The Distribution of Points on Hyperelliptic Curves Over $\mathbb{F}_q$ of Genus g in Finite Extensions of $\mathbb{F}_q$

Manal Alzaharni

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics and Statistics) at
Concordia University
Montreal, Quebec, Canada

August 2015

Concordia University

School of Graduate Studies

This is to certify that the thesis prepared

By *Manal Alzahrani*

Entitled *The Distribution of Points on Hyperelliptic Curves Over $\mathbb{F}_q$ of Genus g in Finite Extensions of $\mathbb{F}_q$*

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

Master of Science (Mathematics and Statistics)

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

Signed by the final examining committee:

_____ Chair

Christopher Cummins, PhD

_____ Examiner

Christopher Cummins, PhD

_____ Examiner

Hershy Kisilevsky, PhD

_____ Supervisor

Chantal David, PhD

Approved by _____

Chair of Department or Graduate Program Director

_____ 2015 _____

Dean of Faculty

Abstract

The Distribution of Points on Hyperelliptic Curves Over $\mathbb{F}_q$ of Genus g in Finite Extensions of $\mathbb{F}_q$

Manal Alzahrani

For a fixed q and any $n \geq 1$, the number of $\mathbb{F}_{q^n}$-points on a hyperelliptic curve over $\mathbb{F}_q$ of genus g can be written as a $q^n + 1 + S$, where S is a certain character sum. We show that S behaves as a sum of $q^n + 1$ independent random variables as $g \to \infty$, with values depending on the parity of n. We get our result by generalizing the result of Kurlberg and Rudnick [1] for the distribution of the affine $\mathbb{F}_q$-points to any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, and using the techniques of Bucur, David, Feigon, and Lalin [2] to also consider the points at infinity over the full space of of hyperelliptic curves of genus g.

Acknowledgements

I would like to express my sincerest gratitude to Prof. Chantal David, whose expertise and guidance have supported me during my whole graduate experience at Concordia University. A thank you is extended to Iakovos Chinis for his valuable input in this research.

I am also grateful to the Saudi Arabian Cultural Bureau in Canada and the University of Dammam for offering me this scholarship to pursue my masters degree.

I also thank my loving husband, Mohammad Alzahrani for his support and patience throughout this trip. A thank you is also extended to my Father and Mother, who inspire me to strive to bring out the best in me, and to my cherished brother and sisters.

Contents

Notations

Throughout this thesis we will be using the following notations to describe sets of polynomials over $\mathbb{F}_q$, were $\mathbb{F}_q$ is a finite field of a fixed odd cardinality q :

$$V_d = \{f \in \mathbb{F}_q[x] : f \text{ monic, and } \deg(f) = d\}$$

$$\widetilde{V}_d = \{f \in \mathbb{F}_q[x] : \deg(f) \leq d-1\}$$

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

$$\widehat{\mathcal{F}}_d = \{f \in \mathbb{F}_q[x] : f \text{ square free, and } \deg(f) = d\}$$

Introduction

Given a finite field $\mathbb{F}_q$ of odd cardinality q and a square free monic polynomial $f \in \mathbb{F}_q[x]$, we get a smooth projective curve C_f of genus g with the affine model

$$C_f : y^2 = f(x) \ ,$$

where d is the degree of f. Since the genus of the curve is g, then $d = 2g + 1$ or $d = 2g + 2$.

The number of affine $\mathbb{F}_{q^n}$-points on such curve C_f is given by

$$\sum_{x \in \mathbb{F}_{q^n}} 1 + \chi_n(f(x)) = q^n + \mathcal{R}(f),$$

where $\mathcal{R}(f) = \sum_{x \in \mathbb{F}_{q^n}} \chi_n(f(x))$, and

$$\chi_n(x) = \begin{cases} 1 & x \text{ is a square in } \mathbb{F}_{q^n}^{\times} \\ 0 & x = 0 \\ -1 & x \text{ is not a square in } \mathbb{F}_{q^n}^{\times}, \end{cases}$$

for any $x \in \mathbb{F}_{q^n}$.

In the case of $n = 1$, which will be discussed in Chapter 3, Kurlberg and Rudnick [1] showed that $\mathcal{R}(f)$, as f ranges over monic square free polynomials of a certain degree d denoted by $\mathcal{F}_d$, behaves as a sum of q independent and identically distributed (i.i.d.) trinomial random variables taking the values ± 1 with probabilities $\dfrac{1}{2(1+q^{-1})}$, and the value 0 with probability $\dfrac{1}{q+1}$.

