Dwork's theorem on the zeta-functions of affine hypersurfaces
Directed studies II

András Földesi
Advisor: Dr. Ambrus Pál

2026

Chapter 1

Introduction

Following the results of the previous term, the goal of this work is to highlight the main steps in Bernard Dwork's proof of the rationality of the zeta-functions of affine hypersurfaces over finite fields.

Definition 1.0.1. Let X be a non-singular affine hypersurface defined by the polynomial f in n variables with coefficients in $\mathbb{F}_q$. Define

$$H_f(k) = \{(x_1, ..., x_n) \in k^n : f(x_1, ..., x_n) = 0\},$$

for a finite field k, and let N_s be the number of points in $H_f(\mathbb{F}_{q^s})$. With these notations the zeta-function of X is:

$$\zeta(X/F_q, t) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{t^s}{s}\right).$$

The zeta function of projective hypersurfaces can be defined in a similar fashion using as N_s the number of points lying on the projective hypersurface over $\mathbb{F}_{q^s}$.

Theorem 1.0.2 (Dwork)**.** *The zeta-function of any affine (or projective) hypersurface is a rational function.*

What interests us is the affine case, because using the decomposition of the projective space into disjoint affine spaces (with decreasing dimension), it is easy to see that the case of projective hypersurfaces follows from the case of affine ones. It is also true that the rationality of the zeta function of affine varieties defined in a similar fashion easily follows from this case.

Chapter 2

The rationality of the zeta-function

2.1 Characters and their lifting

We will work with multiplicative $\mathbb{C}_p$ valued $\mathbb{F}_q \to \mathbb{C}_p^\times$ characters, where on $\mathbb{F}_p$ we take the additive and on $\mathbb{C}_p^\times$ the multiplicative group structure.

Definition 2.1.1. The trace of an element $a \in \mathbb{F}_q$ for $q = p^s$ is the trace of the linear map over $\mathbb{F}_p$ defined by the multiplication by a. Equivalently this means:

$$\operatorname{Tr} a = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \sigma(a) = a + a^p + ... + a^{p^{s-1}}.$$

From the definition it follows that $(\operatorname{Tr} a)^p = \operatorname{Tr} a$, i.e., $\operatorname{Tr} a \in \mathbb{F}_p$, and $\operatorname{Tr}(a+b) = \operatorname{Tr} a + \operatorname{Tr} b$. Now let $\varepsilon \in \mathbb{C}_p$ be a pth root of unity, then the map

$$a \mapsto \varepsilon^{\operatorname{Tr} a}$$

is a multiplicative $\mathbb{C}_p$ valued character.

Similarly to the trace of an element of the field extension $[\mathbb{F}_q : \mathbb{F}_p]$ we define the trace of an element of the field extension $[\mathbb{Q}_q : \mathbb{Q}_p]$ (denote this as $\operatorname{Tr}_{\mathbb{Q}_q}$) via the trace of a linear map. It can be easily seen that for the Teichmüller representative $t \in \mathbb{Q}_q$ of an arbitrary $a \in \mathbb{F}_q^\times$:

$$\operatorname{Tr}_{\mathbb{Q}_q} t = t + t^p + ... + t^{p^{s-1}} \in \mathbb{Z}_p,$$

and the mod p reduction of $\operatorname{Tr}_{\mathbb{Q}_q} t$ is $\operatorname{Tr} a$. Hence $\varepsilon^{\operatorname{Tr} a} = \varepsilon^{\operatorname{Tr}_{\mathbb{Q}_q} t}$, since the power of ε depends only on the congruence class mod p.

Now to express this character as a power series, the naive thing to do would be:

$$\varepsilon^{x+x^p+...+x^{p^{s-1}}} = B_{x,p}(\varepsilon - 1)B_{x^p,p}(\varepsilon - 1)...B_{x^{p^{s-1}},p}(\varepsilon - 1),$$

where $B_{a,p}(x)$ is the (p-adic) binomial expansion, but the binomial expansion does not converge on the whole closed unit disk, and this causes problems in the Teichmüller representatives, which are unit roots.

To avoid this issue, define the following infinite product:

$$F(x,y) = (1+y)^x (1+y^p)^{(x^p-x)/p} (1+y^{p^2})^{(x^{p^2}-x^p)/p^2} ... (1+y^{p^n})^{(x^{p^n}-x^{p^{n-1}})/p^n} ...,$$

for fixed y this can be expressed as a power series in x that is convergent in the closed unit disk (F is constructed in a way to eliminate the coeffiecients that caused the problem in the binomial expansion due to de p-adic norm).

Let

$$\Theta(x) = F(x, \varepsilon - 1) = \sum_{n=1}^{\infty} a_n x^n.$$

Now it is easy to see that

$$\varepsilon^{\operatorname{Tr} a} = \varepsilon^{\operatorname{Tr}_{\mathbb{Q}_q} t} = \Theta(t)\Theta(t^p)...\Theta(t^{p^{s-1}}).$$

2.2 The trace formula

Let R denote the set of formal power series over $\mathbb{C}_p$ in n variables, and U the set of ordered n-tuples of nonnegative integers.

