DISTRIBUTION OF POINTS ON ABELIAN COVERS OVER
FINITE FIELDS

PATRICK MEISNER

ABSTRACT. We determine in this paper the distribution of the number of
points on the covers of $\mathbb{P}^1(\mathbb{F}_q)$ such that $K(C)$ is a Galois extension and
$\text{Gal}(K(C)/K)$ is abelian when $q$ is fixed and the genus, $g$, tends to infinity. This generalizes the work of Kurlberg and Rudnick and Bucur, David,
Feigon and Lalin who considered different families of curves over $\mathbb{F}_q$. In all
cases, the distribution is given by a sum of $q + 1$ random variables.

1. Introduction

Let $q$ be a power of a prime and $C$ a smooth, projective curve over $\mathbb{F}_q$. Denote
$\mathbb{F}_q(X)$ as $K$ and $K(C)$ as the field of functions of $C$. Then $K(C)$ is a finite
extension of $K$. Moreover, if we fix a copy of $\mathbb{P}^1(\mathbb{F}_q)$, then every finite extension of
$K$ corresponds to smooth, projective curve (Corollary 6.6 and Theorem 6.9 from
Chapter I of [5]).

If $K(C)/K$ is Galois, then denote $\text{Gal}(C) = \text{Gal}(K(C)/K)$. Let $g(C)$ be the
genus of $C$. Define the family of smooth, projective curves

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

We want to determine the probability, that a random curve in this family has a
given number of points. That is, for every $N \in \mathbb{Z}_{\geq 0}$, we want to determine

$$\text{Prob}(C \in \mathcal{H}_{G, g} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = N) = \frac{|\{ C \in \mathcal{H}_{G, g} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = N \}|}{|\mathcal{H}_{G, g}|}.$$ 

It is well know that

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 - \text{Tr}(\text{Frob}_q)$$

where $\text{Frob}_q$ is the $q^{th}$-power Frobenius. Moreover, a classical result due to Katz
and Sarnak [6] says that if $g$ is fixed and we let $q$ tend to infinity then the trace
of the Frobenius in a family is distributed like the trace of a random matrix in the
monodromy group associated to the family. We will be interested in what happens
when $q$ is fixed and we let $g$ tend to infinity.

Several cases of this are known for specific family of groups. It was first done by
Kurlberg and Rudnick [7] for hyper-elliptic curves ($G = \mathbb{Z}/2\mathbb{Z}$). This was extended
by Bucur, David, Feigon and Lalin [2],[3] for prime cyclic curves ($G = \mathbb{Z}/p\mathbb{Z}$, $p$
a prime). Lorenzo, Meleleo and Milione [8] then determined this for $n$-quadratic
curves ($G = (\mathbb{Z}/2\mathbb{Z})^n$). More recently the author [9] extended the work of Bucur,
David, Feigon and Lalin to the case of arbitrary cyclic curves ($G = \mathbb{Z}/r\mathbb{Z}$, $r$ not
necessarily a prime).

In all the works mentioned above the probability is not determine for the whole
family $\mathcal{H}_{G, g}$ but instead for an irreducible moduli space of the family. That is, we
can write
\[ \mathcal{H}_{G,g} = \bigcup_{\vec{d}(\vec{\alpha})} \mathcal{H}_{\vec{d}(\vec{\alpha})} \]
where \( \vec{d}(\vec{\alpha}) = (d(\vec{\alpha}))_{\vec{\alpha}} \) in a non-negative integer valued vector indexed by a set of \( |G| - 1 \) vectors (the \( \vec{\alpha} \)) and the union is over all such vectors that satisfy a linear equation and a set of linear congruence conditions. Moreover, \( \mathcal{H}_{\vec{d}(\vec{\alpha})} \) is a set of tuples of polynomials of prescribed degree that correspond to a curve with Galois group \( G \) and genus \( g(C) \). See Section 2 for a full description of these sets.

Remark 1.1. There is a natural correspondence between the genus of the curve and the degree of the discriminant of \( K(C) \). Through this correspondence we can view \( \mathcal{H}_{\vec{d}(\vec{\alpha})} \) as the set of curves such that the degree of the conductor of \( K(C) \) is fixed. Then the linear relationships that the union is over is the conductor-discriminant formula.

Moreover, all the previous results restrict to the case that \( q \equiv 1 \mod \exp(G) \) where \( \exp(G) = \min(n : ng = e \text{ for all } g \in G) \). This is in order to use Kummer theory to get a classification of the curves. Therefore, our main result will be for this irreducible moduli space under this same assumption.

**Theorem 1.2.** Let \( G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z} \) such that \( r_j | r_{j+1} \) and fix \( q \) such that \( q \equiv 1 \pmod{r_n} \) then as \( d(\vec{\alpha}) \to \infty \) for all \( \vec{\alpha} \in \mathcal{R} \),
\[
|\{ C \in \mathcal{H}_{\vec{d}(\vec{\alpha})} : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M \} | \sim \text{Prob} \left( \sum_{i=1}^{q+1} X_i = M \right)
\]
where the \( X_i \) are i.i.d. random variables taking value 0 or \( \frac{|G|}{s} \) for some \( s \mid r_n \) such that
\[
X_i = \begin{cases} \frac{|G|}{s} & \text{with probability } \frac{s\phi_G(s)}{|G|(|q^s+|G|-1)|} \text{ if } s \neq 1 \\ \frac{|G|}{s} & \text{with probability } \frac{q}{(|G|-1)(q+|G|)-2\sigma_{r_S} \phi_G(s)+1} \\ 0 & \text{with probability } \frac{|G|}{|G|(|q^s+|G|-1)|} \end{cases}
\]
where \( \phi_G(s) \) is the number of elements of \( G \) of order \( s \).

Remark 1.3. Notice that in our result, we require \( d(\vec{\alpha}) \) to tend to infinity for all \( \vec{\alpha} \). This implies that the genus tends to infinity as the genus can be written as a linear combination of the \( d(\vec{\alpha}) \). However, the converse is not true. That is, if \( g \) tends to infinity, this only implies that at least one of the \( d(\vec{\alpha}) \) would tend to infinity. In this case, the error term would not necessarily go to zero. Bucur, David, Feigon, Kaplan, Lalin, Ozman and Wood [1] solve this problem for the whole space \( \mathcal{H}_{G,g} \) where \( G \) is a prime cyclic. Work is done towards extending this by the author to any abelian group in a forthcoming paper with success in the case \( G \) is a power of a prime cyclic \( (G = (\mathbb{Z}/p\mathbb{Z})^n, p \text{ a prime}) \).

## 2. Genus Formula and Irreducible Moduli Space

In this section we will first determine a formula for the genus of the curve and from this formula create the irreducible moduli spaces \( \mathcal{H}_{\vec{d}(\vec{\alpha})} \).

Let \( C \) be a curve such that \( \text{Gal}(C) = G \) is abelian. Then we can find unique \( r_j \) such that \( r_j | r_{j+1} \) and \( G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z} \). Therefore, \( \exp(G) = r_n \). Since we are assuming \( q \equiv 1 \pmod{r_n} \), we get that \( \mu_{r_n} \subset K \) and hence \( K(C)/K \) is a
Kummer extension. Then Kummer Theory (Chap. 14 Proposition 37 of [4]) tells us
that there exists $F_1, \ldots, F_n \in \mathbb{F}_q[X]$ such that $F_j$ is $r_j$th-power free and

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

Let $g = g(C)$, be the genus of the curve $C$. Then the Riemann-Hurwitz formula
(Theorem 7.16 of [10]), says that

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

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 $\mathcal{O}_{K(C)}/\mathfrak{P}$ as a vector space over $\mathbb{F}_q$. By Proposition
7.7 of [10], 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 $\mathfrak{P}, \mathfrak{P}|P$, $e(\mathfrak{P}/P) = e(P)$ and $f(\mathfrak{P}/P) = f(\mathfrak{P}/P) := f(P)$. 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, (2.1) becomes

$$2g + 2|G| - 2 = \sum_{P} \left( |G| - \frac{|G|}{e(P)} \right) \deg_{K}(P)$$

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 2.1. Let $K \subset L \subset L(\sqrt[2]{F(X)}) = L'$ be an extension of fields where
$F \in \mathbb{F}_q[X]$ is $r$th-power free and $[L' : L] = r$. Let $\mathfrak{P}$ be a prime in $L$ and $\mathfrak{P}'$
be a prime in $L'$, lying over $\mathfrak{P}$. If $\text{ord}_\mathfrak{P}(F) = n$, then $e(\mathfrak{P}'/\mathfrak{P}) = \frac{n}{(r, n)}$.

Proof. Since $[L' : L] = r$, 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 $(F_1(X)\mathcal{O}_L, \mathfrak{P}) = 1$.
Then $Y^r - F(X) \equiv Y^r \pmod{\mathfrak{P}}$. Hence,

$$\mathfrak{P}' = \mathfrak{P}\mathcal{O}_{L'} + \sqrt[2]{F(X)}\mathcal{O}_{L'}$$

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

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

$$(\mathfrak{P}')^e = \sum_{j=0}^{e} \mathfrak{P}^{e-j} \left( \sqrt[2]{F(X)}\mathcal{O}_{L'} \right)^j.$$

Now,

$$\sum_{j=0}^{e-1} \mathfrak{P}^{e-j} \left( \sqrt[2]{F(X)}\mathcal{O}_{L'} \right)^j \subset \mathfrak{P}\mathcal{O}_{L'}.$$
so it remains to determine when \( \left( \sqrt[r]{F(X)}\mathcal{O}_{L'} \right)^e \subset \mathcal{O}_{L'} \). Finally,

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

and we see that \( e(\mathfrak{P}'/\mathfrak{P}) = \frac{r_1}{(r_2, m)} \).

