Distribution of the Number of Points on Abelian Curves over Finite Fields

Patrick Meisner

A Thesis

In The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy (Mathematics) at

Concordia University

Montreal, Quebec, Canada

June 2016

© Patrick Meisner, 2016

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: Patrick Meisner

Entitled: Distribution of the Number of Points on Abelian Curves over Finite Fields

and submitted in partial fulfillment of the requirements for the degree of

Ph.D (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Pablo Bianucci — Chair

Yu-Ru Liu — External Examiner

Mariana Frank — External to Program

Hershy Kisilevski — Examiner

Lea Popovic — Examiner

Chantal David — Thesis Supervisor

Approved by

Chair of Department or Graduate Program Director

Dean of Faculty

ABSTRACT

Distribution of the Number of Points on Abelian Curves over Finite Fields

Patrick Meisner, Ph.D.

Concordia University, 2016

Classical results due to Katz and Sarnak [8] show that if the genus is fixed and $q \to \infty$, then the number of points on a family of curves over $\mathbb{F}_q$ is distributed as the trace of a random matrix in the monodromy group associated to the family.

Every smooth projective curve C corresponds to a finite Galois extension of $\mathbb{F}_q[X]$. Therefore, some natural families to consider are the curves that correspond to a extensions with a fixed Galois group. This thesis involves determining the distribution of the families with fixed abelian Galois group, G, when q is fixed and the genus tends to infinity.

Several authors determined that the distribution for the family of prime-cyclic curves ($G = \mathbb{Z}/p\mathbb{Z}$, p a prime) [2],[3],[9] as well as for the family of biquadratic curves ($G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) [10] is that of a sum of $q+1$ random variables. This thesis shows that if we fix *any* abelian group, the distribution will be that of $q+1$ random variables.

The above results deal only with the distribution for the coarse irreducible moduli space of the families. It has been shown in [1] that if you look at the whole (coarse) moduli space, the distribution is the same in the case of prime-cyclic curves. We are able to show that the distribution is the same for the coarse moduli space of curves with $G = (\mathbb{Z}/Q\mathbb{Z})^n$, Q a prime. Some work is done towards proving this true for all abelian groups.

Acknowledgements

I would like to thank my advisor, Chantal David. Her knowledge and guidance have been invaluable to the completion of this thesis.

I would also like to thank my fellow graduate students for all the fun these past four years. Without whom I may have completed this thesis a year earlier at the cost of my sanity.

Finally, I would like to thank my family for their constant support and belief in me.

Contents

Chapter 0

Notation List

- q, a power of a prime
- $\mathbb{F}_q$, the finite field with q elements
- $\mathbb{P}^1(\mathbb{F}_q)$, the projective line of $\mathbb{F}_q$
- $x_1, \ldots, x_q$, a fixed ordering of the elements of $\mathbb{F}_q$
- x_{q+1}, the point at infinity on $\mathbb{P}^1(\mathbb{F}_q)$
- $K = \mathbb{F}_q(X)$, the field of rational polynomials with coefficients in $\mathbb{F}_q$
- C, a smooth, projective curve over $\mathbb{F}_q$
- $K(C)$, the function field of C
- $\mathrm{Gal}(C)$, the Galois group of $K(C)/K$
- $g(C)$, the genus of C
- $G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$, an arbitrary abelian group written in the unique form where $r_j | r_{j+1}$
- $\exp(G) = r_n$, the exponent of G
- Q, the smallest prime divisor of $|G|$

- $\phi_G(s)$, the number of elements of G of order s for all $s|r_n$
- $\mathcal{R} = [0, \ldots, r_1 - 1] \times \cdots \times [0, \ldots, r_n - 1] \setminus \{(0, \ldots, 0)\}$, a set of vectors with non-negative integer coordinates
- $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$, an element of $\mathcal{R}$
- $\mathcal{R}' = \mathcal{R} \cup \{(0, \ldots, 0)\}$
- $e(\vec{\alpha}) = \underset{j=1,\ldots,n}{\operatorname{lcm}} \left(\frac{r_j}{(r_j, \alpha_j)} \right)$ for all $\vec{\alpha} \in \mathcal{R}'$
- $c(\vec{\alpha}) = |G| - \frac{|G|}{e(\vec{\alpha})}$ for all $\vec{\alpha} \in \mathcal{R}$
- F, a polynomial in K (usually assumed to be r^{th}-power free for some r)
- f, a monic, squarefree polynomial in K
- $(f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}}$, a set of monic, squarefree, pairwise coprime polynomials in K indexed by the vectors in $\mathcal{R}$ (usually denoted just by $(f_{\vec{\alpha}})$)
- $F^{(**)}_{(*)}$, a polynomial in K that can be written as a product of $(f_{\vec{\alpha}})$ in a way controlled by $(*)$ and $(**)$
- $\vec{d}(\vec{\alpha}) = (d(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}}$, a non-negative integer valued vector indexed by the vectors in $\mathcal{R}$
- $\mathcal{F}_{\vec{d}(\vec{\alpha})}$, the set of $(f_{\vec{\alpha}})$ such that $\deg(f_{\vec{\alpha}}) = d(\vec{\alpha})$
- $\mathcal{H}_{G,g}$, the coarse moduli space of curves with $\mathrm{Gal}(C) = G$ and $g(C) = g$
- $\mathcal{H}_{r,g}$, the coarse moduli space of curves with $\mathrm{Gal}(C) = \mathbb{Z}/r\mathbb{Z}$ and $g(C) = g$
- $\mathcal{H}^{(\vec{d}(\vec{\alpha}))}$, an irreducible coarse moduli space of $\mathcal{H}_{G,g}$

Chapter 1

Introduction

Let $\mathcal{H}$ be a family of smooth, projective curves over $\mathbb{F}_q$, the finite field with q elements. We are interested in determining the probability that a curve, chosen randomly from our family, has a given number of points. Classical results due to Katz and Sarnak [8] tell us what happens if we fix the genus of the curve, g and let $q \to \infty$. Less is know about what happens when q is fixed and $g \to \infty$. However, we are able to answer this question for some families.

Let $K = \mathbb{F}_q(X)$ and $K(C)$ be the field of functions of C. Then we know that $K(C)$ will be a finite field extension of K. Moreover, every such finite extension corresponds to a smooth, projective curve (Corollary 6.6 and Theorem 6.9 from Chapter I of [7]). If $K(C)$ is a Galois extension of K, denote $\mathrm{Gal}(C) := \mathrm{Gal}(K(C)/K)$ and $g(C)$ to be the genus of C. If we fix an abelian group, G, then for $q \equiv 1 \pmod{\exp(G)}$ we determine

$$\mathrm{Prob}(C : \mathrm{Gal}(C) = G, g(C) = g, \#C(\mathbb{P}^1(\mathbb{F}_q)) = M)$$

as $g \to \infty$.

1.1 Classical Results

The zeta function for C is defined as

$$Z_C(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m\right) \tag{1.1.1}$$

where $N_m = \#C(\mathbb{F}_{q^m})$, the number of $\mathbb{F}_{q^m}$ points on C. If we embed C into $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ and define the q^m-Frobenius automorphism on C by

$$\mathrm{Frob}_{q^m}[x_0 : x_1 : \cdots : x_n] = [x_0^{q^m} : x_1^{q^m} : \cdots : x_n^{q^m}]$$

then $N_m = |\ker(\mathrm{Frob}_{q^m} - 1)|$. Moreover, it is a well known result (Theorem 5.9 from [12]) that

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} \tag{1.1.2}$$

such that $P_C(u)$ is a degree $2g$ polynomial with coefficients in $\mathbb{Z}$ where g is the genus of the curve. Further, $u^{2g}P_C(1/u)$ is the characteristic polynomial for Frob_q ([13]).

If we write $P_C(u) = \prod_{j=1}^{2g}(1 - u\alpha_j(C))$ then, by equating the coefficients of u on the left hand side and right hand side of (1.1.2), we get the equation

$$N_m = q + 1 - \sum_{j=1}^{2g} \alpha_j^m(C).$$

Therefore, setting $m = 1$, we get

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 - \sum_{j=1}^{2g} \alpha_j(C) = q + 1 - \mathrm{Tr}(\mathrm{Frob}_q(C)).$$

The Riemann hypothesis for function fields says that $|\alpha_j(C)| = \sqrt{q}$ for $j = 1, \ldots, 2g$.

If we fix a family of curves C over $\mathbb{F}_q$, we want to determine what the distribution over the number of points on this family is. It is enough then to determine the distribution of the normalized trace function of the Frobenius

$$\frac{\mathrm{Tr}(\mathrm{Frob}_q(C))}{\sqrt{q}} = \frac{\sum_{j=1}^{2g} \alpha_j(C)}{\sqrt{q}}. \tag{1.1.3}$$

Katz and Sarnak [8] showed that if $q \to \infty$, then (1.1.3) is distributed as the trace of a random matrix in the monodromy group of the family.

1.2 Cyclic Curves

The distribution of the number points on families of curves over finite fields with q fixed while the genus tends to infinity has been a topic of much research recently. It began with Kurlberg

and Rudnick [9] determining the distribution of the number of points on hyperelliptic curves. Hyperelliptic curves are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/2\mathbb{Z}$. Bucur, David, Feigon and Lalin [2],[3] extended this result to smooth projective curves that are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/p\mathbb{Z}$, where p is a prime such that $q \equiv 1 \pmod{p}$. In Chapter 3 we extend this to all cyclic curves.

Define

$$\mathcal{H}_{r,g} = \{C : \mathrm{Gal}(C) = \mathbb{Z}/r\mathbb{Z}, g(C) = g\} \tag{1.2.1}$$

be the family of curves such that $\mathrm{Gal}(C) = \mathbb{Z}/r\mathbb{Z}$ and $g(C) = g$.

Remark 1.2.1. When talking about curves in $\mathcal{H}_{r,g}$, we will always be assuming $q \equiv 1 \pmod{r}$.

If $C \in \mathcal{H}_{r,g}$ then it will have an affine model of the form

$$Y^r = F(X) \qquad F(X) \in \mathbb{F}_q[X]/(\mathbb{F}_q[X])^r.$$

Since $F(X) \in \mathbb{F}_q[X]/(\mathbb{F}_q[X])^r$, we can find $f_1, \ldots, f_{r-1} \in \mathbb{F}_q[X]$ and $c \in \mathbb{F}_q^*$ where the f_i are squarefree and $(f_i, f_j) = 1$ for $i \neq j$ such that

$$F(X) = cf_1 f_2^2 \cdots f_{r-1}^{r-1}.$$

If $\deg(f_j) = d_j$ and $\deg(F) = d = \sum_{j=1}^{r-1} jd_j$ then the Riemann-Hurwitz formula (Theorem 7.16 of [12]) tells us the genus g of the curve C is given by

$$2g + 2r - 2 = \sum_{j=1}^{r-1} (r - (r, j))d_j + (r - (r, d)) \tag{1.2.2}$$

where $(r, j) = \gcd(r, j)$.

Now, define $\mathcal{H}^{(d_1,\ldots,d_{r-1})} \subset \mathcal{H}_{r,g}$ to be the family of curves such that the corresponding polynomials f_j have degrees d_j or $d_j - 1$, where at most one of the f_j can have degree $d_j - 1$. Then

$$\mathcal{H}_{r,g} = \bigcup_{\substack{\sum_{j=1}^{r-1}(r-(r,j))d_j = 2g+2r-2 \\ \sum_{j=1}^{r-1} jd_j \equiv 0 \pmod{r}}} \mathcal{H}^{(d_1,\ldots,d_{r-1})}. \tag{1.2.3}$$

Note that under the condition that $\sum_{j=1}^{r-1} jd_j \equiv 0 \pmod{r}$, the set $\mathcal{H}^{(d_1,\ldots,d_{r-1})}$ is genus-invariant. We will perform statistics on the components $\mathcal{H}^{(d_1,\ldots,d_{r-1})}$ instead of the whole $\mathcal{H}_{r,g}$.

For $s|r$, define

$$F_{(s)}(X) := c\prod_{i=1}^{s-1}\left(\prod_{j=0}^{\frac{r}{s}-1} f_{js+i}(X)\right)^i = c\prod_{i=1}^{r-1} f_i(X)^{i \pmod{s}}.$$

Remark 1.2.2. When we write $i \pmod{s}$, we mean the smallest non-negative integer that is congruent to i modulo s. Moreover, we use the convention that $f_i(X)^0$ is identically the constant polynomial 1. Therefore, $F_{(1)}(X)$ is identically the constant polynomial c.

Notice that we could write an affine model for our curve as $Y^r = F_{(r)}(X)$. Further, the $F_{(s)}(X)$ correspond to the subfield extension of $K(C)$. That is, if we have $K \subset L \subset K(C)$, then $L = K(C_s)$, where C_s is a curve with affine model $Y^s = F_{(s)}(X)$ for some $s|r$. Then Lemma 3.3.2 shows that

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 + \sum_{s|r}\sum_{\substack{i=1\\(i,s)=1}}^{s-1}\sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_s^i(F_{(s)}(x)) \tag{1.2.4}$$

where χ_s is a primitive character on $\mathbb{F}_q$ of order s. Such a character exists since $s|r$ and we are assuming that $q \equiv 1 \pmod{r}$. Hence if we define

$$S_s(F_{(s)}) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_s(F_{(s)}(x))$$

then the number of points on the curve will be determined by the $S_s(F_{(s)})$ for all $s|r$. Note that since $F_{(1)}(X)$ is a non-zero constant polynomials we get that $S_1(F_{(1)}) = q+1$, regardless of our choice of F. This leads us to the main theorem of Chapter 3.

Theorem 1.2.3. *Write $r = \prod_{j=1}^n p_j^{t_j}$. If q is fixed such that $q \equiv 1 \pmod{r}$, then as $d_1, \ldots, d_{r-1} \to \infty$ for any $M_s \in \mathbb{Z}[\zeta_s]$, where ζ_s is a primitive s^{th} root of unity,*

$$\frac{|\{C \in \mathcal{H}^{(d_1,\ldots,d_{r-1})} : S_s(F_{(s)})) = M_s, \forall s|r, s \neq 1\}|}{|\mathcal{H}^{(d_1,\ldots,d_{r-1})}|} \sim Prob\left(\sum_{i=1}^{q+1} X_{s,i} = M_s, \forall s|r, s \neq 1\right)$$

where $X_{s,i}$ are random variables taking values in $\mu_s \cup \{0\}$, the s^{th} roots of unity or 0, such that for any $\epsilon_{s,i} \in \mu_s$,

$$Prob(X_{s,i} = 0) = \frac{r - \frac{r}{s}}{q + r - 1}$$

$$Prob(X_{s,i} = \epsilon_{s,i} \neq 0) = \frac{q + \frac{r}{s} - 1}{s(q + r - 1)}.$$

Moreover, if $i \neq j$ *then* $X_{s,i}$ *and* $X_{s',j}$ *are independent for all* $s, s'|r$. *However, if we fix* i, *then for all* $s|r$

$$X_{s,i} = \prod_{\substack{p|s \\ p \text{ prime}}} (X_{p^{v_p(s)},i})^{\sigma_p} \text{ where } 1 \leq \sigma_p \leq \frac{s}{p^{v_p(s)}} \text{ such that } \sigma_p \equiv (p^{v_p(s)})^{-1} \pmod{\frac{s}{p^{v_p(s)}}}$$

where v_p *is the* p*-adic valuation. Further, for all* $p|r$ *and* $1 < v \leq v_p(r)$

$$Prob\left(X_{p^v,i} = 0 | X_{p^{v-1},i} = 0\right) = 1$$

$$Prob\left(X_{p^{v-1},i} = \epsilon^p_{p^v,i} | X_{p^v,i} = \epsilon_{p^v,i}\right) = 1.$$

Finally, if $s|r$ *but* $s \neq r$ *then*

$$Prob\left(X_{p^v,i} = \epsilon_{p^v,i} \neq 0, 1 \leq v \leq v_p(s) \text{ and } X_{p^v,i} = 0, v_p(s) < v \leq v_p(r) \text{ for all } p|r\right)$$

$$= \begin{cases} \frac{\phi(\frac{r}{s})}{s(q+r-1)} & \text{if } \epsilon_{p^{v-1},i} = \epsilon^p_{p^v,i} \text{ for all } p|r, 1 \leq v \leq v_p(s) \\ 0 & \text{otherwise} \end{cases}$$

and, if $s = r$,

$$Prob\left(X_{p^v,i} = \epsilon_{p^v,i}, v \leq v_p(r), \text{ for all } p|r\right) = \begin{cases} \frac{q}{r(q+r-1)} & \text{if } \epsilon_{p^{v-1},i} = \epsilon^p_{p^v,i}, 1 \leq v \leq v_p(r), \text{ for all } p|r \\ 0 & \text{otherwise.} \end{cases}$$

Remark 1.2.4. The random variable $X_{s,i}$ models the value of $\chi_s(F_{(s)}(x_i))$.

With a little more work we would be able to prove the following corollary from Theorem 1.2.3.

Corollary 1.2.5. *If* q *is fixed such that* $q \equiv 1 \pmod{r}$, *then as* $d_1, \ldots, d_{r-1} \to \infty$,

$$\frac{|\{C \in \mathcal{H}^{(d_1,\ldots,d_{r-1})} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}^{(d_1,\ldots,d_{r-1})}|} \sim Prob\left(\sum_{i=1}^{q+1} X_i = M\right)$$

where the X_i *are i.i.d. random variables taking value* 0 *or* s *for* $s|r$ *such that*

$$X_i = \begin{cases} s & \text{with probability } \frac{\phi(\frac{r}{s})}{s(q+r-1)} \text{ if } s \neq r \\ r & \text{with probability } \frac{q}{r(q+r-1)} \\ 0 & \text{with probability } \frac{(r-1)(q+r) - \sum_{s|r} s\phi(s) + 1}{r(q+r-1)} \end{cases}.$$

1.3 Abelian Curves

Lorenzo, Meleleo, Milione and Bucur [10] were the first to investigate the distribution of the number of points for non-cyclic curves. They determine the case when $G = (\mathbb{Z}/2\mathbb{Z})^n$. In Chapter 4 we extend this to all abelian curves.

Fix an abelian group,

$$G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$$

such that $r_1|r_2|\ldots|r_n$. Define

$$\mathcal{H}_{G,g} = \{C : \mathrm{Gal}(C) = G, g(C) = g\}.$$

Remark 1.3.1. Again, when talking about curves in $\mathcal{H}_{G,g}$ we will always be supposing the $q \equiv 1 \pmod{\exp(G)}$. Further, with our notation, $\exp(G) = r_n$.

If $C \in \mathcal{H}_{G,g}$ then it will have an affine model of the form

$$Y_j^{r_j} = F_j(X) \qquad F_j(X) \in \mathbb{F}_q[X]/(\mathbb{F}_q[X])^{r_j}, j = 1, \ldots, n.$$

Let $\mathcal{R} = [0, \ldots, r_1 - 1] \times \cdots \times [0, \ldots, r_n - 1] \setminus \{(0, \ldots, 0)\}$. Write $\vec{\alpha} \in \mathcal{R}$ as $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Then we can find a set of monic, square-free and pairwise coprime polynomials $(f_{\vec{\alpha}})_{\vec{\alpha}\in\mathcal{R}}$ and $c_1, \ldots, c_n \in \mathbb{F}_q^*$ such that

$$F_j(X) = c_j \prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}.$$

Denote $d(\vec{\alpha}) = \deg(f_{\vec{\alpha}})$, $d_j = \deg(F_j) = \sum_{\vec{\alpha}\in\mathcal{R}} \alpha_j d(\vec{\alpha})$ and $\vec{d} = (d_1, \ldots, d_n)$. Further, define

$$e(\vec{\alpha}) := \operatorname*{lcm}_{j=1,\ldots,n} \left(\frac{r_j}{(r_j, \alpha_j)} \right) \qquad e(\vec{d}) := \operatorname*{lcm}_{j=1,\ldots,n} \left(\frac{r_j}{(r_j, d_j)} \right).$$

Then the Riemann-Hurwitz formula (Theorem 7.16 from [12]) tells us the genus of C satisfies the formula

$$2g + 2|G| - 2 = \sum_{\vec{\alpha}\in\mathcal{R}} \left(|G| - \frac{|G|}{e(\vec{\alpha})} \right) d(\vec{\alpha}) + |G| - \frac{|G|}{e(\vec{d})}. \tag{1.3.1}$$

Remark 1.3.2. If we assume

$$\sum_{\vec{\alpha}\in\mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv 0 \pmod{r_j}, j = 1, \ldots, n \tag{1.3.2}$$

then (1.3.1) simplifies to

$$2g + 2|G| - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} \left(|G| - \frac{|G|}{e(\vec{\alpha})} \right) d(\vec{\alpha}). \tag{1.3.3}$$

Let $\vec{d}(\vec{\alpha}) = (d(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}}$ be a vector of non-negative integers indexed by the vectors in $\mathcal{R}$. Now, let $\mathcal{H}^{\vec{d}(\vec{\alpha})} \subset \mathcal{H}_{G,g}$ to be the family of curves such that the corresponding polynomials $(f_{\vec{\alpha}})$ have degrees $d(\vec{\alpha})$ or $d(\vec{\alpha}) - 1$, where at most one of the $f_{\vec{\alpha}}$ can have degree $d(\vec{\alpha}) - 1$.

Then

$$\mathcal{H}_{G,g} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{H}^{\vec{d}(\vec{\alpha})}, \tag{1.3.4}$$

where the union is over all $\vec{d}(\vec{\alpha})$ that satisfy (1.3.2) and (1.3.3). Note that under the condition (1.3.2), the set $\mathcal{H}^{\vec{d}(\vec{\alpha})}$ is genus-invariant. We will perform statistics on the components $\mathcal{H}^{\vec{d}(\vec{\alpha})}$ instead of the whole $\mathcal{H}_{G,g}$.

Define $\mathcal{S} = \{\vec{s} = (s_1, \dots, s_n) : s_j | r_j\}$ and for all $\vec{s} \in \mathcal{S}$ let

$$\Omega_{\vec{s}} = \{\vec{\omega} = (\omega_1, \dots, \omega_n) : 1 \leq \omega_j \leq s_j, (\omega_j, s_j) = 1\} \subset \mathcal{R}$$

$$\ell(\vec{s}) = \operatorname{lcm}(s_1, \dots, s_n)$$

For any $\vec{s} \in \mathcal{S}$ and $\vec{\omega} \in \Omega_{\vec{s}}$, define

$$F^{(\vec{\omega})}_{(\vec{s})}(X) = c^{(\vec{\omega})}_{(\vec{s})} \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j} \omega_j \alpha_j \pmod{\ell(\vec{s})}}$$

where

$$c^{(\vec{\omega})}_{(\vec{s})} = \prod_{j=1}^{n} c_j^{\frac{\ell(\vec{s})}{s_j} \omega_j \pmod{\ell(\vec{s})}}.$$

Then we can write

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_{\vec{s}}} \chi_{\vec{\ell}(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x))$$

Using this formula we get the main theorem of Chapter 4.

Theorem 1.3.3. *Let $G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$ and fix q such that $q \equiv 1 \pmod{r_n}$ then as $d(\vec{\alpha}) \to \infty$ for all $\vec{\alpha} \in \mathcal{R}$,*

$$\frac{|\{C \in \mathcal{H}^{(\vec{d}(\vec{\alpha}))} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}^{(\vec{d}(\vec{\alpha}))}|} \sim Prob\left(\sum_{i=1}^{q+1} X_i = M\right)$$

where the X_i *are i.i.d. random variables taking value* 0 *or* $\frac{|G|}{s}$ *for some* $s|r_n$ *such that*

$$X_i = \begin{cases} \frac{|G|}{s} & \text{with probability } \frac{s\phi_G(s)}{|G|(q+|G|-1)} \text{ if } s \neq 1 \\ |G| & \text{with probability } \frac{q}{|G|(q+|G|-1)} \\ 0 & \text{with probability } \frac{(|G|-1)(q+|G|)-\sum_{s|r_n} s\phi_G(s)+1}{|G|(q+|G|-1)} \end{cases}$$

where $\phi_G(s)$ *is the number of elements of* G *of order* s*.*

Remark 1.3.4. Theorem 1.3.3 reduces to Theorem 1.2.3 when G is cyclic, even though it is not obvious. In fact, how we prove Theorem 1.3.3 is to prove an analog of Theorem 1.2.3 and then do a little more work to get the finished form. The reason we leave Theorem 1.2.3 in the form it is in is to more clearly see the relation with the result of Bucur, David, Feigon and Lalın whereas we write Theorem 1.3.3 in the form it is in because this mirrors the form that Lorenzo, Meleleo, Milione and Bucur write their result in.

Remark 1.3.5. Theorem 1.3.3 reduces to Theorem 1.2.3 when G is cyclic, even though it is not obvious. In fact, how we prove Theorem 1.3.3 is to prove an analog of Theorem 1.2.3 and then do a little more work to get the finished form. The reason we leave Theorem 1.2.3 in the form it is in is to more clearly see the relation with the result of Bucur, David, Feigon and Lalın whereas we write Theorem 1.3.3 in the form it is in because this mirrors the form that Lorenzo, Meleleo, Milione and Bucur write their result in.

1.4 Statistics on the Whole Space

In all the previous work we restrict to the irreducible coarse moduli space $\mathcal{H}^{\vec{d}(\vec{\alpha})}$. The question remains: can we find results on the whole space $\mathcal{H}_{G,g}$? The first questions we may ask is what is the size of $\mathcal{H}_{G,g}$. A similar question was answered by Wright [14].

If $C \in \mathcal{H}_{G,g}$ then it corresponds to an extension L/K such that $\mathrm{Gal}(L/K) = G$. Moreover, the discriminant of L will be $q^{2g+2|G|-2}$ where g is the genus of C. Define

$$N(G, q^m) := \{L/K : \mathrm{Gal}(L/K) = G, \mathscr{D}(L/K) = q^m\} \tag{1.4.1}$$

where $\mathscr{D}(L/K)$ is the absolute norm of the relative discriminant of L over K.

Then Wright showed if $q \equiv 1 \pmod{\exp(G)}$, then as $m \to \infty$

$$\sum_{j=0}^{|G|-\frac{|G|}{Q}-1} q^{-\frac{j}{|G|-\frac{|G|}{Q}}} |N(G, q^{m+j})| \sim C(K,G) m^{\phi_G(Q)-1} q^{\frac{m}{|G|-\frac{|G|}{Q}}} \tag{1.4.2}$$

where $C(K,G)$ is a constant and Q is the smallest prime divisor of $|G|$. (Note: Wright's actual theorem does not depend on the fact that $q \equiv 1 \pmod{\exp(G)}$ but has a simpler form if we do assume it. Further, he proves analogous results for number field extensions.) He does not give an explicit formula for this constant nor does he determine an error term. This was addressed by several authors for the case of prime cyclic extensions. Cohen, Diaz and Olivier ([4]) in the number field setting and Bucur, David, Feigon, Kaplan, Lalın, Ozman and Wood ([1]) in the function field setting.

Proposition 2.1.12 shows that if $\vec{d}(\vec{\alpha}) \to \infty$ for all $\vec{\alpha} \in \mathcal{R}$ then

$$|\mathcal{H}^{\vec{d}(\vec{\alpha})}| \sim C q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})} \tag{1.4.3}$$

for some constant C that can be made explicit. Moreover, we can show that if there is a solution to (1.3.2) and (1.3.3) then as $g \to \infty$,

$$\sum_{\vec{d}(\vec{\alpha})} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})} = C' g^{\phi_G(Q)-1} q^{\frac{2g+2|G|-2}{|G|-\frac{|G|}{Q}}} \left(1 + O\left(\frac{1}{g}\right)\right) \tag{1.4.4}$$

where the sum is over all $\vec{d}(\vec{\alpha})$ that satisfy (1.3.2) and (1.3.3), C' is some constant that can be made explicit and Q is the smallest prime divisor of $|G|$. However, we can not conclude a similar formula for $|\mathcal{H}_{G,g}|$ as the error term in (1.4.3) is only valid if all $\vec{d}(\vec{\alpha}) \to \infty$ and hence when we apply the sum we get that the error term may be as big as the main term.

If we define

$$N(G,g) := \{C : \mathrm{Gal}(C) = G, g(C) = g\}$$

then, we can show

Theorem 1.4.1. *If there exists a solution to* (1.3.2) *and* (1.3.3) *then*

$$|N(G,g)| = \sum_{j=1}^{\eta} P_j(2g) q^{\frac{2g+2|G|-2}{|G|-\frac{|G|}{s_j}}} + O\left(q^{\frac{(1+\epsilon)g}{|G|-\frac{|G|}{s_1}}}\right)$$

where $1 = s_0 < s_1 < \cdots < s_\eta = r_n$ *are the divisors of* r_n *and* P_j *is a polynomial of degree at most* $\phi_G(s_j) - 1$. *If no solution to* (1.3.2) *and* (1.3.3) *exists then* $|N(G, g)| = 0$.

Moreover, if $G = (\mathbb{Z}/Q\mathbb{Z})^n$, *for* Q *a prime, and* $2g + 2Q^n - 2 \equiv 0 \pmod{Q^n - Q^{n-1}}$ *then*

$$|N(\mathbb{Z}/Q\mathbb{Z})^n, g)| = P\left(\frac{2g + 2Q^n - 2}{Q^n - Q^{n-1}}\right) q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}} + O\left(q^{\frac{(1+\epsilon)g}{Q^n-Q^{n-1}}}\right)$$

where P *is a polynomial of degree* $Q^n - 2$ *with leading coefficient*

$$\frac{1}{(Q^n - 2)!} \frac{q + Q^n - 1}{q} \frac{L_{Q^n-2}}{\zeta_q(2)^{Q^n-1}}$$

where L_{Q^n-2} *is a constant to be defined in Lemma 2.1.5 later and* $\zeta_q(s)$ *is the zeta-function associated to* K *((2.1.1)). If* $2g + 2Q^n - 2 \not\equiv 0 \pmod{Q^n - Q^{n-1}}$, *then* $|N(\mathbb{Z}/Q^n\mathbb{Z}, g)| = 0$.

Define $\mathcal{R}' = \mathcal{R} \cup \{(0, \ldots, 0\}$ and let $\vec{k} = (k_1, \ldots, k_n) \in \mathcal{R}'$. Moreover let

$$E = \begin{pmatrix} \epsilon_{1,1} & \cdots & \epsilon_{1,n} \\ \vdots & \ddots & \vdots \\ \epsilon_{\ell,1} & \cdots & \epsilon_{\ell,n} \end{pmatrix} \in M_{\ell,n}$$

where $\epsilon_{i,j} \in \mu_{r_j}$. For every such $\vec{k}$ and E let

$$N_{\vec{k},E}(G, g) = \{C : \mathrm{Gal}(C) = G, g(C) = g, \deg(F_j) \equiv k_j \pmod{r_j}$$
$$\chi_{r_j}(F_j(x_i) = \epsilon_{i,j}, i = 1, \ldots, \ell, j = 1, \ldots, n\}$$

where the F_j are the polynomials corresponding to the affine model of C.

Proposition 1.4.2. *If there exists a solution to* (1.3.1) *and*

$$\sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv k_j \pmod{r_j}, j = 1, \ldots, n \tag{1.4.5}$$

then

$$|N_{\vec{k},E}(G, g)| = \sum_{j=1}^{\eta} P_{j;\vec{k},E}(2g) q^{\frac{2g+2|G|-2}{|G|-\frac{|G|}{s_j}}} + O\left(q^{\frac{(1+\epsilon)g}{|G|-\frac{|G|}{s_1}}}\right)$$

where $1 = s_0 < s_1 < \cdots < s_\eta = r_n$ *are the divisors of* r_n *and* $P_{j;\vec{k},E}$ *is a polynomial of degree at most* $\phi_G(s_j) - 1$. *If there is no solution to* (1.3.1) *and* (1.4.5) *then* $|N_{\vec{k},E}(G, g)| = 0$.

Moreover, if $G = (\mathbb{Z}/Q\mathbb{Z})^n$, *for* Q *a prime, and* $2g + 2Q^n - 2 \equiv 0 \pmod{Q^n - Q^{n-1}}$ *then*

$$|N_{\vec{k},E}((\mathbb{Z}/Q\mathbb{Z})^n, g)| = P_{\vec{k},E}\left(\frac{2g + 2Q^n - 2}{Q^n - Q^{n-1}}\right) q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}} + O\left(q^{\frac{(1+\epsilon)g}{Q^n-Q^{n-1}}}\right)$$

where $P_{\vec{k},E}$ *is a polynomial of degree* $Q^n - 2$ *with leading coefficient*

$$\frac{(q-1)^n}{Q^n(Q^n-2)!}\frac{L_{Q^n-2}}{\zeta_q(2)^{Q^n-1}}\left(\frac{q}{Q^n(q+Q^n-1)}\right)^{\ell}.$$

If $2g + 2Q^n - 2 \not\equiv 0 \pmod{Q^n - Q^{n-1}}$ *then* $|N_{\vec{k},E}((\mathbb{Z}/Q\mathbb{Z})^n, g)| = 0$.

Remark 1.4.3. We actually show that the P_j and $P_{j;\vec{k},E}$ are polynomials of *exact* degree $\phi_G(s_j) - 1$ and can write down a formula for the leading coefficient. However, it is not clear what this leading coefficient is or even that it is non-zero in the case $G \neq (\mathbb{Z}/Q\mathbb{Z})^n$.

Since the leading coefficient of $P_{\vec{k},E}$ is independent of $\vec{k}$ and E when $G = (\mathbb{Z}/Q\mathbb{Z})^n$, we can extend Theorem 1.3.3 to the whole space $\mathcal{H}_{(\mathbb{Z}/Q\mathbb{Z})^n,g}$.

Theorem 1.4.4. *Let* $G = (\mathbb{Z}/Q\mathbb{Z})^n$ *and fix* q *such that* $q \equiv 1 \pmod{Q}$. *If* $2g + 2Q^n - 2 \equiv 0 \pmod{Q^n - Q^{n-1}}$ *then as* $g \to \infty$,

$$\frac{|\{C \in \mathcal{H}_{G,g} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}_{G,g}|} = Prob\left(\sum_{i=1}^{q+1} X_i = M\right)\left(1 + O\left(\frac{1}{g}\right)\right)$$

where the X_i *are i.i.d. random variables taking value* 0, Q^n *or* Q^{n-1} *such that*

$$X_i = \begin{cases} Q^{n-1} & \text{with probability } \frac{Q^n-1}{Q^{n-1}(q+Q^n-1)} \\ Q^n & \text{with probability } \frac{q}{Q^n(q+Q^n-1)} \\ 0 & \text{with probability } \frac{(Q^n-1)(q+Q^n-Q)}{Q^n(q+Q^n-1)} \end{cases}.$$

Chapter 2

Preliminary Results

2.1 Value Taking Polynomials

Let $F_1, \ldots, F_n$ be polynomials such that F_j is r_j^{th}-power free for $j = 1, \ldots, n$. In this section we will determine the number of such polynomials that take non-zero prescribed values at points in $\mathbb{F}_q$. That is if we fix an ordering $x_1, \ldots, x_q$ of the elements of $\mathbb{F}_q$ and let $a_{i,j} \in \mathbb{F}_q^*$ for $i = 1, \ldots, \ell$, $j = 1, \ldots, n$ we want to determine the size of the set

$$\{F_1, \ldots, F_n : F_j \text{ is } r_j^{th} - \text{power free and } F_j(x_i) = a_{i,j}, i = 1, \ldots, \ell, j = 1, \ldots, n\}$$

for $0 \leq \ell \leq q$. Many results of this nature have been proven by the authors who have worked on the main problem of this thesis. We will briefly recall the known results and use them to prove the fully general result that we need.

Remark 2.1.1. The ordering of $\mathbb{F}_q$, $x_1, \ldots, x_q$ will be fixed for the rest of the thesis.

2.1.1 Known Results

Denote by $\zeta_q(s)$ the zeta function of $K = \mathbb{F}_q[X]$ given by

$$\zeta_q(s) = \sum_F \frac{1}{|F|^s} = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} = (1 - q^{1-s})^{-1} \tag{2.1.1}$$

where the sum (product) is over all monic (irreducible) polynomials in K and $|F| = q^{\deg(F)}$.

We will need various different sets of polynomials. The first of which are

$$V_d = \{F \in \mathbb{F}_q[X] : F \text{ monic, } \deg(F) = d\} \tag{2.1.2}$$

$$\mathcal{F}_d = \{F \in \mathbb{F}_q[X] : F \text{ monic, square-free and } \deg(F) = d\} \tag{2.1.3}$$

$$\hat{\mathcal{F}}_d = \{cF \in \mathbb{F}_q[X] : F \text{ monic, square-free, } \deg(F) = d \text{ and } c \in \mathbb{F}_q^*\} \tag{2.1.4}$$

Clearly, $|\hat{\mathcal{F}}_d| = (q-1)|\mathcal{F}_d|$. In their work on hyper-elliptic curves Kurlberg and Rudnick [9] proved the following results.

Lemma 2.1.2 (Lemma 3 of [9]). *The number of square-free monic polynomials of degree d is*

$$|\mathcal{F}_d| = \begin{cases} q^d(1-q^{-1}) & d \geq 2 \\ q^d & d = 0, 1 \end{cases}$$

Lemma 2.1.3 (Lemma 4 of [9]). *For $0 \leq \ell \leq q$, let $a_1, \dots, a_\ell \in \mathbb{F}_q$. If $d \geq \ell$, then*

$$|\{\mathcal{F} \in V_d : F(x_1) = a_1, \dots, F(x_\ell) = a_\ell\}| = q^{d-\ell}$$

Lemma 2.1.4 (Lemma 5 of [9]). *Let $d \geq 2$ and $0 \leq \ell \leq q$ be positive integers and let $a_1, \dots, a_\ell \in \mathbb{F}_q^*$. Then*

$$|\{F \in \mathcal{F}_d : F(x_1) = a_1, \dots, F(x_\ell) = a_\ell\}| = \frac{q^{d-\ell}}{\zeta_q(2)(1-q^{-2})^\ell} + O\left(q^{d/2}\right)$$

Notice that $1 - q^{-1} = \frac{1}{\zeta_q(2)}$ so Lemmas 2.1.2 and 2.1.4 are, in fact, consistent. Moreover, it is easy to see that if we replace $\mathcal{F}_d$ with $\hat{\mathcal{F}}_d$, it will only add a factor of $q-1$.

