Applications of Generalized Fermat Varieties to Zeta Functions of Artin-Schreier Curves

by

Alexander Mueller

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2013

Doctoral Committee:

Professor Michael E. Zieve, Chair
Professor Kevin J. Compton
Professor Jeffrey C. Lagarias
Professor Mircea Immanuel Mustata
Assistant Professor Dani Neftin

ACKNOWLEDGEMENTS

I would like to thank my adviser Michael Zieve for teaching me to fish. I would like to thank Jeffrey Lagarias for helpful feedback in writing this thesis. I would like to thank my family (Peter, Susan, and Holly), my beautiful girlfriend Becky, and the community of Michigan graduate students for keeping me sane.

TABLE OF CONTENTS

CHAPTER I

Introduction

1.1 Generalities

In this thesis we study the arithmetic of Artin-Schreier curves, a certain class of curves (defined over finite fields) that are associated with equations of the form $y^q - y = f(x)$. We will define a curve to be an algebraic set (as defined on pages 2 and 9 of [12]) of which every irreducible component has dimension 1. In what follows, we will fix $q = p^N$ a power of a prime p.

Definition I.1 (Artin-Schreier Curves)**.** We define an *affine Artin-Schreier curve* to be an affine plane curve defined over $\mathbb{F}_q$ by a polynomial with the form $y^q - y - f(x)$ for some non-constant $f(x) \in \mathbb{F}_q[x]$. We define a *complete Artin-Schreier curve* to be a smooth, complete model of a geometrically irreducible affine Artin-Schreier curve.

Note that we permit an *affine* Artin-Schreier curve to be reducible (notably in Theorem I.11). Now fix a non-constant $f \in \mathbb{F}_q[x]$ of degree d with $(d, q) = 1$. Let $U_{f,q}$ denote the affine Artin-Schreier curve defined the equation $y^q - y = f(x)$. When $U_{f,q}$ is geometrically irreducible, let $X_{f,q}$ denote the associated complete Artin-Schreier curve. The results of this thesis deal primarily with the number of $\mathbb{F}_{q^n}$ points on our affine Artin-Schreier curve

$$M_{f,q,n} := |U_{f,q}(\mathbb{F}_{q^n})| = |\{(s,t) \in (\mathbb{F}_{q^n})^2 : t^q - t - f(s) = 0\}|$$

and the zeta function

$$Z(X_{f,q}, T) := \exp(\sum_{n\geq 1} |X_{f,q}(\mathbb{F}_{q^n})| \frac{T^n}{n})$$

of $X_{f,q}$. Note that $|X_{f,q}(\mathbb{F}_{q^n})| = M_{f,q,n} + 1$ (see Section 2.2.1) and we study $M_{f,q,n}$ instead of $|X_{f,q}(\mathbb{F}_{q^n})|$ to provide simplicity to the statements of some of our results. To count these integers, we will use the fact that the $\mathbb{F}_{q^n}$-rational points of $U_{f,q}$ are exactly the fixed points of the *Frobenius automorphism.*

Let F denote the automorphism of $U_{f,q}$ given by applying the q-th power map to each coordinate

$$(s, t) \mapsto (s^q, t^q). \tag{1.1}$$

We will refer to this map as the *Frobenius automorphism.* It is most tangibly defined on $U_{f,q}$ and it is easiest to see that it is an automorphism in this case. Suppose that (s_0, t_0) is a point of $U_{f,q}(\mathbb{F}_{q^n})$, so that

$$t_0^q - t_0 - f(s_0) = 0.$$

Note that as we have assumed $f \in \mathbb{F}_q[x]$, it follows that

$$0 = (t_0^q - t_0 - f(s_0))^q = (t_0^q)^q - t_0^q - f(s_0^q).$$

In Section 2.2.1 we will extend F to an automorphism of $X_{f,q}$, which we will also denote F and refer to as the Frobenius automorphism. We are interested in this automorphism because the $\mathbb{F}_{q^n}$-rational points of $X_{f,q}$ are the fixed points of F^n. This is easiest to see for an affine Artin-Schreier curve $U_{f,q}$, as s and t are both fixed by the q^n-th power map exactly when they both lie in $\mathbb{F}_{q^n}$. The benefit of recasting our problem in terms of the fixed points of an automorphism is related to certain connections with algebraic topology that can be best illustrated via a historical survey.

After E. Artin's 1921 Ph.D. thesis on algebraic function fields of hyperelliptic curves (see [2] [3]), F. K. Schmidt proved in 1926 (see [28]) that, for *any* smooth, projective, geometrically irreducible genus g_0 curve C over $\mathbb{F}_q$, there are complex numbers $\pi_1, ..., \pi_{2g_0}$ such that $\prod_i (x - \pi_i)$ is in $\mathbb{Z}[x]$ and such that for any positive integer n

$$|C(\mathbb{F}_{q^n})| = (q^n + 1) - \sum_i (\pi_i)^n. \tag{1.2}$$

Then H. Hasse (for $g_0 = 1$ in 1936 [13]) and A. Weil (for arbitrary g_0 in 1948 [32]) proved the "Riemann hypothesis for curves over finite fields," namely that $|\pi_i| = \sqrt{q}$. One consequence is Weil's bound. By Schmidt's theorem above, we have that

$$||C(\mathbb{F}_{q^n})| - (q^n + 1)| = |\sum_{i=1}^{2g_0} (\pi_i)^n|.$$

The triangle inequality implies that the right-hand side is

$$\leq \sum_{i=1}^{2g_0} |(\pi_i)^n| = 2g_0 q^{n/2}.$$

This yield the Weil bound:

$$||C(\mathbb{F}_{q^n})| - (q^n + 1)| \leq 2g_0 q^{n/2}.$$

This work was motivated by the analogy between number fields and function fields over finite fields. In the 1940s, Weil discovered an analogy between function fields over finite fields and function fields over the complex numbers, and via an analogue of the Lefschetz fixed point theorem from algebraic topology he gave a geometric interpretation of the π_i as the eigenvalues of the Frobenius operator on Abelian varieties (see [33]). Weil also conjectured generalizations of these results to arbitrary varieties, which were later proved by the combined efforts of many mathematicians. In particular, work on Weil's conjectures led to the development of

ℓ-adic étale cohomology (by Artin, Grothendieck, Serre, and others) and culminated in Deligne's 1974 proof of the analogue of the Riemann hypothesis for varieties over finite fields. Note that below we will discuss this cohomology theory but treat it as a black box; we will discuss its definition and properties in more detail in Section 3.2.1.

In this thesis, we will employ this ℓ-adic étale cohomology theory (for $\ell \neq p$) and study the fixed points of F via the Lefschetz fixed point theorem. This theorem states that

$$\mathrm{Fix}(F^n|X_{f,q}) = \sum_{i=0}^{2}(-1)^i \operatorname{Tr}(F^n|H^i(X_{f,q})).$$

Note that the traces of the Frobenius maps do not depend on the choice of ℓ. The ℓ-adic étale cohomology groups H^0 and H^2 are 1-dimensional, and F^n acts on them as the scalars 1 and q^n, respectively. The cohomology group H^1 has dimension $(d-1)(q-1)$ (see Section 2.2.1), and if $\pi_1, ..., \pi_{(d-1)(q-1)}$ are the eigenvalues of F on H^1, we then have that

$$|\mathrm{Fix}(F^n|X_{f,q})| = (q^n+1) - \sum_{i=1}^{(d-1)(q-1)} (\pi_i)^n.$$

Comparing the above equation to Equation 1.2, we see that the eigenvalues π_i are "the same" complex numbers discussed in Equation 1.2 (after applying an isomorphism $v : \overline{\mathbb{Q}_\ell} \to \mathbb{C}$ discussed in Section 3.2.1). In this case the Weil bound for $X_{f,q}$ is

$$||\mathrm{Fix}(F^n|X_{f,q})|| - (q^n+1)| \leq (d-1)(q-1)q^{n/2}.$$

The familiar lemma below implies that these π_i are the reciprocals of the zeroes of the zeta function.

Lemma I.2. *Let F_0 be an endomorphism of a finite-dimensional vector space V_0*

over a field K. Then we have an identity of formal power series

$$\exp\big(\sum_{n\geq 1}\mathrm{Tr}(F_0^n|V_0)\frac{T^n}{n}\big) = \det(1-F_0T|V_0)^{-1}.$$

Proof. See Appendix C.4 of [12] (which is also a good source of background information on zeta functions and the Weil conjectures). □

It is immediate from this lemma that

$$Z(X_{f,q},T) = \frac{\det(1-TF|H^1(X_{f,q}))}{(1-T)(1-qT)}.$$

The interested reader should see Chapter 2 of Rosen [26] for additional discussion of the zeta functions of curves and Appendix A of [26] for an elementary proof of the Riemann hypothesis for curves over a finite field.

Our methods of studying $M_{f,q,n}$ will almost invariably involve relating the arithmetic of $X_{f,q}$ to the arithmetic *and* the geometry of an $(n-1)$-dimensional auxiliary variety. The methods we will apply to these varieties are similar to those described above. In particular, we will use ℓ-adic étale cohomology and Deligne's proof of the Riemann hypothesis for varieties over finite fields (see 3.2.1).

In what follows, we will prove refinements to the Weil bound and the existence of multiplicative relations among the Frobenius eigenvalues π_i. (The specific relations may be different for different complete Artin-Schreier curves. See Theorem I.6).

1.2 Summary of Results

We will study bounds that for fixed n and d guarantee improvement to the Weil bound when q is sufficiently large. These bounds replace a factor of $\approx \sqrt{q}$ appearing in the Weil bound with a constant $C_{d,n}$ that does not depend on q. There is one non-degeneracy hypothesis on $f(x)$ we will often require; we will show it is equivalent to the smoothness of our affine auxiliary varieties (in Proposition III.7).

Definition I.3. Define $\mathscr{V} := \{f(t) : t \in \overline{\mathbb{F}_q}, f'(t) = 0\}$. We say that $f(x)$ is *n-smooth* if there **do not** exist $b_1, ..., b_n \in \mathscr{V}$ (not necessarily distinct) such that $\sum_{i=1}^{n} b_i = 0$.

Most polynomials $f(x)$ of degree d satisfy this condition when q is large, although polynomials that do not satisfy it can be common when q is small. Note that commonly studied example $f(x) = x^d$ is never n-smooth.

In the following, let $\mathscr{P}_{n,k}$ denote the set of partitions of n with k parts. Define $i_{(j)} := \binom{i}{j} j!$ and the multinomial coefficient $\binom{n}{\lambda} := \binom{n}{\lambda_1, \ldots, \lambda_k}$ for λ a partition in $\mathscr{P}_{n,k}$.

Theorem I.4. *(or IV.1) For any positive integers d and n define*

$$C_{d,n} := \sum_{k=1}^{d-1} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{d-1} \frac{(d-1)_{(k)} \binom{k}{i}}{\binom{n}{\lambda}}.$$

Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d, q) = 1$ and let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. If $f(x)$ is n-smooth (see Definition I.3 above) for $n \geq 2$, then

$$||U_{f,q}(\mathbb{F}_{q^n})| - q^n| \leq C_{d,n} \sqrt{q} q^{n/2} + C_{d,n-1} q^{n/2}.$$

For any fixed n the constant $C_{d,n}$ satisfies

$$\lim_{d \to \infty} \frac{C_{d,n}}{(d-1)^n} \frac{n!}{2^n - 1} = 1.$$

This bound is strongest (relative to existing results) when $q \gg d \gg n$. Note that for fixed $f(x)$ and q the constant $C_{d,n}$ contributes to the growth of the error term, and the bound above is always weaker than certain other bounds when n is sufficiently large. In particular, the bound above may improve the Weil bound

$$||U_{f,q}(\mathbb{F}_{q^n})| - q^n| \leq (d-1)(q-1)q^{n/2}$$

for sufficiently small (but certainly not all) positive integers n. In Section 1.5, we will provide more detail on when this theorem improves existing results.

Remark I.5. The hypotheses of Theorem I.4 are related to the smoothness of certain auxiliary varieties used in the proofs. In particular, we will consider an affine auxiliary variety $Y_{n,f,q}$ and its projective closure $Y'_{n,f,q}$ (see Section 3.1.1). The latter projective variety is a disjoint union of $Y_{n,f,q}$ and a Fermat variety. The affine variety $Y_{n,f,q}$ is smooth when f is n-smooth, while the Fermat variety is smooth when $(d,p)=1$.

Note that in the above bound the coefficient of $q^{n/2}$ grows more slowly in q and more quickly in d than the comparable coefficient in the Weil bound. More precisely, in Chapter IV we will explain why $C_{d,n} < (d-1)^n$ is a natural (if crude) upper bound, so Theorem I.4 improves the Weil bound when $(d-1)^{n-1} \ll \sqrt{q}$.

That such bounds exist at all is notable because Artin-Schreier curves are often studied for their "extreme" function field arithmetic: they are often used in the construction of curves with very many or very few points relative to what the Weil bound permits to curves of their genus. Specific examples of these curves are often fibre products of Artin-Schreier curves or they are constructed using class field theory (in which Artin-Schreier curves play a special role).

Although the bounds we study are weaker than the Weil bound when n is sufficiently large, we can still use similar methods to study relations among the arguments of the zeta zeroes. To state our main theorem along these lines, we must first recall that $\mathbb{F}_q$ acts on $X_{f,q}$ via the automorphisms $y \mapsto y+t$ and that $H^1(X_{f,q})$ has a decomposition into isotypic components $H^1(X_{f,q}) = \oplus_{\psi\neq 1\in\widehat{\mathbb{F}_q^+}} H^1(X_{f,q})^{\psi}$. In Chapter V we will prove that

Theorem I.6. *(or V.5) Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d,q)=1$, let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$, and let $X_{f,q}$ denote the smooth, complete model of $U_{f,q}$. Suppose n is any integer such that $d \leq n \leq p-1$ and that $f(x)+t$ is n-smooth for all $t \in \mathbb{F}_q$.*

For any $1 \neq \psi \in \widehat{\mathbb{F}_q}$ *and any eigenvalue* π *of Frobenius on* $H^1(X_{f,q})^{\psi}$ *there exists an* $i \in \{2, ..., n\}$ *and eigenvalues* $\beta_1, ..., \beta_n$ *(not necessarily distinct) of Frobenius on* $H^1(X_{f,q})^{\psi^i}$ *such that*

$$\pi^n = \prod_{j=1}^{n} \beta_j.$$

Remark I.7. As the relations among the eigenvalues are multiplicative, they imply $\mathbb{Z}$-linear relations modulo 1 among the arguments of the Frobenius eigenvalues (which we refer to as *Frobenius angles*).

Remark I.8. As discussed in Remark I.5, the requirements that $(d, q) = 1$, $(n, p) = 1$, and that $f(x) + t$ is n-smooth for all $t \in \mathbb{F}_q$ are necessary to ensure that auxiliary varieties used in the proof are smooth. The proof of this theorem actually shows that many more relations exist among the Frobenius eigenvalues and the hypothesis $d \leq n \leq p - 1$ guarantees that the particular form of relation given in the theorem occurs.

Remark I.9. Note that (by the Lefschetz fixed point theorem and Lemma I.2) the theorem above also implies similar relations among the zeroes of $Z(X_{f,q}, T)$.

When Theorem I.6 applies, it implies that $X_{f,q}$ possesses or at least mimics (speaking informally) the strong, unusual property given below ("mimicry" is discussed in Section 1.4).

Definition I.10. We say that a smooth, complete curve C defined over $\mathbb{F}_q$ is *supersingular* if its each of its zeta zeroes π has the form $\zeta_\pi\sqrt{q}$ for some root of unity ζ_π.

It can be shown that this definition is in fact equivalent to other definitions of supersingularity; for example, it is equivalent to the statement that the Jacobian of C is isogenous over $\overline{\mathbb{F}_q}$ to a product of supersingular elliptic curves. Note also that

$X_{f,q}$ is supersingular if and only if it attains the Weil lower bound $|X_{f,q}(\mathbb{F}_{q^n})| = q^n + 1 - (d-1)(q-1)q^{n/2}$ for some n. We will use this criterion as the basis of a new proof, given in Chapter VI, that the Artin-Schreier curves in the large family studied by van der Geer and van der Vlugt [30] [31] are supersingular.

We will also study the integers $M_{f,q,n}$ in the p-adic norm, and provide a non-Archimedean version of Theorem I.4. Note the similarity of the following result to the celebrated Chevalley-Warning theorem, which states that if $F_0 \in \mathbb{F}_p[x_1, ..., x_n]$ (F_0 need not be homogeneous) and n is greater than the degree of F_0, then the number of $(\mathbb{F}_q)^n$ roots of F_0 is divisible by p. One might describe Theorem I.11 informally as an arithmetic Chevalley-Warning theorem for Artin-Schreier curves where the dimension of the ambient space n has been replaced by the degree of an extension field of interest. (For further discussion of the Chevalley-Warning theorem, see Section 6.6 of Lidl and Niederreiter [19].) Note that below we will not require n-smoothness nor will we require that $(d, q) = 1$. Once again we take $U_{f,q}$ to be the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. As previously mentioned, we allow affine Artin-Schreier curves to be reducible.

Theorem I.11. *(or VI.3) Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d and let $U_{f,q}$ denote the affine Artin-Schreier curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. If $n \geq 2$, then the number of $\mathbb{F}_{q^n}$-rational points on $U_{f,q}$ satisfies the congruence*

$$|U_{f,q}(\mathbb{F}_{q^n})| \equiv 0 \pmod{q^{u+1}}$$

where

$$u = \lceil \frac{n-d}{d} \rceil.$$

In Chapter VI, we will prove a slightly stronger version of this theorem. We will also provide methods for computing $M_{f,q,n} \bmod q^{u+1}$ that imply, under certain hypotheses, that Theorem I.11 is the best possible bound of this form.

1.3 Examples

In this section we will discuss some specific choices of $f(x)$ to give the reader a sense of when the theorems above hold and why. In particular, we will explain why certain obvious "bad" $f(x)$ can cause the proofs to fail. We will also explain how Theorem I.11 is valid for ostensibly "bad" $f(x)$, notably when $U_{f,q}$ is reducible.

Example I.12. We will first consider $f(x) = x^d$, both because it is a commonly studied example and to show the significance of the n-smoothness hypothesis. In this case, 0 is a root of both $f'(x)$ and $f(x)$, so $f(x)$ is not n-smooth for any n and neither Theorem I.4 nor Theorem I.6 apply.

For concreteness, consider $q = 5$, $d = 3$, and $n = 2$. In this case, the constant $C_{d,n} = (d-1)(d-2)$ and were Theorem I.4 applicable it would imply

$$|M_{f,5,2} - 25| < 2 \cdot 1 \cdot 5^{3/2} \approx 22$$

while the Weil bound states that

$$|M_{f,5,2} - 25| \leq 4 \cdot 2 \cdot 5 = 40.$$

In fact, we have that $M_{f,5,2} = 65$, so the conclusion of Theorem I.4 fails and the Weil bound is achieved.

Example I.13. Take $f(x) = x^d$ once again. It *is* possible to apply Theorem I.11 in this case. If we take $q = 5$, $d = 3$ and $n = 4$, Theorem I.11 states that $M_{f,q,n}$ should be divisible by

$$5^{1+\lceil\frac{4-3}{3}\rceil} = 5^2 = 25$$

In fact, we have that $25|425 = M_{f,q,n}$ as stated in the theorem.

Example I.14. Let $q = 5$ and define $f(x) = 2x^3 + 2x^2 + 2x$. This $f(x)$ is 2-smooth so we may apply Theorem I.6. If we take $n = 2$, then $C_{d,n} = (d-1)(d-2)$ once again and the theorem implies that

$$|M_{f,5,2} - 25| < 2 \cdot 1 \cdot 5^{3/2} \approx 22$$

while the Weil bound states that

$$|M_{f,5,2} - 25| < 4 \cdot 2 \cdot 5 = 40.$$

In fact, we have that $M_{f,5,2} = 35$.

Example I.15 (A Class of Additive Polynomials)**.** We will now discuss a class of examples in which Theorems I.4 and I.6 fail because $p|d$. Suppose $q = p^2$ and $f(x) = x^p - x$. Note that we have the factorization

$$y^q - y - (x^p - x) = \prod_{t \in \mathbb{F}_p} (y^p + y - x + t)$$

so $U_{f,q}$ is reducible and we should expect this affine curve to have many points over $\mathbb{F}_{q^n}$.

The proof of Theorem I.4 fails because $p|d$. In Proposition IV.4, we will see that the term $C_{d,n-1}q^{(n-1)/2}$ in the statement of Theorem I.4 comes from the cohomology of the Fermat variety defined by the equation $\sum_{i=1}^{n} x_i^d$. The proof requires that this variety be smooth, but where p divides d it is singular.

Concretely, suppose that $p = 5$ and $n = 2$. In this case, the constant $C_{d,n}$ is once again equal to $(d-1)(d-2)$, and as we are assuming that $d = p$ we have $C_{5,2} = 12$. For our choice of f, we have $M_{f,25,2} = 3125$ and thus

$$|M_{f,25,2} - q^2| = |3125 - 625| = 2500 > 1500 = 5 \cdot 12 \cdot 25 = C_{d,n}\sqrt{q}q^{n/2}.$$

This violates the bound stated in Theorem I.4.

Example I.16. Consider $q = 5$, $n = 2$, and $f(x) = x^5 - x$. Note that $U_{f,q}$ is a reducible curve in this case. A stronger version of Theorem I.11, stated as Theorem VI.3, implies that 5^2 must divide $M_{f,q,n}$. Specifically, we have that $\sigma_q(f) = 1$ (see Definition VI.1), so $M_{f,5,2}$ should be congruent to zero modulo

$$5^{\lceil \frac{n-\sigma_q(f)}{\sigma_q(f)} \rceil + 1} = 5^{\lceil \frac{2-1}{1} \rceil + 1} = 25$$

All is well, as $M_{f,5,2} = 125$ and $25|125$.