\( \square \)

**Lemma 2.2.** Let \( K \subset L \subset \mathbb{L}( \sqrt[r]{F_1(X)} ) = L' \subset \mathbb{L}( \sqrt[r]{F_1(X)}, \sqrt[r]{F_2(X)} = L'' \) be extensions of fields where \( F_1, F_2 \in \mathbb{F}_q[X] \) are \( r_1 \)th and \( r_2 \)th power free respectively and \([L': L] = r_1, [L'': L'] = r_2\). Let \( \mathfrak{P} \) be a prime in \( L \) and \( \mathfrak{P}' \) be a prime in \( L' \) lying above \( \mathfrak{P} \). If \( ord_{\mathfrak{P}}(F_1) = n \) and \( ord_{\mathfrak{P}}(F_2) = m \), then \( e(\mathfrak{P}'/\mathfrak{P}) = \text{lcm}(\frac{r_1}{(r_2, m)}, \frac{r_2}{(r_2, m)}) \).

**Proof.** Let \( \mathfrak{P}' \) be a prime in \( L' \) such that \( \mathfrak{P}'/\mathfrak{P}' \mathfrak{P} \), then by Lemma 2.1, \( e(\mathfrak{P}'/\mathfrak{P}) = \frac{r_1}{(r_1, m)} \). Therefore, \( ord_{\mathfrak{P}}(F_2) = m \frac{r_1}{r_2} \) and, again by Lemma 2.1, \( e(\mathfrak{P}'/\mathfrak{P}) = \frac{r_1}{(r_1, m)} \frac{r_2}{(r_2, m)} \). Hence, \( e(\mathfrak{P}'/\mathfrak{P}) = \frac{r_1}{(r_1, m)} \frac{r_2}{(r_2, m)} \). So it remains to show that this is \( \text{lcm}(\frac{r_1}{(r_1, m)}, \frac{r_2}{(r_2, m)}) \).

Let \( A, B, C \) be positive integers. We will show that \( A \frac{B}{B + C} = \text{lcm}(A, \frac{B}{B + C}) \).

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

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

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.

\[\square\]

So, we see that in order to determine the genus, we need to keep track of \( \text{ord}_P(F_j) \) for all \( P \in \mathbb{F}_q[X] \) and \( 1 \leq j \leq n \). Towards this define the set

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

to be the set of integer-valued vectors with \( j \) entry between 0 and \( r_j - 1 \) such that not all entries are 0. Write an element of \( \mathcal{R} \) as \( \vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \). Then, for every \( \vec{\alpha} \in \mathcal{R} \), let

\[
f_{\vec{\alpha}} = \prod_{\text{ord}_P(F_j) = \alpha_j} P
\]

where the product is over all (finite) monic prime polynomials of \( \mathbb{F}_q[X] \). Then we can write

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

for some \( c_j \in \mathbb{F}_q^* \) where we use the convention that \( f^0 \) is identically the constant polynomial 1.

**Proposition 2.3.** If \( P | f_{\vec{\alpha}} \) then \( e(P) = \text{lcm}_{j=1,\ldots,n} \left( \frac{r_j}{(r_j, \alpha_j)} \right) \).
Proof. If $P | f_\circ$ then $\ord_P(F_j) = \alpha_j$ for all $j$. Thus if we recursively apply Lemma 2.2, we get the result.

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

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

Therefore, we can rewrite (2.2) as

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

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

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

Thus, what we want to keep track of is $\deg(f_{\vec{\alpha}})$. Hence, we will let $d(\vec{\alpha})$ be a non-negative integer for all $\vec{\alpha} \in R$ and

$$\vec{d}(\vec{\alpha}) = (d(\vec{\alpha}))_{\vec{\alpha} \in R}$$

be a vector indexed by the elements of $\vec{\alpha} \in R$. Moreover, for every $\vec{d}(\vec{\alpha})$ define

$$d_j := \sum_{\vec{\alpha} \in R} \alpha_j d(\vec{\alpha})$$

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

Define the sets

$$\mathcal{F}_d = \{ f : f, \text{ monic, squarefree and } \deg(f) = d \}$$

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

That is, the set of monic, square-free and pairwise coprime tuples of polynomials with prescribed degrees.

Consider $\vec{d}(\vec{\alpha})$ such that $d_j \equiv 0 \mod r_j$ for $j = 1, \ldots, n$, then for $(f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})}$, the right side of (2.3) becomes

$$\sum_{\vec{\alpha} \in R} \left( |G| - \frac{|G|}{e(\vec{\alpha})} \right) d(\vec{\alpha}).$$

Now, consider $\vec{d}(\vec{\alpha})$ such that $d_j \equiv r_j - \beta_j \mod r_j$ for some $\vec{\beta} \in R$. Define $d'(\vec{\beta}) = d(\vec{\beta}) + 1$ and $d'(\vec{\alpha}) = d(\vec{\alpha})$ for $\vec{\alpha} \neq \vec{\beta}$ and $\vec{d}'(\vec{\alpha}) = (d'(\vec{\alpha}))$. Then

$$d'_j := \sum_{\vec{\alpha} \in R} \alpha_j d'(\vec{\alpha}) \equiv 0 \mod r_j.$$ 

This motivates define the set

$$\mathcal{F}_{\vec{d}'(\vec{\alpha})} = \{(f_{\vec{\beta}}, (f_{\vec{\alpha}})) \in \mathcal{F}_{d(\vec{\beta}) - 1} \times \prod_{\vec{\alpha} \in R} \mathcal{F}_{d(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\gamma}}) = 1 \text{ for all } \vec{\alpha}, \vec{\gamma} \in R \}.$$  

This set is the same as the previous set except that the degree is dropped by 1 in the $\vec{\beta}^{th}$-coordinate.
Therefore, by the above argument we get that any tuple \((f_\bar{\alpha})\) lives in a unique \(F_{\vec{d}(\bar{\alpha})}\) such that \(d_j \equiv 0 \mod r_j\).

Hence if we define the set
\[
F_{[\vec{d}(\bar{\alpha})]} = F_{\vec{d}(\bar{\alpha})} \cup \bigcup_{\vec{\beta} \in \mathcal{R}} F_{\vec{d}(\bar{\alpha})}^{\vec{\beta}}
\]
then as \(\vec{d}(\bar{\alpha})\) runs over all vectors such that \(d_j \equiv 0 \mod r_j\), we get that the set \(F_{[\vec{d}(\bar{\alpha})]}\) runs over all tuples. Therefore, from now on we will always be assuming \(d_j \equiv 0 \mod r_j, j = 1, \ldots, n\).

Moreover, the genus of the curves corresponding to the tuples in \(F_{[\vec{d}(\bar{\alpha})]}\) is invariant. Indeed, if \((f_\bar{\alpha}) \in F_{\vec{d}(\bar{\alpha})}\), then we get that the genus, \(g\), satisfies
\[
2g + 2|G| - 2 = \sum_{\bar{\alpha} \in \mathcal{R}} \left( |G| - \frac{|G|}{e(\bar{\alpha})} \right) d(\bar{\alpha}).
\]

Further, if \((f_\bar{\alpha}) \in F_{\vec{d}(\bar{\alpha})}^{\vec{\beta}}\), the genus, \(g'\), satisfies
\[
2g' + 2|G| - 2 = \sum_{\bar{\alpha} \in \mathcal{R}} \left( |G| - \frac{|G|}{e(\bar{\alpha})} \right) d(\bar{\alpha}) + \left( |G| - \frac{|G|}{e(\bar{\alpha})} (d(\bar{\beta}) - 1) \right) + |G| - \frac{|G|}{e(\vec{d})} \sum_{\bar{\alpha} \in \mathcal{R}} d(\bar{\alpha})
\]
\[
= 2g + 2|G| - 2.
\]

Now, we need to add information about the leading coefficients, so define
\[
\tilde{F}_{\vec{d}(\bar{\alpha})} = (F_q^n)^n \times F_{\vec{d}(\bar{\alpha})}
\]
\[
\tilde{F}_{\vec{d}(\bar{\alpha})}^{\vec{\beta}} = (F_q^n)^n \times F_{\vec{d}(\bar{\alpha})}^{\vec{\beta}}
\]
\[
\tilde{F}_{[\vec{d}(\bar{\alpha})]} = (F_q^n)^n \times F_{[\vec{d}(\bar{\alpha})]}
\]

Every element of \(\tilde{F}_{[\vec{d}(\bar{\alpha})]}\) corresponds to a curve and every curve corresponds to an element of \(\tilde{F}_{[\vec{d}(\bar{\alpha})]}\). With that being said, we define
\[
\mathcal{H}_{\vec{d}(\bar{\alpha})} = \{ C : C \text{ corresponds to an element of } \tilde{F}_{[\vec{d}(\bar{\alpha})]} \}
\]
and we get
\[
\mathcal{H}_{G,g} = \bigcup \mathcal{H}_{\vec{d}(\bar{\alpha})}
\]
where the union is over all \(\vec{d}(\bar{\alpha})\) that satisfy
\[
2g + 2|G| - 2 = \sum_{\bar{\alpha} \in \mathcal{R}} \left( |G| - \frac{|G|}{e(\bar{\alpha})} \right) d(\bar{\alpha})
\]
\[
\sum_{\bar{\alpha} \in \mathcal{R}} \alpha_j d(\bar{\alpha}) \equiv 0 \mod r_j, j = 1, \ldots, n.
\]
3. Number of Points on the Curve

In this section, we will find a formula for the number of points on a curve in \( \mathcal{H}^G \). To begin, we will determine a formula for the number of points lying above \( x \) for all \( x \in \mathbb{P}^1(\mathbb{F}_q) \). In order to do this, however, we need a smooth, affine model of our curve at \( x \).