Define

$$\mathcal{F}_{(d_1,\dots,d_{r-1})} = \{F = f_1 f_2^2 \cdots f_{r-1}^{r-1} : f_i \in \mathcal{F}_{d_i} \text{ and } (f_i, f_j) = 1\} \tag{2.1.5}$$

$$\hat{\mathcal{F}}_{(d_1,\dots,d_{r-1})} = \{F = c f_1 f_2^2 \cdots f_{r-1}^{r-1} : f_i \in \mathcal{F}_{d_i}, (f_i, f_j) = 1 \text{ and } c \in \mathbb{F}_q^*\} \tag{2.1.6}$$

to be the set of r^{th}-power free polynomials with prescribed degrees. Then Bucur, David, Fiegon and Lalin [3] solve an analogous result of Lemma 2.1.4 for this set.

Lemma 2.1.5 (Proposition 7.1 of [3]). *Fix $0 \leq \ell \leq q$ and $a_1, \dots, a_\ell \in \mathbb{F}_q^*$. Then for each $r \geq 2$ and $\epsilon > 0$,*

$$|\{F \in \mathcal{F}_{(d_1,\dots,d_{r-1})} : F(x_i) = a_i, 1 \leq i \leq \ell\}| = \frac{L_{r-2} q^{d_1+\cdots+d_{r-1}}}{\zeta_q(2)^{r-1}} \left(\frac{q}{(q+r)(q-1)}\right)^\ell \times \left(1 + O\left(q^{\epsilon\ell} \sum_{h=2}^{r-1} q^{\epsilon(d_h+\cdots+d_{r-1})-d_h} + q^{-d_1/2+\ell}\right)\right),$$

where

$$L_{r-2} = \prod_P \left(\frac{|P|^{r-2}(|P|+r-1)}{(|P|+1)^{r-1}} \right).$$

Furthermore, taking $\ell = 0$*, this gives,*

$$|\{F \in \mathcal{F}_{(d_1,\dots,d_{r-1})}| = \frac{L_{r-2}q^{d_1+\cdots+d_{r-1}}}{\zeta_q(2)^{r-1}} \left(1 + O\left(\sum_{h=2}^{r-1} q^{\epsilon(d_h+\cdots+d_{r-1})-d_h} + q^{-d_1/2}\right)\right),$$

There is a technical lemma in [2] that we need to prove Lemma 2.1.11 and Proposition 2.1.12.

Lemma 2.1.6 (Lemma 3.2 of [2])**.** *Let* U *be a polynomial of degree* u *such that* $U(x_i) \neq 0$ *for* $1 \leq i \leq \ell$*. For any* $j \geq 1$*, and* $F \in \mathbb{F}_q[X]$*, let*

$$c_j^U(F) = \begin{cases} \mu^2(F) \prod_{P|F}(1+j|P|^{-1})^{-1} & \text{if } F(x_i) \neq 0, 1 \leq i \leq \ell, (F,U) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then, for any $1 > \epsilon > 0$*,*

$$\sum_{\deg(F)=d} c_j^U(F) = \frac{K_j q^d}{\zeta_q(2)} \left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+1}\right)\right) \left(1 + O\left(q^{\epsilon(d+u+\ell)-d}\right)\right),$$

where

$$K_j = \prod_P \left(\frac{|P|(|P|+j+1)}{(|P|+1)(|P|+j)} \right).$$

Remark 2.1.7. Notice that $L_n = K_1 K_2 \cdots K_n$. Moreover, from now on, whenever we write L_r or K_j, we will mean them to be these constants.

Remark 2.1.8. The error term of Lemma 2.1.5 comes from the error term of Lemma 2.1.6. In particular, the

$$O\left(q^{\epsilon\ell} \sum_{h=2}^{r-1} q^{\epsilon(d_h+\cdots+d_{r-1})-d_h}\right)$$

comes from the error term appearing in Lemma 2.1.6. We show in Lemma 2.1.10 that we can improve this to

$$O\left(q^{\epsilon\ell-(1-\epsilon)\min(d_i)}\right).$$

However, since we still have the

$$O\left(q^{-d_1/2+\ell}\right)$$

term appearing, we can only improve the error term to

$$O\left(q^{-\min(d_i)/2+\ell}\right).$$

This isn't much of an improvement as we still need all the $d_i \to \infty$ for the error term to be less than the main term, but it is at least more aesthetically pleasing and easier to understand.

The last result we need is due to Lorenzo, Meleleo, Milione and Bucur [10].

Lemma 2.1.9 (Lemma 6.4 from [10]). *Let $d_1, \dots, d_n$ be positive integers. For $0 \le \ell \le q$, let $U \in \mathbb{F}_q[X]$ be such that $U(x_i) \neq 0$ for $i = 1, \dots, \ell$. Let $a_{i,j} \in \mathbb{F}_q^*$, $i = 1, \dots, \ell$, $j = 1, \dots, n$. Then the number of elements in the set*

$$\mathcal{R}^U_{d_1,\dots,d_n}(a_{i,j}) := \{(f_1, \dots, f_n) \in \mathcal{F}_{d_1} \times \cdots \times \mathcal{F}_{d_n} : (f_j, U) = (f_j, f_k) = 1, f_j(x_i) = a_{i,j}, \\ 1 \le i \le \ell, 1 \le j, k \le n, j \neq k\}$$

is the number

$$R^U_n(\ell) = \frac{q^{d_1+\cdots+d_n} L_{n-1}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n(q+n)}\right)^\ell \prod_{P|U} \left(\frac{1}{1+n|P|^{-1}}\right) \left(1 + O\left(q^{\ell - \frac{\min(d_i)}{2}}\right)\right).$$

2.1.2 Key Proposition

In this section we use the results of the Section 2.1.1 to prove a key proposition on how many polynomials take prescribed non-zero values. This will be instrumental in calculating the statistics that is the main result of this thesis. But first, let us extend Lemma 2.1.6 a little.

Lemma 2.1.10. *Let $d_1, \dots, d_n$ be positive integers and U a polynomial of degree u such that $U(x_i) \neq 0$ for $i = 1, \dots, \ell$. For any j and $F \in \mathbb{F}_q[X]$, let $c_j^U(F)$ be as in Lemma 2.1.6. Then for any $1 > \epsilon > 0$,*

$$\sum_{\deg(F_1)=d_1} \cdots \sum_{\deg(F_n)=d_n} c_j^U(F_1 \cdots F_n) = \frac{L_{j+n-1} q^{d_1+\cdots+d_n}}{L_{j-1}\zeta_q(2)^n} \left(\frac{q+j}{q+j+n}\right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+n}\right)\right) \times \\ \left(1 + O\left(q^{\epsilon(u+\ell) - (1-\epsilon)\min(d_i)}\right)\right)$$

Proof. We will prove it true for $n = 2$ and the generic case follows by the same logic. By Lemma 2.1.6, for any $1 > \epsilon_1, \epsilon_2 > 0$,

$$\sum_{\deg(F_1)=d_1} \sum_{\deg(F_2)=d_2} c_j^U(F_1F_2) = \sum_{\deg(F_1)=d_1} c_j^U(F_1) \sum_{\deg(F_2)=d_2} c_j^{UF_1}(F_2)$$

$$= \sum_{\deg(F_1)=d_1} c_j^U(F_1) \frac{K_j q^{d_2}}{\zeta_q(2)} \left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|UF_1} \left(\frac{|P|+j}{|P|+j+1}\right)\right) \left(1+O\left(q^{\epsilon_2(d_1+d_2+u+\ell)-d_2}\right)\right)$$

$$= \frac{K_j q^{d_2}}{\zeta_q(2)} \left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+1}\right)\right) \left(1+O\left(q^{\epsilon_2(d_1+d_2+u+\ell)-d_2}\right)\right) \sum_{\deg(F_1)=d_1} c_{j+1}^U(F_1)$$

$$= \frac{K_j K_{j+1} q^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q+j}{q+j+2}\right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+2}\right)\right) \left(1+O\left(q^{\epsilon_2(d_1+d_2+u+\ell)-d_2}+q^{\epsilon_1(d_1+u+\ell)-d_1}\right)\right).$$

However, we could have summed F_2 before F_1 to get that for any $1>\epsilon_1', \epsilon_2'>0$,

$$\sum_{\deg(F_1)=d_1} \sum_{\deg(F_2)=d_2} c_j^U(F_1F_2) = \sum_{\deg(F_2)=d_2} \sum_{\deg(F_1)=d_1} c_j^U(F_2F_1)$$

$$= \frac{K_j K_{j+1} q^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q+j}{q+j+2}\right)^\ell \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+2}\right)\right) \left(1+O\left(q^{\epsilon_1'(d_1+d_2+u+\ell)-d_1}+q^{\epsilon_2'(d_2+u+\ell)-d_2}\right)\right)$$

where the error term is different. Thus the true error term must be smaller than both of these error terms.

If $d_1 \le d_2$, then if we let $\epsilon_2 = \frac{1}{2}\epsilon_1$ then,

$$q^{\epsilon_2(d_1+d_2+u+\ell)-d_2} \le q^{\epsilon_1(d_1+u+\ell)-d_1}.$$

Therefore, using the first version of the error we get the true error term is $O\left(q^{\epsilon_1(d_1+u+\ell)-d_1}\right)$. Finally, if $d_2 \le d_1$, then we do the same argument with the second version of the error term.

Finally, we remark that $K_j K_{j+1} = L_{j+1}/L_{j-1}$.

□

Lemma 2.1.11. *Let $d_{1,1}, \dots, d_{1,r_1-1}, \dots, d_{n,1}, \dots, d_{n,r_n-1}$ be positive integers. For $0 \le \ell \le q$, let $U \in \mathbb{F}_q[X]$ be such that $U(x_i) \ne 0$ for $1 \le i \le \ell$. Let $a_{1,1}, \dots, a_{\ell,1}, \dots, a_{1,n}, \dots, a_{\ell,n} \in \mathbb{F}_q^*$. Then the size of*

$$\{(F_1, \dots, F_n) \in \mathcal{F}_{d_{1,1},\dots,d_{1,r_1-1}} \times \cdots \times \mathcal{F}_{d_{n,1},\dots,d_{n,r_n-1}} : (F_j, F_k) = (F_j, U) = 1, F_j(x_i) = a_{i,j}, \\ 1 \le i \le \ell, 1 \le j,k \le n, j \ne k\}$$

is

$$T_n^U(\ell) := \frac{L_{r_1+\cdots+r_n-n-1} q^{d_{1,1}+\cdots+d_{n,r_n-1}}}{\zeta_q(2)^{r_1+\cdots+r_n-n}} \left(\frac{q}{(q-1)^n(q+r_1+\cdots+r_n-n)}\right)^\ell \\ \times \prod_{P|U} \frac{|P|}{|P|+r_1+\cdots+r_n-n} \left(1+O\left(q^{\ell-\frac{\min(d_{i,j})}{2}}\right)\right).$$

Proof. For any $1 \leq j \leq n$, let $f_{j,k}$, $k = 1, \ldots, r_j - 1$ such that $f_{j,k}$ are square-free, monic, $\deg(f_{j,k}) = d_{j,k}$ and $(f_{j,k}, f_{j,k'}) = 1$ for all $k \neq k'$ and

$$F_j = \prod_{k=1}^{r_j - 1} f_{j,k}^k.$$

Moreover, since we are assuming $(F_j, F_{j'}) = 1$, for all $j \neq j'$, we also have $(f_{j,k}, f_{j',k'}) = 1$ for all $(j,k) \neq (j',k')$. Further, by the same reasoning we have $(f_{j,k}, U) = 1$ for all (j,k).

Therefore,

$$T_n^U(\ell) = \sum_{\substack{f_{j,k} \in \mathcal{F}_{d_{j,k}}, k \neq 1 \\ (f_{j,k}, f_{j',k'}) = 1 \\ f_{j,k}(x_i) \neq 0 \\ (f_{j,k}, U) = 1}} |\{(f_{1,1}, \ldots, f_{n,1}) \in \mathcal{F}_{d_{1,1}} \times \ldots \mathcal{F}_{d_{n,1}} : (f_{j,1}, f_{j',1}) = (f_{j,1}, U \prod_{k \neq 1} f_{j,k}) = 1$$
$$f_{j,1}(x_i) = a_{i,j} \prod_{k=2}^{r_i - 1} f_{j,k}(x_i)^{-k}, 1 \leq i \leq \ell, 1 \leq j, j' \leq n, j \neq j'\}|$$

However, the summand above is exactly $R_n^U(\ell)$ as defined in Lemma 2.1.9. Hence,

$$\begin{aligned}
T_n^U(\ell) &= \sum_{\substack{f_{j,k} \in \mathcal{F}_{d_{j,k}}, k \neq 1 \\ (f_{j,k}, f_{j',k'}) = 1 \\ f_{j,k}(x_i) \neq 0 \\ (f_{j,k}, U) = 1}} R_n^{U \prod_{k \neq 1} f_{j,k}}(\ell) \\
&= \sum_{\substack{f_{j,k} \in \mathcal{F}_{d_{j,k}}, k \neq 1 \\ (f_{j,k}, f_{j',k'}) = 1 \\ f_{j,k}(x_i) \neq 0 \\ (f_{j,k}, U) = 1}} \frac{L_{n-1} q^{d_{1,1} + \cdots + d_{n,1}}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n (q+n)} \right)^\ell \prod_{P | U \prod_{k \neq 1} f_{j,k}} \frac{|P|}{|P| + n} \times \\
&\quad \left(1 + O\left(q^{\ell - \frac{\min(d_{1,k})}{2}} \right) \right) \\
&= \frac{L_{n-1} q^{d_{1,1} + \cdots + d_{n,1}}}{\zeta_q^n(2)} \left(\frac{q}{(q-1)^n (q+n)} \right)^\ell \left(1 + O\left(q^{\ell - \frac{\min(d_{j,1})}{2}} \right) \right) \times \\
&\quad \sum_{\substack{f_{j,k} \in \mathcal{F}_{d_{j,k}}, k \neq 1 \\ (f_{j,k}, f_{j',k'}) = 1 \\ f_{j,k}(x_i) \neq 0 \\ (f_{j,k}, U) = 1}} \prod_{P | U \prod_{k \neq 1} f_{j,k}} \frac{|P|}{|P| + n}.
\end{aligned}$$

Lemma 2.1.10 shows that for any $1 > \epsilon > 0$,

$$\sum_{\substack{f_{j,k}\in\mathcal{F}_{d_{j,k}},k\neq 1\\(f_{j,k},f_{j',k'})=1\\f_{j,k}(x_i)\neq 0}}\prod_{P|U}\frac{|P|}{|P|+n}=\sum_{\deg(f_{1,2})=d_{1,2}}\cdots\sum_{\deg(f_{r_n-1,n})=d_{r_n-1,n}}c_n^U\left(\prod_{k\neq 1}f_{j,k}\right)$$

$$\begin{aligned}=&\frac{L_{r_1+\cdots+r_n-n-1}q^{d_{1,1}+\cdots+d_{n,r_n-1}}}{L_{n-1}\zeta_q(2)^{r_1+\cdots+r_n-n}}\left(\frac{q+n}{(q+r_1+\cdots+r_n-n)}\right)^{\ell}\\&\times\prod_{P|U}\frac{|P|}{|P|+r_1+\cdots+r_n-n}\left(1+O\left(q^{\epsilon(u+\ell)-(1-\epsilon)\min(d_{j,k})}\right)\right)\end{aligned}$$

which completes the proof.

□

Lemma 2.1.11 deals with the case where the F_j are all coprime. We want, however the case where they are not necessarily coprime. Suppose now that we have $(F_1,\dots,F_n)\in\mathcal{F}_{d_{1,1},\dots,d_{1,r_1-1}}\times\cdots\times\mathcal{F}_{d_{n,1},\dots,d_{n,r_n-1}}$ which are not necessarily coprime. Suppose

$$F_j=\prod_{k=1}^{r_j-1}f_{j,k}^k.$$

We want to rewrite the F_j as products of square-free polynomials that are all coprime to one another. For example, if $n=2,r_1=r_2=4$ then we would have

$$F_1=f_{1,1}f_{1,2}^2f_{1,3}^3\qquad F_2=f_{2,1}f_{2,2}^2f_{2,3}^3.$$

If we define

$$f_{(i,j)}=\gcd(f_{1,i},f_{2,j}),1\leq i,j\leq 3$$

and

$$f_{(i,0)}=\frac{f_{1,i}}{f_{(i,1)}f_{(i,2)}f_{(i,3)}}\quad f_{(0,j)}=\frac{f_{2,j}}{f_{(1,j)}f_{(2,j)}f_{(3,j)}},1\leq i,j\leq 3$$

then all the $f_{(i,j)}$ are square-free and coprime to one another. Moreover

$$F_1=f_{(1,0)}f_{(1,1)}f_{(1,2)}f_{(1,3)}f_{(2,0)}^2f_{(2,1)}^2f_{(2,2)}^2f_{(2,3)}^2f_{(3,0)}^3f_{(3,1)}^3f_{(3,2)}^3f_{(3,3)}^3=\prod_{\substack{i=0\\(i,j)\neq(0,0)}}^{3}\prod_{j=0}^{3}f_{(i,j)}^i$$

$$F_2=f_{(0,1)}f_{(1,1)}f_{(2,1)}f_{(3,1)}f_{(0,2)}^2f_{(1,2)}^2f_{(2,2)}^2f_{(3,2)}^2f_{(0,3)}^3f_{(1,3)}^3f_{(2,3)}^3f_{(3,3)}^3=\prod_{\substack{i=0\\(i,j)\neq(0,0)}}^{3}\prod_{j=0}^{3}f_{(i,j)}^j.$$

In general, define

$$\mathcal{R} = [0, \ldots, r_1 - 1] \times \cdots \times [0, \ldots, r_n - 1] \setminus \{(0, 0, \ldots, 0)\}$$

and write $\vec{\alpha} \in \mathcal{R}$ as $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Define also $f_{\vec{\alpha}}$ to be the largest monic polynomial such that

$$f_{\vec{\alpha}} \text{ divides } \gcd_{\substack{j=1,\ldots,n \\ \alpha_j \neq 0}} (f_{j,\alpha_j}) \quad \text{and} \quad (f_{\vec{\alpha}}, \prod_{\substack{j=1 \\ \alpha_j = 0}}^{n} F_j) = 1.$$

With this definition we get if $\vec{\alpha} \neq \vec{\beta}$ then $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$. Indeed, suppose we have $\alpha_j \neq \beta_j$ and $\alpha_j, \beta_j \neq 0$. Then $f_{\vec{\alpha}} | f_{j,\alpha_j}$ and $f_{\vec{\beta}} | f_{j,\beta_j}$ and since $(f_{j,\alpha_j}, f_{j,\beta_j}) = 1$, we get that $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$. On the other hand suppose we have $\alpha_j \neq \beta_j = 0$. Then $f_{\vec{\alpha}} | f_{j,\alpha_j} | F_j$ but $(f_{\vec{\beta}}, F_j) = 1$ hence $(f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1$.

Fix a $1 \leq j \leq n$ and $1 \leq k \leq r_j - 1$. Let $\vec{\beta} = (0, \ldots, 0, k, 0, \ldots, 0)$, where the k is in the j^{th} position. Then $f_{\vec{\beta}}$ is the largest polynomial that divides $f_{j,k}$ that is coprime to all the other $f_{j',k'}$. If $f_{\vec{\beta}} \neq f_{j,k}$ then

$$\prod_{\substack{\vec{\alpha} \in \mathcal{R} \setminus \{\vec{\beta}\} \\ \alpha_j = k}} f_{\vec{\alpha}}$$

is the largest polynomial that divides $f_{j,k}$ that is not coprime to at least one of the other $f_{j',k'}$. If $f_{\vec{\beta}} = f_{j,k}$, then $f_{\vec{\alpha}} = 1$ for all $\vec{\alpha} \neq \vec{\beta}$ such that $\alpha_j = k$. In either case we get

$$f_{j,k} = f_{\vec{\beta}} \prod_{\substack{\vec{\alpha} \neq \vec{\beta} \\ \alpha_j = k}} f_{\vec{\alpha}} = \prod_{\alpha_j = k} f_{\vec{\alpha}}.$$

We can then rewrite

$$F_j = \prod_{k=1}^{r_j - 1} f_{j,k}^k \qquad \text{as} \qquad F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$$

where we use the convention that $f_{\vec{\alpha}}^0$ is identically the constant polynomial 1.

Define $\vec{d}(\vec{\alpha}) := (d(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}}$ to be an integer vector with non-negative entries indexed by the vectors of $\mathcal{R}$. Further, define the set

$$\mathcal{F}_{\vec{d}(\vec{\alpha})} = \{(f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}} \in \prod_{\vec{\alpha} \in \mathcal{R}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \text{ for all } \vec{\alpha} \neq \vec{\beta} \in \mathcal{R}\}. \tag{2.1.7}$$

To ease notation, we will write just $(f_{\vec{\alpha}})$ instead of $(f_{\vec{\alpha}})_{\alpha\in\mathcal{R}}$ if it is clear what set the indices $\vec{\alpha}$ run over. Hence,

$$\begin{aligned}&\{(F_1,\dots,F_n)\in\mathcal{F}_{d_{1,1},\dots,d_{1,r_1-1}}\times\cdots\times\mathcal{F}_{d_{n,1},\dots,d_{n,r_n-1}}:F_j(x_i)=a_{i,j},1\le i\le\ell,1\le j\le n\}\\ =&\bigcup_{\substack{\vec{d}(\vec{\alpha})\\ \sum_{\alpha_j=k}d(\vec{\alpha})=d_{j,k}}}\{(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})}:\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}}^{\alpha_j}(x_i)=a_{i,j},1\le i\le\ell,1\le j\le n\}\end{aligned}$$

From now on we will work with the set $\mathcal{F}_{\vec{d}(\vec{\alpha})}$. This leads to key proposition for our statistics: Proposition 2.1.12.

Proposition 2.1.12. *Let $\vec{d}(\vec{\alpha})$ be as above. For $0\le\ell\le q$, let $a_{i,j}\in\mathbb{F}_q^*$ for $1\le i\le\ell$, $1\le j\le n$. Then the size of*

$$\{(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})}:F_j(x_i):=\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}}^{\alpha_j}(x_i)=a_{i,j},1\le i\le\ell,1\le j\le n\}$$

is

$$S_n(\ell):=\frac{L_{r_1\cdots r_n-2}q^{\sum_{\vec{\alpha}\in\mathcal{R}}d_{\vec{\alpha}}}}{\zeta_q(2)^{r_1\cdots r_n-1}}\left(\frac{q}{(q-1)^n(q+r_1\cdots r_n-1)}\right)^{\ell}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}}d_{\vec{\alpha}}}{2}}\right)\right).$$

Proof. We will apply Lemma 2.1.11 to the factors of $F_j:=\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}}^{\alpha_j}$ that is coprime to all the other F_k, $k\neq j$. In order to do this we will need some new notation. Define

$$\mathcal{S}_j:=\{(0,\dots,0,\alpha_j,0,\dots,0):1\le\alpha_j\le r_j-1\}\subset\mathcal{R}$$

where the non-zero entry is in the j^{th} coordinate. Define,

$$\mathcal{S}=\bigcup_{j=1}^{n}\mathcal{S}_j.$$

Then the factor of $F_j=\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}}^{\alpha_j}$ that is coprime to all F_k such that $j\neq k$ will be $\prod_{\vec{\alpha}\in\mathcal{S}_j}f_{\vec{\alpha}}^{\alpha_j}$. Further for any subset $\mathcal{T}\subset\mathcal{R}$, define

$$\mathcal{F}^{\mathcal{T}}_{(d(\vec{\alpha}))_{\vec{\alpha}\in\mathcal{T}}}=\{(f_{\vec{\alpha}})\in\prod_{\vec{\alpha}\in\mathcal{T}}\mathcal{F}_{d(\vec{\alpha})}:(f_{\vec{\alpha}},f_{\vec{\beta}})=1,\text{ for }\vec{\alpha}\neq\vec{\beta}\in\mathcal{T}\}.$$

We will denote this as just $\mathcal{F}^{\mathcal{T}}_{\vec{d}(\vec{\alpha})}$ with the understanding that in this context $\vec{d}(\vec{\alpha})$ is indexed by $\mathcal{T}$ instead of $\mathcal{R}$. Then,

$$
\begin{aligned}
S_n(\ell) &= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \le i \le \ell, 1 \le j \le n\}| \\
&= \sum_{\substack{(f_{\vec{\alpha}})\in\mathcal{F}^{\mathcal{R}\setminus\mathcal{S}}_{\vec{d}(\vec{\alpha})} \\ f_{\vec{\alpha}}(x_i)\neq 0}} |\{(f_{\vec{\alpha}}) \in \mathcal{F}^{\mathcal{S}}_{\vec{d}(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1, \vec{\alpha} \in \mathcal{S}, \vec{\beta} \in \mathcal{R}\setminus\mathcal{S}, \prod_{\vec{\alpha}\in\mathcal{S}_j} f_{\vec{\alpha}}^{\alpha_j}(x_i) = b_{i,j}\}| \\
&= \sum_{\substack{(f_{\vec{\alpha}})\in\mathcal{F}^{\mathcal{R}\setminus\mathcal{S}}_{\vec{d}(\vec{\alpha})} \\ f_{\vec{\alpha}}(x_i)\neq 0}} T_n^{\prod_{\vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}} f_{\vec{\alpha}}}(\ell)
\end{aligned}
$$

where $T_n^{\prod_{\vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}} f_{\vec{\alpha}}}(\ell)$ is as in Lemma 2.1.11 and

$$
b_{i,j} = a_{i,j} \prod_{\vec{\alpha}\in\mathcal{R}\setminus S} f_{\vec{\alpha}}(x_i)^{-\alpha_j}.
$$

Thus, using Lemma 2.1.11

$$
\begin{aligned}
S_n(\ell) = &\sum_{\substack{(f_{\vec{\alpha}})\in\mathcal{F}^{\mathcal{R}\setminus\mathcal{S}}_{d(\vec{\alpha})} \\ f_{\vec{\alpha}}(x_i)\neq 0}} \frac{L_{r_1+\cdots+r_n-n-1} q^{\sum_{\vec{\alpha}\in\mathcal{S}} \vec{d}(\vec{\alpha})}}{\zeta_q(2)^{r_1+\cdots+r_n-n}} \left(\frac{q}{(q-1)^n(q+r_1+\cdots+r_n-n)}\right)^{\ell} \\
&\times \prod_{\substack{P | f_{\vec{\alpha}} \\ \vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}}} \frac{|P|}{|P|+r_1+\cdots+r_n-n}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{S}} d_{\vec{\alpha}}}{2}}\right)\right) \\
&= M \frac{L_{r_1+\cdots+r_n-n-1} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r_1+\cdots+r_n-n}} \left(\frac{q}{(q-1)^n(q+r_1+\cdots+r_n-n)}\right)^{\ell} \left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{S}} d_{\vec{\alpha}}}{2}}\right)\right),
\end{aligned}
$$

where

$$
\begin{aligned}
M = &\sum_{\substack{(f_{\vec{\alpha}})\in\mathcal{F}^{\mathcal{R}\setminus\mathcal{S}}_{\vec{d}(\vec{\alpha})} \\ f_{\vec{\alpha}}(x_i)\neq 0}} \prod_{\substack{P | f_{\vec{\alpha}} \\ \vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}}} \frac{|P|}{|P|+r_1+\cdots+r_n-n} \\
= &\sum_{(f_{\vec{\alpha}})\in\mathcal{F}^{\mathcal{R}\setminus\mathcal{S}}_{\vec{d}(\vec{\alpha})}} c^1_{r_1+\cdots+r_n-n}\left(\prod_{\vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}} f_{\vec{\alpha}}\right) \\
= &\frac{L_{r_1\ldots r_n-1} q^{\sum_{\vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}} d_{\vec{\alpha}}}}{L_{r_1+\cdots+r_n-n-1}\zeta_q(2)^{r_1\cdots r_n-r_1-\ldots r_n+n-1}} \left(\frac{q+r_1+\cdots+r_n-n-1}{q+r_1\cdots r_n-1}\right)^{\ell} \left(1+O\left(q^{-\epsilon\min_{\vec{\alpha}\in\mathcal{R}\setminus\mathcal{S}} d_{\vec{\alpha}}}\right)\right)
\end{aligned}
$$

by Lemma 2.1.10 where $c^1_j(F)$ is defined in Lemma 2.1.6.

□

Corollary 2.1.13. *Let $\vec{d}(\vec{\alpha})$ be as above. For $0 \leq \ell \leq q$, let $\epsilon_{1,1}, \ldots, \epsilon_{\ell,1}, \ldots, \epsilon_{1,n}, \ldots, \epsilon_{\ell,n}$ be roots of unity such that $\epsilon_{i,j} \in \mu_{r_j}$. Let χ_{r_j} be primitive multiplicative characters of order r_j on $\mathbb{F}_q$, then*

$$|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}|$$
$$= \frac{L_{r_1 \cdots r_n - 2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}}{\zeta_q(2)^{r_1 \cdots r_n - 1}} \left(\frac{q}{r_1 \ldots r_n (q + r_1 \cdots r_n - 1)} \right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}{2}} \right) \right).$$

Proof. This follows immediately from Proposition 2.1.12 and the fact that if $\chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}$ then there are $\frac{q-1}{r_j}$ different $a_{i,j}$ such that $F_j(x_i) = a_{i,j}$.

□

2.2 Genus Formula

Let C be a curve such that $\mathrm{Gal}(C) = G := \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$. (Recall we defined $\mathrm{Gal}(C) = \mathrm{Gal}(K(C)/K)$.) Since we are assuming $q \equiv 1 \pmod{\exp(G)}$, we get that $K(C)/K$ is a Kummer extension. Then Kummer Theory (Chap.14 Proposition 37 of [6]) tells us that there exists $F_1, \ldots, F_n \in K$ such that F_j is r_j^{th}-power free and

$$K(C) = K(\sqrt[r_1]{F_1}, \ldots, \sqrt[r_n]{F_n}).$$

Let $g = g(C)$, be the genus of the curve C. Then the Riemann-Hurwitz formula (Theorem 7.16 of [12]), says that

$$2g + 2|G| - 2 = \sum_{\mathfrak{P}} (e(\mathfrak{P}/P) - 1) \deg_{K(C)}(\mathfrak{P}) \tag{2.2.1}$$

where the sum is over all primes $\mathfrak{P}$ of $K(C)$, $e(\mathfrak{P}/P)$ is the ramification index and $\deg_{K(C)}(\mathfrak{P})$ is the dimension of $K(C)/\mathfrak{P}$ as a vector space over $\mathbb{F}_q$. By Proposition 7.7 of [12], we get that if $\mathfrak{P}|P$, then $\deg_{K(C)}(\mathfrak{P}) = f(\mathfrak{P}/P) \deg_K(P)$, where $f(\mathfrak{P}/P)$ is the inertia degree and $\deg_K(P)$ is the degree of the polynomial P. Moreover, since our extension is Galois, we get that for any $\mathfrak{P}_1, \mathfrak{P}_2|P$, $e(\mathfrak{P}_1/P) = e(\mathfrak{P}_2/P) := e(P)$ and $f(\mathfrak{P}_1/P) = f(\mathfrak{P}_2/P) := f(P)$. Hence,

$$\sum_{\mathfrak{P}|P} (e(\mathfrak{P}/P) - 1) \deg_{K(C)}(\mathfrak{P}) = g(P)(e(P) - 1) f(P) \deg_K(P)$$

$$= \left(|G| - \frac{|G|}{e(P)}\right) \deg_K(P),$$

where $g(P)$ is the number of $\mathfrak{P}|P$.

Therefore, (2.2.1) becomes

$$2g + 2|G| - 2 = \sum_P \left(|G| - \frac{|G|}{e(P)}\right) \deg_K(P) \tag{2.2.2}$$

where the sum is over all the primes in K. Hence it is enough to determine the ramification index for all P in K.

Lemma 2.2.1. *Let $K \subset K' \subset K'(\sqrt[r]{F(X)}) = K_1'$ be an extension of fields where $F \in \mathbb{F}_q[X]^*/(\mathbb{F}_q[X]^*)^r$ and $[K_1' : K'] = r$. Let $\mathfrak{P}$ be a prime in K' and $\mathfrak{P}'$ be a prime in K_1', lying over $\mathfrak{P}$. If $ord_{\mathfrak{P}}(F) = n$, then $e(\mathfrak{P}'/\mathfrak{P}) = \frac{r}{(r,n)}$.*

Proof. Since $[K_1' : K'] = r$, the characteristic polynomial is $Y^r - F(X)$. We can write $F(X) = F_1(X)F_2(X)^n$ where $\text{ord}_{\mathfrak{P}}(F_2(X)) = 1$ and $(F_1(X)\mathcal{O}_{K'}, \mathfrak{P}) = 1$. Then $Y^r - F(X) \equiv Y^r \pmod{\mathfrak{P}}$. Hence,

$$\mathfrak{P}' = \mathfrak{P}\mathcal{O}_{K_1'} + \sqrt[r]{F(X)}\mathcal{O}_{K_1'}$$

will be a prime lying over $\mathfrak{P}$.

Now, $e(\mathfrak{P}'/\mathfrak{P})$ will be the smallest integer e such that $(\mathfrak{P}')^e \subset \mathfrak{P}\mathcal{O}_{K_1'}$. We have that

$$(\mathfrak{P}')^e = \sum_{j=0}^{e} \mathfrak{P}^{e-j} \left(\sqrt[r]{F(X)}\mathcal{O}_{K_1'}\right)^j.$$

Now,

$$\sum_{j=0}^{e-1} \mathfrak{P}^{e-j} \left(\sqrt[r]{F(X)}\mathcal{O}_{K_1'}\right)^j \subset \mathfrak{P}O_{K_1'}$$

so it remains to determine when $\left(\sqrt[r]{F(X)}\mathcal{O}_{K_1'}\right)^e \subset \mathfrak{P}O_{K_1'}$. Finally,

$$\left(\sqrt[r]{F(X)}\mathcal{O}_{K_1'}\right)^e = \left(\sqrt[r]{F_1(X)F_2(X)^n}\mathcal{O}_{K_1'}\right)^e = \left(\sqrt[\frac{r}{(r,n)}]{F_2(X)^{\frac{n}{(r,n)}}}\sqrt[r]{F_1(X)}\mathcal{O}_{K_1'}\right)^e$$

and we see that $e(\mathfrak{P}'/\mathfrak{P}) = \frac{r}{(r,n)}$.

□

Lemma 2.2.2. *Let $K \subset K' \subset K'(\sqrt[r_1]{F_1(X)}) = K_1' \subset K'(\sqrt[r_1]{F_1(X)}, \sqrt[r_2]{F_2(X)}) = K_2'$ be extensions of fields where $F_1 \in K^*/(K^*)^{r_1}$, $F_2 \in K^*/(K^*)^{r_2}$ and $[K_1' : K'] = r_1, [K_2' : K_1'] = r_2$. Let $\mathfrak{P}$ be a prime in K' and $\mathfrak{P}'$ be a prime in K_2' lying above $\mathfrak{P}$. If $ord_{\mathfrak{P}}(F_1) = n$ and $ord_{\mathfrak{P}}(F_2) = m$, then $e(\mathfrak{P}'/\mathfrak{P}) = lcm\left(\frac{r_1}{(r_1,n)}, \frac{r_2}{(r_2,m)}\right)$*

Proof. Let $\mathfrak{P}''$ be a prime in K_1' such that $\mathfrak{P}'|\mathfrak{P}''|\mathfrak{P}$, then by Lemma 2.2.1, $e(\mathfrak{P}''/\mathfrak{P}) = \frac{r_1}{(r_1,n)}$. Therefore, $\text{ord}_{\mathfrak{P}''}(F_2) = m\frac{r_1}{(r_1,n)}$ and, again by Lemma 2.2.1, $e(\mathfrak{P}'/\mathfrak{P}'') = \frac{r_2}{(r_2, m\frac{r_1}{(r_1,n)})}$. Hence, $e(\mathfrak{P}'/\mathfrak{P}) = \frac{r_1}{(r_1,n)}\frac{r_2}{(r_2,m\frac{r_1}{(r_1,n)})}$. So it remains to show that this is $\text{lcm}\left(\frac{r_1}{(r_1,n)}, \frac{r_2}{(r_2,m)}\right)$.

Let A, B, C be positive integers. We will show that $A\frac{B}{(B,AC)} = \text{lcm}(A, \frac{B}{(B,C)})$. Let $A = \prod p_i^{a_i}$, $B = \prod p_i^{b_i}$, $C = \prod p_i^{c_i}$. Then the left hand and right hand sides are

$$\prod p_i^{a_i+b_i-\min(b_i,a_i+c_i)} \qquad \prod p_i^{\max(a_i,b_i-\min(b_i,c_i))}$$

respectively. If $b_i \leq a_i + c_i$, then the left hand exponent becomes a_i. Moreover, $b_i \leq c_i$ so the right hand exponent would become $\max(a_i, b_i - c_i) = a_i$ as $a_i \geq b_i - c_i$. If $b_i \geq a_i + c_i$ then the left hand exponent becomes $b_i - c_i$. Further, $b_i \geq c_i$ so then the right hand exponent would become $\max(a_i, b_i - c_i) = b_i - c_i$ as $a_i \leq b_i - c_i$. This completes the proof.

□

Let $\mathcal{R}$ and $(f_{\vec{\alpha}})$ be as in Section 2.1.2. That is, the $f_{\vec{\alpha}}$ are monic, squarefree and coprime such that there exists $c_j \in \mathbb{F}_q^*$ such that

$$F_j = c_j \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}, j = 1, \ldots, n$$

Proposition 2.2.3. *If $P|f_{\vec{\alpha}}$ then $e(P) = \underset{j=1,\ldots,n}{lcm}\left(\frac{r_j}{(r_j,\alpha_j)}\right)$*

Proof. If $P|f_{\vec{\alpha}}$ then $\text{ord}_P(F_j) = \alpha_j$ for all j. Thus if we recursively apply Lemma 2.2.2, we get the result.