Example I.17. Although the polynomial $f(x) = x^d$ fails to be n-smooth for all positive integers n, there *are* relations among the zeta zeroes of $X_{f,q}$ for this choice of $f(x)$. These relations have connections with Fermat varieties and classic results on exponential sums that *do not* fit exactly into the framework of the other results of this thesis.

Let X denote the smooth, complete curve associated to the equation $y^p - y = x^d$ and Y the smooth, complete (Fermat) plane curve with projective equation $x_1^d + x_2^d + x_3^d = 0$. Suppose $d|(p-1)$ and that χ is a generator of $\widehat{\mathbb{F}_p^\times}$. The reciprocals of the zeta zeroes of X are the Gauss sums

$$G(\psi, i) := -\sum_{t \in \mathbb{F}_p^\times} \psi(t)\chi^{i(p-1)/d}(t)$$

for $1 \neq \psi \in \widehat{\mathbb{F}_p}$ and $i \in \{1, ..., d-1\}$ (so there are $(d-1)(p-1)$ as required) while the reciprocals of the zeta zeroes of Y are the Jacobi sums

$$J(i, j) := -\sum_{0,1 \neq t \in \mathbb{F}_p} \chi^{i(p-1)/d}(t)\chi^{j(p-1)/d}(1-t)$$

for $i \neq j \in \{1, ..., d-1\}$ (so there are $(d-1)(d-2)$ as required by the genus-degree formula). Proofs that these exponential sums give the reciprocals of the zeta zeroes is given in Chapter 2 of [16]. The Gauss and Jacobi sums above are related by the familiar identity

$$J(i,j) := \frac{G(\psi,i)G(\psi,j)}{G(\psi,i+j)} \tag{1.3}$$

(see Chapter 1 of [18] for discussion of this identity). Note that the right-hand side of the above equation depends on the character ψ while the left-hand side does not. Thus, for any two characters ψ and ψ' of $\mathbb{F}_q$, we have that

$$\frac{G(\psi,i)G(\psi,j)}{G(\psi,i+j)} = \frac{G(\psi',i)G(\psi',j)}{G(\psi',i+j)}$$

The interested reader should see the seminal paper of Weil [34] for more information on the zeta functions of Fermat varieties, as well as Chapter 1 of [11] for generalizations of Equation 1.3.

Note that the affine surface defined by the equation $x_1^d + x_2^d + x_3^d = 0$ has a singularity at the origin, and in this case we can not apply precisely the methods we develop later in the thesis.

1.4 Observations on Frobenius Angle Rank

As the relations of Theorem I.6 are multiplicative, they imply $\mathbb{Z}$-linear relations modulo 1 among the Frobenius angles. Specifically, the zeta function of any smooth, complete, irreducible curve C of genus g_0 is determined by the $2g_0$ Frobenius eigenvalues $\{\pi_i : 1 \leq i \leq 2g_0\}$ (their inverses are the zeroes of $Z(C,T)$). Let $a_i := \frac{1}{2\pi}\text{Arg}(\pi_i)$ denote the argument of the Frobenius eigenvalue π_i, normalized so that it lies in $(\frac{-1}{2}, \frac{1}{2}]$. We have that

$$\pi_i = \sqrt{q}\exp(2\pi i a_i)$$

A natural object of study is the dimension of $\mathbb{Q}$-vector space generated by these Frobenius angles.

Definition I.18. For a smooth, complete, irreducible curve defined over $\mathbb{F}_q$ we define the *Frobenius angle rank* $\delta(C)$ to be the integer

$$\delta(C) := \dim_{\mathbb{Q}}(\mathbb{Q}[1, a_1, ..., a_{2g_0}]) - 1.$$

As the eigenvalues are real or come in complex conjugate pairs, we have that

$$0 \leq \delta(X_{f,q}) \leq g_0.$$

We will discuss the behavior of $\delta(X_{f,q})$ explicitly below and implicitly in Section **??**.

The following describes the outcomes of computations done in Magma [6]. Empirically, there are many relations among the π_i when d is small relative to q, and these relations often take a specific form: given an eigenvalue π_i of Frobenius on $H^1(X_{f,q})^{\psi}$, there exists a $\psi' \neq \psi$, an eigenvalue π_j of Frobenius on $H^1(X_{f,q})^{\psi'}$, and a positive integer m such that

$$\pi_i^m = \pi_j^m.$$

Relations of this form are most common when $d \ll q$. The integer m is invariably divisible by p; this is notable because $f(x)$ fails to be n-smooth for any positive integer n divisible by p.

Note that a given $f \in \mathbb{F}_q[x]$ can be used to define complete Artin-Schreier curves of arbitrarily large genus via the equations $y^{q^i} - y = f(x)$. We may then consider the dimension of $\delta(X_{f,q})$ as a function of q. The theorems of this thesis and the prevalence of the relations discussed above (particularly when $d \ll q$) suggest the possibility that *for some restricted (but large) class of polynomials f, there exists a bound $\theta(d)$ (depending only on d) such that $\delta(X_{f,q}) < \theta(d)$ regardless of the choice of q.* In particular, Theorem I.6 implies a bound for $\delta(X_{f,q})$, the exact form of which depends on the structure of the group $\mathbb{F}_q^\times$. We also prove in Theorem VI.13 that $\delta(X_{f,q}) = 0$ iff f belongs to a large class which includes all the quadratic polynomials.

1.5 Background

Our approach to these problems is motivated in part by the recent work of Rojas-Leon and Wan [25]. They prove bounds with the same form as Theorem I.4 in that they replace a factor of $\sqrt{q}$ with a constant that depends only on d and n. Their method, which is different from those employed in this thesis, is to study the monodromy of a $\overline{\mathbb{Q}_\ell}$-adic sheaf $\mathscr{L}$ on $\mathbb{G}_m$ (or one of its Adams powers) whose local Frobenius traces sum to $M_{f,q,n}$. From these Adams powers they obtain a bound

$$|M_{f,q,n} - q^n| \leq C'_{d,n}\sqrt{q}q^{n/2}$$

with explicit constant

$$C'_{d,n} := \sum_{i=0}^{n} |i-1| \binom{d-2+n-i}{n-i}\binom{d-1}{i}.$$

For fixed n, the ratio of this constant to that of Theorem I.4 (with each considered as a function of d) approaches a finite constant which depends on n

$$c(n) := \lim_{d\to\infty} \frac{C_{d,n}}{C'_{d,n}} = \frac{1-2^{-n}}{\frac{1}{2}n - 1 + 2^{1-n}}.$$

as d approaches infinity. These constants, one for each n, approach zero

$$\lim_{n\to\infty} c(n) = 0$$

as n approaches infinity (see Section 4.1.3 for proofs of these facts). Thus, Theorem I.4 improves the Weil bound when q is large relative to d and n and it improves more recent results when d is large relative to n.

In Theorem 2.1 of [24], Rojas-Leon obtains (under the weaker hypothesis that $f \in \mathbb{F}_{q^n}[x]$) the bound

$$|M_{f,q,n} - q^n| \leq (d-1)^n\sqrt{q}q^{n/2}$$

by constructing an $(n-1)$-dimensional auxiliary variety $L_{n,f,q}$ (see Definition VI.6) whose $\mathbb{F}_q$-points are bijective with the $\mathbb{F}_{q^n}$-points of $X_{f,q}$. In Section 3.1.1, we will define a related affine auxiliary variety $Y_{n,f,q}$ and its projective closure $Y'_{n,f,q}$. These three auxiliary varieties are primary objects of study in this thesis. For each n, $Y'_{n,f,q}$ has an S_n action, previously unstudied, and we will show how to extract arithmetic information about $X_{f,q}$ from representations of S_n on the cohomology of $Y'_{n,f,q}$. In particular, we will deduce Theorem I.4 by using representation theory to show that the cohomology of $Y'_{n,f,q}$ has a large subspace on which the trace of Frobenius is 0.

In Chapter II we will review basic results about the curve $X_{f,q}$ that we will need to construct the auxiliary varieties. The most important of these is Corollary 2.1.2

$$M_{f,q,n} = q|\{t \in \mathbb{F}_{q^n} : \operatorname{Tr}_{q,n} f(t) = 0\}|$$

where $\operatorname{Tr}_{q,n} f(z) := \sum_{i=0}^{n-1} f(z)^{q^i}$. In Chapter IV, we will apply a construction similar to Weil restriction to these trace polynomials to produce a polynomial $Q_n \in \mathbb{F}_q[x_1, ..., x_n]$ of degree $\leq d$ such that

$$M_{f,q,n} = q|\{\bar{t} \in (\mathbb{F}_q)^n : Q_n(\bar{t}) = 0\}|$$

In Chapter VI we take $L_{n,f,q}$ to be the vanishing set of this Q_n. This set-up allows us to apply results in low-degree algebraic geometry and obtain analogous conclusions about $M_{f,q,n}$; for example, we will apply the refinement of the Chevalley-Warning theorem first proven by Ax [5] and refined by Katz [15]. We will fully develop this argument in Chapter VI, in addition to proving sharpness by studying the hyperplane sections of $L_{n,f,q}$ and the congruences amongst the cardinalities of their sets of $\mathbb{F}_q$-rational points implied by the result of Warning recently refined by Heath-Brown [14].

For some choices of $f(x)$ the polynomial Q_n has degree 2, even if $f(x)$ itself has degree greater than 2. This polynomial has a known constant term, and thus the exact number of $\mathbb{F}_q$-rational points on $L_{n,f,q}$ can be computed using standard results on quadratic forms. Using the aforementioned property of the zeta zeroes of curves with supersingular Jacobian, this technique leads to a new proof that the the curves corresponding to polynomials in a certain class are supersingular. We should note that some of the inspiration for this approach was provided by Wolfmann's work [35], [36], [37] on maximal curves and their relation to Fermat varieties.

1.6 Methods of Proof

The methods of proof used in this thesis invariably involve auxiliary varieties of higher dimension. Let $Y_{n,f,q}$ denote the affine variety defined over $\mathbb{F}_q$ by the polynomial $\sum_{i=1}^n f(x_i)$ and let $Y'_{n,f,q}$ denote its projective closure. Both varieties $Y_{n,f,q}$ and $Y'_{n,f,q}$ have an obvious action of S_n by permutation of coordinates and thus their cohomology groups do as well. In Chapter III, we prove a number of propositions about these varieties and their cohomological S_n-representations. To state the most significant of these, we must recall again the decomposition $H^1(X_{f,q}) = \oplus_{\psi\neq 1\in\widehat{\mathbb{F}_q}} H^1(X_{f,q})^{\psi}$ into isotypic components and suppose that each $g \in S_n$ has a decomposition into disjoint cycles $g = g_1 ... g_{l(g)}$ with each g_i and $l_i(g)$ cycle. The key proposition applied in Chapters IV and V is:

Proposition I.19. *(or III.8) For any $g \in S_n$ consider the fixed locus*

$$|Fix(g \circ F|Y_{n,f,q})| := \{\boldsymbol{x} \in \mathbb{A}^n(\mathbb{F}_q) : \boldsymbol{x} \in Y_{n,f,q} \text{ with } (x_{g(i)})^q = x_i, 1 \leq i \leq n\}.$$

We have the equality

$$q|Fix(g \circ F|Y_{n,f,q})| = \sum_{\psi\in\widehat{\mathbb{F}_q}} \prod_{i=1}^{l(g)} \mathrm{Tr}(F^{l_i(g)}|H^1(X_{f,q})^{\psi}).$$

Note that if ϕ is the n-cycle $x_i \mapsto x_{i+1}$, then q times the cardinality of $\mathrm{Fix}(\phi \circ F|Y_{n,f,q})$ is the trace of Frobenius on $H^1(X_{f,q})$. Much of the work done in Chapters

IV and V will involve studying the cohomology groups of $Y'_{n,f,q}$ as S_n-representations and using this information to prove various statements about weighted sums over S_n of such $|\mathrm{Fix}(g \circ F|Y_{n,f,q})|$.

Chapter IV focuses primarily on applying Proposition I.19 in the $l(g) = 1$ case, where $g = \phi$. The above formula specializes to the statement

$$q|\mathrm{Fix}(\phi \circ F|Y_{n,f,q})| = \mathrm{Tr}(F^n|H^1(X_{f,q})) \tag{1.4}$$

and this implies that bounding the trace of Frobenius on the cohomology of $Y'_{n,f,q}$ implies a similar bound for $H^1(X_{f,q})$. If one considers the obvious analogue of the Weil bound for $Y'_{n,f,q}$, $n \geq 2$, and $h_{n-1,d}$ denotes the $(n-1)$-st Betti number of a smooth projective hypersurface of degree d, then one obtains

$$|M_{f,q,n} - q^n| \leq h_{n-1,d}\sqrt{q}q^{n/2} + h_{n-2,d}q^{n/2}.$$

The previously mentioned result of Rojas-Leon is obtained by applying a bound for $h_{n-1,d}$. Theorem I.2 significantly improves the constant above by showing there is a large subspace of $H^{n-1}(Y'_{n,f,q})$ on which the trace of $\phi \circ F$ is 0. We will show in Chapter IV that the trace of $\phi \circ F$ is zero on all but a very restricted class of irreducible subrepresentations of $H^{n-1}(Y'_{n,f,q})$; in Chapter III we will show the S_n-representation $H^{n-1}(Y'_{n,f,q})$ is (non-canonically) isomorphic to one arising from a Fermat variety, explicitly describe these representations, and later use this description to count the appearances of the aforementioned irreducibles and show they appear rarely. The formula given in Theorem I.2 in fact represents the sum of the multiplicities with which these restricted irreducibles occur.

In Chapter V, we will apply Proposition I.19 for more general $g \in S_n$ and define exponential sums

$$R(g,\psi,m,n) := qq^{-m}\sum_{x\in\mathbb{F}_{q^m}}\psi(x)\mathrm{Fix}(g\circ F^m|Y_{n,f+x/n})$$

and generating functions

$$Z(g,\psi,n,T) := \exp\big(\sum_{m\geq 1}R(g,\psi,m,n)\frac{T^m}{m}\big)$$

using the cardinalities of the fixed loci described by the proposition. We will prove that these generating functions are in fact rational. In Chapter III, we will show that there is an irreducible representation V whose isotypic component in $H^{n-1}(Y'_{n,f,q})$ is zero-dimensional. The exponential sum

$$\frac{1}{n!}\sum_{g\in S_n}\mathrm{Tr}(g^{-1}|V)\mathrm{Fix}(g\circ F|Y'_{n,f,q})$$

gives the trace of Frobenius on this isotypic component and it is thus equal to zero. We will use these facts to prove a similar relation among the $R(g,\psi,m,n)$ and then that a corresponding product of the $Z(g,\psi,n,T)$ is equal to 1. In Chapter V, we will show that the zeroes and poles of the $Z(g,\psi,n,T)$ are certain products of the zeta zeroes of $X_{f,q}$. Any zero which occurs as a pole of a rational function in the aforementioned trivial product must also occur as a zero; this implies many relations amongst various products of zeta zeroes. We will complete the proof of Theorem I.6 by showing that the equality given in the theorem must be one of these relations.

In Chapter VI, we will construct another affine auxiliary variety $L_{n,f,q}$ and use it to deduce Theorem I.11. This auxiliary variety $L_{n,f,q}$ (defined in Definition VI.6) is in fact a twist of the generalized Fermat variety $Y_{n,f,q}$, and Equation 1.4 reflects the fact that $\phi\circ F$ is the Frobenius map of the twist $L_{n,f,q}$. However, we will not make use of these facts. We will study $Y_{n,f,q}$ in Chapters IV and V because it is more tangible (it is difficult to give defining equations for an arbitrary $L_{n,f,q}$), but in Chapter VI we will be able to study $L_{n,f,q}$ directly.

CHAPTER II

Basic Artin-Schreier Theory

2.1 Study of the Affine Curve $U_{f,q}$

In this section, we will relate the number of $\mathbb{F}_{q^n}$-rational points on an affine Artin-Schreier curve to the number of a roots of a polynomial in $\mathbb{F}_q[x]$. This will allow us to express the number of points on the curve in terms of certain exponential sums. These exponential sums are a key object of study throughout this thesis: in Chapter III we will study auxiliary varieties related to these sums and this machinery will be used to prove Theorems I.4 and I.6.

2.1.1 Definitions Related to $U_{f,q}$

Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d, q) = 1$. In the following, we will establish basic properties of $U_{f,q}$, the affine curve defined over $\mathbb{F}_q$ by the polynomial $y^q - y = f(x)$. Our eventual goal will be to study the number $M_{f,q,n} := |U_{f,q}(\mathbb{F}_{q^n})|$ on $\mathbb{F}_{q^n}$-points $U_{f,q}(\mathbb{F}_{q^n})$ of this affine curve

$$U_{f,q}(\mathbb{F}_{q^n}) = |\{(s,t) \in (\mathbb{F}_{q^n})^2 : t^q - t = f(s)\}|. \tag{2.1}$$

Let F denote the Frobenius automorphism of $U_{f,q}$ given by applying the q-th power map to each coordinate

$$(s,t) \mapsto (s^q, t^q) \tag{2.2}$$

and note that the $\mathbb{F}_{q^n}$ points of $U_{f,q}$ are the fixed points of F^n. The affine curve $U_{f,q}$ also has an action of $\mathbb{F}_q$ such that t_0 maps (s,t) to $(s,t+t_0)$. Let $X_{f,q}$ denote the smooth, complete model of $U_{f,q}$; in Section 2.2.1 we will explain why this curve has a related Frobenius map F and an action of $\mathbb{F}_q$.

One important step in studying the integers $M_{f,q,n}$ is showing that they are related to the number of roots of certain polynomials in $\mathbb{F}_q[x]$. For any $f(x)$ this polynomial takes the form $\operatorname{Tr}_{q,n} f(x)$ where $\operatorname{Tr}_{q,n}$ is the polynomial

$$\operatorname{Tr}_{q,n}(x) := \sum_{i=0}^{n-1} x^{q^i}. \tag{2.3}$$

Note that $\operatorname{Tr}_{q,n}(x)$ gives the trace map $\mathbb{F}_{q^n} \to \mathbb{F}_q$. We will use the polynomials $\operatorname{Tr}_{q,n} f(x)$ in two related ways. In Chapter VI, we will use these these polynomials to construct auxiliary affine varieties needed for the proof of Theorem I.11. Also, we will prove later in this section that $M_{f,q,n}$ has an expression in terms of exponential sums

$$M_{f,q,n} := q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} S(\psi, n). \tag{2.4}$$

The $S(\psi,n)$ are themselves exponential sums defined using $\operatorname{Tr}_{q,n} f(x)$ and the additive character ψ.

$$S(\psi,n) := \sum_{t \in \mathbb{F}_{q^n}} \psi(\operatorname{Tr}_{q,n} f(t)). \tag{2.5}$$

Note that these exponential sums are also discussed in Chapter III, where we will study their relationship to the affine auxiliary variety $Y_{n,f,q}$ defined over $\mathbb{F}_q$ by the equation $\sum_{i=1}^n f(x_i)$.

2.1.2 Relating $U_{f,q}(\mathbb{F}_{q^n})$ to $\operatorname{Tr}_{q,n} f(x)$

Proposition II.1. *Let $\pi : U_{f,q}(\mathbb{F}_{q^n}) \to \mathbb{F}_{q^n}$ be the map given by projection onto the x coordinate. A point $s \in \mathbb{F}_{q^n}$ has q pre-images under π if* $\operatorname{Tr}_{q,n} f(s) = 0$ *and 0* *pre-images otherwise.*

Proof. For any $s \in \mathbb{F}_{q^n}$ we may identify the set of pre-images of s under π with the set

$$\{t \in \mathbb{F}_{q^n} : t^q - t = f(s)\}$$

In particular, $f(s)$ must lie in the image of the map $t \mapsto t^q - t$. Note that the kernel of this map is exactly the $t \in \mathbb{F}_q$ so its image must have dimension $n-1$ as an $\mathbb{F}_q$ vector space. As $t \in \mathbb{F}_{q^n}$ we have that $t^{q^n} = t$, so $\mathrm{Tr}_{q,n}(t^q) = \mathrm{Tr}_{q,n}(t)$ and $\mathrm{Tr}_{q,n}(t^q - t) = 0$. This implies that $f(s)$ is contained in the kernel of $\mathrm{Tr}_{q,n}$, and this kernel has the same $\mathbb{F}_q$ vector space dimension as the image of $t \mapsto t^q - t$. It follows that $\mathrm{Tr}_{q,n} f(s) = 0$. Similar reasoning can be used to show that when $\mathrm{Tr}_{q,n} f(s) = 0$, $f(s)$ lies in the image of $t \mapsto t^q - t$ and s must have a pre-image.

We may identify the set of pre-images with the roots of the polynomial $x^q - x = f(s)$, and where this polynomial has a single root t_0 it must in fact have the q roots $t_0 + t_1$ for all $t_1 \in \mathbb{F}_q$. □

The following corollary is an immediate consequence of the proposition above.