We can view \( K(C) \) as a vector space over \( K \) with dimension \( |G| \). Let 
\[ \mathcal{B} = \{ B_1, \ldots, B_{|G|} \} \]
be a basis of \( K(C) \) over \( K \). Since \( q \equiv 1 \pmod{\exp(G)} \), by Kummer Theory, we can assume that for all \( B_i \in \mathcal{B} \), there exists an \( m_i \in \mathbb{Z}_{>0} \) and \( H_i \in \mathbb{F}_q[X] \) such that \( H_i \) is \( m_i \)-power free and \( B_i = \sqrt[m_i]{H_i} \). Now, if \( x \in \mathbb{P}^1(\mathbb{F}_q) \), then we can find \( H_{j_1}, \ldots, H_{j_n} \) such that the smooth affine model of \( C \) at \( x \) is of the form
\[
Y_1^{m_{j_1}} = H_{j_1}(X) \quad Y_2^{m_{j_2}} = H_{j_2}(X) \quad \ldots \quad Y_n^{m_{j_n}} = H_{j_n}(X)
\]
Since \( x \) is smooth in this model, at most one of the \( H_{j_k} \) may have a root at \( x \) of order at most 1. Therefore, we see that the number of points lying over \( x \) will be
\[
\left\{ \begin{array}{ll}
\frac{m_{j_1} m_{j_2} \cdots m_{j_n}}{m_{j_k}} & H_{j_k}(x) \in (\mathbb{F}_q^*)^{m_{j_k}}, i = 1, \ldots, n \\
H_{j_k}(x) = 0, H_{j_i}(x) \in (\mathbb{F}_q^*)^{m_{j_i}}, i = 1, \ldots, n, i \neq k & \\
0 & \text{otherwise}
\end{array} \right.
\]
If we let \( \chi_m : \mathbb{F}_q^* \rightarrow \mu_m \) be a multiplicative character of order \( m \), and extend it to all of \( \mathbb{F}_q \) by setting \( \chi_m(0) = 0 \) then we see that we can write the number of points lying over \( x \) as
\[
\prod_{k=1}^n \left( 1 + \sum_{i=1}^{m_{j_k}-1} \chi_{m_{j_k}}^i \left( H_{j_k}(x) \right) \right).
\]
Let \( B_i \notin K(B_{j_1}, \ldots, B_{j_n}) \). Then I claim that \( H_i(x) = 0 \). 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
\[
Y_s^{m_{j_1}} = H_i(X) \quad Y_k^{m_{j_k}} = H_{j_k}(X), 1 \leq k \leq n, k \neq s.
\]
That is \( H_i \) will replace \( H_{j_k} \) for some \( 1 \leq s \leq n \).

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

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

Hence, the number of points lying over \( x \) is
\[
\prod_{k=1}^n \left( 1 + \sum_{i=1}^{m_{j_k}-1} \chi_{m_{j_k}}^i \left( H_{j_k}(x) \right) \right) = \sum_{j=1}^{|G|} \chi_{m_j}(H_j^{m_j}(x))
\]
Lemma 3.1. Let \( \mathcal{C} \in \mathcal{H}(\vec{d}(\vec{a})) \) such that \( C \) corresponds to \((\vec{c}, (f_{\vec{a}})) \in \hat{\mathcal{F}}(\vec{d}(\vec{a}))^*\). To use the discussion above, we want to find a basis for \( K(C) \) over \( K \) such that each element in the basis is an \( m \text{th} \) root of an \( m \text{th} \)-powerfree polynomial. Towards this, define

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

the set of vectors whose \( j \text{th} \) component divides \( r_j \). 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 \((\vec{c}, (f_{\vec{a}})) \in \hat{\mathcal{F}}(\vec{d}(\vec{a}))\) define

\[
F_{(\vec{s})}(X) := c_{(\vec{s})} \prod_{\vec{a} \in \mathcal{R}} f_{\vec{a}}(X)^{\sum_j 1 \ell(\vec{a}) \omega_j \alpha_j \pmod{\ell(\vec{s})}}
\]

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

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 \( f_{\vec{a}}(X)^0 \) is identically the constant polynomial 1. Hence, if \( \sum_{j=1}^n \ell(\vec{a}) \omega_j \alpha_j \equiv 0 \pmod{\ell(\vec{s})} \), then \( f_{\vec{a}}(X) \) does not divide \( F_{(\vec{s})}(X) \). In particular, if \( \vec{s} = (1, \ldots, 1) \), then \( \Omega_\vec{s} = \{ (1, \ldots, 1) \} \) and we make the identification

\[
F_{(1, \ldots, 1)}(X) = 1, c_{(1, \ldots, 1)} = 1
\]

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

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

This basis has the required property and hence the number of points lying over any \( x \in \mathbb{F}_q \) can be written as

\[
\sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_\vec{s}} \chi_\vec{\omega}(x) F_{(\vec{s})}(x).
\]

This leads to following lemma.

**Lemma 3.1.** Let \( C \in \mathcal{H}(\vec{d}(\vec{a})) \) that corresponds to \((\vec{c}, (f_{\vec{a}})) \in \hat{\mathcal{F}}(\vec{d}(\vec{a}))^*\). Then the number of affine points on the curve is

\[
\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{F}_q} \sum_{\vec{s} \in \mathcal{S}} \sum_{\vec{\omega} \in \Omega_\vec{s}} \chi_\vec{\omega}(x) F_{(\vec{s})}(x).
\]

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 $F(X) = (X')^{-d}\bar{F}(X')$, where $d = \deg(F)$. Hence to determine what happens at $x_{q+1}$, we need to determine what happens when $X' = 0$. We see that

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

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

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

So, we see we get a root at $x_{q+1}$ if and only if $k_j \neq r_j$ if and only if $d_j \neq 0 \mod r_j$. Therefore, we can write

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

Likewise, we see that

$$F_{(\alpha)}^{(\omega)}(x_{q+1}) = \begin{cases} c_{(\alpha)}^{(\omega)} & \sum_{j=1}^n \ell(\bar{\omega})_j \omega_j d_j \equiv 0 \mod \ell(\bar{\omega}) \\ 0 & \sum_{j=1}^n \ell(\bar{\omega})_j \omega_j d_j \neq 0 \mod \ell(\bar{\omega}) \end{cases}.$$  

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

$$\sum_{\bar{\omega} \in \mathcal{S}} \sum_{\Omega_x} \chi_{\ell(\bar{\omega})} \left( F_{(\alpha)}^{(\omega)}(x_{q+1}) \right)$$

and we get the following lemma.

**Lemma 3.2.** Let $C \in \mathcal{H}_{d(\bar{\alpha})}$ that corresponds to $(\bar{c}, (f, \bar{\alpha})) \in \mathcal{F}_{d(\bar{\alpha})}$. Then the number of projective points on the curve is

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

**Remark 3.3.** As we stated above, if $\bar{s} = (1, \ldots, 1)$, then $\Omega_{\bar{s}} = \{1, \ldots, 1\}$ and $F_{(1, \ldots, 1)}(X) = 1$. Hence

$$\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{\omega \in \Omega_{(1, \ldots, 1)}} \chi_{(1, \ldots, 1)} \left( F_{(1, \ldots, 1)}^{(\omega)}(x) \right) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} 1 = q + 1.$$  

Thus,

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 + \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{\bar{\omega} \in \mathcal{S}} \sum_{\bar{s} \neq (1, \ldots, 1)} \chi_{\ell(\bar{\omega})} \left( F_{(\alpha)}^{(\omega)}(x) \right)$$

and we get that

$$\text{Tr}(\text{Frob}_q) = -\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{\bar{\omega} \in \mathcal{S}} \sum_{\bar{s} \neq (1, \ldots, 1)} \chi_{\ell(\bar{\omega})} \left( F_{(\alpha)}^{(\omega)}(x) \right)$$
4. Admissibility

From now on, we fix an ordering of the elements of $F_q = \{x_1, \ldots, x_q\}$ and let $x_{q+1}$ denote the point at infinity of $\mathbb{P}^1(F_q)$, then we have reduced the problem down to determine the size of the set

$$\{(\vec{c}, (f_{\vec{a}})) \in \hat{F}_{[\bar{d}(\vec{a})]} : \chi_{\ell(p)}(F_{(\vec{s})}^{(\omega)}(x_i)) = \epsilon_{\vec{s}, \omega, i}, \vec{s} \in S, \omega \in \Omega_{\omega}, i = 1, \ldots, \ell\}$$

for some choices of $\epsilon_{\vec{s}, \omega, i} \in \mu_{\ell(p)} \cup \{0\}$ and $\ell = q + 1$. In fact, we will need to determine this for $\ell = 0$ as well as $\ell = q + 1$ in order to determine the probability. However, we will determine it for an arbitrary $\ell$.