□

If P_∞ is the prime at infinity, then we see that $\text{ord}_{P_\infty}(F) = \deg(F)$. Therefore, if $\deg(F_j) = d_j$,

$$e(P_\infty) = \underset{j=1,\ldots,n}{\text{lcm}}\left(\frac{r_j}{(r_j, d_j)}\right).$$

Therefore, we can rewrite (2.2.2) as

$$2g + 2|G| - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} \left(|G| - \frac{|G|}{e(\vec{\alpha})} \right) \deg(f_{\vec{\alpha}}) + |G| - \frac{|G|}{e(\vec{d})} \tag{2.2.3}$$

where $\vec{d} = (d_1, \ldots, d_n)$ and for any $\vec{v} = (v_1, \ldots, v_n)$,

$$e(\vec{v}) = \operatorname*{lcm}_{j=1,\ldots,n} \left(\frac{r_j}{(r_j, v_j)} \right)$$

Chapter 3

Cyclic Curves

3.1 Known Results

Theorem 1.2.3 was first proved for hyper-elliptic curves ($G = \mathbb{Z}/2\mathbb{Z}$) by Kurlberg and Rudnick [9]. It was then extended to prime cyclic curves ($G = \mathbb{Z}/p\mathbb{Z}$, p a prime) by Bucur, David, Feigon and Lalin [2],[3]. We will briefly discuss the methods used in [2],[3] so every unreferenced claim stated in this section will be from [2] or [3].

As discussed in Section 2.2 if $\mathrm{Gal}(C) = \mathbb{Z}/p\mathbb{Z}$, then $K(C) = K(\sqrt[p]{F(X)})$ such that $F \in \hat{\mathcal{F}}_{(d_1,\dots,d_{p-1})}$ (as defined in (2.1.6)). An affine model for the curve will be

$$Y^p = F(X).$$

Looking at the affine model we can write the number of affine points on the curve by

$$\#C(\mathbb{F}_q) = \sum_{x\in\mathbb{F}_q}\left(1 + \sum_{i=1}^{p-1}\chi_p^i(F(x))\right)$$

where χ_p is a primitive character on $\mathbb{F}_q^*$ of order p. Such a one exists since we are assuming $q \equiv 1 \pmod{p}$.

The genus formula (2.2.3) becomes

$$2g + 2p - 2 = \begin{cases} (p-1)(d_1 + \cdots + d_{p-1}) & \sum_{i=1}^{p-1} id_i \equiv 0 \pmod{p} \\ (p-1)(d_1 + \cdots + d_{p-1} + 1) & \sum_{i=1}^{p-1} id_i \not\equiv 0 \pmod{p} \end{cases}. \tag{3.1.1}$$

This motivates the definition of the following sets

$$\mathcal{F}^{j}_{(d_1,\dots,d_{p-1})} = \mathcal{F}_{d_1,\dots,d_{j-1},d_j-1,d_{j+1},\dots,d_{p-1}} \tag{3.1.2}$$

$$\mathcal{F}_{[d_1,\dots,d_{p-1}]} = \mathcal{F}_{(d_1,\dots,d_{p-1})} \cup \bigcup_{j=1}^{p-1} \mathcal{F}^{j}_{(d_1,\dots,d_{p-1})}. \tag{3.1.3}$$

Moreover, we let $\hat{\mathcal{F}}^{j}_{(d_1,\dots,d_{p-1})}$ and $\hat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$ to be the corresponding set of polynomials whose leading coefficient is not necessarily 1. Hence if we suppose $\sum_{i=1}^{p-1} id_i \equiv 0 \pmod{p}$, then the genus is invariant under curves with affine models of the form $Y^p = F(X)$ with $F \in \hat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$. Therefore, with $\mathcal{H}_{r,g}$ as defined in (1.2.1), we can write

$$\mathcal{H}_{p,g} = \bigcup_{\substack{2g+2p-2=(p-1)(d_1+\cdots+d_{p-1}) \\ \sum_{i=1}^{p-1} id_i \equiv 0 \pmod{p}}} \mathcal{H}^{(d_1,\dots,d_{p-1})} \tag{3.1.4}$$

where $\mathcal{H}^{(d_1,\dots,d_{p-1})}$ is the set of all curves with affine model coming from $\hat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$.

If we let x_{q+1} denote the point at infinity then for any $F \in \hat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$

$$F(x_{q+1}) = \begin{cases} c & F \in c\mathcal{F}_{(d_1,\dots,d_{p-1})} \\ 0 & F \in \hat{\mathcal{F}}^{j}_{(d_1,\dots,d_{p-1})} \end{cases}.$$

Note that the c above would be the leading coefficient of F. Then with this notation we get that the number of projective points on our curve is

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \left(1 + \sum_{i=1}^{p-1} \chi_p^i(F(x))\right).$$

Therefore, $\#C(\mathbb{P}^1(\mathbb{F}_q))$ will be determine by the value of the character sum

$$S_p(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_p(F(x)).$$

Finally Bucur, Daivd, Feigon and Lalin prove that

Theorem 3.1.1 (Theorem 7.3 of [3]). *If q is fixed and $d_1, \dots, d_{p-1} \to \infty$, then for any $t \in \mathbb{Z}[\zeta_p]$*

$$\frac{|\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} : S_p(F) = t\}|}{|\{\mathcal{H}^{(d_1,\dots,d_{p-1})}\}|} \sim Prob\left(\sum_{i=1}^{q+1} X_i = t\right)$$

where X_i are i.i.d. random variables taking values in $\mu_p \cup \{0\}$ such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{p-1}{q+p-1} \\ \zeta_p^j & \text{with probability } \frac{q}{p(q+p-1)} \end{cases}.$$

Remark 3.1.2. What Bucur, David, Feigon and Lalın actually show is the above result with the curves weighted by $1/|\mathrm{Aut}(C)|$. However, they show that in the prime cyclic case it is the same as the unweighted probability. Their argument relies on the fact that they have a *prime* cyclic curve. That is, the results of this thesis will always be the unweighted probability so we reproduced Bucur, Daivd, Feigon and Lalın's results to better match these results.

The rest of the section will be devoted to proving Theorem 1.2.3. We will do this by following the same approach that was outlined in Section 3.1.

3.2 Moduli Space Decomposition

Let C be a smooth projective curve over $\mathbb{F}_q$ such that $\mathrm{Gal}(C) = \mathbb{Z}/r\mathbb{Z}$. The $K(C) = K(\sqrt[r]{F(X)})$ for some $F \in \hat{\mathcal{F}}_{(d_1,\dots,d_{r-1})}$.

For any $F \in \hat{\mathcal{F}}_{(d_1,\dots,d_{r-1})}$, we can find $f_1, \dots, f_{r-1}$ and $c \in \mathbb{F}_q^*$ such that the f_i are square-free monic, pairwise coprime, $\deg(f_i) = d_i$ and $F = c\prod_{i=1}^{r-1} f_i^i$. Denote $d := \sum_{i=1}^{r-1} id_i = \deg(F)$. Therefore we can rewrite (2.2.3) as

$$2g + 2r - 2 = \sum_{i=1}^{r-1} (r - (r,i))\, d_i + r - (r,d). \tag{3.2.1}$$

This leads us to define the following two sets

$$\mathcal{F}^j_{(d_1,\dots,d_{r-1})} = \mathcal{F}_{(d_1,\dots,d_{j-1},d_j-1,d_{j+1},\dots,d_{r-1})} \tag{3.2.2}$$

$$\mathcal{F}_{[d_1,\dots,d_{r-1}]} = \mathcal{F}_{(d_1,\dots,d_{r-1})} \cup \bigcup_{j=1}^{r-1} \mathcal{F}^j_{(d_1,\dots,d_{r-1})}. \tag{3.2.3}$$

Moreover, we let $\hat{\mathcal{F}}^j_{(d_1,\dots,d_{r-1})}$ and $\hat{\mathcal{F}}_{[d_1,\dots,d_{r-1}]}$ to be the corresponding set of polynomials whose leading coefficient is not necessarily 1.

If we suppose

$$\sum_{i=1}^{r-1} id_i \equiv 0 \pmod{r}, \tag{3.2.4}$$

then (3.2.1) can be simplified to

$$2g + 2r - 2 = \sum_{i=1}^{r-1} (r - (r, i))\, d_i. \tag{3.2.5}$$

Let $d_1, \ldots, d_{r-1}$ be non-negative integers that satisfy (3.2.4) and (3.2.5), and suppose we have a curve, C, with affine model $Y^r = F(X)$ such that $F \in \hat{\mathcal{F}}^j_{(d_1,\ldots,d_{r-1})}$. Write $F = c\prod_{i=1}^{r-1} f_i^i$ then

$$\deg(F) = \sum_{i=1}^{r-1} i \deg(f_i) = \sum_{i=1}^{r-1} id_i - j \equiv -j \pmod{r}$$

and the genus of C, g', would satisfy

$$\begin{aligned} 2g' + 2r - 2 &= \sum_{i=1}^{r-1} (r - (r, i)) \deg(f_i) + r - (r, \deg(F)) \\ &= \sum_{i=1}^{r-1} (r - (r, i))\, d_i - (r - (r, j)) + r - (r, j) \\ &= \sum_{i=1}^{r-1} (r - (r, i))\, d_i \\ &= 2g + 2r - 2. \end{aligned}$$

That is, $g' = g$.

Hence if we suppose $\sum_{i=1}^{r-1} id_i \equiv 0 \pmod{r}$, then the genus is invariant under curves with affine models of the form $Y^r = F(X)$ with $F \in \hat{\mathcal{F}}_{[d_1,\ldots,d_{r-1}]}$. Therefore, we can write

$$\mathcal{H}_{r,g} = \bigcup_{d_1,\ldots,d_{r-1}} \mathcal{H}^{(d_1,\ldots,d_{r-1})}$$

where the union is over all $d_1, \ldots, d_{r-1}$ satisfying (3.2.4) and (3.2.5) and $\mathcal{H}^{(d_1,\ldots,d_{r-1})}$ is the set of all curves with affine model $Y^r = F(X)$ for some $F \in \hat{\mathcal{F}}_{[d_1,\ldots,d_{r-1}]}$.

We will now restrict our attention to only work on curves in $\mathcal{H}^{(d_1,\ldots,d_{r-1})}$ such that $d_1, \ldots, d_{r-1}$ satisfy (3.2.4) and (3.2.5).

3.3 Number of Points on the Curve

Let $C \in \mathcal{H}^{(d_1,\ldots,d_{r-1})}$ such that $d_1, \ldots, d_{r-1}$ satisfy (3.2.4) and (3.2.5) and $F \in \hat{\mathcal{F}}_{[d_1,\ldots,d_{r-1}]}$ such that C has an affine model of the form

$$Y^r = F(X).$$

For any j such that $(j,r)=1$, we define

$$F^{(j)} = c^j \prod_{i=1}^{r-1} f_i^{ij \pmod r}.$$

Note when we write $ij \pmod r$, we mean the smallest non-negative integer congruent to ij modulo r. Then $F^{(1)} = F$, $F^j = F^{(j)}H^r$ for some $H \in \mathbb{F}_q[X]$ and $Y^r = F^{(j)}(X)$ is another affine model for the curve C.

Fix $x \in \mathbb{F}_q$. If $F(x) \neq 0$ then any of the models will be smooth at x. If $F(x) = 0$, then there exists a unique f_i such that $f_i(x) = 0$ since all the f_i are pairwise coprime. Suppose $f_i(x) = 0$ for some i such that $(i,r) = s$ then we can find some j such that $(j,r) = 1$ and $ij \equiv s \pmod r$. Hence $F^{(j)}$ would have a s^{th} root at x and the model $Y^r = F^{(j)}(X)$ would be smooth at x if and only if $s = 1$.

Therefore, without loss of generality, we may assume we have an affine model $Y^r = F(X)$ such that $f_s(x) = 0$ for some $x \in \mathbb{F}_q$ and $s|r$, $s \neq 1$. Moreover, without loss of generality, we may assume $x = 0$. Blowing-up the curve at $(0,0)$, we get the variety defined by

$$(Y^r - cf_1^1(X)f_2^2(X)\dots f_{r-1}^{r-1}(X), Xw - Yz)$$

where w, z are projective coordinates. If $z \neq 0$, then $Y = Xw$ and by writing $f_s(X) = Xf_s'(X)$ we get

$$\begin{aligned} 0 &= (Xw)^r - X^s cf_1(X)f_2^2(X)\dots f_s'^s(X)\dots f_{r-1}^{r-1}(X) \\ &= X^s\left((X^{\frac{r}{s}-1}w^{\frac{r}{s}})^s - cf_1(X)f_2^2(X)\dots f_s'^s(X)\dots f_{r-1}^{r-1}(X)\right). \end{aligned}$$

If we let $Y' = X^{\frac{r}{s}-1}w^{\frac{r}{s}}$, we get the affine model

$$Y'^s = cf_1(X)f_2^2(X)\dots f_s'^s(X)\dots f_{r-1}^{r-1}(X)$$

which is birationally equivalent to

$$Y^s = c\prod_{i=1}^{s-1}\left(\prod_{j=0}^{\frac{r}{s}-1} f_{js+i}(X)\right)^i = c\prod_{i=1}^{r-1}(f_i(X))^{i \pmod s} := F_{(s)}(X).$$

Again, we denote $i \pmod s$ to be the smallest non-negative integer that is congruent to i modulo s. Moreover, we use the convention that $f_i(X)^0$ is identically the constant polynomial

1. Then, with this convention, $F_{(1)}(X)$ is idenitcally the constant polyomial c. Therefore, $f_s(X) \not| F_{(s)}(X)$, hence $F_{(s)}(0) \neq 0$ and the affine model will be smooth at 0. (Note that $F_{(r)}(X) = F(X)$.

This leads to the following lemma

Lemma 3.3.1. *Let $C \in \mathcal{H}^{(d_1,\ldots,d_{r-1})}$ such that $d_1, \ldots, d_{r-1}$ satisfy (3.2.4) and (3.2.5) and $K(C) = K(\sqrt[r]{F(X)})$. Then the number of affine points on C will be*

$$\#C(\mathbb{F}_q) = q + \sum_{s|r} \sum_{\substack{i=1 \\ (i,s)=1}}^{s-1} \sum_{x \in \mathbb{F}_q} \chi_s^i(F_{(s)}(x)).$$

Proof. If x is not a root of any of the f_i, then the smooth affine model at x will be $Y^r = F(X)$ and there will be r points lying over x, if $F(x) = F_{(r)}(x)$ is an r^{th} power and no points otherwise. We can write this as

$$1 + \sum_{i=1}^{r-1} \chi_r(F_{(r)}^i(x)) = 1 + \sum_{s|r} \sum_{\substack{i=1 \\ (i,s)=1}}^{s-1} \chi_s^i(F_{(s)}(x)).$$

If $f_i(x) = 0$ for some $(i, r) = 1$, then the smooth affine model at x will be $Y^r = F^{(j)}(X)$ where j is such that $ij \equiv 1 \pmod{r}$. Then there will be one point lying over x. Further in this case $F_s(x) = 0$ for all $s|r$ so we can write this as

$$1 + \sum_{s|r} \sum_{\substack{i=1 \\ (i,s)=1}}^{s-1} \chi_s^i(F_{(s)}(x)).$$

If $f_i(x) = 0$ for some i such that $(i, r) = s \neq 1$, then we have to look at the smooth model $Y^s = F_{(s)}(X)$. Thus there will be s points lying over x if $F_{(s)}(x)$ is a s^{th} power and no points otherwise. We can write this as

$$1 + \sum_{i=1}^{s} \chi_s(F_{(s)}^i(x)) = 1 + \sum_{s'|s} \sum_{\substack{i=1 \\ (i,s')=1}}^{s'-1} \chi_{s'}^i(F_{(s')}(x)).$$

Further for any $s'|r$ such that $s' \not| s$ we get that the exponent of f_i in $F_{(s')}$ is non-zero. Hence $F_{(s')}(x) = 0$. Therefore, regardless of the behavior at x, the number or points lying above x is

$$1 + \sum_{s|r} \sum_{\substack{i=1 \\ (i,s)=1}}^{s-1} \chi_s^i(F_{(s)}(x)).$$

Summing up over all x, we find that

$$\begin{aligned}\#C(\mathbb{F}_q) &= \sum_{x\in\mathbb{F}_q}\left(1+\sum_{s|r}\sum_{\substack{i=1\\(i,s)=1}}^{s-1}\chi_s^i(F_{(s)}(x))\right)\\ &= q+\sum_{s|r}\sum_{\substack{i=1\\(i,s)=1}}^{s-1}\sum_{x\in\mathbb{F}_q}\chi_s^i(F_{(s)}(x)).\end{aligned}$$

□

Now, let us determine what affine models we need to consider the point at infinity. Let x_{q+1} denote the point at infinity and let $d := \deg(F)$. To discuss what happens at x_{q+1}, we must make a change of variables $X \to 1/X := X'$ and consider what happens when $X' = 0$. Note that

$$F(X) = \left(\frac{1}{X'}\right)^d G(X')$$

where $G(X') = (X')^d F(1/X')$. Therefore, we will consider the affine model

$$(X')^d Y^r = G(X')$$

at $X' = 0$. Note that $G(0) =$ leading coefficient of $F = c \neq 0$.

Let $1 \leq k \leq r$ be such that $d \equiv k \pmod r$. Then if we make the change of variable $Y \to (X')^{\frac{d+r-k}{r}} Y := Y'$, then we get an affine model

$$(Y')^r = (X')^{r-k} G(X').$$

If $k = r$ (and so $r|d$), then we see this affine model will not have a root at 0. Hence the number of points will be determined by whether $G(0) = c$ is an r^{th} power or not. That is, the number of points lying over x_{q+1} in this case can be written as

$$1 + \sum_{i=1}^{r-1} \chi_r^i(c).$$

So if we define $F_{(s)}(x_{q+1}) = c$ for all $s|r$ when $r|d$, then the formula for the number of points lying over x_{q+1} matches the formula for the number of points lying over an affine point.

If $k \neq r$, then find a j such that $(j, r) = 1$ and $(r-k)j \equiv s \pmod r$ where $s = (r, r-k) = (r, d)$. Then, as in the affine case, we get an affine model of the form

$$(Y')^r = (X')^s G^{(j)}(X').$$

If $s = 1$, then the model is smooth and we get there is one point lying over 0, namely $(0, 0)$. Therefore, if we define $F_{(s)}(x_{q+1}) = 0$ for all $s|r$ in this case, then the formula for the number of points lying over x_{q+1} matches the formula for the number of points lying over an affine point.

If $s \neq 1$, then the model is not smooth. Therefore, if we blow-up at the singularity then, as in the affine case, we get a smooth model of the form

$$(Y')^s = G_{(s)}(X').$$

Moreover, $G_{(s)}(0) = c$, so the number of points lying over x_{q+1} can be written

$$1 + \sum_{i=1}^{s-1} \chi_s(c).$$

Therefore, if we define $F_{(s')}(x_{q+1}) = c$ for all $s'|s$ and $F_{(s')}(x_{q+1}) = 0$ for all $s' \nmid s$, then the formula for the number of points lying over x_{q+1} matches the formula for the number of points lying over an affine point.

Therefore, we have defined

$$F_{(s)}(x_{q+1}) = \begin{cases} c & \text{if } s|(\deg(F), r) \\ 0 & \text{otherwise} \end{cases}.$$

However, since $F \in \hat{\mathcal{F}}_{[d_1,\ldots,d_{r-1}]}$, such that $d_1, \ldots, d_{r-1}$ satisfy (3.2.4) and (3.2.5) we see that $s|(\deg(F), r)$ if and only if $F \in \hat{\mathcal{F}}^{sj}_{(d_1,\ldots,d_{r_1})}$ for some $0 \leq j \leq \frac{r}{s} - 1$ where we use the convention $\hat{\mathcal{F}}^0_{(d_1,\ldots,d_{r-1})} = \hat{\mathcal{F}}_{(d_1,\ldots,d_{r-1})}$. Therefore,

$$F_{(s)}(x_{q+1}) = \begin{cases} c & \text{if } F \in c\mathcal{F}^{sj}_{(d_1,\ldots,d_{r-1})}, j = 0, \ldots, \frac{r}{s} - 1 \\ 0 & \text{otherwise} \end{cases}. \tag{3.3.1}$$

Hence, we get the following lemma for the number of projective points.

Lemma 3.3.2. *Let $C \in \mathcal{H}^{(d_1,\ldots,d_{r-1})}$ such that $d_1, \ldots, d_{r-1}$ satisfies (3.2.4) and (3.2.5) and $K(C) = K\left(\sqrt[r]{F(X)}\right)$ then the number of projective points on C will be*

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 + \sum_{s|r} \sum_{\substack{i=1 \\ (i,s)=1}}^{s-1} \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_s^i(F_{(s)}(x)).$$

For all $s|r$, define

$$S_s(F_{(s)}) := \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_s(F_{(s)}(x)).$$

Then knowing the value of $S_s(F_{(s)})$ for all $s|r$, is enough to determine $\#C(\mathbb{P}^1(\mathbb{F}_q))$. Indeed

$$\sum_{\substack{i=1\\(i,s)=1}}^{s-1} \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_s^i(F_{(s)}(x)) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \sum_{\substack{i=1\\(i,s)=1}}^{s-1} \chi_s^i(F_{(s)}(x))$$

$$= \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \mathrm{Tr}_s\left(\chi_s^i(F_{(s)}(x))\right) = \mathrm{Tr}_s\left(S_s(F_{(s)})\right)$$

where Tr_s is the trace function for the field extension $\mathbb{Q}(\zeta_s)/\mathbb{Q}$.

3.4 Prime Power Cyclic Curves

In this section we will prove Theorem 1.2.3 when $G = \mathbb{Z}/p^n\mathbb{Z}$ for p a prime. It is not absolutely necessary to do this before doing the general cyclic case however we include this section to introduce the reader to the notation that will be used as it is simpler for prime power cyclic curves.

The results of Section 3.3 shows that it is enough to determine the number of polynomials $\hat{\mathcal{F}}_{[d_1,\ldots,d_{p^n-1}]}$ such that $S_{p^j}(F_{(p^j)})$ takes on prescribed values for $j = 1,\ldots,n$. To do this we will determine the number of polynomials $\hat{\mathcal{F}}_{[d_1,\ldots,d_{p^n-1}]}$ such that $\chi_{p^j}(F_{(p^j)}(x))$ takes prescribed values for all $x \in \mathbb{P}^1(\mathbb{F}_q)$ and $j = 1,\ldots,n$.

For the rest of this section, we will assume $F \in \hat{\mathcal{F}}_{[d_1,\ldots,d_{p^n-1}]}$, $c \in \mathbb{F}_q^*$ and f_i, $i = 1,\ldots,p^n-1$, be the square-free coprime polynomials such that $F = c\prod_{i=1}^{p^n-1} f_i^i$.

In order to apply the counting formula of Proposition 2.1.12 we want to write the n polynomials defined by

$$F_{(p^j)}(X) = c\prod_{i=1}^{p^n-1} f_i^{i \pmod{p^j}} \quad 1 \le j \le n$$

in terms of coprime polynomials.

To apply the results of Section 2.1.2 we define,

$$\mathcal{R} = [0,\ldots,p-1]^n \setminus \{(0,\ldots,0)\}.$$

If $\vec{\alpha} \in \mathcal{R}$ we will denote it $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Define a bijection

$$\begin{aligned} \phi : \mathcal{R} &\to [1, \ldots, p^n - 1] \\ \vec{\alpha} &\to \alpha_1 + p\alpha_2 + \cdots + p^{n-1}\alpha_n. \end{aligned}$$

For all $\vec{\alpha}$ define $f_{\vec{\alpha}} = f_{\phi(\vec{\alpha})}$. Then, we can rewrite

$$F(X) = c \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_1 + p\alpha_2 + \cdots + p^{n-1}\alpha_n}.$$

Let $\vec{d}(\vec{\alpha})$ be a vector of non-negative integers indexed by the elements of $\vec{\alpha}$. Define the sets

$$\begin{aligned} \mathcal{F}_{\vec{d}(\vec{\alpha})} &= \{(f_{\vec{\alpha}}) \in \prod_{\vec{\alpha} \in \mathcal{R}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1, \vec{\alpha} \neq \vec{\beta} \in \mathcal{R}\} \\ \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} &= \{(c, (f_{\vec{\alpha}})) \in \mathbb{F}_q^* \times \mathcal{F}_{\vec{d}(\vec{\alpha})}\} \\ \mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} &= \{(f_{\vec{\beta}}, (f_{\vec{\alpha}})) \in \mathcal{F}_{d(\vec{\beta})-1} \times \prod_{\substack{\vec{\alpha} \in \mathcal{R} \\ \vec{\alpha} \neq \vec{\beta}}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\gamma}}) = 1, \vec{\alpha} \neq \vec{\gamma} \in \mathcal{R}\} \\ \hat{\mathcal{F}}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} &= \{(c, (f_{\vec{\alpha}})) \in \mathbb{F}_q^* \times \mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})}\} \\ \mathcal{F}_{[\vec{d}(\vec{\alpha})]} &= \mathcal{F}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} \\ \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} &= \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \hat{\mathcal{F}}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})}. \end{aligned}$$

Then, ϕ induces an bijection from $\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ to $\hat{\mathcal{F}}_{[d_1, \ldots, d_{p^n-1}]}$. With this new notation we get (3.2.4) and (3.2.5) becomes

$$\sum_{\vec{\alpha} \in \mathcal{R}} \phi(\vec{\alpha}) d(\vec{\alpha}) \equiv 0 \pmod{p^n} \tag{3.4.1}$$

$$2g + 2p^n - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} \left(p^n - (p^n, \phi(\vec{\alpha}))\right) d(\vec{\alpha}). \tag{3.4.2}$$

Moreover, if we identify $\mathcal{H}^{(d_1, \ldots, d_{p^n-1})}$ with $\mathcal{H}^{\vec{d}(\vec{\alpha})}$ in the natural way then we can write

$$\mathcal{H}_{r,g} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{H}^{\vec{d}(\vec{\alpha})}$$

where the union is over all $\vec{d}(\vec{\alpha})$ that satisfy (3.4.1) and (3.4.2).

Furthermore,

$$F_{(p^j)}(X) = c \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\alpha_1 + p\alpha_2 + \cdots + p^{j-1}\alpha_j}$$

for $j = 1, \ldots, n$. Recall, we use the convention $F_{(1)}(X) = 1$.

With this new notation we get that for $x \neq x_{q+1}$, $F_{(p^m)}(x) = 0$ if and only if $f_{\vec{\beta}}(x) = 0$ for some $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in \mathcal{R}$ such that $\beta_i \neq 0$ for some $i \leq j$.

If $x = x_{q+1}$, the point at infinity, then we can rewrite (3.3.1),

$$F_{(p^j)}(x_{q+1}) = \begin{cases} c & (f_{\vec{\alpha}}) \in \mathcal{F}^{\beta}_{\vec{d}(\vec{\alpha})} \\ 0 & \text{otherwise} \end{cases}$$

where $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in \mathcal{R}$ is any tuple such that $\beta_i = 0$ for all $i \leq j$.

We begin by determining the size of

$$|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha}))} : F_{(p^j)}(x_i) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \tag{3.4.3}$$

for some $a_{i,j} \in \mathbb{F}_q^*$. As in the statement of Proposition 2.1.12, define $F_j := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$, for $j = 1, \ldots, n$, then we see we have the relationship

$$F_{(p^j)} = F_{(p^{j-1})} F_j^{p^{j-1}}. \tag{3.4.4}$$

For (3.4.3) to be non-empty, we need $a_{i,j} = a_{i,j-1}(b_{i,j})^{p^{j-1}}$ for some $b_{i,j} \in \mathbb{F}_q^*$ where we let $a_{i,0} = 1$ so that $a_{i,1} = b_{i,1}$. In fact, this is the only condition we need.

Lemma 3.4.1. *Let $a_{i,j} \in \mathbb{F}_q^*$, $1 \leq i \leq \ell, 1 \leq j \leq n$ such that $a_{i,j} = a_{i,j-1}(b_{i,j})^{p^{j-1}}$ for some $b_{i,j} \in \mathbb{F}_q^*$. We let $a_{i,0} = 1$ so that $a_{i,1} = b_{i,1}$. Then*

$$\begin{aligned} &|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha}))} : F_{(p^j)}(x_i) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| \\ &= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} \vec{d}(\vec{\alpha})}}{\zeta_q(2) p^{n-1}} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q + p^n - 1)} \right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}{2}} \right) \right). \end{aligned}$$

Proof. Since $F_{(p^j)} = F_{(p^{j-1})} F_j^{p^{j-1}}$ then $F_{(p^j)}(x_i) = a_{i,j}$ for all i, j is equivalent to $F_j(x_i) = \epsilon_{i,j} b_{i,j}$ for all i, j for some $\epsilon_{i,j} \in \mu_{p^{j-1}}$. Hence,

$$
\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p^j)}(x_i) = a_{i,j}, 1 \le i \le \ell, 1 \le j \le n\}| \\
&= \sum_{\substack{\epsilon_{i,j} \in \mu_{p^j-1} \\ 1 \le i \le \ell \\ 1 \le j \le \ell}} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) = \epsilon_{i,j} b_{i,j}, , 1 \le j \le n, 1 \le i \le \ell\}| \\
&= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q+p^n-1)} \right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}}\right)\right).
\end{aligned}
$$

Where the second equality comes from Proposition 2.1.12 and that there are $(p^{\frac{n(n-1)}{2}})^{\ell}$ different choices for the $\epsilon_{i,j}$.

□

Next we want to determine the size of (3.4.3) where we let some of the $a_{i,j} = 0$. Since $F_{(p^j)} | F_{(p^{j+1})}$, we see that $a_{i,j} = 0$ implies that $a_{i,j+1} = 0$. However, we may have that $a_{i,j+1} = 0$ but $a_{i,j} \neq 0$. Moreover, as above, if $a_{i,j}, a_{i,j+1} \neq 0$, then there exists a $b_{i,j+1}$ such that $a_{i,j+1} = a_{i,j}(b_{i,j+1})^{p^j}$. This motivates the following definition.

Definition 3.4.2. A set of elements $\{a_1, \dots, a_n\} \in \mathbb{F}_q$ are said to be k-**admissible** if there exists $b_1, \dots, b_k \in \mathbb{F}_q^*$ such that

$$a_1, \dots, a_k \neq 0, a_{k+1}, \dots, a_n = 0$$

$$a_j = a_{j-1}(b_j)^{p^{j-1}}, j = 1, \dots, k$$

where we set $a_0 = 1$.

Therefore, for $1 \le i \le \ell$, we need $\{a_{i,1}, \dots, a_{i,n}\}$ to be k-admissible for some k. Moreover, if $\{a_{i,1}, \dots, a_{i,n}\}$ is n-admissible, then $a_{i,j} \neq 0$ for $j = 1, \dots, n$.

Proposition 3.4.3. *Let $a_{i,j} \in \mathbb{F}_q$, $1 \le j \le n, 1 \le i \le \ell$ such that for all i, the set $\{a_{i,1}, \dots, a_{i,n}\}$ is k-admissible for some k. Let*

$$m_k = \#\{1 \le i \le \ell : \{a_{i,1}, \dots, a_{i,n}\} \text{ is } k\text{-admissible}\}$$

for $k = 0, \dots, n$. Then $\sum m_k = \ell$ and

$$|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p^j)}(x_i) = a_{i,j}, 1 \le j \le n, 1 \le i \le \ell\}|$$

$$= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2) p^{n^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2+\frac{(k-1)(k-2)}{2}}}{(q-1)^k(q+p^n-1)} \right)^{m_k}$$
$$\times \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n(q+p^n-1)} \right)^{m_n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right).$$

Proof. For $k = 1, \ldots, n$, let

$$M_k = \{1 \leq i \leq \ell : \{a_{i,1}, \ldots, a_{i,n}\} \text{ is } k\text{-admissible}\}.$$

Then $m_k = |M_k|$. Consider $i \in M_k$. Then $f_{\vec{\alpha}}(x_i) = 0$ for some $\vec{\alpha}$ such that $\alpha_{k+1} \neq 0$ but $\alpha_j = 0$ for all $j < k+1$. There are $(p-1)p^{n-k-1}$ different such $\vec{\alpha}$. For all such $\vec{\alpha}$, let

$$M_{k,\vec{\alpha}} = \{i \in M_k : f_{\vec{\alpha}}(x_i) = 0\}.$$

Define $m_{k,\vec{\alpha}} = |M_{k,\vec{\alpha}}|$. Then $M_k = \cup M_{k,\vec{\alpha}}$ and $m_k = \sum m_{k,\vec{\alpha}}$.

Define $g_{\vec{\alpha}}(X)$ to be the polynomials such that

$$f_{\vec{\alpha}}(X) = g_{\vec{\alpha}}(X) \prod_{i \in M_{k,\vec{\alpha}}} (X - x_i)$$

and let $G_{(p^j)}(X)$ be the corresponding products of the $g_{\vec{\alpha}}$. Notice that $\deg(g_{\vec{\alpha}}) = \deg(f_{\vec{\alpha}}) - m_{k,\vec{\alpha}}$. If we denote $\deg(f_{\vec{\alpha}}) = d(\vec{\alpha})$, define

$$\vec{d'}(\vec{\alpha}) = (d(\vec{\alpha}) - m_{k,\vec{\alpha}})_{\vec{\alpha}\in\mathcal{R}}$$

If $i \in M_k$, then $F_{(p^j)}(x_i) \neq 0$ for all $j \leq k$. Hence if $f_{\vec{\alpha}}(X) | F_{(p^j)}(X)$ then $f_{\vec{\alpha}}(x_i) \neq 0$. Therefore, we can find an $H_{i,j}$ such that $H_{i,j}(x_i) \neq 0$ and

$$F_{(p^j)}(X) = G_{(p^j)}(X) H_{i,j}(X).$$

Moreover, this $H_{i,j}$ will be uniquely determined by the $M_{k,\vec{\alpha}}$. Therefore if $i \in M_k$, the value of $G_{(p^j)}(x_i)$ will be uniquely determined by $F_{(p^j)}(x_i)$ and $M_{k,\vec{\alpha}}$.

Moreover, if $i \in M_k$ then for all $j > k$, $F_{(p^j)}(x_i) = 0$ but $G_{(p^j)}(x_i) \neq 0$. However, by the same reasoning as in (3.4.4) there exists an $H(X)$ such that

$$G_{(p^j)}(X) = G_{(p^k)}(X) \left(H(X)\right)^{p^{j-1}}$$

That is $G_{(p^j)}(x_i)$ will be determined, up to a p^{j-1} root of unity.

Hence, we can conclude that if $i \in M_k$ there are

$$\left(\prod_{j=k+1}^{n} \frac{q-1}{p^{j-1}}\right)^{m_k} = \left(\frac{(q-1)^{n-k}}{p^{\frac{(n-k)(n+k-1)}{2}}}\right)^{m_k}.$$

different choices for $G_{(p^j)}(x_i)$ for $j = 1, \ldots, n$.

Applying this, we obtain

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p^j)}(x_i) = a_{i,j}, 0 \le j \le n, 1 \le i \le \ell\}| \\
=&\sum_{M_{k,\vec{\alpha}}} \sum_{b_{i,j}} |\{(g_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}'(\vec{\alpha})} : G_{(p^j)}(x_i) = b_{i,j}, 0 \le j \le n, 1 \le i \le \ell\}|
\end{aligned}$$

where the first sum is over all partitions of $M_k = \cup M_{k,\vec{\alpha}}$ and the second sum is over all possible choices $b_{i,j} \in \mathbb{F}_q^*$ such that $G_{(p^j)}(x_i) = b_{i,j}$, $1 \le i \le \ell, 1 \le j \le n$. Therefore, by Lemma 3.4.1, the above is equal to

$$\begin{aligned}
&\sum_{M_{k,\vec{\alpha}}} \sum_{b_{i,j}} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha}\in\mathcal{R}}(d(\vec{\alpha})-m_{k,\vec{\alpha}})}}{\zeta_q(2)p^{n-1}} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n(q+p^n-1)}\right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right) \\
=&\prod_{k=0}^{n-1} \left((p-1)p^{n-k-1}\right)^{m_k} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha}) - \sum_{k=0}^{n-1} m_k}}{\zeta_q(2)p^{n-1}} \prod_{k=0}^{n-1} \left(\frac{(q-1)^{n-k}}{p^{\frac{(n-k)(n+k-1)}{2}}}\right)^{m_k} \\
&\times \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n(q+p^n-1)}\right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right) \\
=&\frac{L_{p^n-2} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)p^{n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2+\frac{(k-1)(k-2)}{2}}}{(q-1)^k(q+p^n-1)}\right)^{m_k} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n(q+p^n-1)}\right)^{m_n} \\
&\times \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right).
\end{aligned}$$

□

Finally, we want to determine the size of the set

$$\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \le j \le n, 1 \le i \le \ell\}. \tag{3.4.5}$$

Likewise we will define what it means for a set of p^nth roots of unity to be k-admissible.

Definition 3.4.4. A set $\{\epsilon_1, \ldots, \epsilon_n\} \in \mu_{p^n} \cup \{0\}$ is said to be k-**admissible** if

$$\epsilon_1, \ldots, \epsilon_k \neq 0, \epsilon_{k+1}, \ldots, \epsilon_n = 0$$

$$\epsilon_{j-1} = (\epsilon_j)^p, j = 1, \dots, k$$

where we set $\epsilon_0 = 1$.

Then, for each i, the set $\{\epsilon_{i,1}, \dots, \epsilon_{i,n}\}$ must be k-admissible for some k.

