

PLANE MAXIMAL CURVES

APPLIED ALGEBRA, ALGEBRAIC ALGORITHMS AND CORRECTING CODES
(AAECC-18) TARRAGONA, SPAIN, JUNE 8-12, 2009

FERNANDO TORRES

INSTITUTE OF MATHEMATICS, STATISTIC AND COMPUTER SCIENCES
UNIVERSITY OF CAMPINAS, P.O. BOX 6065, 13083-970, CAMPINAS, SP, BRAZIL
FTORRES AT IME.UNICAMP.BR

ABSTRACT. We are interested in non-singular plane curves whose number of rational points attains the Hasse-Weil upper bound.

Dedicated with affection to J.W.P. Hirschfeld and G. Korchmáros

Contents.

- (1) Maximal Curves: Basic Facts
- (2) Studying Maximal Curves Via Stöhr-Voloch Theory
- (3) Plane Curves

References:

- (I) “Many Rational Points, Coding Theory and Algebraic Geometry”, N.E. Hurt, Kluwer Academic Publishers, Dordrecht, Boston, London, 2003.
- (II) “Algebraic Curves over a Finite Field”, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Princenton University Press, USA, 2008.
- (III) *Algebraic curves with many points over finite fields*, F. Torres (eds. E. Martínez-Moro, C. Munuera and D. Ruano) *Advances in Algebraic Geometry Codes, Series on Coding Theory and Cryptology Vol. 5*, World Scientific Home, 2008, 221–256.

Main Problem. The number of rational points of curves over finite fields.

Acknowledgment. I am extremely grateful to M. Abdón, A. Aguglia, A. Cossidente, R. Fuhmann, A. Garcia, M. Giulietti, J.W.P. Hirschfeld and G. Korchsmáros with whom I spent many hours doing research on maximal curves.

Keywords: finite field, maximal plane curves, Hürwitz curves.

July 16, 2009.

Throughout, by a curve we mean a “projective, non-singular geometrically irreducible algebraic curve” of positive genus.

1. MAXIMAL CURVES: BASIC FACTS

Let \mathcal{X} be a curve of genus g defined over the finite field \mathbb{F}_q with q elements. If \mathcal{X} is embedded in $\mathbb{P}^r(\overline{\mathbb{F}}_q)$, $\Phi(\mathcal{X}) = \mathcal{X}$ where $\Phi((x_0 : \dots : x_r)) := (x_0^q : \dots : x_r^q)$ is the so-called *Frobenius morphism* (over \mathbb{F}_q). Thus the fixed points of Φ are called the \mathbb{F}_q -rational points of \mathcal{X} ; in general, for $i \in \mathbb{N}$, the fixed points of Φ^i are the \mathbb{F}_{q^i} -rational points of \mathcal{X} . Let

$$N_i := \#\mathcal{X}(\mathbb{F}_{q^i}).$$

To deal with these numbers one considers the “zeta function” of \mathcal{X} over \mathbb{F}_q namely, the formal series

$$(1.1) \quad Z(t) = Z(t, q; \mathcal{X}) := \exp\left(\sum_{i=1}^{\infty} \frac{N_i}{i} t^i\right).$$

By the Riemann-Roch theorem, there exists $p(t) = p(t, q; \mathcal{X}) \in \mathbb{Z}[t]$ such that

$$(1.2) \quad p(t) = Z(t)(1-t)(1-qt).$$

Here the polynomial $h(t) = h(t, q; \mathcal{X}) := t^{2g}p(t^{-1})$ is monic of degree $2g$. Let $\alpha_1, \dots, \alpha_{2g}$ be the roots of $h(t)$. From (1.1) and (1.2) we obtain

$$(1.3) \quad N_i = q^i + 1 - \sum_{j=1}^{2g} \alpha_j^i.$$

Hasse-Weil Theorem. (Riemann Hypothesis for curves over finite fields) $|\alpha_j| = \sqrt{q}$.

Thus (1.3) implies the Hasse-Weil bound on N_i :

$$(1.4) \quad |N_i - (q^i + 1)| \leq 2g\sqrt{q^i}.$$

The curve \mathcal{X} is *maximal* (over \mathbb{F}_q) if $N_1 = q + 1 + 2g\sqrt{q}$. Thus q must be a square, says $q = \ell^2$. In this case $\alpha_j = -\ell$ by (1.3). Two important facts come out:

I. $g \leq \ell(\ell-1)/2$ (Yhara’s bound); this follows from the inequality $N_2 = \ell^4 + 1 - 2g\ell^2 \geq N_1$.

II. $h(t) = (t + \ell)^{2g}$. This is the characteristic polynomial of the Frobenius morphism (over \mathbb{F}_{ℓ^2}) $\tilde{\Phi} : \mathcal{J} \rightarrow \mathcal{J}$ so that $\tilde{\Phi} + \ell I = 0$ due to the semi-simplicity of $\tilde{\Phi}$ and that the representation of endomorphisms of \mathcal{J} on the Tate module are faithfully (Tate).