Clearly, not all choices give a non-empty set as the polynomials $F_{(\vec{s})}^{(\omega)}$ are highly dependent on each other. This section will be devoted to determining properties of the choices of $\epsilon_{\vec{s}, \omega}$ that give a non-empty set.

**Definition 4.1.** A set

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

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

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

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

Clearly, therefore, (4.1) will be non-empty if and only if the set

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

is admissible for all $i$ and distinct $x_i$.

**Lemma 4.2.** For all $\vec{s} \in S, \omega \in \Omega_{\omega}$ and $p|r_n$, prime, define

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

$$\vec{\omega}_p = (\omega_1 \pmod{p^{v_p(s_1)}}, \ldots, \omega_n \pmod{p^{v_p(s_n)}}) \in \Omega_{\omega_p}.$$ 

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

$$\epsilon_{\vec{s}, \omega} = \prod_{p|r_n} \ell(\vec{s}_p)$$

**Proof.** Let $\vec{s} \in S$. If there exists a $p|r_n$, prime such that $s_j = p^{v_j}$ for $j = 1, \ldots, n$, then $s_{j'} = (1, \ldots, 1), \omega_{j'} = (1, \ldots, 1) \text{ and } m_{j'} = 1 \text{ for all } j' \neq p$, making the statement trivial. Therefore, suppose there exists $\vec{s}', \vec{s}'' \in S \text{ such that } \vec{s}', \vec{s}'' \neq (1, \ldots, 1), s_j = s_j', s_j'' \text{ and } \gcd(\ell(\vec{s}'), \ell(\vec{s}'')) = 1$. (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

$$\vec{\omega}' = (\omega_1', \ldots, \omega_n') = (\omega_1 \pmod{s_1'}, \ldots, \omega_n \pmod{s_n'}) \in \Omega_{\omega'}$$

$$\vec{\omega}'' = (\omega_1'', \ldots, \omega_n'') = (\omega_1 \pmod{s_1''}, \ldots, \omega_n \pmod{s_n''}) \in \Omega_{\omega''}.$$

Then there exists some polynomial $H$ such that

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

\[
\chi_{\ell}(x) \left( F_{(\tilde{s})}(x) \right) = \chi_{\ell(\tilde{s}^\prime)}(x) \chi_{\ell(s^\prime)}(x)
\]

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

\[ \square \]

**Corollary 4.3.** \( \epsilon_{\tilde{s},\tilde{\omega}} \) uniquely determines and is uniquely determined by \( \epsilon_{\tilde{s},\tilde{\omega}_p} \) for all \( p \mid r_n \).

**Proof.** Straight forward from Lemma 4.2.

\[ \square \]

**Lemma 4.4.** For any \( \tilde{s} = (s_1, \ldots, s_n) \in \mathcal{S} \), define \( \bar{s}_j \) to be the vector in \( \mathcal{S} \) that has \( s_j \) in the \( j \)th coordinate and 1 everywhere else. Let \( \bar{1} = (1, \ldots, 1) \in \Omega_{\bar{s}_j} \subset \Omega_{\tilde{s}} \). If \( \{ \epsilon_{\tilde{s},\tilde{\omega}} : \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} \} \) is admissible and \( \epsilon_{\tilde{s},\tilde{\omega}} \not\equiv 0 \) for all \( j \) then

\[
\epsilon_{\tilde{s},\tilde{\omega}} = \prod_{j=1}^{n} \omega_j^{s_j_{\tilde{\omega}_j}}
\]

**Proof.** Recall that \( F_{j}(X) = \prod_{s \in \mathcal{R}} f_{s_j}(X) \). For all \( s_j \rvert r_j \) define

\[
F_{j,s_j}(X) := \prod_{s \in \mathcal{R}} f_{s_j}(X)^{s_j} = F_{(\bar{1})}(X).
\]

Therefore, there exists an \( H \) such that

\[
\prod_{j=1}^{n} F_{j,s_j}(X)^{\ell_j \omega_j} = F_{(\tilde{s})}(X)H(X)^{\ell_{\tilde{s}}}.
\]

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

\[
\epsilon_{\tilde{s},\tilde{\omega}} = \chi_{\ell(\tilde{s})}(F_{(\tilde{s})}(x)) = \prod_{j=1}^{n} \omega_j^{s_j_{\tilde{\omega}_j}}(F_{j,s_j}(x)) = \prod_{j=1}^{n} \epsilon_{\tilde{s},\tilde{\omega}_j}.
\]

\[ \square \]

As in the cyclic case in [9], it will be important to keep track of when and how an admissible set can have zero values. Fix a \( \tilde{\beta} \) such that \( f_{\tilde{\beta}}(x) = 0 \). Then \( F_{(\tilde{s})}(x) = 0 \) if and only if \( f_{\tilde{\beta}}(X) \mid F_{(\tilde{s})}(X) \) if and only if

\[
\sum_{j=1}^{n} \frac{\ell(\tilde{s})}{s_j} \omega_j_{\beta_j} \not\equiv 0 \pmod{\ell(\tilde{s})}.
\]

Define the set

\[
A_{\tilde{\beta}} := \{ \tilde{s}, \tilde{\omega} : \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}}, \sum_{j=1}^{n} \frac{\ell(\tilde{s})}{s_j} \omega_j_{\beta_j} = 0 \pmod{\ell(\tilde{s})} \}.
\]

Then \( F_{(\tilde{s})}(X) \neq 0 \) if and only if \( (\tilde{s}, \tilde{\omega}) \in A_{\tilde{\beta}} \).
There is a natural bijective correspondence from \( A_{\vec{\beta}} \) to
\[ \{ \vec{\omega} \in R^1 : \sum_{j=1}^{n} \frac{r_j}{r_n} \omega_j \beta_j \equiv 0 \pmod{r_n} \} \]
which sends \((\vec{s}, \vec{\omega}) \rightarrow (\frac{r_1}{s_1} \omega_1, \ldots, \frac{r_n}{s_n} \omega_n)\) where
\[ R^1 = [1, \ldots, r_1] \times \cdots \times [1, \ldots, r_n]. \]

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

**Definition 4.5.** An admissible set
\[ \{ \vec{\epsilon}_{\vec{s}, \vec{\omega}} \in \mu_{\ell(\vec{s})} \cup \{0\}, \vec{s} \in S, \vec{\omega} \in \Omega_x \} \]
is called \([\vec{\beta}]\)-admissible if \( \vec{\epsilon}_{\vec{s}, \vec{\omega}} = 0 \) if and only if \((\vec{s}, \vec{\omega}) \notin A_{\vec{\beta}}\).

**Remark 4.6.** If \( \{ \vec{\epsilon}_{\vec{s}, \vec{\omega}} : \vec{s} \in S, \vec{\omega} \in \Omega_x \} \) is \([0]\)-admissible then \( \vec{\epsilon}_{\vec{s}, \vec{\omega}} \neq 0 \) for all \( \vec{s} \in S, \vec{\omega} \in \Omega_x \).

It will be useful later to classify the equivalence classes of \( \tilde{R} \). Towards this, for all \( p| r_n \), define
\[ S_p = \{ \vec{s} = (s_1, \ldots, s_n) : s_j = p^{v_j}, 0 \leq v_j \leq v_p(r_j) \} \subset S \]
\[ A_{\vec{\beta}, p} := \{ (\vec{s}, \vec{\omega}) : \vec{s} \in S_p, \vec{\omega} \in \Omega_x \sum_{j=1}^{n} \frac{\ell(\vec{s})}{s_j} \omega_j \beta_j \equiv 0 \pmod{\ell(\vec{s})} \} \]
\[ = \{ \vec{\omega} \in R_p^1 : \sum_{j=1}^{n} p^{v_p(r_j) - v_p(r_j)} \omega_j \beta_j \equiv 0 \pmod{p^{v_p(r_n)}} \} \]
where we identify the two sets under the map \( (\vec{s}, \vec{\omega}) \rightarrow (p^{v_p(r_1)} \omega_1, \ldots, p^{v_p(r_n)} \omega_n) \)
and \( R_p = [1, \ldots, p^{v_p(r_1)}] \times \cdots \times [1, \ldots, p^{v_p(r_n)}] \).

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 4.7.** 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 \( v_p((\beta_j, r_j)) = v_p(r_j) \). 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. \( \square \)
Lemma 4.8. $\vec{\beta} \sim_p \vec{\gamma}$ if and only if there exists an $1 \leq m \leq p^{\max (0, \max (v_p (\frac{r_j}{r_j})))}$, $(m, p) = 1$ such that $\beta'_j \equiv m \beta_j \pmod{p^{v_p (r_j)}}$ for all $j$.