Corollary 3.4.5. *Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \le i \le \ell, 1 \le j \le n$ such that for all i, the set $\{\epsilon_{i,1}, \dots, \epsilon_{i,n}\}$ is k-admissible for some k. Let*

$$m_k = \#\{1 \le i \le \ell : \{\epsilon_{i,1}, \dots, \epsilon_{i,n}\} \text{ is } k\text{-admissible}\}$$

for $k = 0, \dots, n$. Then $\sum m_k = \ell$ and

$$|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \le j \le n, 1 \le i \le \ell\}|$$

$$= \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2) p^{n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q + p^n - 1} \right)^{m_k} \left(\frac{q}{p^n(q + p^n - 1)} \right)^{m_n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).$$

Proof. Let M_k be as in the proof of Proposition 3.4.3. Then $F_{(p^j)}(x_i)$ will be zero if and only if $i \in M_k$ for $k = 1, \dots, j-1$ and will have $\frac{q-1}{p^j}$ choices if $i \in M_k$ for $k \ge j$. Therefore there are

$$\prod_{j=1}^{n} \left(\frac{q-1}{p^j} \right)^{\sum_{k=j}^{n} m_k}$$

choices for the the $F_{(p^j)}(x_i)$, $i = 1, \dots, \ell$, $j = 1, \dots, n$.

Hence,

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \le j \le n, 1 \le i \le \ell\}| \\
=&\prod_{j=1}^{n} \left(\frac{q-1}{p^j} \right)^{\sum_{k=j}^{n} m_k} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2) p^{n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2+\frac{(k-1)(k-2)}{2}}}{(q-1)^k (q + p^n - 1)} \right)^{m_k} \left(\frac{p^{\frac{n(n-1)}{2}} q}{(q-1)^n (q + p^n - 1)} \right)^{m_n} \\
&\times \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right) \\
=&\frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2) p^{n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q + p^n - 1} \right)^{m_k} \left(\frac{q}{p^n(q + p^n - 1)} \right)^{m_n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).
\end{aligned}$$

□

Up until now, we have been looking only at points in $\mathbb{F}_q$. What we need to look at however, is points in $\mathbb{P}^1(\mathbb{F}_q)$. We do this by looking at polynomials in $\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ instead.

Corollary 3.4.6. *Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \leq j \leq n, 1 \leq i \leq q+1$ such that the set $\{\epsilon_{i,1}, \ldots, \epsilon_{i,n}\}$ is k-admissible for some k. Let*

$$m_k = \#\{1 \leq i \leq q+1 : \{\epsilon_{i,1}, \ldots, \epsilon_{i,n}\} \text{ is } k\text{-admissible}\}$$

for $k = 0, \ldots, n$. Then $\sum m_k = q+1$

$$\frac{|\{(c, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q+1\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q+p^n-1} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^{m_n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).$$

Proof. **Case 1:** $\{\epsilon_{q+1,1}, \ldots, \epsilon_{q+1,n}\}$ is n-admissible.

In this case we get that $(c, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$ such that $\chi_{p^n}(c) = \epsilon_{q+1,n}$. Hence there are $\frac{q-1}{p^n}$ choices for c and

$$|\{(c, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q+1\}|$$

$$= \frac{q-1}{p^n} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q\}|$$

$$= \frac{q-1}{p^n} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q+p^n-1} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^{m_n-1}$$

$$= \frac{(q-1)(q+p^n-1)}{q} \frac{L_{p^n-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q+p^n-1} \right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)} \right)^{m_n}.$$

Case 2: $\{\epsilon_{q+1,1}, \ldots, \epsilon_{q+1,n}\}$ is k-admissible for some $k \neq n$.

In this case we get $(c, f_{\vec{\alpha}}) \in \hat{\mathcal{F}}^{\vec{\beta}}_{(d(\vec{\alpha}))}$ where $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in \mathcal{R}$ such that $\beta_j = 0$ for all $j \leq k$ and $\beta_{k+1} \neq 0$ and $\chi_{p^k}(c) = \epsilon_{q+1,k}$. There are $(p-1)p^{n-k-1}$ such $\vec{\beta}$. Further m_k will go to $m_k - 1$ and there are $\frac{q-1}{p^k}$ choices for c. Then,

$$
\begin{aligned}
&|\{(c,(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \le j \le n, 1 \le i \le q+1\}| \\
=&\frac{q-1}{p^k}\sum_{\vec{\beta}} |\{(f_{\vec{\alpha}}) \in \mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} : \chi_{p^j}(F_{(p^j)}(x_i)) = \epsilon_{i,j}, 1 \le j \le n, 1 \le i \le q\}| \\
=&\frac{q-1}{p^k}(p-1)p^{n-k-1}\frac{L_{p^n-2}q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})-1}}{\zeta_q(2)^{p^n-1}}\prod_{j=0}^{n-1}\left(\frac{(p-1)p^{n-2j-1}}{q+p^n-1}\right)^{m_j} \\
&\times\left(\frac{(p-1)p^{n-2k-1}}{q+p^n-1}\right)^{-1}\left(\frac{q}{p^n(q+p^n-1)}\right)^{m_n}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right) \\
=&\frac{(q-1)(q+p^n-1)}{q}\frac{L_{p^n-2}q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{p^n-1}}\prod_{j=0}^{n-1}\left(\frac{(p-1)p^{n-2j-1}}{q+p^n-1}\right)^{m_j} \\
&\times\left(\frac{q}{p^n(q+p^n-1)}\right)^{m_n}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right).
\end{aligned}
$$

Thus, independent of the behavior at x_{q+1}, we get our result.

□

Which leads us to restate and prove Theorem 1.2.3 for $r = p^n$.

Theorem 3.4.7. *Let $M_j \in \mathbb{Z}[\zeta_{p^j}]$ for $j = 1, \dots, n$. Then*

$$
\frac{|\{C \in \mathcal{H}^{\vec{d}(\vec{\alpha})} : S_{p^j}(F_{(p^j)}) = M_j, 1 \le j \le n\}|}{|\mathcal{H}^{\vec{d}(\vec{\alpha})}|}
$$

$$
= Prob\left(\sum_i X_{i,1} = M_1 \text{ and } \dots \text{ and } \sum_i X_{i,n} = M_n\right)\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right)
$$

where the $X_{i,j}$ are random variables that take values in $\mu_{p^j} \cup \{0\}$ such that $X_{i,j}$ and $X_{h,k}$ are independent unless $i = h$ and

$$
Prob(X_{i,j} = 0) = \frac{p^n - p^{n-j}}{q+p^n-1} \qquad Prob(X_{i,j} = \epsilon_{i,j}) = \frac{q+p^{n-j}-1}{p^j(q+p^n-1)}
$$

$$
Prob(X_{i,j+1} = 0 | X_{i,j} = 0) = 1 \qquad Prob(X_{i,j-1} = (X_{i,j})^p | X_{i,j} \neq 0) = 1
$$

$$
Prob(X_{i,1} = \epsilon_{i,1}, \dots, X_{i,j} = \epsilon_{i,j} \text{ and } X_{i,j+1}, \dots, X_{i,n} = 0) = \begin{cases} \frac{(p-1)p^{n-2j-1}}{q+p^n-1} & \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \dots, j \\ 0 & \text{otherwise} \end{cases}
$$

$$
Prob(X_{i,1} = \epsilon_{i,1}, \dots, X_{i,n} = \epsilon_{i,n}) = \begin{cases} \frac{q}{p^n(q+p^n-1)} & \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \dots, n \\ 0 & \text{otherwise} \end{cases}
$$

Proof.

$$\frac{|\{C \in \mathcal{H}^{\vec{d}(\vec{\alpha})} : S_{p^j}(F_{(p^j)}) = M_j, 1 \le j \le n\}|}{|\mathcal{H}^{\vec{d}(\vec{\alpha})}|}$$

$$= \frac{|\{(c,(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : S_{p^j}(F_{(p^j)}) = M_j, 1 \le j \le n\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \sum_{\substack{(E_{1,j},\dots,E_{q+1,j}) \in \mu_{p^j} \cup \{0\} \\ \sum_i E_{i,j} = M_j \\ E_{i,j}=0 \implies E_{i,j+1}=0 \\ E_{i,j}\neq 0 \implies E_{i,j-1}=(E_{i,j})^p \\ j=1,\dots,n}} \prod_{k=0}^{n-1} \left(\frac{(p-1)p^{n-2k-1}}{q+p^n-1}\right)^{m_k} \left(\frac{q}{p^n(q+p^n-1)}\right)^{m_n} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right)$$

$$= \text{Prob}\left(\sum_i X_{i,1} = M_1 \text{ and } \dots \text{ and } \sum_i X_{i,n} = M_n\right)\left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right)$$

where the X_i have the desired conditional properties.

Now,

$$\text{Prob}(X_{i,j} = 0) = \sum_{k=1}^{j-1} \sum_{\epsilon_{i,k} \in \mu_{p^k}} \text{Prob}(X_{i,1} = \epsilon_{i,k}^{p^{k-1}}, \dots, X_{i,k} = \epsilon_{i,k}, X_{i,k+1} = \cdots = X_{i,n} = 0)$$

$$= \sum_{k=1}^{j-1} p^k \frac{(p-1)p^{n-2k-1}}{q+p^n-1} = \frac{p^n - p^{n-j}}{q+p^n-1}.$$

Since the conditional probabilities are independent of the choices of the $\epsilon_{i,j}$'s, $\text{Prob}(X_{i,j} = \epsilon_{i,j})$ will be independent of the choice of $\epsilon_{i,j}$. Therefore,

$$\text{Prob}(X_{i,j} = \epsilon_{i,j}) = \frac{1}{p^j}(1 - \text{Prob}(X_{i,j} = 0)) = \frac{q + p^{n-j} - 1}{p^j(q+p^n-1)}.$$

□

3.5 General Cyclic Curves

In this section we will prove the full Theorem 1.2.3. As in the Section 3.4 it will be enough to determine the number of $F \in \hat{\mathcal{F}}_{[d_1,\dots,d_{r-1}]}$ that have a prescribed value of $S_s(F_{(s)})$ for all $s|r$. We will use the same methods of Section 3.4 to write the $F_{(s)}$ as products of square-free coprime polynomials and then apply the results of Section 2.1. But first, we show that we do not need to look at *all* divisors of s, just the prime power divisors.

Let $c \in \mathbb{F}_q^*$ and $f_1, \ldots, f_{r-1}$ be square-free coprime polynomials such that $F = \prod_{i=1}^{r-1} f_i^i$. Suppose that $r = s_1 s_2$ with $(s_1, s_2) = 1$. Let $m_1 \equiv s_1^{-1} \pmod{s_2}$ and $m_2 \equiv s_2^{-2} \pmod{s_1}$, then we can define an bijection

$$\begin{aligned} \phi : \quad [0, \ldots, s_1 - 1] \times [0, \ldots, s_2 - 1] &\to [0, \ldots, r-1] \\ (i, j) &\to m_2 s_2 i + m_1 s_1 j \pmod{r} \end{aligned}$$

where as usual when we write $* \pmod{r}$, we mean the smallest, non-negative integer that is congruent to $*$ modulo r. Then if we define $f_{i,j} = f_{\phi(i,j)}$, then we can write

$$F(X) = \prod_{\substack{i=0,\ldots,s_1-1 \\ j=0,\ldots,s_2-1 \\ (i,j)\neq(0,0)}} f_{i,j}(X)^{m_2 s_2 i + m_1 s_1 j \pmod{r}}.$$

With this notation, we then have

$$F_{(s_1)} = \prod_{\substack{i=0,\ldots,s_1-1 \\ j=0,\ldots,s_2-1 \\ (i,j)\neq(0,0)}} f_{i,j}^{i \pmod{s_1}} \qquad F_{(s_2)} = \prod_{\substack{i=0,\ldots,s_1-1 \\ j=0,\ldots,s_2-1 \\ (i,j)\neq(0,0)}} f_{i,j}^{j \pmod{s_2}}.$$

Therefore

$$F_{(s_1)}(X)^{m_2 s_2} F_{(s_2)}(X)^{m_1 s_1} = F(X) \left(\prod_{i,j} f_{i,j}(X)^{n_{i,j}} \right)^r$$

for some, potentially 0, exponents $n_{i,j}$.

Since, if $F(x) \neq 0$, then $f_{i,j}(x) \neq 0$ for all (i, j), we get

$$\begin{aligned} \chi_r(F(x)) &= \chi_r \left(F(x) \left(\prod_{i,j} f_{i,j}(x)^{n_{i,j}} \right)^r \right) \\ &= \chi_r \left(F_{(s_1)}(x)^{m_2 s_2} F_{(s_2)}(x)^{m_1 s_1} \right) \\ &= \chi_{s_1}^{m_2}(F_{(s_1)}(x)) \chi_{s_2}^{m_1}(F_{(s_2)}(x)). \end{aligned}$$

Further, if $F(x) = 0$, then at least one of $F_{(s_1)}(x) = 0$ or $F_{(s_2)}(x) = 0$ as all the polynomials that divide $F(X)$ divides either $F_{(s_1)}(X)$ or $F_{(s_2)}(X)$. Therefore, trivially in this case we get

$$\chi_r(F(x)) = \chi_{s_1}^{m_2}(F_{(s_1)}(x)) \chi_{s_2}^{m_1}(F_{(s_2)}(x)).$$

Therefore, the value of $\chi_r(F(x))$ will be uniquely determined by the values of $\chi_{s_1}(F_{(s_1)}(x))$ and $\chi_{s_2}(F_{(s_2)}(x))$. Hence the values of $\chi_s(F_{(s)}(x))$ for all $s|r$ are determined by the values of $\chi_{p^n}(F_{(p^n)}(x))$ where p is a prime such that $p^n | r$. That is,

$$|\{F \in \mathcal{F}_{(d_1,\ldots,d_r)} : \chi_s(F_{(s)}(x_i)) = \epsilon_{s,i}, \text{ for all } s|r, 1 \leq i \leq \ell\}|$$

$$= |\{F \in \mathcal{F}_{(d_1,\ldots,d_r)} : \chi_s(F_{(s)}(x_i)) = \epsilon_{s,i}, s = p^n | r, p \text{ a prime}, 1 \le i \le \ell\}|.$$

Now, suppose $r = p_1^{t_1} \cdots p_n^{t_n}$. Define

$$\mathcal{R}^* = [0, \ldots, p_1^{t_1} - 1] \times \cdots \times [0, \ldots, p_n^{t_n} - 1] \setminus \{(0, \ldots, 0)\}.$$

Write $\vec{\beta} \in \mathcal{R}^*$ as $\vec{\beta} = (\beta_1, \ldots, \beta_n)$.

Let

$$\phi : \mathcal{R}^* \to [1, \ldots, r-1]$$

be the bijection that comes from the Chinese Remainder Theorem. Define $f_{\vec{\beta}} = f_{\phi(\vec{\beta})}$, then

$$F = \prod_{\vec{\beta} \in \mathcal{R}^*} f_{\vec{\beta}}^{\phi(\vec{\beta})}.$$

Notice that $\phi(\vec{\beta}) \equiv k \pmod{p_j^{t_j}}$ if and only if $\beta_j = k$. Therefore

$$F_{(p_j^{t_j})} = \prod_{\vec{\beta} \in \mathcal{R}^*} f_{\vec{\beta}}^{\phi(\vec{\beta}) \pmod{p_j^{t_j}}} = \prod_{k=0}^{p_j^{t_j}-1} \prod_{\substack{\beta \in \mathcal{R}^* \\ \beta_j = k}} f_{\vec{\beta}}^{k} = \prod_{\vec{\beta} \in \mathcal{R}^*} f_{\vec{\beta}}^{\beta_j}.$$

However, we need all powers of the primes. Therefore we define

$$\mathcal{R} = [0, \ldots, p_1 - 1]^{t_1} \times \cdots \times [0, \ldots, p_n - 1]^{t_n} \setminus \{(0, \ldots, 0)\}.$$

Let $T_j = \sum_{i=1}^{j} t_i$. As usual, for $\vec{\alpha} \in \mathcal{R}$ we write it as $\vec{\alpha} = (\alpha_1, \ldots, \alpha_{T_n})$. Then there is a bijection $\psi : \mathcal{R} \to \mathcal{R}^*$ such that

$$\psi(\vec{\alpha}) = (\alpha_1 + p_1\alpha_2 + \cdots + p_1^{t_1-1}\alpha_{T_1}, \ldots, \alpha_{T_{n-1}+1} + p_n\alpha_{T_{n-1}+2} + \cdots + p_n^{t_n-1}\alpha_{T_n}).$$

For all $\vec{\alpha} \in \mathcal{R}$, if we define $f_{\vec{\alpha}} = f_{\psi(\vec{\alpha})}$, then we can write

$$F_{(p_j^{t_j})}(X) = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\alpha_{T_{j-1}+1} + p\alpha_{T_{j-1}+2} + \ldots p^{t_j-1}\alpha_{T_j}}.$$

Moreover, for any $1 \le k_j \le t_j$

$$F_{(p_j^{k_j})}(X) = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\alpha_{T_{j-1}+1} + p\alpha_{T_{j-1}+2} + \ldots p^{k_j-1}\alpha_{T_{j-1}+k_j}}.$$

For any vector of non-negative integers $\vec{d}(\vec{\alpha})$ indexed by $\mathcal{R}$, define $\mathcal{F}_{\vec{d}(\vec{\alpha})}$, $\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$, $\mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})}$, $\hat{\mathcal{F}}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})}$, $\mathcal{F}_{[\vec{d}(\vec{\alpha})]}$ and $\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ in the same way as in Section 3.4. Then ϕ and ψ induce a bijection

from $\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ to $\hat{\mathcal{F}}_{(d_1,\dots,d_{r-1})}$ that sends $d(\vec{\alpha})$ to $d_{\phi\circ\psi(\vec{\alpha})}$. Under this bijection (3.2.4) and (3.2.5) become

$$\sum_{\vec{\alpha}\in\mathcal{R}} \phi\circ\psi(\vec{\alpha})d(\vec{\alpha}) \equiv 0 \pmod{r} \tag{3.5.1}$$

$$2g+2r-2 = \sum_{\vec{\alpha}\in\mathcal{R}} \left(r-(r,\phi\circ\psi(\vec{\alpha}))\right). \tag{3.5.2}$$

Then we can write

$$\mathcal{H}_{r,g} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{H}^{\vec{d}(\vec{\alpha})}$$

where the union is over all $\vec{d}(\vec{\alpha})$ that satisfy (3.5.1) and (3.5.2).

Lemma 3.5.1, Proposition 3.5.3 and Corollary 3.5.5 are analogues of Lemma 3.4.1, Proposition 3.4.3 and Corollary 3.4.6 from Section 3.4. As such, we will state them and explain how the same techniques to prove their analogues in Section 3.4 can be used to prove them.

Lemma 3.5.1. *Suppose* $r=\prod_{j=1}^n p_j^{t_j}$ *and let* $a_{i,j,k_j}\in\mathbb{F}_q^*$ $i=1,\dots,\ell$, $j=1,\dots,n$, $k_j=1,\dots,t_j$, *such that* $a_{i,j,k_j}=a_{i,j,k_j-1}(b_{i,j,k_j})^{p^{k_j-1}}$ *for some* $b_{i,j,k_j}\in\mathbb{F}_q^*$. *Further we let* $a_{i,j,0}=1$ *so that* $a_{i,j,1}=b_{i,j,1}$. *Then*

$$\begin{aligned}&|\{(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i)=a_{i,j,k_j}, 1\le j\le n, 1\le k_j\le t_j, 1\le i\le\ell\}|\\ =&\frac{L_{r-2}q^{\sum_{\vec{\alpha}\in\mathcal{R}}d(\vec{\alpha})}}{\zeta_q(2)^{r-1}}\left(\frac{q\prod_{j=1}^n p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n}(q+r-1)}\right)^{\ell}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}}d(\vec{\alpha})}{2}}\right)\right).\end{aligned}$$

Proof. Recall, we define $T_j=\sum_{i=1}^j t_i$. As we saw in the proof of Lemma 3.4.1, it will be enough to consider what values the polynomials

$$F_{(j,k_j)}=\prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}^{\alpha_{T_{j-1}+k_j}}$$

take, up to some root of unity. That is,

$$\begin{aligned}&|\{(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i)=a_{i,j,k_j}, 1\le j\le n, 1\le k_j\le t_j, 1\le i\le\ell\}|\\ =&|\{(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(j,k_j)}(x_i)=\epsilon_{i,j,k_j}b_{i,j,k_j}, \epsilon_{i,j,k_j}\in\mu_{p^{k_j-1}}, 1\le j\le n, 1\le k_j\le t_j, 1\le i\le\ell\}|.\end{aligned}$$

We can define a bijection

$$\phi:\{(j,k_j): 1\le j\le n, 1\le k_j\le t_j\}\to\{1,\dots,T_n\}$$

by

$$\phi(j,k_j) = T_{j-1} + k_j.$$

Define $\epsilon_{i,j} = \epsilon_{i,\phi^{-1}(j)}$, $b_{i,j} = b_{i,\phi^{-1}(j)}$ and $F_j = F_{\phi^{-1}(j)}$, then

$$F_j = \prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}.$$

If we denote $\mu_m = \mu_{p_j^{k_j}}$ where $\phi(j,k_j) = m$ then,

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(j,k_j)}(x_i) = \epsilon_{i,j,k_j} b_{i,j,k_j}, \epsilon_{i,j,k_j} \in \mu_{p_j^{k_j-1}}, 1 \le j \le n, 1 \le k_j \le t_j, 1 \le i \le \ell\}| \\
&= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) = \epsilon_{i,j} b_{i,j}, \epsilon_{i,j} \in \mu_j, 1 \le j \le T_n, 1 \le i \le \ell\}| \\
&= \frac{L_{r-2} q^{\sum_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r-1}} \left(\frac{q \prod_{j=1}^n p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n}(q+r-1)} \right)^{\ell} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}} d(\vec{\alpha})}{2}}\right)\right)
\end{aligned}$$

where the last equality comes from Proposition 2.1.12.

□

Now we want to determine the size of the set

$$\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \le j \le n, 1 \le k_j \le t_j, 1 \le i \le \ell\} \tag{3.5.3}$$

where some of the $a_{i,j,k_j} = 0$. Like in the prime power case if $a_{i,j,k_j} = 0$ then $a_{i,j,k_j+1} = 0$ since $F_{(p_j^{k_j})}(X) | F_{(p_j^{k_j+1})}(X)$. With this in mind, we create a new definition.

Definition 3.5.2. Let $\mathcal{T} := [0,\dots,t_1] \times \cdots \times [0,\dots,t_n]$. For any $\vec{\tau} \in \mathcal{T}$ we will write $\vec{\tau} = (\tau_1,\dots,\tau_n)$. We say a set of elements $\{a_{j,k_j}, j = 1,\dots,n, k_j = 1,\dots,t_j\} \in \mathbb{F}_q$ is **$\vec{\tau}$-admissible** if there exists $\{b_{j,k_j}, j = 1,\dots,n, k_j = 1,\dots,t_j\} \in \mathbb{F}_q^*$ such that

$$a_{j,1},\dots,a_{j,\tau_j} \neq 0, a_{j,\tau_j+1} = \cdots = a_{j,t_j} = 0, j = 1,\dots,n$$

$$a_{j,k_j} = a_{j,k_j-1} (b_{j,k_j})^{p_j^{k_j-1}}, j = 1,\dots,n, k_j = 1,\dots,\tau_j$$

where we set $a_{j,0} = 1$.

Therefore, for all i the set $\{a_{i,j,k_j}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ must be $\vec{\tau}$-admissible for some $\vec{\tau} \in \mathcal{T}$. Moreover, if $\{a_{i,j,k_j}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ is $\vec{\tau}$-admissible where $\tau_j = t_j$ for some j, then $F_{(p_j^{k_j})}(x_i) \neq 0$ for all k_j. As we will see, these cases are important. With this in mind we define, for every $\vec{\tau} \in \mathcal{T}$,

$$J_{\vec{\tau}} = \{j : \tau_j \neq t_j\}.$$

Finally denote $\vec{t} = (t_1, \dots, t_n) \in \mathcal{T}$. Then, if a set if $\vec{t}$-admissible, this means that all the $a_{i,j,k_j} \neq 0$.

Proposition 3.5.3. *Let $a_{i,j,k_j} \in \mathbb{F}_q$ such that for all i, $\{a_{i,j,k_j}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ is $\vec{\tau}$-admissible for some $\vec{\tau} \in \mathcal{T}$. Let*

$$m_{\vec{\tau}} = \#\{1 \leq i \leq \ell : \{a_{i,j,k_j}, j = 1, \dots, n, k_j = 1, \dots, t_j\} \text{ is } \vec{\tau}\text{-admissible}\}$$

Then $\sum_{\vec{\tau} \in \mathcal{T}} m_{\vec{\tau}} = \ell$ and

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_{(p_j^{k_j})}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}| \\
=&\frac{L_{r-2} q^{\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}}{\zeta_q(2)^{r-1}} \prod_{\substack{\vec{\tau} \in \mathcal{T} \\ \vec{\tau} \neq \vec{t}}} \left(\frac{\prod_{j \in J_{\vec{t}}} (p_j - 1) p_j^{t_j - \tau_j - 1} \prod_{j=1}^n p_j^{\frac{\tau_j(\tau_j-1)}{2}}}{(q + r - 1) \prod_{j=1}^n (q-1)^{\tau_j}} \right)^{m_{\vec{\tau}}} \\
&\times \left(\frac{q \prod_{j=1}^n p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{T_n}(q + r - 1)} \right)^{m_{\vec{t}}} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}}\right)\right).
\end{aligned}$$

Proof. Define $g_{\vec{\alpha}}$ to be $f_{\vec{\alpha}}$ divided by its roots, and $G_{(p_j^{k_j})}$ as the corresponding product of $g_{\vec{\alpha}}$. If $\{a_{i,j,k_j}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ is $\vec{\tau}$-admissible then $G_{(p_j^{k_j})}(x_i)$ will be determined by $F_{(p_j^{k_j})}(x_i)$ for $k_j \leq \tau_j$ and $G_{(p_j^{k_j})}(x_i)$ will be determined, up to a $p_j^{k_j - 1}$th root of unity, by $F_{(p_j^{k_j - 1})}(x_i)$ for $\tau_j < k_j \leq t_j$. Summing up over all the necessary partitions of $m_{\vec{\tau}}$ will give the desired result.

□

Let $s|r$ and write it as $s = \prod_{j=1}^n p_j^{k_j}$, then we can write

$$\prod_{j \in J_{\vec{\tau}}} (p_j - 1) p_j^{t_j - k_j - 1} = \phi\left(\frac{r}{s}\right).$$

This illustrates why it was important to consider the set $J_{\vec{\tau}}$ for if the left hand product was over all the j, we would not get this nice equality.

Definition 3.5.4. We say a set $\{\epsilon_{j,k_j} \in \mu_{p_j^{k_j}}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ is $\vec{\tau}$-**admissible** if

$$\epsilon_{j,1}, \dots, \epsilon_{j,\tau_j} \neq 0, \epsilon_{j,\tau_j+1} = \cdots = \epsilon_{j,t_j} = 0, j = 1, \dots, n$$

$$\epsilon_{j,k_j} = (\epsilon_{j,k_j-1})^p, j - 1, \dots, n, k_j = 1, \dots, \tau_j$$

where we set $\epsilon_{j,0} = 1$.

Corollary 3.5.5. *Let $\epsilon_{i,j,k_j} \in \mu_{p_j^{k_j}} \cup \{0\}$ such that for all i, the set $\{\epsilon_{i,j,k_j} \in \mu_{p_j^{k_j}}, j = 1, \dots, n, k_j = 1, \dots, t_j\}$ is $\vec{\tau}$-admissible for some $\vec{\tau} \in \mathcal{T}$. Let*

$$m_{\vec{\tau}} = \#\{1 \leq i \leq q+1 : \{\epsilon_{i,j,k_j} \in \mu_{p_j^{k_j}}, j = 1, \dots, n, k_j = 1, \dots, t_j\} \text{ is } \vec{\tau}\text{-admissible}\}$$

Then $\sum m_{\vec{\tau}} = q + 1$ and

$$\frac{|\{(c, (f_{\vec{\alpha}})) \in \hat{F}_{[\vec{d}(\vec{\alpha})]} : \chi_{p_j^{k_j}}(F_{(p_j^{k_j})}(x_i)) = \epsilon_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq q+1\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \prod_{\substack{\vec{\tau} \in \mathcal{T} \\ \vec{\tau} \neq \vec{t}}} \left(\frac{\prod_{j \in J_{\vec{\tau}}} (p_j - 1) p_j^{t_j - \tau_j - 1}}{\prod_{j=1}^n p_j^{\tau_j} (q + r - 1)} \right)^{m_{\vec{\tau}}} \left(\frac{q}{r(q+r-1)} \right)^{m_{\vec{t}}} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).$$

Proof. The proof of this follows the same steps as in Corollaries 3.4.5, 3.4.6.

□

Remark 3.5.6. For every $\vec{\tau} \in \mathcal{T}$, we can associate a divisor of r in the the natural way

$$s = \prod_{j=1}^n p_j^{\tau_j}.$$

With this identification we then obtain

$$\frac{|\{(c, (f_{\vec{\alpha}})) \in \hat{F}_{[\vec{d}(\vec{\alpha})]} : \chi_{p_j^{k_j}}(F_{(p_j^{k_j})}(x_i)) = \epsilon_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq q+1\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \prod_{\substack{s|r \\ s \neq r}} \left(\frac{\phi\left(\frac{r}{s}\right)}{s(q+r-1)} \right)^{m_s} \left(\frac{q}{r(q+r-1)} \right)^{m_r} \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha})}{2}} \right) \right).$$

where

$$m_s = m_{\left(v_{p_1}(s), \dots, v_{p_n}(s)\right)}$$

Proof of Theorem 1.2.3.

$$\frac{|\{(c,(f_{\vec{\alpha}}))\in \hat{F}_{[\vec{d}(\vec{\alpha})]} : S_s(F_{(s)})=M_s, \forall s|r\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \sum_{\substack{E_{s,1},\dots,E_{s,q+1}\in\mu_s\cup\{0\}\\ \sum_{i=1}^{q+1}E_{s,i}=M_s\\ E_{s,i}=\prod_{p|s}(E_{p^{v_p(s)},i})^{\sigma_p}\forall s|r\\ E_{p_j^{k_j},i}=0\Longrightarrow E_{p_j^{k_j+1},i}=0 \text{ and}\\ E_{p_j^{k_j},i}\neq 0\Longrightarrow E_{p_j^{k_j-1},i}=E^{p_j}_{p_j^{k_j},i}\ \forall j,1<k_j\leq t_j}} \frac{|\{(c,(f_{\vec{\alpha}}))\in \hat{F}_{[\vec{d}(\vec{\alpha})]} : \chi_s(F_{(s)}(x_i))=E_{s,i}, \forall s|r, 1\leq i\leq q+1\}|}{|\hat{F}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \sum{}' \left(\frac{\phi\left(\frac{r}{s}\right)}{s(q+r-1)}\right)^{m_s}\left(\frac{q}{r(q+r-1)}\right)^{m_r}\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}}d(\vec{\alpha})}{2}}\right)\right)$$

$$= \text{Prob}(\sum_{i=1}^{q+1}X_{s,i}=M_s \text{ for all } s|r)\left(1+O\left(q^{-\frac{\min_{\vec{\alpha}\in\mathcal{R}}d(\vec{\alpha})}{2}}\right)\right)$$

where $\sum'$ is the same sum as in the previous line and in the subscript we have σ_p is the smallest positive integer such that $\sigma_p \equiv p^{-v_p(s)} \pmod{\frac{s}{p^{v_p(s)}}}$ and the $X_{s,i}$ satisfy the conditions the if $i\neq j$ then $X_{s,i}$ and $X_{s',j}$ are independent for all $s|s'$ whereas if $i=j$, then

$$X_{s,i}=\prod_{p|s}(X_{p^{v_p(s)},i})^{\sigma_p} \text{ where } 1\leq\sigma_p\leq\frac{s}{p^{v_p(s)}} \text{ such that } \sigma_p\equiv(p^{v_p(s)})^{-1}\pmod{\frac{s}{p^{v_p(s)}}}.$$

Further, for all $p|r$ and $1<v\leq v_p(r)$

$$\text{Prob}\left(X_{p^v,i}=0|X_{p^{v-1},i}=0\right)=1$$

$$\text{Prob}\left(X_{p^{v-1},i}=\epsilon^p_{p^v,i}|X_{p^v,i}=\epsilon_{p^v,i}\right)=1,$$

if $s\neq r$ then

$$\text{Prob}\left(X_{p^v,i}=\epsilon_{p^v,i}\neq 0, 1\leq v\leq v_p(s) \text{ and } X_{p^v,i}=0, v_p(s)<v\leq v_p(r) \text{ for all } p|r\right)$$

$$=\begin{cases}\frac{\phi(\frac{r}{s})}{s(q+r-1)} & \text{if } \epsilon_{p^{v-1},i}=\epsilon^p_{p^v,i} \text{ for all } p|r, 1\leq v\leq v_p(s)\\ 0 & \text{otherwise}\end{cases}$$

and, if $s=r$,

$$\text{Prob}\left(X_{p^v,i}=\epsilon_{p^v,i}, v\leq v_p(r), \text{ for all } p|r\right)=\begin{cases}\frac{q}{r(q+r-1)} & \text{if } \epsilon_{p^{v-1},i}=\epsilon^p_{p^v,i}, 1\leq v\leq v_p(r), \text{ for all } p|r\\ 0 & \text{otherwise}\end{cases}.$$

From these conditions we can determine

$$\begin{aligned}&\text{Prob}\left(X_{s,i}=\epsilon_{s,i}\neq 0\right)\\&=\sum_{\substack{s_1\\ s|s_1}}{\sum}'\text{Prob}\left(X_{p^v,i}=\epsilon_{p^{v_p(s_1)},i}^{p^{v_p(s_1)-v}},1\leq v\leq v_p(s_1)\text{ and }X_{p^v,i}=0,v_p(d_1)<v\leq v_p(r)\text{ for all }p|r\right)\end{aligned}$$

where $\sum'$ is the sum that runs over all

$$\epsilon_{p^{v_p(s_1)},i}\in\mu_{p^{v_p(s_1)}}\text{ such that }\epsilon_{p^{v_p(s_1)},i}^{p^{v_p(s_1)-v_p(s)}}=\epsilon_{p^{v_p(s)},i}\text{ for all }p|r.$$

Hence,

$$\begin{aligned}\text{Prob}\left(X_{s,i}=\epsilon_{s,i}\neq 0\right)&=\sum_{\substack{s_1\neq r\\ s|s_1}}{\sum}'\frac{\phi\left(\frac{r}{s_1}\right)}{s_1(q+r-1)}+\sum_{s_1=r}{\sum}'\frac{q}{r(q+r-1)}\\&=\frac{q+\sum_{\substack{s_1\neq r\\ s|s_1}}\phi\left(\frac{r}{s_1}\right)}{s(q+r-1)}=\frac{q+\sum_{n|\frac{r}{s}}\phi\left(\frac{r/s}{n}\right)-1}{s(q+r-1)}\\&=\frac{q+\frac{r}{s}-1}{s(q+r-1)}\end{aligned}$$

and

$$\text{Prob}(X_{s,i}=0)=1-\sum_{\epsilon_{s,i}\in\mu_s}\text{Prob}(X_{s,i}=\epsilon_{s,i})=1-\frac{q+\frac{r}{s}-1}{q+r-1}=\frac{r-\frac{r}{s}}{q+r-1}.$$

□

Chapter 4

Abelian Curves

In this section, outside of Section 4.1, C will always be a curve such that

$$\mathrm{Gal}(C) = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$$

where r_j is chosen such that $r_j | r_{j+1}$.

4.1 Known Results

Lorenzo, Meleleo, Milione and Bucur were the first ones to study this question when G is not cyclic. Specifically, they answered the question for curves such that $\mathrm{Gal}(C) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence, there exists two square-free polynomials F_1, F_2 such that C has an affine model of the form

$$Y_1^2 = F_1(X) \qquad Y_2^2 = F_2(X)$$

Following the same line of work as in the literature, they define the sets

$$\hat{\mathcal{F}}_{(d_1,d_2,d_3)} = \{(c_1, c_2, f_1, f_2, f_3) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathcal{F}_{d_1} \times \mathcal{F}_{d_2} \times \mathcal{F}_{d_3} : (f_1, f_2) = (f_1, f_3) = (f_2, f_3) = 1\}$$

$$\mathcal{F}_{[d_1,d_2,d_3]} = \mathcal{F}_{(d_1,d_2,d_3)} \cup \mathcal{F}_{(d_1-1,d_2,d_3)} \cup \mathcal{F}_{(d_1,d_2-1,d_3)} \cup \mathcal{F}_{(d_1,d_2,d_3-1)}$$

$$\hat{\mathcal{F}}_{[d_1,d_2,d_3]} = \hat{\mathcal{F}}_{(d_1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1-1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2-1,d_3)} \cup \mathcal{F}_{(d_1,d_2,d_3-1)}.$$

Remark 4.1.1. In Section 3 the notation for $\hat{\mathcal{F}}$ only had one element on $\mathbb{F}_q^*$ whereas the above needs *two* elements of $\mathbb{F}_q^*$. In the following sections we will redefine $\hat{\mathcal{F}}$ to include n different elements of $\mathbb{F}_q^*$ where $\mathrm{Gal}(C) = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$.