We translate this information to \mathcal{X} via the following commutative diagram:

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{f} & \mathcal{J} \\ \Phi \downarrow & & \downarrow \tilde{\Phi} \\ \mathcal{X} & \xrightarrow{f} & \mathcal{J} \end{array}$$

where $\Phi : \mathcal{X} \rightarrow \mathcal{X}$ is the Frobenius morphism on \mathcal{X} (over \mathbb{F}_{ℓ^2}) and $f : P \mapsto [P - P_0]$ is the natural embedding of \mathcal{X} into its Jacobian variety \mathcal{J} with P_0 a fixed \mathbb{F}_{ℓ^2} -rational point. This gives the following linear equivalence of divisors on \mathcal{X} :

$$(\ell + 1)P_0 \sim \ell P + \Phi(P).$$

We define the following base-point-free complete linear series on \mathcal{X} :

$$\boxed{\mathcal{D} := |(\ell + 1)P_0|}$$

Three more properties arise:

III. The definition of \mathcal{D} is independent of $P_0 \in \mathcal{X}(\mathbb{F}_{\ell^2})$ as $(\ell + 1)P \sim (\ell + 1)P_0$ for all $P \in \mathcal{X}(\mathbb{F}_{\ell^2})$; in particular, $\ell + 1 \in H(P)$, the Weierstrass semigroup at P (which is the set of poles of regular functions outside P). As a matter of fact, we also have that $\ell \in H(P)$ (see Example 2.4); thus from $H(P) \supseteq \langle \ell, \ell + 1 \rangle$ we also obtain $g \leq \ell(\ell - 1)/2$, namely Yhara's bound.

IV. Let $r + 1$ be the dimension of $\mathcal{L} := \mathcal{L}((\ell + 1)P_0)$ (as a \mathbb{F}_{ℓ^2} -vector space). By the very definition of \mathcal{D} , $r \geq 2$. Let

$$\boxed{\pi = (f_0 : f_1 : \dots : f_r) : \mathcal{X} \rightarrow \mathbb{P}^r := \mathbb{P}^r(\overline{\mathbb{F}_{\ell^2}})}$$

be the morphism (up to change of coordinates) associated to \mathcal{D} . Then \mathcal{D} is very ample; i.e., π is an embedding.

V. \mathcal{X} is contained in the Hermitian variety $\mathcal{H}_r : X_0^{\ell+1} + X_1^{\ell+1} + \dots + X_r^{\ell+1} = 0$. Conversely, if \mathcal{X} is a curve of degree $\ell + 1$ contained in \mathcal{H}_r , then \mathcal{X} is \mathbb{F}_{ℓ^2} -maximal.

These results are proved via the Stöhr-Voloch theory. We can use results and techniques concerning curves in projective spaces such as Castelnuovo's genus bound in the form

$$g \leq \frac{d - 1 - \epsilon}{2(r - 1)}(d - r + \epsilon) \leq F(r) := \begin{cases} \frac{(2\ell - (r-1))^2 - 1}{8(r-1)}, & \text{if } r \text{ is even;} \\ \frac{(2\ell - (r-1))^2}{8(r-1)}, & \text{if } r \text{ is odd,} \end{cases}$$

whit $d = \ell + 1$. It may be noted that $F(r) \leq F(s)$ for $s \leq r$. Thus we improve Yhara's bound as follows:

$$(1.5) \quad g \leq g_2 := \lfloor (\ell - 1)^2/4 \rfloor \quad \text{or} \quad g_1 := \ell(\ell - 1)/2.$$

This result was conjectured by Stichtenoth and Xing. There is a unique \mathbb{F}_{ℓ^2} -maximal curve of genus g_1 , namely the Hermitian curve: $\mathcal{H} := \mathcal{H}_2 : X_0^{\ell+1} + X_1^{\ell+1} + X_2^{\ell+1} = 0$ (Rück-Stichtenoth). For $g = g_2$ there is also a unique \mathbb{F}_{ℓ^2} -maximal curve having this genus which arise from a quotient of the Hermitian curve \mathcal{H} by a certain involution.

We can further improve (1.5) by using Halphen's theorem which imposes constraints on curves contained in quadratic surfaces. We obtain

$$(1.6) \quad g \leq g_3 := \lfloor (q^2 - q + 4)/6 \rfloor \quad \text{or} \quad g = g_2 \quad \text{or} \quad g = g_1.$$

The case $g = g_3$ is realized via the quotient of \mathcal{H} by certain automorphisms of order three.

Question 1.1. Is a \mathbb{F}_{ℓ^2} -maximal curve of genus g_3 unique?

Problem 1.2. (Serre) Fixed ℓ , find the true values of genus of \mathbb{F}_{ℓ^2} -maximal curves.

A way to obtain examples of maximal curves is by means of the following.

Remark 1.3. (Serre) Let $\pi : \mathcal{X} \rightarrow \mathcal{Y}$ be a non constant \mathbb{F}_q -covering of curves defined over \mathbb{F}_q . Then $h(t, q, \mathcal{Y})$ divides $h(t, q, \mathcal{X})$. In particular, if \mathcal{X} is \mathbb{F}_{ℓ^2} -maximal so \mathcal{Y} is.

Thus the quotient of \mathcal{H} by any subgroup of automorphisms is \mathbb{F}_{ℓ^2} -maximal.

Question 1.4. (Stichtenoth) Is any \mathbb{F}_{ℓ^2} -maximal curve covered by the Hermitian curve?

The answer to this question is negative as the following example shows.

