The Riemann hypothesis over Finite Fields. Lecture 2.

Elisa Lorenzo García

8th February 2016

Contents

1 The Riemann hypothesis over finite fields **1**

2 The Hasse-Weil bound **3**

3 A proof of the RH for finite fields **4**

4 Exercises **6**

André Weil proves in the 40's the Riemann hypothesis for curves over finite fields. Schmidt had already proved the Racionality and the functional equation for the Zeta function, and Hasse had proved the genus 1 case. After that, Weil states the so-called Weil conjectures, that it is the natural generalization for curves. Dwork proves the racionality, Grothendieck the functional equation, and Deligne finally proves the "Riemann hypothesis" in 1976. In this lecture, we will discuss the main ideas in Weil proof and we will see the simplified Stepanov proof by Bombieri of the Riemann hypothesis for curves over finite fields. The main reference is [1].

1 The Riemann hypothesis over finite fields

The simplest statement of the RH for finite fields is

Theorem 1.1. *Let $f \in \mathbb{Z}[X,Y]$ an irreducible polynomial. let us denote by $N_p(f)$ the number of solutions $f(X,Y) \equiv 0$ mod p. Then, there exist a constant A, only depending on f such that*

$$| N_p(f) - p | \leq A\sqrt{p}.$$

Corollary 1.2. *If $p \geq A^2$, then there always exists a solution modulo p.*

Once we know the concept of genus of a curve, we can express it in a more precise way.

Theorem 1.3 (Riemann hypothesis for finite fields)**.** *Let C be a genus g smooth, irreducible, projective curve over a finite field $\mathbb{F}_q$. There exist algebraic integers (roots of monic olynomials with integer coefficients) $\alpha_1, ..., \alpha_{2g}$ of norm $\mid \alpha_i \mid = \sqrt{q}$ such that, for all $m \geq 1$,*

$$\#C(\mathbb{F}_{q^m}) = q^m + 1 - (\alpha_1^m + ... + \alpha_{2g}^m).$$

Therefore, $\mid \#C(\mathbb{F}_{q^m}) - q^m - 1 \mid \leq 2gq^{m/2}$.

We can reinterpret this, as saying that the number of points of a curve over $\mathbb{F}_q$ is close to the number of points of the projective line $\mathbb{P}^1/\mathbb{F}_q$ ($g(\mathbb{P}^1) = 0$, and $\#\mathbb{P}^1(\mathbb{F}_q)$=1+q). So, we can reinterpret this number as a bound for the error of the number of points to be equal to the number of points of the projective line.

Definition 1.4 (Riemann Zeta function)**.** *The Riemann Zeta function is defined, for Re $s > 1$, by the Dirichlet series (that has an Euler product)*

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

Definition 1.5. *We define the Euler Gamma function, for Re $s > 1$, as*

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt,$$

that can be extended to all $\mathbb{C}$ via the identity $\Gamma(s+1) = s\Gamma(s)$.

Theorem 1.6 (Riemann)**.**

1. *(Analitical continuation) The function $\zeta(s)$ can be extended to a meromorphic function in the whole complex plane. It only has a simple pole at $s = 1$ with residue equal to 1.*

2. *(Functional equation) We define the complete Zeta function by $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, then*
$$\xi(1-s) = \xi(s).$$

Conjecture 1.7 (Riemann hypothesis)**.** *The zeros of the function $\xi(s)$ lie over the critical line Re $s = 1/2$.*

For the analogy for finite fields, we define the Zeta function

$$\zeta_C(s) = \prod_{x \in C} (1 - \mathrm{N}(x)^s)^{-1},$$

where the ring of coordinates $k[C] = \mathbb{F}_q[C]$ replaces the ring $\mathbb{Z}$, and the points in the curve replace the prime numbers in $\mathbb{Z}$. The norm of a prime number is the cardinality of the residue field $\mathbb{Z}/p\mathbb{Z}$ that it is equal to p. While the norm of a point in a curve, is the cardinality of the residue field $k[C]/k[C]_p$.

An alternative definition is the next one, $\zeta_C(s) = Z(C, q^{-s})$, where

$$Z(C/\mathbb{F}_q, T) = \exp(\sum_{m=1}^{\infty} \frac{\#C(\mathbb{F}_{q^m})}{m} T^m). \tag{1}$$

For genus 1 curves, Hasse proved that the Zeta function look like

$$Z(C/\mathbb{F}_q, T) = \frac{1 - aq + qT^2}{(1-T)(1-qT)}, \tag{2}$$

where $\mid a \mid \leq 2\sqrt{q}$ and $\#C(\mathbb{F}_q) = q+1-a$. This implies that $\#C(\mathbb{F}_q) \geq q+1-2\sqrt{q} = (\sqrt{q}-1)^2 > 0$, so genus 1 curves, that is, elliptic curves, always have at least one point.

