal{F}_0) = \{P \in \mathcal{C}_1 \mid X_1(P) \in \mathbb{F}_p \text{ or } X_1(P) = \infty\}.$$

In case $p = 2$ the tower $\mathcal{F}_0$ is the same as the tower in Example 5.2 with $\ell = 2$, and hence it attains the Drinfeld-Vladut bound over $\mathbb{F}_4$. In case $p \geqslant 3$, the limit of the tower $\mathcal{F}_0$ satisfies $\lambda(\mathcal{F}_0) = 0$, for each prime $p \geqslant 3$. This result that $\lambda(\mathcal{F}_0) = 0$ is obtained in [**2**] from the following result on the classification of recursive Artin-Schreier towers: Let $\mathbb{F}_q$ be the finite field with q elements and denote by $p = \mathrm{char}(\mathbb{F}_q)$. Let $\varphi(Y) = Y^p + \alpha Y \in \mathbb{F}_q[Y]$ be a separable additive polynomial (*i.e.*, $\alpha \neq 0$) with all roots in the finite field $\mathbb{F}_q$. Suppose that $\mathcal{F}$ is a recursive tower defined over $\mathbb{F}_q$ by an equation

$$f(X,Y) = \varphi(Y) - \psi(X) \text{ with } \psi(X) \in \mathbb{F}_q(X).$$

If the tower $\mathcal{F}$ is *good* over $\mathbb{F}_q$; *i.e.*, if the limit over $\mathbb{F}_q$ satisfies $\lambda(\mathcal{F}) > 0$, then the rational function $\psi(X)$ has degree equal to p and it is of one of the following three types:

Type A. — $\psi(X) = c + (X-b)^p/\psi_1(X)$, with elements $b, c \in \mathbb{F}_q$ and with $\psi_1(X) \in \mathbb{F}_q[X]$ a polynomial satisfying $\deg(\psi_1(X)) \leqslant p$ and $\psi_1(b) \neq 0$.

Type B. — $\psi(X) = \psi_0(X)/(X-b)^p$, with $b \in \mathbb{F}_q$ and with $\psi_0(X) \in \mathbb{F}_q[X]$ a polynomial satisfying $\deg(\psi_0(X)) \leqslant p$ and $\psi_0(b) \neq 0$.

Type C. — $\psi(X) = c + 1/\psi_1(X)$, with $c \in \mathbb{F}_q$ and with $\psi_1(X) \in \mathbb{F}_q[X]$ a polynomial satisfying $\deg(\psi_1(X)) = p$.

All known good towers given recursively by $f(X,Y) = \varphi(Y) - \psi(X)$ as above, are towers of Type A (see Example 5.2).

The rational function $\psi(X) = (X+1)(X^{p-1}-1)/X^{p-1}$ in the definition of the tower $\mathcal{F}_0$ above is not of Type A, B or C if the characteristic p satisfies $p \neq 2$, and hence $\lambda(\mathcal{F}_0) = 0$.

Example 5.7. — Consider the tower $\mathcal{F}_1$ over $\mathbb{F}_8$ given recursively by (see [**21**])

$$f(X,Y) = Y^2 + Y + \frac{(X+1)^2}{X} + 1.$$

This is a tower of Type A and its limit over the finite field with 8 elements satisfies

$$\lambda(\mathcal{F}_1) = \frac{2\cdot(2^2-1)}{2+2} = \frac{3}{2}.$$

We have that the splitting locus is given by

$$S(\mathcal{F}_1) = \{P \in \mathcal{C}_1 \mid X_1(P) \in \mathbb{F}_8 \smallsetminus \mathbb{F}_2\}$$

and that the ramification locus satisfies

$$V(\mathcal{F}_1) = \{P \in \mathcal{C}_1 \mid X_1(P) \in \mathbb{F}_4 \text{ or } X_1(P) = \infty\}.$$

The hard point here is to show that the *limit genus* $\gamma(\mathcal{F}_1)$ is finite and equal to 4; *i.e.*, the hard part is to show that the following equality holds

$$\gamma(\mathcal{F}_1) := \lim_{n\to\infty} \frac{g(\mathcal{C}_n)}{\deg \pi_n} = 4,$$

where $\pi_n\colon \mathcal{C}_n \to \mathcal{C}_1$ is the composite morphism. □

We now present two new towers of curves. One tower is over finite fields $\mathbb{F}_{\ell^2}$ with square cardinalities and it attains the Drinfeld-Vladut bound; the other tower is over finite fields $\mathbb{F}_{\ell^3}$ with cubic cardinalities and it gives in particular a generalization of the bound of Zink. The new feature of both towers above is that the maps $\varphi_n\colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ are non-Galois maps, if the characteristic is odd.