Our first goal is to find the distribution of the affine $\mathbb{F}_{q^n}$-points on C_f. So basically we need to find a way generalize the results of Kurlberg and Rudnick [1] for the case $n = 1$ to any $n \geq 2$.

In Chapter 4, we will give the necessary tools and lemmas for the transition from $\mathbb{F}_q$ to $\mathbb{F}_{q^n}$,

starting by a new representation of the elements of $\mathbb{F}_{q^n}$, which plays an important role in the proof of the counting lemma in $\mathbb{F}_{q^n}$. Then, we will find the number of quadratic residues in each subfield of $\mathbb{F}_{q^n}$.

After preparing all the necessary information, we start generalizing the result of Kurlberg and Rudnick [1] in Chapter 5. We find that $\mathcal{R}(f)$, as f ranges over monic square free polynomials of a fixed degree d, behaves as a sum q^n independent random variables with values depending on the parity of n.

For all $m|n$ we define a_m to be the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m. For each $m|n$ and $1 \leq i \leq a_m$, let $X_{m,i}$ represent a random variable with values depending on the parity of n. So if n is odd, then

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)}. \end{cases}$$

On the other hand, when n is even the values of the random variable depend on the parity of $\frac{n}{m}$. If $2 \nmid \frac{n}{m}$, then

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \end{cases},$$

and if $2|\frac{n}{m}$, we have

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{q^m+1} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \end{cases}.$$

In more detail, we prove the following theorem

Theorem. *For $d \geq 2$ and $s \in \mathbb{Z}$ with $|s| \leq q^n$, we have*

$$\frac{|\{f \in \mathcal{F}_d : \mathcal{R}(f) = s\}|}{|\mathcal{F}_d|} = Prob(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} = s) + \mathcal{O}(q^{2q^n - \frac{d}{2}}).$$

In the work of Kurlberg and Rudnick [1], f was ranging over monic square free polynomials of degree d. Therefore, not all hyperelliptic curves over $\mathbb{F}_q$ of genus g were considered. The method of Bucur, David, Feigon, and Lalin [2] covers the geometric point of view, which considers all hyperelliptic curves over $\mathbb{F}_q$ of genus g and the points at infinity on the curve C_f.

Let $\#C_f(\mathbb{F}_{q^n})$ denote the number of $\mathbb{F}_{q^n}$-points on C_f, where f is a square free polynomial (not necessarily monic) in $\mathbb{F}_q[x]$ with degree $2g+1$ or $2g+2$, as C_f have genus g. Then,

$$\begin{aligned}\#C_f(\mathbb{F}_{q^n}) &= \sum_{x\in\mathbb{P}^1(\mathbb{F}_{q^n})} 1+\chi_n(f(x)) \\ &= q^n+1+S(f)\end{aligned}$$

where $S(f)=\sum\limits_{x\in\mathbb{F}_{q^n}} \chi_n(f(x))+\chi_n(f(x_{q^n+1}))$, and x_{q^n+1} denotes the point at infinity.

For $n=1$, using the results of the affine case in Kurlberg and Rudnick [1] work, Bucur, David, Feigon, and Lalin [2] showed that as $g\to\infty$, $S(f)$ behaves as a sum of $q+1$ i.i.d. trinomial random variable taking the values ± 1 with probabilities $\dfrac{1}{2(1+q^{-1})}$, and the value 0 with probability $\dfrac{1}{q+1}$.

Our main result deals with the case $n\geq 2$. We prove in Chapter 6 that $S(f)$ behaves as a sum of q^n+1 independent random variables, where the possible values depend on the parity of n. For all $m|n$ and $1\leq i\leq a_m$, the random variables $X_{m,i}$ are defined as in the affine case, where their values depend on the parity of n. The extra random variable, denoted by X_{q^n+1} takes the following values, if n even

$$X_{q^n+1}=\begin{cases}1 & \text{with probability } \dfrac{q}{q^+1}\\ 0 & \text{with probability } \dfrac{1}{q+1}\end{cases},$$

and if n odd

$$X_{q^n+1}=\begin{cases}1 & \text{with probability } \dfrac{q}{q^+1}\\ 0 & \text{with probability } \dfrac{1}{q+1}\\ -1 & \text{with probability } \dfrac{q}{q^+1}\end{cases}.$$

In more detail, we prove the following,

Theorem. *For $g \geq 1$ and $s \in \mathbb{Z}$ with $|s| \leq q^n + 1$, we have*

$$\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \mathcal{S}(f) = s\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} = Prob(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} + X_{q^n+1} = s) + \mathcal{O}(q^{-g+2q^n}).$$