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

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

Moreover, for all $j$, define $\gamma_j$ to be such that

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

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

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

Define $\vec{\omega} \in \mathcal{R}'_1$ such that $\omega_j = 1$, $\omega_k$ is as above and $\omega_l = p^{v_p (r_l)}$ otherwise. Then $\vec{\omega} \in A_{\vec{\beta}, p} = A_{\vec{\beta}, p}$. Hence,

$$0 \equiv p^{v_p (\frac{r_j}{r_j} \beta_k)} \omega_k + p^{v_p (\frac{r_j}{r_j} \beta_j)} \beta'_j \equiv p^{v_p (\frac{r_j}{r_j} \beta_k)} \beta_k \omega_k + p^{v_p (\frac{r_j}{r_j} \beta_j)} \beta_j m_j$$

$$\equiv -p^{v_p (\frac{r_j}{r_j} \beta_k)} \gamma_k m_k + p^{v_p (\frac{r_j}{r_j} \beta_j)} \gamma_j \gamma_k^{-1} + p^{v_p (\frac{r_j}{r_j} \beta_j)} \gamma_j \beta_j m_j$$

$$\equiv p^{v_p (\frac{r_j}{r_j} \beta_k)} \gamma_j (m_j - m_k) \pmod{p^{v_p (r_k)}}.$$ 

Therefore,

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

Hence,

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

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

Conversely, suppose there exists an $1 \leq m \leq p^{\max (0, \max (v_p (\frac{r_j}{r_j})))}$, $(m, p) = 1$ 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

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

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

$$\square$$

Note that

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

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 4.9. $\vec{\beta} \sim \vec{\gamma}$ if and only if there exists an $1 \leq m \leq e(\vec{\beta})$, $(m, e(\vec{\beta})) = 1$ such that $m \vec{\beta} = m \vec{\gamma}.$
Proof. Suppose $\tilde{\beta} \sim \tilde{\beta}'$. Then $\tilde{\beta} \sim_p \tilde{\beta}'$ for all $p|\gamma_n$ and we can find an $1 \leq m_p \leq p_{\max(0, \min(v_p(\tilde{\beta}_j))}$, $(m_p, p) = 1$ such that $\beta_j = m_p \beta_j$ (mod $p_{\max(0, \min(v_p(\tilde{\beta}_j))}$). Let $1 \leq m \leq \prod_{p|\gamma_n} p_{\max(0, \min(v_p(\tilde{\beta}_j))}$, $(m, \gamma_n) = 1$ such that $m \equiv m_p \pmod{p_{\max(0, \min(v_p(\tilde{\beta}_j))}}$ for all $p|\gamma_n$. Then $\beta_j \equiv m \beta_j$ (mod $r_j$) and $\tilde{\beta}' = m \tilde{\beta}$.

Conversely, suppose such an $m$ exists. Then let $m_p \equiv m \pmod{p_{\max(0, \min(v_p(\tilde{\beta}_j))}}$. Then $\beta_j \equiv m_p \beta_j$ (mod $p_{\max(\gamma_n)}$). Thus $\tilde{\beta} \sim_p \tilde{\beta}'$ for all $p$ and therefore $\tilde{\beta} \sim \tilde{\beta}'$.

□

Corollary 4.10. There are $\phi(e(\tilde{\beta}))$ different $\tilde{\beta}'$ such that $\tilde{\beta}' \sim \tilde{\beta}$.

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

□

Lemma 4.11. $|A_{\tilde{\beta}, p}| = p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n) - v_p(e(\tilde{\beta}))}$

Proof. Consider the map

$\phi_{\tilde{\beta}} : \mathbb{Z}/p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n) - v_p(e(\tilde{\beta}))} \to \mathbb{Z}/p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n)}$

$(x_1, \ldots, x_n) \to \sum_{j=1}^{n} p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n) - v_p(r_j)} \beta_j x_j$

Then $A_{\tilde{\beta}, p} = \ker(\phi_{\tilde{\beta}})$. Let $1 \leq k \leq n$ such that $v_p(\tilde{\beta}k) = \min(v_p(\tilde{\beta}_j))$. Then $\ker(\phi_{\tilde{\beta}}) \subseteq \mathbb{Z}/p_{\max(0, v_p(\tilde{\beta}))}^{\gamma_k}$.

Moreover

$\phi_{\tilde{\beta}}(0, \ldots, 0, x_k, 0, \ldots, 0) = p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_k)} \gamma_k x_k$

where $\beta_k = p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_k)} \gamma_k$. Therefore, since $(\gamma_k, p) = 1$, we get that $\ker(\phi_{\tilde{\beta}}) = \mathbb{Z}/p_{\max(0, v_p(\tilde{\beta}))}^{\gamma_k}$.

Hence

$|A_{\tilde{\beta}, p}| = |\ker(\phi_{\tilde{\beta}})| = p_{\max(0, v_p(\tilde{\beta}))}^{\gamma_k} = p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n) - v_p(e(\tilde{\beta}))}$.

□

Corollary 4.12. $|A_{\tilde{\beta}}| = \frac{|G|}{e(\tilde{\beta})}$

Proof.

$|A_{\tilde{\beta}}| = \prod_{p|r_n} |A_{\tilde{\beta}, p}| = \prod_{p|r_n} p_{\max(0, v_p(\tilde{\beta}))}^{v_p(\gamma_n) - v_p(e(\tilde{\beta}))} = \frac{|G|}{e(\tilde{\beta})}$.

□

5. Value Taking

In this section we will determine for $0 \leq \ell \leq q$, the size of the set

$$\{ f_{\tilde{s}, \omega, i} \in \mathcal{F}_{\tilde{s}, \omega, \ell} : \chi_i(\tilde{s})(F_{\tilde{s}}(x_i)) = \epsilon_{i, \omega, \ell}(\tilde{s}) \}$$

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

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

is admissible.
Remark 5.1. Since we are assuming for now that \( \ell \leq q \), we are only dealing with the affine points, hence we need only look at the set \( \mathcal{F}_{\vec{d};(\vec{\alpha})} \). If we want to incorporate the point at infinity by setting \( \ell = q + 1 \), we need to consider the full set \( \mathcal{F}_{[d;(\vec{\alpha})]} \) as will be done in Proposition 5.8.

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

\[
F_j(X) := \prod_{\vec{\alpha} \in R} F^{(\vec{\alpha})}_{\vec{\rho}_j} = F^{(\vec{\Gamma})}_{(\vec{\rho}_j)}(X).
\]

By Lemmas 4.2 and 4.4, we get that if \( \epsilon_{\vec{\xi},\vec{\omega},i} \neq 0 \) for all \( \vec{\xi} \in S, \vec{\omega} \in \Omega_x \) and \( i = 1, \ldots, \ell \), then the values of \( \epsilon_{\vec{\xi},\vec{\omega},i} \) will be uniquely determined by the values of \( \epsilon_{\vec{\rho}_j,\vec{\Gamma},i} \) for \( j = 1, \ldots, n \), \( i = 1, \ldots, \ell \). Moreover, (5.2) will be admissible for any choices of \( \epsilon_{\vec{\rho}_j,\vec{\Gamma},i} \). Therefore,

\[
|\{(f_{\vec{\alpha}}) \in \mathcal{F}_{d;\vec{\alpha}} : \chi_{(\vec{\alpha})}(F^{(\vec{\alpha})}_{\vec{x}}(x_i)) = \epsilon_{\vec{\xi},\vec{\omega},i} \in S, \vec{\omega} \in \Omega_x, i = 1, \ldots, \ell \}|\]

\[
= |\{(f_{\vec{G}}) \in \mathcal{F}_{d;\vec{G}} : \chi_{(\vec{G})}(F^{(\vec{G})}_{\vec{x}}(x_i)) = \epsilon_{\vec{\rho}_j,\vec{\Gamma},i} \in S, \vec{\omega} \in \Omega_x, i = 1, \ldots, \ell, j = 1, \ldots, n \}|\]

The size of this set is easily deduced from Proposition 3.4 of [9].

**Proposition 5.2.** Let \( \vec{d}(\vec{\alpha}) \) be as above. For \( 0 \leq \ell \leq q \) let \( \epsilon_{\vec{\rho}_j,\vec{\Gamma},i} \in \mu_{r_j} \) for \( i = 1, \ldots, \ell \). Then the size of

\[
\{ (f_{\vec{\alpha}}) \in \mathcal{F}_{d;\vec{\alpha}} : \chi_{r_j}(F^{(\vec{\alpha})}_{j}(x_i)) = \epsilon_{\vec{\rho}_j,\vec{\Gamma},i}, 1 \leq i \leq \ell, 1 \leq j \leq n \}
\]

is

\[
S_n(\ell) = \frac{L_{|G|} - 2q\sum d(\vec{\alpha})}{\zeta_q(2)|G|^{n-1}} \left( \prod_{\vec{\alpha} \in R} \frac{q}{|G|(q + |G| - 1)} \right)^{\ell} \left( 1 + O \left( q^{\frac{\min(d(\vec{\alpha}))}{2}} \right) \right)
\]

where \( \zeta_q(s) \) is the zeta function for \( K \) and

\[
L_n = \prod_{j=1}^{n} \frac{1 - \frac{j}{(|P| - 1)(|P| + j)}}{p}
\]

where the product is over all monic, irreducible polynomials of \( K \) and \( |P| = q^{\deg(P)} \).

**Remark 5.3.** First, note that \( |G| = r_1 \cdots r_n \). Moreover, Proposition 3.4 of [9] does not rely on the fact that the \( r_j | r_{j+1} \) and hence define a group. Secondly, observe that the size of the set is independent of the choices of \( \epsilon_{\vec{\rho}_j,\vec{\Gamma},i} \) as long as they are non-zero.

