RATIONALITY OF ZETA FUNCTIONS OVER FINITE FIELDS

SUN WOO PARK

Abstract. The zeta function of an affine variety over a finite field contains comprehensive information on the number of points of the variety for all the field extensions of the finite field. This expository paper follows Koblitz's treatment [2] of Dwork's proof [1] of the rationality of zeta functions of affine varieties over finite fields, also known as the rationality statement of the Weil Conjectures.

Contents

1. Introduction

Let $f(x_1, ..., x_n)$ be a polynomial with n variables over a finite field $\mathbb{F}_q$ where $q = p^r$ is a power of a prime p. The natural question then arises as to what are the roots of the polynomial, which motivates the definition of the affine hypersurface of the polynomial.

Definition 1.1. Let $\mathbb{F}_q$ be a finite field with q a power of a prime p. The n-dimensional affine space over the finite field $\mathbb{F}_q$ is the set of ordered n-tuples $(a_1, ..., a_n)$ where each element a_i is in the finite field $\mathbb{F}_q$. Denote the affine space as $\mathbb{A}^n_{\mathbb{F}_q}$.

Let $f(x_1, ..., x_n)$ be a polynomial with n variables over $\mathbb{F}_q$. Then the affine hypersurface H_f of the polynomial $f(x_1, ..., x_n)$ is the set of all the roots of $f(x_1, ..., x_n)$ in the affine space $\mathbb{A}^n_{\mathbb{F}_q}$.

$$H_f = \{(a_1, ..., a_n) \in \mathbb{A}^n_{\mathbb{F}_q} \mid f(a_1, ..., a_n) = 0\}$$

Let s be a positive integer and let $\mathbb{F}_{q^s}$ be a field extension of $\mathbb{F}_q$. Observe that the coefficients of the polynomial $f(x_1, ..., x_n)$ are also in $\mathbb{F}_{q^s}$ for any s. This allows

us to consider the set of all the roots of the polynomial $f(x_1, ..., x_n)$ in the affine space of $\mathbb{F}_{q^s}$.

Definition 1.2. Let $\mathbb{F}_{q^s}$ be a field extension of $\mathbb{F}_q$. Let H_f be the affine hypersurface of a polynomial $f(x_1, ..., x_n)$ with n variables over $\mathbb{F}_q$. Then the set of $\mathbb{F}_{q^s}$-points of H_f, denoted as $H_f(\mathbb{F}_{q^s})$, is the set of all the roots of $f(x_1, ..., x_n)$ in the affine space of $\mathbb{F}_{q^s}$.

$$H_f(\mathbb{F}_{q^s}) = \{(a_1, ..., a_n) \in \mathbb{A}^n_{\mathbb{F}_{q^s}} \mid f(a_1, ..., a_n) = 0\}$$

The order of the set $H_f(\mathbb{F}_{q^s})$ can be understood as the number of roots of the polynomial $f(x_1, ..., x_n)$ over $\mathbb{F}_{q^s}$. Using the definition above, we can construct a function over $\mathbb{C}_p$, the analogue of $\mathbb{C}$ in the field of p-adic numbers $\mathbb{Q}_p$. Before we construct the function, we state the definition of the field of p-adic numbers $\mathbb{Q}_p$.

Definition 1.3. Let p be a prime number. The ring of p-adic integers $\mathbb{Z}_p$ is the inverse limit of the inverse system $((\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}, (f_{nm})_{n>m\in\mathbb{N}})$ where the transition morphism $f_{nm} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ is given by reduction mod p^m. The fraction field of $\mathbb{Z}_p$ is the field of p-adic numbers $\mathbb{Q}_p$ and the completion of the algebraic closure of $\mathbb{Q}_p$ is the complex field of p-adic numbers $\mathbb{C}_p$.

Notice $\mathbb{C}_p$ is defined as above because the algebraic closure of $\mathbb{Q}_p$ is not complete. The valuation over $\mathbb{Q}_p$ and $\mathbb{C}_p$ is defined as follows, the construction of which is described in Chapter 1 and 3 of Koblitz [1].

Definition 1.4. The valuation of an element $a \in \mathbb{Q}_p$, denoted as $ord_p a$, is the largest integer power l of p such that p^l divides a. The p-adic norm of a is defined as follows.

$$|a|_p = \begin{cases} p^{-ord_p a} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

The norm defined above is a non-Archimedean norm. Let $b \in \overline{\mathbb{Q}_p}$ have the irreducible polynomial $f(x) = x^n + a_1x^{n-1} + ... + a_n$ over $\mathbb{Q}_p$. Then the norm of b is defined as $|b|_p = |a_n|_p^{1/n}$. The norm on $\overline{\mathbb{Q}_p}$ extends to $\mathbb{C}_p$ by defining $|x|_p = \lim_{n\to\infty} |x_n|_p$ where $x \in \mathbb{C}_p$ and $\{x_n\}$ is a sequence in $\overline{\mathbb{Q}_p}$.

Definition 1.5. Let $f(x_1, ..., x_n)$ be a polynomial with n variables over $\mathbb{F}_q$ for $q = p^r$ a power of p. Let H_f be the affine hypersurface of $f(x_1, ..., x_n)$. Denote $N_s = |H_f(\mathbb{F}_{q^s})|$ as the number of $\mathbb{F}_{q^s}$-points of H_f. Then the zeta function of H_f is defined as follows, where Exp_p is the exponential function in $\mathbb{C}_p$.

$$Z(H_f, T) = Exp_p\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right)$$

The zeta function contains all the information on the number of roots of a polynomial over each field extension of the finite field $\mathbb{F}_q$. Bernard Dwork proved the following property of the zeta function of H_f in 1960, which is the primary focus of the paper.

Theorem 1.6 (Dwork, 1960)**.** *Let H_f be the affine hypersurface of a polynomial f with n variables over the finite field $\mathbb{F}_q$. Then the zeta function of H_f is a quotient of two polynomials with coefficients in $\mathbb{Q}_p$.*

In fact, this theorem is one of the statements of the Weil conjectures proposed by André Weil in 1949. The Weil conjectures explain the properties of the zeta functions of algebraic varieties over finite fields. Weil claimed that the zeta functions are quotients of two polynomials over $\mathbb{Q}_p$ and satisfy some forms of functional equations. He further claimed that the roots of the zeta functions appear in restricted places, an analogue of the Riemann hypothesis. As a particular example, the reciprocal roots of the zeta functions $F(s) = Z(\overline{H_f}, q^{-s})$ of projective 1-dimensional hypersurfaces $\overline{H_f}$ are on the line $Re(s) = 1/2$. Dwork's theorem corresponds to the rationality statement of the Weil conjectures. Alexander Grothendieck proved the statement on functional equations in 1965 and Pierre Deligne proved the analogue of the Riemann hypothesis in 1973.

Dwork's proof consists of two steps. The first step, proved by induction on the number of variables, shows that the zeta function is a quotient of two power series over $\mathbb{C}_p$, both of which converge everywhere. Observe that N_s is the sum of the number of roots of the polynomial where each coordinate is non-zero and the number of roots of the polynomial where at least one coordinate is zero. The latter case inductively relates N_s with the number of roots of other polynomials with fewer variables. The former case can be expressed as a sum of a set of p-th roots of unity. By extending the coefficients of the polynomial from the finite field $\mathbb{F}_q$ to the field of p-adic numbers $\mathbb{Q}_p$, Dwork constructs a power series over $\mathbb{C}_p$ and uses the series to change the sum of p-th roots of unity to the sum of power series over $\mathbb{C}_p$. He then shows that the determinant of the power series under the basis of monomials converges everywhere on $\mathbb{C}_p$, which proves the first step.

The second step uses the first step to prove the theorem. Using p-adic analysis, Dwork shows that there exists a polynomial and a power series over $\mathbb{C}_p$ with certain radius of convergence such that the quotient of the polynomial and the power series is the zeta function. He then compares the coefficients of the quotient with those of the zeta function, which allows him to estimate the p-adic norm and the usual norm of the determinant of a matrix consisting of a finite set of coefficients of the zeta function. The comparison between the two norms shows that the determinant of the matrix is 0 which implies that the zeta function is a quotient of two polynomials over $\mathbb{C}_p$.

This paper focuses on carefully following Koblitz's treatment [2] of the proof of Dwork's theorem [1]. The paper first provides important backgrounds on properties of some power series over $\mathbb{C}_p$. Using the properties, the paper then follows Dwork's proof on the rationality of zeta functions. The paper also states an alternate construction of the zeta functions given by Kapranov [5], extending the construction of the zeta functions over finite fields to zeta functions over perfect fields.

2. Power Series over $\mathbb{C}_p$

Let $F(x)$ be a power series over $\mathbb{C}_p$ of the form $F(x) = \sum_{n=0} a_n x^n$. Since $\mathbb{C}_p$ is complete and the norm is non-Archimedean, the series converges if and only if the norm of the term $|a_n x^n|_p \to 0$ as $n \to \infty$. In other words, for certain values of $x \in \mathbb{C}_p$ we can evaluate $F(x)$ by the limit the infinite sum converges to. Observe that if all the coefficients a_n are in $\mathbb{Z}_p$, then the series $F(x)$ converges for $|x|_p < 1$ because $|a_n x^n|_p \leq |x|_p^n \to 0$ as $n \to \infty$. This proves the following lemma.

Lemma 2.1. *If $F(x)$ is a power series in $\mathbb{Z}_p$, then $F(x)$ converges for $|x|_p < 1$.*

Similar to power series over $\mathbb{C}$, we can define the radius of convergence of a power series over $\mathbb{C}_p$.

Definition 2.2. The radius of convergence r of a power series $F(x) = \sum_{n=0}^{\infty} a_n x^n$ is the following limit.

$$r = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}$$

As the term suggests, the series converges if $|x|_p < r$ and diverges if $|x|_p > r$. This can be shown by observing whether the norm of the term $a_n x_n$ approaches 0 as $n \to \infty$. It is not true, however, that the series converges if $|x|_p = r$.

Definition 2.3. The closed and open disks of radius $r \in \mathbb{R}$ around a point $a \in \mathbb{C}_p$ are defined respectively as follows.

$$D_a(r) = \{x \in \mathbb{C}_p || x - a|_p \leq r\}$$
$$D_a(r-) = \{x \in \mathbb{C}_p || x - a|_p < r\}$$

We will abbreviate the disk around the origin $D_0(r)$ as $D(r)$. Using this notation, we can say that a power series $F(x)$ converges in $D(r)$ or $D(r-)$ if it has r as the radius of convergence.

2.1. **Logarithms, Exponents, and Other Power Series.** Several power series defined over $\mathbb{C}$ can be analogously defined over $\mathbb{C}_p$.

Definition 2.4. The logarithmic function Log_p and the exponential function Exp_p is defined as the following power series over $\mathbb{C}_p$.

$$Log_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$
$$Exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

As in the case for complex numbers, the following proposition holds.