***Example 5.8* (See [3]).** — Consider the tower $\mathcal{F}_2$ over $\mathbb{F}_q$ with $q = \ell^2$ given recursively by

$$f(X,Y) = \frac{Y-1}{Y^\ell} - \frac{X^\ell - 1}{X}.$$

We have here that the splitting locus is given by

$$S(\mathcal{F}_2) = \{P \in \mathcal{C}_1 \mid (X_1^\ell + X_1 - 1)(P) = 0\}$$

and that the ramification locus satisfies

$$V(\mathcal{F}_2) = \{P \in \mathcal{C}_1 \mid X_1(P) = 0, 1 \text{ or } \infty\}.$$

The hard part here is to show that the limit genus $\gamma(\mathcal{F}_2)$ is finite; *i.e.*, the hard part is to show the equality below

$$\gamma(\mathcal{F}_2) := \lim_{n\to\infty} \frac{g(\mathcal{C}_n)}{\deg \pi_n} = \frac{\ell}{\ell - 1}.$$

We then conclude that the limit $\lambda(\mathcal{F}_2)$ over the finite field $\mathbb{F}_{\ell^2}$ satisfies

$$\lambda(\mathcal{F}_2) = \ell - 1;$$

i.e., it attains the Drinfeld-Vladut bound. This tower $\mathcal{F}_2$ of Example 5.8 is a subtower of the tower $\mathcal{F}$ of Example 5.2. Indeed using the equation

$$W^\ell + W = \frac{V^\ell}{1 + V^{\ell-1}}$$

and defining $X := (1 + V^{\ell-1})^{-1}$ and $Y := (1 + W^{\ell-1})^{-1}$, one checks easily that those functions X and Y defined above satisfy the equation

$$\frac{Y-1}{Y^\ell} = \frac{X^\ell - 1}{X}.$$

This gives another proof that $\lambda(\mathcal{F}_2) = \ell - 1$ (see [**14**]). □

***Example 5.9* (See [4]).** — Consider the tower $\mathcal{F}_3$ over $\mathbb{F}_q$ with $q = \ell^3$ given recursively by

$$f(X,Y) = \frac{1-Y}{Y^\ell} - \frac{X^\ell + X - 1}{X}.$$

We have here that the ramification locus satisfies

$$V(\mathcal{F}_3) = \{P \in \mathcal{C}_1 \mid (X_1^\ell + X_1 - 1)(P) = 0 \text{ or } X_1(P) = 0, 1, \infty\},$$

and hence $\#V(\mathcal{F}_3) = \ell + 3$.

Denoting by $S_0 = \{\alpha \in \overline{\mathbb{F}}_q \mid \alpha^{\ell+1} = \alpha - 1\}$, we have that S_0 is contained in $\mathbb{F}_q$ and that

$$S(\mathcal{F}_3) \supseteq \{P \in \mathcal{C}_1 \mid \frac{X_1^\ell + X_1 - 1}{X_1}(P) = \alpha \text{ with } \alpha \in S_0\},$$

and hence the cardinality of the splitting locus satisfies $\#S(\mathcal{F}_3) \geqslant \ell \cdot (\ell + 1)$.

Again the hard matter here is to show the equality below

$$\gamma(\mathcal{F}_3) := \lim_{n\to\infty} \frac{g(\mathcal{C}_n)}{\deg \pi_n} = \frac{\ell}{\ell - 1} \cdot \frac{\ell + 2}{2}.$$

We then conclude that the limit $\lambda(\mathcal{F}_3)$ over the finite field $\mathbb{F}_{\ell^3}$ satisfies

$$\lambda(\mathcal{F}_3) \geqslant \frac{2(\ell^2-1)}{\ell+2}.$$

The inequality above implies that

$$A(\ell^3) \geqslant \frac{2(\ell^2-1)}{\ell+2}, \quad \text{for any prime power } \ell.$$

This generalizes a result of Zink (see [**35**]) which corresponds to the particular case when ℓ is a prime number.

The tower $\mathcal{F}_3$ given here in Example 5.9 in the particular case when $\ell = 2$, is the same as the tower $\mathcal{F}_1$ given in Example 5.7. Indeed just perform the substitutions

$$X \longmapsto \frac{1}{X} \quad \text{and} \quad Y \longmapsto \frac{1}{Y}. \qquad \square$$

References

[1] M. Abdon & F. Torres – On maximal curves in characteristic two, *Manuscripta Math.* **99** (1999), p. 39–53.

[2] P. Beelen, A. Garcia & H. Stichtenoth – On towers of function fields of Artin-Schreier type, *Bulletin Braz. Math. Soc.* **35** (2004), p. 151–164.