So now we can find a $(c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1,d_2,d_3)}$ such that

$$F_1(X) = c_1 f_1(X) f_2(X) \qquad F_2(X) = c_2 f_1(X) f_3(X)$$

and (2.2.3) becomes

$$2g + 6 = \begin{cases} 2(d_1 + d_2 + d_3) & d_1 + d_2 \equiv 0 \pmod 2, d_1 + d_3 \equiv 0 \pmod 2, \\ 2(d_1 + d_2 + d_3 + 1) & \text{otherwise.} \end{cases}$$

Therefore, define $\mathcal{H}^{(d_1,d_2,d_3)}$ to be the set of curves coming from $\hat{\mathcal{F}}_{[d_1,d_2,d_3]}$. Then if $d_1 + d_2 \equiv 0 \pmod 2$ and $d_1 + d_3 \equiv 0 \pmod 2$ the genus is invariant among curves in $\mathcal{H}^{(d_1,d_2,d_3)}$. That is we can write

$$\mathcal{H}_{(\mathbb{Z}/2\mathbb{Z})^2,g} = \bigcup_{d_1,d_2,d_3} \mathcal{H}^{(d_1,d_2,d_3)}$$

where the union is over all d_1, d_2, d_3 that satisfy

$$d_1 + d_2 \equiv 0 \pmod 2 \qquad d_1 + d_3 \equiv 0 \pmod 2$$

$$2g + 6 = 2(d_1 + d_2 + d_3)$$

Further, if we define $F_3(X) = c_1 c_2 f_2(X) f_3(X)$ and x_{q+1} the point at infinity, then

$$F_1(x_{q+1}) = \begin{cases} c_1 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2,d_3-1)} \\ 0 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1-1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2-1,d_3)} \end{cases}$$

$$F_2(x_{q+1}) = \begin{cases} c_2 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2-1,d_3)} \\ 0 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1-1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2,d_3-1)} \end{cases}$$

$$F_3(x_{q+1}) = \begin{cases} c_1 c_2 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1,d_2,d_3)} \cup \hat{\mathcal{F}}_{(d_1-1,d_2,d_3)} \\ 0 & (c_1, c_2, f_1, f_2, f_3) \in \hat{\mathcal{F}}_{(d_1,d_2-1,d_3)} \cup \hat{\mathcal{F}}_{(d_1,d_2,d_3-1)} \end{cases}$$

and

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} (1 + \chi_2(F_1(x)) + \chi_2(F_2(x)) + \chi_2(F_3(x)))$$

where χ_2 is a multiplicative character or order 2.

From here Lorenzo, Meleleo, Milione and Bucur show that

Theorem 4.1.2. *If $d_1, d_2, d_3 \to \infty$, then for any $M \in \mathbb{Z}$,*

$$\frac{|\{C \in \mathcal{H}^{(d_1,d_2,d_3)} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}^{(d_1,d_2,d_3)}|} \sim Prob\left(\sum_{i=1}^{q+1} X_i = M\right)$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\ 2 & \text{with probability } \frac{6}{4(q+3)} \\ 4 & \text{with probability } \frac{q}{4(q+3)} \end{cases}.$$

Remark 4.1.3. The actual result of Lorenzo, Meleleo, Milione and Bucur dealt only with

$$\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \left(\chi_2(F_1(x)) + \chi_2(F_2(x)) + \chi_2(F_3(x))\right),$$

which is the trace of the Frobenius as discussed in the introduction. Therefore, their random variables can take the values $-1, 1$ and 3. We change it here to better mirror Theorem 1.3.3

Moreover, Lorenzo, Meleleo, Milione and Bucur extends this to curves such that $\mathrm{Gal}(C) = (\mathbb{Z}/2\mathbb{Z})^n$. In this case we need to consider $2^n - 1$ different square-free coprime polynomials. If we define $\mathcal{H}^{(d_1,\ldots,d_{2^n-1})}$ in an analogous way as above, they show that

Theorem 4.1.4. *If $d_1, \ldots, d_{2^n-1} \to \infty$, then for any $M \in \mathbb{Z}$,*

$$\frac{|\{C \in \mathcal{H}^{(d_1,\ldots,d_{2^n-1})} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}^{(d_1,\ldots,d_{2^n-1})}|} \sim Prob\left(\sum_{i=1}^{q+1} X_i = M\right)$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{(2^n-1)(q+2^n-2)}{2^n(q+2^n-1)} \\ 2^{n-1} & \text{with probability } \frac{2(2^n-1)}{2^n(q+2^n-1)} \\ 2^n & \text{with probability } \frac{q}{2^n(q+2^n-1)} \end{cases}.$$

4.2 Moduli Space Decomposition

Let C be a smooth projective curve over $\mathbb{F}_q$ such that $\mathrm{Gal}(C) = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$. Then, since we are assuming $q \equiv 1 \pmod{r_n}$, by Kummer Theory, we can find $F_1, \ldots, F_n \in K$ such that F_j is r_j^{th}-power free and

$$K(C) = K\left(\sqrt[r_1]{F_1(X)}, \ldots, \sqrt[r_n]{F_n(X)}\right).$$

Then C will have an affine model of the form

$$Y_1^{r_1} = F_1(X), \ldots, Y_n^{r_n} = F_n(X)$$

If we let

$$\mathcal{R} = [0, \ldots, r_1 - 1] \times \cdots \times [0, \ldots, r_n - 1] \setminus \{(0, \ldots, 0)\}$$

then we showed in Section 2.1.2 we can find $(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}$ and $c_1, \ldots, c_n \in \mathbb{F}_q^*$ such that

$$F_j = c_j \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}$$

for $j = 1, \ldots, n$.

Recall that if we let $\vec{d} = (d_1, \ldots, d_n) = (\deg(F_1), \ldots, \deg(F_n))$ and $g(C) = g$, the genus of C, then (2.2.3) says that

$$2g + 2|G| - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} \left(|G| - \frac{|G|}{e(\vec{\alpha})} \right) d(\vec{\alpha}) + |G| - \frac{|G|}{e(\vec{d})}$$

where for any $\vec{v} = (v_1, \ldots, v_n)$ we have

$$e(\vec{v}) = \operatorname*{lcm}_{j=1,\ldots,n} \left(\frac{r_j}{(r_j, v_j)} \right).$$

Notice that $|G| - \frac{|G|}{e(\vec{d})} = 0$ if and only if $d_j = \sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv 0 \pmod{r_j}$ for $j = 1, \ldots, n$. This leads to defining the following sets

$$\begin{aligned}
\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} &= \{(\vec{c}, (f_{\vec{\alpha}})) \in (\mathbb{F}_q^*)^n \times \mathcal{F}_{\vec{d}(\vec{\alpha})}\} \\
\mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} &= \{(f_{\vec{\beta}}, (f_{\vec{\alpha}})) \in \mathcal{F}_{d(\vec{\beta})-1} \times \prod_{\substack{\vec{\alpha} \in \mathcal{R} \\ \vec{\alpha} \neq \vec{\beta}}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\gamma}}) = 1, \vec{\alpha} \neq \vec{\gamma} \in \mathcal{R}\} \\
\hat{\mathcal{F}}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} &= \{(\vec{c}, f_{\vec{\beta}}, (f_{\vec{\alpha}})) \in (\mathbb{F}_q^*)^n \times \mathcal{F}_{d(\vec{\beta})-1} \times \prod_{\substack{\vec{\alpha} \in \mathcal{R} \\ \vec{\alpha} \neq \vec{\beta}}} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\gamma}}) = 1, \vec{\alpha} \neq \vec{\gamma} \in \mathcal{R}\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{F}_{[\vec{d}(\vec{\alpha})]} &= \mathcal{F}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \mathcal{F}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})} \\
\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} &= \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} \hat{\mathcal{F}}^{\vec{\beta}}_{\vec{d}(\vec{\alpha})}.
\end{aligned}$$

Further, we will write $\vec{c} = (c_1, \ldots, c_n) \in \left(\mathbb{F}_q^*\right)^n$.

Let $\mathcal{H}^{\vec{d}(\vec{\alpha})}$ be the set of curves with affine model

$$Y_1^{r_1} = F_1(X), \ldots, Y_n^{r_n} = F_n(X)$$

where

$$F_j(X) = c_j \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}, j = 1, \ldots, n$$

for some $(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$.

Therefore, if we let $\vec{d}(\vec{\alpha})$ be a vector of non-negative integers such that

$$\sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv 0 \pmod{r_j}, j = 1, \ldots, n \tag{4.2.1}$$

Then the genus is invariant among curves in $\mathcal{H}^{\vec{d}(\vec{\alpha})}$ and satisfies the equation

$$2g + 2|G| - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} \left(|G| - \frac{|G|}{e(\vec{\alpha})} \right) d(\vec{\alpha}). \tag{4.2.2}$$

Hence, we can write

$$\mathcal{H}_{G,g} = \bigcup_{d(\vec{\alpha})} \mathcal{H}^{\vec{d}(\vec{\alpha})}$$

where the union is over all $d(\vec{\alpha})$ that satisfy (4.2.1) and (4.2.2).

4.3 Number of Points on the Curve

We can view $K(C)$ as a vector space over K with dimension $|G|$. Let

$$\mathscr{B} = \{B_1, \ldots, B_{|G|}\}$$

be a basis of $K(C)$ over K. Since $q \equiv 1 \pmod{r_n}$, by Kummer Theory, we can assume that for all $B \in \mathscr{B}$, there exists an m such that $B^m \in K$. Let m_i be the smallest positive integer such that $B_i^{m_i} \in K$. Now, if $x \in \mathbb{F}_q$, then we can find a $B_{j_1}, \ldots, B_{j_n} \in \mathscr{B}$ such that the smooth affine model of C at x is of the form

$$Y_1^{m_{j_1}} = B_{j_1}^{m_{j_1}}(X) \qquad Y_2^{m_{j_2}} = B_{j_2}^{m_{j_2}}(X) \qquad \ldots \qquad Y_n^{m_{j_n}} = B_{j_n}^{m_{j_n}}(X)$$

Hence, the number of points lying over x will be $m_{j_1} m_{j_2} \cdots m_{j_n}$ if $B_{j_k}(x)$ is an $m_{j_k}^{th}$ power for $k = 1, \ldots, n$ and 0 otherwise. Therefore, the number of point lying over x can be written as

$$\prod_{k=1}^{n} \sum_{i=0}^{m_{j_k}-1} \chi_{m_{j_k}}^{i} \left(B_{j_k}^{m_{j_k}}(x) \right).$$

Let $B_i \notin K(B_{j_1}, \ldots, B_{j_n})$. Then I claim that $B_i(x) = 0$. Indeed, consider the smooth projective curve C' such that $K(C') = K(B_{j_1}, \ldots, B_{j_n}, B_i)$. Then C' will have an affine model of the form

$$Y_s^{m_i} = B_i^{m_i}(X)$$

$$Y_k^{m_{j_k}} = B_{j_k}^{m_{j_k}}(X), 1 \leq k \leq n, k \neq s.$$

That is B_i will replace B_{j_s} for some $1 \leq s \leq n$.

Moreover, this affine model is not smooth at x by our choices of $B_{j_1}, \ldots, B_{j_n}$. Therefore, one of four things may happen:

1. $B_{j_k}(X)$ is divisible by $(X - x)^2$ for some $1 \leq k \leq n$, $k \neq s$
2. $B_i(X)$ is divisible by $(X - x)^2$
3. $B_{j_k}(x) = B_{j_k'}(x) = 0$ for some $1 \leq k < k' \leq n$, $k, k' \neq s$.
4. $B_{j_k}(x) = B_i(x) = 0$ for some $1 \leq k \leq n$, $k \neq s$.

Case one and three can't happen because this would imply our original model was not smooth at x. Therefore, case two or four must happen and in both of these cases $B_i(x) = 0$

Hence, the number of points lying over x is

$$\prod_{k=1}^{n} \sum_{i=0}^{m_{j_k}-1} \chi_{m_{j_k}}^{i} \left(B_{j_k}^{m_{j_k}}(x)\right) = \sum_{j=1}^{|G|} \chi_{m_j}(B_j^{m_j}(x))$$

as all the terms appearing on the right hand side that don't appear on the left hand side are 0.

Let $C \in \mathcal{H}^{\vec{d}(\vec{\alpha})}$ such that C corresponds to $(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$. To use the discussion above, we want to find a basis for $K(C)$ over K. Towards this, define

$$\mathcal{S} = \{\vec{s} = (s_1, \ldots, s_n) : s_j | r_j\}$$

and for all $\vec{s} \in \mathcal{S}$ define

$$\ell(\vec{s}) = \text{lcm}(s_1, \ldots, s_n)$$

$$\Omega_{\vec{s}} = \{\vec{\omega} = (\omega_1, \ldots, \omega_n) : 1 \leq \omega_j \leq s_j, (\omega_j, s_j) = 1\} \subset \mathcal{R}.$$

For any $\vec{s} \in \mathcal{S}$, $\vec{\omega} \in \Omega_{\vec{s}}$, and $(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$ define

$$F_{(\vec{s})}^{(\vec{\omega})}(X) := c_{(\vec{s})}^{(\vec{\omega})} \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}(X)^{\sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j} \omega_j \alpha_j \pmod{\ell(\vec{s})}}$$

$$c_{(\vec{s})}^{(\vec{\omega})} := \prod_{j=1}^{n} c_j^{\frac{\ell(s)}{s_j} \omega_j \pmod{\ell(\vec{s})}}.$$

Again, when we write in the exponent $* \pmod{\ell(\vec{s})}$, we mean the smallest, non-negative integer that is congruent to $*$ modulo $\ell(\vec{s})$. Moreover, we make the identification that $f_{\vec{\alpha}}(X)^0$ is identically the constant polynomial 1. Hence, if $\sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j} \omega_j \alpha_j \equiv 0 \pmod{\ell(\vec{s})}$, then $f_{\vec{\alpha}}(X)$ does not divide $F_{(\vec{s})}^{(\vec{\omega})}(X)$. In particular, if $\vec{s} = (1, \ldots, 1)$, then $\Omega_{\vec{s}} = \{(1, \ldots, 1)\}$ and we make the identification

$$F_{(1,\ldots,1)}^{(1,\ldots,1)}(X) = 1, c_{(1,\ldots,1)}^{(1,\ldots,1)} = 1$$

Therefore, we see that a basis for $K(C)$ over K can be given by

$$\mathscr{B} = \left\{ \left(F_{(\vec{s})}^{(\vec{\omega})}(X) \right)^{\frac{1}{\ell(\vec{s})}}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}} \right\}$$

Hence the number of points lying over any $x \in \mathbb{F}_q$ can be written as

$$\sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_{\vec{s}}} \chi_{\ell(\vec{s})} \left(F_{(\vec{s})}^{(\vec{\omega})}(x) \right).$$

This leads to following lemma.

Lemma 4.3.1. *Let $C \in \mathcal{H}^{\vec{d}(\vec{\alpha})}$ that corresponds to $(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$. Then the number of affine points on the curve is*

$$\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{F}_q} \sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_{\vec{s}}} \chi_{\ell(\vec{s})} \left(F_{(\vec{s})}^{(\vec{\omega})}(x) \right).$$

It remains to determine what happens at the point at infinity, x_{q+1}. For any $F(X) \in \mathbb{F}_q[X]$, let $\tilde{F}(X)$ denote the polynomial that inverts the order of the coefficients of $F(X)$. That is, if

$$F(X) = a_0 + a_1 X + \cdots + a_d X^d,$$

then

$$\tilde{F}(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d.$$

Further, if we let $X' = 1/X$, then we have $F(X) = (X')^{-d}\tilde{F}(X')$, where $d = \deg(F)$. Hence to determine what happens at x_{q+1}, we need to determine what happens when $X' = 0$ for the curve

$$Y_j^{r_j} = (X')^{-d_j}\tilde{F}_j(X'), j = 1, \ldots, n.$$

If we write $d_j = r_j m_j + k_j$ with $1 \leq k_j \leq r_j$, and let $Y_j' = Y_j(X')^{m_j+1}$, then we have an isomorphism to the curve

$$(Y_j')^{r_j} = (X')^{r_j-k_j}\tilde{F}_j(X'), j = 1, \ldots, n.$$

So, we see we get a root at x_{q+1} if and only if $k_j \neq r_j$ if and only if $d_j \not\equiv 0 \pmod{r_j}$. Therefore, we can write

$$F_j(x_{q+1}) = \begin{cases} c_j & d_j \equiv 0 \pmod{r_j} \\ 0 & d_j \not\equiv 0 \pmod{r_j} \end{cases}$$

Likewise, we see that

$$F_{(\vec{s})}^{(\vec{\omega})}(x_{q+1}) = \begin{cases} c_{(\vec{s})}^{(\vec{\omega})} & \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j d_j \equiv 0 \pmod{\ell(\vec{s})} \\ 0 & \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j d_j \not\equiv 0 \pmod{\ell(\vec{s})}. \end{cases}$$

Thus the number of points lying over x_{q+1} is

$$\sum_{\vec{s}\in\mathcal{S}} \sum_{\vec{\omega}\in\Omega_{\vec{s}}} \chi_{\ell(\vec{s})}\left(F_{(\vec{s})}^{(\vec{\omega})}(x_{q+1})\right)$$

and we get the following lemma.

Lemma 4.3.2. *Let $C \in \mathcal{H}^{\vec{d}(\vec{\alpha})}$ that corresponds to $(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$. Then the number of projective points on the curve is*

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \sum_{\vec{s}\in\mathcal{S}} \sum_{\vec{\omega}\in\Omega_{\vec{s}}} \chi_{\ell(\vec{s})}\left(F_{(\vec{s})}^{(\vec{\omega})}(x)\right).$$

4.4 Admissibility

Definition 4.4.1. A set

$$\{\epsilon_{\vec{s},\vec{\omega}} \in \mu_{\ell(\vec{s})} \cup \{0\}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$$

is called **admissible** if there exists $(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ and an $x \in \mathbb{P}^1(\mathbb{F}_q)$ such that

$$\epsilon_{\vec{s},\vec{\omega}} = \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x))$$

for all $\vec{s} \in \mathcal{S}$, $\vec{\omega} \in \Omega_{\vec{s}}$. (Note that $\epsilon_{(1,\dots,1),(1,\dots,1)} = 1$.)

We will now prove some properties we will need to use about admissible sets.

Lemma 4.4.2. *For all $\vec{s} \in \mathcal{S}$, $\vec{\omega} \in \Omega_{\vec{s}}$ and $p|r_n$, prime, define*

$$\vec{s}_p = (p^{v_p(s_1)}, \dots, p^{v_p(s_n)})$$

$$\vec{\omega}_p = (\omega_1 \ (mod\ p^{v_p(s_1)}), \dots, \omega_n \ (mod\ p^{v_p(s_n)})).$$

Let m_p be the smallest, non-negative integer such that $m_p \equiv \ell(\vec{s}_p)^{-1}$ $(mod\ \frac{\ell(\vec{s})}{\ell(\vec{s}_p)})$. If $\{\epsilon_{\vec{s},\vec{\omega}} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$ is admissible then

$$\epsilon_{\vec{s},\vec{\omega}} = \prod_{p|r_n} \epsilon^{m_p}_{\vec{s}_p,\vec{\omega}_p}$$

Proof. Let $\vec{s} \in \mathcal{S}$. If there exists a $p|r_n$, prime such that $s_j = p^{v_j}$ for $j = 1, \dots, n$, then $s_{p'} = (1, \dots, 1)$, $\omega_{p'} = (1, \dots, 1)$ and $m_{p'} = 1$ for all $p' \neq p$, making the statement trivial. Therefore, suppose there exists $\vec{s'}, \vec{s''} \in \mathcal{S}$ such that $\vec{s'}, \vec{s} \neq (1, \dots, 1)$, $s_j = s'_j s''_j$ and $\gcd(\ell(\vec{s'}), \ell(\vec{s''})) = 1$. (This is an analogue of writing $\vec{s}$ as a product of coprime factors).

Define $m' \equiv \ell(\vec{s'})^{-1} \pmod{\ell(\vec{s''})}$ and $m'' \equiv \ell(\vec{s''})^{-1} \pmod{\ell(\vec{s'})}$. Moreover, let

$$\vec{\omega'} = (\omega'_1, \dots, \omega'_n) = (\omega_1 \pmod{s'_1}, \dots, \omega_n \pmod{s'_n}) \in \Omega_{\vec{s'}}$$

$$\vec{\omega''} = (\omega''_1, \dots, \omega''_n) = (\omega_1 \pmod{s''_1}, \dots, \omega_n \pmod{s''_n}) \in \Omega_{\vec{s''}}$$

Then there exists some polynomial H such that

$$(F^{(\vec{\omega'})}_{(\vec{s'})}(X))^{m''\ell(\vec{s''})}(F^{(\vec{\omega''})}_{(\vec{s''})}(X))^{m'\ell(\vec{s'})} = F^{(\vec{\omega})}_{(\vec{s})}(X)\,(H(X))^{\ell(\vec{s})}$$

Moreover, all the factors that appear in $F^{(\vec{\omega})}_{(\vec{s})}(X)$ appear in either $F^{(\vec{\omega'})}_{(\vec{s'})}(X)$ or $F^{(\vec{\omega''})}_{(\vec{s''})}(X)$. That is to say, the former is zero at x if and only if one of the latter are zero at x. Therefore,

$$\chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right) = \chi^{m''}_{\ell(\vec{s'})}\left(F^{(\vec{\omega'})}_{(\vec{s'})}(x)\right)\chi^{m'}_{\ell(\vec{s''})}\left(F^{(\vec{\omega''})}_{(\vec{s''})}(x)\right)$$

Iterating this process then we get the result with the Chinese Remainder Theorem.

□

Corollary 4.4.3. *$\epsilon_{\vec{s},\vec{\omega}}$ uniquely determines and is uniquely determined by $\epsilon_{\vec{s}_p,\vec{\omega}_p}$ for all $p|r_n$.*

Proof. Straight forward from (4.4.2).

□

Lemma 4.4.4. *For any $\vec{s} = (s_1, \ldots, s_n) \in \mathcal{S}$, define $\vec{\sigma}_j$ to be the vector in $\mathcal{S}$ that has s_j in the j^{th} coordinate and 1 everywhere else. Let $\vec{1} = (1, \ldots, 1) \in \Omega_{\vec{\sigma}_j} \subset \Omega_{\vec{s}}$. If $\{\epsilon_{\vec{s},\vec{\omega}} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$ is admissible and $\epsilon_{\vec{\sigma}_j,\vec{1}} \neq 0$ for all j then*

$$\epsilon_{\vec{s},\vec{\omega}} = \prod_{j=1}^{n} \epsilon_{\vec{\sigma}_j,\vec{1}}^{\omega_j}$$

Proof. Recall that $F_j(X) = \prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(X)$. For all $s_j|r_j$ define

$$F_{j,s_j}(X) := \prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}(X)^{\alpha_j \pmod{s_j}} = F_{(\vec{\sigma}_j)}^{(\vec{1})}(X).$$

Therefore, there exists an H such that

$$\prod_{j=1}^{n} F_{j,s_j}(X)^{\frac{\ell(\vec{s})}{s_j}\omega_j} = F_{(\vec{s})}^{(\vec{\omega})}(X)H(X)^{\ell(\vec{s})}.$$

Hence, if $F_{j,s_j}(x) \neq 0$ for all j, then $H(x) \neq 0$ and

$$\epsilon_{\vec{s},\vec{\omega}} = \chi_{\ell(\vec{s})}(F_{(\vec{s})}^{(\vec{\omega})}(x)) = \prod_{j=1}^{n} \chi_{s_j}^{\omega_j}(F_{j,s_j}(x)) = \prod_{j=1}^{n} \epsilon_{\vec{\sigma}_j,\vec{1}}^{\omega_j}.$$

□

As in the cyclic case, it will be important to keep track of when and how an admissible set can have zero values. Fix a $\vec{\beta}$ such that $f_{\vec{\beta}}(x) = 0$. Then $F_{(\vec{s})}^{(\vec{\omega})}(x) = 0$ if and only if $f_{\vec{\beta}}(X)|F_{(\vec{s})}^{(\vec{\omega})}(X)$ if and only if

$$\sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j\beta_j \not\equiv 0 \pmod{\ell(\vec{s})}.$$

Define the set

$$A_{\vec{\beta}} := \{(\vec{s},\vec{\omega}) : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j\beta_j \equiv 0 \pmod{\ell(\vec{s})}\}.$$

Then $F_{(\vec{s})}^{(\vec{\omega})}(x) \neq 0$ if and only if $(\vec{s},\vec{\omega}) \in A_{\vec{\beta}}$.

There is a natural bijective correspondence from $A_{\vec{\beta}}$ to

$$\{\vec{\omega} \in \mathcal{R}^\dagger : \sum_{j=1}^{n} \frac{r_n}{r_j}\omega_j\beta_j \equiv 0 \pmod{r_n}\}$$

which sends $(\vec{s}, \vec{\omega}) \to (\frac{r_1}{s_1}\omega_1, \ldots, \frac{r_n}{s_n}\omega_n)$ where

$$\mathcal{R}^\dagger = [1, \ldots, r_1] \times \cdots \times [1, \ldots, r_n].$$

We will equate the definition of $A_{\vec{\beta}}$ with this set and either talk about $(\vec{s}, \vec{\omega}) \in A_{\vec{\beta}}$ using the first definition or just $\vec{\omega} \in A_{\vec{\beta}}$ using the second definition depending on whichever is the most convenient.

Let $\mathcal{R}' = \mathcal{R} \cup \{(0, \ldots, 0)\}$ and define an equivalence relationship of $\mathcal{R}'$ by $\vec{\beta} \sim \vec{\beta}'$ if and only if $A_{\vec{\beta}} = A_{\vec{\beta}'}$. Let $\tilde{\mathcal{R}} = \mathcal{R}'/\sim$ and write $[\vec{\beta}] \in \tilde{\mathcal{R}}$ as the equivalence class of $\vec{\beta}$ in $\tilde{\mathcal{R}}$.

Definition 4.4.5. An admissible set

$$\{\epsilon_{\vec{s},\vec{\omega}} \in \mu_{\ell(\vec{s})} \cup \{0\}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$$

is called $[\vec{\beta}]$**-admissible** if $\epsilon_{\vec{s},\vec{\omega}} = 0$ if and only if $(\vec{s}, \vec{\omega}) \notin A_{\vec{\beta}}$.

Remark 4.4.6. If $\{\epsilon_{\vec{s},\vec{\omega}} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$ is $[\vec{0}]$-admissible then $\epsilon_{\vec{s},\vec{\omega}} \neq 0$ for all $\vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}$.

It will be useful later to classify the equivalence classes of $\tilde{\mathcal{R}}$. Towards this, for all $p|r_n$, define

$$\mathcal{S}_p = \{\vec{s} = (s_1, \ldots, s_n) : s_j = p^{v_j}, 0 \leq v_j \leq v_p(r_j)\} \subset \mathcal{S}$$

$$A_{\vec{\beta},p} := \{(\vec{s}, \vec{\omega}) : \vec{s} \in \mathcal{S}_p, \vec{\omega} \in \Omega_{\vec{s}}, \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j\beta_j \equiv 0 \pmod{\ell(\vec{s})}\}$$

$$= \{\vec{\omega} \in \mathcal{R}_p^\dagger : \sum_{j=1}^{n} p^{v_p(r_n)-v_p(r_j)}\omega_j\beta_j \equiv 0 \pmod{p^{v_p(r_n)}}\}$$

where we identify the two sets under the map $(\vec{s}, \vec{\omega}) \to (\frac{p^{v_p(r_1)}}{s_1}\omega_1, \ldots, \frac{p^{v_p(r_n)}}{s_n}\omega_n)$ and $\mathcal{R}_p^\dagger = [1, \ldots, p^{v_p(r_1)}] \times \cdots \times [1, \ldots, p^{v_p(r_n)}]$.

Then say $\vec{\beta} \sim_p \vec{\beta}'$ if $A_{\vec{\beta},p} = A_{\vec{\beta}',p}$. Clearly, $\vec{\beta} \sim \vec{\beta}'$ if and only if $\vec{\beta} \sim_p \vec{\beta}'$ for all $p|r_n$.

Lemma 4.4.7. *If $\vec{\beta} \sim_p \vec{\beta}'$ then $v_p((\beta_j, r_j)) = v_p((\beta_j', r_j))$ for $j = 1, \ldots, n$.*

Proof. Let $\vec{s} = (1, \ldots, 1, p^{v_p((\beta_j, r_j))}, 1, \ldots, 1)$, where the $p^{v_p((\beta_j, r_j))}$ is in the j^{th} coordinate. Then $(\vec{s}, (1, \ldots, 1)) \in A_{\vec{\beta},p} = A_{\vec{\beta}',p}$. This implies that

$$\beta_j' \equiv 0 \pmod{p^{v_p((\beta_j, r_j))}}$$

And so $v_p(\beta_j') \geq v_p((\beta_j, r_j))$. If $v_p(\beta_j) \geq v_p(r_j)$ then $v_p((\beta, r_j)) = v_p(r_j)$. Hence $v_p((\beta_j', r_j)) = r_j = v_p((\beta_j, r_j))$. If $v_p(\beta_j) < v_p(r_j)$ then $v_p(\beta_j') \geq v_p(\beta_j)$. Similarly, we can show that $v_p(\beta_j) \geq v_p((\beta_j', r_j))$. Thus $v_p((\beta_j', r_j)) < v_p(r_j)$. Therefore, $v_p((\beta_j', r_j)) = v_p(\beta_j')$ and we get out result.

□

Lemma 4.4.8. *$\vec{\beta} \sim_p \vec{\beta}'$ if and only if there exists an $1 \leq m \leq p^{\max(0, \max_j(v_p(\frac{r_j}{\beta_j})))}$, $(m, p) = 1$ such that $\beta_j' \equiv m\beta_j \pmod{p^{v_p(r_j)}}$ for all j.*

Proof. Suppose $\vec{\beta} \sim_p \vec{\beta}'$. Then since $v_p(\beta_j, r_j) = v_p(\beta_j', r_j)$, we can find an m_j such that $1 \leq m_j \leq p^{\max(0, v_p(\frac{r_j}{\beta_j}))}$, $(m_j, p) = 1$ and

$$\beta_j' \equiv m_j\beta_j \pmod{p^{v_p(r_j)}}.$$

Moreover, for all j, define γ_j to be such that

$$\beta_j = p^{v_p(\beta_j)}\gamma_j.$$

Let k be such that $\min(v_p(\frac{r_n}{r_j}\beta_j)) = v_p(\frac{r_n}{r_k}\beta_k)$. Fix a j and let $1 \leq \omega_k \leq p^{v_p(r_k)}$ be smallest such that

$$\omega_k \equiv -p^{v_p(\frac{r_k\beta_j}{r_j\beta_k})}\gamma_j\gamma_k^{-1} \pmod{p^{\max(0, v_p(\frac{r_k}{\beta_k}))}}.$$

Define $\vec{\omega} \in \mathcal{R}_p^\dagger$ such that $\omega_j = 1$, ω_k is as above and $\omega_\ell = p^{v_p(r_\ell)}$ otherwise. Then $\vec{\omega} \in A_{\vec{\beta},p} = A_{\vec{\beta}',p}$. Hence,

$$\begin{aligned} 0 &\equiv p^{v_p(\frac{r_n}{r_k})}\beta_k'\omega_k + p^{v_p(\frac{r_n}{r_j})}\beta_j' \equiv p^{v_p(\frac{r_n}{r_k})}\beta_k m_k\omega_k + p^{v_p(\frac{r_n}{r_j})}\beta_j m_j \\ &\equiv -p^{v_p(\frac{r_n}{r_k}\beta_k)}\gamma_k m_k p^{v_p(\frac{r_k\beta_j}{r_j\beta_k})}\gamma_j\gamma_k^{-1} + p^{v_p(\frac{r_n}{r_j}\beta_j)}\gamma_j m_j \\ &\equiv p^{v_p(\frac{r_n}{r_j}\beta_j)}\gamma_j(m_j - m_k) \pmod{p^{v_p(r_n)}} \end{aligned}$$

Therefore,

$$m_j \equiv m_k \pmod{p^{\max(0, v_p(\frac{r_j}{\beta_j}))}}.$$

Hence,

$$\beta'_j \equiv m_j\beta_j \equiv m_k\beta_j \pmod{p^{v_p(r_j)}}.$$

So, setting $m = m_k$ gives our desired result.

Conversely, suppose there exists an $1 \leq m \leq p^{\max(0,\max_j(v_p(\frac{r_j}{\beta_j})))}$, $(m,p) = 1$ such that $\beta'_j \equiv m\beta_j \pmod{p^{v_p(r_j)}}$ for all j. Let $\vec{\omega} \in A_{\vec{\beta},p}$. Then

$$\sum_{j=1}^{n} p^{v_p(r_n)-v_p(r_j)}\omega_j\beta'_j \equiv \sum_{j=1}^{n} p^{v_p(r_n)-v_p(r_j)}\omega_j m\beta_j \equiv m\sum_{j=1}^{n} p^{v_p(r_n)-v_p(r_j)}\omega_j\beta_j \equiv 0 \pmod{p^{v_p(r_n)}}.$$

Therefore, $\vec{\omega} \in A_{\vec{\beta}',p}$. So $A_{\vec{\beta},p} \subset A_{\vec{\beta}',p}$. However, since $(m,p) = 1$, we can find an m' such that $\beta_j \equiv m'\beta'_j$. From which we get $A_{\vec{\beta}',p} \subset A_{\vec{\beta},p}$ and therefore $A_{\vec{\beta},p} = A_{\vec{\beta}',p}$ and $\vec{\beta} \sim_p \vec{\beta}'$.

□

Note that

$$\prod_{p|r_n} p^{\max(0,\max_j(v_p(\frac{r_j}{\beta_j})))} = \operatorname{lcm}\left(\frac{r_j}{(r_j,\beta_j)}\right) = e(\vec{\beta}).$$

For any natural number m and $\vec{\beta} \in \mathcal{R}'$, define $m\vec{\beta} = (m\beta_1 \pmod{r_1}, \ldots, m\beta_n \pmod{r_n})$.

Corollary 4.4.9. *$\vec{\beta} \sim \vec{\beta}'$ if and only if there exists an $1 \leq m \leq e(\vec{\beta})$, $(m, e(\vec{\beta})) = 1$ such that $\vec{\beta}' = m\vec{\beta}$.*

Proof. Suppose $\vec{\beta} \sim \vec{\beta}'$. Then $\vec{\beta} \sim_p \vec{\beta}'$ for all $p|r_n$ and we can find an $1 \leq m_p \leq p^{\max(0,\min_j(v_p(\frac{r_n}{r_j}\beta_j)))}$, $(m_p,p) = 1$ such that $\beta'_j \equiv m_p\beta_j \pmod{p^{v_p(r_j)}}$. Let $1 \leq m \leq \prod_{p|r_n} p^{\max(0,\min_j(v_p(\frac{r_n}{r_j}\beta_j)))}$, $(m,r_n) = 1$ such that $m \equiv m_p \pmod{p^{\max(0,\min_j(v_p(\frac{r_n}{r_j}\beta_j)))}}$ for all $p|r_n$. Then $\beta'_j \equiv m\beta_j \pmod{r_j}$ and $\vec{\beta}' = m\vec{\beta}$

Conversely, suppose such an m exists. Then let $m_p \equiv m \pmod{p^{\max(0,\min_j(v_p(\frac{r_n}{r_j}\beta_j)))}}$. Then $\beta_j \equiv m_p\beta'_j \pmod{p^{v_p(r_n)}}$. Thus $\vec{\beta} \sim_p \vec{\beta}'$ for all p and therefore $\vec{\beta} \sim \vec{\beta}'$.

□

Corollary 4.4.10. *There are $\phi(e(\vec{\beta}))$ different $\vec{\beta}'$ such that $\vec{\beta}' \sim \vec{\beta}$.*

Proof. It is easy to see that, by construction, all the $m\vec{\beta}$ are distinct for $1 \leq m \leq e(\vec{\beta})$, $(m, e(\vec{\beta})) = 1$.

□

Lemma 4.4.11. $|A_{\vec{\beta},p}| = p^{v_p(|G|)-v_p(e(\vec{\beta}))}$

Proof. Consider the map

$$\begin{aligned}\phi_{\vec{\beta}}: \quad \mathbb{Z}/p^{v_p(r_1)}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{v_p(r_n)}\mathbb{Z} &\to \mathbb{Z}/p^{v_p(r_n)}\mathbb{Z} \\ (x_1, \ldots, x_n) &\to \textstyle\sum_{j=1}^{n} p^{v_p(r_n)-v_p(r_j)}\beta_j x_j\end{aligned}$$

Then $A_{\vec{\beta},p} = \ker(\phi_{\vec{\beta}})$. Let $1 \leq k \leq n$ such that $v_p(\frac{r_n}{r_k}\beta_k) = \min(v_p(\frac{r_n}{r_j}\beta_j))$. Then $\mathrm{Im}(\phi_{\vec{\beta}}) \subset \mathbb{Z}/p^{\max(0,v_p(\frac{r_k}{\beta_k}))}\mathbb{Z}$. Moreover

$$\phi_{\vec{\beta}}(0, \ldots, 0, x_k, 0, \ldots, 0) = p^{v_p(\frac{r_n}{r_k}\beta_k)}\gamma_k x_k$$

where $\beta_k = p^{v_p(\beta_k)}\gamma_k$. Therefore, since $(\gamma_k, p) = 1$, we get that $\mathrm{Im}(\phi_{\vec{\beta}}) = \mathbb{Z}/p^{\max(0,v_p(\frac{r_k}{\beta_k}))}\mathbb{Z}$. Hence

$$|A_{\vec{\beta},p}| = |\ker(\phi_{\vec{\beta}})| = \frac{p^{v_p(|G|)}}{|\mathrm{Im}(\phi_{\vec{\beta}})|} = p^{v_p(|G|)-\max(0,v_p(\frac{r_k}{\beta_k}))} = p^{v_p(|G|)-v_p(e(\vec{\beta}))}.$$

□

Corollary 4.4.12. $|A_{\vec{\beta}}| = \frac{|G|}{e(\vec{\beta})}$

Proof.

$$|A_{\vec{\beta}}| = \prod_{p|r_n} |A_{\vec{\beta},p}| = \prod_{p|r_n} p^{v_p(|G|)-v_p(e(\vec{\beta}))} = \frac{|G|}{e(\vec{\beta})}.$$

□

4.5 Value Taking

In this section we will determine the size of the set

$$\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1, \ldots, \ell\} \tag{4.5.1}$$

where for $i = 1, \ldots, \ell$, the set

$$\{\epsilon_{\vec{s},\vec{\omega},i} \in \mu_{\ell(\vec{s})} \cup \{0\} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$$

is admissible.

