Explicit equations for curves over finite fields with many rational points

Arnaldo Garcia

IMPA
Estrada Dona Castorina 110
22.460-320, Rio de Janeiro,
Brazil

1 Introduction

The investigation of rational points on curves over finite fields has a long history in mathematics; for example, Gauss determined the number of rational points in prime fields $\mathbb{F}_p$ with $p \geq 5$ of the Fermat curve of degree three.

By a curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$ we will always mean a geometrically irreducible smooth projective curve defined over $\mathbb{F}_q$. The main result of this theory is due to A. Weil and it gives in particular an upper bound (the so-called Hasse-Weil bound) for the cardinality of the set $\mathcal{C}(\mathbb{F}_q)$ consisting of the $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$:

$$\#\mathcal{C}(\mathbb{F}_q) \leq 1 + q + 2\sqrt{q} \cdot g(\mathcal{C}), \tag{1.1}$$

where $g(\mathcal{C})$ denotes the genus of $\mathcal{C}$. This result of A. Weil is equivalent to the validity of the Riemann Hypothesis for the Zeta Function associated to the curve $\mathcal{C}$.

Ihara [17] was the first one to realize that the Hasse-Weil bound (1.1) could be improved for curves with large genus. Fixing the finite field $\mathbb{F}_q$ and considering curves $\mathcal{C}$ over $\mathbb{F}_q$ with $g(\mathcal{C})$ arbitrarily large, Ihara defined

$$A(q) := \limsup_{g(\mathcal{C})\to\infty} \frac{\#\mathcal{C}(\mathbb{F}_q)}{g(\mathcal{C})} \tag{1.2}$$

and he proved that

- $A(q) \leq \sqrt{2q}$ for all q.
- $A(q) \geq \sqrt{q} - 1$ if q is a square.

Note that the Hasse-Weil bound (1.1) gives only the inequality $A(q) \leq 2\sqrt{q}$. Later Drinfeld-Vladut [4] showed that

$$A(q) \leq \sqrt{q} - 1 \quad \text{for all } q.$$

So we have the equality

$$A(q) = \sqrt{q} - 1 \quad \text{if } q \text{ is a square.} \tag{1.3}$$

The exact value of $A(q)$ for nonsquare q is not known. Serre showed in particular that

$$A(q) > 0 \quad \text{for all } q. \tag{1.4}$$

For cubic powers of prime numbers, Zink [23] showed that

$$A(p^3) \geq \frac{2(p^2-1)}{p+2} \quad \text{for all primes } p. \tag{1.5}$$

Recently the interest on explicit equations for curves over finite fields with many rational points was renewed, after the construction of good linear codes from such curves; this construction is due to Goppa [16]. Another big motivation for explicit equations came from the result of Tsfasman-Vladut-Zink [22] proving the existence of arbitrary long linear codes with limit parameters above the so-called Gilbert-Varshamov bound.

We refer to [14] for an overview of recent developments in this field of curves over finite fields and its applications.

2 Maximal curves

Let q be a square; say $q = \ell^2$. A *maximal curve* $\mathcal{C}$ over $\mathbb{F}_q$ is a curve attaining the upper bound in (1.1); i.e., a curve $\mathcal{C}$ such that

$$\#\mathcal{C}(\mathbb{F}_q) = 1 + \ell^2 + 2\ell \cdot g(\mathcal{C}). \tag{2.1}$$

The genus of a maximal curve $\mathcal{C}$ over $\mathbb{F}_q$ satisfies (see [17]):

$$g(\mathcal{C}) \leq \ell(\ell-1)/2. \tag{2.2}$$

There is a unique maximal curve $\mathcal{H}$ over $\mathbb{F}_q$ with $q = \ell^2$ such that $g(\mathcal{H}) = \ell(\ell-1)/2$; it is the so-called *Hermitian curve* over $\mathbb{F}_q$ and it can be given by the affine plane equation (see [20]):

$$Y^\ell + Y = X^{\ell+1} \quad \text{over } \mathbb{F}_{\ell^2}. \tag{2.3}$$

Not every integer g with $1 \leq g \leq g(\mathcal{H})$ is the genus of a maximal curve over $\mathbb{F}_{\ell^2}$ (see [7]). For example, let $q = \ell^2$ and q odd (i.e., the characteristic p is odd), then the second largest genus g_2 of maximal curves over $\mathbb{F}_q$ is

$$g_2 = (\ell - 1)^2/4. \tag{2.4}$$

There is a unique maximal curve over $\mathbb{F}_q$ with genus given by (2.4); it can be given by the affine plane equation (see [8]):

$$Y^\ell + Y = X^{(\ell+1)/2} \quad \text{over } \mathbb{F}_{\ell^2}. \tag{2.5}$$

The unicity results in (2.3) and (2.5) do not hold in general; i.e., there are nonisomorphic maximal curves over $\mathbb{F}_{\ell^2}$ with the same genus (see [1] and [3]). The problem of determining the genera of all maximal curves over $\mathbb{F}_{\ell^2}$ is an open problem.