**Remark 5.4.** The error term is written in terms of \( \min(d(\vec{\alpha})) \) and so is only smaller than the main term if \( \min(d(\vec{\alpha})) \) tends to infinity. This is equivalent to saying that all the \( d(\vec{\alpha}) \) tend to infinity. This calculation is why we need that assumption in the Theorem 1.2 and why we can not easily extend this result to the whole space \( \mathcal{H}_{G,q} \). Therefore, improving this error term is one way in which we could extend the result however, this seems unlikely. A different method for doing this is the topic of a forthcoming paper by the author.

**Corollary 5.5.**

\[
|\mathcal{F}_{d;\vec{\alpha}}| = \frac{(q - 1)^n(q + |G| - 1) L_{|G|-2q\sum d(\vec{\alpha})}}{\zeta_q(2)|G|^{n-1}} \left( 1 + O \left( q^{\frac{\min(d(\vec{\alpha}))}{2}} \right) \right)
\]
Proof. This is straight forward from setting $\ell = 0$ in Proposition 5.2 and summing up over the components of $\mathcal{F}_{d(\vec{a})}$ and choices of $\vec{c} \in (\mathbb{F}_q^n)$.

\[ \square \]

Let us now determine the size of the set if some of the $\epsilon_{\vec{s}, \vec{\omega}, i}$ can be zero. With the notation of Section 4, we would need the set in 5.2 to be $[\vec{\beta}]$-admissible for some $[\vec{\beta}] \in \tilde{\mathcal{R}}$.

**Proposition 5.6.** Let $\{\epsilon_{\vec{s}, \vec{\omega}, i} : \vec{s} \in \mathcal{S}, \vec{\omega} \in \Omega_\mathcal{S}\}$ be an admissible set for $1 \leq i \leq \ell$ such that

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

then

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

$$= \frac{L(G) - 2q^{\sum d(\vec{a})}}{\zeta_q(2)^{G-1}} \prod_{[\vec{\beta}] \in \tilde{\mathcal{R}}} \frac{\phi(e(\vec{\beta}^2))}{|G|(q + |G| - 1)} m_{[\vec{\beta}]} \left( q \frac{q}{|G|(q + |G| - 1)} \right)^{m_{[\vec{\beta}]} \left( 1 + O(q^{-\min(d(\vec{a}))}) \right)}.$$
by $\chi_{r_j} (G_{j,r_j}(x_i))$, for $j = 1, \ldots, n$. Moreover, by Corollary 4.3 these will be determined by

$$
\chi_{p^r(r_j)} \left( G_{j,p^r(r_j)}(x_i) \right)
$$

for all $p|r_n$, $j = 1, \ldots, n$.

Now fix an $i \in M_{\beta}$. If $(\bar{s}, \bar{\omega}) \in A_{\beta}$, then

$$
F_{(\bar{s}, \bar{\omega})}^{(\gamma)}(X) = G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(X)H(X)
$$

for some $H(X)$ such that $H(x_i) \neq 0$. Moreover, $H(X)$ depends only on the choice of partitions of the $M_{\beta}$. Therefore, for a fixed partition, we see that $\chi_{(\bar{s}, \bar{\omega})} (G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i))$ will be determined by $\chi_{(\bar{s}, \bar{\omega})} (F_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i))$ for all $(\bar{s}, \bar{\omega}) \in A_{\beta}$. It remains to determine how many choices there are for $\chi_{(\bar{s}, \bar{\omega})} (G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i))$ such that $(\bar{s}, \bar{\omega}) \not\in A_{\beta}$.

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 $\chi_{p^r(r_k)} (G_{k,p^r(r_k)}(x_i))$ then we know $\chi_{p^r(r_j)} (G_{j,p^r(r_j)}(x_i))$ for all $1 \leq j \leq n$. If we write $\beta_j = p^{\nu_j}(\beta_j), r_j = p^{\nu_j}(r_j)s_j$ where $(\gamma_j, p) = (s_j, p) = 1$ and let

$$
\omega'_k \equiv \gamma_k^{-1} \beta_k \omega'_k s_k \pmod{v_p(f_n(x_n))},
$$

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 $\bar{\omega} \in \mathcal{R}^\dagger$ as $\omega_j = s_j, \omega_h = r_h, h \neq j, k$ and $\omega_k = \omega'_k s_k$, then $\bar{\omega} \in A_{\beta}$. So, defining $\bar{p} = (p^{\nu_j}(r_1), \ldots, p^{\nu_j}(r_n))$ we get by Lemma 4.4,

$$
\chi_{p^r(r_n)} \left( G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i) \right) = \chi_{p^r(r_n)} \left( G_{k,p^r(r_k)}(x_i) \right) \chi_{p^r(r_j)} \left( G_{j,p^r(r_j)}(x_i) \right)
$$

Moreover, as stated above, $\chi_{p^r(r_n)} \left( G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i) \right)$ is fixed by $\chi_{p^r(r_n)} \left( F_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i) \right)$ and our choices of $M_{\beta}$. Hence knowing $\chi_{p^r(r_k)} (G_{k,p^r(r_k)}(x_i))$ fixes $\chi_{p^r(r_j)} (G_{j,p^r(r_j)}(x_i))$.

Therefore, to determine the number of possible values for $\chi_{p^r(r_j)} (G_{j,p^r(r_j)}(x_i))$, $j = 1, \ldots, n$, it is enough to determine the possible values for $\chi_{p^r(r_k)} (G_{k,p^r(r_k)}(x_i))$.

Finally, since $\chi_{p^r(r_k)} (G_{k,p^r(r_k)}(x_i))$ is determined by $\chi_{p^r(r_k)} (F_{k,p^r(r_k)}(x_i))$ and the choice of $M_{\beta}$ there are $p^{\max(v_p(f_n(x_n))), 0}$ choices for $\chi_{p^r(r_k)} (G_{k,p^r(r_k)}(x_i))$.

All together, therefore, there are

$$
\prod_{p \mid r_n} p^{\max(0, \max_j (v_p(r_j)))} = \prod_{j=1, \ldots, n} \left( \frac{r_j}{(r_j, \beta_j)} \right) = e(\beta)
$$

different choices for

$$
\chi_{p^r(r_j)} \left( G_{j,p^r(r_j)}(x_i) \right) \text{ for all } p \mid r_n, j = 1, \ldots, n
$$

and hence $e(\beta)$ different choices for

$$
\chi_{(\bar{s}, \bar{\omega})}(G_{(\bar{s}, \bar{\omega})}^{(\gamma)}(x_i)), \bar{s} \in \mathcal{S}, \bar{\omega} \in \Omega_{\bar{s}}
$$

for a fixed choice of the $M_{\beta}$. 
Therefore,
\[
\begin{align*}
&\left| \{(f_{\bar{\alpha}}) \in \mathcal{F}_{\bar{\alpha}} : \chi_{\ell(\bar{\alpha})}(F_{\bar{\alpha}}(x_i)) = \epsilon_{x,\bar{\omega},i}, \bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}, i = 1, \ldots, \ell \} \right| \\
= & \sum_{M_\beta} \sum_{\epsilon'_{x,\bar{\omega},i}} \left| \{(g_{\bar{\alpha}}) \in \mathcal{F}_{\bar{\alpha}} : \chi_{\ell(\bar{\alpha})}(G_{\bar{\alpha}}(x_i)) = \epsilon'_{x,\bar{\omega},i}, \bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}, i = 1, \ldots, \ell \} \right|
\end{align*}
\]
where the first sum is over all the partitions \(M_\beta = \bigcup_{\tilde{\beta} \sim \beta} M_\beta\), the second sum is over all \(\epsilon(\tilde{\beta})\) choices of \(\chi_{\ell(\bar{\alpha})}(G_{\bar{\alpha}}(x_i))\) and \(\tilde{\beta}(\bar{\alpha})\) is the vector such that \(d'(\bar{\alpha}) = d(\bar{\alpha}) - m_{\bar{\alpha}}\). Now since \(\epsilon'_{x,\bar{\omega},i} \neq 0\) for all \(\bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}, i = 1, \ldots, \ell\), we get by Proposition 5.2, the above line is equal to
\[
\sum_{M_\beta} \sum_{\epsilon'_{x,\bar{\omega},i}} \frac{L_{(\bar{\alpha})}(-q)^{\sum d'_{(\bar{\alpha})}}}{\zeta_0(2)^{|G|}} \left( \frac{q}{|G|(q + |G| - 1)} \right)^\ell \left( 1 + O \left( q^{-\frac{\min(d(\bar{\alpha}))}{2}} \right) \right)
\]
\[
= \sum_{M_\beta} \prod_{[\tilde{\beta} \in R} \left( \frac{q}{|G|(q + |G| - 1)} \right)^m_{[\tilde{\beta}]} \left( 1 + O \left( q^{-\frac{\min(d(\bar{\alpha}))}{2}} \right) \right)
\]
where the last equality comes from Corollary 4.3 that states that there are \(\phi(\epsilon(\tilde{\beta}))\) different \(\tilde{\beta}'\) such that \(\tilde{\beta}' \sim \tilde{\beta}\).