Finally, we finish with an application of our main result, which is finding the average number of $\mathbb{F}_{q^n}$-points on hyperelliptic curves C_f of genus g as $g \to \infty$, denoted by $< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g}$, where $\mathcal{H}_g = \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$. We will show in Chapter 6 that for $n \geq 1$

$$< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} = q^n + 1 + \begin{cases} q^{n/2} - \sum\limits_{\substack{m|n/2 \\ m \neq 1}} \dfrac{m a_m}{q^m + 1} & n \text{ even} \\ 0 & n \text{ odd} \end{cases} + \mathcal{O}(q^{-g+2q^n+2n}).$$

Another approach to finding the the average number of $\mathbb{F}_{q^n}$-points on hyperelliptic curves over $\mathbb{F}_q$ of genus g, was the work of Rudnick [3], who studied the average over monic, square free polynomials of degree $2g+1$. In the case of n odd, the results of Rudnick [3] agree with our findings but with a much better error term, as our main interest was finding the distribution of the $\mathbb{F}_{q^n}$-points. In the case of n even, his results differ, because he is not considering the whole space, but only polynomials of odd degree.

A more general approach to this problem is the work of Chinis [4], who studied the average over all hyperelliptic curves of genus g, following the techniques of Rudnick [3] for the monic, square free polynomials of degree $2g+1$ and generalizing it to all hyperelliptic curves of genus g. The results of Chinis [4] agree with our findings for the average number of points, but with a much better error term.

Chapter 1

Finite Fields

For more information about *Finite Fields* and for the proofs of the theorems in this chapter check [5].

A commutative ring $\mathbb{F}$ with identity 1 and a finite order is called a *Finite Field* if every nonzero element has a multiplicative inverse in $\mathbb{F}$, i.e. the multiplicative group of $\mathbb{F}$, denoted by $\mathbb{F}^\times$, is $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. With any finite field $\mathbb{F}$ we associate a prime number called *The Characteristic of The Field*, denoted by Char($\mathbb{F}$). It is defined to be the smallest positive integer such that $\text{Char}(\mathbb{F}) \cdot 1 = 0$.

Let p be an odd prime. If $\mathbb{F}$ is a finite field with characteristic p, then $\mathbb{F}$ is a finite dimensional vector space over $\mathbb{F}_p$, where $\mathbb{F}_p$ is the finite field of p elements $\mathbb{Z}/p\mathbb{Z}$. If $[\mathbb{F} : \mathbb{F}_p] = r$, then p^r is the order of $\mathbb{F}$ and it can be denoted by $\mathbb{F}_{p^r}$.

Let $f(x)$ be any polynomial in the Euclidean domain $\mathbb{F}[x]$.The following are some definitions and propositions that will be needed from Field Theory to complete our discussion on finite fields.

Definition 1.1. An extension field K of $\mathbb{F}$ is called a *splitting field* for $f(x) \in \mathbb{F}[x]$ if $f(x)$ factors completely into linear factors in K and not over any proper subfield of K containing F.

Proposition 1.1 (Uniqueness of Splitting Fields)**.** *Any two splitting fields for a polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$ are isomorphic.*

Definition 1.2. A polynomial over $\mathbb{F}$ is called *separable* if it has no multiple roots (i.e. all its roots are distinct).

Let $r \geq 1$ is a positive integer. Consider the separable polynomial $x^{p^r} - x \in \mathbb{F}_p[x]$, which has precisely p^r distinct roots. Let α and β be any two roots of this polynomial, then $\alpha^{p^r} = \alpha$ and

$\beta^{p^r} = \beta$. Since any field extension of $\mathbb{F}_p$ has characteristic p and using the Binomial Theorem we have that

$$(\alpha\beta)^{p^r} = \alpha\beta, \qquad (\alpha + \beta)^{p^r} = \alpha + \beta.$$

As a result, the set of all the p^r distinct roots of $x^{p^r} - x$ form a subfield of the splitting field, but since the splitting field, by definition, is the smallest field containing all the roots we get that the splitting field of $x^{p^r} - x$ is the field $\mathbb{F}_{p^r}$.

