Curves over Finite Fields Attaining the Hasse-Weil Upper Bound

Arnaldo Garcia

Abstract. Curves over finite fields (whose cardinality is a square) attaining the Hasse-Weil upper bound for the number of rational points are called *maximal curves*. Here we deal with three problems on maximal curves:

1. Determination of the possible genera of maximal curves.
2. Determination of explicit equations for maximal curves.
3. Classification of maximal curves having a fixed genus.

1. Introduction

The theory of equations over finite fields (or the theory of congruences) is in the basis of classical number theory. Its foundations were laid, among others, by mathematicians like Fermat, Euler, Lagrange, Gauss, and Galois (see Dickson's book [6]). Historically, the object of the first investigations in this theory were the congruences of the special form

$$y^2 \equiv f(x) \quad \text{(modulo a prime number)}\,, \tag{1}$$

where $f(x)$ is a polynomial (or rational function) with integer coefficients. Such congruences were used to get results such as the representability of integers as sum of four squares, or the distribution of pairs of quadratic residues, or even the estimation of the sum of Legendre's quadratic residues symbols.

E. Artin constructed a quadratic extension of the field $\mathbb{F}_p(x)$, p a prime, by adjoining the roots of the congruence (1) and he introduced a zeta-function for this field, in analogy with Dedekind's zeta-function for quadratic extensions of the field of rational numbers. Assuming that Riemann's hypothesis was valid for his zeta-function , Artin conjectured an upper bound for the number of solutions of congruences such as the one in (1) above. Artin's conjecture was then proved by Hasse for polynomials $f(x)$ of degrees 3 and 4 over arbitrary finite fields, and widely generalized by A. Weil (see [29]) as follows. Let X be a projective geometrically irreducible nonsingular algebraic curve of genus g, defined over a finite field $\mathbb{F}_\ell$ with ℓ elements. Then,

$$|\#X(\mathbb{F}_\ell) - (\ell + 1)| \leq 2g\sqrt{\ell}\,, \tag{2}$$

where $X(\mathbb{F}_\ell)$ denotes the set of $\mathbb{F}_\ell$-rational points of the curve X. Inequality (2) is equivalent to the validity of Riemann's hypothesis for the zeta-function associated to the curve X. Bombieri [2] gave an elementary proof of Inequality (2) following ideas of Stepanov, Postnikov and Manin that were used to treat the special case of hyperelliptic curves; see Chapter 5 in [25].

The interest on curves over finite fields with many rational points was renewed after Goppa's construction of codes with good parameters from such curves, see [15]. Number of solutions of congruences in two variables has other applications such as estimates of exponential sums over finite fields (see [22]), finite geometries (see [16]), correlations of shift register sequences (see [21]).

Here we will be interested in *maximal curves over* $\mathbb{F}_\ell$ with $\ell = q^2$, that is, we will consider curves X attaining Hasse-Weil's upper bound:

$$\#X(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq\,.$$

It is often the case that maximal curves are special (and interesting) from other points of view. For example, it is often the case that they have large automorphism groups, see [18] and [26]. Also, they are always nonclassical for the canonical linear series if $g \geq q - 1$, see Proposition 1.7 in [7].

We will consider here three important problems on maximal curves over $\mathbb{F}_{q^2}$:

1. Determination of the *possible genera* of maximal curves over $\mathbb{F}_{q^2}$.
2. Determination of *explicit equations* for maximal curves over $\mathbb{F}_{q^2}$.
3. *Classification* of maximal curves over $\mathbb{F}_{q^2}$ of a given genus.

The methods used to deal with these three problems are: the action of the Frobenius morphism on the Jacobian of a maximal curve (see the fundamental equation (3) here), Weierstrass Point Theory (including Stöhr-Voloch theory of Frobenius orders of a morphism), Castelnuovo's genus bound for curves in projective spaces and Riemann-Hurwitz genus formula for separable coverings of algebraic curves. It is also crucial the fact that a subcovering of a maximal curve is also a maximal curve.