[3] J. Bezerra & A. Garcia – A tower with non-Galois steps which attains the Drinfeld-Vladut bound, *J. Number Theory* **106** (2004), p. 142–154.

[4] J. Bezerra, A. Garcia & H. Stichtenoth – An explicit tower of function fields over cubic finite fields and Zink's lower bound, *J. reine angew. Math.* (to appear).

[5] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros & F. Torres – On plane maximal curves, *Compositio Math.* **121** (2000), p. 163–181.

[6] A. Cossidente, G. Korchmáros & F. Torres – On curves covered by the Hermitian curve, *J. Algebra* **216** (1999), p. 56–76.

[7] V. Drinfeld & S. Vladut – Number of points of an algebraic curve, *Functional Anal. Appl.* **17** (1983), p. 53–54.

[8] R. Fuhrmann, A. Garcia & F. Torres – On maximal curves, *J. Number Theory* **67** (1997), p. 29–51.

[9] R. Fuhrmann & F. Torres – The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89** (1996), p. 103–106.

[10] W. Fulton – *Algebraic curves*, Benjamin, Reading, Massachusetts, 1974.

[11] A. Garcia & A. Garzon – On Kummer covers with many rational points over finite fields, *J. Pure Appl. Algebra* **185** (2003), p. 177–192.

[12] A. Garcia & L. Quoos – A construction of curves over finite fields, *Acta Arith.* **98** (2001), p. 181–195.

[13] A. Garcia & H. Stichtenoth – A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121** (1995), p. 211–222.

[14] ______, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61** (1996), p. 248–273.

[15] A. Garcia, H. Stichtenoth & H.G. Rück – On tame towers over finite fields, *J. reine angew. Math.* **557** (2003), p. 53–80.

[16] A. Garcia, H. Stichtenoth & M. Thomas – On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997), p. 257–274.

[17] A. Garcia, H. Stichtenoth & C.P. Xing – On subfields of the Hermitian function field, *Compositio Math.* **120** (2000), p. 137–170.

[18] G. van der Geer & M. van der Vlugt – Tables of curves with many points, available at `http://www.science.uva.nl/~geer/`.

[19] ———, Reed-Muller codes and supersingular curves, *Compositio Math.* **84** (1992), p. 333–367.

[20] ———, Kummer covers with many rational points, *Finite Fiels Appl.* **6** (2000), p. 327–341.

[21] ———, An asymptotically good tower of curves over the field with eight elements, *Bull. London Math. Soc.* **34** (2002), p. 291–300.

[22] H. Hasse – Theorie der relativ zyklischen algebraischen Funktionenkörper, *J. reine angew. Math.* **172** (1934), p. 37–54.

[23] Y. 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), p. 721–724.

[24] G. Korchmáros & F. Torres – Embedding of a maximal curve in a Hermitian variety, *Compositio Math.* **128** (2001), p. 95–113.

[25] ———, On the genus of a maximal curve, *Math. Ann.* **108** (2002), p. 589–608.

[26] G. Lachaud – Sommes d'Eisenstein et nombre de points de certaines courbes algbriques sur les corps finis, *C. R. Acad. Sci. Paris* **305** (1987), p. 729–732.

[27] R. Lidl & H. Niederreiter – *Finite fields*, Addison-Wesley, Reading, Massachusetts, 1983.

[28] H.G. Rück & H. Stichtenoth – A characterization of hermitian function fields over finite fields, *J. reine angew. Math.* **457** (1994), p. 185–188.

[29] J.-P. Serre – Résumé des cours de 1983-1984, in *Annuaire College de France*, 1984, Œuvres No. 128, p. 79–83.

[30] H. Stichtenoth – *Algebraic function fields and codes*, Springer, Berlin, 1993.

[31] K.O. Stöhr & J.F. Voloch – Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), p. 1–19.

[32] M. Tsfasman, S. Vladut & T. Zink – Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound, *Math. Nachrichten* **109** (1982), p. 21–28.

[33] A. Weil – *Courbes algébriques et variétés abéliennes*, Herman, Paris, 1971.

[34] J. Wulftange – Zahme Türme algebraischer Funktionenkörper, Ph.D. Thesis, Essen University, 2003.

[35] T. Zink – Degeneration of Shimura surfaces and a problem in coding theory, in *Fundamentals of Computation Theory (Cottbus)* (L. Budach, ed.), Lecture Notes in Computer Science, vol. 199, Springer, N.Y., 1985, p. 503–511.

A. Garcia, IMPA, Estrada Dona Castorina 110, 22460-320 Rio de Janeiro RJ, Brazil
E-mail : `garcia@impa.br`