Proposition 2.5. *Let Log_p and Exp_p be the logarithmic and the exponential function in $\mathbb{C}_p$. Then the following holds.*

1. *$Log_p(1+x)$ converges in $D(1-)$.*
2. *$Exp_p(x)$ converges in $D(p^{-\frac{1}{p-1}}-)$.*
3. *Log_p and Exp_p are mutually inverse isomorphisms between the multiplicative group $D_1(p^{-\frac{1}{p-1}}-)$ and the additive group $D(p^{-\frac{1}{p-1}}-)$.*

Proof. Observe that $\limsup_{n\to\infty} |1/n|_p^{1/n} = \lim_{n\to\infty} p^{\frac{ord_p n}{n}} = 1$. Since $|x^n/n|_p = p^{ord_p n} \geq 1$ if $|x|_p = 1$, $Log_p(1+x)$ converges in $D(1-)$.

Notice that $ord_p n! = \frac{n - S_n}{p-1}$ where S_n is the sum of all p-adic digits of $n!$. Suppose that n has the p-adic expansion $n = a_k p^k + a_{k-1} p^{k-1} + ... + a_0$. Observe that $ord_p n! = \sum_{i=1}^{k} \lfloor \frac{n}{p^i} \rfloor$ as $\lfloor \frac{n}{p} \rfloor$ contributes to a factor p, $\lfloor \frac{n}{p^2} \rfloor$ contributes to a square factor of p, and so on. Then for every i we have $\lfloor \frac{n}{p^i} \rfloor = a_k p^{k-i} + a_{k-1} x^{k-1-i} + ... + a_i$, which implies the following.

$$ord_p n! = \sum_{i=1}^{k} \lfloor \frac{n}{p^i} \rfloor = \sum_{i=1}^{k} a_i \frac{p^i - 1}{p-1} = \frac{\sum_{i=0}^{k} (a_i p^i) - \sum_{i=0}^{k} a_i}{p-1} = \frac{n - S_n}{p-1}$$

This shows that the radius of convergence of Exp_p is $p^{-\frac{1}{p-1}}$ as from the equation below.

$$\limsup_{n\to\infty} |1/n!|_p^{1/n} = \limsup_{n\to\infty} p^{\frac{n-S_n}{n(p-1)}} = p^{\frac{1}{p-1}}$$

Suppose $|x|_p = p^{\frac{-1}{p-1}}$. Choose n to be a power of p such that $S_n = 1$. Then $ord_p x^n/n! = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1}$, which shows $|x^n/n!|_p = p^{-\frac{1}{p-1}}$. Hence Exp_p converges in $D(p^{-\frac{1}{p-1}}-)$.

From the definition of Log_p, $Log_p(1+x)(1+y) = Log_p(1+x) + Log_p(1+y)$, which shows that Log_p is a group homomorphism from the multiplicative group $D_1(p^{-\frac{1}{p-1}}-)$ to the additive group $D(p^{-\frac{1}{p-1}}-)$. Similarly, Exp_p is a group homomorphism from $D(p^{-\frac{1}{p-1}}-)$ to $D_1(p^{-\frac{1}{p-1}}-)$. By the definition of two functions, we also have $Exp_p(Log_p(1+x)) = 1+x$ and $Log_p(Exp_p(x)) = x$ if $x \in D(p^{-\frac{1}{p-1}}-)$. Hence the two functions are mutually inverse isomorphisms. □

Definition 2.6. Let $a \in \mathbb{C}_p$. Then the binomial expansion $(1+x)^a$ is defined as the following power series.

$$B_a(x) = \sum_{n=0}^{\infty} \frac{a(a-1)...(a-n+1)}{n!} x^n$$

If $|a|_p > 1$ then for any integer i, $|a-i|_p = |a|_p$. Hence the norm of the nth term of the binomial power series is $|\frac{a^n x^n}{n!}|_p$. This implies that the power series converges in $D(\frac{p^{-\frac{1}{p-1}}}{|a|_p}-)$. If $|a|_p \leq 1$ then for any integer i, $|a-i|_p \leq 1$. This shows that the norm of the nth term of the binomial power series is $|\frac{a(a-1)...(a-n+1)x^n}{n!}|_p \leq |\frac{x^n}{n!}|_p$. This implies that the power series converges in $D(p^{-\frac{1}{p-1}}-)$.

We now define a new power series which will be used in Dwork's proof of the rationality of zeta functions.

Definition 2.7. Let $F(x,y)$ be a power series with two variables over $\mathbb{C}_p$ defined as follows.

$$F(x,y) = B_x(y) \prod_{i=0}^{\infty} B_{\frac{x^{p^{i+1}} - x^{p^i}}{p^{i+1}}}(y^{p^{i+1}})$$

This can be rewritten as follows.

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

Observe that the power series $F(x,y)$ has all its coefficients in $\mathbb{Q}_p$. The series is also well defined because for any term $x^n y^m$, the corresponding coefficient can be achieved by taking finitely many terms in $\mathbb{Q}_p$. We will analyze this power series further after proving the following lemma.

Lemma 2.8 (Dwork's Lemma)**.** *Let $F(x)$ be a power series over $\mathbb{Q}_p$ such that the constant term is 1. Then $F(x)$ has all its coefficients in $\mathbb{Z}_p$ if and only if $\frac{F(x^p)}{(F(x))^p}$ has all its coefficients other than the constant term in $p\mathbb{Z}_p$.*

Proof. Suppose $F(x)$ has all its coefficients in $\mathbb{Z}_p$ with constant term 1. Notice that $(a+b)^p \equiv a^p + b^p \ mod\ p$ and $a^p \equiv a \ mod\ p$ for any $a, b \in \mathbb{Z}_p$. Then there exists a

power series $G(x) \in x\mathbb{Z}_p[[x]]$ such that the following holds.

$$(F(x))^p = F(x^p) + pG(x)$$

The above equation implies the following equation because $(F(x))^p$ has all its coefficients in $\mathbb{Z}_p$ and $1 + x\mathbb{Z}_p[[x]]$ is a group under multiplication.

$$\frac{F(x^p)}{(F(x))^p} = 1 - p\frac{G(x)}{(F(x))^p} \in 1 + px\mathbb{Z}_p[[x]]$$

Suppose $\frac{F(x^p)}{(F(x))^p}$ has all its coefficients other than the constant term in $p\mathbb{Z}_p$. Then we can find a power series $G(x) \in 1 + px\mathbb{Z}_p[[x]]$ such that $F(x^p) = (F(x))^p G(x)$. Let $F(x) = \sum_{i=0}^{\infty} a_i x^i$ and $G(x) = \sum_{j=0}^{\infty} b_j x^j$ where $b_j \in p\mathbb{Z}_p$ for all j. We want to show that $a_i \in \mathbb{Z}_p$ for all i.

We prove the lemma by induction on the index i. The base case holds because $a_0 = 1$. Suppose $a_i \in \mathbb{Z}_p$ for $i \leq n-1$. Consider the following equation.

$$F(x^p) = (F(x))^p G(x)$$

The coefficients of x^n on both sides of the equation must be the same. Notice that the coefficient of x^n from the RHS of the equation above is determined by the product $(\sum_{i=0}^{n} a_i x^i)^p (1 + \sum_{j=1}^{n} b_j x^j)$. This shows that the coefficient from the RHS consists of terms which contain b_j for some j and terms which only have a_i as factors. The former terms are in $p\mathbb{Z}_p$, which we will denote as pB.

If $p \mid n$, then the coefficient from the LHS is $a_{n/p}$ while the coefficient from the RHS is $pB + pa_n + a_{n/p}^p$. For any $a \in \mathbb{Z}_p$ we have $a^p \equiv a \ mod\ p$. Hence a_n is an element of $\mathbb{Z}_p$. If $p \nmid n$ then the coefficient from the LHS is 0 while the coefficient from the RHS is $pB + pa_n$. This also shows a_n is an element of $\mathbb{Z}_p$. □

The generalization of Dwork's lemma is as follows, the proof of which is analogous to that of Lemma 2.8.

Lemma 2.9 (Generalized Dwork's Lemma)**.** *Let $F(x_1, x_2, ..., x_n)$ be a power series with n variables over $\mathbb{Q}_p$ such that the constant term is 1. Then $F(x_1, ..., x_n)$ has all its coefficients in $\mathbb{Z}_p$ if and only if $\frac{F(x_1^p, ..., x_n^p)}{(F(x_1, ..., x_n))^p}$ has all its coefficients other than the constant term in $p\mathbb{Z}_p$.*

Using the generalized Dwork's lemma, we prove the following proposition.

Proposition 2.10. *The power series $F(x, y)$ has all its coefficients in $\mathbb{Z}_p$.*

Proof. Observe that the following equation holds by Lemma 2.9.

$$\begin{aligned}
\frac{F(x^p, y^p)}{(F(x, y))^p} &= \frac{B_{x^p}(y^p) \prod_{i=0}^{\infty} B_{(x^{p^{i+2}} - x^{p^{i+1}})/p^{i+1}}(y^{p^{i+2}})}{B_{px}(y) \prod_{i=0}^{\infty} B_{(x^{p^{i+1}} - x^{p^i})/p^i}(y^{p^{i+1}})} \\
&= \frac{B_{x^p}(y^p)}{B_{px}(y) B_{x^p - x}(y^p)} \frac{\prod_{i=0}^{\infty} B_{(x^{p^{i+2}} - x^{p^{i+1}})/p^{i+1}}(y^{p^{i+2}})}{\prod_{i=1}^{\infty} B_{(x^{p^{i+1}} - x^{p^i})/p^i}(y^{p^{i+1}})} \\
&= \frac{(1+y^p)^{x^p}}{(1+y)^{px}(1+y)^{x^p - x}} = \frac{(1+y^p)^x}{(1+y)^{px}}
\end{aligned}$$

Hence it suffices to show that $\frac{(1+y^p)^x}{(1+y)^{px}}$ has all its coefficients other than the constant term in $p\mathbb{Z}_p$. Notice that $1 + y$ is an element of $1 + y\mathbb{Z}_p[[y]]$. By Lemma 2.8, there

exists a power series $G(y) \in \mathbb{Z}_p[[y]]$ such that the following holds.

$$\frac{(1+y^p)}{(1+y)^p} = 1 + pyG(y)$$

By the definition of binomial power series, the following equation holds.

$$\frac{(1+y^p)^x}{(1+y)^{px}} = (1+pyG(y))^x \in 1 + px\mathbb{Z}_p[[x,y]] + py\mathbb{Z}_p[[x,y]]$$

□

The proposition shows that $F(x,y)$ can be expressed as follows in which for all non-negative integers n and m, $a_{m,n} \in \mathbb{Z}_p$.

$$F(x,y) = \sum_{n=0}^{\infty}(x^n \sum_{m=n}^{\infty} a_{m,n}y^m)$$

Notice we have $\sum_{m=n}^{\infty} a_{m,n}y^m$ instead of $\sum_{m=0}^{\infty} a_{m,n}y^m$ because for each term in $B_{\frac{x^{p^{i+1}}-x^{p^i}}{p^{i+1}}}(y)$ the power of x is less than or equal to the power of y, i.e.

$$\left(\frac{x^{p^{i+1}}-x^{p^i}}{p^{i+1}}\right)\left(\frac{x^{p^{i+1}}-x^{p^i}}{p^{i+1}}-1\right)...\left(\frac{x^{p^{i+1}}-x^{p^i}}{p^{i+1}}-n+1\right)\frac{y^{np^i}}{n!}$$

2.2. **Newton Polygons.**

Definition 2.11. Let $f(x) = 1 + \sum_{i=1}^{n} a_i x^i$ be a polynomial of degree n over $\mathbb{C}_p$. The Newton polygon of $f(x)$ is the convex hull of the points $(0,0)$, $(1, ord_p a_1)$, ..., $(i, ord_p a_i)$, ..., $(n, ord_p a_n)$ in the real coordinate plane. In other words, it is the highest convex polygonal line which starts at $(0,0)$, ends at $(n, ord_p a_n)$, and joins or passes below all the points $(i, ord_p a_i)$.