2. The Genera of Maximal Curves

There are only finitely many possibilities for the genus g of a maximal curve X over $\mathbb{F}_{q^2}$, since Ihara [17] has shown that

$$g \leq q(q-1)/2\,.$$

The proof of the inequality above uses the knowledge of the zeta-function associated to a maximal curve and the following trivial observation:

$$\#X(\mathbb{F}_{q^4}) \;\geq\; \#X(\mathbb{F}_{q^2})\,.$$

Not every positive integer g with $g \leq q(q-1)/2$ can be the genus of a maximal curve over $\mathbb{F}_{q^2}$. It was shown in [8] that the genus g of a maximal curve over $\mathbb{F}_{q^2}$ satisfies (see also [27]):

$$\text{if} \quad g < q(q-1)/2, \quad \text{then} \quad g \leq (q-1)^2/4\,.$$

In other terms, the second largest genus g of a maximal curve over $\mathbb{F}_{q^2}$ is given by

$$g = [(q-1)^2/4], \qquad \text{where the brackets mean the integer part}\,.$$

The proof of this fact (i.e., that there are no genera of maximal curves over $\mathbb{F}_{q^2}$ in the open interval $\left(\frac{(q-1)^2}{4}, \frac{q(q-1)}{2}\right)$) uses the Castelnuovo genus bound for curves in projective spaces and the following "*fundamental linear equivalence of divisors on a maximal curve over $\mathbb{F}_{q^2}$*":

$$qP + FrP \sim (q+1)P_0\,, \tag{3}$$

where P is any point on the curve, FrP is the image of P by the $\mathbb{F}_{q^2}$-Frobenius morphism and P_0 is any $\mathbb{F}_{q^2}$-rational point on the curve.

It should be pointed out here that the exact value of the third largest genus of a maximal curve is still unknown (see [5]).

It is a result of Serre (see [19]) that if X is maximal over $\mathbb{F}_{q^2}$ and Y is covered by X over $\mathbb{F}_{q^2}$ (i.e., there is a surjective morphism $X \to Y$ defined over $\mathbb{F}_{q^2}$), then Y is also maximal over $\mathbb{F}_{q^2}$. This leads one to the consideration of quotient curves X/G of a maximal curve X over $\mathbb{F}_{q^2}$ under the action of subgroups G of the automorphism group $\mathrm{Aut}(X)$ of X. One then may hope to get several genera of maximal curves by applying the Riemann-Hurwitz formula to the covering $X \twoheadrightarrow X/G$ in order to determine the genus of the curve X/G. These ideas were systematically used in [11], where it is taken as the curve X the Hermitian curve; i.e., the curve X given by the affine equation:

$$y^q + y = x^{q+1} \quad \text{over} \quad \mathbb{F}_{q^2}\,. \tag{4}$$

This is a maximal curve over $\mathbb{F}_{q^2}$ with the biggest genus possible (i.e., with genus given by $g = q(q-1)/2$). The advantage in taking the Hermitian curve X is its huge automorphism group (see [26] and [20])

$$|\mathrm{Aut}(X)| = (q^2-1)\cdot q^3 \cdot (q^3+1)\,.$$

Here it is worthy to mention that there is no example of a maximal curve for which it is known that it cannot be covered by the Hermitian curve.

By a systematic use of subgroups of $\mathrm{Aut}(X)$, it is determined in [11] lots of possible genera of maximal curves over $\mathbb{F}_{q^2}$. In particular it is shown that for a fixed integer $g \geq 1$, there are maximal curves over $\mathbb{F}_{q^2}$ of genus g for infinitely many values of q (see Remark 6.2 in [11]). Another interesting result of this paper (writing $q = p^n$ and assuming that the characteristic p is odd) is the existence of maximal curves over $\mathbb{F}_{q^2}$ with genus g given by:

$$g = \frac{1}{2}p^{n-v}\cdot(p^{n-w}-1)\,, \tag{5}$$

for each $0 \leq v \leq n$ and for each $0 \leq w \leq (n-1)$. The genera above are obtained by considering p-subgroups G of $\mathrm{Aut}(X)$, where X denotes the Hermitian curve (see also [13], [14]).

3. Explicit Equations for Maximal Curves

For the applications to Coding Theory it is necessary that the curves are explicitly given by equations. In Example 6.3 of [11] it is pointed out that (see also Example 6.4 in [11])

$$z^n = t(t+1)^{q-1}, \qquad \text{with } n \text{ a divisor of } (q^2-1)\,, \tag{6}$$

is the equation of a maximal curve over $\mathbb{F}_{q^2}$ with genus given by $g = (n-\delta)/2$, where $\delta = gcd(n, q-1)$. It is with those maximal curves in equation (6) that it is shown in [11] that, for a fixed integer $g \geq 1$, there are maximal curves over $\mathbb{F}_{q^2}$ of genus g for infinitely many values of q (see also [12]).