Corollary II.2. *$M_{f,q,n}$ is related to the number of $\mathbb{F}_{q^n}$-roots of $\mathrm{Tr}_{q,n} f(x)$ by the identity*

$$M_{f,q,n} = q|\{s \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q,n} f(s) = 0\}|.$$

2.1.3 Relating $U_{f,q}(\mathbb{F}_{q^n})$ to the Exponential Sums $S(\psi, n)$

Proposition II.3. *Let ψ be a generator of $\widehat{\mathbb{F}_q}$. Any character of $\mathbb{F}_{q^n}$ has the form $t \mapsto \psi_z(t) := \psi(\mathrm{Tr}_{q,n} zt)$ for some $z \in \mathbb{F}_{q^n}$.*

Proof. The trace map and the maps $t \mapsto zt$ are additive homomorphisms so their composition with a character of $\mathbb{F}_q$ yields another such character. Given $z_1, z_2 \in \mathbb{F}_{q^n}$

we have $\psi_{z_1} = \psi_{z_2}$ if and only if

$$\psi(\mathrm{Tr}_{q,n} z_1 t) = \psi(\mathrm{Tr}_{q,n} z_2 t) \Rightarrow \psi(\mathrm{Tr}_{q,n}(z_1 - z_2)t) = 1$$

for all $t \in \mathbb{F}_{q^n}$. This implies for all t that $\mathrm{Tr}_{q,n}(z_1 - z_2)t = 0$, that $(z_1 - z_2)t = 0$, and thus that $z_1 = z_2$. The map $z \mapsto \psi_z$ is therefore injective, and as both source and target have cardinality q^n it must be bijective. □

Proposition II.4. *We have the following expression for $M_{f,q,n}$:*

$$M_{f,q,n} = q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} S(\psi, n).$$

Proof. Let ψ_0 be an arbitrary character of $\mathbb{F}_q$. Note that for any $t \in \mathbb{F}_{q^n}$ the character sum

$$\sum_{z \in \mathbb{F}_q} \psi_0(z \, \mathrm{Tr}_{q,n} f(t))$$

is equal to q when $\mathrm{Tr}_{q,n} f(t) = 0$ and equal to 0 otherwise. Therefore

$$M_{f,q,n} = \sum_{t \in \mathbb{F}_{q^n}} \sum_{z \in \mathbb{F}_q} \psi_0(z \, \mathrm{Tr}_{q,n} f(t)).$$

By removing the $z = 0$ term and interchanging the order of summation, we obtain

$$M_{f,q,n} = q^n + \sum_{z \in \mathbb{F}_q^\times} \sum_{t \in \mathbb{F}_{q^n}} \psi_0(z \, \mathrm{Tr}_{q,n} f(t)).$$

By Proposition II.3, any non-trivial character of $\mathbb{F}_q^+$ has the form $t \mapsto \psi_0(zt)$ for some $z \neq 0$. This implies that

$$M_{f,q,n} = q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} S(\psi, n)$$

as desired. □

2.2 Basic Results Relating $U_{f,q}$ and $X_{f,q}$

2.2.1 Constructing $X_{f,q}$

In what follows, we will construct the smooth, complete curve $X_{f,q}$, as well as discuss its properties and relation to $U_{f,q}$. Let $\overline{U_{f,q}}$ denote the closure of $U_{f,q}$ in $\mathbb{P}^2$ and $F_{\overline{U_{f,q}}}$ the automorphism of $\overline{U_{f,q}}$ given by applying the q-th power map coordinatewise.

$$[x_1 : x_2 : x_3] \mapsto [x_1^q : x_2^q : x_3^q]$$

Note that $U_{f,q}$ is isomorphic to an open affine subset of $\overline{U_{f,q}}$ and the restriction of $F_{\overline{U_{f,q}}}$ to this subset agrees with $F_{U_{f,q}}$.

Proposition II.5. *There exists a smooth, complete curve $X_{f,q}$ and a morphism $\Pi : X_{f,q} \to \overline{U_{f,q}}$ such that*

- Π *is an isomorphism $\Pi^{-1}(U_{f,q}) \to U_{f,q}$.*
- $X_{f,q}$ *has an action of $\mathbb{F}_q$ and Π is $\mathbb{F}_q$-invariant.*
- $X_{f,q}$ *has an automorphism $F_{X_{f,q}}$ such that $F_{X_{f,q}} \circ \Pi = \Pi \circ F_{\overline{U_{f,q}}}$.*

Proof. This proposition can be deduced from standard results proven in Section 4.1.2 of [20]. □

Example II.6. We will now explain the necessity of the hypothesis $(d, q) = 1$. Suppose $q = p^2$ and $f(x) = x^p - x$ (note that we approach this example from another angle in Example I.15). We have the factorization

$$y^q - y - (x^p - x) = \prod_{t \in \mathbb{F}_p} (y^p + y - x + t)$$

so $\overline{U_{f,q}}$ is reducible. This variety is thus not integral, it does not have a unique normalization, and we cannot apply the results of Section 4.1.2 of [20] that are embodied in the proposition above.

Proposition II.7. *The function field of $X_{f,q}$ is isomorphic to $\mathbb{F}_q(x)[y]/(y^q - y - f(x))$.*

Proof. This proposition is immediate the above. □

Note that this function field has only place at ∞. As we can identify $U_{f,q}$ with an open subvariety of $X_{f,q}$ we can use the Riemann-Hurwitz formula to compute the genus of $X_{f,q}$.

Proposition II.8. *The genus of $X_{f,q}$ is $(d-1)(q-1)$.*

Proof. See Proposition 3.4.14 and 3.7.8 of [29]. □

As $\mathbb{F}_q$ acts on $X_{f,q}$, we have a decomposition of $H^1(X_{f,q})$ into isotypic components

$$H^1(X_{f,q}) = \bigoplus_{\psi \neq 1 \in \widehat{\mathbb{F}_q}} H^1(X_{f,q})^{\psi}.$$

Later, we will make heavy use certain relationships between this decomposition and the exponential sums $S(\psi, n)$ defined in the preceding section.

Proposition II.9. *The trace of $F^n_{X_{f,q}}$ on $H^1(X_{f,q})^{\psi}$ is equal to $S(\psi, n)$.*

Proof. See page 176 of [16] □

The interested reader should see [17] for a more general discussion of the exponential sums $S(\psi, n)$ and their relation to the curve $X_{f,q}$.

CHAPTER III

Basic Properties of $Y_{n,f,q}$

3.1 Study of the Auxiliary Variety $Y_{n,f,q}$

In this section, we will define an auxiliary variety $Y_{n,f,q}$ and prove a number of propositions about it. It is crucially important that the symmetric group S_n acts on this auxiliary variety. Speaking broadly and informally, the purpose of the following propositions is to establish a relationship between the arithmetic of $U_{f,q}$ and this S_n action. We will exploit this relationship in Chapters IV and V to prove the main theorems of the introduction.

3.1.1 Definitions Related to the Auxiliary Variety $Y_{n,f,q}$

Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d, q) = 1$. The primary object of study in this chapter is the $(n-1)$-dimensional affine variety $Y_{n,f,q}$ defined over $\mathbb{F}_q$ by the equation $\sum_{i=1}^{n} f(x_i)$. The symmetric group S_n acts on this variety by permutation of coordinates and this action commutes with the Frobenius automorphism (coordinate-wise q-th power map) F

$$(x_1, ..., x_n) \mapsto (x_1^q, ..., x_n^q).$$

In Section 3.1.4, we will study the cardinality of the set of points fixed by $g \circ F$ for g an element of S_n.

$$|\mathrm{Fix}(g \circ F|Y_{n,f,q})| := \{\mathbf{x} \in \mathbb{A}^n(\mathbb{F}_q) : \mathbf{x} \in Y_{n,f,q} \text{ with } (x_{g(i)})^q = x_i, 1 \leq i \leq n\}. \tag{3.1}$$

Specifically, in Proposition III.8 we will prove a formula for $|\mathrm{Fix}(g \circ F|Y_{n,f,q})|$ stated in terms of the exponential sums

$$S(\psi, m) := \sum_{t \in \mathbb{F}_{q^m}} \psi(\mathrm{Tr}_{q,m} f(t)). \tag{3.2}$$

defined using the non-trivial characters $\psi \in \widehat{\mathbb{F}_q}$. To state this formula, we need to introduce notation describing the decomposition of an arbitrary $g \in S_n$ into a product of disjoint cycles.

Definition III.1 (Cycle Decompositions For $g \in S_n$)**.** Given any $g \in S_n$ let $g = g_1 ... g_{l(g)}$ be the decomposition of g into disjoint cycles. Let $l_i(g)$ denote the length of the cycle g_i and $l(g)$ the total number of cycles in the decomposition.

Note that if g is the identity element then $l(g) = n$. We can now state the formula of Proposition III.8.

$$q|\mathrm{Fix}(g \circ F|Y_{n,f,q})| = q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} \prod_{i=1}^{l(g)} S(\psi, l_i(g)) \tag{3.3}$$

In Chapter IV, we will be interested in applying this formula to a particular automorphism of $Y_{n,f,q}$.

Definition III.2. Let ϕ denote the automorphism of $Y_{n,f,q}$ given by cyclic permutation of coordinates $x_i \mapsto x_{i+1}$.

Note that $l(\phi) = 1$, and that when $g = \phi$ the right hand side of Equation 3.3 is the exponential sum considered in Proposition II.4.

Finally, let $Y'_{n,f,q}$ denote the projective closure of $Y_{n,f,q}$ in $\mathbb{P}^n$, and let $Z_{n,d,q}$ denote the $(n-2)$-dimensional projective (Fermat) variety defined by the equation $\sum_{i=1}^n x_i^d$. We will see in Section 3.1.3 that $Z_{n,d,q}$ is $Y'_{n,f,q}$'s subvariety at ∞. Define $f_0(x_0, x) := x_0^d f(\frac{x}{x_0})$. In order to discuss the $Y'_{n,f,q}$'s subvariety at ∞, we will also consider it as the projective variety defined over $\mathbb{F}_q$ by the polynomial

$$\sum_{i=1}^{n} f_0(x_0, x_i) \tag{3.4}$$

3.1.2 Relating $U_{f,q}(\mathbb{F}_{q^n})$ to Fix$(\phi \circ F^n | Y_{n,f,q})$

We will now state and prove a special case of Proposition III.8, and this special case is all that is required for Chapter IV.

Proposition III.3. *If ϕ is the automorphism of $Y_{n,f,q}$ given by cyclic permutation of coordinates $x_i \mapsto x_{i+1}$, then*

$$q|Fix(\phi \circ F | Y_{n,f,q})| = U_{f,q}(\mathbb{F}_{q^n}).$$

Proof. Suppose $(t_1, ..., t_n)$ is a point of $Y_{n,f,q}$ fixed by $\phi \circ F$. It follows that $t_{i+1} = t_i^q$ for all i (with i considered modulo n) and thus any such point is determined by its t_1 coordinate. We also have that

$$\sum_{i=1}^{n} f(t_i) = 0$$

and thus that

$$\sum_{i=1}^{n} f(t_1^{q^{i-1}}) = 0.$$

$f(x)$ has its coefficients in $\mathbb{F}_q$, so it follows that

$$\sum_{i=1}^{n} f(t_1)^{q^{i-1}} = \mathrm{Tr}_{q,n}\, f(t_1) = 0.$$

and the result follows from Proposition II.2. □

Note that by Proposition III.8

$$q|\mathrm{Fix}(\phi \circ F^n Y_{n,f,q})| = q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} \prod_{i=1}^{l(g)} S(\psi, n)$$

3.1.3 Basic Properties of $Y_{n,f,q}$

In this section, we will warm up by proving some of the most basic required properties of $Y_{n,f,q}$. In particular, we will show that under certain hypotheses $Y'_{n,f,q}$ is smooth.

Proposition III.4. *The projective closure $Y'_{n,f,q}$ of $Y_{n,f,q}$ is a disjoint union $Y'_{n,f,q} = Y_{n,f,q} \cup Z_{n,d,q}$.*

Proof. The complement of $Y_{n,f,q}$ in $Y'_{n,f,q}$ is the x_0 section (see Equation 3.4), and by inspection this is the vanishing set of $\sum_{i=1}^n x_i^d$ in $\mathbb{P}^{n-1}$. □

The following corollary is immediate.

Corollary III.5. *$M_{f,q,n}$ has the following expression via the cardinalities of fixed loci on $Y'_{n,f,q}$:*

$$M_{f,q,n} = |Fix(\phi \circ F|Y'_{n,f,q})| - |Fix(\phi \circ F|Z_{n,d,q})|.$$

Recall our non-degeneracy assumption on $f(x)$ from the introduction.

Definition III.6. Define $\mathscr{V} := \{f(t) : t \in \overline{\mathbb{F}_q}, f'(t) = 0\}$. We say that $f(x)$ is *n-smooth* if there **do not** exist $b_1, ..., b_n \in \mathscr{V}$ (not necessarily distinct) such that $\sum_{i=1}^n b_i = 0$.

We will now show how this smoothness condition is related to the smoothness of $Y'_{n,f,q}$.

Proposition III.7. *The polynomial $f(x)$ is n-smooth if and only if $Y'_{n,f,q}$ is smooth.*

Proof. We will use the Jacobian criterion for smoothness, which in this case states that the singular locus is the common vanishing set of $\sum_{i=1}^{n} f_0(x_0, x)$ and its partial derivatives. Fermat varieties are smooth when $(n, p) = 1$ (and no f is n-smooth when $p|n$), and it follows that the intersection of the singular locus with the x_0 section of $Y'_{n,f,q}$ is empty. As for the $x_0 = 1$ affine, a point $(t_1, ..., t_n) \in Y_{n,f,q}$ is singular if and only if $f'(t_i) = 0$ for all i. For such a point to lie in $Y_{n,f,q}$ requires also that an n-fold sum of the $f(t_i)$ is 0, and thus $Y_{n,f,q}$ (and $Y'_{n,f,q}$) has a singular point if and only if some sum of n of the β_i is 0. Note that $Y_{n,f,q}$ is always singular when p divides n. □

3.1.4 A Fixed Point Formula for $Y_{n,f,q}$

In this section we will prove a formula relating the fixed loci of the composition $g \circ F$ to products of the exponential sums $S(\psi, n)$. In Chapter IV, we will apply this formula in the $g = \psi$ case to bound $M_{f,q,n}$ and in Chapter V we will apply it more generally to the zeta function of $U_{f,q}$'s smooth, complete model $X_{f,q}$.

Proposition III.8. *The cardinality of the fixed locus of $g \circ F$ on $Y_{n,f,q}$ has the following expression in terms the exponential sums $S(\psi, m)$:*

$$q|Fix(g \circ F|Y_{n,f,q})| = q^n + \sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} \prod_{i=1}^{l(g)} S(\psi, l_i(g)).$$

Proof. We will prove the proposition by direct manipulation of character sums related to the fixed loci $g \circ F$. Define $E(g) := \prod_{i=1}^{l(g)} \mathbb{F}_{q^{l_i(g)}}$ and $\eta(g) : E(g) \to \mathbb{F}_q$ by requiring that

$$\eta(g)(x_1, ..., x_{l(g)}) := \sum_{i=1}^{l(g)} \mathrm{Tr}_{q,l_i(g)} f(x_i)$$

We have that

$$|\mathrm{Fix}(g \circ F|Y_n)| = |\{x \in E(g) : \sum_{i=1}^{l(g)} \eta(g)(x) = 0\}|.$$

Note that

$$\sum_{y\in\mathbb{F}_q}\psi(y\cdot\sum_{i=1}^{l(g)}\eta(g)(x))$$

is equal to q if $\eta(g)(x)=0$ and 0 otherwise, so we have that

$$\begin{aligned}q|\mathrm{Fix}(g\circ F)| &= \sum_{x\in E(g)}\sum_{y\in\mathbb{F}_q}\psi(y\cdot\sum_{i=1}^{l(g)}\eta(g)(x))\\ &= \sum_{y\in\mathbb{F}_q}\sum_{x\in E(g)}\psi(y\cdot\eta(g)(x))\\ &= \sum_{y\in\mathbb{F}_q}\prod_{i=1}^{l(g)}\sum_{x\in\mathbb{F}_p^{l_i(g)}}\psi(y\cdot\mathrm{Tr}_{q,l_i(g)}f(x_i))\end{aligned}$$

Removing the $y=0$ term and applying the definition of the sums $S(\psi,n)$ we obtain

$$q|\mathrm{Fix}(g\circ F|Y_{n,f,q})|=q^n+\sum_{1\neq\psi\in\widehat{\mathbb{F}_q}}\prod_{i=1}^{l(g)}S(\psi,l_i(g))$$

as desired. □

3.2 Cohomology and Representation Theory

3.2.1 Definition of Cohomology Groups

We will frequently study varieties via their ℓ-adic étale cohomology groups, and we will now establish some notation for use later in the thesis. For any smooth, projective variety $\mathscr{X}$, we will denote by $H^i(\mathscr{X})$ the cohomology group

$$H^i(\mathscr{X}):=H^i(\mathscr{X},K_\ell):=\varprojlim_m H^i_{\acute{e}t}(\mathscr{X}\times\mathrm{Spec}\ \overline{\mathbb{F}_q},\mathbb{Z}/\ell^m\mathbb{Z})\otimes K_\ell$$

where $l\neq p$ is prime and K_ℓ is a finite algebraic extension of $\mathbb{Q}_\ell$ (we will discuss K_ℓ in more detail momentarily). More details on the definition of these cohomology groups can be found in the text of Freitag and Kiehl [9]. Specifically, more information on the definition of $H^i_{\acute{e}t}(L\times\mathrm{Spec}\ \overline{\mathbb{F}_q},\mathbb{Z}/\ell^m\mathbb{Z})$ (for a fixed m) can be found in Section 1.2. Discussion of the inverse limit taken above, as well as the tensor product with K_ℓ, can be found in Sections 1.4 and 1.12.

Key properties of the cohomology groups $H^i(\mathscr{X})$ are discussed in Chapter 4 of [9]. In particular, the polynomial

$$\det(1 - TF|H^i(\mathscr{X})),$$

does not depend on the choice of K_ℓ or on the choice of a prime ℓ. We will consider $\mathscr{X}$ with an action of a finite group G, and we will always assume that K_ℓ has sufficient scalars to realize all the irreducible complex representations of G with respect to some complex embedding $\nu : K_\ell \to \mathbb{C}$. We will now fix a K_ℓ large enough to realize all the complex representations of both $G = S_n$ and $G = \mathbb{F}_q$ as well as an embedding ν.

Deligne proved in 1974 [8] that if α is an eigenvalue of Frobenius on $H^i(\mathscr{X})$, then $|\nu(\alpha)| = q^{i/2}$ (also discussed in Chapter 4 of [9]). In the following chapters we will make repeated and essential use of this fact. By the Lefschetz fixed point theorem (discussed further in Section III.19), the zeta function of $\mathscr{X}$ is the alternating product of the characteristic polynomials of Frobenius on its cohomology groups, and thus the zeta zeroes of $X_{f,q}$ have absolute value $\sqrt{q}$. As their absolute values are known, we emphasize again that the results presented in the following chapters are implicitly or explicitly statements about the arguments of the zeta zeroes of $X_{f,q}$.

For a second opinion regarding these cohomology groups, the interested reader should see Milne's lecture notes [22] or go straight to the source in SGA 4.5 [7].

In what follows, we will need a notation for the dimensions of the cohomology groups. For any smooth, projective variety $\mathscr{X}$, let $h_i(\mathscr{X})$ denote the dimension of $H^i(\mathscr{X})$ as a vector space over K_ℓ.

3.2.2 Cohomology of Smooth Projective Hypersurfaces

In this section we give the Betti numbers of a smooth projective hypersurface. We say "the" because these Betti numbers are determined solely by the degree and the dimension of the hypersurface, and we will need to use this fact in Section 3.4. A smooth projective hypersurface has only one Betti number which is not 0 or 1, and this will simplify our later study of $H^{n-1}(Y'_{n,f,q})$ as an S_n representation.

The Weil bound, discussed in Chapter I, can be deduced from the Lefschetz fixed point theorem, the Riemann hypothesis for curves, and the fact that $h_1(X_{f,q}) = (d-1)(q-1)$. All of these ingredients generalize easily to higher dimension, and in Chapter IV we will discuss a similar bound for $Y'_{n,f,q}$ and a related result of Rojas-Leon (Theorem 2.1 of [24]).

Proposition III.9. *Suppose that $\mathscr{X}$ is a smooth, projective hypersurface of degree d. If $i \neq \dim \mathscr{X}$ then $h_i = 0$ for i odd and $h_i = 1$ for i even. In the remaining case*

$$h_{\dim \mathscr{X}} = \frac{(d-1)^{n+1} + (-1)^n(d-1)}{d}.$$

In particular, the closed generalized Fermat variety $Y'_{n,f,q}$ and the Fermat variety $Z_{n,d,q}$ are smooth projective hypersurfaces and they have the Betti numbers described above.

Proof. A proof of this result can be found in Section 2.6 of Zak [38]. □

3.3 Fermat Varieties

In this section, we will prove propositions about the Fermat variety $Z_{n,d,q}$ (defined in Section 3.1.1 above or Section 3.3.1 below). Later, we will apply Theorem III.18 to show that similar propositions about $Y_{n,f,q}$ hold, and we will need these facts about

$Y_{n,f,q}$ in Chapters IV and V. We are also interested in $Z_{n,d,q}$ because it is isomorphic to $Y'_{n,f,q}$'s subvariety at ∞, as proven in Proposition III.4.

3.3.1 Definitions Related to the Fermat Variety $Z_{n,d,q}$

We will retain the assumption that $(d, q) = 1$. Let $Z_{n,d,q}$ denote $(n-2)$ dimensional, smooth, projective Fermat variety over $\mathbb{F}_q$ defined by the polynomial $\sum_{i=1}^{n} x_i^d$. The symmetric group S_n acts by permutation of coordinates on this variety, but $Z_{n,d,q}$ is especially useful because it has an additional group action.