Let $F(x) = 1 + \sum_{i=1}^{\infty} a_i x^i$ be a power series over $\mathbb{C}_p$. Let $f_n(x)$ be the n-th partial sum of $F(x)$. Then the Newton polygon of $F(x)$ is the limit of the Newton polygons of $f_n(x)$.

The way to construct the Newton polygon of a polynomial or a power series is as follows. Plot all the set of points $(i, ord_p i)$. Rotate the vertical line passing through $(0,0)$ counter-clockwise until it hits a point $(i, ord_p a_i)$ for some i. Then rotate the line with respect to the point $(i, ord_p a_i)$ and repeat the process.

For convenience we will define the terms as follows. The set of vertices of the Newton polygon is the set of points where the slopes change. The length of a segment is the length of the projection of the segments onto the horizontal axis.

The Newton polygon of a polynomial $f(x)$ over $\mathbb{C}_p$ gives important properties of the roots of $f(x)$. We omit the proof of the following lemma which is written in Chapter 4 of Koblitz [2].

Lemma 2.12. *Let $f(x) = \prod_{i=1}^{n}(1 - x/a_i)$ be a polynomial over $\mathbb{C}_p$ with roots $\{a_i\}_{i=1}^{n}$. Let $ord_p a_i = m_i$. If m is a slope of the Newton polygon of $f(x)$ with length q, then precisely q of m_i are equal to m.*

The Newton polygon of a power series can be classified into three categories.

(1) There are infinitely many segments of finite length. Consider the power series $F(x) = 1 + \sum_{n=1}^{\infty} p^{i^2} x^i$. The Newton polygon is an infinite set of finite line segments which connects the lattices (n, n^2) on the graph $y = x^2$.

(2) There are finitely many segment in which the last segment is infinitely long. The power series $F(x) = 1 + \sum_{n=1}^{\infty} x^n$ has an infinite horizontal line as its Newton polygon.
(3) There may be a case such that it is not possible to draw the Newton polygon using the method above. Consider the power series $F(x) = 1 + \sum_{n=1}^{\infty} px^n$. Observe that there exists an integer n such that the point $(n, 1)$ lies below a line segment which is obtained from rotating the horizontal line passing through the origin counterclockwise. In this case, we let the last segment of the Newton polygon have the slope to be the least upper bound of all slopes of which any point $(i, ord_p a_i)$ lies above or on the line. In the previous example, the Newton polygon is the infinite horizontal line passing through the origin.

Newton polygons provide a different way of understanding the power series over $\mathbb{C}_p$. The slope of the Newton polygon of a power series gives additional information on the radius of convergence of the series as well as the valuations of the roots of the power series. The following theorem, which is an analogue of Lemma 2.12 for power series, will prove useful for understanding Dwork's proof in subsequent sections.

Theorem 2.13 (p-adic Weierstrass Preparation Theorem)**.** *Let $F(x)$ be a power series over $\mathbb{C}_p$ which converges on $D(p^m)$. Denote the terms of the power series as $F(x) = 1 + \sum_{n=1} a_n x^n$. Suppose the Newton polygon of $F(x)$ does not have the infinitely long last segment of slope m. Denote N as the total length of all finite segments having slope less than m. If the Newton polygon of $F(x)$ has the last segment of slope m, denote N as the greatest n such that $(n, ord_p a_n)$ lies on the last segment. Then there exists a unique polynomial $h(x)$ in $\mathbb{C}_p$ with constant term 1 of degree N and a power series $G(x) = 1 + \sum_{n=1}^{\infty} b_n x^n$ which converges and is nonzero in $D(p^m)$ such that $h(x) = F(x)G(x)$.*

Corollary 2.14. *Suppose $F(x)$ is a power series over $\mathbb{C}_p$ with the constant term 1. If a segment of the Newton polygon of $F(x)$ has horizontal length N and slope m, then there are precisely N roots x of $F(x)$ counting multiplicity such that the valuation $ord_p x = -m$.*

We first prove the following lemmas which will help us prove Theorem 2.13.

Lemma 2.15. *Let $F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ be a power series over $\mathbb{C}_p$. Let m be the least upper bound of all the slopes of the Newton polygon of $F(x)$. Here m may be infinite. Then the radius of convergence of $F(x)$ is p^m.*

Proof. Suppose $x \in \mathbb{C}_p$ such that $ord_p x = -m' > -m$. Then $ord_p(a_n x^n) = ord_p a_n - nm'$. Notice that $(n, ord_p a_n)$ lies above the Newton polygon while (n, nm') lies above a line of slope m' passing through the origin. By the definition of m, $ord_p a_n - nm' \to \infty$ as $n \to \infty$, which implies that the series converges. Now assume $ord_p x = -m'' < -m$. By the similar argument as above, for infinitely many n, the value $ord_p a_n - nm''$ is negative, proving that the series does not converge. □

The above lemma does not explain whether the power series converges when $ord_p x$ is equal to the least upper bound of all slopes of the Newton polygon.

Remark 2.16. Let $F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ be a power series over $\mathbb{C}_p$. Suppose $c \in \mathbb{C}_p$ such that $ord_p c = d$ and $G(x) = F(x/c) = 1 + \sum_{n=1}^{\infty} b_n x^n$ is also a power

series over $\mathbb{C}_p$. Notice that for each n, $ord_p b_n = ord_p(a_n/c^n) = ord_p a_n - dn$. This shows that the Newton polygon of $G(x)$ is obtained by subtracting the line $y = dx$ from the Newton polygon of $F(x)$.

Lemma 2.17. *Suppose m_1 is the first slope of the Newton polygon of a power series $F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ over $\mathbb{C}_p$. Let $c \in \mathbb{C}_p$ such that $ord_p c = m \leq m_1$.*

Let $G(x)$ be the power series defined as $G(x) = (1 - cx)F(x)$. Suppose $F(x)$ converges on the closed disk $D(p^m)$. Then the Newton polygon of $G(x)$ is obtained by first joining $(0, 0)$ to $(1, m)$ and then shifting the Newton polygon of $F(x)$ by 1 to the right and d upwards.

Suppose further that the last slope of the Newton polygon of $F(x)$ is m_f. Then the Newton polygon of $G(x)$ also has m_f as the last slope. In addition, $F(x)$ converges in $D(p^{m_f})$ if and only if $G(x)$ does.

Proof. We will first prove the lemma when $c = 1$. Then $G(x) = (1 - x)F(x)$ satisfies $G(x) = 1 + \sum_{n=1}^{\infty}(a_n - a_{n-1})x^n$. Denote $b_n = a_n - a_{n-1}$. It follows that $ord_p b_n \geq min(ord_p a_n, ord_p a_{n-1})$. Since both points $(n, ord_p a_n), (n - 1, ord_p a_{n-1})$ lie above or on the Newton polygon of $F(x)$, the points $(n, ord_p b_n)$ all lie above the Newton polygon of $F(x)$ translated by 1 to the right. Notice that the translation includes an extra segment connecting $(0, 0)$ and $(1, 0)$. If $(n - 1, ord_p a_{n-1})$ is one of the vertices of the Newton polygon of $F(x)$, then $ord_p b_n = ord_p a_{n-1}$ because $ord_p a_n > ord_p a_{n-1}$. This shows $(n, ord_p b_n)$ is also a corner of the translated Newton Polygon.

Now we prove the second statement of the lemma. Notice that since $ord_p b_n \geq min(ord_p a_n, ord_p a_{n-1})$, $G(x)$ converges whenever $F(x)$ converges. Suppose that the Newton polygon of $G(x)$ has a slope such that $m_g > m_f$. Then for some n, $(n + 1, ord_p a_n)$ lies below the Newton polygon of $G(x)$. This shows that for all $k \geq n + 1$, $ord_p b_k > ord_p a_n$. Since $a_{n+1} = b_{n+1} + a_n$, $ord_p a_{n+1} = ord_p a_n$. By the similar argument, $ord_p a_k = ord_p a_n$ for all such $k \geq n + 1$. This contradicts the assumption that the power series $F(x)$ converges on $D(1)$. The converse holds analogously.

Now we prove the lemma for arbitrary choice of c. Define the power series $F_1(x) = F(x/c)$ and $G_1(x) = (1 - x)F_1(x)$. Notice that the lemma holds for $F_1(x)$ and $G_1(x)$ because both power series satisfy the base case of the proof of the lemma. By Remark 2.16, we obtain the desired results for the Newton polygon of $G(x)$. □

Lemma 2.18. *Let $F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ be a power series over $\mathbb{C}_p$. Suppose the Newton polygon of $F(x)$ has the first slope m_1. If $F(x)$ converges on the closed disk $D(p^{m_1})$ and the line through $(0, 0)$ with slope m_1 passes through $(n, ord_p a_n)$ for some n, then there exists a root x of $F(x)$ such that $ord_p x = -m_1$.*

Proof. We first prove the lemma when $m_1 = 0$. This implies that for all n we have $ord_p a_n \geq 0$ and $ord_p a_n \to \infty$ as $n \to \infty$. Let M be the greatest integer n such that $ord_p a_n = 0$. Denote $f_n(x)$ as the n-th partial sum of $F(x)$. By Lemma 2.12, for $n \geq M$, the polynomial $f_n(x)$ has precisely M roots $x_{n,1}, x_{n,2}, ..., x_{n,M}$ such that for every i, $ord_p x_{n,i} = 0$.