Another interesting instance of an explicit equation for a maximal curve over $\mathbb{F}_{q^2}$ is given in Remark 4.4 of [10]. Denoting by $\varphi_n(T)$ the reduction modulo p of the (normalized) Chebyshev polynomial (i.e., the (monic) polynomial expressing $\cos n\theta$ in terms of $\cos\theta$), it is shown in [10] that (see also Remark 5.2 in [10])

$$v^{q+1} = \varphi_n(u) + 2, \qquad \text{with } n \text{ odd}\,, \tag{7}$$

is the equation of a maximal curve over $\mathbb{F}_{q^2}$. It is interesting to point out that properties of Chebyshev polynomials were deduced from the fact that equation (7) defines a maximal curve (see Section 6 of [10]).

We now mention a situation showing that sometimes it is hard to get such explicit equations. In Theorem 5.1 of [11] it is shown that there are maximal curves over $\mathbb{F}_{q^2}$ having genus g given by:

$$g = \frac{s-1}{2}, \qquad \text{for each divisor } s \text{ of } (q^2-q+1)\,. \tag{8}$$

This is shown by considering subgroups G of a certain cyclic subgroup of order (q^2-q+1) of the automorphism group of the Hermitian curve. The determination of explicit equations for the maximal curves over $\mathbb{F}_{q^2}$ with genera as in formula (8) above is not so easy (see [4]).

We end up this section with the following explicit equation for a maximal curve over $\mathbb{F}_{q^{2k}}$ with $k \geq 2$ (see [9]):

$$\sum_{j=0}^{k-1} y^{q^j} = w \cdot x^{q^k+1}, \qquad \text{with} \qquad w^{q^k-1} = -1. \tag{9}$$

This curve has genus $g = q^k(q^{k-1}-1)/2$ and, in particular, its genus appears among those given in formula (5). It can be shown that this curve is Galois covered by the Hermitian curve with a Galois group G of order q. In the particular case when $q = p$, this curve also appears in Theorem 2.1 of [5].

4. Classification of Maximal Curves

Since it is not known whether all maximal curves are covered by the Hermitian curve, one sees that the classification problem for maximal curves is a wide open problem. General results on this problem have been obtained (so far) when the genus of the maximal curve is large compared with the cardinality of the finite field.

The first result on the classification of maximal curves (see [23]) asserts that the Hermitian curve over $\mathbb{F}_{q^2}$ given by equation (4) is the **unique maximal curve** over $\mathbb{F}_{q^2}$ with genus $g = q(q-1)/2$. The main ingredient of the proof of this uniqueness of the Hermitian curve is the fundamental linear equivalence in equation (3) above.

Consider now the curve over $\mathbb{F}_{q^2}$ given by

$$y^q + y = x^m, \quad m \text{ a divisor of } (q+1)\,. \tag{10}$$

Since the curve in equation (10) is covered by the Hermitian curve, we have that it is a maximal curve. Its genus g is given by $g = (m-1)(q-1)/2$. For q odd and for $m = (q+1)/2$, we get a maximal curve over $\mathbb{F}_{q^2}$ with the second largest possible genus $g = (q-1)^2/4$. It was shown in [7] that this curve (equation (10) with q odd and $m = (q+1)/2$) is the **unique maximal curve** over $\mathbb{F}_{q^2}$ with genus $g = (q-1)^2/4$. In Theorem 2.3 of [7] it is given a characterization of the maximal curves in equation (10) above, but this characterization requires an extra-hypothesis on Weierstrass nongaps at a rational point over $\mathbb{F}_{q^2}$.

Write $q = p^t$ and consider the curve over $\mathbb{F}_{q^2}$ given by the affine equation:

$$\sum_{i=1}^{t} y^{q/p^i} + w \cdot x^{q+1} = 0, \qquad \text{with } w^{q-1} = -1\,. \tag{11}$$

Equation (11) defines a maximal curve and its genus g is given by $g = q(q-p)/2p$. In the case of characteristic $p = 2$, one gets the second largest genus possible and this curve (i.e., equation (11) with $p = 2$) is characterized in [1] with a similar extra-hypothesis on Weierstrass nongaps at a rational point. Also, equation (11) appears in Theorem 2.1 of [5] where it is classified the **Galois subcoverings of prime degrees** of the Hermitian curve. Besides the fundamental linear equivalence in equation (3), the other main ingredient for the classification problem of maximal curves over $\mathbb{F}_{q^2}$ of a given genus is the Stöhr-Voloch theory of Frobenius-orders (see [28]). This theory is similar to Weierstrass Point Theory in prime characteristics (see [24]) and provides also a proof of Weil's theorem (i.e., a proof of Inequality (2)). Roughly speaking, instead of counting rational points on the curve (i.e., the fixed points for the Frobenius action on the curve) Stöhr-Voloch's approach counts the number of points such that the image under the Frobenius action of a point lies on the osculating hyperplane to the curve at that point.