A special type of splitting fields is defined below:

Definition 1.3. Let $K/\mathbb{F}$ be a finite extension and let $\mathrm{Aut}(K/\mathbb{F})$ be the collection of automorphisms of K fixing $\mathbb{F}$. Then K is said to be *Galois* over $\mathbb{F}$ and $K/\mathbb{F}$ is a *Galois* extension if $|\mathrm{Aut}(K/\mathbb{F})| = [K : \mathbb{F}]$. If $K/\mathbb{F}$ is Galois then the group of automorphisms $\mathrm{Aut}(K/\mathbb{F})$ is called the *Galois group of* $K/\mathbb{F}$, denoted by $\mathrm{Gal}(K/\mathbb{F})$.

Definition 1.4. Let $K/\mathbb{F}$ be a Galois extension. If $\alpha \in K$ then the elements $\sigma(\alpha)$ for σ in $\mathrm{Gal}(K/\mathbb{F})$ are called *Galois conjugates* of α over $\mathbb{F}$.

Theorem 1.1. *The extension $K/\mathbb{F}$ is Galois if and only if K is the splitting field of some separable polynomial over $\mathbb{F}$.*

Theorem 1.2 (The Fundamental Theorem of Galois Theory)**.** *Let $K/\mathbb{F}$ be a Galois extension and $G = Gal(K/\mathbb{F})$, then there is a bijection between the subfields of K containing $\mathbb{F}$ and the subgroups of G, sending the subfield $E \subseteq K$ to $Gal(K/E)$ and the subgroup $H \leq G$ to the fixed field of H.*

Now, since $\mathbb{F}_{p^r}$ is the splitting field of the separable polynomial $x^{p^r} - x$ over $\mathbb{F}_p$, then $\mathbb{F}_{p^r}$ is unique up to isomorphism and is Galois over $\mathbb{F}_p$, with the cyclic Galois group of order r generated by the Frobenius automorphism σ_p, where $\sigma_p : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ is given by $\sigma_p(\alpha) = \alpha^p$, which fixes $\mathbb{F}_p$ since $\alpha = \alpha^p$ for $\alpha \in \mathbb{F}_p$, i.e.

$$\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/r\mathbb{Z}.$$

By the Fundamental Theorem of Galois Theory, we get that for each divisor of r there exists a corresponding subfield of $\mathbb{F}_{p^r}$.

Let $r = mn$ and $q = p^m$. Since $\mathbb{F}_{q^n}$ is Galois over $\mathbb{F}_p$, then $\mathbb{F}_{q^n}$ is Galois over $\mathbb{F}_q$ with a Galois group of order n.

From now on, we will fix $\mathbb{F}_q$ to be the base field of any Galois extension $\mathbb{F}_{q^n}$, where $n \geq 1$ and q is a power of an odd prime . As a result we get that $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ for all $m|n$.

Chapter 2

Polynomials Over Finite Fields

This chapter covers some topics from Chapters 1 and 2 of Michael Rosen's *Number Theory in Function Fields* [6].

Using the notations we defined in Chapter 1, let $\mathbb{F}_q$ be a finite field of order q, where q is a power of an odd prime.

Since the ring of polynomials $\mathbb{F}_q[x]$ is an Euclidean Domain, then it is a Unique Factorization Domain (UFD). Therefore, for any $f \in \mathbb{F}_q[x]$, $f \neq 0$, f can be written uniquely as

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t},$$

where $\alpha \in \mathbb{F}^\times$, P_i are monic irreducible polynomials in $\mathbb{F}_q[x]$. If $e_i = 1$ for all $1 \leq i \leq t$, then f is called a *square free* polynomial. We will denote the set of all square free polynomials in $\mathbb{F}_q[x]$ of degree d by $\widehat{\mathcal{F}}_d$, and the set of all all monic square free polynomials in $\mathbb{F}_q[x]$ of degree d by $\mathcal{F}_d$, i.e. $\alpha = 1$.

2.1 The Zeta Function in the Ring of Polynomials over a Finite Field

The analogous zeta function in $\mathbb{F}_q[x]$ is defined to be

$$\zeta_q(s) = \sum_{\substack{f \in \mathbb{F}_q[x] \\ f \text{monic}}} \frac{1}{|f|^s},$$

where $|f| = q^{\deg(f)}$. Note that all the terms in $\zeta_q(s)$ with the same degree have the same value, therefore we only need to know the number of monic polynomials of a certain degree to be able to rewrite $\zeta_q(s)$ with respect to degrees. Now since the number of monic polynomials of degree d is q^d, we see that

$$\begin{aligned}\sum_{\substack{\deg(f)\leq d\\ f\text{monic}}} \frac{1}{|f|^s} &= 1 \times \frac{1}{q^{0\times s}} + q \times \frac{1}{q^{1\times s}} + q^2 \times \frac{1}{q^{2\times s}} + \cdots + q^d \times \frac{1}{q^{d\times s}} \\ &= 1 + q^{1-s} + q^{2(1-s)} + \cdots + q^{d(1-s)} \\ &= \sum_{m=0}^{d} q^{m(1-s)}.\end{aligned}$$