Definition III.10. Let μ_d denote the group of d-th roots of unity in $\overline{\mathbb{F}_q}$

In Section 3.3.2 we will see that μ_d^{n-1} acts on $Z_{n,d,q}$ (although this action need not be defined over $\mathbb{F}_q$). We will be interested in one particular subset of μ_d^{n-1}.

$$\mathscr{A}_n^d := \{a = (a_1, ..., a_{n-1}) \in \mu_d^{n-1} : \prod_{i=1}^{n-1} a_i \neq 1, a_1, ..., a_{n-1} \neq 1\} \tag{3.5}$$

The isotypic components of $H^{n-1}(Z_{n,d,q})$, each of them 1-dimensional, correspond bijectively with the elements of this subset. In Proposition 3.3.3 we will prove that S_n acts on $H^{n-1}(Z_{n,d,q})$ by permuting the characters of μ_d^{n-1} and that $\mathscr{A}_n^d$ will allow us an explicit description of these permutations.

3.3.2 μ_d^{n-1} Action

Over any finite field containing the d-th roots of unity the Fermat variety $Z_{n,d,q}$ has an action of μ_d^{n-1}. An element $(a_1, ..., a_{n-1})$ of μ_d^{n-1} acts by the automorphism

$$[t_1 : ... : t_{n-1} : t_n] \mapsto [a_1 t_1 : ... : a_{n-1} t_{n-1} : t_n].$$

$H^{n-1}(Z_n)$ has a decomposition into isotypics corresponding to the irreducible representations of μ_d^{n-1}. As μ_d is commutative, these irreducibles are $(n-1)$-fold products of the characters in $\widehat{\mu_d}$. Now define

$$\mathscr{A}_n^d := \{a = (a_1, ..., a_{n-1}) \in \mu_d^{n-1} : \prod_{i=1}^{n-1} a_i \neq 1, a_1, ..., a_{n-1} \neq 1\}$$

and the following description of $H^{n-1}(Z_{n,d,q})$:

Proposition III.11. *The isotypic components of $H^{n-1}(Z_{n,d,q})$ are in bijective correspondence with the elements of $\mathscr{A}_n^d$.*

Discussion of the results of this section can be found in Chapters 1 and 2 of Gouvea and Yui [11]. We will also consider the set of characters

$$\mathscr{B}_n^d := \{a = (a_1, ..., a_n) \in \mu_d^n : \prod_{i=1}^{n} a_i = 1, a_1, ..., a_n \neq 1\}$$

which we will use in the following section in our description of the S_n action. Note that for fixed n and d the sets $\mathscr{A}_n^d$ and $\mathscr{B}_n^d$ are bijective under the map $a \in \mathscr{B}_n^d \mapsto (a_1, ..., a_{n-1}, -\prod_{i=1}^{n-1} a_i)$, and that $\mathscr{B}_n^d$ is $\mathfrak{A}_{n+2}^d$ in the notation of Gouvea and Yui.

3.3.3 Permutation of μ_d^{n-1} Characters

Proposition III.12. *S_n acts on $H^{n-1}(Z_{n,d,q})$ via permutation of characters, with a given $g \in S_n$ acting on the set $\mathscr{A}_n^d$ as it does on the corresponding element of $\mathscr{B}_n^d$.*

Proof. Let $\tau : \langle \mu_d^{n-1}, S_n \rangle \to \mathrm{Aut}(H^{n-1}(Y'_{n,f,q}))$ denote the functorial representation of S_n on $H^{n-1}(Y'_{n,f,q})$. Note that for any $t \in \mu_d^{n-1}$ and $g \in S_n$ we have that $g^{-1}tg \in \mu_d^{n-1}$, that $\alpha \mapsto \tau(g^{-1}\alpha g)$ gives a representation of μ_d^{n-1} which must also decompose into isotypics, and thus that any eigenvector of τ must also be one of this representation. It follows that g acts by permutation of characters, and computing the map $(t \mapsto \chi(t)) \mapsto (t \mapsto \chi(g^{-1}tg))$ for $\chi \in \mathscr{A}_n^d$ verifies that this permutation is the obvious one induced on the corresponding elements of $\mathscr{B}_n^d$. □

3.3.4 Irreducible Decomposition of $H^{n-1}(Z_{n,d,q})$

In this section we summarize some facts about the representation theory of S_n proven in Sagan [27]. We will use the well-known correspondence between partitions of n and irreducible representations of S_n; given a partition λ (a sequence of positive integers λ_i with $\lambda_i \geq \lambda_{i+1}$ and $\sum_{i=1}^{k} \lambda_i = n$) we will denote the associated irreducible V_λ. We will make oblique references to Young tableaux, but for the purposes of this thesis we need only assume that any irreducible representation of S_n has a positive integer invariant k which we will refer to as the number of rows in its tableaux, and that if W_n is the standard representation, then $\bigwedge^i W_n$ is the irreducible representation corresponding to $\lambda = (n-i, 1, ..., 1)$ and it has $i+1$ rows in its Young tableaux for $0 \leq i \leq n-1$.

The eventual goal of this section is to study the decomposition of the S_n representation $H^{n-1}(Z_{n+1,d,q})$ into irreducibles. In Section 3.4, we will show this decomposition is the same as that of $H^{n-1}(Y'_{n,f,q})$. First we need to establish some notation.

- Let $\mathscr{P}_{n,k}$ denote the set of partitions of n with k parts.
- For $\lambda \in \mathscr{P}_{n,k}$ define $k(\lambda) := k$.
- Define $\binom{n}{\lambda} := \binom{n}{\lambda_1, ..., \lambda_k}$
- For any $\lambda \in \mathscr{P}_{n,k}$ with $n = \sum_{i=1}^{k} \lambda_i$ let $S_\lambda := \prod_{i=1}^{k} S_{\lambda_i}$.
- Let $M^\lambda := \mathrm{Ind}_{S_\lambda}^{S_n} 1$ (see Theorem 2.1.12 of [27]).
- For any $\overline{\chi} \in \mathscr{A}_n^d$ let $\lambda(\chi)$ denote the partition of n obtained by considering the multiplicity of each $\chi \in \mu_d$ in the corresponding element of $\mathscr{B}_n^d$.
- Let $i_{(j)}$ denote the Pochhammer symbol $i_{(j)} := \binom{i}{j} j!$.
- Let W_n denote the standard representation of S_n.

We now summarize the needed results proven in Chapter II of Sagan [27].

Proposition III.13. *For any $\overline{\chi} := (\chi_1, ..., \chi_{n-1}) \in \mathscr{A}_n^d$ the cyclic S_n-representation $S_n \cdot H^{n-1}(Z_{n,d,q})^{\overline{\chi}}$ is isomorphic to $M^{\lambda(\overline{\chi})}$.*

Proof. This proposition follows from Proposition 3.3.3, Proposition 1.12.3 of [27], and Theorem 2.1.12 of [27]. More useful discussion can be found on page 54 of [27]. □

Proposition III.14. *The multiplicity of* $\bigwedge^i W_n$ *in an irreducible decomposition of* M^λ *is* $\binom{k(\lambda)}{i}$.

Proof. Here $\bigwedge^i W_n \cong V_\lambda$ for $\lambda = (n-i, 1, ..., 1)$, and the desired result follows from Young's rule (Theorem 2.11.2 of [27]). □

In Chapter V, we will be interested in the existence of irreducible representations of S_n with trivial isotypic component in $H^{n-1}(Y'_{n,f,q})$. Later, we will prove that $H^{n-1}(Y'_{n,f,q})$ has the same decomposition into irreducibles as the Fermat variety of the same dimension and apply the corollary below.

Corollary III.15. *If* $i \geq d-1$, *then* $\bigwedge^i W_n$ *does not occur in a decomposition of* $H^{n-1}(Z_{n+1,d,q})$ *into irreducibles.*

Proof. This corollary is immediate from Proposition III.14. □

3.4 Comparing the S_n-Representations $H^{n-1}(Y_{n,f,q})$ and $H^{n-1}(Z_{n+1,d,q})$

In this section, we will compare the S_n-representation arising from the variety $Y'_{n,f,q}$ to that of the Fermat variety of like dimension and degree. In particular, in Theorem III.18 we will show that these two representations have the same character and thus the same irreducible decomposition. We will do this by relating the characters of these representations to the fixed loci of the corresponding $g \in S_n$ and proving that these fixed loci are smooth, complete varieties of like dimension and degree in both cases.

3.4.1 Definitions Related to Comparing Representations

Later we will apply the Lefschetz fixed point theorem. This will allow us to relate the Lefschetz number of an automorphism g of $Y'_{n,f,q}$ to properties of its fixed locus.

Definition III.16. : For any smooth projective variety $\mathscr{X}$ and any automorphism g of $\mathscr{X}$ defined over, we define the *Lefschetz number* of g to be the integer

$$\rho(g) := \sum_{i=0}^{2\dim\mathscr{X}} (-1)^i \operatorname{Tr}(g|H^i(\mathscr{X})).$$

Specifically, the Lefschetz fixed point theorem relates the Lefschetz number of g to the Euler characteristic of its fixed locus.

Definition III.17. For any smooth projective variety $\mathscr{X}$, we define the *Euler characteristic* of $\mathscr{X}$ to be the integer

$$e(\mathscr{X}) := \sum_{i=0}^{2\dim\mathscr{X}} (-1)^i \operatorname{Tr}(I|H^i(\mathscr{X}))$$

for $I : \mathscr{X} \to \mathscr{X}$ the identity map.

In what follows, we will prove that for each g, the fixed loci of g on $Y'_{n,f,q}$ and $Z_{n+1,d,q}$ have the same Euler characteristic and thus that g has the same Lefschetz number in both cases. By Proposition III.9, these varieties each have only one cohomology group with dimension $\notin \{0, 1\}$, and it follows that the S_n-representations $H^{n-1}(Y_{n,f,q})$ and $H^{n-1}(Z_{n+1,d,q})$ have the same character.

3.4.2 The Comparison Theorem

The primary goal of this section is to prove the theorem below. Note that we will consider the action of S_n on $Z_{n+1,d,q}$, even though this variety has an action of S_{n+1}. In the following, we fix an injection $S_n \to S_{n+1}$ such that each $g \in S_n$ fixes the x_{n+1} coordinate on $Z_{n+1,d,q}$.

Theorem III.18. *If f is n-smooth and $(d, q) = 1$, then for all $g \in S_n$*

$$\rho_{Y'_{n,f,q}}(g) = \rho_{Z_{n+1,d,q}}(g).$$

Note that by Proposition III.9 , it follows that the S_n-representations $H^1(X_{f,q})$ and $H^{n-1}(Z_{n+1,d,q})$ have the same character and thus the same decomposition into irreducibles.

3.4.3 The Lefschetz Fixed Point Theorem

In Chapters IV and V we will require knowledge of $H^{n-1}(Y'_{n,f,q})$ as an S_n-representation. By Proposition III.9, we know that $Y'_{n,f,q}$ has only one cohomology group whose dimension is not 0 or 1 and thus to compute a decomposition of $H^{n-1}(Y'_{n,f,q})$ it is sufficient to know the Lefschetz number (see Definition III.16) of each $g \in S_n$.

Theorem III.19. *(The Lefschetz Fixed Point Theorem) Suppose g is an automorphism of dimensional smooth projective variety $\mathscr{X}$, as above. If g has fixed locus $\mathscr{X}_g$, then*

$$\rho(g) = e(\mathscr{X}_g)$$

where $e(\mathscr{X}_g) := \sum_{i=0}^{2\dim \mathscr{X}_g} (-1)^i \operatorname{Tr}(I_{\mathscr{X}} | H^i(\mathscr{X}_g))$ denotes the Euler characteristic of $\mathscr{X}_g$.

Proof. Discussion of this result can be found on page 111 of [1]. □

3.4.4 Fixed Loci on $Y_{n,f,q}$ and $Z_{n,d,q}$

We will now prove some properties of the fixed loci $\operatorname{Fix}(g \circ F | Y_{n,f,q})$ and $\operatorname{Fix}(g \circ F | Z_{n,d,q})$. We will use the proposition below in our proof of Theorem III.18.

Proposition III.20. *Suppose g is an element of S_n. Define $\mathscr{X}_Y := Fix(g|Y'_{n,f,q})$ and $\mathscr{X}_Z := Fix(g|Z_{n+1,d,q})$, both subvarieties of $\mathbb{P}^n$. If $Y'_{n,f,q}$ is smooth, then*

1. *$\mathscr{X}_Z$ and $\mathscr{X}_Y$ are each isomorphic to respective disjoint unions of smooth projective hypersurfaces.*

2. *$\mathscr{Z}_Z \cap \mathbb{V}(x_{n+1})$ (in the Fermat variety case) and $\mathscr{Z}_Z \cap \mathbb{V}(x_0)$ (in the $Y'_{n,f,q}$ case) are each isomorphic to an $(n-2)$-dimensional smooth projective hypersurface.*

Proof. We will first prove that the fixed loci on a Fermat variety are isomorphic to disjoint unions of smooth projective hypersurfaces. For notational reasons we will work with $Z_{n,d,q}$ but the arguments given are valid for any n. For any $g \in S_n$ define

$$Z_g := \mathbb{V}(\sum_{i=1}^{l(g)} l_i(g) x_i^d) \subset \mathbb{P}^{l(g)-1}$$

and a map

$$\tau_{g,1} : Z_g \to Z_{n,d,q}$$

such that

$$[t_1 : ... : t_l] \mapsto [t_1 : t_1 ... : t_1 : t_2 : t_2 ... : t_2 : ...]$$

with t_i occurring $l_i(g)$ times. Let $u(g)$ denote the greatest common divisor of the $l_i(g)$ and $U(g)$ the collection of $u(g)$-th roots of unity. For any such g and $\zeta \in U(g) \setminus \{1\}$ define

$$\tau_{g,\zeta} : Z_g \to Z_{n,d,q}$$

$$[t_1 : ... : t_l] \mapsto [t_1 : \zeta t_1 ... : \zeta^{n-1} t_1 : t_2 : \zeta t_2 ... : \zeta^{n-1} t_2 : ...]$$

with t_i occurring $l_i(g)$ times once again. Note that these maps are closed embeddings when d does not divide n, $\tau_{g,1}$ is always a closed embedding, their images are fixed by g, and for $\zeta_1 \neq \zeta_2$ the images of τ_{g,ζ_1} and τ_{g,ζ_2} are disjoint. We will show that the fixed locus of g is the precisely the set of images of the $\tau_{g,\zeta}$ for $\zeta \in U(g)$. Suppose $[t_1 : ... : t_n]$ is fixed by g_1, and without loss of generality that g_1 acts as an $l_1(g)$ cycle on $t_1, ..., t_{l(g)}$, so we have that

$$g \cdot [t_1 : ... : t_n] = [t_1 : ... : t_n] \Rightarrow$$

$$[t_{l_1(g)} : t_1 : ... : t_{l_1(g)-1} : t_{l_1(g)+1} : .. : t_n] = [t_1 : ... : t_n]$$

and this implies that for some $l_1(g)$-th root of unity ζ_0 the t_i satisfy a relation for $i \in \{1, ..., l_1(g)\}$

$$x_i - \zeta_0 x_{i+1} = 0$$

with i considered modulo $l_1(g)$. We introduce the x_i because we will soon consider the set of $(t_1 : .. : t_n)$ which simultaneously satisfy all such relations. Each g_i generates such a relation, and the set of such relations associated to a fixed ζ_0 and all g_i has either $\emptyset$ or the image of τ_{g,ζ_0} as its vanishing set. As all Z_g are smooth, the $\tau_{g,\zeta}$ are closed embeddings with disjoint image, and all fixed points of g lie on one of these images, the first conclusion of the proposition is true for Fermat varieties.

For any g containing a 1-cycle, we have that $u(g) = 1$ and it is immediate from the above that $\tau_{g,1}$ is the unique component $\mathscr{Z}_Z := \mathrm{Fix}(g|Z_{n,d,q})$ and that its intersection with $\mathbb{V}(x_n)$ satisfies the second conclusion of the proposition.

Now define $Y_{g,n,f} := \mathbb{V}(l_1(g)f(y_1) + ... + l_l(g)f(y_l)) \subset \mathbb{A}^{l(g)}$ and let $Y'_{g,n,f}$ denote its projective closure. As in Proposition III.7 , the Jacobian criterion implies that for this variety to have a singularity, there must be a relation $\sum_{i=1}^{l} l_i(g)f(a_i) = 0$ with the a_i among the roots of $f'(x)$, and this implies a similar relation of n terms among $f(a_i)$. By hypothesis, no such relation exists, and $Y'_{g,n,f}$ is smooth. Now consider the map

$$\tau_{g,n,f} : Y'_{g,n,f} \to Y'_{n,f,q}$$

defined by analogy with $\tau_{g,1}$ and identically with it at infinity. The intersection of its image with the $x_0 = 0$ section of $Y'_{n,f,q}$ is Z_g and by the argument above it contains any fixed point of g lying in $Y_{n,f,q}$, and thus in any fixed point of g is contained in this image or in the image of a smooth projective hypersurface on the $x_0 = 0$ section, and the proof is complete. □

3.4.5 Proof of Theorem III.18

We will now complete the proof of this section's main theorem.

Proof of Theorem III.18. It follows from Section 3.2.2 that the Euler characteristic of an i-dimensional smooth projective hypersurface depends only on i and the degree d. Let $e(i,d)$ denote the Euler characteristic of such a hypersurface with the given dimension and degree. We will prove the proposition by proving the two equalities

$$(\rho_{Y'_{n,f}} - \rho_{Z_{n,d,q}})(g) = e(l(g)-1,d) - e(l(g)-2,d)$$

$$(\rho_{Z_{n+1,d,q}}|_{S_n} - \rho_{Z_{n,d,q}})(g) = e(l(g)-1,d) - e(l(g)-2,d)$$

from which the result follows by an algebraic manipulation. Note that both fixed loci are disjoint unions of smooth, irreducible subvarieties. As the Euler characteristic is additive on disjoint unions and the image $\tau_{g,n,f}$ is the only component of the fixed locus of g on $Y'_{n,f,q}$ which intersects $\mathbb{V}(x_0)$, we have that

$$\rho_{Y'_{n,f,q}} := e(l-1,d) - e(l-2,d) + \sum_{h \in H} e(h)$$

where H is the set of components which lie entirely in $\mathbb{V}(x_0)$. As the x_{n+1} section of $Z_{n+1,d,q}$ in $\mathbb{P}^n$ and x_0 section of $Y'_{n,f,q}$ in $\mathbb{P}^n$ are both isomorphic to $Z_{n,d,q}$, it is sufficient to prove that $\mathrm{Fix}(g|Z_{n+1,d,q})$ has only one component which intersects $\mathbb{V}(x_{n+1})$ and also produces a section isomorphic to an $(n-2)$ dimensional smooth projective hypersurface. By Proposition III.20, we are done. □

CHAPTER IV

Archimedean Bounds

4.1 Discussion of Theorem I.4

In this chapter we prove bounds for the number of $\mathbb{F}_{q^n}$-rational points on affine Artin-Schreier curves. Our proofs will make use of the auxiliary affine variety $Y_{n,f,q}$ covered in Chapter III and its projective closure $Y'_{n,f,q}$. We will prove a bound stated in terms of the multiplicities of certain irreducibles in the decomposition of the S_n-representation $H^{n-1}(Y'_{n,f,q})$. We will then use the results of the preceeding chapter to show that the constant $C_{d,n}$ given in the theorem is in fact the sum of these multiplicities.

4.1.1 Definitions Related to Archimedean Bounds

Let $q = p^N$ be a power of a prime p and $f \in \mathbb{F}_q[x]$ a non-constant poynomial of degree d with $(d, q) = 1$. Let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. In this chapter, we will prove bounds for $M_{f,q,n} := |U_{f,q}(\mathbb{F}_{q^n})|$.

We will study the affine variety $Y_{n,f,q}$ defined over $\mathbb{F}_q$ by the equation $\sum_{i=1}^{n} f(x_i)$, as well as its projective closure $Y'_{n,f,q}$. These varieties are the primary objects studied in Chapter III, and we will apply many of the propositions of that chapter. In particular, we will show how the irreducible decomposition $H^{n-1}(Y'_{n,f,q})$ as an S_n-representation is related to bounds for $M_{f,q,n}$.

Let W_n denote the standard representation of S_n and $r_i(n,d)$ the multiplicity with which the representation $\bigwedge^i W_n$ appears in an irreducible decomposition of the S_n-representation $H^{n-1}(Y'_{n,f,q})$. We will prove a bound for $M_{f,q,n}$ in terms of the sum of these multiplicities $r(n,d) := \sum_{i=1} r_i(n,d)$. We will then use Chapter III's description of $H^{n-1}(Y'_{n,f,q})$ in terms of $H^{n-1}(Z_{n+1,d,q})$ and the set

$$\mathscr{A}_n^d := \{a = (a_1, ..., a_{n-1}) \in \mu_d^{n-1} : \prod_{i=1}^{n-1} a_i \neq 1, a_1, ..., a_{n-1} \neq 1\}$$

to show that $r(n,d)$ is equal to the constant

$$C_{d,n} := \sum_{k=1}^{d-1} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{d-1} \frac{(d-1)_{(k)} \binom{k}{i}}{\binom{n}{\lambda}}$$

appearing in the theorem.

We will be particularly interested in the automorphism ϕ of $Y_{n,f,q}$ (or of $Z_{n,d,q}$) given by cyclic permutation of coordinates $x_i \mapsto x_{i+1}$. In what follows, we will crucially apply Proposition III.8 , but only in this $g = \phi$ case.