Example 1.5. (Giulietti-Korchmáros, GK's curve; 2007) Let $\ell = n^3$. Set $p(X) := \sum_{i=0}^n (-1)^{i+1} X^{i(n-1)}$. The non-singular model \mathcal{X} of the following space curve defined by the affine surfaces

$$z^{n^2-n+1} = yp(x) \quad \text{and} \quad y^{n+1} = x^n + x$$

is \mathbb{F}_{ℓ^2} -maximal which cannot be covered by the Hermitian curve whenever $\ell > 8$. Its genus is $g = (n^3 + 1)(n^2 - 2)/2 + 1$ and satisfies at least the following two nice properties:

a. It can be characterized by means of its automorphism group; this group is “large” with respect to its genus. To show this property one requires a quite strong background on Group Theory.

b. It has just one point P in the plane $W = 0$ (here the coordinates of \mathbb{P}^3 are denote by $(X : Y : Z : W)$). The Weierstrass semigroup $H(P)$ at P can be computed as follows: from the definition of \mathcal{X} , $\bar{\ell} := (\ell + 1)/(\ell^{1/3} + 1) \in H(P)$. We already know that $\ell, \ell + 1 \in H(P)$ and thus $H(P) \supseteq \tilde{H} := \langle \bar{\ell}, \ell, \ell + 1 \rangle$. It is not difficult to show that the genus of \tilde{H} equals g and thus $H(P) = \tilde{H}$. It turns out that this semigroup is “telescopic”; in particular, its order bound can be computed (Høholdt, van Lint, Pellikaan).

Related examples.

Example 1.6. (Garcia-Stichtenoth; 2007-2008)

(1) The curve $x^7 = y^9 - y$ over \mathbb{F}_{27^2} is maximal. If it is covered by the respective Hermitian curve, then the covering is not Galois. As far as I know the general answer is not know.

The maximality property of GK's curves are generalized:

(2) Let $r \geq 3$ be an odd integer and $\ell = n^r$. The following space curve defined by the affine surfaces

$$z^{\frac{n^r+1}{n+1}} = y^{q^2} - y \quad \text{and} \quad y^{q+1} = x^q + x$$

is \mathbb{F}_{ℓ^2} -maximal. Its genus is $g = (n - 1)(n^{r+1} + n^r - n^2)/2$. It is the GK's curve for $r = 3$.

Question 1.7. For $r > 3$, is this curve covered by the Hermitian curve?

So far as I know, this question is open.

Next we state a proposal. Let $r \geq 3$ and odd integer and $\ell = n^r$. Set

$$M(n-1) + 1 = (n^r + 1)/(n + 1), \quad \text{and} \quad p(X) = \sum_{i=0}^M (-1)^{i+1} X^{(n-1)i}.$$

Define the space curve \mathcal{X} as follows:

$$z^{\frac{n^r+1}{n+1}} = yp(x) \quad \text{and} \quad y^{n+1} = (x^n + x)^{M/n}.$$

For $r = 3$ we obtain the GK's curve. After some computations one shows that \mathcal{X} is contained in the Hermitian surface \mathcal{H}_3 ; thus the non-singular model of any irreducible component \mathcal{X}_i is maximal (criterion of maximality via Hermitian varieties).

Conjecture. The number $g = \frac{1}{2}(n^r + 1)(Mn - 2) + 1$ is the genus of some \mathcal{X}_i .

If this is true, \mathcal{X}_i is not covered by the Hermitian (for $r > 3$, these examples are different from the aforementioned Garcia-Stichtenoth examples in (2)).

Finally, from (1.6), a \mathbb{F}_{ℓ^2} -maximal curve of genus g is Galois covered by the Hermitian curve \mathcal{H} provided that $g > g_3$.

Problem 1.8. (1) For a given ℓ , find the smallest constant $c(\ell)$ such that any \mathbb{F}_{ℓ^2} -maximal curve of genus $g > c(\ell)$ is covered by \mathcal{H} .

(2) Characterize maximal curves which cannot be covered by the Hermitian curve.

2. STUDYING MAXIMAL CURVES VIA STÖHR-VOLOCH THEORY

Stöhr and Voloch development a geometrical way to bound the number of rational points of curves over finite fields. Applying this theory to maximal curves we obtain further constraints on these curves.

Let us subsume some very basic results concerning Stöhr-Voloch theory. Let \mathcal{X} be a curve (over $\bar{\mathbb{F}}_q$) equipped with a base-point-free linear series \mathcal{D} of dimension r and degree d . Thus there exists $E \in \text{Div}(\mathcal{X})$ and a vector sub space \mathcal{L} of $\mathcal{L}(E)$ whose dimension is $r + 1$ such that

$$\mathcal{D} = \{E + \text{div}(f) : f \in \mathcal{L}\}.$$

Let $\pi := (f_0 : f_1 : \dots : f_r) : \mathcal{X} \rightarrow \mathbb{P}^r$ be the morphism defined by a set of coordinates which form a base of \mathcal{L} . This morphism is (up to coordinates) uniquely defined by \mathcal{D} (the converse is also true). For $P \in \mathcal{X}$ and $i \geq 0$ an integer, we define sub-sets of \mathcal{D} which will provide with geometric information on \mathcal{X} . Let $\mathcal{D}_i(P) := \{D \in \mathcal{D} : v_P(D) \geq i\}$ (here $D = \sum_P v_P(D)P$). We have $\mathcal{D}_i(P) = \emptyset$ for $i > d$,

$$\mathcal{D} \supseteq \mathcal{D}_0(P) \supseteq \mathcal{D}_1(P) \supseteq \dots \supseteq \mathcal{D}_{d-1}(P) \supseteq \mathcal{D}_d(P)$$