Suppose that $\mathcal{C}_2$ is a *subcover* of $\mathcal{C}_1$; i.e., we have a surjective map

$$\varphi\colon \mathcal{C}_1 \twoheadrightarrow \mathcal{C}_2$$

where both curves $\mathcal{C}_1, \mathcal{C}_2$ and the map φ are defined over the finite field $\mathbb{F}_q$. It is a result of Serre (see [18]) that

$$\mathcal{C}_1 \text{ maximal} \qquad \text{implies} \qquad \mathcal{C}_2 \text{ maximal}. \tag{2.6}$$

So subcovers $\mathcal{C}$ of the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{\ell^2}$ are maximal curves. The converse statement is an open problem:

Open Problem. *Is any maximal curve $\mathcal{C}$ over $\mathbb{F}_q$ with $q = \ell^2$ a subcover of $\mathcal{H}$?*

We now want to present a maximal curve $\mathcal{C}_2$ over $\mathbb{F}_q$ with $q = 27^2$ which is not a Galois subcover of $\mathcal{H}$; i.e., there is no surjective Galois map φ (see [9])

$$\varphi\colon \mathcal{H} \twoheadrightarrow \mathcal{C}_2.$$

For $q = \ell^2$ and $\ell = p^n$, with p prime and n odd, consider the curve $\mathcal{C}(p, n)$ given by the affine plane equation

$$Y^{p^2} - Y = X^{(p^n+1)/(p+1)}. \tag{2.7}$$

One can show that (2.7) defines a maximal curve over $\mathbb{F}_q$ and we then take $\mathcal{C}_2 := \mathcal{C}(3, 3)$.

We refer to [10] for an overview on results on maximal curves.

3 Recursive towers of curves

The fundamental result of Tsfasman-Vladut-Zink (see [22] and Proposition VII.2.5 of [21]) asks for good lower bounds for Ihara's quantity $A(q)$ which was defined in (1.2) above. One way to get lower bounds on $A(q)$ is by considering the limits $\lambda(\mathcal{F})$ of towers $\mathcal{F}$ of curves defined over the finite field $\mathbb{F}_q$ (see (3.2) below). Such a tower $\mathcal{F}$ is an infinite sequence of curves and surjective maps

$$..... \twoheadrightarrow \mathcal{C}_4 \twoheadrightarrow \mathcal{C}_3 \twoheadrightarrow \mathcal{C}_2 \twoheadrightarrow \mathcal{C}_1$$

such that all curves and all maps are defined over $\mathbb{F}_q$ and moreover

$$g(\mathcal{C}_n) \to \infty \quad \text{as} \quad n \to \infty.$$

The limit $\lambda(\mathcal{F})$ of an $\mathbb{F}_q$-tower $\mathcal{F}$ is defined by (see [11])

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \frac{\#\mathcal{C}_n(\mathbb{F}_q)}{g(\mathcal{C}_n)}. \tag{3.1}$$

By the definitions we have

$$0 \le \lambda(\mathcal{F}) \le A(q) \quad \text{for any } \mathbb{F}_q\text{-tower } \mathcal{F}. \tag{3.2}$$

There is a way of "cooking up" an $\mathbb{F}_q$-tower $\mathcal{F}$ from a single absolutely irreducible polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$; the towers $\mathcal{F}$ obtained are then called *recursive* (or recursively defined by the polynomial $f(X,Y)$). If we write

$$\mathcal{F} = (..... \twoheadrightarrow \mathcal{C}_4 \twoheadrightarrow \mathcal{C}_3 \twoheadrightarrow \mathcal{C}_2 \twoheadrightarrow \mathcal{C}_1) \quad \text{then :}$$

- $\mathcal{C}_1$ is the projective line $\mathbb{P}^1$.
- $\mathcal{C}_2$ is the curve (nonsingular projective model) given by the affine plane equation

$$f(X_1, X_2) = 0.$$

- $\mathcal{C}_3$ is the curve (nonsingular projective model) given in 3-space by the two equations

$$f(X_1, X_2) = 0 \quad \text{and } f(X_2, X_3) = 0.$$

- $\mathcal{C}_4$ is the curve (nonsingular projective model) given in 4-space by the three equations

$$f(X_1, X_2) = f(X_2, X_3) = f(X_3, X_4) = 0,$$

and so on ...