We know now all the concepts needed to formulate the Riemann hypothesis for finite fields.

Theorem 1.8. *[Weil] Let C be a genus g smooth projective curve defined over a finite field $\mathbb{F}_q$. There exist algebraic integers $\alpha_1, ..., \alpha_{2g}$ such that*

1. *(Rationality) $Z(C/\mathbb{F}_q, T) = \frac{(1-\alpha_1 T)...(1-\alpha_{2g} T)}{(1-T)(1-qT)} \in \mathbb{F}_q(T)$,*
2. *(Functional equation) The Zeta function satisfies*

$$Z(C/\mathbb{F}_q, T) = q^{g-1} T^{2g-2} Z(C/\mathbb{F}_q, \frac{1}{qT}).$$

3. *(Riemann hypothesis) the algebraic integer α_i have norm $\mid \alpha_i \mid = q^{1/2}$, that is, all the zeros of the zeta function lie over the critical line Re $s = 1/2$.*

2 The Hasse-Weil bound

From the RH, we deduce that

$$\mid \#C(\mathbb{F}_q) - (q+1) \mid \leq \lfloor 2gq^{1/2} \rfloor.$$

In 1983, J.P. Serre improves this equality, when q is a square, by

$$\mid \#C(\mathbb{F}_q) - (q+1) \mid \leq g\lfloor 2q^{1/2} \rfloor.$$

Lemma 2.1. *Let $S = \alpha_1, ..., \alpha_s$ be a set of algebraic integers stable by the action of the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, and such that $\mid \alpha_i \mid = p^{\omega/2}$ for an odd ω. Then, s is an even number and*

$$\mid \alpha_1 + ... + \alpha_s \mid \leq \frac{s}{2} \lfloor 2p^{\omega/2} \rfloor.$$

Proof. If α_i is a real number, then $\alpha_i = \pm p^{\omega/2}$ and $-\alpha_i$ is its conjugate and it is also in S. The other elements can be pair up with their complex conjugates, so $s = 2t$ is even. Since $p^{\omega/2} - p^{\omega/2} = 0$, we can assume that there are not real elements and we write $S = T \cup \overline{T}$ with $T = \alpha_1, ..., \alpha_t$. Let us define $m = \lfloor 2p^{\omega/2} \rfloor$ and $x_i = m + 1 + \alpha_i + \overline{\alpha}_i$. The x_i are real positive algebraic integers and they are stable by the Galois actions. Hence, the product $x_1 ... x_t \geq 1$ is a positive integer. The arithmetic-geometric means equality implies

$$\frac{1}{t}\sum_{i=1}^{t} x_i \geq \sqrt[t]{x_1 ... x_t} \geq 1,$$

which implies $tm + \sum_{i=1}^{s} \alpha_i \geq 0$. By replacing α_i by $-\alpha_i$, we get the other inequality. □

Definition 2.2. *We say that a genus g curve $C/\mathbb{F}_q$ is maximal if*

$$\#C(\mathbb{F}_q) = \max_{C' \text{ genus } g} \{\#C'(\mathbb{F}_q)\}.$$

3 A proof of the RH for finite fields

Weil's proof of the Riemann hypothesis for curves uses Riemann-Roch Theorem and Bezout's Theorem about intersections of curves, the proof can be found in [1]. Instead of that proof, we will show here a simplified verion of Stepanov's proof by Bombieri.

We will assume the racionality and the functional equation part in Theorem 1.8 due to Schmidt, see 1.2.3 in [2] for a proof.

Notice that if $C/\mathbb{F}_q$ has associated numbers $\beta_1, ..., \beta_{2g}$, then extension of scalars $C/\mathbb{F}_{q^r}$ has numbers $\beta_i' = \beta_i^r$ and $\mid \beta_i' \mid = q^{r/2}$ is equivalent to $\mid \beta_i \mid = \sqrt{q}$. So, we can replace $\mathbb{F}_q$ by $\mathbb{F}_{q^r}$ and assume that q is enough large.

Proposition 3.1. *Assume that q is a square and $q > (g+1)^4$, then*

$$\#C(\mathbb{F}_q) \leqq +1 + (2g+1)\sqrt{q}.$$

Proof. Denote by $N := \#C(\mathbb{F}_q)$ and $q = q_0^2$. We can assume that there exist $Q \in C(\mathbb{F}_q)$. The idea will be constructing a function with a single pole of order less or equal than H at Q and vanishing with order T at each point in $C(\mathbb{F}_q)/\{Q\}$. Hence, $T(N-1) \leq H$, that is, $N \leq 1 + H/T$.