\[
\square
\]
Recall that \(x_{q+1}\) is the point at infinity and if \((\bar{c}, (f_{\bar{\alpha}})) \in \hat{\mathcal{F}}_{\bar{\alpha}}\), then
\[
F_{\bar{\alpha}}(x_{q+1}) = \begin{cases} 
0 & \text{if } \sum_{j=1}^n \frac{\ell(\bar{\omega})}{\epsilon_{x,j}(s)} \omega_j d_j \equiv 0 \mod \ell(\bar{\omega}) \\
\epsilon_{x,j}(s) & \sum_{j=1}^n \frac{\ell(\bar{\omega})}{\epsilon_{x,j}(s)} \omega_j d_j \neq 0 \mod \ell(\bar{\omega})
\end{cases}
\]

**Proposition 5.8.** Let \(\{\epsilon_{x,\bar{\omega},i} : \bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}\}\) be an admissible set for \(1 \leq i \leq q + 1\) such that
\[
m_{[\tilde{\beta}]} := |\{1 \leq i \leq q + 1 : \epsilon_{x,\bar{\omega},i} : \bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}\} is \tilde{\beta} - admissible|
\]
then
\[
\left| \{(\bar{c}, (f_{\bar{\alpha}})) \in \hat{\mathcal{F}}_{\bar{\alpha}} : \chi_{\ell(\bar{\alpha})}(F_{\bar{\alpha}}(x_i)) = \epsilon_{x,\bar{\omega},i}, \bar{s} \in S, \bar{\omega} \in \Omega_{\bar{\alpha}}, i = 1, \ldots, q + 1 \} \right|
\]
\[
= \frac{(q - 1)^n(q + |G| - 1)}{q} \prod_{[\tilde{\beta} \in R} \left( \frac{q}{|G|(q + |G| - 1)} \right)^m_{[\tilde{\beta}]} \left( 1 + O \left( q^{-\frac{\min(d(\bar{\alpha}))}{2}} \right) \right)
\]
Remark 5.9. Notice that we are looking at \((\vec{c}, (f_\vec{s})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{c})}\). That is, when we add in the point at infinity, we must consider the whole irreducible coarse moduli space.

**Proof.** **Case 1:** \(\epsilon_{k, \vec{s}, q+1} \neq 0\) for all \(\vec{s} \in S, \vec{w} \in \Omega_{\vec{x}}\).

This means that \((\vec{c}, (f_\vec{c})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{c})}\) and \(\chi_{\ell}(\vec{s})(F_{\vec{s}}(x_{q+1}))\) will be determine by \(\chi_{r_j}(F_j(x_{q+1})), j = 1, \ldots, n\). 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

\[
|\{(\vec{c}, (f_\vec{c})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{c})} : \chi_{\ell}(\vec{s})(F_{\vec{s}}(x_i)) = \epsilon_{k, \vec{s}, i}, \vec{s} \in S, \vec{w} \in \Omega_{\vec{x}}, 1 \leq i \leq q + 1\}| = \sum_{c_j} |\{(f_\vec{s}) \in \mathcal{F}_{\vec{d}(\vec{c})} : \chi_{\ell}(\vec{s})(F_{\vec{s}}(x_i)) = \epsilon_{k, \vec{s}, i}, \vec{s} \in S, \vec{w} \in \Omega_{\vec{x}}, 1 \leq i \leq q\}|
\]

\[
= \sum_{c_j} \frac{L_{|G|}^{-2q} \sum_{d(\vec{c})} \phi(e(\vec{\beta}))}{\zeta_0(2)|G|^{-1}} \prod_{[\beta] \in \mathcal{R}} \left( \frac{\phi(e(\vec{\beta}))}{|G|(q + |G| - 1)} \right)^{m_{[\beta]}} \frac{q}{|G|(q + |G| - 1)}^{m_{[\beta]} - 1} \left( 1 + O \left( q^{\min(m(\vec{d}(\vec{c})))} \right) \right)
\]

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 \(\{\epsilon_{k, \vec{s}, q+1} : \vec{s} \in S, \vec{w} \in \Omega_{\vec{x}}\}\) is \([\vec{\beta}]\)-admissible for some \([\vec{\beta}] \in \hat{\mathcal{R}}, [\vec{\beta}] \neq [\vec{0}]\).

This means that \(\deg(F_j) = \beta_j^\prime\) (mod \(r_j\)) for some \(\vec{\beta} \sim \vec{\beta}\) and that \((\vec{c}, (f_\vec{c})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{c})}\). Fix a \(p|\vec{r}, n\) and let \(k\) be such that \(\sum(v_p(\gamma_j \beta_j^\prime))^j = v_p(\gamma_k \beta_k^\prime)\). Then \(\chi_{p^\gamma_j \beta_j^\prime}(F_{k, p^\gamma_j \beta_j^\prime}(x_{q+1})) = \chi_{p^\gamma_j \beta_j^\prime}(c_k)\). So \(c_k\) has \(\frac{q-1}{p^\gamma_j \beta_j^\prime}\) choices.

Now suppose \(\vec{\beta} = p^\gamma_j \gamma_j\) and let \(\omega_k\) be such that

\[
\omega_k \equiv \gamma_k^{-1} \gamma_j p^{\gamma_j \beta_j^\prime} (r_j \beta_j^\prime)^j (\mod p^{\gamma_j \beta_j^\prime}).
\]

then \(\chi_{p^\gamma_j \beta_j^\prime}(c_k, c_j) \neq 0\) will be fixed. Therefore, for a choice of \(c_k\) there are \(\frac{q-1}{p^\gamma_j \beta_j^\prime}\) choices for \(c_j\) that satisfy this property.

Likewise for another \(p'|\vec{r}, n, p \neq p', k'\) be such that \(\sum(v_p'(\gamma_j' \beta_j'^\prime))^j = v_p'(\gamma_k' \beta_k'^\prime)\). Then the number of choices for \(c_k\) will be divided by \((p')^{\gamma_j' \beta_j'^\prime}\) whereas the number of choice for \(c_j, j \neq k'\) will be divided by \((p')^{\gamma_j' \beta_j'^\prime}\). Hence, the number of choices for the \(c_j\) will be

\[
\frac{(q - 1)^n}{\prod_{p|\vec{r}} (p^{\gamma_j \beta_j^\prime} \prod_{j \neq k} p^{\gamma_j \beta_j^\prime})} = e(\vec{\beta}) \prod_{j = 1}^n \frac{(q - 1)}{r_j}
\]

Moreover, \(m_{[\beta]}\) goes to \(m_{[\beta]} - 1\). So,

\[
|\{(\vec{c}, (f_\vec{c})) \in \hat{\mathcal{F}}_{\vec{d}(\vec{c})} : \chi_{\ell}(\vec{s})(F_{\vec{s}}(x_i)) = \epsilon_{k, \vec{s}, i}, \vec{s} \in S, \vec{w} \in \Omega_{\vec{x}}, 1 \leq i \leq q + 1\}|
\]
Corollary 5.10. Let \( \{ \epsilon_{\tilde{s}, \tilde{\omega}}, i : \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} \} \) be an admissible set for \( 1 \leq i \leq q + 1 \) such that
\[
m_{\tilde{\beta}} := |\{ 1 \leq i \leq q + 1 : \{ \epsilon_{\tilde{s}, \tilde{\omega}}, i : \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} \} \text{ is } [\tilde{\beta}] - \text{admissible} \}|
\]
then
\[
|\{ (\tilde{c}, (f_{\tilde{s}})) \in \tilde{F}_{[\tilde{d}, \tilde{\alpha}]} : \chi_{\tilde{\alpha}}(F^{(\tilde{\omega})}_{(\tilde{s})}) (x_i) = \epsilon_{\tilde{s}, \tilde{\omega}, i}, \tilde{s}, \tilde{\omega} \in \Omega_{\tilde{x}}, i = 1, \ldots, q + 1 \}| = \prod_{\tilde{\beta} \in \mathcal{R}' \setminus [\tilde{\beta}] \neq 0} \left( \frac{\phi(e(\tilde{\beta})^2)}{|G|(q + |G| - 1)} \right)^{m_{\tilde{\beta}}} \left( \frac{q}{|G|(q + |G| - 1)} \right)^{m_{[\tilde{\beta}]}} \left( 1 + O \left( q^{-\frac{\min(d(\tilde{\alpha}))}{2}} \right) \right).
\]

Proof. Straight forward from Proposition 5.8 and Corollary 5.5. \( \square \)

6. PROOF OF THEOREM 1.2

For any \( (\tilde{c}, (f_{\tilde{s}})) \in \tilde{F}_{[\tilde{d}, \tilde{\alpha}]} \) and \( x \in \mathbb{P}^1(F_q) \),
\[
\sum_{\tilde{s} \in \mathcal{S}} \sum_{\tilde{\omega} \in \Omega_{\tilde{s}}} \chi_{\tilde{\alpha}} \left( F^{(\tilde{\omega})}_{(\tilde{s})} (x) \right) = |\{ \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} : \chi_{\tilde{\alpha}} \left( F^{(\tilde{\omega})}_{(\tilde{s})} (x) \right) \neq 0 \}|
\]
if \( \chi_{\tilde{\alpha}} \left( F^{(\tilde{\omega})}_{(\tilde{s})} (x) \right) = 0 \) or 1 for all \( \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} \) and 0 otherwise.