In the next section we will present recursive towers $\mathcal{F}$ over $\mathbb{F}_q$ giving proofs of the results in (1.3), (1.4) and (1.5). The advantages here are:

- The proofs are simpler than the original ones.
- They provide explicit equations for the curves $\mathcal{C}_n$ in the towers, and also explicit formulas for $g(\mathcal{C}_n)$.

Other methods to get information on $A(q)$ are from Class Field (see [19]) and from Modular Curves (elliptic, Shimura, Drinfeld). We refer to [5] and [6] for the modular interpretation of some of the recursive towers in the next section.

4 Explicit recursive towers

Let $\mathcal{F} = (... \twoheadrightarrow \mathcal{C}_4 \twoheadrightarrow \mathcal{C}_3 \twoheadrightarrow \mathcal{C}_2 \twoheadrightarrow \mathcal{C}_1)$ be an $\mathbb{F}_q$-tower. The tower $\mathcal{F}$ is called *tame* if all maps $\varphi\colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ are tame maps (i.e., the characteristic p does not divide any ramification index of the map φ). Otherwise we call $\mathcal{F}$ an *wild tower*. We present in this section two tame towers and three wild towers, all of them recursively defined by polynomials $f(X, Y) \in \mathbb{F}_q[X, Y]$. We start with the tame towers:

Example 4.1. Let $q = p^t$ with p prime and $t \geq 2$. Consider the tower $\mathcal{F}_1$ over $\mathbb{F}_q$ given recursively by the polynomial (see [13])

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

We have that its limit satisfies

$$\lambda(\mathcal{F}_1) \geq 2/(q - 2) > 0. \tag{4.1}$$

The result in (4.1) above is obtained in a very simple manner and it gives:

- A very simple proof of the result of Serre in (1.4) for nonprime finite fields (i.e., for $q \neq p$).
- A very simple proof of the equality $A(4) = 1$; i.e., the result in (1.3) for $q = 4$.

□

Example 4.2. Let $q = p^2$ with p an odd prime. Consider the recursive tower $\mathcal{F}_2$ over $\mathbb{F}_q$ given by (see [12])

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

This means that $\mathcal{F}_2$ is the tower over $\mathbb{F}_q$ given recursively by the polynomial

$$f(X,Y) = 2XY^2 - X^2 - 1.$$

We have that its limit satisfies

$$\lambda(\mathcal{F}_2) = p - 1 = \sqrt{q} - 1. \tag{4.2}$$

The result in (4.2) is much harder to obtain than the one in (4.1). To get it we needed an investigation of the roots of Deuring polynomial (which is a polynomial parametrizing supersingular elliptic curves). The result in (4.2) and the one in (4.1) for the case $q = 4$, show that we have

$$A(p^2) = p - 1 \quad \text{for all primes } p.$$

□

The towers $\mathcal{F}_1$ and $\mathcal{F}_2$ above are such that each step $\varphi\colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ is a Kummer cover. The next two towers $\mathcal{F}_3$ and $\mathcal{F}_4$ are such that each step is an Artin-Schreier cover; in particular $\mathcal{F}_3$ and $\mathcal{F}_4$ are wild towers. The determination of explicit formulas for $g(\mathcal{C}_n)$ for all values of $n \in \mathbb{N}$, is much harder in the case of wild towers.

Example 4.3. Let $q = \ell^2$ where ℓ is a prime power. Consider the recursive tower $\mathcal{F}_3$ over $\mathbb{F}_q$ given by the equation below (see [11]):

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

We have that its limit satisfies

$$\lambda(\mathcal{F}_3) = \ell - 1 = \sqrt{q} - 1. \tag{4.3}$$

As mentioned above the determination of the individual genus $g(\mathcal{C}_n)$ for all values of $n \in \mathbb{N}$ is a hard task. In our case of the tower $\mathcal{F}_3$ we get for example (see Remark 3.8 of [11]):

$$g(\mathcal{C}_n) = (\ell^{n/2} - 1)^2 \quad \text{if } n \text{ is even.}$$

□

The result in (4.3) above gives a complete proof of the statement in (1.3) in the introduction, with the advantage of providing explicit equations for the infinite sequence of algebraic curves involved. Now we turn our attention to finite fields with cubic cardinalities.