Let S_n be the set of roots of $f_n(x)$ counting multiplicities. Consider the following sequence $\{x_n\}$ such that $x_M = x_{M,1}$ and $x_{n+1} = a \in S_{n+1}$ such that $ord_p a = 0$ and $|a - x_n|$ is minimal. Notice that if $a \in S_n + 1$ such that $ord_p a < 0$, then $|1 - x_n/a|_p = 1$. Hence the following holds for $n > M$. The equation below shows that $\{x_n\}$ is a cauchy sequence because $|a_n|_p \to \infty$ as $n \to \infty$.

$$\begin{aligned}|a_n+1|_p &= |a_{n+1}x_n^{n+1}|_p = |f_{n+1}(x)-f_n(x)|_p \\ &= |f_{n+1}(x_n)|_p = \prod_{a\in S_{n+1}} \left|1-\frac{x_n}{a}\right|_p \\ &= \prod_{i=1}^{M}\left|1-\frac{x_n}{x_{n+1,i}}\right|_p = \prod_{i=1}^{M}|x_{n+1,i}-x_n|_p \\ &\geq |x_{n+1}-x_n|_p\end{aligned}$$

Suppose x is the limit of the sequence $\{x_n\}$. Then the following holds.

$$\begin{aligned}|f_n(x)|_p = |f_n(x)-f_n(x_n)|_p &= |x-x_n|_p\left|\sum_{k=1}^{n} a_k\frac{x^k-x_n^k}{x-x_n}\right|_p \\ &\leq |x-x_n|_p \to 0 \; as \; n\to\infty\end{aligned}$$

Since $F(x) = lim_{n\to\infty} f_n(x) = 0$, x is the root of the power series, proving the lemma. Notice that the general case follows directly from the base case. Let $b \in \mathbb{C}_p$ such that $ord_p b = m_1$. Define $G(x) = F(x/b)$. Then $G(x)$ satisfies the conditions for the base case of the proof. The analogous result holds for $F(x)$ as well. □

Lemma 2.19. *Let $F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ be a power series over $\mathbb{C}_p$ which converges and vanishes to 0 at $a \in \mathbb{C}_p$. Let $G(x) = \frac{F(x)}{1-x/a} = 1 + \sum_{k=1}^{\infty} b_k x^k$ be a power series over $\mathbb{C}_p$. Then $G(x)$ converges on $D(|a|_p)$.*

Proof. Let $f_n(x)$ be the n-th partial sum of $F(x)$. Notice that $G(x)$ can be obtained by multiplying $F(x)$ with the power series $\sum_{m=0}^{\infty} x^m/a^m$. This implies that for each n, $b_n = \sum_{j=0}^{n} \frac{a_j}{a^{n-j}} = \frac{f_n(a)}{a^n}$. Since $f(a) = 0$, we have $|b_n a^n|_p = |f_n(a)|_p \to 0$ as $n \to \infty$. □

We now prove Theorem 2.13.

Theorem 2.13. We prove the theorem by induction on N, the degree of the polynomial $h(x)$. Without loss of generality, assume $m = 0$. The general case for any value of m is analogous to the proof of Lemma 2.17 and Lemma 2.18.

Suppose $N = 0$. It suffices to show that the inverse power series of $F(x)$ is convergent and nonzero in $D(p^m)$. Let $G(x)$ be the inverse of $F(x)$. Assume for every n, $ord_p a_n > 0$. Observe that $ord_p a_n \to \infty$ as $n \to \infty$ because $F(x)$ converges in $D(1)$. Since $F(x)G(x) = 1$, $b_n = -\sum_{k=1}^{n} b_{n-k}a_k$, which shows that $ord_p b_n > 0$ for every n. Notice that $ord_p b_n \to \infty$ as $n \to \infty$. For fixed $C > 0$, choose c such that for all $n > c$, $ord_p a_n > C$. Denote $\epsilon = min(ord_p a_1, ord_p a_2, ..., ord_p a_c)$. We claim that for all $n > ic$, $ord_p b_n > min(C, i\epsilon)$, which proves the theorem for $N = 0$. We prove the theorem by by induction on i. The case in which $i = 0$ is trivial. Suppose the claim holds for $i-1$. Then from the sum $b_n = -\sum_{k=1}^{n} b_{n-k}a_k$, the terms $b_{n-k}a_k$ with $k > c$ have $ord_p(b_{n-k}a_k) \geq ord_p a_k > C$ while the terms $b_{n-k}a_k$ with $k \leq c$ have $ord_p(b_{n-k}a_k) \geq ord_p b_{n-k} + \epsilon > min(C, (i-1)\epsilon) + \epsilon$ by the induction hypothesis. Hence $ord_p b_n > min(C, i\epsilon)$.

Now suppose $N \geq 1$ and the theorem holds for $N-1$. Let $m_1 \leq m$ be the first slope of the Newton polygon of $F(x)$. By Lemma 2.18, there exists $a \in \mathbb{C}_p$ such that $F(a) = 0$ and $ord_p a = -m_1$. Consider the following power series over $\mathbb{C}_p$.

$$F_1(x) = \frac{F(x)}{1 - x/a} = 1 + \sum_{n=1}^{\infty} a'_n x^n$$

By Lemma 2.19, $F_1(x)$ converges on $D(p^{m_1})$. Let m'_1 be the first slope of the Newton polygon of $F_1(x)$. Suppose $m'_1 < m_1$. Then by Lemma 2.18, $F_1(x)$ has a root a' with $ord_p a' = -m'_1$. By the equation above, a' is also a root of $F(x)$. This is a contradiction to the base case $N = 0$. Hence $m'_1 \geq m_1$. By Lemma 2.17, the Newton Polygon of $F_1(x)$ is the same as that of $F(x)$ with the segment from $(0, 0)$ to $(1, m_1)$ subtracted. In fact, Lemma 2.17 implies that $F_1(x)$ also converges in $D(p^m)$ if the Newton polygon of $F(x)$ has m as the last slope. Notice that $F_1(x)$ satisfies the condition of the theorem with a total length of $N - 1$. By the induction hypothesis, there exist a polynomial $h_1(x) \in 1 + x\mathbb{C}_p[x]$ of degree $N - 1$ and a power series $G(x) \in 1 + x\mathbb{C}_p[[x]]$ which is convergent and nonzero on $D(p^m)$ such that $h_1(x) = F_1(x)G(x)$. Multiply both sides of the equation by $(1 - x/a)$ and set $h(x) = (1 - x/a)h_1(x)$ to derive $h(x) = F(x)G(x)$.

Notice that our choice of $h(x)$ is unique. Suppose there is another polynomial $h'(x)$ and a power series $G'(x)$ such that satisfy the conditions of the theorem. It suffices to show that $h(x)$ and $h'(x)$ have the same zeroes with the same multiplicities. We prove the claim by induction on the degree N. The base case in which $N = 1$ is trivial. Suppose the claim holds for $N - 1$. Without loss of generality, let $a \in \mathbb{C}_p$ be a root of $h(x)$ such that $ord_p a = -m$. Since $h(x)G(x) = h'(x)G'(x)$, a is also the root of $h'(x)$. In other words, we can divide both sides of the equation by $(1 - x/a)$. By Lemma 2.19, the equation reduces to a case with degree $N - 1$. □

2.3. **Overconvergent Power Series.** We now consider power series over $\mathbb{C}_p$ with n variables in the space of overconvergent power series. The results obtained from this subsection will be used for proving that the zeta function of a hypersurface is a quotient of two power series over $\mathbb{C}_p$, both of which converge everywhere.

Definition 2.20. Let $R = \mathbb{C}_p[[x_1, ..., x_n]]$ be the space of power series with n variables. Let W be the space of ordered n-tuples where each coordinate is a non-negative integer. Define the norm of an element $w = (w_1, ..., w_n) \in W$ as the sum of all coordinates of w, i.e. $|w| = \sum_{k=1}^{n} w_k$.

The above definition allows us to write any power series $G(x_1, ..., x_n) \in R$ as $G(x_1, ..., x_n) = G(x) = \sum_{w \in W} g_w x^w$ where for each $w = (w_1, ..., w_n)$, $x^w = x_1^{w_1} x_2^{w_2} ... x_n^{w_n}$ and $g_w \in \mathbb{C}_p$. We also abbreviate the n-tuple $(a_1, ..., a_n)$ as a if $a_i = a \in \mathbb{N}$ for every i. In this case the monomial x^a is an abbreviation of $x^a = x_1^a x_2^a ... x_n^a$.

Definition 2.21. The space of overconvergent power series R_0 is defined as follows.

$$R_0 = \{G(x) = \sum_{w \in W} g_w x^w \in R \mid \exists\, M > 0 \; such \; that \; \forall\, w \in W, ord_p g_w \geq M|w|\}$$

The definition implies that the power series in R_0 converges in some disk $D(r)$ that strictly contains $D(1)$. It is clear that R_0, closed under multiplication, is a subring of R. Notice that we can consider the space R_0 as an infinite vector space of $\mathbb{C}_p$ with the set of monomials $\{x^w\}_{w \in W}$ as the basis. This allows us to view any linear operator of R_0 as an infinite matrix, which motivates the definition of trace and determinant as follows.

Definition 2.22. Let $\phi : R_0 \to R_0$ be a linear operator on R_0. Suppose $A = \{a_{w,v}\}_{w,v\in W}$ is the infinite matrix of ϕ under the basis of monomials. Then the trace of A is defined as follows if the infinite sum converges.

$$Tr(A) = \sum_{w\in W} a_{w,w}$$

Let T be an independent variable. Then the matrix $(1-AT)$ is an infinite matrix with entries in $\mathbb{C}_p[T]$. Analogous to finite matrices, the determinant of $(1-AT)$ is defined as

$$det(1-AT) = \sum_{k=0}^{\infty} b_k T^k$$

where b_k is defined as follows.

$$b_k = (-1)^k \sum_{\substack{w_1,w_2,\ldots,w_k\in W \\ \sigma\in S_k}} \left(sgn(\sigma) \prod_{i=1}^{k} a_{w_i,\sigma(w_i)} \right)$$

Before we construct an operator which we will use in the first step of Dwork's proof, we define the following operators on R_0.

Definition 2.23. Let q be a positive integer. Then the translation operator $T_q : R_0 \to R_0$ is defined as follows where for any $w \in W$, $qw = (qw_1, qw_2, ..., qw_n)$.

$$T_q \left(\sum_{w\in W} g_w x^w \right) = \sum_{w\in W} g_{qw} x^w$$

Definition 2.24. Let $G(x)$ be a power series in R_0. The $G(x)$-multiplication operator $G : R_0 \to R_0$ is defined as multiplication by $G(x)$.

Definition 2.25. Let q be a positive integer and let $G(x)$ be a power series in R_0. Then the power series $G_q(x)$ is defined as $G_q(X) = G(x^q)$. We also define the operator $\psi_{q,G} = T_q \circ G$ where $F \circ G$ denotes the composition of power series $F(x)$ and $G(x)$ over $\mathbb{C}_p$.