4.1.2 Discussion of Results

In this chapter, we will prove a bound for $M_{f,q,n} := |U_{f,q}(\mathbb{F}_{q^n})|$. Recall that $X_{f,q}(\mathbb{F}_{q^n})$ is $U_{f,q}(\mathbb{F}_{q^n})$ with one additional point at ∞, so we have that

$$M_{f,q,n} = q^n - \mathrm{Tr}(F|H^1(X_{f,q})).$$

In this section, we will primarily be interested in bounding the contribution $|M_{f,q,n} - q^n|$ of $H^1(X_{f,q})$ in the Archimedean norm. The most familiar result of this form is the Weil bound

$$|M_{f,q,n} - q^n| \leq (q-1)(d-1)q^{n/2}.$$

This result can be improved in a number of ways; recently Rojas-Leon [24] proved that

$$|M_{f,q,n} - q^n| \leq (d-1)^n \sqrt{q} q^{n/2}$$

by studying the auxiliary variety $Y_{n,f,q} := \mathbb{V}(\sum_{i=1}^n f(x_i))$. Informally speaking, this result is the Weil conjectures combined with the fact that the $(n-1)$-st Betti number of $Y'_{n,f,q}$ is less than $(d-1)^n$, but it implies cancellation among the eigenvalues of Frobenius on $H^1(X_{f,q})$ itself when $(d-1)^{n-1} \ll \sqrt{q}$. We refer the reader to Section 1.5 for discussion of another such bound due to Rojas-Leon and Wan [25], or to Section 4.1.3 for a comparison of this bound to Theorem IV.1.

In this chapter, we will show how to improve the approach of Rojas-Leon by studying the action of S_n on $Y_{n,f,q}$ and the representation of S_n on the cohomology of $Y'_{n,f,q}$. In the following, let $\mathscr{P}_{n,k}$ denote the set of partitions of n with k parts. Define $i_{(j)} := \binom{i}{j} j!$ and $\binom{n}{\lambda} := \binom{n}{\lambda_1,\ldots,\lambda_k}$. We will consider bounds for $M_{f,q,n}$ of the form

Theorem IV.1. *For any positive integers d and n define*

$$C_{d,n} := \sum_{k=1}^{d-1} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{d-1} \frac{(d-1)_{(k)}\binom{k}{i}}{\binom{n}{\lambda}}.$$

Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d,q) = 1$ and let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. If $f(x)$ is n-smooth (see Definition III.6) for $n \geq 2$, then

$$||U_{f,q}(\mathbb{F}_{q^n})| - q^n| \leq C_{d,n}\sqrt{q}q^{n/2} + C_{d,n-1}q^{n/2}.$$

For any fixed n the constant $C_{d,n}$ satisfies

$$\lim_{d\to\infty} \frac{C_{d,n}}{(d-1)^n} \frac{n!}{2^n - 1} = 1.$$

Note that we will prove $C_{d,n}$ has the required growth in d in Proposition IV.9. We will prove this result by relating the trace of Frobenius on $H^1(X_{f,q})$ to the trace of Frobenius on $H^{n-1}(Y'_{n,f,q})$ and using the structure of $H^{n-1}(Y'_{n,f,q})$ as an S_n-representation to prove it has a large subspace on which the trace of Frobenius is zero.

4.1.3 Comparison of $C_{d,n}$ with $C'_{d,n}$

In this section, we will compare the growth of the constant $C_{d,n}$ from Theorem IV.1 above

$$C_{d,n} := \sum_{k=1}^{d-1} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{d-1} \frac{(d-1)_{(k)} \binom{k}{i}}{\binom{n}{\lambda}}$$

to the constant $C'_{d,n}$ appearing in the similar result of Rojas-Leon and Wan (see [25])

$$C'_{d,n} := \sum_{i=0}^{n} |i-1| \binom{d-2+n-i}{n-i} \binom{d-1}{i}.$$

In particular, we will fix n and study the limit

$$c(n) := \lim_{d \to \infty} \frac{C'_{d,n}}{C_{d,n}}.$$

Below, we will provide an explicit formula for $c(n)$. Note that $c(n) \to 0$ as $n \to \infty$.

Proposition IV.2. *(Zieve) We have the limit*

$$\lim_{d \to \infty} \frac{C_{d,n}}{C'_{d,n}} = c(n) := \frac{1 - 2^{-n}}{\frac{1}{2}n - 1 + 2^{1-n}}.$$

Proof. If $d > n$ then, since $\mathscr{P}_{n,k}$ is empty when $k > n$, we have

$$C_{d,n} = \sum_{k=1}^{n} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{k} \frac{(d-1)_{(k)} \binom{k}{i}}{\binom{n}{\lambda}}.$$

Now let d be an indeterminate, and define $C_{d,n}$ by the above formula. For any fixed positive integer n, each summand is a polynomial in $\mathbb{Q}[d]$ of degree k. Thus $C_{d,n}$ is a polynomial of degree at most n, and the coefficient of d^n is

$$\sum_{\lambda \in \mathscr{P}_{n,n}} \sum_{i=1}^{n} \frac{\binom{n}{i}}{\binom{n}{\lambda}}.$$

Since $\mathscr{P}_{n,n} = \{(1, 1, 1, ..., 1)\}$, this coefficient equals $\sum_{i=1}^{n} \frac{\binom{n}{i}}{n!} = \frac{2^n - 1}{n!}$. Likewise, for any fixed positive integer n the expression

$$C'_{d,n} = \sum_{i=0}^{n} |i-1| \binom{d-2+n-i}{n-i} \binom{d-1}{i}$$

is a polynomial in $\mathbb{Z}[d]$ of degree at most n, and the coefficient of d^n in this expression is

$$\begin{aligned}\sum_{i=0}^{n}\frac{|i-1|}{(n-i)!i!} &= \frac{2}{n!}+\sum_{i=0}^{n}\frac{i-1}{(n-i)!i!}\\ &= \frac{2}{n!}+\frac{1}{n!}(\sum_{i=0}^{n} i\binom{n}{i}-\sum_{i=0}^{n}\binom{n}{i})\\ &= \frac{2}{n!}+\frac{1}{n!}\big(n2^{n-1}-2^n\big)\\ &= \frac{2+(n-2)2^{n-1}}{n!}\end{aligned}$$

It follows that

$$\lim_{d\to\infty}\frac{C_{d,n}}{C'_{d,n}}=\frac{1-2^{-n}}{\frac{1}{2}n-1+2^{1-n}}.$$ □

4.1.4 The Rojas-Leon Bound

We prove Theorem 2.1 of Rojas-Leon's paper [24] and then explain its relationship with Theorem IV.1.

Theorem IV.3. *(Rojas-Leon) Suppose $f\in\mathbb{F}_{q^n}[x]$ has degree d with $(d,q)=1$. If $Y'_{n,f,q}$ is smooth, then*

$$|M_{f,q,n}-q^n|\le(d-1)^n\sqrt{q}q^{n/2}$$

Proof. This proof follows that of Rojas-Leon. $Y'_{n,f,q}$ is smooth by hypothesis, so $Y_{n,f,q}$ and $Z_{n,d,q}$ are smoothas well. By Proposition 3.2.2, because $Y'_{n,f,q}$ and $Z_{n,d,q}$ are smooth, projective hypersurfaces the dimension of $H^{n-1}(Y'_{n,f,q})$ satisfies the identity of Section 3.2.2

$$h_{n-1}(Y'_{n,f,q})=\frac{(d-1)^{n+1}+(-1)^{n+1}(d-1)}{d},$$

with a similar identity for $h_{n-2}(Z_{n,d,q})$. In Proposition III.4, we proved for $n\ge 2$ that $Y'_{n,f,q}=Y_{n,f,q}\cup Z_{n,d,q}$, and by Deligne's results [8] the eigenvalues of the Frobenius map F on $H^{n-1}(Y'_{n,f,q})$ must have absolute value $q^{(n-1)/2}$. We then have that

$$|M_{f,q,n}-q^n|\le h_{n-1}(Y'_{n,f,q})q^{(n+1)/2}+h_{n-2}(Z_{n,d,q})q^{n/2} \tag{4.1}$$

and Proposition III.9 implies

$$|M_{f,q,n} - q^n| \leq (d-1)^n \sqrt{q} q^{n/2}.$$

the desired bound. □

Theorem IV.1 takes Rojas-Leon's theorem as its starting point and improves on the bound of Equation 4.1 (under the n-smoothness hypothesis) by analyzing $H^{n-1}(Y'_{n,f,q})$ as an S_n-representation. In next section, we will show how to construct a large subspace of $H^{n-1}(Y'_{n,f,q})$ on which the trace of $\phi \circ F$ is zero. In the proof, we will show that $C_{d,n}$ is equal to the sum of the multiplicities in $H^{n-1}(Y'_{n,f,q})$ of certain irreducible representations of S_n.

4.1.5 Bounds in Terms of the Sum of Multiplicities $r(n, d)$

In this section we will show how information about the decomposition of $H^{n-1}(Y'_{n,f,q})$ as an S_n-representation can be used to improve bounds of the form discussed in the previous section. We will make use of background information regarding the representation theory of S_n discussed in Section 3.3.4. Let W_n denote the standard representation of S_n. Define $r_i(n, d)$ to be the multiplicity with which $\bigwedge^i W_n$ appears in a decomposition of $H^{n-1}(Y'_{n,f,q})$ and $r(n, d) := \sum_{i=0}^{n} r_i(n, d)$. Note Proposition IV.4 is a bound stated in terms of $r(n, d)$. In the latter part of this chapter, we will bound $r(n, d)$ and deduce Theorem IV.1 from this bound and the proposition below.

Proposition IV.4. *If f is n-smooth (see Definition III.6) for $n \geq 2$, then*

$$|M_{f,q,n} - q^n| < r(n, d)\sqrt{q} q^{n/2} + r(n-1, d) q^{n/2}.$$

To prove this, we will need to use the corollary of the Frobenius character formula given below.

Corollary IV.5. *If V is an irreducible representation of S_n, then* $\mathrm{Tr}(\phi|V) = 0$ *unless* $V \cong \bigwedge^i W_n$ *for some i, in which case* $\mathrm{Tr}(\phi|V) = \pm 1$.

This result is immediate from the Frobenius character formula (stated in Proposition IV.6 below) and the fact that the Young tableaux of any $\bigwedge^i W_n$ has only one row with length greater than one.

To state the character formula, we need to introduce some notation. Suppose $V := V_\lambda$ is the irreducible representation corresponding to a partition λ (a sequence of integers λ_i with $\sum_{i=1}^k \lambda_i = n$). Define integer polynomials $\Delta(x) = \prod_{1 \leq i < j \leq k}(x_i - x_j)$ and $P_j(x) := \sum_{i=1}^k x_i^j$. Let k denote the number of rows in the Young tableaux of V and define $m_i := \lambda_i + k - i$. For any integer polynomial $g(x)$, let $[g(x)]_{(m_1,\dots,m_k)}$ denote the coefficient of $x_1^{m_1} \dots x_k^{m_k}$. We will consider a cycle decomposition $g = g_1 \dots g_{l(g)}$ with g_i an $l_i(g)$ cycle as before.

Proposition IV.6. *(Frobenius) We have the following formula for the character of V_λ:*

$$\mathrm{Tr}(g|V_\lambda) = \big[\Delta(x) \prod_{j=1}^k P_j(x)^{l_j(g)}\big]_{(m_1,\dots,m_k)}.$$

Proof. For a proof of this result, see Section 1.4 of Fulton and Harris [10]. □

Proof of Proposition IV.4. Recall from Proposition III.3 that if ϕ is the automorphism given by cyclic permutation of coordinates, then

$$q|\mathrm{Fix}(\phi \circ F|Y_{n,f})| = |U_{f,q}(\mathbb{F}_{q^n})|.$$

In the following, let $\mathscr{Z}_n$ denote either $Y'_{n,f,q}$ or $Z_{n+1,d,q}$. Each $g \in S_n$ commutes with the action of Frobenius on $\mathscr{Z}_n$ and thus the representation of Frobenius on $H^{n-1}(\mathscr{Z})$ is therefore an intertwining operator for the corresponding S_n-representation. Consider a decomposition

$$H^{n-1}(\mathscr{Z}) = \oplus_{i=1}^{r'(n,d)} V_i$$

into irreducibles, which by Schur's lemma may be chosen so that Frobenius acts as a scalar α_i on V_i. Without loss of generality we may assume that $V_1, ..., V_{r(n,d)}$ are the only irreducibles in the decomposition which are isomorphic to some $\bigwedge^i W_n$. We have

$$|\mathrm{Tr}(F|H^{n-1}(\mathscr{X}))| \leq \sum_{i=1}^{r'(n,d)} \mathrm{Tr}(\phi|V_i) \cdot \alpha_i$$

and this implies the bound

$$|\mathrm{Tr}(F|H^{n-1}(L_n))| \leq r(n,d)q^{(n-1)/2}. \tag{4.2}$$

By Corollary III.5, we have that

$$\frac{1}{q}M_{f,q,n} = |\mathrm{Fix}(\phi \circ F|Y'_{n,f,q})| - |\mathrm{Fix}(\phi \circ F|Z_{n,d,q})|.$$

By Proposition III.9 and III.19, it follows that

$$\frac{1}{q}M_{f,q,n} = \big(\sum_{i=1}^{n-1} q^i\big) + (-1)^{n-1}\mathrm{Tr}(F|H^{n-1}(Y'_{n,f,q})) - \big(\sum_{i=1}^{n-2} q^i\big) - (-1)^{n-2}\mathrm{Tr}(F|H^{n-2}(Z_{n,d,q}))$$

and then that

$$\frac{1}{q}M_{f,q,n} = q^{n-1} + (-1)^{n-1}\big(\mathrm{Tr}(F|H^{n-1}(Y'_{n,f,q})) + \mathrm{Tr}(F|H^{n-2}(Z_{n,d,q}))\big)$$

Combining this equality with the Equation 4.2, we have the desired result. □

The direct sum of the isotypic components of all the irreducibles not of the form $\bigwedge^i W_n$ is the previously discussed subspace of $H^{n-1}(Y'_{n,f,q})$ on which the trace of Frobenius is zero. For book-keeping reasons it is easier to state the corresponding bound for $M_{f,q,n}$ in terms of the complement of this subspace and the integer $r(n,d)$. In the following sections, we will use the results of Theorem III.18 and the results of Section 3.3.4 concerning to prove bounds for the multiplicities $r_i(n,d)$ and thus for $M_{f,q,n}$.

4.1.6 A Combinatorial Description of $r(n,d)$ Via Fermat Varieties

Let O denote the set of S_n orbits on $\mathscr{A}_n$ (recall that $\mathscr{A}_n$ is the subset of the character group of μ_d^{n-1} defined in Section 3.3.2). If $o' \in \mathscr{A}_n$ lies in an orbit o let o_χ denote the mutiplicity with which a given $\chi \in \widehat{\mu}_d$ appears in o'. For each such orbit o, let $\lambda(o)$ denote the partition obtained determined by the integers o_χ; this is well-defined as for any $g \in S_n$ passing from o' to go' permutes the o_χ.

Proposition IV.7. *Suppose that f is n-smooth for $n \geq 2$. We have that*

$$r(n,d) = \sum_{k=1}^{d-1} \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{i=1}^{d-1} \frac{(d-1)_{(k)} \binom{k}{i}}{\binom{n}{\lambda}}$$

for the sum of multiplicities $r(n,d) = \sum_{i=0}^{n-1} r_i(n,d)$, or equivalently we have that $r(d,n) = C_{d,n}$.

Proof. By the results proven in Section 3.3.4 and and Section 3.4 (we will retain the notation of these sections as well), we have that

$$\mathscr{A}_n^d \cong \sum_{\lambda \in \mathscr{P}_{n,k}} \sum_{\substack{o \in O \\ \xi(o) = \lambda}} M^\lambda$$

as representations of S_n. By standard results on the decomposition of cyclic S_n-representations discussed in Section 3.3.4, the multiplicity of $\bigwedge^i W_n$ in M^λ is $\binom{k(\lambda)}{i}$. The cyclic representation associated to any $o \in O$ has dimension $\binom{n}{\lambda(o)}$ and if $\sum_{i=1}^{k(\lambda)} =$ n there are $(d-1)_{(k(\lambda))}$ elements of $\mathscr{A}_n$ whose orbit corresponds to a given λ. We thus have

$$r_i(n) = \sum_{\lambda \in \mathscr{P}_n} \frac{(d-1)_{(k(\lambda))} \binom{k(\lambda)}{i}}{\binom{n}{\lambda}}$$

and thus

$$r(n) = \sum_{i=1}^{n} \sum_{\lambda \in \mathscr{P}_n} \frac{(d-1)_{(l(\lambda))} \binom{k(\lambda)}{i}}{\binom{n}{\lambda}}.$$

By breaking up the sum over $\mathscr{P}_n$ into sums over $\mathscr{P}_{n,k}$ we obtain the desired result. Note that we state the result in this way because the growth of $C_{d,n}$ is controlled by the growth of $\mathscr{P}_{n,d-1}$. □

4.1.7 Bounds for $r(n, d)$ as $d \to \infty$

Recall from Section 3.2.2 that h_{n-1} is approximately $(d-1)^n$. We will prove that any central function on S_n which is "small" on $g \in S_n$ with few cycles in their decomposition resembles the character of the regular representation. First, we will prove a needed lemma that holds for any finite group G.

Lemma IV.8. *Let κ be a central function on a finite group G such that for all $g \neq I_G$*

$$\frac{\kappa(g)}{\kappa(I)} < c < 1.$$

Let κ_1 be the character of an arbitrary irreducible representation V_{κ_1} of G. Suppose V_{κ_1} is the virtual representation corresponding to κ_1 and define $m_{\kappa_1}(n)$ to the multiplicity with which V_{κ_1} appears in a decomposition of the virtual representation $\otimes^n V_\kappa$. If $C := sup_{g \neq I}|\kappa_1(g)|$ then we have that

$$|\frac{m_{\kappa_1}(n)}{\kappa(I_G)} - \frac{\kappa_1(I_G)}{n!}| \leq Cc^n.$$

Proof. Consider the following central function on G:

$$f : g \mapsto \sum (\frac{m_{\kappa_1}(n)}{\kappa(I_G)} - \frac{\kappa_1(I_G)}{n!})\kappa_1(g)$$

By construction we have that

$$\langle f, \kappa_1 \rangle = \frac{m_{\kappa_1}(n)}{\kappa(I_G)} - \frac{\kappa_1(I_G)}{n!}$$

so we need only bound $\langle f, \kappa_1 \rangle$ for each χ. If Reg is the character of the regular representation, then

$$f(g) = (\frac{\kappa(g)}{\kappa(I_G)})^n - \frac{\mathrm{Reg}(g)}{n!}$$

and thus $f(I_G) = 0$. For $g \neq I_G$, the regular representation has trace zero and $\left(\frac{\kappa(g)}{\kappa(I_G)}\right)^n < c^n$. It follows that

$$\langle f, \kappa_1 \rangle := \frac{1}{n!} \sum_{g \in G} f(g)\kappa_1(g) \leq \frac{1}{n!} \sum_{g \in G} Cc^n = Cc^n$$

as desired. □

We need one more proposition to prove the final claim in Theorem IV.1. Note that we proved in Proposition IV.7 that $\sum_{i=1}^n r_i(n,d) = C_{d,n}$.

Proposition IV.9. *We have the limit*

$$\lim_{d \to \infty} \frac{r_i(n,d)}{h_{n-1,d}} = \frac{\binom{n}{i}}{n!}.$$

Proof. Let τ_d be the character of the representation of S_n arising functorially from its action on $H^{n-1}(Y'_{n,f,q})$. As we have shown previously, this central function is in fact determined only by d and not other information about f. By definition

$$r_i(n,d) := \frac{1}{n!} \sum_{g \in S_n} \mathrm{Tr}(g | \bigwedge^i W_n) \tau_d(g).$$

Via the exponential series we have that

$$\tau(g) = \sum_{m=1}^{\infty} \frac{\ln(\tau_d(g))^m}{m!}$$

and so we can rewrite the above

$$r_i(n,d) = \sum_{m=1}^{\infty} \langle \bigwedge^i W_n, \frac{\ln(\tau_d(g))^m}{m!} \rangle.$$

Note that for any positive integer m_0 we have that

$$\lim_{d \to \infty} \frac{\sum_{m=1}^{m_0} \langle \bigwedge^i W_n, \frac{\ln(\tau_d(g))^m}{m!} \rangle}{\sum_{m=m_0+1}^{\infty} \langle \bigwedge^i W_n, \frac{\ln(\tau_d(g))^m}{m!} \rangle} = 0$$

and the desired result then follows from Lemma IV.8 and the fact that $\bigwedge^i W_n$ has dimension $\binom{n}{i}$. □

In the following section, we will use the propositions proven earlier in this chapter to complete the proof of Theorem IV.1 .

4.1.8 Proof of the Main Theorem

Proof of Theorem IV.1. By Proposition IV.4, we have that

$$|M_{f,q,n} - q^n| \leq r(n,d)\sqrt{q}q^{n/2} + r(n-1,d)q^{n/2}$$

where $r(n,d) := \sum_{i=1}^{n} r_i(n)$ is the sum of the multiplicities $r_i(n,d)$ of the irreducibles $\bigwedge^i W_n$ in a decomposition of the S_n-representation $H^{n-1}(Y'_{n,f,q})$. In Proposition IV.7 we proved that $r(n,d)$ is equal to the constant $C_{d,n}$ defined in Theorem IV.1, so by substituting $C_{d,n}$ for $r(n,d)$ in the above inequality we have the desired bound. From Proposition IV.9 and Proposition III.9, we have that

$$\lim_{d\to\infty} \frac{r(n,d)}{(d-1)^n} \frac{n!}{2^n - 1} = 1.$$

for all positive integers n, and as we have shown that $r(n,d) = C_{d,n}$, the proof is complete. □

CHAPTER V

Relations Among Frobenius Eigenvalues

5.1 Discussion of Theorem I.6

In this section, we will prove that multiplicative algebraic relations exist among the Frobenius eigenvalues, or equivalently among the zeta zeroes, of a smooth, complete Artin-Schreier curve satisfying suitable hypotheses. In particular, we will use Proposition III.8 to relate the exponential sums $S(\psi, m)$ (defined in Section 3.1.1 or below) to the actions of Frobenius and S_n on $H^{n-1}(Y'_{n,f,q})$. We will use this proposition to show that certain algebraic expressions in the $S(\psi, m)$ are equal to zero. This implies that a certain rational function is constant, but we will also give another expression for this rational function in which products of the zeta zeroes of our curve occur as zeroes and poles. We will then deduce the main result, Theorem V.5, from the existence of this rational function and our contrasting descriptions of it.

