A Weil theorem for singular curves

Yves Aubry and Marc Perret

Abstract. We generalize Weil's theorem on the number of rational points of smooth curves over a finite field to singular ones.

1991 Mathematics Subject Classification: 14G10, 14H20.

1. Introduction

Throughout this paper a *curve* stands for a reduced absolutely irreducible projective algebraic curve defined over the finite field $\mathbb{F}_q$ with q elements. André Weil [6] proved that the number $\sharp X(\mathbb{F}_q)$ of rational points over $\mathbb{F}_q$ of any smooth curve X satisfies

$$| \sharp X(\mathbb{F}_q) - (q+1) | \leq 2g\sqrt{q}$$

where g is the genus of X. Moreover, the zeta function Z_X of X is a rational function $\frac{P_X(T)}{(1-T)(1-qT)}$ where $P_X(T)$ is a polynomial of degree $2g$, with integer coefficients and whose inverse roots have modulus $\sqrt{q}$ (this is the so called "Riemann Hypothesis").

In this paper, we first give an explicit form of the zeta function of any singular curve X. We know by Dwork's theorem that it is a rational function. Here again, we show that $Z_X(T) = \frac{P_X(T)}{(1-T)(1-qT)}$, where $P_X(T)$ is a polynomial with integer coefficients which is the product of the numerator of the zeta function of the normalization $\tilde{X}$ of X with an explicit product of cyclotomic polynomials.

Then, the study of the difference between the number of rational points of $\tilde{X}$ and of X will enable us to show that the Weil inequality still holds for X, provided that we replace the geometric genus g of X by its arithmetic genus π (in fact, we give a better estimate).

Finally, we give some applications to permutation polynomials and explicit formulas.

Offprint from: Arithmetic, Geometry and Coding Theory, Eds.: Pellikaan/Perret/Vlăduţ

2. The zeta function of a singular curve

The zeta function

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

of a curve X can be written as

$$Z_X(T) = \frac{\det(1 - TF \mid \mathrm{H}^1_c(X, \mathbb{Q}_\ell))}{(1-T)(1-qT)},$$

where F is the Frobenius morphism on the first ℓ-adic cohomology group with compact support $\mathrm{H}^1_c(X, \mathbb{Q}_\ell)$ of X, and the eigenvalues of the Frobenius have modulus $\sqrt{q}$ or 1 (see [1]). The purpose of this section is to give a more precise statement, using only elementary methods.

We denote by $\tilde{X}$ the normalization of X and by $\nu : \tilde{X} \longrightarrow X$ the normalization map. If P is a point, we denote by $d_P = [\mathbb{F}_q(P) : \mathbb{F}_q]$ its degree over $\mathbb{F}_q$ (i.e. the degree of the extension of the residue field of P over $\mathbb{F}_q$).

Theorem 2.1. *Let S be the (finite) set of singular points of X. Then*

$$Z_X(T) = \frac{P_X(T)}{(1-T)(1-qT)}$$

where

$$P_X(T) = P_{\tilde{X}}(T) \prod_{P \in S} \left(\frac{\prod_{Q \in \nu^{-1}(P)} (1 - T^{d_Q})}{1 - T^{d_P}} \right),$$

and where $P_{\tilde{X}}$ is the numerator of the zeta function $Z_{\tilde{X}}$ of $\tilde{X}$.

Proof. We have

$$\begin{aligned}\frac{Z_X(T)}{Z_{\tilde{X}}(T)} &= \exp\left(-\sum_{n=1}^{\infty} (\sharp \tilde{X}(\mathbb{F}_{q^n}) - \sharp X(\mathbb{F}_{q^n}))\frac{T^n}{n}\right) \\ &= \prod_{P \in S} \exp\left(-\sum_{n=1}^{\infty} (\alpha_P(n) - d_P)\delta_{d_P|n}\frac{T^n}{n}\right),\end{aligned}$$

where $\delta_{m|n} = 1$ if $m \mid n$, else $\delta_{m|n} = 0$, and where $\alpha_P(n)$ is the number of points of $\tilde{X}$ lying over P, that are rational over $\mathbb{F}_{q^n}$.