and each $\mathcal{D}_i(P)$ is a sub-linear series of \mathcal{D} such that the codimension of $\mathcal{D}_{i+1}(P)$ in $\mathcal{D}_i(P)$ is at most one. If $\mathcal{D}_i(P) \not\supseteq \mathcal{D}_{i+1}(P)$, the integer i is called a (\mathcal{D}, P) -order; thus by Linear Algebra we have a sequence of $(r + 1)$ -orders at P :

$$0 = j_0(P) < j_1(P) < \dots < j_r(P) \leq d.$$

Here $\mathcal{D} = \mathcal{D}_0(P)$ since \mathcal{D} is base-point-free by hypothesis. We describe now the linear series $\mathcal{D}_{j_i}(P)$ by means of a very special set of coordinates. There exists $D \in \mathcal{D}$ such that $v_P(D) = j_i(P)$. Choose the coordinates f_i 's in such a way that

$$v_P(E) + v_P(f_i) = j_i(P).$$

Set $\mathcal{L}_i(P) = \langle f_i, \dots, f_r \rangle$. Thus

$$\mathcal{D}_i(P) = \{E + \operatorname{div}(f) : f \in \mathcal{L}_i(P)\}.$$

We have the following linear spaces in \mathbb{P}^r :

$$T_{r-1}(P) : X_r = 0 \text{ (the osculating hyperplane); } T_{r-2} : X_r = X_{r-1} = 0; \dots;$$

$$T_2(P) : X_r = X_{r-1} = \dots = X_3 = 0; T_1(P) : X_r = X_{r-1} = \dots = X_2 = 0 \text{ (the tangent line).}$$

For arbitrary coordinates f_0, f_1, \dots, f_r , one can show that $T_{r-1}(P)$ is defined by the equation

$$(2.1) \quad \det \begin{pmatrix} X_0 & X_1 & \dots & X_r \\ D_t^{j_0} g_0(P) & D_t^{j_0} g_1(P) & \dots & D_t^{j_0} g_r(P) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ D_t^{j_{r-1}} g_0(P) & D_t^{j_{r-1}} g_1(P) & \dots & D_t^{j_{r-1}} g_r(P) \end{pmatrix} = 0,$$

where t is a separating element of $\bar{\mathbb{F}}_q(\mathcal{X})|\bar{\mathbb{F}}_q$, the operators $D_t^{j_i}$'s are the Hasse derivatives of order j_i and $g_i := t^{-e_P} f_i$ with $e_P := \min\{v_P(f_i)\}$.

(Hürwitz Wronskian method). It is a fundamental result the fact that the sequence $(j_i(P))$ is the same for all but finitely many points P of \mathcal{X} . This sequence is called the *order sequence* of \mathcal{D} and will be denoted by

$$0 = \epsilon_0 < \epsilon_1 < \dots < \epsilon_r.$$

The finitely many points P , where exceptional (\mathcal{D}, P) -orders occur, are called the *\mathcal{D} -Weierstrass points* of X . If \mathcal{D} is the canonical linear series, the \mathcal{D} -Weierstrass points are the usual Weierstrass points of the curve. There is a divisor R , the so-called *Ramification Divisor*, whose support is the set of \mathcal{D} -Weierstrass points:

$$R = \operatorname{div}(\det(D_t^{\epsilon_i} f_j)_{i=0, \dots, r; j=0, \dots, r}) + \left(\sum_{i=0}^r \epsilon_i \right) dt + (r + 1)E$$

Key facts.

- (1) $j_i(P) \geq \epsilon_i$ for each i , for each $P \in \mathcal{X}$;
- (2) $v_P(R) \geq \sum_{i=1}^r (j_i(P) - \epsilon_i)$;
- (3) Let p be the characteristic of \mathbb{F}_q ; *p-adic criterion*: If ϵ is an order and $\binom{\epsilon}{\eta} \not\equiv 0 \pmod{p}$, then η is also an order.

Now we deal with rational points. Let \mathcal{X} be defined over \mathbb{F}_q as well as \mathcal{D} . Let $\Phi : \mathcal{X} \rightarrow \mathcal{X}$ be the \mathbb{F}_q -Frobenius morphism on \mathcal{X} . The Stöhr-Voloch theory is based in the following three basic facts:

(SV1) If for a generic point P , $\pi(\Phi(P)) \in T_{r-1}(P)$, then there exists an integer $1 \leq I \leq r-1$ such that $\pi(\Phi(P)) \in T_I(P) \setminus T_{I-1}(P)$. Define $\nu_j := \epsilon_j$ for $0 \leq j \leq I-1$ and $\nu_j = \epsilon_{j+1}$ for $j = I, \dots, r-1$. This sequence is called the \mathbb{F}_q -Frobenius order sequence of \mathcal{D} . We can characterize the ν_j 's as follows. For a sequence $0 = \mu_0 < \mu_1 < \dots < \mu_{r-1}$, let

$$\Delta^\mu := \begin{pmatrix} f_0^q & f_1^q & \dots & f_r^q \\ D_t^{\mu_0} f_0 & D_t^{\mu_0} f_1 & \dots & D_t^{\mu_0} f_r \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ D_t^{\mu_{r-1}} f_0 & D_t^{\mu_{r-1}} f_1 & \dots & D_t^{\mu_{r-1}} f_r \end{pmatrix}.$$

Then the sequence (ν_j) is the minimum (in the lexicographically order) among the sequences (μ_j) such that $\det(\Delta^\mu) \neq 0$. Observe that $\Delta(P) = 0$ for $P \in \mathcal{X}(\mathbb{F}_q)$.