5.1.1 Definitions Related to Relations Among Frobenius Eigenvalues

Let $q = p^N$ be a power of a prime p and $f \in \mathbb{F}_q[x]$ a non-constant poynomial of degree d with $(d, q) = 1$. Let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$ and $X_{f,q}$ its complete, smooth model. In this chapter, we will study the zeroes of the zeta function

$$Z(X_{f,q}, T) := \exp(\sum_{n\geq 1} |X_{f,q}(\mathbb{F}_{q^n})| \frac{T^n}{n}).$$

Lemma I.2 implies that these zeta zeroes are the reciprocals of the eigenvalues of Frobenius on $H^1(X_{f,q})$.

Definition V.1. For any $m \geq 1$ and $t \in \mathbb{F}_q$ we define the exponential sum

$$S(\psi, m, t) := \sum_{x \in \mathbb{F}_q^m} \psi(\mathrm{Tr}_{q,m} f(x) + t).$$

Observe that for any $t \in \mathbb{F}_q$

$$S(\psi, m, t) = \psi(mt) S(\psi, m, 0). \tag{5.1}$$

Let $F = F_{X_{f,q}}$ denote the Frobenius automorphism of $X_{f,q}$ defined in Section II.5. It follows from Proposition II.4 that

$$\sum_{1 \neq \psi \in \widehat{\mathbb{F}_q}} S(\psi, m, 0) = \mathrm{Tr}(F | H^1(X_{f,q})). \tag{5.2}$$

and in fact (see pp. 176-179 of [16])

$$\mathrm{Tr}(F | H^1(X_{f,q})^\psi) = S(\psi, m, 0). \tag{5.3}$$

Definition V.2. For any additive character ψ of $\mathbb{F}_q$ we define the generating function

$$W(\psi, T) := \exp(\sum_{m \geq 1} S(\psi, m, 0) \frac{T^m}{m}).$$

It follows from Equation 5.3 and Lemma I.2 that

$$W(\psi, T)^{-1} = \det(1 - TF | H^1(X_{f,q})^\psi).$$

In particular, $W(\psi, T)^{-1}$ is a polynomial.

In this chapter, we will also study sums defined via $Y'_{n,f,q}$.

Definition V.3. For any $g \in S_n$, $\psi \in \widehat{\mathbb{F}_q}$, $m \geq 1$, and $n \geq 2$ we define the exponential sum

$$R(g, \psi, m, n) := qq^{-m} \sum_{x \in \mathbb{F}_{q^m}} \psi(x) \mathrm{Fix}(g \circ F^m | Y'_{n,f+x/n,q}).$$

We will use these expoenential sums to define generating functions that we will use in the proof of Theorem V.5.

Definition V.4. For any $g \in S_n$, $\psi \in \widehat{\mathbb{F}_q}$, and $n \geq 1$ we define the generating function

$$Z(g, \psi, n, T) := \exp\big(\sum_{m \geq 1} R(g, \psi, m, n) \frac{T^m}{m}\big).$$

We will later show that $Z(g, \psi, n, T)$ is the reciprocal of a polynomial and prove the main theorem by showing for each ψ that a certain product of the polynomials $Z(g, \psi, n, T)$ and their reciprocals is equal to 1.

The sums $R(g, \psi, m, n)$ are of interest because we can relate them both to $H^{n-1}(Y'_{n,f,q})$ (directly) and to the sums $S(\psi, m, 0)$ (via Proposition III.8). Note that by Corollary III.5 we have $Y'_{n,f+x/n,q} = Y_{n,f+x/n,q} \cup Z_{n,d,q}$ for each x, so it is also true that

$$R(g, \psi, m, n) = qq^{-m} \sum_{x \in \mathbb{F}_{q^m}} \psi(x) \mathrm{Fix}(g \circ F^m | Y_{n,f+x/n,q})$$

and when $n < p$ we have that

$$\sum_{1 \neq \psi \in \widehat{\mathbb{F}_q^m}} R(g, \psi, m, n) = q \mathrm{Fix}(g \circ F^m | Y_{n,f,q}). \tag{5.4}$$

Where $g = \phi$ the right hand side above is equal to $\mathrm{Tr}(F | H^1(X_{f,q}))$, a case we considered in more detail in Chapter IV.

In the following we will make frequent use of cycle decompositions for $g \in S_n$. As in Chapter III, we consider a decomposition of g into disjoint cycles with the form $g = g_1, ..., g_{l(g)}$ where g_i is an $l_i(g)$-cycle. Note that the identity is considered as the product of n 1-cycles.

5.1.2 Discussion of Results

In this chapter, we will focus on the zeta function $Z(X_{f,q},T) := \exp(\sum_{n\geq 1} |X_{f,q}(\mathbb{F}_{q^n})|\frac{T^n}{n})$ of $X_{f,q}$ defined using the integers $|X_{f,q}(\mathbb{F}_{q^n})|$. Recall that

$$Z(X_{f,q},T) = \frac{\det(1 - TF|H^1(X_{f,q}))}{(1-T)(1-qT)}.$$

Our eventual goal will be to be to show that there are multiplicative relations among the eigenvalues of Frobenius on $H^1(X_{f,q})$ and thus among the zeroes of $Z(X_{f,q},T)$. The main theorem of this chapter, stated below, uses the smoothness condition on $f(x)$ given in Definition III.6.

Theorem V.5. *Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d,q) = 1$, let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$, and let $X_{f,q}$ denote the smooth, complete model of $U_{f,q}$. Suppose n is any integer such that $d \leq n \leq p-1$ and that $f(x)+t$ is n-smooth for all $t \in \mathbb{F}_q$. For any $1 \neq \psi \in \widehat{\mathbb{F}_q}$ and any eigenvalue π of Frobenius on $H^1(X_{f,q})^{\psi}$ there exists an $i \in \{2,...,n\}$ and eigenvalues $\beta_1,...,\beta_n$ (not necessarily distinct) of Frobenius on $H^1(X_{f,q})^{\psi^i}$ such that*

$$\pi^n = \prod_{j=1}^{n} \beta_j.$$

The fixed point formula for $g\circ F$ given in Proposition III.8 implies that $H^{n-1}(Y'_{n,f,q})$ contains information about the zeroes of $Z(X_{f,q},T)$. Ostensibly this information is coarse, but in this chapter we will show how it can be used to prove that there are multiplicative relations among the zeta zeroes. Recall that Corollary III.15 states that certain irreducible representations have zero-dimensional isotypic component in $H^{n-1}(Z_{n,d,q})$ (and in $H^{n-1}(Y'_{n,f,q})$ by Theorem III.18). We will consider the generating functions $Z(g,\psi,n,T)$ (defined in the previous section) and use Corollary III.15

to prove in Proposition V.7 that a certain product of these functions and their reciprocrals is constant. In Proposition V.6, we will prove that all the $Z(g, \psi, n, T)^{-1}$ are polynomials and show that their zeroes are certain products of the zeroes of $\det(1 - TF|H^1(X_{f,q})^{\psi^{l(g)}})$. In Section 5.1.4, we will deduce the theorem above from this rationality and the fact that the aforementioned product is constant.

Theorem V.5 relates the eigenvalues of Frobenius on $H^1(X_{f,q})^{\psi}$ to those on $H^1(X_{f,q})^{\psi^i}$, and thus the relations which occur depend in part on the structure of the group $\mathbb{F}_q^{\times}$.

5.1.3 From Vanishing Isotypics to Relations Among Rational Functions

In this section, we will prove that $Z(g, \psi, n, T)^{-1}$ is a polynomial as advertised. We will prove this by showing it is in fact equal to polynomial with particular zeroes, and we will crucially use this knowledge in the following sections.

Proposition V.6. *If $n < p$, then $Z(g, \psi, n, T)^{-1}$ is a polynomial and each of its roots has the form $\alpha_1^{-l_1(g)} \cdot ... \cdot \alpha_{l(g)}^{-l_{l(g)}(g)}$ for $l(g)$ eigenvalues $\alpha_1, ..., \alpha_{l(g)}$ of Frobenius on $H^1(X_{f,q})^{\psi^{-l(g)}}$. Moreover, all products of this form occur as roots.*

Proof. We will show that

$$R(g, \psi, m, n) = q \prod_{i=1}^{l(g)} \mathrm{Tr}(F^{ml_i(g)}|H^1(X_{f,q})^{\psi^{-l(g)}}). \tag{5.5}$$

Let $\mathscr{F}$ denote the set of functions $\{1, ..., l(g)\} \to \{1, ..., d-1\}$. Note that if $\pi_1, ..., \pi_{d-1}$ are the eigenvalues of Frobenius on $H^1(X_{f,q})^{\psi^{-l}}$, then for each positive integer m the right-hand side of Equation 5.5 is equal to

$$q \sum_{s \in \mathscr{F}} \big(\prod_{i=1}^{l(g)} \pi_{s(i)}^{l_i(g)} \big)^m$$

and the desired result follows from Lemma II.2. By Proposition III.8 and Equation 5.3 we have that

$$R(g, \psi, m, n) = qq^{-m} \sum_{x \in \mathbb{F}_{q^m}} \psi(x) \sum_{1 \neq \psi_0 \in \widehat{\mathbb{F}_{q^m}}} \prod_{i=1}^{l(g)} \mathrm{Tr}(F^{ml_i(g)}|H^1(X_{f+x/m,q})^{\psi_0})$$

By Equation 5.1, for any $t \in \mathbb{F}_q$ we have that

$$\psi(mt)S(\psi, m) := \sum_{x \in \mathbb{F}_q^m} \psi((\operatorname{Tr}_{q,n} f(x) + t))$$

and as $\psi(-) \mapsto \psi(m-)$ is a bijection on $\widehat{\mathbb{F}_{q^m}}$ we can rewrite our formula for $R(g, \psi, m, n)$

$$R(g, \psi, m, n) = qq^{-m} \sum_{x \in \mathbb{F}_{q^m}} \psi(x) \sum_{1 \neq \psi_0 \in \widehat{\mathbb{F}_{q^m}}} \prod_{i=1}^{l(g)} \psi_0(x) \operatorname{Tr}(F^{ml_i(g)} | H^1(X_{f,q})^{\psi_0})$$

before interchanging the order of summation inside to obtain

$$R(g, \psi, m, n) = qq^{-m} \sum_{1 \neq \psi_0 \in \widehat{\mathbb{F}_{q^m}}} \sum_{x \in \mathbb{F}_{q^m}} \psi(x)\psi_0^{l(g)}(x) \prod_{i=1}^{l(g)} \operatorname{Tr}(F^{ml_i(g)} | H^1(X_{f,q})^{\psi_0}).$$

For any ψ and ψ_0 the sum $\sum_{x \in \mathbb{F}_{q^m}} \psi(x)\psi_0^{l(g)}(x)$ is equal to q^m if $\psi^{-1} \neq \psi_0^{l(g)}$ and equal to 0 otherwise. We then have that the above is equal to

$$q \prod_{i=1}^{l(g)} \operatorname{Tr}(F^{ml_i(g)} | H^1(X_{f,q})^{\psi^{-l(g)}})$$

as desired. □

Proposition V.7. *Suppose V is an irreducible representation of S_n and ψ is a non-trivial character of $\mathbb{F}_q$. If $f(x) + t$ is n-smooth for all $t \in \mathbb{F}_q$ and the V-isotypic component $H^{n-1}(Y'_{n,f,q})^V$ of $H^{n-1}(Y'_{n,f,q})$ is zero-dimensional, then*

$$\prod_{g \in S_n} Z(g, \psi, n, T)^{\operatorname{Tr}(g^{-1}|V)} = 1.$$

Proof. Note that the sum

$$\sum_{g \in S_n} \operatorname{Tr}(g^{-1}|V) \operatorname{Tr}(g | H^{n-1}(Y'_{n,f,q}))$$

is equal to the multiplicity with which V appears in an irreducible decomposition of $H^{n-1}(Y'_{n,f,q})$, and it follows that the sum

$$\sum_{g \in S_n} \operatorname{Tr}(g^{-1}|V) \operatorname{Tr}(g \circ F | H^{n-1}(Y'_{n,f,q}))$$

gives the trace of Frobenius on $H^{n-1}(Y'_{n,f,q})^V$. As this subspace is zero-dimensional, the trace of Frobenius on it must be zero. We then have that

$$\prod_{g\in S_n} Z(g,\psi,n,T)^{\mathrm{Tr}(g^{-1}|V)} = \exp(\sum_{g\in S_n} \mathrm{Tr}(g^{-1}|V) \sum_{m\geq 1} R(g,\psi,m,n)\frac{T^m}{m}).$$

By interchanging the order of summation inside the exponential we obtain

$$\exp(\sum_{m\geq 1} \frac{T^m}{m} \sum_{g\in S_n} \mathrm{Tr}(g^{-1}|V) R(g,\psi,m,n)).$$

By the above and another change in the order of summation, this is equal to

$$\sum_{\psi\in\widehat{\mathbb{F}_q^m}} qq^{-m} \sum_{x\in\mathbb{F}_{q^m}} \psi(x) \sum_{g\in S_n} \mathrm{Tr}(g^{-1}|V)\mathrm{Fix}(g\circ F^m|Y'_{n,f+x/n,q})$$

and this sum must be zero for all m because

$$\sum_{g\in S_n} \mathrm{Tr}(g^{-1}|V)\mathrm{Fix}(g\circ F^m|Y'_{n,f+x/n,q})$$

is. The result follows. □

5.1.4 Proof of the Main Theorem

We will now complete the proof of Theorem V.5.

Proof. Let Alt denote the alternating representation of S_n. As Alt $\cong \bigwedge^{n-1} W_n$, Corollary III.15 implies the Alt-isotypic component of $H^{n-1}(Z_{n+1,d,q})$ has dimension zero. By Theorem III.18, it follows that the Alt-isotypic component of $H^{n-1}(Y'_{n,f,q})$ has dimension zero as well. Proposition V.7 states that for each non-trivial ψ we have

$$\prod_{g\in S_n} Z(g,\psi^{-1},n,T)^{\mathrm{Tr}(g^{-1}|\mathrm{Alt})} = 1.$$

Note that $\mathrm{Tr}(g^{-1}|\mathrm{Alt}) \in \{0,1\}$ for all $g\in S_n$, so $Z(g,\psi^{-1},n,T)$ occurs in the product above for all $g\in S_n$. Suppose π is an eigenvalue of Frobenius on $H^1(X_{f,q})^{\psi}$. Recall that ϕ denotes the n-cycle $x_i\mapsto x_{i+1}$. Note that $l(\phi)=1$, and for these n-cycles

Proposition V.6 states that π^{-n} is a zero of $Z(\phi, \psi^{-1}, n, T)^{-1}$. As the product above is trivial, there must exist some $g_1 \in S_n$ with $\mathrm{Tr}(g_1|\mathrm{Alt}) \neq \mathrm{Tr}(\phi|\mathrm{Alt})$ such that π^{-n} is zero of $Z(g_1, \psi^{-1}, n, T)$. Applying Proposition V.6 once again, this implies that there exist eigenvalues $\beta_1, ..., \beta_{l(g_1)}$ of Frobenius on $H^1(X_{f,q})^{\psi^{l(g_1)}}$ such that

$$\pi^{-n} = \beta_1^{-l_1(g_1)} \cdot ... \cdot \beta_{l(g_1)}^{-l_{l(g_1)}(g_1)}.$$

All elements of S_n with $l(g) = 1$ are in the same conjugacy class with ϕ and thus have the same trace on Alt, so $l(g_1)$ must be contained in $\{2, ..., n\}$ and the proof is complete. □

CHAPTER VI

Non-Archimedean Bounds

6.1 Discussion of Theorem I.11

In this section, we will prove congruences for the number of $\mathbb{F}_{q^n}$-rational points on an affine Artin-Schreier curve. This chapter is nearly independent of the rest of this thesis; the only result of the previous sections we will need is Corollary II.2, which relates the number of points on our affine curve to the roots of a certain polynomial. We will use this polynomial to define an $(n-1)$-dimensional auxiliary affine variety $L_{n,f,q}$ whose $\mathbb{F}_q$ points correspond bijectively with the $\mathbb{F}_{q^n}$ points of our curve. The main theorems of this section are then deduced by studying this affine variety.

6.1.1 Definitions Related to Non-Archimedean Bounds

Let $q = p^N$ be a power of a prime and $f(x)$ a non-constant polynomial in $\mathbb{F}_q[x]$ of degree d. As before, let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. In this chapter we will permit $f(x)$ with $(d, q) > 1$, and thus $U_{f,q}$ may be reducible. We will also permit $f(x)$ are not n-smooth. Once again, we study the number of $\mathbb{F}_{q^n}$-rational points $M_{f,q,n}$ on this affine curve

$$M_{f,q,n} := U_{f,q}(\mathbb{F}_{q^n}) := |\{(s,t) \in (\mathbb{F}_{q^n})^2 : t^q - t = f(s)\}| \tag{6.1}$$

Recall that in Chapter II we defined the trace polynomial

$$\mathrm{Tr}_{q,n}(x) := \sum_{i=0}^{n-1} x^{q^i} \tag{6.2}$$

and proved that

$$M_{f,q,n} = q|\{s \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q,n} f(s) = 0\}|.$$

In this chapter, we prove congruences for $M_{f,q,n}$ modulo powers of q. In some cases, it is not the degree of $f(x)$ that appears in these results but a smaller integer $\sigma_q(f)$.

Definition VI.1. For any positive integer m, let $\overline{\sigma}_q(m)$ denote the sum of the base q digits of m. If $f(x) = \sum_{i=0}^{d} c_i x^i$, define

$$\sigma_q(f) := \max_{\{i : c_i \neq 0\}} \overline{\sigma}_q(i).$$

Example VI.2. Consider $f(x) = x^{34} + x^{17}$ and $p = 3$. We will compute examples for $q = 3$ and $q = 9$. First, we have that

$$\overline{\sigma}_3(34) = 4 \quad \overline{\sigma}_3(17) = 5$$

$$\overline{\sigma}_9(34) = 10 \quad \overline{\sigma}_9(17) = 9$$

and thus that

$$\overline{\sigma}_3(f) = \max(\overline{\sigma}_3(34), \overline{\sigma}_3(17)) = 5$$

$$\overline{\sigma}_9(f) = \max(\overline{\sigma}_9(34), \overline{\sigma}_9(17)) = 10.$$

As in the other chapters of this thesis, our proofs will involve a sequence (one for each positive integer n) of auxiliary varieties of higher dimension. We will prove that for each n, there exists a polynomial $Q_n(\overline{x}) \in \mathbb{F}_q[x_1, ..., x_n]$ such that

$$|\{s \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q,n} f(s) = 0\}| = |\{(s_1, ..., s_n) \in \mathbb{F}_q^n : Q_n(\overline{s}) = 0\}|. \tag{6.3}$$

Let $L_{n,f,q}$ denote the $(n-1)$-dimensional affine variety defined over $\mathbb{F}_q$ by the polynomia Q_n. We will deduce the theorems of this chapter by studying this affine variety.

Note that we now have

$$|U_{f,q}(\mathbb{F}_{q^n})| = q|L_{n,f,q}(\mathbb{F}_q)| \tag{6.4}$$

Some of our congruences will be stated in terms of exponential sums. Let μ_d denote the group of d-th roots of unity in $\overline{\mathbb{F}_q}$ and suppose that χ and ψ are non-trivial characters of μ_d and $\mathbb{F}_q$ respectively. We will give a congruence for $M_{f,q,n}$ in terms of the Gauss sums

$$G_{q^n}(\psi, \chi) := -\sum_{t \in \mathbb{F}_{q^n}} \chi(t)\psi(\mathrm{Tr}_{q,n}(t)). \tag{6.5}$$

6.1.2 Discussion of Results

In this chapter, we prove a series of congruences for $M_{f,q,n}$. The primary result considered in this section is Theorem VI.3 below. This congruence takes a form more often observed for high-dimensional varieties of low degree, and we will provide two proofs using ostensibly different methods, the first of which explicitly develops this connection. In Sections 6.1.3, we will relate the $\mathbb{F}_{q^n}$ roots of the polynomial $\mathrm{Tr}_{q,n} f(x)$ to the $\mathbb{F}_q$-rational points of an affine variety $L_{n,f,q}$ of dimension $n-1$. In Section 6.1.4, we will state the Ax-Katz theorem and discuss its proof. We then obtain Theorem VI.3 by applying the theorem to the aforementioned affine varieties. Note that the results of this section do not require n-smoothness or other additional hypotheses on $f(x)$. We now state the main theorem.