Thus,

$$\frac{Z_X(T)}{Z_{\tilde{X}}(T)} = \prod_{P \in S} \exp\left(-\sum_{m=1}^{\infty} (\alpha_P(md_P) - d_P)\frac{T^{md_P}}{md_P}\right).$$

But

$$\alpha_P(md_P) = \sum_{Q \in \nu^{-1}(P)} d_Q \delta_{d_Q|md_P},$$

hence

$$\frac{Z_X(T)}{Z_{\tilde{X}}(T)} = \prod_{P\in S}\left(\frac{\prod_{Q\in\nu^{-1}(P)}\exp\left(-\sum_{m=1}^{\infty} d_Q\delta_{d_Q|md_P}\frac{T^{md_p}}{md_p}\right)}{1-T^{d_P}}\right)$$

$$= \prod_{P\in S}\left(\frac{\prod_{Q\in\nu^{-1}(P)}\exp\left(-\sum_{\ell=1}^{\infty}\frac{T^{\ell d_Q}}{\ell}\right)}{1-T^{d_P}}\right)$$

$$= \prod_{P\in S}\left(\frac{\prod_{Q\in\nu^{-1}(P)}(1-T^{d_Q})}{1-T^{d_P}}\right)$$

and the theorem is proved. □

The zeta function of X is thus the product of a polynomial of degree $2g_X$ by a polynomial of degree

$$\Delta_X = \sharp\{\tilde{X}(\overline{\mathbb{F}}_q) \setminus X(\overline{\mathbb{F}}_q)\},$$

where $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. Note that the quantity Δ_X is well-defined, since the set of singular points is a finite subset of X. We now have to evaluate Δ_X (which can be seen as the dimension of the toric component of the generalized Jacobian of X (see [4])).

As in the proof of Theorem 2.1, if $P \in X(\overline{\mathbb{F}}_q)$ let $\alpha_P(1) = \alpha$ (respectively $\alpha_P(\infty)$) be the number of rational points over $\mathbb{F}_q$ (respectively over $\overline{\mathbb{F}}_q$) of $\tilde{X}$, lying over P. Let $\mathcal{O}_P$ be the local ring of P on X and $\overline{\mathcal{O}_P}$ its integral closure in the function field $\mathbb{F}_q(X)$ of the curve X. The quotient $\overline{\mathcal{O}_P}/\mathcal{O}_P$ is a finite dimensional $\mathbb{F}_q$-vector space whose dimension is denoted by δ_P.

We get the following lemma.

Lemma 2.2. *Let P be an $\mathbb{F}_q$-rational point of X. Then*

$$\alpha_P(1) - 1 \leq \delta_P.$$

Proof. Let $Q_1, \ldots, Q_{\alpha_P(\infty)}$ be the points of $\tilde{X}(\overline{\mathbb{F}}_q)$ lying over P (where the first α points are the $\mathbb{F}_q$-rational ones), and ϕ the linear map of $\mathbb{F}_q$-vector spaces

$$\begin{array}{rccc} \phi : & \overline{\mathcal{O}_P} & \longrightarrow & {\mathbb{F}_q}^{\alpha} \\ & f & \longmapsto & (f(Q_i))_{1\leq i\leq\alpha} \end{array}$$

Let us show that ϕ is surjective. Let $(x_1, \ldots, x_\alpha) \in {\mathbb{F}_q}^{\alpha}$ and $f_i = x_i \in \mathbb{F}_q \subset \mathbb{F}_q(X)$ for $i \leq \alpha$. For $i \geq \alpha + 1$, we set $f_i = 0$. By the weak approximation theorem, there exists $g \in \mathbb{F}_q(X)$ such that $v_{Q_i}(g - f_i) \geq 1$ for $1 \leq i \leq \alpha_P(\infty)$. Hence, $\phi(g) = (x_1, \ldots, x_\alpha)$ and

$$g \in \bigcap_{1\leq i\leq\alpha_P(\infty)} \mathcal{O}_{Q_i} = \overline{\mathcal{O}_P}.$$

Since $f(Q_1) = \cdots = f(Q_\alpha)$ for $f \in \mathcal{O}_P$, we have that $\phi(\mathcal{O}_P)$ is contained in a one dimensional vector space $L \subset {\mathbb{F}_q}^\alpha$. We obtain a surjective linear map

$$\tilde{\phi} : \tilde{\mathcal{O}}_P/\mathcal{O}_P \longrightarrow {\mathbb{F}_q}^\alpha/L,$$

and the lemma is proved. □

Proposition 2.3.

