

Zeta functions of small-defect curves over finite fields

Graeme Taylor

January 31, 2007

Abstract

Connections between the geometry of curves over finite fields and constraints on algebraic integers arise from the Weil bounds for the number of rational points. In particular, tables by Smyth ([4]) relating the degree and trace of algebraic integers can be adapted to describe the zeta functions of curves which are close to attaining the bound. The standard reference is Serre [3], but these notes remain unpublished, so the procedure is described in full detail here. Some slight refinements are possible from advances in the constraints on algebraic integers, and a brief indication of geometric considerations (mostly from [2]) is given at the end.

1 Background

For curves of given genus over a finite field the Weil conjectures for curves give rise to a bound on the maximum number of points. Further, a precise description of the number of points can be given if the zeta function is known; and since this expression depends on the roots of the polynomial, we can use results regarding sums of algebraic integers to further refine our knowledge of the situation, characterising the possible zeta functions for which the number of points is very close to the bound. Throughout we consider curves C of genus g over the field $\mathbb{F}_q = \mathbb{F}_{p^r}$; we denote by $N_q(g)$ the maximum number of points of such a curve over this field, i.e., $\sup_X \{ \#C(\mathbb{F}_q) \}$.

1.1 Weil Conjectures for Curves

Definition 1.1.1. For a curve C the *zeta function* of C over \mathbb{F}_q is given by

$$Z(T) = \exp \left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{q^r}) \frac{T^r}{r} \right) \in \mathbb{Q}[[T]]$$

Theorem 1.1.2. *Weil conjectures for curves.* We have

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)}$$

such that

$$P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T) \in \mathbb{Z}[T]$$

with the α_i algebraic integers such that $|\alpha_i| = \sqrt{q}$.

1.2 Hasse-Weil bound

We have that

$$\#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

which, as $-\sqrt{q^r} \leq |\alpha_i|^r \leq \sqrt{q^r}$ immediately gives

$$\#C(\mathbb{F}_{q^r}) \leq q^r + 1 + \lfloor 2g\sqrt{q^r} \rfloor$$

hence from $r = 1$ we have the *Hasse-Weil bound*:

$$N_q(g) \leq q + 1 + \lfloor 2g\sqrt{q} \rfloor$$

1.3 Algebraic Integers

Consider a totally positive algebraic number α of degree d with conjugates $0 < \alpha_1 < \dots < \alpha_d$ (that is, the minimal polynomial of α is of degree d and factors over \mathbb{C} as $\prod (x - \alpha_i)$).

Definition 1.3.1. The *mean trace* of α is

$$\text{tr}(\alpha) = \frac{1}{d} \sum_{i=1}^d \alpha_i$$

The set

$$\mathcal{T} = \{ \text{tr}(\alpha) \mid \alpha \text{ is a totally positive algebraic integer} \}$$

is of considerable interest; see for instance [1]. In particular, it can be easily demonstrated that 2 is a limit point of the set; it is unknown whether a smaller limit point exists.

However, there are results concerning the lower bound for the mean trace of such algebraic integers. From [1] we have:

Theorem 1.3.2. *For all totally positive algebraic numbers α , except a finite number of explicit exceptions,*

$$\text{tr}(\alpha) > 1.780022$$

The exceptions arise as the roots of the polynomials

$$\begin{aligned} &x - 1 \\ &x^2 - 3x + 1 \\ &x^3 - 5x^2 + 6x - 1 \\ &x^4 - 7x^3 + 13x^2 - 7x + 1 \\ &x^4 - 7x^3 + 14x^2 - 8x + 1 \end{aligned}$$

2 Application of the trace to bounds

Given the results of the previous section, it is natural to recast the quantity $\#C(\mathbb{F}_q)$ in terms of totally positive algebraic integers. To do this, we introduce new quantities

$$\beta_i = \lfloor 2\sqrt{q} + 1 \rfloor + \alpha_i + \bar{\alpha}_i > 0 \in \mathbb{R}$$

Then $\sum_{i=1}^{2g} \alpha_i = \sum_{i=1}^g (\beta_i - \lfloor 2\sqrt{q} + 1 \rfloor) = \sum_{i=1}^g \beta_i - g\lfloor 2\sqrt{q} + 1 \rfloor$ so

$$\#C(\mathbb{F}_q) = q + 1 - \left(\sum_{i=1}^g \beta_i - g\lfloor 2\sqrt{q} + 1 \rfloor \right) = q + 1 + g\lfloor 2\sqrt{q} + 1 \rfloor - \sum_{i=1}^g \beta_i \quad (1)$$

2.1 The refined Weil Bound

From Galois Theory we have that $\prod \beta_i > 0$ is an integer; hence by the AM-GM inequality it follows that

$$\frac{1}{g} \sum_{i=1}^g \beta_i \geq \left(\prod_{i=1}^g \beta_i \right)^{1/g} \geq 1$$

i.e., $\sum \beta_i \geq g$. We can incorporate this into (1) to obtain the *refined Weil bound*

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor \quad (2)$$

We will use this version (from Serre) of the Weil bound to assess the deficiency of curves, as follows:

Definition 2.1.1. A curve C is said to be of *defect* k if $\#C(\mathbb{F}_q) = q + 1 + g\lfloor 2\sqrt{q} \rfloor - k$.