Theorem 2.26. *Let q be a positive number and $G(x) = \sum_{w\in W} g_w x^w$ be a power series in R_0 with n variables. Let $\psi_{q,G} = T_q \circ G$ and let A be the infinite matrix of $\psi_{q,G}$ under the basis of monomials $\{x^w\}_{w\in W}$. Then the following holds for every positive integer s.*

1. *The trace $Tr(\psi^s_{q,G})$ exists.*
2. *$(q^s-1)^n Tr(\psi^s_{q,G}) = \sum_{\substack{x\in\mathbb{C}_p^n \\ x^{q^{s-1}}=1}} \prod_{j=0}^{s-1} G(x^{q^j})$*
3. *The determinant $det(1-AT)$ is a well defined power series in $\mathbb{C}_p$ with infinite radius of convergence.*
4. *$det(1-AT) = Exp_p\left(-\sum_{s=1}^{\infty} \frac{Tr(\psi^s_{q,G})T^s}{s}\right)$*

Proof. We first prove the theorem when $s = 1$. Observe that for any $u \in W$, the following holds.

$$\psi_{q,G}(x^u) = T_q(x^u G(x)) = T_q\left(\sum_{w\in W} g_w x^{w+u} \right) = \sum_{w\in W} g_{qw-u} x^w$$

Here if $qw-u$ is not in W, define $g_{qw-u}=0$. By the definition of the trace, $Tr(\psi_{q,G})=\sum_{w\in W} g_{qw-w}=\sum_{w\in W} g_{(q-1)w}$. Since $\psi_{q,G}\in R_0$, the series converges.

Observe that for each $i=1,2,...,n$ and w_i a non-negative integer, the following holds because each x_i is the $(q-1)$-th root of unity.

$$\sum_{\substack{x_i\in\mathbb{C}_p\\ x_i^{q-1}=1}} x_i^{w_i}=\begin{cases} q-1 & \text{if } q-1\mid w\\ 0 & \text{if } otherwise\end{cases}$$

Hence the following equation holds for any $w\in W$.

$$\sum_{\substack{x\in\mathbb{C}_p^n\\ x^{q^{s-1}}=1}} x^w=\prod_{i=1}^{n}\left(\sum_{x_i^{q-1}=1} x_i^{w_i}\right)=\begin{cases}(q-1)^n & \text{if } q-1\mid w_i \text{ for every } w_i\\ 0 & \text{if } otherwise\end{cases}$$

This implies the following, which proves the theorem for the base case.

$$\sum_{\substack{x\in\mathbb{C}_p^n\\ x^{q^{s-1}}=1}} G(x)=\sum_{w\in W} g_w \sum_{x^{q-1}=1} x^w=(q-1)^n\sum_{w\in W} g_{(q-1)w}=(q-1)^n Tr(\psi_{q,G})$$

Now suppose $s\geq 2$. Notice that the following equation holds.

$$G\circ T_q=T_q\circ G_q$$

For the LHS of the equation above, the following holds if $q\mid w$.

$$G\circ T_q(x^w)=G(x)x^{w/q}=\sum_{v\in W} g_v x^v+w/q=\sum_{v\in W} g_{v-w/q}x^v=\sum_{v\in W} g_{qv}x^{qv+w}$$

If not, then $G\circ T_q(x^w)=0$. For the RHS the following holds.

$$T_q\circ G_q(x^w)=T_q(\sum_{v\in W} g_v x^{qv+w})=\sum_{v\in W} g_{qv}x^{qv+w}$$

Hence the two operators $G\circ T_q$ and $T_q\circ G_q$ are equal to each other. This implies the following where $F\bullet G$ denotes the product of two power series $F(x)$ and $G(x)$ over $\mathbb{C}_p$.

$$\begin{aligned}\psi_{q,G}^s&=T_q\circ G\circ T_q\circ G\circ\psi_{q,G}^{s-2}=T_q\circ T_q\circ G_q\circ G\circ\psi_{q,G}^{s-2}\\ &=T_{q^2}\circ(G\bullet G_q)\circ\psi_{q,G}^{s-2}=T_{q^2}\circ(G\bullet G_q)\circ T_q\circ G\circ\psi_{q,G}^{s-3}\\ &=T_{q^3}\circ(G\bullet G_q)_q\circ G\circ\psi_{q,G}^{s-3}=T_{q^3}\circ(G\bullet G_q\bullet G_{q^2})\circ\psi_{q,G}^{s-3}\\ &=...=T_{q^s}\circ(G\bullet G_q\bullet...\bullet G_{q^{s-1}})=\psi_{q^s,G\bullet G_q\bullet...\bullet G_{q^{s-1}}}\end{aligned}$$

Applying the theorem for the base case $s=1$ proves (1) and (2).

Notice from the proof of statement (1), each entry $a_{i,j}$ of A is of form g_{qw-v} for $w,v\in W$. From the definition of $det(1-AT)$, we have the following.

$$\begin{aligned}ord_p\left(\prod_{i=1}^{k} a_{w_i,\sigma(w_i)}\right)&=ord_p\left(\prod_{i=1}^{k} g_{q\sigma(w_i)-w_i}\right)\geq M\sum_{i=1}^{k}|q\sigma(w_i)-w_i|\\ &\geq M\left(\sum_{i=1}^{k}|q\sigma(w_i)|-\sum_{i=1}^{k}|u_i|\right)=M(q-1)\sum_{i=1}^{k}|w_i|\end{aligned}$$

Notice $\frac{1}{k}ord_p b_k\to\infty$ as $k\to\infty$ because $\frac{1}{k}\sum_{i=1}^{k}|w_i|\to\infty$ as $k\to\infty$. Thus, the power series $det(1-AT)$ is well defined and has infinite radius of convergence.

We now prove statement (4) of the theorem. Let $A : R_0 \to R_0$ be a matrix with entries $\{a_{w,v}\}_{w,v\in W}$ such that $det(1 - AT)$ and $Tr(A^s)$ are well defined for all positive integers s. Let $\{A^{(m)}\}$ be a sequence of matrices with finite supports. For each m and for every $w, v \in W$, the set of entries $\{a^{(m)}_{w,v}\}_{w,v\in W}$ of the matrix $A^{(m)}$ is defined as $a^{(m)}_{w,v} = a_{w,v}$ or $a^{(m)}_{w,v} = 0$. We first show that statement (4) holds for all $A^{(m)}$. It suffices to show that the statement holds for any finite dimensional matrix $V = \{v_{ij}\}_{i,j=1,2,...,r}$. Notice we can assume V is an upper triangular matrix because there exists a change of basis such that V is upper triangular, such as the Jordan canonical forms. This implies that $det(1 - VT) = \prod_{i=1}^{r}(1 - v_{ii}T)$. Since $Tr(V^s) = \sum_{i=1}^{r} v_{ii}^s$, we have the following.

$$\begin{aligned} Exp_p\left(-\sum_{s=1}^{\infty}\sum_{i=1}^{r} v_{ii}^s T^s/s\right) &= \prod_{i=1}^{r} Exp_p\left(-\sum_{s=1}^{\infty}(v_{ii}T)^s/s\right) \\ &= \prod_{i=1}^{r} Exp_p(Log_p(1 - v_{ii}T)) \\ &= \prod_{i=1}^{r}(1 - a_{ii}T) = det(1 - VT) \end{aligned}$$

Now we return to the sequence of matrices $\{A^{(m)}\}$. By the aforementioned claim, for all m, $A^{(m)}$ satisfies the theorem. To prove that the theorem holds for A, it suffices to show the following.

(1) $\lim_{m\to\infty} det(1 - A^{(m)}T) = det(1 - AT)$
(2) $\lim_{m\to\infty} Tr((A^{(m)})^s) = Tr(A^s)$ for every positive integer s.

For each m, let $det(1 - A^{(m)}T) = \sum_{k=1}^{\infty} b_k^{(m)} T^k$ and $det(1 - AT) = \sum_{k=1}^{\infty} b_k T^k$. From the definition of the determinant, the following holds.

$$b_k^{(m)} = (-1)^k \sum_{\substack{w_1,w_2,...,w_k\in W \\ \sigma\in S_k}} \left(sgn(\sigma)\prod_{i=1}^{k} a^{(m)}_{w_i,\sigma(w_i)}\right)$$

Notice that the construction of $A^{(m)}$ implies that every product in the sum is 0 or equal to the term $sgn(\sigma)\prod_{i=1}^{k} a_{w_i,\sigma(w_i)}$ in b_k. For sufficiently large m, the term $sgn(\sigma)\prod_{i=1}^{k} a_{w_i,\sigma(w_i)}$ appears for any choice of $\sigma \in S_k$ and $w_1, w_2, ..., w_k$. Hence the first statement holds. The argument for the second statement is analogous. □

3. Rationality of Zeta Functions

Using the results obtained from the previous section on power series over $\mathbb{C}_p$, we will follow Dwork's proof of the rationality of zeta functions. In the first subsection we recall the definition of the zeta function and explore its properties. Next we prove that the zeta function is a quotient of two p-adic entire power series by constructing a suitable overconvergent power series in $\mathbb{C}_p$. We will then use these properties to show that the zeta function is rational.

3.1. **Zeta Functions over Finite Fields.**

We recall the definition of the zeta function of a hypersurface over a finite field. The following is a restatement of Definition 1.5.

Definition 3.1. Let $f(x_1, ..., x_n)$ be a polynomial with n variables over $\mathbb{F}_q$ for $q = p^r$ a power of p. Let H_f be the affine hypersurface of $f(x_1, ..., x_n)$. Then the zeta function of H_f is defined as follows, where $N_s = |H_f(\mathbb{F}_{q^s})|$ denotes the number of $\mathbb{F}_{q^s}$-points of H_f.

$$Z(H_f, T) = Exp_p\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right)$$

Example 3.2. We first calculate the zeta functions for some affine hypersurfaces.

(1) Let $\mathbb{A}^n_{\mathbb{F}_q}$ be the affine space over the finite field $\mathbb{F}_q$. For each s, $N_s = q^{ns}$. Hence the zeta function of the affine space is as follows.

$$Z(\mathbb{A}^n_{\mathbb{F}_q}, T) = Exp_p\left(\sum_{s=1}^{\infty} \frac{q^{ns}T^s}{s}\right) = Exp_p(-Log_p(1 - q^n T)) = \frac{1}{1 - q^n T}$$

(2) Let $\mathbb{P}^n_{\mathbb{F}_q}$ be the projective space over the finite field $\mathbb{F}_q$. Notice that the projective space $\mathbb{P}^n_{\mathbb{F}_q}$ is the union $\sqcup_{k=1}^n \mathbb{A}^k_{\mathbb{F}_q}$. Hence we have $N_s = \sum_{k=1}^n q^{ks}$ for each s. The zeta function of the projective space is a product of those of affine spaces, which is $Z(\mathbb{P}^n_{\mathbb{F}_q}, T) = \prod_{k=1}^n \frac{1}{1-q^k T}$.