(SV2) There exists a divisor S , the so-called **\mathbb{F}_q -Frobenius Divisor**, which allows to bound $\#\mathcal{X}(\mathbb{F}_q)$:

$$S = \det(\Delta^\nu) + \left(\sum_{i=0}^{r-1} \nu_i \right) \text{div}(dt) + (\ell + r)E$$

Key Facts. Let $P \in \mathcal{X}(\mathbb{F}_q)$.

- (1) $v_P(S) \geq (j_r(P) - \nu_{r-1}) + \dots + (j_1(P) - \nu_0)$;
- (2) $\nu_i \leq j_{i+1}(P) - j_1(P)$ for $i = 0, \dots, r-1$.

Thus

(SV3) $v_P(S) \geq r$ so that

$$\#\mathcal{X}(\mathbb{F}_q) \leq \deg(S)/r$$

Example 2.1. If $r = 2$ and $\nu_1 = 1$, then

$$2\#\mathcal{X}(\mathbb{F}_q) \leq \deg(S) = (2g - 2) + (q + r)d.$$

Example 2.2. (Hefez-Voloch) Suppose that $\nu_1 > 1$, then

$$\#\mathcal{X}(\mathbb{F}_q) = \deg(S) - \deg(R) = d(q - 1) - (2g - 2).$$

In particular, if \mathcal{X} is a plane curve of degree d , $\#\mathcal{X}(\mathbb{F}_q) = d(q - d + 2)$.

Example 2.3. (Serre, Voloch, Top) Let \mathcal{X} be a plane curve of genus 3 over \mathbb{F}_q such that $N := \#\mathcal{X}(\mathbb{F}_q) > 2q + 6$. Then:

- (1) $q = 9$ and \mathcal{X} is the Hermitian curve $X^4 + Y^4 + Z^4 = 0$, or
- (2) $q = 8$ and \mathcal{X} is the Klein curve $X^3Y + Y^3Z + Z^3X = 0$.

The curve \mathcal{X} is non hyperelliptic and thus \mathcal{D} is the canonical linear series. By Example 2.1, $\nu_1 > 1$ and the previous example implies $N_q := \#\mathcal{X}(\mathbb{F}_q) = 4(q - 2)$. That $q = 9$ or $q = 8$ follows by using the ramification divisor and the Frobenius \mathbb{F}_q -divisor. We have $N_9 = 28 = 1 + 3^3$ and thus \mathcal{X} is the Hermitian curve by a result of Rück-Stichtenoth. We have $N_8 = 24$ and \mathcal{X} is the Klein curve which is a result due to Top.

Example 2.4. (Maximal Curves) Let \mathcal{X} be a \mathbb{F}_{ℓ^2} -maximal curve. Let $\mathcal{D} = |(\ell + 1)P_0|$. We have $\ell P + \Phi(P) \sim (\ell + 1)P_0$ and thus $D = \ell P + \Phi(P) \in \mathcal{D}$. It follows that $j_r(P) = \ell + 1$ for $P \in \mathcal{X}(\mathbb{F}_{\ell^2})$. For $P \notin \mathcal{X}(\mathbb{F}_{\ell^2})$, $j_r(P) = \ell$; otherwise, there exists D such that $v_P(D) = (\ell + 1)P$ and so $(\ell + 1)P \sim \ell P + \Phi(P)$ implies $P \sim \Phi(P)$ which implies $g = 0$. Moreover, from the definition of \mathcal{D} , $\Phi(P) \in T_{r-1}(P)$ and hence $\nu_{r-1} = \epsilon_r = \ell$.

Let $P \in \mathcal{X}(\mathcal{F}_2)$. Observe that $\mathcal{L}((\ell + 1)P)$ is related to the first $(r + 1)$ Weierstrass non-gaps at P_0 , says

$$0 = m_0 < m_1 < m_2 < \dots < m_{r-1} < \ell + 1 = m_r;$$

($m_i = m_i(P)$). The orders at P are: $j_0 = m_r - m_r < j_1 = m_r - m_{r-1} < \dots < j_{r-2} = m_r - m_2 < j_{r-1} = m_r - m_1 < j_r = m_r$. Now let us see that $j =_1(P) = 1$ for all $P \in \mathcal{X}$.

- (1) If $P \in \mathcal{X}(\mathcal{F}_2)$, from $\nu_{r-1} \leq j_r - j_1(P)$, $j_1(P) = 1$; in particular, $\ell \in H(P)$;
- (2) If $P \notin \mathcal{X}(\mathbb{F}_{\ell^2})$, the fact that $\ell P + \Phi(P) \in \mathcal{D}$ implies $j_1(P) = 1$.

Concrete Application.