Define $\vec{\rho}_j = (1, \dots, r_j, \dots, 1) \in \mathcal{S}$ where the r_j is in the j^{th} coordinate. Denote $\vec{1} = (1, \dots, 1)$. Then

$$F_j(X) := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j} = F_{(\vec{\rho}_j)}^{(\vec{1})}(X).$$

By Lemmas 4.4.2 and 4.4.4, we get that if $\epsilon_{\vec{s},\vec{\omega},i} \neq 0$ for all $\vec{s} \in \mathcal{S}$, $\vec{\omega} \in \Omega_{\vec{s}}$ and $i = 1, \dots, \ell$, then the values of $\epsilon_{\vec{s},\vec{\omega},i}$ will be uniquely determined by the values of $\epsilon_{\vec{\rho}_j,\vec{1},i}$ for $j = 1, \dots, n$, $i = 1, \dots, \ell$. That is, by (2.1.13)

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(F_{(\vec{s})}^{(\vec{\omega})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1, \dots, \ell\}| \\
&= |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{r_j}(F_j(x_i)) = \epsilon_{\vec{\rho}_j,\vec{1},i}, i = 1 \dots, \ell, j = 1, \dots, n\}| \\
&= \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{\ell} \left(1 + O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).
\end{aligned}$$

Let us now determine the size of the set if some of the $\epsilon_{\vec{s},\vec{\omega},i}$ can be zero.

Proposition 4.5.1. *Let $\{\epsilon_{\vec{s},\vec{\omega},i} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$ be an admissible set for $1 \leq i \leq \ell$ such that*

$$m_{[\vec{\beta}]} := |\{1 \leq i \leq \ell : \{\epsilon_{\vec{s},\vec{\omega},i} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\} \text{ is } [\vec{\beta}] - \text{admissible}\}|$$

then

$$\begin{aligned}
&|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(F_{(\vec{s})}^{(\vec{\omega})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1, \dots, \ell\}| \\
&= \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \prod_{\substack{[\vec{\beta}] \in \tilde{\mathcal{R}} \\ [\vec{\beta}] \neq [\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{[\vec{0}]}} \left(1 + O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).
\end{aligned}$$

Proof. For every $[\vec{\beta}] \in \tilde{\mathcal{R}}$, define

$$M_{[\vec{\beta}]} = \{1 \leq i \leq \ell : \{\epsilon_{\vec{d},\vec{i},i} : \vec{d} \in D, \vec{i} \in I_{\vec{d}}\} \text{ is } [\vec{\beta}]\text{-admissible}\}$$

Then $m_{[\vec{\beta}]} = |M_{[\vec{\beta}]}|$ and

$$\sum_{[\vec{\beta}] \in \tilde{\mathcal{R}}} m_{[\vec{\beta}]} = \ell.$$

Moreover, if $i \in M_{[\vec{\beta}]}$ for $\vec{\beta} \neq \vec{0}$ then $f_{\vec{\beta}'}(x_i) = 0$ for some $\vec{\beta}' \sim \vec{\beta}$.

For all $\vec{\beta} \neq \vec{0}$, fix a partition of $M_{[\vec{\beta}]}$ as

$$M_{[\vec{\beta}]} = \bigcup_{\vec{\beta}' \sim \vec{\beta}} M_{\vec{\beta}'} = \bigcup_{\vec{\beta}' \sim \vec{\beta}} \{1 \leq i \leq \ell : f_{\vec{\beta}'}(x_i) = 0\}$$

and let $m_{\vec{\beta}} = |M_{\vec{\beta}}|$.

For all $\vec{\beta} \in \mathcal{R}$ define $g_{\vec{\beta}}(X)$ as

$$f_{\vec{\beta}}(X) = g_{\vec{\beta}}(X) \prod_{i \in M_{\vec{\beta}}} (X - x_i).$$

Likewise, define $G^{(\vec{\omega})}_{(\vec{s})}(X)$ as the corresponding products of the $g_{\vec{\alpha}}(X)$. Recall, for any $\vec{s} \in \mathcal{S}$, we let $\vec{\sigma}_j \in \mathcal{S}$ be the vector that has s_j in the j^{th} coordinate and 1 everywhere else. Then

$$G_{j,s_j}(X) := \prod_{\vec{\alpha} \in \mathcal{R}} g_{\vec{\alpha}}(X)^{\alpha_j \pmod{s_j}} = G^{(\vec{1})}_{(\vec{\sigma}_j)}(X)$$

where we use the convention that $G_{j,1}(X) = 1$.

Since $g_{\vec{\alpha}}(x_i) \neq 0$ for all $1 \leq i \leq \ell$ we get that $G^{(\vec{\omega})}_{(\vec{s})}(x_i) \neq 0$ for all $1 \leq i \leq \ell$ and hence, by Lemmas 4.4.2 and 4.4.4, $\chi_{\ell(\vec{s})}\left(G^{(\vec{\omega})}_{(\vec{s})}(x_i)\right)$ will be determined by $\chi_{r_j}\left(G_{j,r_j}(x_i)\right)$, for $j = 1, \ldots, n$. Moreover,by Corollary 4.4.3 these will be determined by

$$\chi_{p^{v_p(r_j)}}\left(G_{j,p^{v_p(r_j)}}(x_i)\right) \text{ for all } p | r_n,\ j = 1, \ldots, n$$

Now fix an $i \in M_{\vec{\beta}}$. If $(\vec{s}, \vec{\omega}) \in A_{\vec{\beta}}$, then

$$F^{(\vec{\omega})}_{(\vec{s})}(X) = G^{(\vec{\omega})}_{(\vec{s})}(X) H(X)$$

for some $H(X)$ such that $H(x_i) \neq 0$. Moreover, $H(X)$ depends only on the choice of partitions of the $M_{[\vec{\beta}]}$. Therefore, for a fixed partition, we see that $\chi_{\ell(\vec{s})}(G^{(\vec{\omega})}_{(\vec{s})}(x_i))$ will be determined by $\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i))$ for all $(\vec{s}, \vec{\omega}) \in A_{\vec{\beta}}$. It remains to determine how many choices there are for $\chi_{\ell(\vec{s})}(G^{(\vec{\omega})}_{(\vec{s})}(x_i))$ such that $(\vec{s}, \vec{\omega}) \notin A_{\vec{\beta}}$.

Fix a $p | r_n$ and let k be such that

$$\min\left(v_p\left(\frac{r_n}{r_j}\beta_j\right)\right) = v_p\left(\frac{r_n}{r_k}\beta_k\right)$$

Then I claim that if we know $\chi_{p^{v_p(r_k)}}(G_{k,p^{v_p(r_k)}}(x_i))$ then we know $\chi_{p^{v_p(r_j)}}(G_{j,p^{v_p(r_j)}}(x_i))$ for all $1 \leq j \leq n$. If we write $\beta_j = p^{v_p(\beta_j)}\gamma_j$, $r_j = p^{v_p(r_j)}s_j$ where $(\gamma_j, p) = (s_j, p) = 1$ and let

$$\omega'_k \equiv \gamma_k^{-1}\gamma_j p^{v_p\left(\frac{r_k\beta_j}{r_j\beta_k}\right)} \pmod{p^{\max(v_p\left(\frac{r_k}{\beta_k}\right),0)}}$$

then we see that

$$\frac{r_n}{r_k}\beta_k\omega'_k s_k + \frac{r_n}{r_j}\beta_j s_j \equiv 0 \pmod{r_n}$$

Therefore, defining $\vec{\omega} \in \mathcal{R}^\dagger$ as $\omega_j = s_j$, $\omega_h = r_h$, $h \neq j,k$ and $\omega_k = \omega_k' s_k$, then $\vec{\omega} \in A_{\vec{\beta}}$. So, defining $\vec{p} = (p^{v_p(r_1)}, \ldots, p^{v_p(r_n)})$ we get by Lemma 4.4.4,

$$\chi_{p^{v_p(r_n)}}\left(G_{(\vec{p})}^{(\vec{\omega})}(x_i)\right) = \chi_{p^{v_p(r_k)}}^{\omega_k'}\left(G_{k,p^{v_p(r_k)}}(x_i)\right)\chi_{p^{v_p(r_j)}}\left(G_{j,p^{v_p(r_j)}}(x_i)\right)$$

Moreover, as stated above, $\chi_{p^{v_p(r_n)}}\left(G_{(\vec{p})}^{(\vec{\omega})}(x_i)\right)$ is fixed by $\chi_{p^{v_p(r_n)}}\left(F_{(\vec{p})}^{(\vec{\omega})}(x_i)\right)$ and our choices of $M_{\vec{\beta}}$. Hence knowing $\chi_{p^{v_p(r_k)}}(G_{k,p^{v_p(r_k)}}(x_i))$ fixes $\chi_{p^{v_p(r_j)}}(G_{j,p^{v_p(r_j)}}(x_i))$.

Therefore, to determine the number of possible values for $\chi_{p^{v_p(r_j)}}(G_{j,p^{v_p(r_j)}}(x_i))$, $j = 1,\ldots,n$, it is enough to determine the possible values for $\chi_{p^{v_p(r_k)}}(G_{k,p^{v_p(r_k)}}(x_i))$.

Finally, since $\chi_{p^{v_p(\beta_k)}}(G_{k,p^{v_p(\beta_k)}}(x_i))$ is determined by $\chi_{p^{v_p(\beta_k)}}(F_{k,p^{v_p(\beta_k)}}(x_i))$ and the choice of $M_{\vec{\beta}}$ there are $p^{\max(v_p\left(\frac{r_k}{\beta_k}\right),0)}$ choices for $\chi_{p^{v_p(r_k)}}(G_{k,p^{v_p(r_k)}}(x_i))$.

All together, therefore, there are

$$\prod_{p|r_n} p^{\max(0,\max_j(v_p(\frac{r_j}{\beta_j})))} = \operatorname*{lcm}_{j=1,\ldots,n}\left(\frac{r_j}{(r_j,\beta_j)}\right) = e(\vec{\beta})$$

different choices for

$$\chi_{p^{v_p(r_j)}}\left(G_{j,p^{v_p(r_j)}}(x_i)\right) \text{ for all } p|r_n,\ j = 1,\ldots,n$$

and hence $e(\vec{\beta})$ different choices for

$$\chi_{\ell(\vec{s})}(G_{(\vec{s})}^{(\vec{\omega})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}$$

for a fixed choice of the $M_{\vec{\beta}}$

Therefore,

$$|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(F_{(\vec{s})}^{(\vec{\omega})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1,\ldots,\ell\}|$$

$$= \sum_{M_{\vec{\beta}}} \sum_{\epsilon'_{\vec{s},\vec{\omega}}} |\{(g_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d'}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(G_{(\vec{s})}^{(\vec{\omega})}(x_i)) = \epsilon'_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1,\ldots,\ell\}|$$

where the first sum is over all the partitions $M_{[\vec{\beta}]} = \bigcup_{\vec{\beta} \sim \vec{\beta'}} M_{\vec{\beta}}$, the second sum is over all $e(\vec{\beta})$ choices of $\chi_{\ell(\vec{s})}(G_{(\vec{s})}^{(\vec{\omega})}(x_i))$ and $\vec{d'}(\vec{\alpha})$ is the vector such that $d'(\vec{\alpha}) = d(\vec{\alpha}) - m_{\vec{\alpha}}$. Now since $\epsilon'_{\vec{s},\vec{\omega},i} \neq 0$ for all $\vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}$, $i = 1,\ldots,\ell$, we get the above line is equal to

$$\sum_{M_{\vec{\beta}}} \sum_{\epsilon'_{\vec{s},\vec{\omega}}} \frac{L_{|G|-2} q^{\sum d'(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{\ell} \left(1 + O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$= \sum_{M_{\vec{\beta}}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} e(\vec{\beta}) \frac{L_{|G|-2} q^{\sum (d(\vec{\alpha})-m_{\vec{\alpha}})}}{\zeta_q(2)^{|G|-1}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{\ell} \left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$= \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \sum_{M_{\vec{\beta}}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} \left(\frac{e(\vec{\beta})}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{[\vec{0}]}} \left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$= \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{[\vec{0}]}} \left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

where the last equality comes from Corollary 4.4.3 that states that there are $\phi(e(\vec{\beta}))$ different $\vec{\beta}'$ such that $\vec{\beta}' \sim \vec{\beta}$.

□

Recall that x_{q+1} is the point at infinity and if $(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$, then

$$F^{(\vec{\omega})}_{(\vec{s})}(x_{q+1}) = \begin{cases} 0 & \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j d_j \not\equiv 0 \pmod{\ell(\vec{s})} \\ c^{(\vec{\omega})}_{(\vec{s})} & \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j}\omega_j d_j \equiv 0 \pmod{\ell(\vec{s})} \end{cases}.$$

Proposition 4.5.2. *Let $\{\epsilon_{\vec{s},\vec{\omega},i} : \vec{s}\in\mathcal{S}, \vec{\omega}\in\Omega_{\vec{s}}\}$ be an admissible set for $1\leq i\leq q+1$ such that*

$$m_{[\vec{\beta}]} := |\{1\leq i\leq q+1 : \{\epsilon_{\vec{s},\vec{\omega},i} : \vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}\} \text{ is } [\vec{\beta}]-\text{admissible}\}|$$

then

$$|\{(\vec{c},(f_{\vec{\alpha}}))\in\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}, i=1,\dots,q+1\}|$$

$$= \frac{(q-1)^n(q+|G|-1)}{q} \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{[\vec{0}]}} \times$$
$$\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).$$

Remark 4.5.3. Notice that we are looking at $(\vec{c},(f_{\vec{\alpha}}))\in\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$. That is, when we add in the point at infinity, we must consider the whole irreducible coarse moduli space.

Proof. **Case 1:** $\epsilon_{\vec{s},\vec{\omega},q+1} \neq 0$ for all $\vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}$

This means that $(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$ and $\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_{q+1}))$ will be determine by $\chi_{r_j}(F_j(x_{q+1}))$, $j = 1,\dots,n$. Moreover, $\chi_{r_j}(c_j) = \chi_{r_j}(F_j(x_{q+1}))$, so c_j has $(q-1)/r_j$ choices for all j. That is

$$\begin{aligned}
&|\{(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, 1 \leq i \leq q+1\}| \\
&= \sum_{c_j} |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, 1 \leq i \leq q\}|
\end{aligned}$$

$$= \sum_{c_j} \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{\vec{0}}-1} \left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$= \frac{(q-1)^n(q+|G|-1)}{q} \frac{L_{|G|-2} q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}} \prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}} \\ [\vec{\beta}]\neq[\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}} \left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{\vec{0}}} \times$$

$$\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

where the sum is over all c_j such that $\chi_{r_j}(c_j) = \chi_{r_j}(F_j(x_{q+1}))$.

Case 2: the set $\{\epsilon_{\vec{s},\vec{\omega},q+1} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}\}$ is $[\vec{\beta}]$-admissible for some $[\vec{\beta}] \in \tilde{\mathcal{R}}$, $[\vec{\beta}] \neq [\vec{0}]$.

This means that $\deg(F_j) \equiv \beta'_j \pmod{r_j}$ for some $\vec{\beta}' \sim \vec{\beta}$ and that $(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}^{\vec{\beta}'}_{\vec{d}(\vec{\alpha})}$. Fix a $p|r_n$ and let k be such that $\max(v_p(\frac{r_n}{r_j}\beta'_j)) = v_p(\frac{r_n}{r_k}\beta'_k)$. Then $\chi_{p^{v_p(\beta_k)}}(F_{k,p^{v_p(\beta_k)}}(x_{q+1})) = \chi_{p^{v_p(\beta_k)}}(c_k)$. So c_k has $\frac{q-1}{p^{v_p(\beta_k)}}$ choices.

Now suppose $\beta'_j = p^{b_j}\gamma_j$ and let ω_k be such that

$$\omega_k \equiv \gamma_k^{-1}\gamma_j p^{v_p(r_k\beta_j/r_j\beta_k)} \pmod{p^{v_p(r_k/\beta_k)}}.$$

then $\chi_{p^{v_p(r_j)}}(c_k^{\omega_k}c_j) \neq 0$ will be fixed. Therefore, for a choice of c_k there are $\frac{q-1}{p^{v_p(r_j)}}$ choices for c_j that satisfy this property.

Likewise for another $p'|r_n$, $p \neq p'$, let k' be such that $\max(v_{p'}(\frac{r_n}{r_j}\beta'_j)) = v_{p'}(\frac{r_n}{r_{k'}}\beta'_{k'})$. Then the number of choices for $c_{k'}$ will be divided by $(p')^{v_{p'}(\beta'_{k'})}$ whereas the number of choice for c_j, $j \neq k'$ will be divided by $(p')^{v_{p'}(\beta'_j)}$. Hence, the number of choices for the c_j will be

$$\frac{(q-1)^n}{\prod_{p|r_n}\left(p^{v_p(\beta_k)}\prod_{j\neq k}p^{v_p(r_j)}\right)} = \prod_{j=1}^{n}\frac{e(\vec{\beta})(q-1)}{r_j}$$

Moreover, $m_{[\vec{\beta}]}$ goes to $m_{[\vec{\beta}]} - 1$. So,

$$|\{(\vec{c},(f_{\vec{\alpha}}))\in\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}:\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i))=\epsilon_{\vec{s},\vec{\omega},i},\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}},1\le i\le q+1\}|$$

$$=\prod_{j=1}^{n}\frac{e(\vec{\beta})(q-1)}{r_j}\sum_{\vec{\beta}'\sim\vec{\beta}}|\{(f_{\vec{\alpha}})\in\mathcal{F}^{\vec{\beta}'}_{\vec{d}(\vec{\alpha})}:\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i))=\epsilon_{\vec{s},\vec{\omega},i},\vec{s}\in\omega,\vec{\omega}\in\Omega_{\vec{s}},1\le i\le q\}|$$

$$=\prod_{j=1}^{n}\frac{e(\vec{\beta})(q-1)}{r_j}\sum_{\vec{\beta}'\sim\vec{\beta}}\frac{L_{|G|-2}q^{\sum d(\vec{\alpha})-1}}{\zeta_q(2)^{|G|-1}}\prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}}\\ [\vec{\beta}]\neq[\vec{0}]}}\left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}}\times$$

$$\left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{-1}\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{\vec{0}}}\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$=\frac{(q-1)^n(q+|G|-1)}{q}\frac{L_{|G|-2}q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}}\prod_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}}\\ [\vec{\beta}]\neq[\vec{0}]}}\left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}}\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{\vec{0}}}\times$$

$$\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).$$

Therefore, regardless of what happens at x_{q+1}, we get the same result.

□

Corollary 4.5.4. *Let $\{\epsilon_{\vec{s},\vec{\omega},i}:\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}\}$ be an admissible set for $1\le i\le q+1$ such that*

$$m_{[\vec{\beta}]}:=|\{1\le i\le q+1:\{\epsilon_{\vec{s},\vec{\omega},i}:\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}\}\ \textit{is}\ [\vec{\beta}]-\textit{admissible}\}|$$

then

$$\frac{|\{(\vec{c},(f_{\vec{\alpha}}))\in\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}:\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i))=\epsilon_{\vec{s},\vec{\omega},i},\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}},i=1,\dots,q+1\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

$$=\prod_{\substack{\vec{\beta}\in\mathcal{R}'\\ [\vec{\beta}]\neq[\vec{0}]}}\left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q+|G|-1)}\right)^{m_{[\vec{\beta}]}}\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_{[\vec{0}]}}\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).$$

Proof. The same reasoning as in the proof of Proposition 4.5.2 shows that

$$|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|=\frac{(q-1)^n(q+|G|-1)}{q}\frac{L_{|G|-2}q^{\sum d(\vec{\alpha})}}{\zeta_q(2)^{|G|-1}}\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

and the result follows from there. □

4.6 Proof of Theorem 1.4.1

For any $(\vec{c},(f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}$ and $x \in \mathbb{P}^1(\mathbb{F}_q)$,

$$\sum_{\vec{s}\in\mathcal{S}}\sum_{\vec{\omega}\in\Omega_{\vec{s}}} \chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right) = |\{\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}} : \chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right)\neq 0\}|$$

if $\chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right) = 0$ or 1 for all $\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}$ and 0 otherwise.

Now, if $\{\chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right), \vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}}\}$ is $[\vec{\beta}]$-admissible then

$$|\{\vec{s}\in\mathcal{S},\vec{\omega}\in\Omega_{\vec{s}} : \chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x)\right)\neq 0\}| = |A_{\vec{\beta}}| = \frac{|G|}{e(\vec{\beta})}.$$

Recall that $e(\vec{\beta}) = \operatorname{lcm}\left(\frac{r_j}{(r_j,\beta_j)}\right)|r_n$. Then the number of points lying over $x\in\mathbb{P}^1(\mathbb{F}_q)$ will be $\frac{|G|}{s_n}$ for some $s_n|r_n$.

Proposition 4.6.1. *Let $e_1,\dots,e_{q+1}$ be such that $e_i = 0$ or $e_i = \frac{|G|}{s_{n,i}}$ for some $s_{n,i}|r_n$. For all $s|r_n$ let*

$$m_s = |\{1\le i\le q+1 : e_i = \frac{|G|}{s}\}|$$

and

$$m_0 = |\{1\le i\le q+1 : e_i = 0\}|$$

then

$$|\{(\vec{c},(f_{\vec{\alpha}}))\in\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \sum_{\vec{s}\in\mathcal{S}}\sum_{\vec{\omega}\in\Omega_{\vec{s}}}\chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x_i)\right) = e_i, i=1,\dots,q+1\}|$$

$$= \left(\frac{(|G|-1)(q+|G|)-\sum_{s|r_n}s\phi_G(s)+1}{|G|(q+|G|-1)}\right)^{m_0}\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_1}\prod_{\substack{s|r_n\\ s\neq 1}}\left(\frac{s\phi_G(s)}{|G|(q+|G|-1)}\right)^{m_s}\times$$

$$\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

where $\phi_G(s)$ is the number of elements of G with order s.

Proof. Let

$$M_s = \{1\le i\le q+1 : e_i = \frac{|G|}{s}\}$$

$$M_0 = \{1\le i\le q+1 : e_i = 0\}.$$

If $i \in M_s$, $s \neq 0$, then the set

$$\{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\}$$

will be $[\vec{\beta}]$-admissible for some $\vec{\beta}$ such that $e(\vec{\beta}) = s$. Moreover, if $(\vec{s}, \vec{\omega}) \in A_{\vec{\beta}}$ then $\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = 1$.

Fix a partition of M_s as

$$M_s = \bigcup_{\substack{[\vec{\beta}] \in \tilde{\mathcal{R}} \\ e(\vec{\beta})=s}} M_{[\vec{\beta}]} = \bigcup_{\substack{[\vec{\beta}] \in \tilde{\mathcal{R}} \\ e(\vec{\beta})=s}} \{i \in M_s : \{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\} \text{ is } [\vec{\beta}]\text{-admissible}\}$$

and let $m_{[\vec{\beta}]} = |M_{[\vec{\beta}]}|$.

If $i \in M_0$, then the set

$$\{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\}$$

can be $[\vec{\beta}]$-admissible for any $[\vec{\beta}] \in \tilde{\mathcal{R}}$ as long as at least one of $\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}) \neq 0$ or 1.

Fix a partition of M_0 as

$$M_0 = \bigcup_{[\vec{\beta}] \in \tilde{\mathcal{R}}} M_{0,[\vec{\beta}]} = \bigcup_{[\vec{\beta}] \in \tilde{\mathcal{R}}} \{i \in M_0 : \{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\} \text{ is } [\vec{\beta}]\text{-admissible}\}$$

and let $m_{0,[\vec{\beta}]} = |M_{0,[\vec{\beta}]}|$.

If $i \in M_{[\vec{\beta}]}$ then there is only one choice for the set $\{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\}$. (Namely, $\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = 1$ if $(\vec{s}, \vec{\omega}) \in A_{\vec{\beta}}$ and 0 otherwise.) If $i \in M_{0,[\vec{\beta}]}$, then there will be $|A_{\vec{\beta}}| - 1 = \frac{|G|}{e(\vec{\beta})} - 1$ choices for the set $\{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\}$.

Therefore,

$$\frac{|\{(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_{\vec{s}}} \chi_{\ell(\vec{s})}\left(F^{(\vec{\omega})}_{(\vec{s})}(x_i)\right) = \frac{|G|}{s_{n,i}}, i = 1, \ldots, q+1\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

$$= \sum_{M_{[\vec{\beta}]}} \sum_{M_{0,[\vec{\beta}]}} \sum_{\epsilon_{\vec{s},\vec{\omega},i}} \frac{|\{(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)) = \epsilon_{\vec{s},\vec{\omega},i}, \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_{\vec{s}}, i = 1, \ldots, q+1\}|}{|\hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]}|}$$

where the first two sums are over all the partitions of M_s, $s|r_n$ and M_0, respectively, and the third sum is over all possible choices for $\{\chi_{\ell(\vec{s})}(F^{(\vec{\omega})}_{(\vec{s})}(x_i)), \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega\}$.

$$= \sum_{M_{[\vec{\beta}]}} \sum_{M_{0,[\vec{\beta}]}} \sum_{\epsilon_{\vec{s},\vec{\omega},i}} \prod_{\substack{\vec{\beta} \in \mathcal{R}' \\ [\vec{\beta}] \neq [\vec{0}]}} \left(\frac{\phi(e(\vec{\beta})^2)}{|G|(q + |G| - 1)}\right)^{m_{[\vec{\beta}]} + m_{0,[\vec{\beta}]}} \left(\frac{q}{|G|(q + |G| - 1)}\right)^{m_{[\vec{0}]} + m_{0,[\vec{0}]}} \times$$

$$\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$=\sum_{M_{[\vec{\beta}]}}\prod_{\substack{s|r_n\\ s\neq 1}}\left(\frac{\phi(s^2)}{|G|(q+|G|-1)}\right)^{m_s}\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_1}\times$$

$$\sum_{M_{0,[\vec{\beta}]}}\prod_{\substack{\vec{\beta}\in\mathcal{R}'\\ [\vec{\beta}]\neq[\vec{0}]}}\left(\frac{\phi(e(\vec{\beta}))(|G|-e(\vec{\beta}))}{|G|(q+|G|-1)}\right)^{m_{0,[\vec{\beta}]}}\left(\frac{(|G|-1)q}{|G|(q+|G|-1)}\right)^{m_{0,[\vec{0}]}}\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

$$=\prod_{\substack{s|r_n\\ s\neq 1}}\left(\frac{\phi(s^2)\sum_{e([\vec{\beta}])=s}1}{|G|(q+|G|-1)}\right)^{m_s}\left(\frac{(|G|-1)q+\sum_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}}\\ [\vec{\beta}]\neq[\vec{0}]}}\phi(e(\vec{\beta}))(|G|-e(\vec{\beta}))}{|G|(q+|G|-1)}\right)^{m_0}\times$$

$$\left(\frac{q}{|G|(q+|G|-1)}\right)^{m_1}\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right).$$

First note that since there exists $\phi(e(\vec{\beta}))$ such $\vec{\beta}'$ such that $[\vec{\beta}']=[\vec{\beta}]$ so we can write

$$\phi(s^2)\sum_{e([\vec{\beta}])=s}1=s\sum_{e(\vec{\beta})=s}1$$

and

$$\sum_{\substack{[\vec{\beta}]\in\tilde{\mathcal{R}}\\ [\vec{\beta}]\neq[\vec{0}]}}\phi(e(\vec{\beta}))(|G|-e(\vec{\beta}))=\sum_{\vec{\beta}\in\mathcal{R}}(|G|-e(\vec{\beta}))=(|G|-1)|G|-\sum_{\vec{\beta}\in\mathcal{R}}e(\vec{\beta}).$$

Now, for every $\vec{\beta}\in\mathcal{R}'$, we can view it in a natural way as element of G. Moreover, the order of $\vec{\beta}$ would be $e(\vec{\beta})$. Hence $s\sum_{e(\vec{\beta})=s}1=s\phi_G(s)$. Further

$$\sum_{\vec{\beta}\in\mathcal{R}}e(\vec{\beta})=\sum_{\substack{s|r_n\\ s\neq 1}}s\sum_{e(\vec{\beta})=s}1=\sum_{s|r_n}s\phi_G(s)-1.$$

□

Theorem 4.6.2.

$$\frac{|\{C\in\mathcal{H}^{(\vec{d}(\vec{\alpha}))}:\#C(\mathbb{P}^1(\mathbb{F}_q))=M\}|}{|\mathcal{H}^{(\vec{d}(\vec{\alpha}))}|}=Prob\left(\sum_{i=1}^{q+1}X_i=M\right)\left(1+O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}}\right)\right)$$

where the X_i are i.i.d. random variables taking value 0 or $\frac{|G|}{s}$ for some $s|r_n$ such that

$$X_i=\begin{cases}\frac{|G|}{s} & \text{with probability } \frac{s\phi_G(s)}{|G|(q+|G|-1)} \text{ if } s\neq 1\\ |G| & \text{with probability } \frac{q}{|G|(q+|G|-1)}\\ 0 & \text{with probability } \frac{(|G|-1)(q+|G|)-\sum_{s|r_n}s\phi_G(s)+1}{|G|(q+|G|-1)}\end{cases}$$

where $\phi_G(s)$ is the number of elements of G of order s.

Proof.

$$\frac{|\{C \in \mathcal{H}^{(\vec{d}(\vec{\alpha}))} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M\}|}{|\mathcal{H}^{(\vec{d}(\vec{\alpha}))}|}$$

$$= \sum_{\substack{e_1,\ldots,e_{q+1} \\ \sum e_i = M}} |\{(\vec{c}, (f_{\vec{\alpha}})) \in \hat{\mathcal{F}}_{[\vec{d}(\vec{\alpha})]} : \sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_{\vec{s}}} \chi_{\ell(\vec{s})} \left(F_{(\vec{s})}^{(\vec{\omega})}(x_i) \right) = e_i, i = 1, \ldots, q+1\}|$$

$$= \sum_{\substack{e_1,\ldots,e_{q+1} \\ \sum e_i = M}} \left(\frac{(|G|-1)(q+|G|) - \sum_{s|r_n} s\phi_G(s) + 1}{|G|(q+|G|-1)} \right)^{m_0} \left(\frac{q}{|G|(q+|G|-1)} \right)^{m_1} \times$$

$$\prod_{\substack{s|r_n \\ s \neq 1}} \left(\frac{s\phi_G(s)}{|G|(q+|G|-1)} \right)^{m_s} \left(1 + O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}} \right) \right)$$

$$= \text{Prob}\left(\sum_{i=1}^{q+1} X_i = M \right) \left(1 + O\left(q^{-\frac{\min(d(\vec{\alpha}))}{2}} \right) \right).$$

□

Chapter 5

Whole Moduli Space

5.1 Known Results

As we mentioned in the introduction Wright [14] determined the number of extensions of K with a fixed, abelian Galois group. His methods involved using class field theory to determine a generating series for the number of extensions. Then, using the conductor-discriminant formula, he is able to write this generating series as a finite sum of Euler products. He then removes appropriate zeta functions and uses a Tauberian Theorem (Theorem 3.9 in Chapter III of [11]) to arrive at his result.

Bucur, David, Feigon, Kaplan, Lalin, Ozman and Wood [1] look deeper into the calculations for Wright's proof in the case that $G = \mathbb{Z}/Q\mathbb{Z}$ for Q a prime. Define $N(\mathbb{Z}/Q\mathbb{Z}, m)$ to be the set of extensions of K with Galois group $\mathbb{Z}/Q\mathbb{Z}$ and degree of conductor m. Define $\mathcal{V}_K$ to be the set of places of K and let $\mathcal{V}_R$, $\mathcal{V}_S$ and $\mathcal{V}_I$ be three finite sets of places of K. Let $N(\mathbb{Z}/Q\mathbb{Z}, m; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)$ be the set of extensions of K with Galois group $\mathbb{Z}/Q\mathbb{Z}$, degree of conductor m which are ramified at the places in $\mathcal{V}_R$, split at the places in $\mathcal{V}_S$ and inert at the places in $\mathcal{V}_I$. Moreover, let $\mathcal{V} = \mathcal{V}_R \cup \mathcal{V}_S \cup \mathcal{V}_I$.

Theorem 5.1.1. *With the notation above, we get*

$$|N(\mathbb{Z}/Q\mathbb{Z}, m; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)| = C_Q \left(\prod_{\nu \in \mathcal{V}} c_\nu \right) q^m P_{\mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I}(m) + O\left(q^{(\frac{1}{2}+\epsilon)m} \right)$$

where $P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}$ *is a monic polynomial of degree* $Q-2$*,*

$$C_Q = \frac{(1-q^{-2})^{Q-1}}{(Q-2)!}\prod_{j=1}^{Q-2}\prod_{\nu\in\mathcal{V}_K}\left(1-\frac{jq^{-2\deg(\nu)}}{(1+q^{-\deg(\nu)})(1+jq^{-\deg(\nu)})}\right)$$

and

$$c_\nu = \begin{cases} \frac{(Q-1)q^{-\deg(\nu)}}{1+(Q-1)q^{-\deg(\nu)}} & \text{if } \nu\in\mathcal{V}_R \\ \frac{1}{Q(1+(Q-1)q^{-\deg(\nu)})} & \text{if } \nu\in\mathcal{V}_S \\ \frac{Q-1}{Q(1+(Q-1)q^{-\deg(\nu)})} & \text{if } \nu\in\mathcal{V}_I \end{cases}.$$

In particular, setting $\mathcal{V}_R=\mathcal{V}_S=\mathcal{V}_I=\emptyset$*, we get*

$$|N(\mathbb{Z}/Q\mathbb{Z},m)| = C_Q q^m P(m) + O\left(q^{(\frac{1}{2}+\epsilon)m}\right)$$

where P *is a monic polynomial of degree* $Q-2$*.*

Remark 5.1.2. Notice that C_Q is defined as a product over all the places of K. The places of K correspond to irreducible polynomials and the prime at infinity. If we were to write C_Q as a product of irreducible polynomials, and take out the factor at the prime at infinity, we would get that

$$C_Q = \frac{1}{(Q-2)!}\frac{q+Q-1}{q}\frac{L_{Q-2}}{\zeta_q(2)^{Q-1}}$$

where L_{Q-2} and $\zeta_q(2)$ are as defined in Chapter 2.

If we let C be a smooth projective curve such that $\mathrm{Gal}(C)=\mathbb{Z}/Q\mathbb{Z}$, and we let ν_i be the place corresponding to the prime polynomial $(X-x_i)$, then we see that the number of points lying over x_i on C will be

$$\begin{cases} 0 & \nu_i \text{ is inert in } K(C) \\ 1 & \nu_i \text{ ramifies in } K(C) \\ Q & \nu_i \text{ splits in } K(C) \end{cases}.$$

Therefore, they get the following result.

Theorem 5.1.3. *As* $g\to\infty$*,*

$$\frac{|\{C\in\mathcal{H}_{\mathbb{Z}/Q\mathbb{Z},g} : \#C(\mathbb{P}^1(\mathbb{F}_q))=M\}|'}{|\mathcal{H}_{\mathbb{Z}/Q\mathbb{Z},g}|'} = Prob\left(\sum_{i=1}^{q+1}X_i=M\right)+O\left(\frac{1}{g}\right)$$

where the X_i are i.i.d. random variables taking values

$$X_i = \begin{cases} 0 & \text{with probability } \frac{(Q-1)q}{Q(q+Q-1)} \\ 1 & \text{with probability } \frac{Q-1}{q+Q-1} \\ Q & \text{with probability } \frac{q}{Q(q+Q-1)} \end{cases}$$

where the $'$ notation indicates that the curves are counted with the weight $\frac{1}{|Aut(C)|}$.

Remark 5.1.4. The only reason we can make the connection between splitting type of the place and the number of point lying over x_i is because $G = \mathbb{Z}/Q\mathbb{Z}$ and therefore, there are only three splitting types: inert, completely split and completely ramified. If Q were not a prime, then there could be places that split but are not completely split or that are ramified but not completely ramified.

In the following section we will prove an analogue of Theorem 5.1.1 but for any abelian group G. However, we will only be able to determine the leading coefficient in the case that $G = (\mathbb{Z}/Q\mathbb{Z})^n$. Moreover, we avoid using class field theory. As a result of this, we will not get a result about extensions of K of a fixed Galois group as the conductor tends to infinity, but a result about the curves of a fixed Galois group as the genus tends to infinity. (Note that in the case $G = (\mathbb{Z}/Q\mathbb{Z})^n$, the discriminant is just a multiple of the conductor and so a count by conductor is the same as a count by genus.) Finally, we will be able to use the leading coefficient in the case of $G = (\mathbb{Z}/Q\mathbb{Z})^n$ to determine an analogue of Theorem 5.1.3.

5.2 Generating Series

Recall that for every $\vec{v} = (v_1, \ldots, v_n)$,

$$e(\vec{v}) = \operatorname*{lcm}_{j=1,\ldots,n} \left(\frac{r_j}{(r_j, \alpha_j)} \right).$$

Define

$$c(\vec{v}) := |G| - \frac{|G|}{e(\vec{v})}. \tag{5.2.1}$$

Then we can write the genus formula as

$$2g + 2|G| - 2 = \sum_{\vec{\alpha} \in \mathcal{R}} c(\vec{\alpha}) d(\vec{\alpha}) + c(\vec{d}) \tag{5.2.2}$$

where $\vec{d} = (d_1, \dots, d_n)$ and $d_j = \sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j d(\vec{\alpha})$. Then we have

$$\sum_{\vec{d}(\vec{\alpha})} |\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}| = (q-1)^n \sum_{\vec{d}(\vec{\alpha})} |\mathcal{F}_{\vec{d}(\vec{\alpha})}|$$

where the sum if over all $\vec{d}(\vec{\alpha})$ that satisfy (5.2.2).

Remark 5.2.1. We would like to conclude that

$$|\mathcal{H}_{G,g}| = \sum_{\vec{d}(\vec{\alpha})} |\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}|.$$

However, as we will show in Section 5.7, this is not true, but it will be possible to deduce $|\mathcal{H}_{G,g}|$ from $\sum_{\vec{d}(\vec{\alpha})} |\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}|$ using an inclusion-exclusion argument.