(3) The equation $x_1x_2 + x_3x_4 - 1 = 0$ has $q^{3s} - q^s$ solutions over a finite field $\mathbb{F}_{q^s}$. Hence the zeta function of the hypersurface of the polynomial is $Z(H_f, T) = \frac{1-qT}{1-q^3T}$.

Using the examples, we can derive some properties of the zeta function.

Proposition 3.3. *Let H_f be an affine hypersurface over a finite field and let $Z(H_f, T)$ be the zeta function of the hypersurface. Then the following holds.*

(1) The coefficients of T^s in $Z(H_f, T)$ are at most q^{ns}.
(2) $Z(H_f, T)$ has coefficients in $\mathbb{Z}$.

Proof. From Example 3.2, the maximum value of N_s of a hypersurface is $q^{ns} = |\mathbb{A}^n_{\mathbb{F}_q}|$. Since the coefficients of $Z(H_f, T)$ are less or equal to those of $Z(\mathbb{A}^n_{\mathbb{F}_q}, T)$, the statement holds.

Order the $\mathbb{F}_{q^s}$-points $P = (x_1, x_2, ..., x_n)$ of H_f according to the least s such that all $x_i \in \mathbb{F}_{q^s}$. For $j = 1, 2, ..., s$, let $P_j = (x_{1,j}, ..., x_{n,j})$ be the conjugates of P where $P_1 = P$ and each $x_{i,j}$ is a conjugate of x_i over $\mathbb{F}_q$. Notice that all the points P_j are distinct. Suppose all x_i are fixed by $\sigma \in Gal(\mathbb{F}_{q^s}/\mathbb{F}_q)$. Then the point P should be in a fixed field of σ, which is a field smaller than $\mathbb{F}_{q^s}$. This is a contradiction.

We will now observe how each point $P_1, P_2, ..., P_s$ contributes to the terms of the zeta function $Z(H_f, T)$. Notice that for each j and for some r, P_j is an $\mathbb{F}_{q^r}$-point of H_f if $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^r}$, or $q^s \mid q^r$. Hence the point P_j contributes to N_{ks} for any positive integer k. The contributions the points $P_1, ..., P_s$ give to the zeta function are as follows.

$$Exp_p\left(\sum_{k=1}^{\infty} \frac{sT^{ks}}{ks}\right) = Exp_p(-Log_p(1 - T^s)) = \frac{1}{1 - T^s} = \sum_{k=0}^{\infty} T^{ks}$$

Extending the analogous argument for all possible s, we obtain that the zeta function is a product of the above series, which implies that the zeta function has integer coefficients. □

We recall the statement of the main theorem.

Theorem 3.4. *Let H_f be an affine hypersurface over a finite field and let $Z(H_f, T)$ be the zeta function of the hypersurface. Then $Z(H_f, T)$ is rational, i.e. a quotient of two polynomials with coefficients in $\mathbb{Q}$.*

Before we prove the theorem in subsequent sections, we first show that the theorem also holds for any affine variety over a finite field.

Corollary 3.5. *The zeta function of an affine variety over a finite field is rational.*

Proof. Let $f_1(x)$ and $f_2(x)$ be polynomials with n variables over $\mathbb{F}_q$. It suffices to show that if Dwork's theorem holds for hypersurfaces H_{f_1} and H_{f_2}, then it holds for the affine variety $H_{f_1,f_2} = \{x \in \mathbb{A}^n_{\mathbb{F}_q} | f_1(x) = f_2(x) = 0\}$. Notice that the following holds where $H_{f_1 f_2}$ is a hypersurface for the polynomial $f_1 f_2(x)$.

$$|H_{f_1,f_2}(\mathbb{F}_{q^s})| = |H_{f_1}(\mathbb{F}_{q^s})| + |H_{f_2}(\mathbb{F}_{q^s})| - |H_{f_1 f_2}(\mathbb{F}_{q^s})|$$

The above equation implies the following.

$$Z(H_{f_1,f_2}, T) = \frac{Z(H_{f_1}, T) Z(H_{f_2}, T)}{Z(H_{f_1 f_2}, T)}$$

Since all the power series on the RHS is rational, the power series in the LHS is rational. □

The analogous proof shows that Dwork's theorem also holds for a union of hypersurfaces over a finite field.

Corollary 3.6. *The zeta function of a union of hypersurfaces over a finite field is rational.*

3.2. **p-adic Meromorphic.** We first show that the zeta function of an affine hypersurface $Z(H_f, T)$ is p-adic meromorphic, meaning that it is a quotient of two power series with infinite radius of convergence.

Definition 3.7. Let $a \in \mathbb{F}_q$ such that $q = p^r$ for prime p. Then the Teichmüller representative t of a is an element of $\mathbb{C}_p$ which satisfies the following.

(1) t is a root of the equation $x^q - x = 0$.
(2) $t \equiv a \ mod \ p$

The existence and uniqueness of Teichmüller representatives follow from the following lemma whose proof is in Chapter 1 of Koblitz [1].

Theorem 3.8 (Hensel's Lemma)**.** *Let $f(x)$ be a polynomial over $\mathbb{Z}_p$ and let $f'(x)$ be the derivative of $f(x)$. Let a_0 be an element in $\mathbb{Z}_p$ such that $f(a_0) \equiv 0 \ mod \ p$ and $f'(a_0) \not\equiv 0 \ mod \ p$. Then there exists a unique element $a \in \mathbb{Z}_p$ such that the following holds.*

(1) $f(a) = 0$
(2) $a \equiv a_0 \ mod \ p$

The Teichmüller representatives allow us to extend any element in the finite field to an element in p-adic complex numbers. In fact, by the definition the representative is the uniformizer of the unramified field extension K of $\mathbb{Q}_p$. This implies two observations. One is that the p-adic ordinal of the Teichmüller representative is either 0 or 1. The other is that the trace of the element t is given by $Tr_K(t) = \sum_{i=0}^{r-1} t^{p^i}$. Notice that we have $\zeta_p^{Tr(a)} = \zeta_p^{Tr_K(t)}$ because the trace of t satisfies $Tr_K(t) \equiv \sum_{i=0}^{r-1} a^{p^i} = Tr(a) \ mod \ p$.

Definition 3.9. Let $\theta(T)$ be a power series over $\mathbb{C}_p$ with the following construction.

$$\theta(T) = F(T, \zeta_p - 1) = \sum_{n=0}^{\infty} \left(\sum_{m=n}^{\infty} a_{m,n}(\zeta_p - 1)^m \right) T^n = \sum_{n=0}^{\infty} a_n T^n$$

In the equation above, $F(x, y)$ is the power series from Definition 2.7 and ζ_p is a primitive p-th root of unity. The coefficient a_n is the sum $\sum_{m=n}^{\infty} a_{m,n}(\zeta_p - 1)^m$ for each n.

Lemma 3.10. *The power series $\theta(T)$ converges in the disk $D(p^{\frac{1}{p-1}}-)$.*

Before we prove the lemma, we state the analogue of Eisenstein's criterion for a polynomial over $\mathbb{Z}_p$, the proof of which is similar to that of Eisenstein's criterion for a polynomial over $\mathbb{Z}$.

Theorem 3.11 (Eisenstein's Criterion)**.** *Let $f(x) = a_n x^n + ... + a_1 x + a_0$ be a polynomial over $\mathbb{Z}_p$. Suppose the following conditions hold.*

(1) $a_i \equiv 0$ mod p for $i = 0, 1, ..., n-1$.
(2) $a_n \not\equiv 0$ mod p.
(3) $a_0 \not\equiv 0$ mod p^2.

Then the polynomial $f(x)$ is irreducible over $\mathbb{Q}_p$.

Lemma 3.10. We first show that $ord_p(\zeta_p - 1) = \frac{1}{p-1}$. Observe that $\zeta_p - 1$ is a root of the polynomial $f(x) = x^{p-1} + \sum_{n=1}^{p-1} \binom{p}{n} x^{p-1-n}$ because $(1 + \zeta_p - 1)^p = 1$. By Theorem 3.11, $f(x)$ is irreducible. This shows that the field extension $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\zeta_p - 1)$. Let $G = Gal(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$. Notice that the Galois conjugates of $\zeta_p - 1$ are $\zeta_p^i - 1$ for $i = 1, 2, ..., p-1$. Since the p-adic norm is invariant under the action of the Galois group G, we have $|\zeta_p - 1|_p = |\zeta_p^i - 1|_p$. From cyclotomic polynomials, we have $\sum_{n=0}^{p-1} x^n = \prod_{i=1}^{p-1}(x - \zeta_p^i)$. Substituting $x = 1$ gives $\prod_{i=1}^{p-1}(1 - \zeta_p^i) = p$, which implies $|\zeta_p^i - 1|_p = |p|_p^{\frac{1}{p-1}} = p^{-\frac{1}{p-1}}$.

From Proposition 2.10, the power series $F(x, y)$ has all its coefficients in $\mathbb{Z}_p$. This implies that $|a_{m,n}|_p \leq 1$ for all $m \geq n$. The above claim and the proposition shows that for all the coefficients a_n of $\theta(T)$, $ord_p a_n \geq \frac{n}{p-1}$. Hence $\theta(T)$ converges in the disk $D(p^{\frac{1}{p-1}}-)$. □

The lemma above shows that the power series $\theta(T)$ converges in a disk strictly bigger than $D(1)$. Recall that the Teichmüller representative has p-adic ordinal of 1 or 0. This allows us to evaluate the power series $\theta(T)$ at $T = t^{p^i}$ for any $i = 0, 1, ..., r-1$, where t is the Teichmüller representative of an element $a \in \mathbb{F}_q$. Using the Teichmüller representative, we prove the following lemma. The lemma gives an insight to understanding the sum of a set of p-th roots of unity, which appears in the first step of the proof of Dwork's theorem.