Theorem VI.3. *Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d and let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$. If $n \geq 2$, then the number of $M_{f,q,n}$ of $\mathbb{F}_{q^n}$-rational points on $U_{f,q}$ satisfies the congruence*

$$M_{f,q,n} \equiv 0 \pmod{q^{u+1}}$$

where

$$u = \lceil \frac{n - \sigma_q(f)}{\sigma_q(f)} \rceil.$$

This result can be interpreted as a p-adic refinement to the Weil bound as it implies $|\operatorname{Tr}_{q,n}(F|H^1(X_{f,q}))|_p$ is small for n large. We will give two proofs, a geometric one in Section 6.1.5 and a slightly weaker p-adic analytic one in in Section 6.2.2.

In Section 6.1.6, we will state the Warning Hyperplane Theorem (recently refined by Heath-Brown [14]) and deduce it from the Ax-Katz theorem. This theorem states that the number of $\mathbb{F}_q$-rational points on parallel hyperplane sections of an affine variety are congruent modulo a power of q similar in form to that above. By studying such hyperplane sections on a projective closure of $Y'_{n,f,q}$ we will prove Theorem VI.4.

Theorem VI.4. *Suppose χ_0 is a generator for the character group of μ_d, the d-th roots of unity. If $d|n$, $q \equiv 1 \pmod{d}$, and $f \in \mathbb{F}_p[x]$, then*

$$M_{f,q,n} \equiv (q-1) \sum_{i=1}^{d-1} G_{q^n}(\chi_0^{i\frac{q^n-1}{d}}) \pmod{q^{u+2}}$$

where

$$u = \lceil \frac{n-d}{d} \rceil.$$

In Section 6.2.1, we use a qualititatively different method to prove a congruence for $M_{f,q,n}$ mod p (and not q^u), and explain how this result implies the sharpness of Theorems VI.3 and VI.4 in some cases. Finally, in Section 6.3 we apply the results of Section 6.1.3 to the study of supersingular curves. As we are only interested in studying $\mathbb{F}_q$-rational points, for f of large degree we can replace the polynomials defining $L_{n,f,q}$ by polynomials of lesser degree that give the same functions on $\mathbb{F}_q$. We will study a class of f with $\sigma_q(f) = 2$ and produce a large family of supersingular Artin-Schreier curves; this family contains and strictly extends that of van der Geer and van der Vlugt [30] [31]. We will provide a novel proof that these curves are supersingular by a method which involves studying the n for which $X_{f,q}(\mathbb{F}_{q^n})$ can attain the Weil bound. Note that any results regarding $X_{f,q}$ require the additional hypothesis that $(d, q) = 1$.

6.1.3 Construction of the Auxiliary Variety $L_{n,f,q}$

Note that $\mathrm{Tr}_{q,n} f(x)$ satisfies the hypotheses of the following proposition. Essentially, this proposition asserts that the Weil restrictions of these polynomials can be defined using "too few" polynomials. The Weil restriction of a polynomial in one variable from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined by n polynomials in n variables that together define an algebraic set of dimension zero. However, for $\mathrm{Tr}_{q,n} f(x)$ all of these polynomials agree as functions on $\mathbb{F}_q$, and we will study the variety defined by a polynomial of minimal degree that gives this function.

Proposition VI.5. *If $h(x) \in \mathbb{F}_{q^n}[x]$ maps $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$, then there exists a polynomial $Q_n(\overline{x}) \in \mathbb{F}_q[x_1, ..., x_n]$ of degree at most $\sigma_q(f)$ such that*

$$|\{\bar{t} \in (\mathbb{F}_q)^n : Q_n(\bar{t}) = 0\}| = |\{t \in \mathbb{F}_{q^n} : h(t) = 0\}|.$$

Proof. By the normal basis theorem, there exists an $\mathbb{F}_q$ basis $\{e_1, ..., e_n\}$ for $\mathbb{F}_{q^n}$ such that $e_1^{q^i} = e_{1+i}$ for all $i \in \mathbb{Z}/n\mathbb{Z}$. Given any $h(x) \in \mathbb{F}_{q^n}[x]$ mapping into $\mathbb{F}_q$, we may compute polynomials $h_1, ..., h_n \in \mathbb{F}_q[x_1, ..., x_n]$ such that

$$h(\sum_{i=1}^{n} e_i x_i) = e_1 h_1(\overline{x}) + ... + e_n h_n(\overline{x}).$$

Since $h(x)$ takes values in $\mathbb{F}_q$ we have that $h(x)^{q^i} = h(x)$ as functions on $\mathbb{F}_{q^n}$ for all i. It follows that

$$e_{1-i} h_1(\overline{x})^{q^i} + ... + e_{n-i} h_n(\overline{x})^{q^i} = e_1 h_1(\overline{x}) + ... + e_n h_n(\overline{x}), \text{all } \overline{x} \in (\mathbb{F}_q)^n$$

with subscripts of the e_i considered modulo n. Each h_i has coefficients in $\mathbb{F}_q$, and this implies that that for all pairs i, j

$$h_i(\overline{x}) = h_j(\overline{x}), \text{all } \overline{x} \in (\mathbb{F}_q)^n.$$

This implies the roots of h_1 in $(\mathbb{F}_q)^n$ are precisely the $\mathbb{F}_q$ rational points of the Weil restriction of f (the common vanishing set of all the h_i).

To show we may take the h_i to have degree at most $\sigma_q(f)$, it is sufficient to prove that monomials x^d produce forms of small degree. Suppose that $d = m_0 + m_1 q + ... + m_{n-1}q^{n-1}$. It follows that

$$(e_1 x_1 + ... + e_n x_n)^d = \prod_{i=0}^{n-1} (e_{1+i} x_1^{q^i} + ... + e_{n+i} x_n^{q^i})^{m_i}$$

and as a function on $(\mathbb{F}_q)^n$ this polynomial is equal to

$$\prod_{i=0}^{n-1} (e_{1+i} x_1 + ... + e_{n+i} x_n)^{m_i}$$

which has degree at most $\overline{\sigma}_q(d)$, as desired. □

A noteworthy aspect of the above proposition is the potential for degree reduction; if $d > q$, then d is greater $\sigma_q(f)$ and in some cases $\sigma_q(f)$ is much smaller. This degree reduction phenomenon also occurs more generally; the interested reader should see [23]. Later in this chapter we will study f with $\sigma_q(f) = 2$ and use the theory of quadratic forms to study when an Artin-Schreier curve can be supersingular.

Definition VI.6. The polynomial $\mathrm{Tr}_{q,n} f(x)$ maps $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$, so by Proposition VI.5 there exists $Q_n(\overline{x}) \in \mathbb{F}_q[x_1, ..., x_n]$ such that

$$|\{t \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q,n} f(t) = 0\}| = |\{\overline{t} := (t_1, ..., t_n) \in \mathbb{F}_q^n : Q_n(\overline{t}) = 0\}|.$$

Let $L_{n,f,q}$ denote the affine variety defined over $\mathbb{F}_q$ by $Q_n(\overline{x})$, so by Proposition II.2

$$q|L_{n,f,q}(\mathbb{F}_q)| = M_{f,q,n}.$$

6.1.4 The Ax-Katz Theorem

We now discuss the Ax-Katz theorem. We will also explain how this theorem, together with the results of the previous section, implies Theorem VI.3. For the purposes of Theorem VI.3, the reader should consider the $a = 1$ case with F_1 the polynomial $Q_n(\overline{x})$ constructed in Proposition VI.5.

Theorem VI.7. *(Ax,Katz)*

If $F_1, ..., F_a \in \mathbb{F}_q[x_1, ..., x_n]$ *have respective total degrees* $d_1, ..., d_a$*, then*

$$|\mathbb{V}(F_1, ..., F_a)(\mathbb{F}_q)| \equiv 0 \pmod{q^u}$$

with

$$u = \lceil \frac{n - \sum_{i=1}^{a} d_i}{\max_i d_i} \rceil.$$

In the following remark, we will discuss certain exponential sums that can be used to count solutions of polynomial equations. In particular, we will construct a character of the additive group of $\mathbb{F}_q$ such that any $t \in \mathbb{F}_{q^n}$ maps to a certain polynomial one of its Teichmüller lifts (see Section 1.2 of [18]), and such that the coefficients of this polynomial are Gauss sums. Ax [5] manipulates these exponential sums to obtain an expression for $|\mathbb{V}(F_1)(\mathbb{F}_q)|$ (his original result treats the hypersurface case) in which a product of many Gauss sums appears as a coefficient of each term. Producing a congruence is then a matter of applying Stickelberger's congruence (See Proposition VI.9) to these products. In Section 6.2.2 we will make these constructions explicit for polynomials of the form $\mathrm{Tr}_{q,n} f(x)$ and give a direct p-adic proof of Theorem VI.3.

Our p-adic proof of Theorem VI.3 will make use of the discussion below, but we include it here to emphasize its origins and appearance in the original proof of Ax.

Remark VI.8. Given $f_1, ..., f_a \in \mathbb{F}_{q^n}[x]$, let M denote the number of common roots of the polynomials $\mathrm{Tr}_{q,n} f_i(x)$ for $i = 1, ..., a$. If ψ is a non-trivial character of the additive group of $\mathbb{F}_q$, then for any $u \in \mathbb{F}_{q^n}$ we have

$$\sum_{y \in \mathbb{F}_q} \psi(y \operatorname{Tr}_{q,n} f(u)) \begin{cases} q, & \text{if } \operatorname{Tr}_{q,n} f_i(u) = 0. \\ 0, & \text{otherwise.} \end{cases}$$

We have that

$$q^a M = \sum_{u \in \mathbb{F}_{q^n}} \sum_{y \in \mathbb{F}_q} \prod_{i=1}^{a} \psi\left(y \operatorname{Tr}_{q,n} f_i(u)\right). \tag{6.6}$$

We will now construct such an additive character ψ with properties amenable to estimating M via the equation above. Let K_p be the unique unramified extension of $\mathbb{Q}_p$ with degree Nn and ξ a primitive p-th root of unity. Let T_{q^n} denote the set of Teichmuller lifts $\mathbb{F}_{q^n}$ to K_p (see Proposition VI.9). For any $t \in T_{q^n}$ define $S(t)$ to be the constant coefficient of the power series representation of the trace of t in $\mathbb{Q}_p$. Let $P(x)$ be the unique polynomial in $K_p(\xi)[x]$ of degree $\leq q^n - 1$ such that $P(t) = \xi^{S(t)}$ for all $t \in T_{q^n}$ and let $C(i)$ denote the coefficient of its degree i term. Via Lagrange interpolation and a straightforward computation, the reader may verify that $C(0) = 1$, $C(q-1) = \frac{-q^n}{q^n - 1}$, and

$$C(i) = \frac{\sum_{t \in T_{q^n}^{\times}} t^{-j} \xi^{S(t))}}{q^n - 1}$$

for the remaining $i = 1, ..., q^n - 1$. Note that we now have

$$P(x) = \sum_{i=1}^{q^n - 1} C(i) x^i$$

and if t is the Teichmuller lift of $u \in \mathbb{F}_{q^n}$, then the mapping $\chi : u \mapsto P(t)$ is a character of the additive group of $\mathbb{F}_{q^n}$.

Proposition VI.9. *(Stickelberger) For all $i \in \{1, ..., q^n - 1\}$ the Gauss sums $C(i)$ (defined above) satisfies the congruence*

$$C(i) \equiv 0 \pmod{(\xi - 1)^{\overline{\sigma}_p(i)}}$$

Proof. See Section 1.2 of [18] . □

The remainder of the proof involves presenting Equation 6.6 so that a product of the Gauss sums $C(j)$ appears prominently as a coefficient of each term, and then showing that the sum of the j appearing is large (see Section 6.2.2). We will provide a specialized example in Section 6.2.1. For the remainder of the original argument, see Ax [5] for the original proof in the hypersurface case. Some similar constructions appear implicitly in the more general work of Katz [15], which achieves the same result by studying p-adic Banach spaces.

6.1.5 Proof of the Main Theorem

We may now prove Theorem VI.3

Proof of Theorem VI.3. By Corollary II.2, we have that

$$M_{f,q,n} = q|\{s \in \mathbb{F}_{q^n} : \operatorname{Tr}_{q,n} f(s) = 0\}|$$

and by Proposition VI.5 we have that

$$|\{s \in \mathbb{F}_{q^n} : \operatorname{Tr}_{q,n} f(s) = 0\}| = |\{(s_1, ..., s_n) \in \mathbb{F}_q^n : Q_n(\overline{s}) = 0\}| = |L_{n,f,q}(\mathbb{F}_q)|.$$

By applying Theorem VI.7 to $L_{n,f,q}$, we obtain the desired result. □

6.1.6 The Hyperplane Theorem

In order to study the residue of $M_{f,q,n}$ modulo q^v, we will use the following theorem.

Theorem VI.10. *(Warning, Heath-Brown) Suppose that $F_1, ..., F_a \in \mathbb{F}_q[x_1, ..., x_n]$ have respective degrees $d_1, ..., d_a$ and that $L_1 := \mathbb{V}(\beta_1 + \sum_{i=1}^n \alpha_i x_i)$ and $L_2 := \mathbb{V}(\beta_2 + \sum_{i=1}^n \alpha_i x_i)$ are two parallel hyperplanes in $\mathbb{A}^n(\mathbb{F}_q)$ that are defined over $\mathbb{F}_q$. The number of $\mathbb{F}_q$ rational points on the intersections $L_1 \cap \mathbb{V}(F_1, ..., F_a)$ and $L_2 \cap \mathbb{V}(F_1, ..., F_a)$*

are congruent

$$|L_1 \cap \mathbb{V}(F_1, ..., F_a)(\mathbb{F}_q)| \equiv |L_2 \cap \mathbb{V}(F_1, ..., F_a)(\mathbb{F}_q)| \pmod{q^u}$$

with

$$u = \lceil \frac{n - \sum_{i=0}^{b} d_i}{\max_i\{d_i\}} \rceil.$$

Proof. We include a proof of this result for the reader's convenience. We will first prove that the number of $\mathbb{F}_q$-rational points mod q^u depends only on the top degree d_i homogeneous pieces of the F_i. For each F_i we can define two forms as follows:

- Let $F_i^+(z, x_1, ..., x_n) = z^d F_i(x_1/z, ..., x_n/z)$.
- Let F_i^- denote the degree d homogeneous part of F_i.

By considering $\mathbb{F}_q$-rational points on the affine cone (see Exercise 2.10 of [12]) of $\mathbb{V}(F_1, ..., F_a)$, we see that

$$|\mathbb{V}(F_1^+, ..., F_a^+)(\mathbb{F}_q)| = (q-1)|\mathbb{V}(F_1, ..., F_a)(\mathbb{F}_q)| + |\mathbb{V}(F_1^-, ..., F_a^-)(\mathbb{F}_q)|$$

We have assumed that $d|n$, and as each F_i^+ is a polynomial in $n+1$ variables it follows that $|\mathbb{V}(F_1^+, ..., F_a^+)(\mathbb{F}_q)|$ is congruent to zero modulo q^{u+1}. Applying Ax-Katz on the right hand side as well, we find that

$$|\mathbb{V}(F_1, ..., F_a)(\mathbb{F}_q)| \equiv |\mathbb{V}(F_1^-, ..., F_a^-)(\mathbb{F}_q)| \pmod{q^u}.$$

To complete the proof, note that the intersection of $\mathbb{V}(F_1, ..., F_a)$ with L_1 (or L_2) is the vanishing set of the polynomials $F_i(-\beta_1 - \sum_{i=2}^{n} x_i, x_2, ..., x_n)$, and the top degree homogeneous parts of these polynomials do not depend on β_1 (or β_2). □

Proof of Theorem VI.4. Let $h_i(x_1, ..., x_n)$ be as in Proposition VI.5 for $h(x) = \mathrm{Tr}_{q,n} f(x)$, and let $\gamma(h_i)$ denote the top degree homogeneous piece of h_i. The sum $\sum_{i=1}^{n} \gamma(h_i)$

must be the sum of the n polynomials X_i obtained by applying the arguments of Proposition VI.5 to x^d. It follows that

$$|\mathbb{V}(\sum_{i=1}^{n} h_i)(\mathbb{F}_q)| \equiv |\mathbb{V}(\sum_{i=1}^{n} X_i)(\mathbb{F}_q)|$$

modulo q^{u+1}. However, we also have that

$$q|\mathbb{V}(\sum_{i=1}^{n} X_i)(\mathbb{F}_q)| + 1 = |X_{q,x^d}(\mathbb{F}_q)|$$

By Corollary 2.2 of [16], the $|X_{q,x^d}(\mathbb{F}_q)|$ has an expression in terms of Gauss sums from which the result follows. □

6.2 Alternative Approaches to Non-Archimedean Bounds

6.2.1 A Specialized Result Modulo p

In this section we prove a specialized result regarding the number of roots of $\mathrm{Tr}_{q,n} f(x)$ modulo p. This result informs the sharpness of the results of the previous sections: in the boundary case $n = d$, the residue mod p can be congruent to p or not depending on the divisibility of the multinomial coefficient $\binom{q-1}{\frac{q-1}{n},\ldots,\frac{q-1}{n}}$.

Theorem VI.11. *If $f(x) = \sum_{j=0}^{d} a_j x^j \in \mathbb{F}_p[x]$ is a polynomial of exact degree $d = n$ with $n|(q-1)$, then the number of roots of $\mathrm{Tr}_{q,n} f(x)$ in $\mathbb{F}_{q^n}$ is congruent modulo p to*

$$a_d^{-\frac{1}{d}} \binom{q-1}{\frac{q-1}{n},\ldots,\frac{q-1}{n}}.$$

Proof. Consider the sum

$$\sum_{z\in\mathbb{F}_{q^n}} \left(1 - (\mathrm{Tr}_{q,n}(f(z)))^{q-1}\right). \tag{6.7}$$

If $z \in \mathbb{F}_{q^n}$ then $\mathrm{Tr}_{q,n}(f(z)) \in \mathbb{F}_q$, so $(\mathrm{Tr}_{q,n} f(x))^{q-1} \in \{0,1\}$. The expression $(1 - (\mathrm{Tr}_{q,n}(f(z)))^{q-1})$ is equal to 1 if z is a root of $\mathrm{Tr}_{q,n}(f(x))$ and 0 otherwise, and the above sum gives the number of roots mod p. The sum $\sum_{z\in\mathbb{F}_{q^n}} z^m$ (with

$m > 0$) is equal to $q^n - 1$ if $(q^n - 1)|m$ and zero otherwise. We therefore need only consider those monomials in the expansion $\mathrm{Tr}_{q,n}(f(x))^{q-1}$ with degree divisible by $q^n - 1$, so we consider this expansion in the form

$$\sum_{\gamma \in \Gamma} \binom{q-1}{\{\gamma_{i,j}\}} \prod_{i,j} \left((a_j x^j)^{q^i}\right)^{\gamma_{i,j}}$$

where Γ is the set of functions mapping $i \in \{0, ..., n\}$ and $j \in \{0, ..., d\}$ into $\mathbb{Z}_{\geq 0}$ with $\sum_{i,j} \gamma_{i,j} = q - 1$ and

$$\sum_{i,j} \gamma_{i,j} j q^i = c_\gamma (q^n - 1).$$

Considering this equation modulo each power q^k of q we have

$$\sum_{j=0}^{d} j \gamma_{k,j} = \beta_k q^k - \beta_{k-1}$$

with $\beta_0 = \beta_n = c_\gamma$. Note that the integers β_i must be positive because the left hand side of the above equation is positive and β_0 is assumed to be positive.

The remainder of our argument has three pieces. First, we prove that each $\beta_k = 1$. Second, we prove that $\sum_{i=k} \gamma_{i,j} = \frac{q-1}{n}$ for each k; this requires the hypothesis $d = n$. Once we have proved these facts we can explicitly compute 6.7 modulo p.

By the above, for each β_k we have

$$\sum_{j=0}^{d} \gamma_{k,j} \geq \frac{q\beta_k - \beta_{k-1}}{d}. \tag{6.8}$$

By summing both sides of this equation over all k we obtain

$$q - 1 = \sum_{i=1}^{n} \sum_{j=0}^{d} \gamma_{i,j} \geq \sum_{i=1}^{n} \frac{q\beta_i - \beta_{i-1}}{d} = \frac{q-1}{d} \sum_{i=1}^{n} \beta_i$$

and as the β_i are positive this equation is invalid except when all $\beta_i = 1$.

We now prove that $\sum_{j=1}^{d} \gamma_{k,j} = \frac{q-1}{n} = \frac{q-1}{d}$ for each i_0. If not, it follows that there exists some k such that $\sum_{j=1}^{d} \gamma_{k,j} < \frac{q-1}{d}$ and thus such that

$$\sum_{j=1}^{d} j \gamma_{k,j} \leq d \sum_{j=1}^{d} \gamma_{k,j} < d \frac{q-1}{d} = q - 1$$

which cannot be the case. It also follows that $\gamma_d^i = \frac{q-1}{d}$ for all i and $\gamma_j^i = 0$ for all i and $j \neq d$. We now explicitly compute

$$\sum_{z\in\mathbb{F}_{q^n}} \mathrm{Tr}_{q,n}(f(z))^{q-1} = \sum_{z\in\mathbb{F}_{q^n}} \sum_{\overline{\gamma}} \prod_{\gamma_j^i} \left((a_j z^j)^{q^i}\right)^{\gamma_i^j}$$

which by the above is equal to

$$\sum_{z\in\mathbb{F}_{q^n}} \prod_{i=0}^{n-1} \left((a_d z^d)^{q^i}\right)^{\frac{q-1}{d}}$$

and then to

$$\sum_{z\in\mathbb{F}_{q^n}} a_d^{\frac{q^n-1}{d}} z^{q^n-1}.$$

Equation 6.7 is therefore equal to

$$a_d^{-\frac{1}{d}}$$

modulo p as desired. □

6.2.2 A p-adic Analytic Proof of Theorem I.11

We now provide the promised, direct, p-adic analytic proof of Theorem VI.3. We will in fact prove a specialized analog of the Ax-Katz theorem which applies to polynomials of one variable. A slightly weaker version of Theorem VI.3 can be deduced from this result in the same way as in Section 6.1.5.