Remark 5.2.2. While we need $c(\vec{\alpha})$ to be as defined as above for (5.2.2) to be accurate, we won't need this exact formula. That is, all the results from this section until Section 5.6 will be for an arbitrary set of positive integers $c(\vec{\alpha})$ with the idea that we will eventually set them equal to $|G| - \frac{|G|}{e(\vec{\alpha})}$. This will come in handy in Section 5.10 where we show that if $G = (\mathbb{Z}/Q\mathbb{Z})^n$ for Q a prime, we can actually set $c(\vec{\alpha}) = 1$ for all $\vec{\alpha} \in \mathcal{R}$ and the computations become much simpler.

As an analogue of Proposition 2.1.12, we want to determine the size of the set

$$\bigcup_{\vec{d}(\vec{\alpha})} \{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1, \dots, \ell, j = 1, \dots, n\}$$

for some $\epsilon_{i,j} \in \mu_{r_j}$ where the union is over all $\vec{d}(\vec{\alpha})$ that satisfy (5.2.2).

Define E to be an $\ell \times n$ matrix with such that

$$E = \begin{pmatrix} \epsilon_{1,1} & \dots & \epsilon_{1,n} \\ \vdots & \ddots & \vdots \\ \epsilon_{\ell,1} & \dots & \epsilon_{\ell,n} \end{pmatrix}$$

where $\epsilon_{i,j} \in \mu_{r_j}$. Moreover, since $c(\vec{d})$ only depends on what d_j is modulo r_j, let $\vec{k} \in \mathcal{R}'$ such that

$$d_j = \sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv k_j \pmod{r_j}, j = 1, \dots, n. \tag{5.2.3}$$

Then $c(\vec{d}) = c(\vec{k})$ and (5.2.2) can then be rewritten as

$$2g + 2|G| - 2 - c(\vec{k}) = \sum_{\vec{\alpha} \in \mathcal{R}} c(\vec{\alpha}) d(\vec{\alpha}). \tag{5.2.4}$$

With this in mind, define

$$\mathcal{F}_{\vec{d}(\vec{\alpha});\vec{k},E} = \begin{cases} \{(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1, \dots, \ell, j = 1, \dots, n\} & \text{(5.2.3) is satisfied} \\ \emptyset & \text{otherwise} \end{cases}$$

and

$$\mathcal{F}_{D;\vec{k},E} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{F}_{\vec{d}(\vec{\alpha});\vec{k},E} \tag{5.2.5}$$

where the union is over all solutions to (5.2.4) such that $D = 2g + 2|G| - 2 - c(\vec{k})$. We will be interested in determining $|\mathcal{F}_{D;\vec{k},E}|$ as $D \to \infty$.

We do this by creating a generating series whose coefficients are $|\mathcal{F}_{D;\vec{k},E}|$. But first, we need indicator functions for the relations

$$d_j \equiv k_j \pmod{r_j}, j = 1, \dots, n$$

$$\chi_{r_j}(F(x_i)) = \epsilon_{i,j}, i = 1, \dots, \ell, j = 1, \dots, n.$$

That is, if we let $\xi_{r_j} = e^{\frac{2\pi i}{r_j}}$, a primitive r_j^{th} root of unity, then

$$\frac{1}{r_1 \cdots r_n} \prod_{j=1}^{n} \sum_{t_j=0}^{r_j-1} \xi_{r_j}^{t_j(\sum \alpha_j \deg(f_{\vec{\alpha}}) - k_j)} = \begin{cases} 1 & \sum_{\vec{\alpha} \in \mathcal{R}} \alpha_j \deg(f_{\vec{\alpha}}) \equiv k_j \pmod{r_j} \\ 0 & \text{otherwise} \end{cases} \tag{5.2.6}$$

and,

$$\left(\frac{1}{r_1 \cdots r_n}\right)^{\ell} \prod_{i=1}^{\ell} \prod_{j=1}^{n} \sum_{\nu_{i,j}=0}^{r_j-1} (\epsilon_{i,j}^{-1} \chi_{r_j}(F_j(x_i))^{\nu_{i,j}} = \begin{cases} 1 & \chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1, \dots, \ell, j = 1, \dots, n \\ 0 & \text{otherwise} \end{cases}. \tag{5.2.7}$$

Remark 5.2.3. The sum in the exponent in (5.2.6) is a sum over all $\vec{\alpha} \in \mathcal{R}$.

For ease of notation, for every set of polynomials $(f_{\vec{\alpha}})$, let $I_{\vec{k},E}((f_{\vec{\alpha}}))$ be the indicator function defined as

$$I_{\vec{k},E}((f_{\vec{\alpha}})) = \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1}\left(\prod_{j=1}^{n}\sum_{t_j=0}^{r_j-1}\xi_{r_j}^{t_j(\sum\alpha_j\deg(f_{\vec{\alpha}})-k_j)}\right)\left(\prod_{i=1}^{\ell}\prod_{j=1}^{n}\sum_{\nu_{i,j}=0}^{r_j-1}(\epsilon_{i,j}^{-1}\chi_{r_j}(F_j(x_i))^{\nu_{i,j}}\right). \tag{5.2.8}$$

Now, define the multi-variable complex function

$$\mathcal{G}_{\vec{k},E}((s_{\vec{\alpha}})) = \sum_{(f_{\vec{\alpha}})}\frac{\mu^2(\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}})I_{\vec{k},E}((f_{\vec{\alpha}}))}{\prod_{\vec{\alpha}\in\mathcal{R}}|f_{\vec{\alpha}}|^{c(\vec{\alpha})s_{\vec{\alpha}}}}. \tag{5.2.9}$$

Remark 5.2.4. The sum is over *all* $r_1\cdots r_n-1$-tuples of monic polynomials $(f_{\vec{\alpha}})_{\vec{\alpha}\in\mathcal{R}}$. However, the factor $\mu^2(\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}})$ means that it is zero whenever the set of polynomials $(f_{\vec{\alpha}})$ are not square-free and coprime. Moreover, as usual, we let $|f_{\vec{\alpha}}| = q^{\deg(f_{\vec{\alpha}})}$.

Now, if we let $z_{\vec{\alpha}} = q^{-s_{\vec{\alpha}}}$ and define $F_{\vec{k},E}((z_{\vec{\alpha}})) = \mathcal{G}_{\vec{k},E}((q^{-s_{\vec{\alpha}}}))$, then

$$\begin{aligned}F_{\vec{k},E}((z_{\vec{\alpha}})) &= \sum_{(f_{\vec{\alpha}})}\mu^2(\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}})I_{\vec{k},E}((f_{\vec{\alpha}}))\prod_{\vec{\alpha}\in\mathcal{R}}z_{\vec{\alpha}}^{c(\vec{\alpha})\deg(f_{\vec{\alpha}})}\\ &= \sum_{\substack{d(\vec{\alpha})=0\\ \vec{\alpha}\in\mathcal{R}}}^{\infty}|\mathcal{F}_{\vec{d}(\vec{\alpha});\vec{k},E}|\prod_{\vec{\alpha}\in\mathcal{R}}z_{\vec{\alpha}}^{c(\vec{\alpha})d(\vec{\alpha})}.\end{aligned}$$

With some abuse of notation, if we let $F_{\vec{k},E}(z)$ be the function that sets all the $z_{\vec{\alpha}} = z$ to be the same in $F_{\vec{k},E}((z_{\vec{\alpha}}))$, then we get

$$\begin{aligned}F_{\vec{k},E}(z) &= \sum_{\substack{d(\vec{\alpha})=0\\ \vec{\alpha}\in\mathcal{R}}}^{\infty}|\mathcal{F}_{\vec{d}(\vec{\alpha});\vec{k},E}|z^{\sum_{\vec{\alpha}\in\mathcal{R}}c(\vec{\alpha})d(\vec{\alpha})}\\ &= \sum_{D=0}^{\infty}|\mathcal{F}_{D;\vec{k},E}|z^{D}.\end{aligned} \tag{5.2.10}$$

5.3 Euler Products

In this section, we will write $F_{\vec{k},E}(z)$ as a sum of functions which can be written as product of prime polynomials. But first, we need some notation. Let

$$\mathcal{M} := \left\{\nu = \begin{pmatrix}\nu_{1,1} & \dots & \nu_{1,n}\\ \vdots & & \vdots\\ \nu_{\ell,1} & \dots & \nu_{\ell,n}\end{pmatrix} \in M_{\ell,n} : \nu_{i,j}\in\mathbb{Z}/r_j\mathbb{Z}\right\}.$$

We can define an action on $\mathcal{R}'$ and E by $\mathcal{M}$ by

$$\nu\vec{\alpha} := \begin{pmatrix} \sum_{j=1}^{n} \frac{r_n}{r_j}\nu_{1,j}\alpha_j \\ \vdots \\ \sum_{j=1}^{n} \frac{r_n}{r_j}\nu_{\ell,j}\alpha_j \end{pmatrix} \in (\mathbb{Z}/r_n\mathbb{Z})^{\ell} \tag{5.3.1}$$

$$E^{\nu} := \prod_{i=1}^{\ell}\prod_{j=1}^{n} \epsilon_{i,j}^{\nu_{i,j}} \in \mu_{r_n} \tag{5.3.2}$$

Moreover, for any $\vec{\alpha}, \vec{\beta} \in \mathcal{R}'$ define

$$\vec{\alpha}\cdot\vec{\beta} = \sum_{j=1}^{n} \frac{r_n}{r_j}\alpha_j\beta_j \in \mathbb{Z}/r_n\mathbb{Z}. \tag{5.3.3}$$

With this notation, we can rewrite (5.2.6) as

$$\frac{1}{r_1\cdots r_n}\prod_{j=1}^{n}\sum_{t_j=0}^{r_j-1} \xi_{r_j}^{t_j(\sum \alpha_j \deg(f_{\vec{\alpha}})-k_j)} = \frac{1}{r_1\cdots r_n}\sum_{\vec{t}\in\mathcal{R}'}\prod_{j=1}^{n} \xi_{r_j}^{t_j(\sum \alpha_j \deg(f_{\vec{\alpha}})-k_j)}$$

$$= \frac{1}{r_1\cdots r_n}\sum_{\vec{t}\in\mathcal{R}'} \xi_{r_n}^{-\vec{t}\cdot\vec{k}}\prod_{\vec{\alpha}\in\mathcal{R}} \xi_{r_n}^{\vec{t}\cdot\vec{\alpha}\deg(f_{\vec{\alpha}})}.$$

Let $h(X) = \prod_{i=1}^{\ell}(X - x_i)$ and for every $\nu \in \mathcal{M}$ and $\vec{\alpha} \in \mathcal{R}$, define

$$\chi_{r_n}^{\nu\vec{\alpha}}(F(X)) = \begin{cases} \prod_{i=1}^{\ell} \chi_{r_n}^{(\nu\vec{\alpha})_i}(F(x_i)) & (F,h) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then, $\chi_{r_n}^{\nu\vec{\alpha}}$ if a multiplicative character on $\mathbb{F}_q[X]$ modulo $h(X)$. Moreover, it will be a primitive character if and only if $\nu\vec{\alpha} = \vec{0}$. Hence, we can rewrite (5.2.7) as

$$\left(\frac{1}{r_1\cdots r_n}\right)^{\ell}\prod_{i=1}^{\ell}\prod_{j=1}^{n}\sum_{\nu_{i,j}=0}^{r_j-1}(\epsilon_{i,j}^{-1}\chi_{r_j}(F_j(x_i))^{\nu_{i,j}} = \left(\frac{1}{r_1\cdots r_n}\right)^{\ell}\sum_{\nu\in\mathcal{M}}\prod_{i=1}^{\ell}\prod_{j=1}^{n}(\epsilon_{i,j}^{-1}\chi_{r_j}(F_j(x_i))^{\nu_{i,j}}$$

$$= \left(\frac{1}{r_1\cdots r_n}\right)^{\ell}\sum_{\nu\in\mathcal{M}} E^{-\nu}\prod_{\vec{\alpha}\in\mathcal{R}}\prod_{i=1}^{\ell}\prod_{j=1}^{n}\chi_{r_j}^{\nu_{i,j}}(f_{\vec{\alpha}}^{\alpha_j}(x_i)) = \left(\frac{1}{r_1\cdots r_n}\right)^{\ell}\sum_{\nu\in\mathcal{M}} E^{-\nu}\prod_{\vec{\alpha}\in\mathcal{R}}\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}}(X)).$$

Therefore, we can rewrite the indicator function in (5.2.8) as

$$I_{\vec{k},E}((f_{\vec{\alpha}})) = \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1}\sum_{\vec{t}\in\mathcal{R}'}\sum_{\nu\in\mathcal{M}} E^{-\nu}\xi_{r_n}^{-\vec{t}\cdot\vec{k}}\prod_{\vec{\alpha}\in\mathcal{R}}\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}\deg(f_{\vec{\alpha}})}\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}}(X)). \tag{5.3.4}$$

Using this, we can write $F_{\vec{k},E}(z)$ as a sum of Euler products.

$$\begin{aligned}
F_{\vec{k},E}(z) &= \sum_{(f_{\vec{\alpha}})} \mu^2(\prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}) I_{\vec{k},E}((f_{\vec{\alpha}})) z^{\sum c(\vec{\alpha})\deg(f_{\vec{\alpha}})} \\
&= \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1} \sum_{(f_{\vec{\alpha}})} \mu^2(\prod_{\vec{\alpha}\in\mathcal{R}} f_{\vec{\alpha}}) \sum_{\vec{t}\in\mathcal{R}'} \sum_{\nu\in\mathcal{M}} E^{-\nu} \xi_{r_n}^{-\vec{t}\cdot\vec{k}} \prod_{\vec{\alpha}\in\mathcal{R}} \left(\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}})(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(f_{\vec{\alpha}})}\right) \\
&= \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1} \sum_{\vec{t}\in\mathcal{R}'} \sum_{\nu\in\mathcal{M}} E^{-\nu} \xi_{r_n}^{-\vec{t}\cdot\vec{k}} A_{\vec{t},\nu}(z)
\end{aligned}$$

where

$$A_{\vec{t},\nu}(z) := \sum_{(f_{\vec{\alpha}})} \mu^2(\prod_{\vec{\alpha}} f_{\vec{\alpha}}) \prod_{\vec{\alpha}\in\mathcal{R}} \left(\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}})(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(f_{\vec{\alpha}})}\right).$$

Definition 5.3.1. We call a function $G : \mathbb{F}_q[X]^n \to \mathbb{C}$ an **n-dimensional multiplicative** function if

$$G(f_1,\ldots,f_n) = \prod_P G(P^{v_P(f_1)},\ldots,P^{v_P(f_n)})$$

where the product is over all prime polynomial P dividing $f_1\cdots f_n$.

Therefore, if G is an n-dimensional multiplicative function, then

$$\sum_{f_1,\ldots,f_n} G(f_1,\ldots,f_n) = \prod_P \left(1 + \sum_{(a_1,\ldots,a_n)\neq(0,\ldots,0)} G(P^{a_1},\ldots,P^{a_n})\right).$$

where the sum is over all monic polynomials in $\mathbb{F}_q[X]$ and the product is over all monic prime polynomials.

Now,

$$G((f_{\vec{\alpha}})) = \mu^2(\prod_{\vec{\alpha}} f_{\vec{\alpha}}) \prod_{\vec{\alpha}\in\mathcal{R}} \left(\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}})(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(f_{\vec{\alpha}})}\right)$$

is an $|R|$-dimensional multiplicative function. Moreover, if P is a prime polynomial then

$$G((P^{a_{\vec{\alpha}}})) = \begin{cases} \chi_{r_n}^{\nu\vec{\alpha_0}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha_0}} z^{c(\vec{\alpha_0})})^{\deg(P)} & a_{\vec{\alpha_0}} = 1 \text{ for some } \vec{\alpha_0}, a_{\vec{\beta}} = 0 \text{ for all } \vec{\beta} \neq \vec{\alpha_0} \\ 0 & \text{otherwise} \end{cases}$$

Therefore,

$$A_{\vec{t},\nu}(z) = \sum_{\substack{f_{\vec{\alpha}} \\ \vec{\alpha}\in\mathcal{R}}} \mu^2(\prod_{\vec{\alpha}} f_{\vec{\alpha}}) \prod_{\vec{\alpha}\in\mathcal{R}} \left(\chi_{r_n}^{\nu\vec{\alpha}}(f_{\vec{\alpha}})(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(f_{\vec{\alpha}})}\right)$$
$$= \prod_{P} \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}} \chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right).$$

5.4 First Residue Calculation

Let $1 = s_0 < s_1 < \cdots < s_\eta = r_n$ be the unique divisors of r_n. If we define

$$c_i = |G| - \frac{|G|}{s_i}$$

then we have that $c_1 < c_2 < \cdots < c_\eta$ are exactly the values of the $c(\vec{\alpha})$. Recall that $z = q^{-s}$. Hence from the Euler product, we see that $A_{\vec{t},\nu}(z)$ will absolutely converge for $\Re(s) > 1/c_1$ for all $\vec{t} \in \mathcal{R}'$ and $\nu \in \mathcal{M}$. Therefore $A_{\vec{t},\nu}(z)$ and $F_{\vec{k},E}(z)$ absolutely converges for $|z| < q^{-1/c_1}$. This allows us to write $|\mathcal{F}_{D;\vec{k},E}|$ in terms of a contour integral.

Proposition 5.4.1. *Let $0 < \delta_1 < q^{-1/c_1}$ and let $C_{\delta_1} = \{z \in \mathbb{C} : |z| = \delta_1\}$, oriented counterclockwise. Then*

$$\frac{1}{2\pi i} \oint_{C_{\delta_1}} \frac{F_{\vec{k},E}(z)}{z^{D+1}} dz = |\mathcal{F}_{D;\vec{k},E}|. \tag{5.4.1}$$

Proof. By (5.2.10), we have

$$F_{\vec{k},E}(z) = \sum_{D=0}^{\infty} |\mathcal{F}_{D;\vec{k},E}| z^D.$$

By our discussion above, $\frac{F_{\vec{k},E}(z)}{z^{D+1}}$ has only one pole at 0 in the region contained in C_{δ_1} and it's residue is $|\mathcal{F}_{D;\vec{k},E}|$.

□

We will use this and an analytic continuation of the $A_{\vec{t},\nu}(z)$ to find an asymptotic formula for $|\mathcal{F}_{D;\vec{k},E}|$.

5.5 Analytic Continuation of $A_{\vec{t},\nu}(z)$

Recall $h(X) = \prod_{i=1}^{\ell}(x - x_i)$ and define $\mathcal{R}_\nu = \{\vec{\alpha} \in \mathcal{R} : \nu\vec{\alpha} = \vec{0}\}$, then

$$\begin{aligned}
A_{\vec{t},\nu}(z) &= \prod_P \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}} \chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right) \\
&= \prod_{\substack{P \\ (P,h)=1}} \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}_\nu} (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)} + \sum_{\vec{\alpha}\notin\mathcal{R}_\nu} \chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right) \\
&= \prod_P \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}_\nu} (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)} + \sum_{\vec{\alpha}\notin\mathcal{R}_\nu} \chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right) \times \\
&\quad \prod_{P|h} \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}_\nu} (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right)^{-1} \\
&= \prod_{\vec{\alpha}\in\mathcal{R}_\nu} \prod_P \left(1 + (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right) H_{\vec{t},\nu}(z) \\
&= \prod_{\vec{\alpha}\in\mathcal{R}_\nu} \frac{Z_K(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})}{Z_K(\xi_{r_n}^{2\vec{t}\cdot\vec{\alpha}} z^{2c(\vec{\alpha})})} H_{\vec{t},\nu}(z)
\end{aligned}$$

where

$$Z_K(z) = \prod_P \left(1 - z^{\deg(P)}\right)^{-1} = (1 - qz)^{-1}$$

is the zeta-function of K in the z-variable and

$$H_{\vec{t},\nu}(z) = \prod_P \left(\frac{1 + \sum_{\vec{\alpha}\in\mathcal{R}_\nu} (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)} + \sum_{\vec{\alpha}\notin\mathcal{R}_\nu} \chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}}{\prod_{\vec{\alpha}\in\mathcal{R}_\nu} \left(1 + (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right)}\right) \times$$

$$\prod_{P|h} \left(1 + \sum_{\vec{\alpha}\in\mathcal{R}_\nu} (\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})^{\deg(P)}\right)^{-1}.$$

Now, for all $\vec{\alpha} \in \mathcal{R}$,

$$\frac{Z_K(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}} z^{c(\vec{\alpha})})}{Z_K(\xi_{r_n}^{2\vec{t}\cdot\vec{\alpha}} z^{2c(\vec{\alpha})})}$$

is a meromorphic function with simple poles at $z = \xi_{c(\vec{\alpha})}^k (q\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}})^{-1/c(\vec{\alpha})}$ for $k = 1, \ldots, c(\vec{\alpha})$. So it remains to determine where $H_{\vec{t},\nu}(z)$ converges.

Lemma 5.5.1. *$H_{\vec{t},\nu}(z)$ absolutely converges for all $|z| < q^{-1/2c_1}$.*

Proof. Since

$$\prod_{P|h}\left(1+\sum_{\vec{\alpha}\in\mathcal{R}_\nu}(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)^{-1}$$

is a finite product, it will always converge and thus we need only consider the factor consisting of the infinite product.

$$\prod_{P}\left(\frac{1+\sum_{\vec{\alpha}\in\mathcal{R}_\nu}(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}+\sum_{\vec{\alpha}\notin\mathcal{R}_\nu}\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}}{\prod_{\vec{\alpha}\in\mathcal{R}_\nu}\left(1+(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)}\right)$$
$$=\prod_{\vec{\alpha}\notin\mathcal{R}_\nu}\prod_{P}\left(1+\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)H_{\vec{t},\nu}^*(z).$$

Since, for all $\vec{\alpha}\notin\mathcal{R}_\nu$, $\chi_{r_n}^{\nu\vec{\alpha}}$ is a non-trivial character we get that

$$\prod_{\vec{\alpha}\notin\mathcal{R}_\nu}\prod_{P}\left(1+\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)$$

is an entire function. Moreover,

$$H_{\vec{t},\nu}^*(z)=\prod_{P}\left(\frac{1+\sum_{\vec{\alpha}\in\mathcal{R}_\nu}(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}+\sum_{\vec{\alpha}\notin\mathcal{R}_\nu}\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}}{\prod_{\vec{\alpha}\in\mathcal{R}_\nu}\left(1+(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)\prod_{\vec{\alpha}\notin\mathcal{R}_\nu}\left(1+\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)}\right)$$
$$=\prod_{P}\left(1-\frac{h_P(z)}{\prod_{\vec{\alpha}\in\mathcal{R}_\nu}\left(1+(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)\prod_{\vec{\alpha}\notin\mathcal{R}_\nu}\left(1+\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)}\right)$$

where

$$h_p(z)=\prod_{\vec{\alpha}\in\mathcal{R}_\nu}\left(1+(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)\prod_{\vec{\alpha}\notin\mathcal{R}_\nu}\left(1+\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)$$
$$-\left(1+\sum_{\vec{\alpha}\in\mathcal{R}_\nu}(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}+\sum_{\vec{\alpha}\notin\mathcal{R}_\nu}\chi_{r_n}^{\nu\vec{\alpha}}(P)(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})^{\deg(P)}\right)$$
$$=O\left(z^{\min_{\vec{\alpha}\neq\vec{\beta}}(c(\vec{\alpha})+c(\vec{\beta}))}\right)=O\left(z^{2c_1}\right).$$

Therefore, if $|z|<q^{-1/2c_1}$, then $H_{\vec{t},\nu}^*(z)$ converges absolutely and hence so does $H_{\vec{t},\nu}(z)$.

□

For $0\leq a\leq r_n-1$, and $i=1,\ldots,\eta$, define

$$\mathcal{R}_{\vec{t},\nu;a,i}=\{\vec{\alpha}\in\mathcal{R}_\nu : c(\vec{\alpha})=c_i \text{ and } \vec{t}\cdot\vec{\alpha}\equiv a \pmod{r_n}\} \tag{5.5.1}$$

and let

$$m_{\vec{t},\nu;a,i}=|\mathcal{R}_{\vec{t},\nu;a,i}|. \tag{5.5.2}$$

Corollary 5.5.2. *$A_{\vec{t},\nu}(z)$ is meromorphic on the disc $|z| < q^{-1/2c_1}$ with poles of order $m_{\vec{t},\nu;a,i}$ at*

$$z = \xi_{c_i}^k \left(q\xi_{r_n}^a\right)^{-1/c_i}$$

for $k = 1, \ldots, c_i$.

Proof. Immediate from Lemma 5.5.1 and the factors of $Z_K(z)$ appearing.

□

Remark 5.5.3. It is highly possible that $m_{\vec{t},\nu;a,i} = 0$ for some values of $\vec{t}, \nu, a, i$. In this case when we say a pole of order 0, we mean there is no pole.

5.6 Residue Calculations

Before we begin the residue calculations, we need to define a quasi-polynomial.

Definition 5.6.1. A quasi-polynomial is a function that can be written as

$$p(x) = c_n(x)x^n + c_{n-1}(x)x^{n-1} + \cdots + c_0(x)$$

where $c_i(x)$ is a periodic function on integer period. We call the c_i the coefficients of the quasi-polynomial. Moreover, if $c_n(x)$ is not identically the zero function then we say p has degree n and call it the leading coefficient.

Now, we can calculate the residues of $A_{\vec{t},\nu}(z)$ at each of its poles.

Lemma 5.6.2. *Let a, i be such that $m_{\vec{t},\nu;a,i} \neq 0$, then for any $1 \leq k \leq c_i$,*

$$Res_{z=\xi_{c_i}^k\left(q\xi_{r_n}^a\right)^{-1/c_i}} \left(\frac{A_{\vec{t},\nu}(z)}{z^{D+1}}\right) = P_{\vec{t},\nu;a,i,k}(D)q^{\frac{D}{c_i}}$$

where $P_{\vec{t},\nu;a,i,k}$ is a quasi-polynomial of degree $(m_{\vec{t},\nu;a,i} - 1)$ with leading coefficient $-C_{\vec{t},\nu;a,i,k}$ such that

$$C_{\vec{t},\nu;a,i,k} = \frac{1}{(m_{\vec{t},\nu;a,i}-1)!}\left(\frac{1-q^{-1}}{c_i}\right)^{m_{\vec{t},\nu;a,i}} \xi_{c_i}^{-kD}\left(\xi_{r_n}^a\right)^{\frac{D}{c_i}} H_{\vec{t},\nu;a,i}(\xi_{c_i}^k(\xi_{r_n}^a q)^{-1/c_i})$$

and $H_{\vec{t},\nu;a,i}$ is defined in the proof.

Proof.

$$\begin{aligned}\frac{A_{\vec{t},\nu}(z)}{z^{D+1}} &= \frac{1}{z^{D+1}}\prod_{\vec{\alpha}\in\mathcal{R}_\nu}\frac{Z_K(\xi_{r_n}^{\vec{t}\cdot\vec{\alpha}}z^{c(\vec{\alpha})})}{Z_K(\xi_{r_n}^{2\vec{t}\cdot\vec{\alpha}}z^{2c(\vec{\alpha})})}H_{\vec{t},\nu}(z)\\ &= \frac{1}{z^{D+1}}\prod_{\substack{j=1\\ m_{\vec{t},\nu;b,j\neq 0}}}^{\eta}\prod_{b=0}^{r_n-1}\left(\frac{Z_K(\xi_{r_n}^{b}z^{c_j})}{Z_K(\xi_{r_n}^{2b}z^{2c_j})}\right)^{m_{\vec{t},\nu;b,j}}H_{\vec{t},\nu}(z)\\ &= \frac{1}{z^{D+1}}\left(\frac{1-q\xi_{r_n}^{2a}z^{2c_i}}{1-q\xi_{r_n}^{a}z^{c_i}}\right)^{m_{\vec{t},\nu;a,i}}H_{\vec{t},\nu;a,i}(z)\end{aligned}$$

where

$$H_{\vec{t},\nu;a,i}(z)=\prod_{\substack{j=1\\ (b,j)\neq(a,i)\\ m_{\vec{t},\nu;b,j\neq 0}}}^{\eta}\prod_{b=0}^{r_n-1}\left(\frac{Z_K(\xi_{r_n}^{b}z^{c_j})}{Z_K(\xi_{r_n}^{2b}z^{2c_j})}\right)^{m_{\vec{t},\nu;b,j}}H_{\vec{t},\nu}(z).$$

Therefore, for any $1\le k\le c_i$, if we let

$$R_{a,i,k}(z)=\frac{z^{c_i}-(q\xi_{r_n}^{a})^{-1}}{z-\xi_{c_i}^{k}(q\xi_{r_n}^{a})^{-1/c_i}},$$

then

$$\begin{aligned}&(m_{\vec{t},\nu;a,i}-1)!\mathrm{Res}_{z=\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i}}\left(\frac{A_{\vec{t},\nu}(z)}{z^{D+1}}\right)\\ =&\lim_{z\to\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i}}\frac{d^{m_{\vec{t},\nu;a,i}-1}}{dz^{m_{\vec{t},\nu;a,i}-1}}\frac{(z-\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i})^{m_{\vec{t},\nu;a,i}}}{z^{D+1}}\left(\frac{1-q\xi_{r_n}^{2a}z^{2c_i}}{1-q\xi_{r_n}^{a}z^{c_i}}\right)^{m_{\vec{t},\nu;a,i}}H_{\vec{t},\nu;a,i}(z)\\ =&\lim_{z\to\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i}}\frac{d^{m_{\vec{t},\nu;a,i}-1}}{dz^{m_{\vec{t},\nu;a,i}-1}}\frac{1}{z^{D+1}}\left(\frac{1-q\xi_{r_n}^{2a}z^{2c_i}}{-q\xi_{r_n}^{a}R_{a,i,k}(z)}\right)^{m_{\vec{t},\nu;a,i}}H_{\vec{t},\nu;a,i}(z)\\ =&\lim_{z\to\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i}}\sum_{j=0}^{m_{\vec{t},\nu;a,i}-1}\binom{m_{\vec{t},\nu;a,i}-1}{j}\frac{d^{j}}{dz^{j}}\left(\frac{1}{z^{D+1}}\right)\frac{d^{m_{\vec{t},\nu;a,i}-1-j}}{dz^{m_{\vec{t},\nu;a,i}-1-j}}\left(\frac{1-q\xi_{r_n}^{2a}z^{2c_i}}{-q\xi_{r_n}^{a}R_{a,i,k}(z)}\right)^{m_{\vec{t},\nu;a,i}}\times\\ &H_{\vec{t},\nu;a,i}(z)\\ =&\sum_{j=0}^{m_{\vec{t},\nu;a,i}-1}\binom{m_{\vec{t},\nu;a,i}-1}{j}(-1)^{j}(D+1)\cdots(D+j)\xi_{c_i}^{-k(D+j+1)}(\xi_{r_n}^{a}q)^{(D+j+1)/c_i}\times\\ &\frac{d^{m_{\vec{t},\nu;a,i}-1-j}}{dz^{m_{\vec{t},\nu;a,i}-1-j}}\left(\frac{1-q\xi_{r_n}^{2a}z^{2c_i}}{-q\xi_{r_n}^{a}R_{a,i,k}(z)}\right)^{m_{\vec{t},\nu;a,i}}H_{\vec{t},\nu;a,i}(z)\Big|_{z=\xi_{c_i}^{k}(\xi_{r_n}^{a}q)^{-1/c_i}}\\ =&P_{\vec{t},\nu;a,i,k}(D)q^{\frac{D}{c_i}}\end{aligned}$$

where $P_{\vec{t},\nu;a,i,k}$ is a quasi-polynomial of degree $m_{\vec{t},\nu;a,i}-1$. Moreover, we see that the leading coefficient of $P_{\vec{t},\nu;a,i,k}$ arises when $j=m_{\vec{t},\nu;a,i}-1$. That is

$$\begin{aligned}P_{\vec{t},\nu;a,i,k}(D)q^{\frac{D}{c_i}} =&(-D)^{m_{\vec{t},\nu;a,i}-1}\xi_{c_i}^{-k(D+m_{\vec{t},\nu;a,i})}\left(\xi_{r_n}^a q\right)^{(D+m_{\vec{t},\nu;a,i})/c_i}\left(\frac{1-q^{-1}}{-c_i\xi_{c_i}^{k(c_i-1)}\left(\xi_{r_n}^a q\right)^{1/c_i}}\right)^{m_{\vec{t},\nu;a,i}}\times\\ &H_{\vec{t},\nu;a,i}(\xi_{c_i}^k(\xi_{r_n}^a q)^{-1/c_i})\left(1+O\left(\frac{1}{D}\right)\right)\\ =&-\left(\frac{1-q^{-1}}{c_i}\right)^{m_{\vec{t},\nu;a,i}}\xi_{c_i}^{-kD}D^{m_{\vec{t},\nu;a,i}-1}\left(\xi_{r_n}^a q\right)^{\frac{D}{c_i}}H_{\vec{t},\nu;a,i}(\xi_{c_i}^k(\xi_{r_n}^a q)^{-1/c_i})\times\\ &\left(1+O\left(\frac{1}{D}\right)\right).\end{aligned}$$

□

Corollary 5.6.3. *Let* $m_{\vec{t},\nu,i}=\max\limits_{0\le a\le r_n-1}(m_{\vec{t},\nu;a,i})$. *Let* $0<\delta_1<q^{-1/c_1}$, $\delta_2=\frac{1+\epsilon}{2c_1}$ *for some* $\epsilon>0$ *and let* $C_{\delta_1}=\{z\in\mathbb{C}:|z|=\delta_1\}$ *oriented counterclockwise and* $C_{\delta_2}=\{z\in\mathbb{C}:|z|=q^{-\delta_2}\}$ *oriented clockwise. Then*

$$\frac{1}{2\pi i}\oint_{C_{\delta_1}+C_{\delta_2}}\frac{A_{\vec{t},\nu}(z)}{z^{D+1}}dz=\sum_{i=1}^{\eta}P_{\vec{t},\nu,i}(D)q^{\frac{D}{c_i}}$$

where $P_{\vec{t},\nu,i}$ *is a quasi-polynomial of degree* $m_{\vec{t},\nu;i}-1$ *with leading coefficient*

$$C_{\vec{t},\nu,i}=\sum_{\substack{a=0\\ m_{\vec{t},\nu;a,i}=m_{\vec{t},\nu;i}}}^{r_n-1}\sum_{k=0}^{c_i-1}C_{\vec{t},\nu;a,i,k}.$$

Proof. By Cauchy's Residue Theorem, and the fact that the larger disc, C_{δ_2}, is oriented clockwise,

$$\begin{aligned}\frac{1}{2\pi i}\oint_{C_{\delta_1}+C_{\delta_2}}\frac{A_{\vec{t},\nu}(z)}{z^{D+1}}dz&=\sum_{\substack{i=1\\ m_{\vec{t},\nu;a,i}\neq 0}}^{\eta}\sum_{a=0}^{r_n-1}\sum_{k=0}^{c_i}-\mathrm{Res}_{z=\xi_{c_i}^k\left(q\xi_{r_n}^a\right)^{-1/c_i}}\left(\frac{A_{\vec{t},\nu}(z)}{z^{D+1}}\right)\\ &=\sum_{\substack{i=1\\ m_{\vec{t},\nu;a,i}\neq 0}}^{\eta}\sum_{a=0}^{r_n-1}\sum_{k=0}^{c_i}-P_{\vec{t},\nu;a,i,k}(D)q^{\frac{D}{c_i}}\\ &=\sum_{i=1}^{\eta}P_{\vec{t},\nu,i}(D)q^{\frac{D}{c_i}}\end{aligned}$$

where $P_{\vec{t},\nu,i}$ has degree $(m_{\vec{t},\nu,i}-1)$. Moreover, the only $P_{\vec{t},\nu;a,i,k}$ that contribute to the leading coefficient are the ones where $m_{\vec{t},\nu;a,i}=m_{\vec{t},\nu,i}$.

□

Proposition 5.6.4. *Let*

$$m_i = \max_{\substack{\vec{t}\in\mathcal{R}\\ \nu\in\mathcal{M}}}(m_{\vec{t},\nu,i}).$$

If there exists a solution to (5.2.4), then for every $\epsilon > 0$,

$$|\mathcal{F}_{D;\vec{k},E}| = \sum_{i=1}^{\eta} P_i(D) q^{\frac{D}{c_i}} + O\left(q^{(\frac{1}{2}+\epsilon)\frac{D}{c_1}}\right)$$

where P_i is a quasi-polynomial of degree $(m_i - 1)$ and the leading coefficient of P_i is

$$C_i = \sum_{\substack{\vec{t}\in\mathcal{R}'\\ m_{\vec{t},\nu,i}=m_i}} \sum_{\nu\in\mathcal{M}} \xi_{r_n}^{-\vec{t}\cdot\vec{k}} E^{-\nu} C_{\vec{t},\nu,i}.$$

Otherwise, if there does not exist a solution to (5.2.4), then $|\mathcal{F}_{D,\vec{k},E}| = 0$.

Proof. Recall that

$$\mathcal{F}_{D;\vec{k},E} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{F}_{\vec{d}(\vec{\alpha});\vec{k},E}$$

where the union is over all solutions to (5.2.4) where $D = 2g + 2|G| - 2 - c(\vec{k})$. Therefore, if there are no solutions to (5.2.4), we have an empty union, so $\mathcal{F}_{D;\vec{k},E} = \emptyset$. Therefore, from now on, we will always assume there is a solution to (5.2.4).