Lemma 3.12. *Let $a \in \mathbb{F}_q$ with $q = p^r$ and let $t \in \mathbb{C}_p$ be the Teichmüller representative of a. Let ζ_p be a primitive p-th root of unity. Then the following holds.*

$$\zeta_p^{Tr(a)} = \prod_{k=0}^{r-1} \theta(t^{p^k})$$

Proof. Observe that the following holds for any independent variable Y because $t^{p^r} = t$ and the telescoping sum in the power of $(1 + Y^{p^i})$ is 0.

$$\begin{aligned}\prod_{i=0}^{r-1} F(t^{p^i}, Y) &= (1+Y)^{t+t^p+\ldots+t^{p^{r-1}}} \prod_{i=1}^{\infty}(1+Y^{p^i})^{\frac{t^{p^i}-t^{p^{i-1}}+t^{p^{i+1}}-t^{p^i}+\ldots+t^{p^{r+i}}-t^{p^{r+i-1}}}{p^i}} \\ &= (1+Y)^{t+t^p+\ldots+t^{p^{r-1}}} \prod_{i=1}^{\infty}(1+Y^{p^i})^{\frac{t^p-t+t^{p^2}-t^p+\ldots+t^{p^r}-t^{p^{r-1}}}{p^i}} \\ &= (1+Y)^{t+t^p+\ldots+t^{p^{r-1}}}\end{aligned}$$

Substituting $Y = \zeta_p - 1$ gives the desired equation. □

Definition 3.13. Let $f(x_1, x_2, ..., x_n) = \sum_{i=0}^{M} b_i x^{u_i}$ be a polynomial over the field $\mathbb{F}_{q^s}$ where u_i is an n-tuple of non-negative integers and $q = p^r$ for prime p. Let x_0 be an independent variable in $\mathbb{F}_{q^s}$. Let $F(x_0, x_1, ..., x_n) = \sum_{i=0}^{M} a_i x^{w_i}$ be a polynomial over $\mathbb{C}_p$ where each a_i is the Teichmüller representative of b_i and $w_i = (1, u_i)$ is an $(n+1)$-tuple of non-negative integers. In other words, $F(x_0, x_1, ..., x_n)$ is a polynomial induced from $x_0 f(x_1, ..., x_n)$ by changing each coefficient to its teichmüller representative.

Denote $G(x)$ as a power series over $\mathbb{C}_p$ which is defined as follows.

$$G(x) = \prod_{i=0}^{M}\prod_{k=0}^{r} \theta(a_i^{p^k} x^{p^k w_i})$$

Lemma 3.14. *$G(x)$ is an overconvergent power series over $\mathbb{C}_p$*

Proof. Since the space of overconvergent power series R_0 is a subring of the space of power series in $\mathbb{C}_p$, it suffices to show that each factor $\theta(a_i^{p^k} x^{p^k w_i})$ is an overconvergent power series.

From the definition of $\theta(T) = \sum_{n=0}^{\infty} b_n T^n$, $\theta(a_i^{p^k} x^{p^k w_i}) = \sum_{n=0}^{\infty} b_n a_i^{np^k} x^{np^k w_i}$ for each i and k. Since each a_i is the Teichmüller representative, we have the following.

$$|b_n a_i^{np^k}|_p = |b_n|_p \leq p^{-\frac{n}{p-1}} \leq p^{-N|nw_i|}$$

where $N = min_{i=0,1,\ldots,M} \frac{1}{(p-1)|w_i|}$. Hence the power series $\theta(a_i^{p^k} x^{p^k w_i}) \in R_0$. □

Using the derivation of the power series $G(x)$ and the remark from the introduction, we prove that the zeta function is p-adic meromorphic.

Theorem 3.15. *Let p be a prime number and $f(x_1, ..., x_n) = \sum_{i=0}^{M} b_i x^{u_i}$ be a polynomial over $\mathbb{F}_q$ with n variables where $q = p^r$ and u_i is an n-tuple of non-negative integers for each i. Then the zeta function $Z(H_f, T)$ of an affine hypersurface H_f over $\mathbb{F}_q$ is p-adic meromorphic.*

Proof. We prove the theorem by induction on the number of variables n. The base case where $n = 0$ is trivial. Suppose the theorem holds for $n - 1$ variables. Let N'_s be the number of $\mathbb{F}_{q^s}$-points $(x_1, x_2, ..., x_n)$ of H_f such that all the coordinates are non-zero. This is same as the number of $\mathbb{F}_{q^s}$-points of H_f such that all the coordinates satisfy $x_i^{q^s-1} = 1$. Define $Z'(H_f, T) = Exp_p\left(\sum_{s=1}^{\infty} \frac{N'_s T^s}{s}\right)$. Then the

following equation holds.

$$Z'(H_f,T)Exp_p\left(\sum_{s=1}^{\infty}\frac{(N_s-N'_s)T^s}{s}\right)=Z(H_f,T)$$

Observe that the expression $Exp_p\left(\sum_{s=1}^{\infty}\frac{(N_s-N'_s)T^s}{s}\right)$ corresponds to the zeta function of a union of n affine varieties H_i where each H_i is defined by two equations: $f(x_1,...,x_n)=0$ and $x_i=0$. Since each H_i is an affine hypersurface of a polynomial with at most $n-1$ variables, the induction hypothesis and Collorary 3.6 imply that the expression is p-adic meromorphic. Hence it suffices to show that $Z'(H_f,T)$ is p-adic meromorphic.

We first derive an expression for N'_s for each s. Let a be an element in $\mathbb{F}_{q^s}$ and t be the Teichmüller representative of a. Then Lemma 3.12 implies the following equation.

$$\zeta_p^{Tr(a)}=\prod_{k=0}^{rs-1}\theta(t^{p^k})$$

Since ζ_p is a primitive p-th root of unity, the following holds for $u\in\mathbb{F}_{q^s}$.

$$\sum_{x_0\in(\mathbb{F}_{q^s})^\times}\zeta_p^{Tr(x_0u)}=\begin{cases}-1 & \text{if } u\in(\mathbb{F}_{q^s})^\times\\ q^s-1 & \text{if } u=0\end{cases}$$

Substitute $u=f(x_1,x_2,...,x_n)$ and sum the expression over all the variables $x_1,x_2,...,x_n\in(\mathbb{F}_{q^s})^\times$.

$$\begin{aligned}\sum_{x_0,x_1,...,x_n\in(\mathbb{F}_{q^s})^\times}\zeta_p^{Tr(x_0f(x_1,x_2,...,x_n))}&=N'_s(q^s-1)+((q^s-1)^n-N'_s)(-1)\\&=N'_sq^s-(q^s-1)^n\end{aligned}$$

Let $F(x_0,x_1,...,x_n)=\sum_{i=0}^{M}a_ix^{w_i}$ be a polynomial over $\mathbb{C}_p$ such that each a_i is the Teichmüller representative of the corresponding coefficient b_i of the polynomial $x_0f(x_1,...,x_n)$. For each i, $w_i=(1,u_i)$ where w_i is an $(n+1)$-tuple of non-negative integers. This gives an expression for N'_s for all s by Lemma 3.12.

$$\begin{aligned}q^sN'_s&=(q^s-1)^n+\sum_{x_0,x_1,...,x_n\in(\mathbb{F}_{q^s})^\times}\zeta_p^{Tr(x_0f(x_1,x_2,...,x_n))}\\&=(q^s-1)^n+\sum_{\substack{x_0,x_1,...,x_n\in\mathbb{C}_p\\ x_i^{q^{s-1}}=1\ for\ all\ i}}\prod_{i=1}^{M}\prod_{k=0}^{rs-1}\theta(a_i^{p^k}x^{p^kw_i})\end{aligned}$$

As in Definition 3.13, define the power series $G(x)$ over $\mathbb{C}_p$ as follows.

$$G(x)=\prod_{i=0}^{M}\prod_{k=0}^{r}\theta(a_i^{p^k}x^{p^kw_i})$$

By definition, the following expression for N'_s also holds.

$$q^sN'_s=(q^s-1)^n+\sum_{\substack{x_0,x_1,...,x_n\in\mathbb{C}_p\\ x_i^{q^{s-1}}=1\ for\ all\ i}}\prod_{j=0}^{s-1}G(x^{q^j})$$

By Lemma 3.14, $G(x)$ is an overconvergent power series over $\mathbb{C}_p$. Consider the operator $\psi_{q,G} = T_q \circ G$ where T_q is the translation operator and G is the multiplication operator by $G(x)$. By Theorem 2.26, the operator $\psi_{q,G}$ satisfies the following equation.

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

This gives the following expression for the zeta function $Z'(H_f, T)$.

$$Z'(H_f,T) = Exp_p\left(\sum_{s=1}^{\infty} \frac{(q^s-1)^n T^s}{sq^s}\right)\ Exp_p\left(\sum_{s=1}^{\infty} \frac{(q^s-1)^{n+1} Tr(\psi^s_{q,G}) T^s}{sq^s}\right)$$

The first factor on the RHS reduces as follows, which is clearly p-adic meromorphic.

$$\begin{aligned}
Exp_p\left(\sum_{s=1}^{\infty} \frac{(q^s-1)^n T^s}{sq^s}\right) &= Exp_p\left(\sum_{s=1}^{\infty}\sum_{i=0}^{n} (-1)^i \binom{n}{i} q^{s(n-1-i)} T^s/s\right) \\
&= \prod_{i=0}^{n} Exp_p\left((-1)^i \binom{n}{i} \sum_{s=1}^{\infty} q^{s(n-1-i)} T^s/s\right) \\
&= \prod_{i=0}^{n} Exp_p\left(-Log_p(1-q^{n-i-1}T)^{(-1)^i \binom{n}{i}}\right) \\
&= \prod_{i=0}^{n} (1-q^{n-i-1}T)^{(-1)^i \binom{n}{i}}
\end{aligned}$$

The second factor on the RHS reduces as follows. In the equation below, A is an infinite matrix of the operator $\psi_{q,G} = T_q \circ G$ under the basis of monomials.

$$\begin{aligned}
&Exp_p\left(\sum_{s=1}^{\infty} \frac{(q^s-1)^{n+1} Tr(\psi^s_{q,G}) T^s}{sq^s}\right) \\
&= Exp_p\left(\sum_{s=1}^{\infty}\sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} q^{s(n-i)} Tr(\psi^s_{q,G}) T^s/s\right) \\
&= \prod_{i=0}^{n+1} Exp_p\left(\sum_{s=1}^{\infty} (-1)^i \binom{n+1}{i} Tr(q^{s(n-i)} \psi^s_{q,G}) T^s/s\right) \\
&= \prod_{i=0}^{n+1} det\left(1 - A(q^{n-i}T)\right)^{(-1)^{i+1}\binom{n+1}{i}}
\end{aligned}$$

By Theorem 2.26, for each $i = 0, 1, ..., n+1$ the term $det\left(1 - A(q^{n-i}T)\right)$ is a power series over $\mathbb{C}_p$ with infinite radius of convergence. This shows that the second factor on the RHS is also p-adic meromorphic. Hence $Z'(H_f, T)$ is an alternating product of p-adic power series with infinite radius of convergence. Thus $Z'(H_f, T)$ is p-adic meromorphic, which implies that the zeta function $Z(H_f, T)$ is p-adic meromorphic. □

3.3. **Rationality.** We first prove the following lemma which we will use to show the rationality of the zeta function.

Lemma 3.16. *Let $F(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series over $\mathbb{C}_p$. Let $A_{s,m} = \{a_{s+i+j}\}_{0 \le i,j \le m}$ be the matrix as follows.*

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{pmatrix}$$

Then $F(x)$ is a quotient of two polynomials over $\mathbb{C}_p$ if and only if there exist integers $m \ge 0$ and S such that $det(A_{s,m}) = 0$ whenever $s \ge S$.