Define the following two ($\mathbb{C}_p$-)linear transformations on R:

$$L_G(r) = Gr, \text{ where } G \in R,$$

$$r = \sum_{u \in U} a_u x^u \mapsto T_q(r) = \sum_{u \in U} a_{qu} x^u, \text{ where } q \in \mathbb{Z}^+.$$

Then let $\Psi_{q,G} = T_q \circ L_G$. For a monomial x^u, and $G = \sum_{w \in U} g_w x^w$:

$$\Psi_{q,G}(x^u) = \sum_{v, qv-u \in U} g_{qv-u} x^v.$$

Denote the power series $G(x^q)$ as $G_q(x)$, then the following relation holds:

$$L_G \circ T_q = T_q \circ L_{G_q}.$$

Let

$$R_0 = \left\{ G = \sum_{w \in U} g_w x^w \in R : \exists M > 0, \quad \mathrm{ord}_p g_w \geq M|w| \quad \forall w \in U \right\}.$$

Definition 2.2.1. For an infinite matrix A define the trace of A as the sum of its diagonal elements provided that this sum converges, similarly to the finite case.

The following lemma provides the core of Dwork's proof.

Lemma 2.2.2. *Let $G \in R_0$. Then $\mathrm{Tr}\,(\Psi^s_{q,G})$ converges for $s \in \mathbb{Z}^+$, and*

$$(q^s - 1)^n \mathrm{Tr}\,(\Psi^s_{q,G}) = \sum_{\substack{x \in \mathbb{C}_p^n x \\ x^{q^s-1}=1}} G(x)G(x^q)...G(x^{q^s-1}).$$

We can also extend the notion of $\det(1 - At)$, where t is an indeterminate, to infinite A matrices in the following way:

$$\det(1 - At) = \sum_{m=0}^{\infty} b_m t^m,$$

where

$$b_m = (-1)^m \sum_{\substack{u_1 < ... < u_m \in \mathbb{Z}^+ \\ \sigma \in S_m}} \mathrm{sgn}(\sigma) a_{u_1, u_{\sigma(1)}} ... a_{u_m, u_{\sigma(m)}}.$$

Naturally, the convergence of each b_m has to be checked in this case. From now on $A = \{g_{qv-u}\}_{u,v \in U}$, the matrix of the transformation $\Psi_{q,G}$, and $G \in R_0$. Due to the restriction o n G one can easily prove that the terms b_m converge and

$$\lim_{m \to \infty} \frac{1}{m} \mathrm{ord}_p b_m = \infty.$$

This shows that $\det(1 - At) = \sum_{m=0}^{\infty} b_m t^m$ not only exists, but converges everywhere on $\mathbb{C}_p$.

The missing part of the following lemma follows from basic linear algebraic results for finite matrices, and can be proven for infinite matrices by taking the limit of finite ones.

Lemma 2.2.3. *If $G(x) = \sum_{w \in U} g_w x^w 0 \in R_0$ and $\Psi = T_q \circ L_G$, so that Ψ has a matrix $A = \{g_{qv-u}\}_{u,v \in U}$, then the series $\det(1 - At)$ is a well-defined power series over $\mathbb{C}_p$ with infnite radius of convergence, and*

$$\det(1 - At) = \exp_p \left(- \sum_{s=1}^{\infty} \mathrm{Tr}\,(A^s) t^s / s \right)$$

2.3 The analytic expression of the zeta function

Lemma 2.3.1. *The zeta function of a hypersurface X defined by $f \in \mathbb{F}_q[x_1, ..., x_n]$ is a quotient of two entire power series over $\mathbb{C}_p$.*

This is proved by induction on n. The first step is to note that it is enough to prove this for $\zeta'(X/\mathbb{F}_q, t) = \exp\left(\sum_{s=1}^{\infty} N'_s t^s\right)$, where N'_s is the number of points satisfying f over $\mathbb{F}_q^s$ with no zero coordinates. The reason for this is that the quotient $\zeta(X/\mathbb{F}_q, t)/\zeta'(X/\mathbb{F}_q, t)$ is the zeta function of $X \cap (\bigcup_{i=1}^{n} H_i)$ where $H_i = \{(x_1, ..., x_n) : x_i = 0\}$, which can be expressed by the alternating product of the zeta functions of affine hypersurfaces of the k-ary intersections of these hyperplanes in an inclusion-exclusion principle like way. By the inductive assumption, all these are the quotient of entire power series.