Proposition 2.1.2. *By (1) The defect of a curve C is given by $\left(\sum_{i=1}^g \beta_i \right) - g$.*

2.2 Controlling the defect

Let

$$Q(x) = \prod_{i=1}^g (x - \beta_i)$$

Then $Q(x)$ factors into some product of irreducibles, say $Q(x) = Q_1(x) \cdots Q_d(x)$, with each Q_j of degree n_j such that $\sum_{j=1}^d n_j = g$. Choose roots β_j of each Q_j . Then the β_i are comprised of the β_j and their conjugates, and hence

$$\sum_{i=1}^g \beta_i = \sum_{j=1}^d \text{Trace}(\beta_j) = \sum_{j=1}^d n_j \text{tr}(\beta_j)$$

from definition 1.3.1.

Consider again the set of exceptional polynomials from theorem 1.3.2, namely

$$S = \{x - 1, x^2 - 3x + 1, x^3 - 5x^2 + 6x - 1, x^4 - 7x^3 + 13x^2 - 7x + 1, x^4 - 7x^3 + 14x^2 - 8x + 1\}$$

We may immediately deduce a condition for small defect:

Proposition 2.2.1. *If $\{Q_1, \dots, Q_d\} \cap S = \emptyset$ then the defect is at least $0.780022g$.*

Proof. Since none of the Q_j is exceptional, for each β_j we know $\text{tr}(\beta_j) \geq 1.780022g$. Hence

$$\begin{aligned} k &= \left(\sum_{i=1}^g \beta_i \right) - g = \left(\sum_{j=1}^d n_j \text{tr}(\beta_j) \right) - g \\ &\geq \left(\sum_{j=1}^d n_j 1.780022 \right) - g = 1.780022 \left(\sum_{j=1}^d n_j \right) - g \\ &= 1.780022g - g \\ &= 0.780022g \end{aligned}$$

■

Unfortunately, this does not give a complete characterisation. For instance, Having

$$\{Q_1, \dots, Q_d\} \subset S$$

does not guarantee a defect of less than $0.780022g$; nor do all curves with small defect give rise to a factorisation purely from elements of S , since the smaller trace of some summands gives enough 'breathing space' for the remaining, possibly non-exceptional summands. However, to ensure a small defect these polynomials are still constrained, and by Siegel's theorem the supply of suitable polynomials is finite. Tables by Smyth [4] specify all the polynomials that give rise to totally positive algebraic integers with trace-degree at most six, and thus for small values of both the defect and genus it is possible to enumerate all the suitable choices of Q .

2.3 Small defect curves of genus 3

For genus 3, Proposition 2.2.1 gives a minimum defect of 2.340066 - effectively, 3 - unless at least one factor of Q is an element of S . Since Q is a degree three polynomial, it is not too taxing to establish all the possibilities for defect 0, 1 or 2. It is possible to arrive at such a list purely by considering the tables in [4], as in [3], but knowing that at least one factor is drawn from S cuts down the search space slightly.

- $Q = Q_1$
If Q is an irreducible cubic from S , then it is necessarily $x^3 - 5x^2 + 6x - 1$. This has trace 5, and thus defect 2.

- $Q = Q_1Q_2$

wlog, let Q_1 be linear and Q_2 quadratic.

If $Q_1 \in S$, then $Q_1 = (x - 1)$. So either $Q_2 \in S$, in which case it is $x^2 - 3x + 1$, and the defect is $1+3-3 = 1$; or Q_2 is some other quadratic, with trace at least $1.780022 \times 2 = 3.560044$. Thus the roots of such a polynomial have $\text{trace} - \text{degree} \geq 1.560044$, a value of at most 2 is permitted (were it 3, then the trace is 5, the summed traces 6 and the defect 3). Consulting [4], we find that the only possibilities are $1 - 4x + x^2$ and $2 - 4x + x^2$.

If $Q_1 \notin S$ then $Q_2 = x^2 - 3x + 1 \in S$, which contributes a trace of 3. As Q_1 is linear, has an integer root and is not $(x - 1)$, it is $(x - n)$ for some $n \in \mathbb{N} \setminus \{1\}$ and the defect is $3 + n - 3 = n \geq 2$. So the best we can achieve is defect 2, and then only with the factor $(x - 2)$.

- $Q = Q_1Q_2Q_3$

Here each factor is simply $(x - n_i)$ for $n_i \in \mathbb{N}$, with at least one of them $(x - 1) \in S$; wlog $1 = n_1 \leq n_2 \leq n_3$ and the defect is $1 + n_2 + n_3 - 3 = n_2 + n_3 - 2$. Thus the possibilities are $n_2 = n_3 = 1$ for defect 0; $n_2 = 1, n_3 = 2$ for defect 1, $n_2 = 1, n_3 = 3$ for defect 2 or $n_2 = n_3 = 2$ for defect 2.