Example 2.5. We improve (1.6) for $\ell \not\equiv 0 \pmod{3}$. Let \mathcal{X} be a \mathbb{F}_{ℓ^2} -maximal curve of genus $g > (\ell - 1)(\ell - 2)/6$. Then

$$g \geq (\ell^2 - 2\ell + 3)/6.$$

To see this, we use the linear series $\mathcal{D} = |(\ell + 1)P_0|$. The Hypothesis on g implies $r \leq 3$ (Castelnuovo's bound). If $r = 2$, Example 2.8 will follow by $g = \ell(\ell - 1)/2$ (in particular, the curve is the Hermitian curve). Let $r = 3$. Here $\epsilon_1 = 1$, $\epsilon_3 = \ell$. We also have that $\nu_1 = 1$, $\nu_2 = \ell$; otherwise, Example 2.2 implies $g = \ell(\ell - 1)/2$, a contradiction. Now we claim that $\epsilon_2 = 2$. Otherwise, $\epsilon_2 \geq 4$ by the p -adic criterion. Thus for $P \in \mathcal{X}(\mathbb{F}_{\ell^2})$,

$$v_P(S) \geq (j_3(P) - \nu_2) + (j_2(P) - \nu_1) + j_1(P) \geq (j_3(P) - \nu_2) + (\epsilon_2 - \nu_1) + j_1(P) \geq 5.$$

By the maximality of \mathcal{X} :

$$\deg(S) = (\ell + 1)(2g - 2) + (\ell + 3)(\ell + 1) \geq 5(\ell + 1)^2 + 5\ell(2g - 2)$$

so that $(\ell + 1)(\ell^2 - 5\ell - 2) \geq (4\ell - 1)(2g - 2)$, a contradiction. Once we know that $\epsilon_2 = 2$ we use the ramification divisor R . Here $v_P(R) \geq (j_2(P) - \epsilon_2) + (j_3(P) - \epsilon_3) \geq 1$ and hence the result follows from the inequality

$$\deg(R) = (1 + 2 + \ell)(2g - 2) + 4(\ell + 1) \geq (\ell + 1)^2 + \ell(2g - 2).$$

Garcia-Stichtenoth-Xing computed the genera of \mathbb{F}_{ℓ^2} -maximal curves for $\ell < 7$. We complement their computations for $\ell = 7$ and $\ell = 8$.

Example 2.6. (1) Let \mathcal{X} be a \mathbb{F}_{49} -maximal curve of genus g . By (1.6)

$$g \leq g_3 = 7, \quad g = g_2 = 9 \quad \text{or} \quad g = g_3 = 21.$$

a. For each $g \neq 6$ above there is a \mathbb{F}_{49} -maximal curves of genus g (Garcia-Stichtenoth-Xing, ...)

b. The case $g = 6$ cannot occur; in fact, by the previous example, $g > (6)(5)/6 = 5$, implies $g \geq (49 - 14 + 3)/6 = 6.3\dots$

(2) Let \mathcal{X} be a \mathbb{F}_{64} -maximal curve of genus g . By (1.6)

$$g \leq g_3 = 10, \quad g = g_2 = 12 \quad \text{or} \quad g = g_3 = 28.$$

a. For each $g \neq 5, 8$ above there is a \mathbb{F}_{64} -maximal curves of genus g (Garcia-Stichtenoth-Xing, ...)

b. The case $g = 8$ cannot occur as the genus of a \mathbb{F}_{64} -maximal curve; in fact, by the previous example, $g > (7)(6)/6 = 7$, implies $g \geq (64 - 16 + 3)/6 = 8.5$.

Question 2.7. What about the case $g = 5$?

We state a characterization of the Hermitian curve.

Example 2.8. Let \mathcal{X} be a \mathbb{F}_{ℓ^2} -maximal curve and $\mathcal{D} = |(\ell + 1)P_0|$. Let r be the dimension of \mathcal{D} . The following sentences are equivalent:

- (1) \mathcal{X} is the Hermitian curve;
- (2) $g > (\ell + 1)^2/4$;
- (3) $r = 2$.

(1) \Rightarrow (2) is clear. That (2) implies (3) follows from Castelnuovo's bound. Let $r = 2$. Hence $\nu_1 = \epsilon_2 = \ell$ and therefore

$$(x^{\ell^2} - x)f = (y^{\ell^2} - y),$$

where $f = D_x y$. By definition of ν_1 and ϵ_2 , $D_x^i f = 0$ for $i = 1, \dots, \ell - 1$ and hence f is a ℓ -th power, says $f = f_1^\ell$ (Hasse-Schmidt). Thus $f_1 = a + bx$ with $b \neq 0$; after a change of coordinates, \mathcal{X} is defined by an equation of type $y^\ell + y = x^{\ell+1}$ which is also a plane model of \mathcal{H} .

Problem 2.9. (van der Geer) Classify maximal curves.

Example 2.10. The following \mathbb{F}_{64} -maximal curves of genus 3 are not $\overline{\mathbb{F}}_{64}$ -isomorphic:

- (1) $\mathcal{X} : y^3 = x^4 + x$ (Rodriguez-Palánquex, Serre);
- (2) $\mathcal{Y} : y^3 = x^4 + x^2 + x$ (Garcia-Stichtenoth-Xing, ...)

As a matter of fact, the curve \mathcal{X} (resp. \mathcal{Y}) has 5 (resp. 17) Weierstrass points.

Example 2.11. An example of a \mathbb{F}_{64} -maximal curve of genus $g = 10$ is the non-singular model of $\mathcal{X} : y^9 = x^6 + x^3$. The GK curve over \mathbb{F}_{64} has genus 10 and it is given by defined by the equations $z^3 = y(1 + x + x^2)$; $y^3 = x^2 + x$. I cannot prove or disprove whether or not they are \mathbb{F}_{64} -isomomorphic.

Example 2.12. Let $\ell \equiv 3 \pmod{4}$. The following \mathbb{F}_{ℓ^2} -maximal curves are not isomorphic over $\overline{\mathbb{F}}_{\ell^2}$.

- (1) $\mathcal{X} : x^{(\ell+1)/4} = y^\ell + y$;
- (2) $\mathcal{Y} : x^{(\ell+1)/2} + y^{(\ell+1)/2} + 1 = 0$.