Fix $s \in \mathbb{Z}^+$, and $q = p^r$. Due to the properties of characters:

$$\sum_{x_0 \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}\,(x_0 u)} = \begin{cases} -1, \text{ if } u \in \mathbb{F}_{q^s}^{\times} \\ q^s - 1, \text{ if } u = 0. \end{cases}$$

This gives us for $u = f(x_1, ..., x_n)$:

$$\sum_{x_0, ..., x_n \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}\,(x_0 f(x_1, ..., x_n))} = q^s N'_s - (q^s - 1)^n.$$

In $x_0 f$ replace the coefficients with their Teichmüller representatives, then we get $F(x_0, ..., x_n) = \sum_{i=1}^{N} [a_i] x^{w_i} \in \mathbb{C}_p[x_0, ..., x_n]$, where $[a_i]$ denotes the Teichmüller lift of $a_i \in \mathbb{F}_{q^s}$. The monomial $[a]x^w$ evaluated in some Teichmüller representative of elements in $\mathbb{F}_{q^s}$ is exactly the Teichmüller representative of the same elements evaluated in ax^w. This gives:

$$q^s N'_s = (q^s - 1)^n + \sum_{x_0, ..., x_n \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}\,(x_0 f(x_1, ..., x_n))} = (q^s - 1)^n + \sum_{x_0, ..., x_n \in \mathbb{F}_{q^s}^{\times}} \prod_{i=1}^{N} \varepsilon^{\mathrm{Tr}\,(a_i x^{w_i})} =$$

$$= (q^s - 1)^n + \sum_{\substack{x_0, ..., x_n \in \mathbb{C}_p \\ x_0^{q^s - 1} = ... = x_n^{q^s - 1} = 1}} \prod_{i=1}^{N} \varepsilon^{\mathrm{Tr}\,([a_i] x^{w_i})} = (q^s - 1)^n + \sum_{\substack{x_0, ..., x_n \in \mathbb{C}_p \\ x_0^{q^s - 1} = ... = x_n^{q^s - 1} = 1}} \prod_{i=1}^{N} \Theta([a_i] x^{w_i}) \Theta([a_i]^p x^{p w_i}) ... \Theta([a_i]^{p^{rs-1}} x^{p^{rs-1} w_i}).$$

Let

$$G(x_0, ..., x_n) = \prod_{i=1}^{N} \Theta([a_i] x^{w_i}) \Theta([a_i]^p x^{p w_i}) ... \Theta([a_i]^{p^{r-1}} x^{p^{r-1} w_i}),$$

so that

$$q^s N'_s = (q^s - 1)^n \sum_{\substack{x_0, ..., x_n \in \mathbb{C}_p \\ x_0^{q^s - 1} = ... = x_n^{q^s - 1} = 1}} G(x) ... G(x^{q^{s-1}}).$$

Since G is a finite product of elements in R_0 it is also in R_0 hence by Lemma 2.2.2

$$q^s N'_s = (q^s - 1)^n + (q^s - 1)^{n+1} \mathrm{Tr}\,(\Psi_{q,G}^s).$$

Substituting the binomial expansion and the result of Lemma 2.2.3 we get

$$\zeta'(X/\mathbb{F}_q, t) = \prod_{i=1}^{n} (1 - q^{n-i-1} t)^{-1^{i+1} \binom{n}{i}} \prod_{i=0}^{n+1} \det(1 - A q^{n-i} t)^{-1^{i+1} \binom{n+1}{i}},$$

where A is the matrix of $\Psi_{q,G}$. By Lemma 2.2.3, each term is an entire function.

2.4 Final steps

Dwork finishes the proof using a linear algebraic lemma.

Lemma 2.4.1. *Let $F(t) = \sum_{n=0}^{\infty} a_n t^n \in K[[t]]$ for any field K. Let $s, m \geq 0$, $A_{s,m} = \{a_{s+i+j}\}_{0 \leq i,j \leq m}$ and $N_{s,m} = \det A_{s,m}$. Then $F(t)$ is a rational function if and only if there exist $m, S \geq 0$ that for all $s \geq S$ $N_{s,m} = 0$.*

The remainder of the proof is rather technical, but the core idea is to write $F(t) = P(t)\zeta(X/\mathbb{F}_q, t)$, where P is a polynomial and F is convergent on a large enough disk. This can be done by the p-adic Weierstrass Preparation Theorem, and due to the convergence, the p-adic norm of the coefficients of F has an upper estimate.

Now the coefficients of F are a linear combination of the coefficients of ζ (P is a polynomial), allowing us to replace the last columns in the matrix corresponding to the one in Lemma 2.4.1, and knowing that the coefficients of ζ are integers, we can give an upper estimate of the p-adic norm of the determinant.

There is a crude upper estimate of the Euclidean norm of the coefficients of the ζ function, using that $N_s \leq q^{ns}$ where n is the number of variables of the function defining X. This gives an upper estimate of the Euclidean norm of the determinant using the original matrix.

By choosing the right parameters one can assure, that the product of the two norms of the determinant converges to zero as s goes to ∞, and given that the determinant is an integer, this suggests that it must vanish for sufficiently large s. This finishes the proof of the theorem.

Bibliography

[1] Koblitz, N. (1984). Rationality of the zeta-function of a set of equations over a finite field. In: p-adic Numbers, p-adic Analysis, and Zeta-Functions. Graduate Texts in Mathematics, vol 58. Springer, New York, NY. https://doi.org/10.1007/978-1-4612-1112-9_5