$$|\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g.$$

Proof. Let P be a point of X and Q be a point of $\tilde{X}$ lying over P. Then P is rational over $\mathbb{F}_q$ if Q is. With the previous notations, we get by Lemma 2.2

$$\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) = \sum_{P \in \mathrm{Sing}\, X(\mathbb{F}_q)} (\alpha_P(1) - 1) \leq \sum_{P \in \mathrm{Sing}\, X(\mathbb{F}_q)} \delta_P \leq \pi - g$$

since

$$\pi - g = \sum_{P \in \mathrm{Sing}\, X(\overline{\mathbb{F}}_q)} \delta_P.$$

On the other hand,

$$\sum_{P \in \mathrm{Sing}\, X(\mathbb{F}_q)} (\alpha_P(1) - 1) \geq -\sharp \mathrm{Sing}\, X(\mathbb{F}_q) \geq -\sharp \mathrm{Sing}\, X(\overline{\mathbb{F}}_q) \geq -(\pi - g),$$

which concludes the proof. □

Thus, the numerator of the zeta function of X is a polynomial with integer coefficients of degree $2g + \Delta_X \in \{2g, \ldots, \pi + g\}$, where $\Delta_X = \sharp\{\tilde{X}(\overline{\mathbb{F}}_q) \setminus X(\overline{\mathbb{F}}_q)\}$, whose inverse roots have either modulus $\sqrt{q}$ (for $2g$ of them) or modulus 1 (for Δ_X of them).

Corollary 2.4. *Let $\omega_1, \ldots, \omega_{2g}$ be the inverse roots of $P_{\tilde{X}}$, and $\beta_1, \ldots, \beta_{\Delta_X}$ be the inverse roots of the cyclotomic part of P_X. Then, for all $n \geq 1$,*

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n - \sum_{j=1}^{\Delta_X} \beta_j^n.$$

In particular,

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q} + \Delta_X \leq 2g\sqrt{q} + \pi - g \leq 2\pi\sqrt{q},$$

and

$$\dim_{\mathbb{Q}_\ell} \mathrm{H}^1_c(X, \mathbb{Q}_\ell) = 2g + \Delta_X. \qquad \square$$

Using the last inequality, we get:

Corollary 2.5. *If X is an absolutely irreducible curve which is a complete intersection in $\mathbb{P}^{n+1}$ of n hypersurfaces of degree $d_1, \ldots, d_n$, and if we set $d = \prod_{i=1}^{n} d_i$, then:*

$$|\, \sharp X(\mathbb{F}_q) - (q+1) \,| \leq (d-1)(d-2)\sqrt{q}.$$

In particular, this inequality holds for any absolutely irreducible plane curve of degree d.

Proof. The arithmetic genus π_X of a complete intersection which is given by $2\pi_X = d(\sum_{i=1}^{n} d_i - n - 2) + 2$ (see [5 p.73]) is clearly at most equal to $(d-1)(d-2)$. The second assertion is obviously a particular case of the first one. Observe that the arithmetic genus of a plane curve of degree d is equal to $\frac{(d-1)(d-2)}{2}$. □

3. Applications

3.1. Explicit formulas

The explicit formulas given by J.-P. Serre in [5] related to the function field of a curve over a finite field still hold in the singular case, provided that we replace the geometric genus g of the curve by its arithmetic genus π. Furthermore, we can replace (and it is better) g by $g + \frac{\Delta_X}{2}$.

Consider a function $f(\theta) = 1 + 2\sum_{n\geq 1} c_n \cos n\theta$ which satisfies $f >> 0$ (i.e. $f(\theta) \geq 0$ for all $\theta \in \mathbb{R}$ and $c_n \geq 0$ for all $n \geq 1$). The formula of Corollary 2.4 gives $\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n - \sum_{j=1}^{\Delta_X} \beta_j^n$. Arguing as in [5], we get

$$\sharp X(\mathbb{F}_q) \leq a_f(g + \frac{\Delta_X}{2}) + b_f \leq a_f \pi + b_f \qquad (*)$$

with $a_f = 1/\Psi(q^{-1/2})$ and $b_f = 1 + \left(\Psi(q^{1/2})/\Psi(q^{-1/2})\right)$, where $\Psi(t) = \sum_{n\geq 1} c_n t^n$.

Furthermore, we obtain the same estimations as the ones in [5] of the maximum number of rational points over $\mathbb{F}_2$ of a curve for $g + \frac{\Delta}{2}$ fixed. For example, a curve with $g + \frac{\Delta}{2} \leq 6$ has at most 10 rational points. These remarks have been communicated to the authors by J.-P. Serre.