The first example of nonisomorphic maximal curves over $\mathbb{F}_{q^2}$ with the same genus was given in [3]. For $q \equiv 3(\text{modulo } 4)$, it is shown in [3] that the following two curves of genus $g = (q-1)(q-3)/8$ are not isomorphic:

$$y^q + y = x^{\frac{q+1}{4}} \quad \text{ and } \quad x^{\frac{q+1}{2}} + y^{\frac{q+1}{2}} = 1\,. \tag{12}$$

Both curves in equation (12) are maximal because they are Galois covered by the Hermitian curve, the first one with a cyclic group $G \simeq \mathbb{Z}/4\mathbb{Z}$ and the second one with a group $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We end up this paper by saying that the second curve in equation (12) above was characterized in [3] as the **unique maximal curve** over $\mathbb{F}_{q^2}$ with genus given by $g = (q-1)(q-3)/8$ that has a nonsingular plane model over $\mathbb{F}_{q^2}$.

References

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

[2] E. Bombieri, *Hilbert's 8th problem: An analogue,* Proc. Symp. Pure Math., **28** (1976), 269–274.

[3] A. Cossidente, J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *On plane maximal curves,* to appear in Compositio Math.

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

[5] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve,* to appear in Comm. Algebra.

[6] L. E. Dickson, *History of the theory of numbers,* Vol. II, Chelsea Publ. Comp., New York, (1971).

[7] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves,* J. Number Theory, **67**(1) (1997), 29–51.

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

[9] A. Garcia and L. Quoos, *A construction of curves over finite fields,* preprint.

[10] A. Garcia and H. Stichtenoth, *On Chebyshev polynomials and maximal curves,* Acta Arithmetica, **90** (1999), 301–311.

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

[12] A. Garcia and F. Torres, *On maximal curves having classical Weierstrass gaps,* Contemporary Math., **245** (1999), 49–59.

[13] G. van der Geer and M. van der Vlugt, *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes,* J. Comb. Theory A, **70** (1995), 337–348.

[14] G. van der Geer and M. van der Vlugt, *Generalized Hamming weights of codes and curves over finite fields with many points,* Israel Math. Conf. Proc., **9** (1996), 417–432.

[15] V. D. Goppa, *Geometry and Codes,* Mathematics and its applications, **24**, Kluwer Academic Publishers, Dordrecht-Boston-London (1988).

[16] J. W. P. Hirschfeld, *Projective geometries over finite fields,* second edition, Oxford University Press, Oxford (1998).

[17] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields,* J. Fac. Sci. Tokio, **28** (1981), 721–724.

[18] A. I. Kontogeorgis, *The group of automorphisms of function fields of the curve $x^n + y^m + 1 = 0$,* J. Number Theory, **72** (1998), 110–136.

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

[20] H. W. Leopoldt, *Über die Automorphismengruppe des Fermatkörpers,* J. Number Theory, **56** (1996), 256–282.

[21] R. Lidl and H. Niederreiter, *Finite fields,* Encyclopedia of mathematics and its applications, **20**, Addison-Wesley (1983).

[22] C. J. Moreno, *Algebraic curves over finite fields,* Cambridge University Press, **97** (1991).

[23] H. G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields,* J. Reine Angew. Math., **457** (1994), 185–188.

[24] F. K. Schmidt, *Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte,* Math. Z., **45** (1939), 75–96.

[25] S. A. Stepanov, *Arithmetic of algebraic curves,* Monographs in contemporary mathematics, Consultants Bureau, New York - London (1994).

[26] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharacteristic,* Arch. Math., **24** (1973), 527–544 and 615–631.

[27] H. Stichtenoth and C. P. Xing, *The genus of maximal function fields over finite fields,* Manuscripta Math., **86** (1995), 217–224.

[28] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields,* Proc. London Math. Soc. (3) **52** (1986), 1–19.

[29] A. Weil, *Courbes algébriques et variétés abeliennes,* Hermann, Paris, (1971).

IMPA,
Estrada Dona Castorina 110,
22.460–320, Rio de Janeiro, RJ,
Brasil
E-mail address: garcia@impa.br