Proposition VI.12. *Given $f_1, ..., f_a \in \mathbb{F}_{q^n}[x]$ of degrees $d_1, ..., d_a$ with $f_i(x) = \sum_{j=1}^{d_i} a_{i,j}x^j$, let M denote the number of common roots of the polynomials $\mathrm{Tr}_{q,n} f_i(x)$. M satisfies the congruence*

$$M \equiv 0 \pmod{p^u}$$

with

$$u = N\lceil \frac{n - a \cdot \max_i\{d_i\}}{\max_i\{d_i\}} \rceil.$$

Proof. Recall that in Remark VI.8, we defined a polynomial P, with Gauss sums as its coefficients, such that for any $t \in \mathbb{F}_q$ with Teichmuller lift T (see Section 1.2 of [18]) the map $t \mapsto P(t)$ is a character of $\mathbb{F}_q$. Suppose ψ is the character associated with P, and recall that

$$q^a M_{f,q,n} = \sum_{x \in \mathbb{F}_{q^n}} \sum_{y \in \mathbb{F}_q} \prod_{i=1}^{a} \psi\left(y \operatorname{Tr}_{q,n}(f_i(x))\right)$$

ψ is a homomorphism from the additive group of F_{q^n} to the multiplicative group of $K_p(\xi)$, so the application of ψ to a sum is equal to the product of the application of ψ to each of its terms. Equation 6.6 is therefore equal to

$$\sum_{x \in \mathbb{F}_{q^n}} \sum_{y \in \mathbb{F}_q} \prod_{i=1}^{a} \prod_{k=0}^{n-1} \psi\left(y f_i^{q^k}(x)\right).$$

We may write $\psi(y f_i^{q^k}(x))$ as a product of ψ evaluated at each term of $y f_i^{q^k}(x)$. The above expression is then equal to

$$\sum_{x \in \mathbb{F}_{q^n}} \sum_{y \in \mathbb{F}_q} \prod_{i=1}^{a} \prod_{k=0}^{n-1} \prod_{j=0}^{d_i} \psi\left(y a_{i,j}^{q^k} x^{jq^k}\right).$$

We are now applying ψ to a product and we may compute it using the polynomial P. The above is equal to

$$= \sum_{X \in T_{q^n}} \sum_{Y \in T_q} \prod_{i=1}^{a} \prod_{j=0}^{d_i} \prod_{k=0}^{n-1} P\left(Y A_{i,j}^{q^k} X^{jq^k}\right)$$

where $A_{i,j}$ denotes a Teichmuller lift of $a_{i,j}$. Any term in the product above corresponds to the choice of a term of P for each i, j, and k. If we let W be the set of functions from the set of indices (i, j, k) to the set of degrees $\{0, ..., q^n - 1\}$, then we can express the above

$$= \sum_{X \in T_{q^e}} \sum_{Y \in T_q} \sum_{w \in W} \prod_{i=1}^{a} \prod_{j=0}^{d_i} \prod_{k=0}^{n-1} C(w(i,j,k)) Y^{w(i,j,k)} A_{i,j}^{q^k w(i,j,k)} X^{jq^k w(i,j,k)}$$

$$= \sum_{w \in W} \left(\prod_{i=1}^{a} \prod_{j=0}^{d_i} \prod_{k=0}^{n-1} A_{i,j}^{q^k w(i,j,k)} \right) \left(\prod_{i=1}^{a} \prod_{j=0}^{d_i} \prod_{k=0}^{n-1} C(w(i,j,k)) \right) \left(\sum_{X \in T_{q^n}} \sum_{Y \in T_q} Y^{u(w)} X^{v(w)} \right)$$

where $u(w)$ and $v(w)$ are defined by

$$u(w) := \sum_{i,j,k} w(i,j,k)$$

$$v(w) := \sum_{i,j,k} j q^k w(i,j,k)$$

Note that $\sum_{X \in T_{q^e}} \sum_{Y \in T_q} Y^{u(w)} X^{v(w)}$ is nonzero if and only if $u(w)$ is a multiple of $q-1$ and $v(w)$ is a multiple of $q^n - 1$. We have that $u(w) = 0$ if and only if $v(w) = 0$, and in this case the sum is divisible by q^{n+1}, so we need only consider positive multiples. Suppose that for some $w \in W$ we have that $v(w) = z(q^n - 1)$. We will show that the term corresponding to w is divisible by the desired power of p.

The arguments above are due in their broad strokes to Ax. The remainder of the proof requires understanding which sums $u(w)$ and $v(w)$ actually appear. The arguments of Ax, intended for sums arising from polynomials in several variables, do not apply here and we provide a specialized argument below for polynomials of the form $\mathrm{Tr}_{q,n} f(x)$.

We will now prove that

$$\overline{\sigma}(z(q^e - 1)) \geq Nn(p-1).$$

Express z in base q^n with the form $z = z_0 + z_1 q^n + ... + z_l q^{nl}$. We then have that

$$z(q^n - 1) = -z_0 + (z_0 - z_1)q^n + ... + (z_{l-1} - z_l)q^{nl} + z_l q^{n(l+1)}.$$

To compute the above sum in base p, we may compute each $z_{i-1} - z_i$ digit by digit (allowing negative values), multiply by q^{in} so that for each k no two terms of the sum have nonzero p^k digit, compute the sum, and perform any necessary carries at the end. Carries will only be required to perform subtraction, and any such carry increases the sum of the digits by $p-1$, so it is sufficient to bound below both the sum of the digits before carrying and the number of carries required. As the q^{in} term has nonzero digits only in the p^{iNn} through $p^{(i+1)Nn-1}$ places, it follows that the sum of the digits before carrying is zero and that Nn carries are required for each i such that $z_{i-1} - z_i < 0$ (with $z_{-1} = z_{l+1} = 0$). There must be at least one such i, and the desired result follows.

The prime p divides $(\xi - 1)^{p-1}$, so via Stickelberger's congruence (see Proposition VI.9) we may show that a large power of p divides each $\prod_{i=1}^{a} \prod_{j=0}^{d_i} \prod_{k=0}^{n-1} C(w(i,j,k))$ if we are able to prove that $\sum_{i=1}^{a} \sum_{j=0}^{d_i} \sum_{k=0}^{n-1} \overline{\sigma}_p(C(i,j,k))$ is greater than a large multiple of $p-1$. Using our claim above, we have that

$$\overline{\sigma}_p \left(\sum_{i,j,k} j q^k w(i,j,k) \right) \geq Nn(p-1) \tag{6.9}$$

For any positive integers i and j, it is immediate that $\overline{\sigma}_p(i+j) = \overline{\sigma}_p(i) + \overline{\sigma}_p(j)$ and $\overline{\sigma}_p(ij) = \overline{\sigma}_p(i)\overline{\sigma}_p(j)$ if these operations can be performed in base p without need of carries. Any carry only decreases the sum of the digits, so we have that

$$\overline{\sigma}_p(ij) \leq \overline{\sigma}_p(i)\overline{\sigma}_p(j)$$

and that

$$\overline{\sigma}_p(i+j) \leq \overline{\sigma}_p(i) + \overline{\sigma}_p(j).$$

It is also immediate that $\overline{\sigma}_p(p^i j) = \overline{\sigma}_p(j)$. Applying these facts to 6.9, we obtain that

$$\sum_{i,j,k} \overline{\sigma}_p(j)\overline{\sigma}_p(m(i,j,k)) \geq Nn(p-1).$$

For any j appearing above we have that $\overline{\sigma}_p(j) \leq \max_i d_i$ and thus

$$\sum_{i,j,k} \overline{\sigma}_p(m(i,j,k)) \geq \frac{Nn(p-1)}{\delta}.$$

It follows that $M_{f,q,n}$ is divisible by p at a power at least

$$\frac{Nn}{\max_i d_i} - Na = N\frac{n - a \cdot \max_i\{d_i\}}{\max_i\{d_i\}}$$

as desired. □

6.3 Supersingular Artin-Schreier Curves with $\sigma_q(f) = 2$

In this section, we will be interested in a class of polynomials with $\sigma_q(f) = 2$ and show that the curves corresponding to such f are supersingular. In the introduction, we discussed how a curve is supersingular if and only if it attains the Weil bound (in which the set of n such that $M_{f,q,n}$ attains the Weil bound forms an arithmetic progression). Here we will use the theory of quadratic forms show that this happens in the $\sigma_q(f) = 2$ case.

Theorem VI.13. *Let $f(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial of degree d with $(d, q) = 1$, let $U_{f,q}$ denote the affine curve defined over $\mathbb{F}_q$ by the equation $y^q - y = f(x)$, and let $X_{f,q}$ denote the smooth, complete model of $U_{f,q}$. Suppose $p \neq 2$ and $n \geq 2$. If $f(x) \in \mathbb{F}_q[x]$ has degree 2 or each of its non-constant terms has degree $p^i + 1$ for some i, then $X_{f,q}$ is supersingular.*

To prove this we will require a standard result regarding quadratic forms in odd characteristic.

Theorem VI.14. *Suppose $p \neq 2$ and $G(x_1, ..., x_n)$ is a quadratic form with rank $n - u$. Let $\Delta := \det G$ denote the determinant of G when restricted to a maximal subspace on which it is non-degenerate, η the quadratic character of $\mathbb{F}_q$, and v the* *function on $\mathbb{F}_q$ defined so that $v(0) = q-1$ and $v(b) = -1$ for any other $b \in \mathbb{F}_q$. The number of solutions to the equation $G(x_1, ..., x_n) = b$ in $(\mathbb{F}_q)^n$ is*

$$\begin{cases} q^{n-1} + v(b)q^u q^{(n-u-2)/2}\eta((-1)^{(n-u)/2}\Delta) & \textit{if } n \textit{ even} \\ q^{n-1} + q^u q^{(n-u-1)/2}\eta((-1)^{(n-u-1)/2}b\Delta) & \textit{if } n \textit{ odd} \end{cases}$$

Proof. See Lidl and Niederreiter [19], Section 6.2. □

Proof of Theorem VI.13. When f has degree 2, we may complete the square to may find a t_0 in $\mathbb{F}_q$ such that

$$|\{s \in \mathbb{F}_{q^n} : \operatorname{Tr}_{q,n} f(s) = 0\}| = |\{s \in \mathbb{F}_{q^n} : \operatorname{Tr}_{q,n}(s^2 + t_0) = 0\}|.$$

Thus, in the degree 2 case we may assume without loss of generality that it has the form $f(x) = x^2 + t_0$. We will use the fact that a curve is supersingular if and only if there exist infinitely many positive integers m such that every zero α_i of the zeta function $Z(X_{f,q}, T)$ satisfies $\alpha_i^m \in \mathbb{R}$. This is in turn equivalent to the requirement that

$$q^{-m/2}\operatorname{Tr}(F^m | H^1(X_{f,q})) = (d-1)(q-1)$$

Let $G \in \mathbb{F}_q[x_1, ..., x_n]$ be the polynomial obtained from $\operatorname{Tr}_{q,n} f(x)$ by applicationg of Proposition VI.5. As all terms of f have degree $p^i + 1$ for some i, G is homogeneous with degree 2. The rank of these quadratic forms varies with n, so in the following we will consider $u := u(\_)$ as a function taking positive integer arguments. If G has constant term t_0, we can apply Theorem VI.14 (we will also retain its notation) to the quadratic form $G - t_0$ (assumed to have rank $n - u(m)$) and show that

$$q^{-m/2}\operatorname{Tr}(F^m | H^1(X_{f,q})) = v(b)q^{-u/2}\eta((-1)^{(m-u(m))/2}\Delta)$$

for m even and

$$q^{-m/2}\operatorname{Tr}(F^m | H^1(X_{f,q})) = \sqrt{q}q^{-u/2}\eta((-1)^{(m-u(m)-1)/2}b\Delta)$$

for m odd. Note that if $\sigma_q(f) = 2$ then the degree of $f(x)$ must have the form $p^j + 1$ for some j. Thus, the above formula for m odd is never equal to $(d-1)(q-1)$, while the formula for m even is equal to $(d-1)(q-1)$ if and only if $u(m) = j$. If m is odd, or if m is even and $u(m) \neq j$, then we have the inequality

$$|q^{-m/2} \operatorname{Tr}(F^m | H^1(X_{f,q}))| \leq (p^{j-1} + 1)(q - 1).$$

By Dirichlet's approximation theorem, for any $\epsilon > 0$ there must exist m_0 such that

$$(d-1)(q-1) - q^{-m_0/2} \operatorname{Tr}(F^{m_0} | H^1(X_{f,q})) < \epsilon$$

and thus there exists an even m_1 such that $u(m_1) = p^j + 1$, as desired. □

CHAPTER VII

Table of Notation

Table 7.1: Table of Notation

p	:=	a prime number, sometimes assumed $\neq 2$
q	:=	p^N a power of p
$f(x)$	:=	an element of $\mathbb{F}_q[x]$
d	:=	the degree of $f(x)$
$\mathbb{V}(F_0)$	:=	the algebraic set defined by a polynomial F_0 (see pages 2 and 9 of [12])
$U_{f,q}$	:=	the affine curve over $\mathbb{F}_q$ defined by the equation $y^q - y = f(x)$ (Section 2.1.1)
$X_{f,q}$	:=	the smooth complete model of $U_{f,q}$ (only discussed when $(d,q) = 1$) (Section 2.2.1)
π_i	:=	the eigenvalues of Frobenius on $H^1(X_{f,q})$
$\mathrm{Tr}_{q,n}(x)$	:=	$\sum_{i=0}^{n-1} x^{q^i}$ (Section 2.1.1)
$M_{f,q,n}$	:=	the number $\lvert X_{f,q}(\mathbb{F}_{q^n})\rvert$ of $\mathbb{F}_{q^n}$-points on $X_{f,q}$.
$Z(X_{f,q},T)$	:=	$\sum_{n=1}^{\infty} M_{f,q,n}\frac{T^n}{n}$ the zeta function of $X_{f,q}$
ν	:=	an embedding $\overline{\mathbb{Q}_p} \to \mathbb{C}$ fixed in Section 3.2.1
μ_d	:=	the group of d-th roots of unity $\cong \mathbb{Z}/d\mathbb{Z}$ (Section 3.3.1)
ψ	:=	a non-trivial character of $\widehat{\mathbb{F}_q^+}$
χ	:=	a non-trivial character of μ_d
$S(\psi,n)$	:=	$\sum_{x\in(\mathbb{F}_q)^n} \psi(\mathrm{Tr}_{q,n} f(x))$ (Section 2.1.1)
$G_{q^n}(\psi,\chi)$	:=	$-\sum_{t\in\mathbb{F}_{q^n}} \chi(t)\psi(\mathrm{Tr}_{q,n}(t))$ (Section 6.1.1)
$Y_{n,f,q}$	:=	the affine variety defined by the polynomial $\sum_{i=1}^{n} f(x_i)$ (Section 3.1.1)
$Y'_{n,f,q}$	:=	the projective closure of $Y_{n,f,q}$(Section 3.1.1)
α_i	:=	the eigenvalues of Frobenius on $H^{n-1}(Y'_{n,f,q})$(Section 4.1.5)
$Z_{n,d,q}$	:=	the Fermat variety defined by the equation $\sum_{i=1}^{n} x_i^d$ (Section 3.1.1)
S_n	:=	the group of permutations of the set $\{1,...,n\}$ (Section 3.1.1)
ϕ	:=	the automorphism of $Y_{n,f,q}$ (or of $Z_{n,d,q}$) given by cyclic permutation of coordinates $x_i \mapsto x_{i+1}$ (Section 3.1.1)
$l_i(g)$	:=	length of the i-th cycle in a decomposition of $g \in S_n$ (Section 3.1.1)
$l(g)$	:=	number of cycles in a decomposition of $g \in S_n$ (Section 3.1.1)
$\mathscr{A}_n^d$	:=	a subset of μ_d^{n-1} defined in Section 3.3.2
$\mathscr{P}_{n,k}$	:=	the set of partitions of n with k parts (Section 3.3.4)
$i_{(j)}$	:=	the Pochhammer symbol $i_{(j)} := \binom{i}{j}j!$ (Section 3.3.4)
W_n	:=	the standard representation of S_n (an $(n-1)$-dimensional irreducible representation) (Section 3.3.4)
$r_i(n,d)$	:=	multiplicity of $\bigwedge^i W_n$ in $H^{n-1}(Y'_{n,f,q})$(Section 4.1.5)
$r(n,d)$	:=	$\sum_{i=1}^{n-1} W_n$ (sometimes written $r_i(n,d)$) (Section 4.1.5)
$W(\psi,T)$	:=	$\exp(\sum_{n\geq 1} S(\psi,n)\frac{T^n}{n})$ (Section 5.1.1)
$R(g,\psi,m,n)$	:=	$qq^{-m}\sum_{x\in\mathbb{F}_{q^m}} \psi(x)\mathrm{Fix}(g\circ F^m \mid Y'_{n,f+x/n,q})$ (Section 5.1.1)
$Z(g,\psi,n,T)$	:=	$\exp\big(\sum_{m\geq 1} R(g,\psi,m,n)\frac{T^m}{m}\big)$ (Section 5.1.1)
Alt	:=	the character of the alternating representation of S_n (Section 5.1.4)
$\sigma_q(f_i)$	:=	degree of a certain auxiliary variety defined in Definition VI.1
$\sigma_q(m)$	:=	sum of the base-p digits of m (Section 6.1.1)
$L_{n,f,q}$	:=	an affine auxiliary variety of dimension $n-1$ (Section 6.1.3)
ξ	:=	a primitive p-th root of unity (Section 6.2.2)

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] *Cohomologie l-adique et fonctions L.* Lecture Notes in Mathematics, Vol. 589. Springer-Verlag, Berlin, 1977. Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie.

[2] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I. *Math. Z.*, 19(1):153–206, 1924.

[3] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. II. *Math. Z.*, 19(1):207–246, 1924.

[4] E. Artin. Quadratische Körper über Polynombereichen Galois'scher Felder und ihre Zetafunktionen. *Abh. Math. Sem. Univ. Hamburg*, 70:3–30, 2000.

[5] James Ax. Zeroes of polynomials over finite fields. *Amer. J. Math.*, 86:255–261, 1964.

[6] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[7] P. Deligne. *Cohomologie étale.* Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA 41*øer*2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

[8] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[9] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

[10] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[11] Fernando Q. Gouvêa and Noriko Yui. *Arithmetic of diagonal hypersurfaces over finite fields*, volume 209 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1995.

[12] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[13] H. Hasse. Proof of the riemann hypothesis for elliptic function fields. *J. Reine Angew. Math.*, 175:193–208, 1936.

[14] D. R. Heath-Brown. A note on the Chevalley-Warning theorems. *Russian Math. Surveys*, 66(2(427)):427–435, 2011.

[15] Nicholas M. Katz. On a theorem of Ax. *Amer. J. Math.*, 93:485–499, 1971.

[16] Nicholas M. Katz. Crystalline cohomology, Dieudonné modules, and Jacobi sums. In *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, volume 10 of *Tata Inst. Fund. Res. Studies in Math.*, pages 165–246. Tata Inst. Fundamental Res., Bombay, 1981.

[17] Gilles Lachaud. Artin-Schreier curves, exponential sums, and coding theory. *Theoret. Comput. Sci.*, 94(2):295–310, 1992. Discrete mathematics and applications to computer science (Marseille, 1989).

[18] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.

[19] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[20] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[21] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[22] James S. Milne. Lectures on etale cohomology (v2.21), 2013. Available at www.jmilne.org/math/.

[23] Oscar Moreno, Kenneth W. Shum, Francis N. Castro, and P. Vijay Kumar. Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications. *Proc. London Math. Soc. (3)*, 88(3):545–564, 2004.

[24] Antonio Rojas-León. On the number of rational points on curves over finite fields with many automorphisms. *Finite Fields Appl.*, 19:1–15, 2013.

[25] Antonio Rojas-León and Daqing Wan. Improvements of the Weil bound for Artin-Schreier curves. *Math. Ann.*, 351(2):417–442, 2011.

[26] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[27] Bruce E. Sagan. *The symmetric group*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001. Representations, combinatorial algorithms, and symmetric functions.

[28] F.K. Schmidt. Zur zahlentheorie in körpern der charakteristik *p*. *Sitz.-Ber. phys. med. Soz. Erlangen*, 58/59:159–172, 1926/1927.

[29] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[30] Gerard van der Geer and Marcel van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Math.*, 84(3):333–367, 1992.

[31] Gerard van der Geer and Marcel van der Vlugt. Fibre products of Artin-Schreier curves and generalized Hamming weights of codes. *J. Combin. Theory Ser. A*, 70(2):337–348, 1995.

[32] A. Weil. *Sur les courbes algébriques et les variétés qui s'en deduisent.* Actualités scientifiques et industrielles, Vol. 1048. Hermann & Cie, Paris, 1948.

[33] André Weil. *Variétés abéliennes et courbes algébriques.* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[34] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[35] J. Wolfmann. The number of points on certain algebraic curves over finite fields. *Comm. Algebra*, 17(8):2055–2060, 1989.

[36] J. Wolfmann. Algebraic curves and varieties over finite fields and irreducible cyclic codes. In *Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991)*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, pages 217–225. Dekker, New York, 1993.

[37] Jacques Wolfmann. The number of solutions of certain diagonal equations over finite fields. *J. Number Theory*, 42(3):247–257, 1992.

[38] F. L. Zak. Castelnuovo bounds for higher-dimensional varieties. *Compos. Math.*, 148(4):1085–1132, 2012.