In summary, the possibilities are

k	Q	$\{\beta_1, \beta_2, \beta_3\}$
0	$(x - 1)^3$	$\{1, 1, 1\}$
1	$(x - 1)^2(x - 2)$	$\{1, 1, 2\}$
	$(x - 1)(x^2 - 3x + 1)$	$\{1, (3 + \sqrt{5})/2, (3 - \sqrt{5})/2\}$
2	$(x - 1)^2(x - 3)$	$\{1, 1, 3\}$
	$(x - 1)(x - 2)^2$	$\{1, 2, 2\}$
	$(x - 2)(x^2 - 3x + 1)$	$\{2, (3 + \sqrt{5})/2, (3 - \sqrt{5})/2\}$
	$(x - 1)(x^2 - 4x + 1)$	$\{1, 2 + \sqrt{3}, 2 - \sqrt{3}\}$
	$(x - 1)(x^2 - 4x + 2)$	$\{1, 2 + \sqrt{2}, 2 - \sqrt{2}\}$
	$x^3 - 5x^2 + 6x - 1$	$\{4 \cos^2(\pi/7), 4 \cos^2(2\pi/7), 4 \cos^2(3\pi/7)\}$

3 Geometry

3.1 Eigenvalues of Frobenius

Recall that $\beta_i = \lfloor 2\sqrt{q} + 1 \rfloor + \alpha_i + \bar{\alpha}_i$. Defining $m = \lfloor 2\sqrt{q} \rfloor$ and $x_i = m + 1 - \beta_i$, we see that $x_i = -(\alpha_i + \bar{\alpha}_i)$. These x_i can be recovered in another way: $\{a_i, \bar{a}_i\}$ is the family of g conjugate pairs of eigenvalues of Frobenius acting on the Jacobian of the curve C . Following Serre in [3] (see e.g., [2]), it is conventional to describe C as having *zeta function of type* (x_1, \dots, x_g) and formulate conditions in terms of the x_i rather than the β_i . Adopting such a convention and generalising the approach above, it can be seen (after transformation) that we have covered all but one possibility for defect 0, 1 or 2, with the addition only possible if the genus is at least 4:

k	(x_1, \dots, x_g)	g
0	(m, \dots, m)	
1	$([m, \dots, m], m - 1)$	$g \geq 1$
	$([m, \dots, m], m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2})$	$g \geq 2$
2	$([m, \dots, m], m - 2)$	$g \geq 1$
	$([m, \dots, m], m - 1, m - 1)$	$g \geq 2$
	$([m, \dots, m], m - 1, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2})$	$g \geq 3$
	$([m, \dots, m], m + \sqrt{3} - 1, m - \sqrt{3} - 1)$	$g \geq 2$
	$([m, \dots, m], m + \sqrt{2} - 1, m - \sqrt{2} - 1)$	$g \geq 2$
	$([m, \dots, m], m + 1 - 4 \cos^2 \pi/7, m + 1 - 4 \cos^2 2\pi/7, m + 1 - 4 \cos^2 3\pi/7)$	$g \geq 3$
	$([m, \dots, m], m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2})$	$g \geq 4$

3.2 Some restrictions on geometry

Having established these limited possibilities through number-theoretic arguments, a geometric approach may introduce further conditions or eliminate entire cases. For instance, the Jacobian cannot admit a non-trivial decomposition into a product as a polarized abelian variety. If $X = (x_1, \dots, x_g)$ is such that $\{x_i\}$ can be partitioned into two nonempty subsets I, J such that $i - j$ is a unit for any $i \in I, j \in J$ and I, J are permuted by $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then just such a decomposition would arise; thus there cannot be a curve of type X . For instance, if $g > 2$ then both possibilities for defect 1 admit a partition in this way; thus, there are no defect 1 curves of genus $g > 2$.

Moreover, stronger number-theoretic bounds allow conclusions to be drawn about the types of zeta functions of curves. The *Ihara bound* is given by

$$N_q(g) \leq \frac{1}{2} \left(\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - (g - 2q - 2) \right)$$

This is stronger than the Weil bound for sufficiently large g relative to q , which ensures a defect; this means that for suitable (g, q) there are no defect 0 curves and hence no zeta functions of type (m, \dots, m) .

For particularly small values of q , types may be eliminated on the grounds that they would require $|x_i| > 2\sqrt{q}$, which is impossible (recall $|\alpha_i| = \sqrt{p}$).

References

- [1] J.Aguirre, M.Bilbao, J. Peral (2005) '*The Trace of Totally Positive Algebraic Integers*'.
- [2] K. Lauter (2001) '*Geometric Methods for Improving the Upper Bounds on the Number of Rational Points on Algebraic Curves over Finite Fields*'.
- [3] J-P. Serre (1985) '*Rational points on curves over finite fields*' (Notes by F.Gouvea from lectures at Harvard University).
- [4] C.Smyth (1984) '*Totally Positive Algebraic Integers of Small Trace*'.