Let C_{δ_1} and C_{δ_2} be as defined in Corollary 5.6.3. Then

$$\begin{aligned}
\frac{1}{2\pi i}\oint_{C_{\delta_1}+C_{\delta_2}} \frac{F_{\vec{k},E}(z)}{z^{D+1}}dz &= \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1} \sum_{\vec{t}\in\mathcal{R}'}\sum_{\nu\in\mathcal{M}} \xi_{r_n}^{-\vec{t}\cdot\vec{k}} E^{-\nu} \frac{1}{2\pi i}\oint_{C_{\delta_1}+C_{\delta_2}} \frac{A_{\vec{t},\nu}(z)}{z^{D+1}}dz \\
&= \left(\frac{1}{r_1\cdots r_n}\right)^{\ell+1} \sum_{\vec{t}\in\mathcal{R}'}\sum_{\nu\in\mathcal{M}} \xi_{r_n}^{-\vec{t}\cdot\vec{k}} E^{-\nu} \sum_{i=1}^{\eta} P_{\vec{t},\nu,i}(D) q^{\frac{D}{c_i}} \\
&= \sum_{i=1}^{\eta} P_i(D) q^{\frac{D}{c_i}}
\end{aligned}$$

where P_i is a quasi-polynomial of degree m_i with leading coefficient C_i. To see that the leading coefficient is as claimed, notice that the only $P_{\vec{t},\nu,i}$ that contribute to the leading coefficient are those $\vec{t}\in\mathcal{R}'$ and $\nu\in\mathcal{M}$ such that $m_{\vec{t},\nu,i} = m_i$.

Now, by Proposition 5.4.1, we know that

$$\frac{1}{2\pi i}\oint_{C_{\delta_1}} \frac{F_{\vec{k},E}(z)}{z^{D+1}}dz = -|\mathcal{F}_{D;\vec{k},E}|.$$

Moreover,

$$\left|\frac{1}{2\pi i}\oint_{C_{\delta_2}}\frac{F_{\vec{k},E}(z)}{z^{D+1}}dz\right| = O\left(q^{(\frac{1}{2}+\epsilon)\frac{D}{c_1}}\right)$$

where the implied constant is the maximum values of $F_{\vec{k},E}(z)$ on C_{δ_2}. □

Remark 5.6.5. If we let $c(\vec{\alpha})$ be any integers, then we could have that $\frac{D}{c_i} \leq \frac{D}{2c_1}$ and thus part of the main term could be absorbed into the error term. However, if we define $c(\vec{\alpha})$ as in (5.2.1), then we actually have that $\frac{D}{c_i} > \frac{D}{2c_1}$ for all $i = 1, \dots, \eta$. So for small enough ϵ, none of our main terms can be absorbed into the error term.

5.7 Curves

Ideally, we would like to say that every curve, C, such that $\mathrm{Gal}(C) = G$, $g(C) = g$, comes from an element $\hat{\mathcal{F}}_{\vec{d}(\vec{\alpha})}$ such that $\vec{d}(\vec{\alpha})$ satisfies (5.2.2). Unfortunately, this is not true.

For example, if we consider the set $\mathcal{F}_{(0,d_2,0)}$ such that $2g+6 = 2d_2$ and $2d_2 \equiv 0 \pmod 4$. Then $(0, d_2, 0)$ satisfies (5.2.2) for $G = 4\mathbb{Z}$ and we would hope that this would correspond to a curve with $\mathrm{Gal}(C) = \mathbb{Z}/4\mathbb{Z}$ and $g(C) = g$. However, an element of $\mathcal{F}_{(0,d_2,0)}$ would look like $(1, f_2, 1)$ where f_2 is a square-free polynomial of degree d_2. This would correspond to a curve with affine model $Y^4 = f_2^2$, which clearly has $K(C) = K(\sqrt{f_2})$ and so $\mathrm{Gal}(C) = \mathbb{Z}/2\mathbb{Z}$. Moreover,

$$g(C) = \frac{d_2 - 2}{2} = \frac{g+3-2}{2} = \frac{g-1}{2} + 1.$$

It is easy to see how this argument can be extended to any group G that does not have prime order. Indeed, what we will show in this section that the elements of $\mathcal{F}_{\vec{d}(\vec{\alpha})}$ correspond to *monic* curves whose Galois group is a *subgroup* of G. First, we must explain what we mean by monic curves.

Definition 5.7.1. We call a smooth, projective curve, C, **monic** if

$$K(C) = K\left(\sqrt[r_1]{F_1(X)}, \dots, \sqrt[r_n]{F_n(X)}\right)$$

where F_j is a monic polynomial for $j = 1, \dots, n$.

Remark 5.7.2. When we talk about all the subgroups of G, we mean all the different possible subsets of G that are subgroups of G. That is, two subgroups $H, H' \subset G$ are said to be the same subgroup if and only if they are equal as subsets. For example, if $G = \mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$, then the subgroups

$$\{(a, 0) : 0 \leq a \leq Q - 1\}$$

$$\{(0, a) : 0 \leq a \leq Q - 1\}$$

$$\{(a, a) : 0 \leq a \leq Q - 1\}$$

are all different even though they are all isomorphic to $\mathbb{Z}/Q\mathbb{Z}$.

Proposition 5.7.3. *Let*

$$M(G, g) = \{C, \ monic \ : Gal(C) = H \subset G, g(C) = \frac{g-1}{|G|/|H|} + 1\}.$$

Then there is a natural bijection from elements of

$$\bigcup_{\vec{d}(\vec{\alpha})} \mathcal{F}_{\vec{d}(\vec{\alpha})}$$

to $M(G, g)$ *where the union is over all* $\vec{d}(\vec{\alpha})$ *that satisfies* (5.2.2).

Proof. Let $(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}$ for some fixed $\vec{d}(\vec{\alpha})$ that satisfies (5.2.2). Define

$$\mathcal{R}^* = \{\vec{\alpha} \in \mathcal{R} : d(\vec{\alpha}) \neq 0\}.$$

For every $\vec{\alpha} \in \mathcal{R}$, we can identify it as element in G in the natural way. Let $H \subset G$ be the subgroup that is generated by $\mathcal{R}^*$ under this identification. (From now on, in this proof, we will identify elements of H and G with elements of $\mathcal{R}$). We will show that $\mathrm{Gal}(C) = H$.

There exists some $s_j | r_j$ (where, potentially, some of the $s_j = 1$) we get

$$H \cong \mathbb{Z}/s_1\mathbb{Z} \times \cdots \times \mathbb{Z}/s_n\mathbb{Z}.$$

Let $\vec{\alpha}_j \in H$ be a generating set of H such that the order of α_j is s_j. Therefore, if $\vec{\alpha} \in \mathcal{R}$, we can find α_j^* such that $0 \leq \alpha_j^* \leq s_j - 1$ and

$$\vec{\alpha} = \sum_{j=1}^{n} \alpha_j^* \vec{\alpha}_j.$$

If we let $\vec{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n})$ then for all $\vec{\alpha} \in \mathcal{R}^*$,

$$\alpha_k = \sum_{j=1}^{n} \alpha_j^* \alpha_{j,k}.$$

Now, a basis element of $K(C) = K\left(\sqrt[r_1]{F_1(X)}, \ldots, \sqrt[r_n]{F_n(X)} \right)$ will be

$$\prod_{k=1}^{n} F_k(X)^{\frac{m_k}{r_k}} = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\sum_{k=1}^{n} \frac{\alpha_k m_k}{r_k}} = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\sum_{k=1}^{n} \frac{m_k}{r_k} \sum_{j=1}^{n} \alpha_j^* \alpha_{j,k}}$$

for some values of $m_k, k = 1, \ldots, n$. Therefore, we can define an action by $h = (h_1, \ldots, h_n) \in H$ on the basis elements by

$$h\left(\prod_{k=1}^{n} F_k(X)^{\frac{m_k}{r_k}} \right) = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\sum_{k=1}^{n} \frac{m_k}{r_k} \sum_{j=1}^{n} h_j \alpha_j^* \alpha_{j,k}}.$$

Therefore if $h \neq (0, \ldots, 0)$, there will be a $\vec{\alpha} \in \mathcal{R}^*$ such that

$$\sum_{k=1}^{n} \frac{m_k}{r_k} \sum_{j=1}^{n} h_j \alpha_j^* \alpha_{j,k} \notin \mathbb{Z}.$$

Hence, every non-trivial element of H gives a non-trivial automorphism of $K(C)$ and $H \subset \mathrm{Gal}(K(C)/K) = \mathrm{Gal}(C)$.

Define

$$F_j^* = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\alpha_j^*}, j = 1, \ldots, n.$$

Since $\vec{\alpha}_j$ has order s_j we get $s_j(\vec{\alpha}_j) = (0, \ldots, 0)$. Therefore, $s_j \alpha_{j,k} \equiv 0 \pmod{r_k}$ and we can find $\alpha'_{j,k}$ such that

$$\alpha_{j,k} = \frac{r_k}{(s_j, r_k)} \alpha'_{j,k}.$$

Therefore,

$$\sqrt[r_k]{F_k(X)} = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\alpha_k / r_k} = \prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\frac{1}{r_k} \sum_{j=1}^{n} \alpha_j^* \alpha_{j,k}} = \prod_{j=1}^{n} \left(\prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\alpha_j^*} \right)^{\alpha_{j,k}/r_k}$$

$$= \prod_{j=1}^{n} \left(\prod_{\vec{\alpha} \in \mathcal{R}^*} f_{\vec{\alpha}}^{\alpha_j^*} \right)^{\alpha'_{j,k}/(s_j, r_k)} = \prod_{j=1}^{n} \left(\sqrt[s_j]{F_j^*(X)} \right)^{\alpha'_{j,k} s_j / (s_j, r_k)}.$$

Hence,

$$K\left(\sqrt[r_1]{F_1(X)}, \ldots, \sqrt[r_n]{F_n(X)} \right) \subset K\left(\sqrt[s_1]{F_1^*(X)}, \ldots, \sqrt[s_n]{F_n^*(X)} \right).$$

Clearly $\mathrm{Gal}\left(K\left(\sqrt[s_1]{F_1^*(X)},\ldots,\sqrt[s_n]{F_n^*(X)}\right)/K\right)\subset H$. Hence $\mathrm{Gal}(C)\subset H$ and therefore $\mathrm{Gal}(C)=H$.

It remains to show that $g(C)=\frac{g-1}{|G|/|H|}+1$.

Recall, $e(\vec{\alpha})=\mathrm{lcm}\left(\frac{r_j}{(r_j,\alpha_j)}\right)$. Then $e(\vec{\alpha})$ will be the order of $\vec{\alpha}$ as viewed as an element in G. Therefore, if $\vec{\alpha}\in\mathcal{R}^*$, then

$$e(\vec{\alpha})=\mathrm{lcm}\left(\frac{r_j}{(r_j,\alpha_j)}\right)=\mathrm{lcm}\left(\frac{s_i}{(s_i,\alpha_i^*)}\right):=e^*(\vec{\alpha})$$

since $e^*(\vec{\alpha})$ would the order of $\vec{\alpha}^*$ as viewed as an element in H (which would be the same as $\vec{\alpha}$ in G). Therefore,

$$c(\vec{\alpha})=|G|-\frac{|G|}{e(\vec{\alpha})}=\frac{|G|}{|H|}\left(|H|-\frac{|H|}{e^*(\vec{\alpha})}\right):=\frac{|G|}{|H|}c^*(\vec{\alpha}).$$

Likewise, if we define $d_j^*=\deg(F_j^*)=\sum_{\vec{\alpha}\in\mathcal{R}^*}\alpha_j^*d(\vec{\alpha})$, then $e^*(\vec{d^*})=e(\vec{d})$ and $\frac{|G|}{|H|}c^*(\vec{d^*})=c(\vec{d})$.

Since $\vec{d}(\vec{\alpha})$ satisfies (5.2.2), we have

$$\begin{aligned}2g+2|G|-2&=\sum_{\vec{\alpha}\in\mathcal{R}}c(\vec{\alpha})d(\vec{\alpha})+c(\vec{d})=\sum_{\vec{\alpha}\in\mathcal{R}^*}c(\vec{\alpha})d(\vec{\alpha})+c(\vec{d})\\&=\frac{|G|}{|H|}\left(\sum_{\vec{\alpha}\in\mathcal{R}^*}c^*(\vec{\alpha})d(\vec{\alpha})+c^*(\vec{d^*})\right).\end{aligned}$$

That is,

$$\left(\sum_{\vec{\alpha}\in\mathcal{R}^*}c^*(\vec{\alpha})d(\vec{\alpha})+c(\vec{d^*})\right)=2\left(\frac{g-1}{|G|/|H|}+1\right)+2|H|-2$$

Therefore, $(f_{\vec{\alpha}})$ corresponds to a monic curve C with $\mathrm{Gal}(C)=H$ and, by the Riemann-Hurwitz formula, $g(C)$ is $\frac{g-1}{|G|/|H|}+1$.

□

Therefore, for any monic curve with $\mathrm{Gal}(C)=H\subset G$ and $g(C)=\frac{g-1}{|G|/|H|}+1$, we can find $(f_{\vec{\alpha}})\in\mathcal{F}_{\vec{d}(\vec{\alpha})}$ such that $\vec{d}(\vec{\alpha})$ satisfies (5.2.2) and C has an affine model of the form

$$Y_1^{r_1}=F_1(X)\qquad\ldots\qquad Y_n^{r_n}=F_n(X)$$

where

$$F_j(X)=\prod_{\vec{\alpha}\in\mathcal{R}}f_{\vec{\alpha}}(X)^{\alpha_j}.$$

Corollary 5.7.4. *Let*

$$M_{\vec{k},E}(G,g) = \{C,\ monic\ : Gal(C) = H \subset G, g(C) = \frac{g-1}{|G|/|H|} + 1, \deg F_j \equiv k_j\ (mod\ r_j)$$
$$\chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1\ldots,\ell, j = 1,\ldots,n\}.$$

Then there is a natural bijection from elements of $\mathcal{F}_{2g+2|G|-2-c(\vec{k});\vec{k},E}$ *to* $M_{\vec{k},E}(G,g)$.

Proof. Follows immediately from Proposition 5.7.3 and the definition of $\mathcal{F}_{2g+2|G|-2-c(\vec{k});\vec{k},E}$. □

5.8 Inclusion-Exclusion of Abelian Groups

As of right now we have determined the size of the set of curves with Galois group the subgroup of G. What we want is the size of the set of curves with Galois group equal to G. Since our G was arbitrary we can perform an inclusion-exclusion argument on abelian groups. Luckily, this has already been done by Delsarte [5].

Let $\mathcal{G}$ be the set of all abelian groups. Define a function

$$\mu : \mathcal{G} \to \mathbb{Z}$$

by

$$\mu\left(\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z}\right) = \begin{cases} (-1)^n p^{\frac{n(n-1)}{2}} & a_1 = \cdots = a_n = 1 \\ 0 & \text{otherwise} \end{cases}.$$

To finish the definition if $G = G_1 \times G_2$ such that $(|G_1|, |G_2|) = 1$, then $\mu(G) = \mu(G_1)\mu(G_2)$. Then we have the property that

$$\sum_{H \subset G} \mu(H) = \begin{cases} 1 & G = \{e\} \\ 0 & \text{otherwise} \end{cases}. \tag{5.8.1}$$

Remark 5.8.1. This formula requires that we sum up over all subgroups of G in the sense of Remark 5.7.2. Hence why it is important that we define $M(G,g)$ and $M_{\vec{k},E}(G,g)$ in the way that we do.

For an example of (5.8.1) consider the group $\mathbb{Z}/Q^2\mathbb{Z}$, for Q a prime. Then the subgroups are $\{e\}, \mathbb{Z}/Q\mathbb{Z}$ and $\mathbb{Z}/Q^2\mathbb{Z}$ and each of them appear once. Therefore,

$$\sum_{H\subset\mathbb{Z}/Q^2\mathbb{Z}} \mu(H) = \mu(\{e\}) + \mu(\mathbb{Z}/Q\mathbb{Z}) + \mu(\mathbb{Z}/Q^2\mathbb{Z})$$
$$= 1 + (-1) + 0 = 0.$$

Whereas if we consider the group $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$, for Q a prime, then the subgroups would be $\{e\}$, $\mathbb{Z}/Q\mathbb{Z}$ and $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$. Obviously $\{e\}$ and $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$ appear only once however, $\mathbb{Z}/Q\mathbb{Z}$ can appear many times. It is easy to see that all the subgroups of $\mathbb{Z}/Q\mathbb{Z}$ lying in $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$ will be generated by $(1, a)$, $a \in \mathbb{Z}/Q\mathbb{Z}$ or $(0, 1)$. That is, there are $Q + 1$ different subgroups of $\mathbb{Z}/Q\mathbb{Z}$ appearing in $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z}$. Therefore,

$$\sum_{H\subset\mathbb{Z}/Q\mathbb{Z}\times\mathbb{Z}/Q\mathbb{Z}} \mu(H) = \mu(\{e\}) + (Q+1)\mu(\mathbb{Z}/Q\mathbb{Z}) + \mu(\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/Q\mathbb{Z})$$
$$= 1 + (Q+1)(-1) + Q = 0.$$

This allows us to perform Möbius inversion on $M(G, g)$.

Lemma 5.8.2. *Let*

$$N^*(G, g) = \{C,\ monic\ : Gal(C) = G, g(C) = g\}$$

then

$$|N^*(G, g)| = \sum_{H\subset G} \mu(G/H) \left| M\left(H, \frac{g-1}{|G|/|H|} + 1\right)\right|.$$

Likewise, if

$$N^*_{\vec{k},E}(G, g) = \{C,\ monic\ : Gal(C) = G, g(C) = \frac{g-1}{|G|/|H|} + 1, \deg F_j \equiv k_j\ (mod\ r_j)$$
$$\chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1\ldots, \ell, j = 1, \ldots, n\}.$$

then $|N^*_{\vec{k},E}(G, g)| = \sum_{H\subset G} \mu(G/H) \left| M_{\vec{k},E}\left(H, \frac{g-1}{|G|/|H|} + 1\right)\right|$.

Proof. Straight from the definition we get

$$|M(G, g)| = \sum_{H\subset G} \left| N^*\left(H, \frac{g-1}{|G|/|H|} + 1\right)\right|.$$

Therefore,

$$\begin{aligned}\sum_{H\subset G}\mu(G/H)\left|M\left(H,\frac{g-1}{|G|/|H|}+1\right)\right| &= \sum_{H\subset G}\mu(G/H)\sum_{H'\subset H}\left|N^*\left(H',\frac{g-1}{|G|/|H'|}+1\right)\right| \\ &= \sum_{H'\subset G}\left|N^*\left(H',\frac{g-1}{|G|/|H'|}+1\right)\right|\sum_{H'\subset H\subset G}\mu(G/H) \\ &= \sum_{H'\subset G}\left|N^*\left(H',\frac{g-1}{|G|/|H'|}+1\right)\right|\sum_{H''\subset G/H'}\mu(H'') \\ &= |N^*(G,g)|.\end{aligned}$$

The proof of the likewise is analogous. □

5.9 Curves Revisited

In this section we will prove the first part of Theorem 1.4.1 and Proposition 1.4.2. But first, we need some more notation, in order to handle the subgroups of G that appear.

As in Section 5.7, there is a natural bijection from $G\setminus\{e\}$ to $\mathcal{R}$. For every $H\subset G$, let $\mathcal{R}_H$ be the image of H under this natural bijection. Recall that $\eta=\eta_G$ is the number of non-trivial divisors of $\exp(G)=r_n$. Then, for all $\vec{t}\in\mathcal{R}'$, $\nu\in\mathcal{M}$, $0\le a\le r_n-1$ and $1\le i\le\eta_G$, define the analogous objects

$$\begin{aligned}\mathcal{R}_{H,\nu} &= \{\vec{\alpha}\in\mathcal{R}_H : \nu\vec{\alpha}=0\} \\ \mathcal{R}_{H,\vec{t},\nu;a,i} &= \{\vec{\alpha}\in\mathcal{R}_{H,\nu} : c(\vec{\alpha})=c_i \text{ and } \vec{t}\cdot\vec{\alpha}\equiv a \pmod{r_n}\} \\ m_{H,t,\nu;a,i} &= |\mathcal{R}_{H,\vec{t},\nu;a,i}| \\ m_{H,\vec{t},\nu,i} &= \max_{0\le a\le r_n-1}(m_{H,\vec{t},\nu;a,i}) \\ m_{H,i} &= \max_{\substack{\vec{t}\in\mathcal{R}'\\ \nu\in\mathcal{M}}}(m_{H,\vec{t},\nu,i})\end{aligned}$$

Now,

$$m_{H,i}=m_{H,0,0;0,i}=|\{\vec{\alpha}\in\mathcal{R}_H : c(\vec{\alpha})=c_i\}|=\phi_H(s_i)$$

since $c_i=|G|-\frac{|G|}{e(\vec{\alpha})}$ and $e(\vec{\alpha})$ is the order of $\vec{\alpha}$ as seen as an element in G. So, if $\vec{\alpha}\in\mathcal{R}_H$, then it can be seen as element in H and will have the same order. Notice, however, that we could have $\phi_H(s)=0$ even if $\phi_G(s)\neq 0$.

Theorem 5.9.1. *Let*

$$N_{\vec{k},E}(G,g) = \{C : Gal(C) = G, g(C) = \frac{g-1}{|G|/|H|} + 1, \deg F_j \equiv k_j \ (mod\ r_j)$$
$$\chi_{r_j}(F_j(x_i)) = \epsilon_{i,j}, i = 1\ldots,\ell, j = 1,\ldots,n\}.$$

If there exists a solution to (5.2.4) then

$$|N_{\vec{k},E}(G,g)| = \sum_{j=1}^{\eta} P_{j;\vec{k},E}(2g) q^{\frac{2g+2|G|-2-c(\vec{k})}{c_j}} + O\left(q^{\frac{(1+\epsilon)g}{c_1}}\right)$$

where the c_j and η are as above and $P_{j;\vec{k},E}$ is a quasi-polynomial of degree at most $\phi_G(s_j)-1$.

Otherwise, if there is no solution to (5.2.4), $|N_{\vec{k},E}(G,g)| = 0$.

Proof. If C is any curve with $\mathrm{Gal}(C) = G$, $g(C) = g$, then

$$K(C) = K(\sqrt[r_1]{c_1 F_1(X)}, \ldots, \sqrt[r_n]{c_n F_n(X)})$$

where $c_j \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^{r_j}$ and F_j are monic. Since the F_j are algebraically independent, all the choices of the c_j contribute unique extensions; that is, $N_{\vec{k},E}(G,g) = r_1 \cdots r_n N^*_{\vec{k},E}(G,g)$.

Further

$$\begin{aligned}|N^*_{\vec{k},E}(G,g)| &= \sum_{H\subset G} \mu(G/H) \left| M_{\vec{k},E}\left(H, \frac{g-1}{|G|/|H|} + 1\right)\right| \\ &= \sum_{H\subset G} \mu(G/H) \sum_{\vec{d}(\vec{\alpha})} |\mathcal{F}_{\vec{d}(\vec{\alpha})}|\end{aligned}$$

where the inner sum is over all $\vec{d}(\vec{\alpha})$ that satisfy

$$\begin{aligned} & d(\vec{\alpha}) = 0, \vec{\alpha} \notin \mathcal{R}_H \\ & d_j = \sum_{\vec{\alpha}\in\mathcal{R}} \alpha_j d(\vec{\alpha}) \equiv k_j \ (\mathrm{mod}\ r_j), j = 1,\ldots,n \\ & \sum_{\vec{\alpha}\in\mathcal{R}} c(\vec{\alpha}) d(\vec{\alpha}) = 2g + 2|G| - 2 - c(\vec{k}).\end{aligned} \tag{5.9.1}$$

Therefore, if there are no solutions to (5.2.4), then the above sum is empty and we have that $|N_{\vec{k},E}(G,g)| = 0$. From now on, we will assume that there exists a solution to (5.2.4) so that the above sum is non-empty. Further, note that if $g \not\equiv 1 \pmod{|G|/|H|}$ for some

H then there would be no solutions to (5.9.1) as this would correspond to a curve with a non-integer genus, which is impossible.

Moreover, if $H \cong \mathbb{Z}/s_1\mathbb{Z} \times \ldots \mathbb{Z}/s_n\mathbb{Z}$ where $s_j | r_j$, then $\mathcal{R}_H$ can be identified with the set

$$[0, \ldots, s_1 - 1] \times \cdots \times [0, \ldots, s_n - 1] \setminus \{(0, \ldots, 0)\}.$$

This allows us to apply the results of Section 5.6 to obtain

$$|N^*_{\vec{k},E}(G, g)| = \sum_{H \subset G} \mu(G/H) \left(\sum_{j=1}^{\eta_H} P_{H;\vec{k},E,j}(2g) q^{\frac{2g+2|G|-2}{|G|-\frac{|G|}{s_{H,j}}}} + O\left(q^{\frac{(1+\epsilon)g}{|G|-\frac{|G|}{s_{H,1}}}} \right) \right)$$

where η_H is the number of non-trivial divisors of $\exp(H)$ and $1 = s_{H,0} < s_{H,1} < \cdots < s_{H,\eta_H} = \exp(H)$ are the divisor of $\exp(H)$ and $P_{H;\vec{k},E,j}$ is a quasi-polynomial of degree $\phi_H(s_{H,j}) - 1$ if $g \equiv 1 \pmod{|G|/|H|}$ and identically the 0 polynomial otherwise. Since $\exp(H) | \exp(G)$ for all $H \subset G$ and $\phi_H(s_{H,j}) \leq \phi_G(s_{G,j})$, we can write

$$|N^*_{\vec{k},E}(G, g)| = \sum_{j=1}^{\eta} P_{\vec{k},E,j}(2g) q^{\frac{2g+2|G|-2}{c_j}} + O\left(q^{\frac{(1+\epsilon)g}{c_1}} \right)$$

where c_j and $\eta = \eta_G$ are as above and $P_{\vec{k},E,j}$ is a quasi-polynomial of degree at most $\phi_G(s_j) - 1$.

□

Corollary 5.9.2. *If we let $N(G, g) = \{C : Gal(C) = G, g(C) = g\}$, then if there exists a solution to (5.2.4)*

$$|N(G, g)| = \sum_{j=1}^{\eta} P_j(2g) q^{\frac{2g+2|G|-2}{c_j}} + O\left(q^{\frac{(1+\epsilon)g}{c_1}} \right).$$

where P_j is a polynomial of at most degree $\phi_G(s_j) - 1$. Otherwise, if there are no solutions to (5.2.4), $|N(G, g)| = 0$.

Proof. Recall that E as in Theorem 5.9.1 is an $\ell \times n$ matrix, were $0 \leq \ell \leq q$. If we choose $\ell = 0$, then the condition of E goes away. Therefore,

$$\begin{aligned} |N(G, g)| &= \sum_{\vec{k} \in \mathcal{R}'} |N_{\vec{k},\emptyset}(G, g)| \\ &= \sum_{\vec{k} \in \mathcal{R}'} \left(\sum_{j=1}^{\eta} P_{j;\vec{k},\emptyset}(2g) q^{\frac{2g+2|G|-2-c(\vec{k})}{c_j}} + O\left(q^{\frac{(1+\epsilon)g}{c_1}} \right) \right) \end{aligned}$$

$$= \sum_{j=1}^{\eta} P_j(2g) q^{\frac{2g+2|G|-2}{c_j}} + O\left(q^{\frac{(1+\epsilon)g}{c_1}}\right)$$

where we denote $\emptyset$ as the empty $0 \times n$ matrix.

□

Remark 5.9.3. We actually get that

$$P_1(2g) = c_{\phi_G(s_1)-1}(g) g^{\phi_G(s_1)-1} + c_{\phi_G(s_1)-2}(g) g^{\phi_G(s_1)-2} + \dots$$

for some periodic function $c_{\phi_G(s_1)-1}(g)$ with integer period. While we can write down a formula for $c_{\phi_G(s_1)-1}(g)$ it is not clear exactly what it is nor that it is non-zero. However, Wright's result tells us that in every interval of length $|G| - \frac{|G|}{Q}$, there exists at least one g such that $c_{\phi_G(s_1)-1}(g) \neq 0$. Therefore we can conclude that $P_1(2g)$ is a quasi-polynomial of *exact* degree $\phi_G(s_1) - 1$.

5.10 $G = (\mathbb{Z}/Q\mathbb{Z})^n$

In this section we will determine the leading coefficient of $P_{\vec{k},E,1}$ and P_1 that appear in Theorem 5.9.1 and Corollary 5.9.2 in the case that $G = (\mathbb{Z}/Q\mathbb{Z})^n$. This will prove the second half of Theorem 1.4.1 and Proposition 1.4.2.

The reason we are able to determine the leading coefficient of P_1 in this case is that the genus and Möbius formulas become simpler when $G = (\mathbb{Z}/Q\mathbb{Z})^n$. Indeed, in this case (5.2.2) becomes

$$2g + 2Q^n - 2 = \begin{cases} (Q^n - Q^{n-1}) \sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha}) & d_j \equiv 0 \pmod{Q}, j = 1, \dots, n \\ (Q^n - Q^{n-1})(\sum_{\vec{\alpha} \in \mathcal{R}} d(\vec{\alpha}) + 1) & \text{otherwise} \end{cases} \tag{5.10.1}$$

Therefore, by Theorem 5.9.1, we get that if $2g + 2Q^n - 2 \equiv 0 \pmod{Q^n - Q^{n-1}}$ then

$$N_{\vec{k},E}((\mathbb{Z}/Q\mathbb{Z}^n), g) = \begin{cases} P_{\vec{0},E}(2g) q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}} & \vec{k} = \vec{0} \\ P_{\vec{k},E}(2g) q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}-1} & \vec{k} \neq \vec{0} \end{cases} + O\left(q^{(1+\epsilon)\frac{g}{Q^n-Q^{n-1}}}\right)$$

for some polynomial $P_{\vec{k},E}$ whose degree is at most $\phi_G(Q) - 1 = Q^n - 2$. In fact we will show it has exact degree $Q^n - 2$. For the rest of this section we will always be assuming that $2g + 2Q^n - 2 \equiv 0 \pmod{Q^n - Q^{n-1}}$.

We see that in this case we get $c(\vec{\alpha}) = c(\vec{d}) = Q^n - Q^{n-1}$ for all $\vec{\alpha} \in \mathcal{R}$. Therefore, since we always assumed $c(\vec{\alpha})$ was arbitrary from Sections 5.2 to 5.6, we can apply the results therein to the case $c(\vec{\alpha}) = c(\vec{d}) = 1$ and $D = \frac{2g+2Q^n-2}{Q^n-Q^{n-1}} \in \mathbb{N}$ in order to find the leading coefficient of $P_{\vec{k},E}$.

Remark 5.10.1. By setting $D = \frac{2g+2Q^n-2}{Q^n-Q^{n-1}}$ instead of just $2g + 2Q^n - 2$, we are now counting by *conductor* instead of discriminant (genus). This is more analogous to what Bucur, et al. did in [1]. Because we can easily switch to counting by conductor is why it is easier to compute the constant in this case

In this setting, for all $\vec{t} \in \mathcal{R}'$ and $\nu \in \mathcal{M}$, we have that $A_{\vec{t},\nu}(z)$ will have poles of order $m_{\vec{t},\nu;a}$ when $z = (q\xi_Q^a)^{-1}$ where

$$m_{\vec{t},\nu;a} = |\{\vec{\alpha} \in \mathcal{R}_\nu : \vec{t} \cdot \vec{\alpha} \equiv a \pmod{Q}\}|.$$

Now, since $(\mathbb{Z}/Q\mathbb{Z})^n$ can be viewed as a vector space over the field $\mathbb{Z}/Q\mathbb{Z}$, we get that the action of ν and $\vec{t}$ on $\mathcal{R}$ are vector space morphisms. Therefore, the set

$$\{\vec{\alpha} \in \mathcal{R}_\nu : \vec{t} \cdot \vec{\alpha} \equiv a \pmod{Q}\} \subsetneq \mathcal{R}$$

unless $\nu = 0$, $\vec{t} = \vec{0}$ and $a = 0$. In which case we get

$$m_{\vec{0},0;0} = |\mathcal{R}| = Q^n - 1.$$

Therefore, combining the results of Section 5.6, we get that the leading coefficient of $P_{\vec{k},E}$ is

$$C_{\vec{k},E} = \frac{1}{(Q^n-2)!}\left(1-q^{-1}\right)^{Q^n-1} \prod_P \left(\frac{|P|^{Q^n-1} + (Q^n-1)|P|^{Q^n-2}}{(|P|+1)^{Q^n-1}}\right)\left(\frac{q}{Q^n(q+Q^n-1)}\right)^\ell$$

$$= \frac{1}{(Q^n-2)!}\frac{L_{Q^n-2}}{\zeta_q(2)^{Q^n-1}}\left(\frac{q}{Q^n(q+Q^n-1)}\right)^\ell$$

Notice that $C_{\vec{k},E}$ does not depend on $\vec{k}$ or E. Therefore, if we set $\ell = 0$ and sum over all $\vec{k}$, we get

$$N((\mathbb{Z}/Q\mathbb{Z})^n, g) = \sum_{\vec{k} \in \mathcal{R}'} N_{\vec{k},\emptyset}((\mathbb{Z}/Q\mathbb{Z})^n, g)$$

$$
\begin{aligned}
=&P_{\vec{0},\emptyset}\left(\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}\right)q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}}+\sum_{\vec{k}\in\mathcal{R}}P_{\vec{k},\emptyset}\left(\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}\right)q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}-1}\\
&+O\left(q^{(1+\epsilon)\frac{g}{Q^n-Q^{n-1}}}\right)\\
=&P\left(\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}\right)q^{\frac{2g+2Q^n-2}{Q^n-Q^{n-1}}}+O\left(q^{(1+\epsilon)\frac{g}{Q^n-Q^{n-1}}}\right)
\end{aligned}
$$

where P is a polynomial of degree Q^n-2 with leading coefficient

$$
\begin{aligned}
C&=C_{0,\emptyset}+\sum_{\vec{k}\in\mathcal{R}}C_{\vec{k},\emptyset}q^{-1}\\
&=\frac{1}{(Q^n-2)!}\frac{q+Q^n-1}{q}\frac{L_{Q^n-2}}{\zeta_q(2)^{Q^n-1}}
\end{aligned}
$$

which is exactly the analogue of the constant in [1].

Since the condition $F_j(x_{q+1})\neq 0$, where x_{q+1} is the point at infinity, is equivalent to saying $\deg(F_j)\equiv 0 \pmod{r_j}$ for $j=1,\dots,n$, we can state an analogue of Proposition 2.1.12.

Let $\epsilon_{i,j}\in\mu_{r_j}$ for $i=1,\dots,q+1$ and $j=1,\dots,n$. Then as $g\to\infty$

$$
\begin{aligned}
&\frac{|\{C\in\mathcal{H}_{G,g}:\chi_{r_j}(F_j(x_i))=\epsilon_{i,j},i=1,\dots,q+1,j=1,\dots,n\}|}{|\mathcal{H}_{G,g}|}\\
=&\frac{\frac{1}{Q^n}|N_{\vec{0},E}(G,g)|}{|N(G,g)|}=\left(\frac{q}{Q^n(q+Q^n-1)}\right)^{q+1}\left(1+O\left(\frac{1}{g}\right)\right)
\end{aligned}
$$

where the $\frac{1}{Q^n}$ factor in the first equality comes from the fact the leading coefficients of the F_j must satisfy $\chi_{r_j}(c_j)=\epsilon_{q+1,j}$.

Finally, if we go through the work of Section 4, using the above result instead of Proposition 2.1.12, we can show that, as $g\to\infty$ we have

$$
\frac{|\{C\in\mathcal{H}_{G,g}:\#C(\mathbb{P}^1(\mathbb{F}_q))=M\}|}{|\mathcal{H}_{G,g}|}=\text{Prob}\left(\sum_{i=1}^{q+1}X_i=M\right)\left(1+O\left(\frac{1}{g}\right)\right)
$$

where the X_i are *i.i.d.* random variables taking value 0, Q^n or Q^{n-1} such that

$$
X_i=\begin{cases}
Q^{n-1} & \text{with probability } \frac{Q^n-1}{Q^{n-1}(q+Q^n-1)}\\
Q^n & \text{with probability } \frac{q}{Q^n(q+Q^n-1)}\\
0 & \text{with probability } \frac{(Q^n-1)(q+Q^n-Q)}{Q^n(q+Q^n-1)}
\end{cases}.
$$

Chapter 6

Bibliography

[1] Alina Bucur, Chantal David, Brooke Feigon, Nathan Kaplan, Matilde Lalın, Ekin Ozman, and Melanie Mathett Wood, *The distribution of points on cyclic covers of genus g*, preprint (2015).

[2] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalın, *Biased statistics for traces of cyclic p-fold covers over finite fields*, WIN–Women in Numbers: Research Directions in Number Theory **60** (2009), 121–143.

[3] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, International Mathematics Research Notices (2009), rnp162.

[4] Henri Cohen, F Diaz Y Diaz, and Michel Olivier, *On the density of discriminants of cyclic extensions of prime degree*, Journal fur die Reine und Angewandte Mathematik **550** (2002), 169–210.

[5] S Delsarte, *Fonctions de mobius sur les groupes abeliens finis*, Annals of Mathematics (1948), 600–609.

[6] David Steven Dummit and Richard M Foote, *Abstract algebra*, vol. 1984, Wiley Hoboken, 2004.

[7] Robin Hartshorne, *Algebraic geometry*, vol. 52, Springer Science & Business Media, 1977.

[8] Nicholas M Katz and Peter Sarnak, *Random matrices, frobenius eigenvalues, and monodromy*, vol. 45, American Mathematical Soc., 1999.

[9] Pär Kurlberg and Zeév Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, Journal of Number Theory **129** (2009), no. 3, 580–587.

[10] Elisa Lorenzo, Giulio Meleleo, Piermarco Milione, and Alina Bucur, *Statistics for biquadratic covers of the projective line over finite fields*, arXiv preprint arXiv:1503.03276 (2015).

[11] Władysław Narkiewicz, *Number theory*, World Scientific, 1983.

[12] Michael Rosen, *Number theory in function fields*, vol. 210, Springer Science & Business Media, 2013.

[13] André Weil, *Sur les courbes algébriques et les variétés qui s' en déduisent*, no. 1041, Hermann, 1948.

[14] David J Wright, *Distribution of discriminants of abelian extensions*, Proceedings of the London Mathematical Society **3** (1989), no. 1, 17–50.