Serre Problem: large g.
Lecture 11

Elisa Lorenzo García

2nd May 2016

Contents

We will study today results concerning Serre's problem for large values of g.

Let $C/\mathbb{F}_q$ be a genus g curve. If it attains the Weyl bound and q is a square, Ihara roved that

$$g \leq \frac{1}{2}(q - q^{1/2}).$$

Proof. (Ihara's bound) Let us write $\#C(\mathbb{F}_q) = q + 1 - \sum_{\alpha+1}^{2g} \pi_\alpha$, where π_α are the eigenvalues of the Frobenius endomorphism, so $\mid \pi_\alpha \mid = q^{1/2}$. if the curve attains the Weyl bound, one has $\pi_\alpha = q^{1/2}$. Then $\#C(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{\alpha=1}^{2g} q = q^2 + 1 - 2gq$, but obviously $\#C(\mathbb{F}_{q^2}) \geq \#C(\mathbb{F}_q)$. Then, the result follows. □

Example 0.1. *The curve $C : x^{q^{1/2}+1} + y^{q^{1/2}+1} + z^{q^{1/2}+1} = 0$, where q is a square, has genus equal to $g = \frac{1}{2}(q - q^{1/2})$ and $\#C(\mathbb{F}_q) = q^{3/2} + 1 = q + 1 + 2gq^{1/2}$. Hence, Ihara's bound is sharper as possible.*

To check it, let us consider the involution $\mathbb{F}_q \to \mathbb{F}_{q^{1/2}} : x \to \overline{x} = x^{q^{1/2}}$. The equation of the curve becomes $x\bar{x} + y\bar{y} + z\bar{z} = 0$. Notice that $x\bar{x} = -y\bar{y} - z\bar{z}$ has 1 solution if $y\bar{y} + z\bar{z} = 0$ and $q + 1$ otherwise. The expression $y\bar{y} + z\bar{z}$ is equal to zero if and only if $y = z = 0$ or for $q + 1$ different values of z if $y \neq 0$.

Proposition 0.2. *Let $\phi : C \to C'$ be a regular and non-constant morphism. If C attains the Weyl bound, also C' does it.*

Proof. If C attains the Weyl bound, then all the eigenvalues of the Frobenius endomorphism in $J(C)$ are equal to $q^{1/2}$. The morphism ϕ induces $\phi^* : J(C') \hookrightarrow J(C)$, then all the eigenvalues of the Froebnius endomorphism for $J(C')$ are also equal to $q^{1/2}$. □

1 Oesterlé bound

Let $C/\mathbb{F}_q$ be a genus g curve. Let us denote by π_α the Frobenius eigenvalues ordered by $\pi_1, ..., \pi_g, \bar{pi}_1, ..., \bar{\pi}_g$. We also write $\pi_\alpha = q^{1/2}e^{i\phi_\alpha}$, where $0 \le \phi_\alpha \le \pi$. By $N_n(C)$ we denote $\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{\alpha=1}^{g}(\pi_\alpha + \bar{\pi}_\alpha) = q^n + 1 - 2\sum_{\alpha+1}^{g} q^{n/2}\cos(n\phi_\alpha)$.

The Zeta-function of C is given by

$$Z(T) = \exp(\sum_1^\infty \frac{N_n(C)T^n}{n}) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) = \prod_{\alpha=1}^{2g}(1 - \pi_\alpha T)$.

If we denote by a_d the number of Galois orbits of points of degree d (that is, in $\mathbb{F}_{q^d}$), we clearly have $N_n = \sum_{d|n} da_d$. Moreover,

$$Z(T) = \prod_{d\ge1} \frac{1}{(1-T^d)^{a_d}}. \tag{1}$$

Let $f(\theta)$ be a trigonometric polynomial of the form

$$f(\theta) = 1 + 2\sum_{n\ge1} c_n\cos(n\theta) = \sum_{n\in\mathbb{Z}} c_n e^{in\theta}, \;\; c_0 = 1, \, c_{-n} = c_n.$$

To f, we can attach polynomials

$$\Psi_d(t) = \sum_{d|n\ge1} c - nt^n, \text{ and } \Psi(t) = \Psi_1(t).$$

We will prove

$$\sum_{\alpha=1}^{g} f(\phi_\alpha) + \sum_{d\ge1} da_d\Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2}).$$

Proof. We have

$$\sum_{alpha=1}^{g} f(\phi_\alpha) = g + 2\sum c_n\cos(n\phi_\alpha) = g + 2\sum c_n \sum \cos(n\phi_\alpha) =$$

$$g + \sum_{n\ge1} c_n(q^{n/2} + q^{-n/2} - q^{-n/2}N_n).$$

We only need to prove that

$$\sum da_d\Psi_d(q^{-1/2}) = \sum c_n q^{-n/2}N_n.$$

□

Example 1.1. *1. If $f = 1$, $c_n = 0$ and $\Psi_d = 0$, we get $g = g$.*

2. If $f = 1 + cos(\theta)$, we recover Weil formula, namely,

$$N = q + 1 - q^{1/2}\sum_\alpha 2cos(\phi_\alpha).$$

If $f(\theta) \geq 0$ for all θ and $c_n \geq 0$ for all n, we say that f is doubly positive and we write $f >> 0$.

If $f >> 0$, then $N - 1 \leq \frac{g+\Psi(q^{1/2})}{\Psi(q^{-1/2})}$, or equivalently

$$g \geq (N-1)\Psi(q^{-1/2}) - \Psi(q^{1/2}).$$

Example 1.2. *For $N = q^2 + 1$, we get with $f = 1 + \sqrt{2}cos(\theta) + \frac{1}{2}cos(2\theta)$ that*

$$g \geq \frac{\sqrt{2}}{2}(q^{3/2} - q^{1/2}).$$

2 The Drinfield-Vladut bound

We denote $A^+(q) = \lim\sup_{g\to\infty} \frac{N_q(g)}{g}$.

Theorem 2.1. *(Drinfield-Vladut) One has $A^+(q) \leq q^{1/2} - 1$.*

Theorem 2.2. *(Ihara, Zink) If q is a square, then $A^+(q) \geq q^{1/2} - 1$.*

Theorem 2.3. *(Elkies, Howe, Kresch, Poonen, Wetherell, Zieve, 2002) For all prime power q, there is a positive constant c_q with the following property: for every integer $g \geq 0$, there is a genus g curve over $\mathbb{F}_q$ with at least $c_q g$ rational points. Moreover, there is a constant $c > 0$ such that for every q, and for every sufficiently large g, there is a genus g curve over $\mathbb{F}_q$ that has at least cg rational points.*

3 Exercises

Exercise 3.1. *Finish the argument in example 0.1.*

Exercise 3.2. *Prove the equality 1.*

Exercise 3.3. *Check the statement in example 1.1.*

Exercise 3.4. *Check the statement in example 1.2.*

References

[1] F.Q. Gouvêa, *Rational Points on Curves over Finite Fields*, Lecture notes given at Havard University by J.-P. Serre in Fall 1985.