Now, if \( \{ \chi_{\tilde{\alpha}} \left( F^{(\tilde{\omega})}_{(\tilde{s})} (x) \right) , \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} \} \) is \( [\tilde{\beta}] \)-admissible then
\[
|\{ \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega_{\tilde{s}} : \chi_{\tilde{\alpha}} \left( F^{(\tilde{\omega})}_{(\tilde{s})} (x) \right) \neq 0 \}| = |A_{\tilde{\beta}}| = \frac{|G|}{e(\tilde{\beta})}
\]
Recall that \( e(\tilde{\beta}) = \text{lcm} \left( \frac{r_j}{(r_j, s_n)} \right) |r_n \). Then the number of points lying over \( x \in \mathbb{P}^1(F_q) \) will be \( \frac{|G|}{s_n} \) for some \( s_n | r_n \).
Proposition 6.1. Let $e_1, \ldots, e_{q+1}$ be such that $e_i = 0$ or $e_i = \frac{|G|}{s_n}$ for some $s_n|r_n$.

For all $s|r_n$ let

$$m_s = \{|1 \leq i \leq q+1 : e_i = \frac{|G|}{s}\}$$

and

$$m_0 = \{|1 \leq i \leq q+1 : e_i = 0\}$$

then

$$\left|\{(\vec{c}, (f_r)) \in \tilde{F}_{[\tilde{\beta}(\tilde{\omega})]} : \sum_{\vec{s} \in \mathcal{S}} \sum_{\tilde{\omega} \in \Omega_{\tilde{\omega}}} \chi_{\ell}(\tilde{\omega}) \left(F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)\right) = e_i, i = 1, \ldots, q+1\}\right|$$

$$= \left(\frac{|G|-1)(q+G|) - \sum_{s|r_n} s \phi_G(s) + 1}{G(q+G| - 1)}\right)^{m_0} \left(\frac{q}{G(q+G| - 1)}\right)^{m_1} \prod_{s|r_n, s \neq 1} \left(\frac{s \phi_G(s)}{G(q+G| - 1)}\right)^{m_s} \times (1 + O\left(q^{-\min(d(G))}\right))$$

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

Proof. Let

$$M_s = \{1 \leq i \leq q+1 : e_i = \frac{|G|}{s}\}$$

$$M_0 = \{1 \leq i \leq q+1 : e_i = 0\}$$

If $i \in M_s$, $s \neq 0$, then the set

$$\{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\}$$

will be $[\tilde{\beta}]$-admissible for some $\tilde{\beta}$ such that $e(\tilde{\beta}) = s$. Moreover, if $(\vec{s}, \bar{\omega}) \in A_{\tilde{\beta}}$ then

$$\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)) = 1.$$

Fix a partition of $M_s$ as

$$M_s = \bigcup_{|\tilde{\beta}| = s} \bigcup_{e(\tilde{\beta}) = s} \{i \in M_s : \{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\} \text{ is } [\tilde{\beta}]\text{-admissible}\}$$

and let $m_{s|\tilde{\beta}} = |M_{s|\tilde{\beta}}|$.

If $i \in M_0$, then the set

$$\{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\}$$

can be $[\tilde{\beta}]$-admissible for any $|\tilde{\beta}| \in \tilde{\mathcal{R}}$ as long as at least one of $\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})})$ is $1$ or $-1$.

Fix a partition of $M_0$ as

$$M_0 = \bigcup_{|\tilde{\beta}| = s} \bigcup_{e(\tilde{\beta}) = s} \{i \in M_0 : \{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\} \text{ is } [\tilde{\beta}]\text{-admissible}\}$$

and let $m_{0|\tilde{\beta}} = |M_{0|\tilde{\beta}}|$.

If $i \in M_{0|\tilde{\beta}}$ then there is only one choice for the set $\{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\}$. (Namely, $\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)) = 1$ if $(\vec{s}, \bar{\omega}) \in A_{\tilde{\beta}}$ and $0$ otherwise.) If $i \in M_{0|\tilde{\beta}}$, then there will be $|A_{\tilde{\beta}}| - 1 = \frac{|G|}{e(\tilde{\beta})} - 1$ choices for the set $\{\chi_{\ell}(\tilde{\omega}) (F_{(\tilde{\omega})}^{(\tilde{\beta})}(x_i)), \tilde{s} \in \mathcal{S}, \tilde{\omega} \in \Omega\}$. 


Therefore,
\[ |\{(\vec{c}, (f_a)) \in \tilde{F}_{[d(\vec{a})]} : \sum_{\vec{s} \in S, \sum_{i=1}^{q+1} \chi_{\ell}(s_i) \left(F^{(i)}_{\vec{a}}(x_i)\right) = \frac{G_i}{s_{n+1}}, i = 1, \ldots, q + 1}\}| \]
\[ = \sum_{M_{[\vec{\beta}]} \sum_{M_{0, [\vec{\beta}]}} \sum_{\vec{c}, \vec{d}, \vec{\omega}} \prod_{\vec{\beta} \in \mathcal{R}'} \left( \frac{\phi(e(\vec{\beta}))}{|G||q + |G|-1|} \right)^{m_{\beta} + m_{0, [\beta]}} \left( \frac{q}{|G||q + |G|-1|} \right)^{m_{0, [\vec{\beta}]}} \times \]
\[ = \sum_{M_{[\vec{\beta}]}} \sum_{M_{0, [\vec{\beta}]}} \sum_{\vec{c}, \vec{d}, \vec{\omega}} \prod_{\vec{\beta} \in \mathcal{R}'} \left( \frac{\phi(s^2)}{|G||q + |G|-1|} \right)^{m_{s}} \left( \frac{q}{|G||q + |G|-1|} \right)^{m_{1}} \times \]
\[ = \prod_{s | r_n} \left( \frac{\phi(s^2)}{|G||q + |G|-1|} \right)^{m_{s}} \sum_{e(\vec{\beta}) = s} 1 = s \sum_{e(\vec{\beta}) = s} 1 \]
\[ \sum_{\vec{\beta} \in \mathcal{R}} \phi(e(\vec{\beta}))|G| - e(\vec{\beta}) = \sum_{\vec{\beta} \in \mathcal{R}} (|G| - e(\vec{\beta})) = (|G| - 1)|G| - \sum_{\vec{\beta} \in \mathcal{R}} e(\vec{\beta}). \]

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
\[ \sum_{\vec{\beta} \in \mathcal{R}} e(\vec{\beta}) = \sum_{s | r_n} s \sum_{e(\vec{\beta}) = s} 1 = \sum_{s | r_n} s \phi_G(s) - 1. \]

Finally, we end it with the proof of Theorem 1.2.
Proof of Theorem 1.2.

\[
\left| \left\{ C \in H^1(d(\tilde{\alpha})) : \#C(\mathbb{P}^1(\mathbb{F}_q)) = M \right\} \right| \\
\frac{\left| H^1(d(\tilde{\alpha})) \right|}{\sum_{e_1, \ldots, e_{q+1}} \sum_{\sum e_i = M} \left| \{ (c_i, (f_\alpha)) \in \hat{F}_{|d(\tilde{\alpha})|} : \sum_{i \in S} \chi(\ell(x_i)) = e_i, i = 1, \ldots, q+1 \right\} |}
\]
\[
= \sum_{e_1, \ldots, e_{q+1}} \sum_{\sum e_i = M} \left( \frac{(|G| - 1)(q + |G|) - \sum_{s|\ell_n} s \phi_G(s) + 1}{|G|(q + |G| - 1)} \right)^{m_0} \left( \frac{q}{|G|(q + |G| - 1)} \right)^{m_1} \times
\]
\[
\prod_{s|\ell_n, s \neq 1} \left( \frac{s \phi_G(s)}{|G|(q + |G| - 1)} \right)^{m_s} \left( 1 + O \left( q^{-\min(d(\tilde{\alpha}))} \right) \right)
\]
\[
= \text{Prob} \left( \sum_{i=1}^{q+1} X_i = M \right) \left( 1 + O \left( q^{-\min(d(\tilde{\alpha}))} \right) \right).
\]

□

Acknowledgements: I would like to thank Chantal David for the countless discussions we had about this topic. I would also like to thank Elisa Lorenzo, Giulio Meleleo and Piermarco Milione for their helpful discussions about their paper which shed light on how to approach this problem.

References

[1] Alina Bucur, Chantal David, Brooke Feigon, Nathan Kaplan, Matilde Lalín, 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 Lalín, 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] David Steven Dummit and Richard M Foote, Abstract algebra, vol. 1984, Wiley Hoboken, 2004.

[5] Robin Hartshorne, Algebraic geometry, vol. 52, Springer Science & Business Media, 1977.

[6] Nicholas M Katz and Peter Sarnak, Random matrices, Frobenius eigenvalues, and monodromy, vol. 45, American Mathematical Soc., 1999.

[7] Pär Kurlberg and Zéev 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.

[8] Elisa Lorenzo, Giulio Meleleo, Piermarco Milione, and Alina Bucur, Statistics for biquadratic covers of the projective line over finite fields, to appear in Journal of Number Theory (2015).

[9] Patrick Meisner, Distribution of points on cyclic curves over finite fields, arXiv preprint arXiv:1511.07814 (submitted) (2015).

[10] Michael Rosen, Number theory in function fields, vol. 210, Springer Science & Business Media, 2013.