Another application of this results is the following one. Consider the number

$$N_q(\pi) = \max_X \sharp X(\mathbb{F}_q)$$

where X runs over the curves (possibly singular!) over $\mathbb{F}_q$ of arithmetic genus π. It is of interest to study the behavior of $N_q(\pi)$ for $\pi \longrightarrow \infty$. We define, in analogy with the quantity $A(q)$ (see [5] for example), the number $A'(q)$ by

$$A'(q) = \limsup_{\pi\to\infty} \frac{N_q(\pi)}{\pi}.$$

Corollary 2.5 readily implies $A'(q) \leq 2\sqrt{q}$. In fact, using the previous explicit formulas we get the following bound which is the same as that for $A(q)$ of Drinfeld and Vlăduţ (see [2]). Note that we obviously have $A(q) \leq A'(q)$.

Proposition 3.1.
$$A'(q) \leq \sqrt{q} - 1.$$

Proof. Take
$$f_m(\theta) = 1 + 2\sum_{n=1}^{m}(1 - \frac{n}{m}) \cos n\theta = \frac{1}{m}|\sum_{k=1}^{m} e^{ik\theta}|^2.$$

Thus $f_m \gg 0$. Now, let
$$\Psi_m(t) = \sum_{n=1}^{m}(1 - \frac{n}{m})t^n.$$

Thus, $(*)$ gives
$$\frac{\sharp X(\mathbb{F}_q)}{\pi} \leq 1/\Psi_m(q^{-1/2}) + \frac{1}{\pi}\Big(1 + \big(\Psi_m(q^{1/2})/\Psi_m(q^{-1/2})\big)\Big)$$
Since $\Psi_m(t) \to t/(1-t)$ for $m \to \infty$ and $|t| < 1$, we get
$$\Psi_m(q^{-1/2}) \to 1/(\sqrt{q} - 1) \quad \text{for } m \to \infty.$$

Hence, for any ϵ there exists m_0 such that $m \geq m_0$ implies
$$1/\Psi_m(q^{-1/2}) < \sqrt{q} - 1 + \frac{\epsilon}{2}.$$

For π large enough, the second term of the right hand side of the inequality is less than $\frac{\epsilon}{2}$, and this concludes the proof. □

3.2. Permutation polynomials and exceptional polynomials

Corollary 2.5 gives us the following explicit form of the Lemma 7.28 of [3]. This result enables us to precise the relationship between permutation polynomials and exceptional polynomials over $\mathbb{F}_q$ (see [3]).

Lemma 3.2. *Let $\phi \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomial of degree d and C_ϕ the affine curve of equation $\phi(x, y) = 0$. Set*
$$k_d = \frac{1}{4}\Big((d-1)(d-2) + \sqrt{d^2 + 5d - 2}\Big)^2.$$

If $q \geq k_d$, then either C_ϕ has a rational point (a, b) with $a \neq b$ or ϕ is of the form $c(x - y)$ for some $c \in \mathbb{F}_q$.

Proof. According to the affine version of Corollary 2.5, the number N of rational points over $\mathbb{F}_q$ of the (affine) curve C_ϕ satisfies

$$| N - q | \leq (d-1)(d-2)\sqrt{q} + d - 1.$$

Arguing as in the proof of Lemma 7.28 of [3], the result holds with any k_d such that $q - (d-1)(d-2)\sqrt{q} - 2d + 1 > 0$ for all $q \geq k_d$. □

Hence, this gives explicit forms for the Propositions 7.29 until 7.33 of [3]. For example, any permutation polynomial of degree 2 is exceptional over $\mathbb{F}_q$ if q is odd.

References

[1] Deligne, P., La conjecture de Weil. II. Publ. Math. IHES **52** (1980), 137–252.

[2] Drinfeld, V.G., S.G. Vlăduţ, Sur le nombre de points d'une courbe algébrique. Anal. Fonct. Appl. **17** (1983), 68–69.

[3] Lidl, R., H. Niederreiter, Finite fields. Encyclopedia Math. Appl. **20**, Addison-Wesley, Reading 1982.

[4] Serre, J.-P., Groupes algébriques et corps de classes. Hermann, Paris 1959.

[5] Serre, J.-P., Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini. C. R. Acad. Sci. Paris **296** Série I, (1983), 397–402.

[6] Weil, A., Sur les courbes algébriques et les variétés qui s'en déduisent. Hermann, Paris 1948.