A reason for that is the fact that the semigroup $\langle (\ell-1)/2, (\ell+1)/2 \rangle$ arises as a Weierstrass semigroup in \mathcal{Y} but cannot be realized by any point in \mathcal{X} .

Remark 2.13. (Nart, Ritzenthaler, Sadornil, ...) Let \mathcal{M}_3 be the coarser moduli of curves of genus 3 over $\overline{\mathbb{F}}_q$, q a power of two. An appropriate stratification of \mathcal{M}_3 (bi-tangents versus 2-rank) and descent theory give the complete classification of curves of genus 3 over \mathbb{F}_q ; in particular $\#\mathcal{M}(\mathbb{F}_q)$ can be computed. If $q = \ell^2$, how can we detect \mathbb{F}_{ℓ^2} -maximal curves from \mathbb{F}_{ℓ^2} -rational points of \mathcal{M}_3 ?

3. PLANE CURVES

Here we restrict ourselves to the case of (non-singular) plane maximal curves $\mathcal{X} : F(X, Y, Z) = 0$ of degree $d \geq 3$ over \mathbb{F}_{ℓ^2} . We let Σ be the linear series cut out by lines. We let $x = X/Z$ and $y = Y/Z$ so that an affine equation for \mathcal{X} is $f(x, y) = F(x, y, 1) = 0$. Let $0 < 1 < \epsilon_2 = \epsilon_2(\Sigma)$ be the generic contact orders of Σ (recall that $\epsilon_2 \leq d$). Let $0 = \nu_0 < \nu_1 = \nu_1(\Sigma)$ be the \mathbb{F}_{ℓ^2} -Frobenius orders of Σ . We have $\nu_1 \in \{1, \epsilon_2\}$. Let us assume that $\overline{\mathbb{F}}_{\ell^2}(\mathcal{X})|\overline{\mathbb{F}}_{\ell^2}(x)$ is separable. We have that $\epsilon_2 > 2$ iff $D_x^2 y = 0$ (one says that any point $P \in \mathcal{X}$ is a “flex”). Here $g = (d-1)(d-2)/2$ is the genus of curve and (1.5) becomes

$$(3.1) \quad d \leq d_2(\ell) := \lfloor (\ell+1)/2 \rfloor \quad \text{or} \quad d = d_1(\ell) := \ell + 1.$$

From the formula of the Frobenius Divisor S of Σ and the maximality of \mathcal{X} we obtain another characterization of the Hermitian curve, namely:

Example 3.1. Let \mathcal{X} be a plane maximal curve of degree d over \mathbb{F}_{ℓ^2} . The following sentences are equivalent:

- (1) $d = \ell + 1$;

- (2) \mathcal{X} is the Hermitian curve;
- (3) $\epsilon_2 = \ell$;
- (4) $\nu_1 = \ell$;
- (5) $j_2(P) = \ell + 1$ for all $P \in \mathcal{X}(\mathbb{F}_{\ell^2})$;
- (6) $\nu_1 > 1$.

The implications (1) \Rightarrow (2) \Rightarrow (3) are clear. Suppose that $\nu_1 = 1$. This gives a contradiction via Example 2.1 and $d \geq \epsilon_2 = \ell$. Let $\nu_1 = \ell$. Since $\nu_1 \leq j_2 - j_1$, $\ell + 1 \leq j_2 \leq d \leq \ell + 1$ by (3.1) and (5) follows. Suppose $\nu_1 = 1$. Then $v_P(S) \geq (\ell + 1)$ for all $P \in \mathcal{X}(\mathbb{F}_{\ell^2})$. Thus

$$\deg(S) = (2g - 2) + (\ell^2 + 2)d \geq (\ell + 1)((\ell + 1)^2 + \ell(2g - 2));$$

this is a contradiction as $d \leq \ell + 1$. If $\nu_1 > 1$, Example 2.2 implies

$$d(\ell^2 - 1) - d(d - 3) = \ell d(d - 3) + (\ell + 1)^2$$

so that $d = \ell + 1$.

Example 3.2. (Fermat Curves) Let $p := \text{char}(\mathbb{F}_{\ell^2})$ and $N \geq 1$ an integer with $p \nmid N$. We let \mathcal{F}_N denote the Fermat curve of degree N , namely

$$\mathcal{F}_N : X^N + Y^N = Z^N.$$

If $N \mid (\ell + 1)$, by Remark 1.3, \mathcal{F}_N is \mathbb{F}_{ℓ^2} -maximal. Tafazolian showed that the converse is also true. Let us write a proof of this fact. We first show the following.

Claim. If \mathcal{F}_N is \mathbb{F}_{ℓ^2} -maximal, then $N \mid (\ell^2 - 1)$. To see this, let $d := \gcd(N, \ell^2 - 1)$. Consider the covering of curves $\mathcal{F}_N \rightarrow \mathcal{Y}$ where \mathcal{Y} is defined by $z^d + y^N = 1$, $z = x^{N/d}$. Therefore $\#\mathcal{F}_N(\mathbb{F}_{\ell^2}) = \#\mathcal{Y}(\mathbb{F}_{\ell^2})$ and the maximality of \mathcal{F}_N gives $N^2 - 3N = 2g - 2$ where g is the genus of \mathcal{Y} . After some computations (via Riemann-Hürwitz formula), $2g - 2 = -2d + N(d - 1)$ so that $d = N$.