Example 4.4. Let $q = 8$; i.e., $q = p^3$ and $p = 2$. Consider the tower $\mathcal{F}_4$ over $\mathbb{F}_8$ given recursively by (see [15]):

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

Its limit satisfies

$$\lambda(\mathcal{F}_4) = \frac{3}{2} = \frac{2(2^2 - 1)}{2 + 2}. \tag{4.4}$$

So $\mathcal{F}_4$ is an explicit recursive tower attaining Zink's lower bound in (1.5) for $p = 2$.

□

In all four towers above we have that each step $\varphi\colon \mathcal{C}_{n+1} \twoheadrightarrow \mathcal{C}_n$ is Galois. The next tower $\mathcal{F}_5$ is an wild tower with nonGalois steps (for $\ell \neq 2$).

Example 4.5. Let $q = \ell^3$ where ℓ is a prime power. Consider the recursive tower $\mathcal{F}_5$ over $\mathbb{F}_q$ given by the equation below (see [2]):

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

Its limit satisfies

$$\lambda(\mathcal{F}_5) \geq \frac{2(\ell^2 - 1)}{\ell + 2}. \tag{4.5}$$

The result in (4.5) proves the following generalization of the statement in (1.5):

$$A(\ell^3) \geq \frac{2(\ell^2 - 1)}{\ell + 2} \quad \text{for all prime powers } \ell. \tag{4.6}$$

The tower $\mathcal{F}_5$ in the case $\ell = 2$ is the same tower as $\mathcal{F}_4$ (after some change of variables).

□

The result in (4.6) is considered as a very good lower bound on the quantity $A(q)$ for $q = \ell^3$. *What about good lower bounds for*

$$A(\ell^5), \quad A(\ell^7), \quad A(\ell^{11}), \ldots?$$

The question above is completely open.

References

[1] M. Abdón and A. Garcia, *On a characterization of certain maximal curves*. Finite Fields Appl. **10** (2004), 133–158.

[2] J. Bezerra, A. Garcia and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*. J. Reine Angew. Math. **589** (2005), 159–199.

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

[4] V.G. Drinfeld and S.G. Vladut, *The number of points of an algebraic curve*. Funktional. Anal. i Prilozhen. **17** (1983), 68–69. [Funct. Anal. Appl. **17** (1983), 53–54].

[5] N. Elkies, *Explicit modular towers*, in: Proceedings of the 35$^{\text{th}}$ Annual Allerton Conference on Communication, Control and Computing (eds. T. Basar et al.) Urbana, IL (1997), 23-32.

[6] N. Elkies, *Explicit towers of Drinfeld modular curves*, in: European Congress of Mathematics, vol. II (eds. C. Casacuberta et al.), Birkhäuser, Basel (2001), 189–198.

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

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

[9] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve*. Bull. Brazilian Math. Soc. (to appear).

[10] A. Garcia, *Curves over finite fields attaining the Hasse-Weil upper bound*, in: European Congress of Mathematics, vol. II (eds. C. Casacuberta et al.), Birkhäuser, Basel (2001), 199–205.

[11] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*. J. Number Theory **61** (1996), 248–273.

[12] A. Garcia and H. Stichtenoth, *On tame towers over finite fields*. J. Reine Angew. Math. **557** (2003), 53–80.

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

[14] G. van der Geer, *Curves over finite fields and codes*, in: European Congress of Mathematics, vol. II (eds. C. Casacuberta et al.), Birkhäuser, Basel (2001), 225–238.

[15] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*. Bull. London Math. Soc. **34** (2002), 291–300.

[16] V.D. Goppa, *Codes on algebraic curves*. (Russian) Dokl. Akad. Nauk SSSR **259** (1981), 1289–1290.

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

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

[19] H. Niederreiter and C.P. Xing, Rational points of curves over finite fields, Cambridge Univ. Press, Cambridge, 2001.

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

[21] H. Stichtenoth, Algebraic function fields and codes, Springer Verlag, Berlin, 1993.

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

[23] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in: Fundamentals of Computation Theory, (ed. L. Budach), Lecture Notes in Computer Science, Vol. **199**, Springer, Berlin, pp. 503–511, 1985.