Proof. Suppose $F(x)$ is a quotient of two polynomials $F(x) = P(x)/Q(x)$ such that $P(x) = \sum_{k=0}^{M} p_k x^k$ and $Q(x) = \sum_{k=0}^{N} q_k x^k$. Equating the coefficients of x^i for $i > max(M, N)$ gives the following.

$$\sum_{l=0}^{N} a_{i-N+l} c_{N-l} = 0$$

Let $S = max(M - N + 1, 1)$ and $m = N$. Then if $s \ge S$, the following equation holds, which shows that $det(A_{s,N}) = 0$ for every $s \ge S$.

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+N} \\ a_{s+1} & a_{s+2} & \cdots & a_{s+N+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+N} & a_{s+N+1} & \cdots & a_{s+2N} \end{pmatrix} \begin{pmatrix} c_N \\ c_{N-1} \\ \vdots \\ c_0 \end{pmatrix} = 0$$

Now suppose there exist S and m such that for $s \ge S$, $det(A_{s,m}) = 0$. Choose the smallest m such that the property $det(A_{s,m}) = 0$ holds for all sufficiently large s. We first show that $det(A_{s,m-1}) \neq 0$ for all $s \ge S$. Assume not. Then some linear combination of the rows $r_0, r_1, ..., r_{m-1}$ of the matrix $A_{s,m}$ vanish, except possibly for the last column. Let r_k be the first row which has non-zero coefficient in the linear combination. In other words, $r_k = a_{k+1} r_{k+1} + a_{k+2} r_{k+2} + ... + a_{m-1} r_{m-1}$ except possibly at the last column. Through row operations we can replace the k-th row r_k by $r_k - a_{k+1} r_{k+1} + a_{k+2} r_{k+2} + ... + a_{m-1} r_{m-1}$. If $k > 0$ then the matrix is of the following form.

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+m-1} & a_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & a_{s+m} & a_{s+m+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m-1} & a_{s+2m} \end{pmatrix}$$

Then the matrix $A_{s+1,m-1}$ with the first row from a_{s+1} to a_{s+N} has determinant 0. The case for $k = 0$ analogously follows. This implies that $det(A_{s',m-1}) = 0$ for all $s' \ge s$ by induction on s, a contradiction to our choice of m as the minimal integer satisfying the condition.

Now we have for all $s \ge S$, $det(A_{s,m}) = 0$ while $det(A_{s,m-1}) \neq 0$. This shows that there exists a linear combination of rows of the matrix $A_{S,m}$ such that the coefficient of the last row of the matrix is non-zero. In other words, the last row of

the matrix $A_{S,m}$ is a linear combination of the other m rows. Hence any solution $(u_0, u_1, ...u_m)$ to the systems of equations

$$\begin{pmatrix} a_S & a_{S+1} & \cdots & a_{S+N} \\ a_{S+1} & a_{S+2} & \cdots & a_{S+N+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{S+N} & a_{S+N+1} & \cdots & a_{S+2N} \end{pmatrix} \begin{pmatrix} u_m \\ u_{m-1} \\ \vdots \\ u_0 \end{pmatrix} = 0$$

is also a solution to the following equation.

$$a_{S+m}u_m + a_{S+m+1}u_{m-1} + ... + a_{S+2m}u_0 = 0$$

By induction on s, for every $s \geq S$, $(u_0, u_1, ...u_m)$ is a solution of the following equation.

$$a_s u_m + a_{s+1}u_{m-1} + ... + a_{s+m}u_0 = 0$$

This implies that the product of the power series $F(x)$ and a polynomial of degree m with coefficients u_i is a polynomial of degree less than $S + m$. □

The lemma implies that a power series over $\mathbb{C}_p$ with repeating coefficients for every sufficiently large index should be a quotient of two polynomials over $\mathbb{C}_p$. We finally prove the rationality of the zeta functions using the lemma.

Theorem 3.17. *The zeta function $Z(H_f, T)$ of an affine hypersurface H_f over a finite field $\mathbb{F}_q$ is rational.*

Proof. From Theorem 3.15, the function $Z(H_f, T)$ is a quotient of two power series over $\mathbb{C}_p$ with infinite radius of convergence, i.e. $Z(H_f, T) = A(T)/G(T)$. Let R be an integer $R = q^{4n} > q^n$ where n is the dimension of the hypersurface H_f. Then the power series $G(T)$ converges in the disk $D(R)$. By Theorem 2.13, there exist a polynomial $P(T) \in 1 + T\mathbb{C}_p[T]$ and a power series $B(T) \in 1 + T\mathbb{C}_p[[T]]$ which converges in $D(R)$ such that $G(T) = P(T)/B(T)$. Denote $F(T) = A(T)B(T)$ which converges on $D(R)$. This gives $Z(H_f, T)P(T) = F(T)$, which also implies that $F(T) \in 1 + T\mathbb{C}_p[[T]]$.

Let $Z(H_f, T) = \sum_{i=0}^{\infty} z_i T^i$, $P(T) = \sum_{i=0}^{N} p_i T^i$ and $F(T) = \sum_{i=0}^{\infty} f_i T^i$. By Proposition 3.3, for each i, $|z_i| \leq q^{in}$. Since $F(T)$ converges in $D(R)$, for i sufficiently large, $|f_i|_p \leq R^{-i} = q^{-4ni}$.

Let m be a fixed integer such that $m > 2N$ where N is the degree of the polynomial $P(T)$. Define the matrix $A_{s,m} = \{z_{s+i+j}\}_{0 \leq i,j \leq m}$ as in Lemma 3.14. We claim that for the fixed integer m, $det(A_{s,m}) = 0$ for sufficiently large s.

From the equation $Z(H_f, T)P(T) = F(T)$, we have the following equation for the coefficient of the term T^{j+N} for each $j = 0, 1, ..., m$.

$$\sum_{i=0}^{N} z_{j+N-i}p_i = f_{j+N}$$

Consider the matrix $A_{s,m}$ with the following column operation implied by the equation above. For each $(j + N)$th column, add the linear combination of $j, (j + 1), ..., (j + N - 1)$ columns with the corresponding coefficient, i.e. the $(j + N - i)$th column has p_i as the corresponding coefficient. This allows to change the entries of the matrix $A_{s,m}$ such that the first N columns are the same as the original matrix $A_{s,m}$ and the rest of the columns are replaced by the corresponding coefficients f_i. Note that the determinant of the matrix does not

change. By Proposition 3.3, $|z_i|_p \leq 1$. Hence, the following holds because $R = q^{4n}$ and $m > 2N$.

$$|det(A_{s,m})|_p \leq (max_{i \geq s+N} |f_i|_p)^{m+1-N} < R^{-s(m+1-N)} < q^{-2ns(m+2)}$$

The following also holds under the euclidean norm.[1]

$$\begin{aligned} |det(A_{s,m})| &\leq \sum_{\sigma \in S_{m+1}} \prod_{i=0}^{m} |z_{s+i+\sigma(i)}| \leq (m+1)!\, q^{2n \sum_{k=0}^{m}(s+k)} \\ &= (m+1)!\, q^{n(m+1)(2s+m)} = (m+1)!\, q^{2ns(m+1)} q^{nm(m+1)} \end{aligned}$$

Comparing the p-adic norm with the euclidean norm gives the following equation.

$$\begin{aligned} |det(A_{s,m})||det(A_{s,m})|_p &< \frac{q^{2ns(m+1)}}{q^{2ns(m+2)}}\, (m+1)!\, q^{nm(m+1)} \\ &= \frac{(m+1)!\, q^{nm(m+1)}}{q^{2ns}} \to 0 \; as \; s \to \infty \end{aligned}$$

Observe that the value $det(A_{s,m})$ is a non-negative integer because $Z(H_f, T)$ has integer coefficients. Hence for sufficiently large s, $det(A_{s,m}) = 0$. By Lemma 3.16, the zeta function $Z(H_f, T)$ is a quotient of two polynomials over $\mathbb{C}_p$. □

So far we have focused on proving that the zeta functions of affine varieties over finite fields are rational. The question then arises as to whether there is an equivalent construction of the zeta function over any field other than the finite field.

Definition 3.18. The nth symmetric power of an affine variety V is the quotient of the natural group action of S_n on V^n. Denote the nth symmetric power of the variety as $Sym^n(V)$.

In fact, if X is an affine variety over $\mathbb{F}_p$, $Sym^n(X)$ is also an affine variety over $\mathbb{F}_p$. This allows us to consider the $\mathbb{F}_{p^s}$-points of $Sym^n(X)$. We will denote the set of these points as $Sym^n(X)(\mathbb{F}_{p^s})$.

We end the paper with the following theorem, the proof of which is in Chapter 7 and Appendix A of Mustata [6]. The concepts needed for understanding the proof is in Chapter 1 and 2 of Hartshorne [7]. The theorem hints the construction of the zeta function of a variety over any perfect field. The formal definition of the extended zeta function over a perfect field is in Kapranov [5] and Chapter 7 of Mustata [6]. The definition of the extended zeta function for any perfect field is out of scope of this paper.

Theorem 3.19. *Let X be an affine variety over $\mathbb{F}_p$ defined by the polynomials $f_1, f_2, ..., f_m \in \mathbb{F}_p[x_1, x_2, ..., x_n]$. Then the following two constructions of the zeta functions are equivalent, where N_s is the number of $\mathbb{F}_{p^s}$-points of X for each s.*

(1) $Z(X,T) = Exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s\right)$
(2) $Z(X,T) = \sum_{s=1}^{\infty} |Sym^s(X)(\mathbb{F}_p)|\, T^s$

[1]There is an error with the estimate in p.128 of Koblitz[1].

Acknowledgments. It is a great pleasure to thank my mentor, Joel Specter, for patiently guiding me through the material and giving me valuable feedback on writing the paper. I also thank my mentor Subhadip Chowdhury for giving me valuable advice on editing the paper. Lastly, I sincerely thank Professor Peter May for organizing the REU and for giving me this wonderful opportunity to delve in mathematics.

References

[1] Dwork, Bernard. "On the Rationality of the Zeta Function of an Algebraic Variety" *American Journal of Mathematics* 82, no.3 (1960): 631-48.
[2] Koblitz, Neal. "P-adic Numbers, P-adic Analysis, and Zeta Functions" New York: Springer-Verlag, 1980.
[3] Serre, Jean-Pierre. "Local Fields" New York: Springer, 1979.
[4] Neukirch, Jurgen. "Algebraic Number Theory" Berlin: Springer-Verlag, 1999.
[5] Kapranov, Mikhail. "The Elliptic Curve in the S-Duality Theory and Eisenstein Series for Kac-Moody Groups" Preprint: arXiv:math/0001005v2, 2000: http://arxiv.org/pdf/math/0001005v2.pdf
[6] Mustata, Mircea. "Zeta Functions in Algebraic Geometry" Lecture Notes, Unpublished: http://www.math.lsa.umich.edu/ mmustata/zeta_book.pdf
[7] Hartshorne, Robin. "Algebraic Geometry" New York: Springer, 1977.