Consider now the affine equation of the curve: $x^N + y^N = 1$. Let $D_\infty := \mathcal{X}_N \cdot (Z = 0)$. For $\alpha^N = 1$, let $P_\alpha = (0 : \alpha : 1)$. Then $\text{div}(y - \alpha) = NP_\alpha - D_\infty$. We also have $\text{div}(y) = \sum_\alpha P_\alpha - D_\infty$. Thus $NP_\alpha \sim NP_\beta$; in addition, the Weierstrass semigroup at P_α is generated by $N - 1$ and N . Since $(\ell + 1)P_\alpha \sim (\ell + 1)P_\beta$, $f := \gcd(N, \ell + 1) \in H(P_\alpha)$. Thus $f = a(N - 1) + bN$ with $a, b \geq 0$ and $N = cf = ca(N - 1) + bN$. It follows that $f = N$.

Example 3.3. Let ℓ be odd. The curve $\mathcal{F}_{(\ell+1)/2}$ is the unique \mathbb{F}_{ℓ^2} -maximal maximal of degree $(\ell + 1)/2$ for $\ell > 11$.

Problem 3.4. Classify plane maximal curves.

Now let $n \geq 2$ and integer, and let $d := n^2 - n + 1$ such that $p \nmid d$. The following curve

$$\mathcal{H}_n : X^n Y + Y^n Z + Z^n X = 0,$$

is the so-called Hürwitz curve. It is non-singular by (*). The case $n = 3$ is the famous Klein quartic.

We give a necessary and sufficient condition for ℓ in order that \mathcal{H}_n be \mathbb{F}_{ℓ^2} -maximal.

Example 3.5. Notation as above. The following sentences are equivalent:

- (1) $\tilde{\mathcal{F}}_d : U^d + V^d + W^d = 0$ is \mathbb{F}_{ℓ^2} -maximal;
- (2) \mathcal{H}_n is \mathbb{F}_{ℓ^2} -maximal;
- (3) $d \mid (\ell + 1)$.

The curve $\tilde{\mathcal{F}}_d$ is an unramified covering of \mathcal{H}_n (of degree d) via:

$$\pi_n : (u : v : 1) \mapsto (u^n v^{-1} : uv^{n-1} : 1).$$

(Here $u = U/W$ and $v = V/W$). Thus implications (1) \Rightarrow (2) and (3) \Rightarrow (1) follow by Remark 1.3. To show the remaining implication we use an argument similar to that in Example 3.2. Let $P_1 = (0 : 1 : 0)$ and $P_2 = (0 : 0 : 1)$. Then $\text{div}(x^{n-1}y) = (n^2 - n + 1)P_2 - (n^2 - n + 1)P_1$; therefore $f := \gcd(n^2 - n + 1, \ell + 1)$ belongs to the Weierstrass semigroup at P_1 which is generated by the set $\{s(n-1) + 1 : s = 1, \dots, n\}$. Therefore $n^2 - n + 1 = cf = ca(n-1) + cb$ with $a \geq b \geq 1$. This implies $f = n^2 - n + 1$.

Remark 3.6. Examples 3.2 and 3.3 involve maximal curves having two rational points, says P, Q , such that $aP \sim aQ$ for some $a \geq 1$ integer. In particular, $\gcd(a, \ell + 1) \in H(P)$ as $(\ell + 1)P \sim (\ell + 1)Q$. This can use to show that if $y^\ell + y = x^m$ defines a \mathbb{F}_{ℓ^2} -maximal curve, then $m \mid (\ell + 1)$ (see remark after Example 3.8).

From now on, let $3 \leq d \leq d_2(\ell) = \lfloor (\ell + 1)/2 \rfloor$.

Example 3.7. A plane maximal curve of degree d over \mathbb{F}_{ℓ^2} is classical provided that one of the following condition holds:

- (1) $p > d$ or $d \not\equiv 1 \pmod{p}$;
- (2) $\ell = 4, 8, 16, 32$;
- (3) $p \geq 3$ and either $\ell = p$ or $\ell = p^2$;
- (4) $p = 2$, $\ell \geq 64$, and either $d \leq 4$, or $d \geq \ell/4 - 1$ for $\ell = 64, 128, 256$, or $d \geq \ell/4$ for $\ell \geq 512$;
- (5) $p \geq 3$, $\ell = p^v$ with $v \geq 3$, and $d \geq \ell/p - p + 2$.

This follows by using the Ramification Divisor of Σ and the maximality of the curve. In particular, if \mathcal{X} is non-classical then $\ell \geq 64$ if $p = 2$ and $\ell \geq p^3$ for $p \geq 3$.

Example 3.8. If \mathcal{X} is non-classical, then $\epsilon_2^2 \leq \ell/p$. To see this we also use the Ramification Divisor of Σ and the maximality of the curve. This condition is sharp. In fact, the Hürwitz curve $x^p y + y^p + x = 0$ is \mathbb{F}_{p^6} -maximal and $\epsilon_2 = p$ for $p > 2$.

It is of interest to notice that Examples 3.7, 3.8 also hold true if we just assume that Σ is a plane model of an arbitrary maximal curve. As an application, we can see that a curve defined by an equation of type $y^{p^2} - y = f(x)$ cannot be \mathbb{F}_{p^6} -maximal since in this case $\epsilon_2 = p^2$.

Further improvements on d arise if we apply Stöhr-Voloch theory to the linear series cut out by conics.