Let us take two parameters $m, n \geq 1$, and let us define

$$T := \{i \in [0, m] \mid \exists u_i \text{ s.t. } \operatorname{div}(u_i)_\infty = iQ\},$$

for each i, we fix a function u_i. We will need some lemmas. □

Lemma 3.2. *The set $\{u_i : i \in T\}$ is a basis for $\mathcal{L}(mQ)$. In particular, $\#T = \ell(mQ)$.*

Proof. Riemann-Roch Theorem implies

$$(\ell((i+1)Q) - \ell(iQ)) + (\ell(K_C - (iQ)) - \ell(K_C - ((i+1)Q))) = 1.$$

□

We define $\mathcal{L} := \mathcal{L}(mQ) \cdot \mathcal{L}(nQ)^{q_0}$.

Lemma 3.3. *The vector space $\mathcal{L}$ is a subvector space of $\mathcal{L}((m+nq_0)Q)$. Moreover, if $m < q_0$, $dim(\mathcal{L}) = \#T \cdot \ell(nQ) = \ell(mQ) \cdot \ell(nQ)$.*

Proof. .... □

We now define the map

$$\begin{array}{rcl} \Phi : \mathcal{L} & \to & \mathcal{L}((q_0 m + n)Q) \\ \sum_{i \in T} u_i z_i^{q_0} & \to & \sum_{i \in T} u_i^{q_0} z_i. \end{array}$$

Lemma 3.4. *One has:*

1. *$\Phi(x+y) = \Phi(x) + \Phi(y)$ and $\Phi(\lambda^{q_0} x) = \lambda \Phi(x)$*
2. *Put $m = q_0 - \epsilon$ and $n = q_0 + \gamma$, and assume*

$$q_0 > \frac{(\gamma + 1 - g)(g + \epsilon)}{\gamma + 1 - 2g}.$$

Then the kernel of Φ is not trivial.

Proof. ... □

We take now $\epsilon = 1$, and $\gamma = 2g$, so inequality below becomes $q_0 > (g+1)^2$.

Lemma 3.5. *Let x be a non-zero function in Ker Φ, then, for all $P \in C(\mathbb{F}_q)/\{Q\}$, one has $x(P) = 0$.*

Proof. ... □

Proof. (Continuation of proposition 3.1 proof) We obtain

$$\#(C(\mathbb{F}_q)/\{Q\}) \leq \deg \operatorname{div}(x)_0 = \deg \operatorname{div}(x)_\infty \leq m + nq_0,$$

from where, we deduce

$$\#(C(\mathbb{F}_q)) \leq q_0 - \epsilon + q_0(q_0 + \gamma) + 1 = q + 1 + (2g+1)\sqrt{q}.$$

□

We refer the readers to pages 91 and 92 in [1] for the end of this proof of the RH for curves over finite fields.

4 Exercises

Exercise 4.1. *Compute the Zeta function $Z(C/\mathbb{F}_q, T)$ for $C = \mathbb{P}^1$ by using formula 1, and check that the functional equation holds.*

Exercise 4.2. *List all the elliptic curves*[1] *over $\mathbb{F}_q$ up to isomorphism for $q = 2, 3, 4, 5$. Compute the number of points over $\mathbb{F}_q$ for each of the elliptic curves in your list. Compare these values with the bounds explained in this lecture.*

Exercise 4.3. *Compute the Zeta function $Z(C/\mathbb{F}_q, T)$ of the elliptic curve $x^3 + y^3 + z^3 = 0$, for $q \equiv 2 \mod 3$ and for $q = 7$ and check the functional equation. Use Hasse result 2.*

Exercise 4.4. *Compute the Zeta function $Z(C/\mathbb{F}_q, T)$ of the Klein quartic*[2] $x^3y+y^3z+z^3x = 0$ *over the finite field $\mathbb{F}_2$. Is it a maximal curve?*

Exercise 4.5. *Complete the proofs of Lemmas 3.3, 3.4 and 3.5.*

References

[1] M. Hindry, *La preuve par André Weil de l'hypothése de Riemann pour une courbe sur un corps fini*, Henri Cartan & André Weil, mathématiciens du XXe siècle, 63-98, Ed. Éc. Polytech., Palaiseau, 2012.

[2] C. Ritzenthaler, *Curves over finite fields*, notes of a course taught at Universitat Politècnica de Catalunya, 2005.

[1] An elliptic curve is always given by an equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Two elliptic curves are isomorphic if and olny if they have the same $j - invariant$. To define the j–invariant, we need first to define other numbers: $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$, $c_4 = b_2^2 - 24b_4$, $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ and we can finally define $j = \frac{c_4^3}{\Delta}$.

[2] Use exercise 3.6 in the lectures notes 1 of this course to compute the genus of the Klein quartic