Therefore,

$$\zeta_q(s) = \sum_{\substack{f\in\mathbb{F}_q[x]\\ f\text{monic}}} \frac{1}{|f|^s} = \lim_{d\to\infty} \sum_{\substack{\deg(f)\leq d\\ f\text{monic}}} \frac{1}{|f|^s} = \sum_{m=0}^{\infty} q^{m(1-s)}.$$

So, when $Re(s) > 1$ we get $|q^{(1-s)}| = q^{1-Re(s)} < 1$, then

$$\zeta_q(s) = \sum_{\substack{f\in\mathbb{F}_q[x]\\ f\text{monic}}} \frac{1}{|f|^s} = \frac{1}{1-q^{1-s}}.$$

Another way for rewriting $\zeta_q(s)$ using the unique factorization in $\mathbb{F}_q[x]$ to write the Euler product, which plays an important role in the proof of the prime number theorem in the ring of polynomials. First note that we can rewrite

$$\prod_{\substack{P\text{ irreducible}\\ P\text{ monic}}} (1 - \frac{1}{|P|^s})^{-1} = \prod_{i=1}^{\infty} (1 - \frac{1}{|P_i|^s})^{-1}.$$

Since $|\frac{1}{|P_i|^s}| = q^{-\mathrm{Re}(s)\ \deg(P)} < 1$ when $\mathrm{Re}(s) > 1$, using the geometric series we have

$$\begin{aligned}\prod_{i=1}^{\infty} (1 - \frac{1}{|P_i|^s})^{-1} &= \prod_{i=1}^{\infty} \sum_{n=0}^{\infty} \frac{1}{|P_i|^{ns}} \\ &= \sum_{n=0}^{\infty} \frac{1}{|P_1|^{ns}} \times \sum_{n=0}^{\infty} \frac{1}{|P_2|^{ns}} \times \dots \\ &= \sum_{n_1=0}^{\infty} \sum_{n_2=0}^{\infty} \cdots \frac{1}{(|P_1|^{n_1}|P_2|^{n_2}\dots)^s}.\end{aligned}$$

Since $\mathbb{F}_q[x]$ is a UFD, we have all possible factorizations of polynomials in $\mathbb{F}_q[x]$ as monic irreducible polynomials, therefore

$$\prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} (1 - \frac{1}{|P|^s})^{-1} = \prod_{i=1}^{\infty} (1 - \frac{1}{|P_i|^s})^{-1} = \sum_{\substack{f \in \mathbb{F}_q[x] \\ f \text{ monic}}} \frac{1}{|f|^s} = \zeta_q(s),$$

which is the Euler product in $\mathbb{F}_q[x]$.

2.2 The Prime Number Theorem in the Ring of Polynomials over a Finite Field

Here, and throughout the thesis, let a_n denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n. In this section we will prove the Prime Number Theorem (PNT) in the ring $\mathbb{F}_q[x]$, which state the following:

Theorem 2.1 (The Prime Number Theorem)**.**

$$a_n = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Proof. As we showed in Section 2.1, we can rewrite $\zeta_q(s)$ such that:

$$\zeta_q(s) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} (1 - \frac{1}{|P|^s})^{-1}.$$

Since $|P| = q^{\deg(P)} = q^d$, we see that all the terms with the same degree have the same representation. Therefore, for each degree d we have a_d terms, also we know that $\zeta_q(s) = \dfrac{1}{1 - q^{1-s}}$. So, we have the following:

$$\frac{1}{1 - q^{1-s}} = \prod_{d=1}^{\infty} \left(1 - q^{-sd}\right)^{-a_d},$$

and letting $u = q^{-s}$, and noting that since $\mathrm{Re}(s) > 1$ then $|u| < 1$, we have

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} \left(1 - u^d\right)^{-a_d}.$$

Now, in order to find a_d we will take the logarithmic derivative, i.e. $(\log(f))' = \dfrac{f'}{f}$. This gives

$$\log(1-qu) = \sum_{d=1}^{\infty} a_d \, \log\left(1-u^d\right),$$

$$\frac{-q}{1-qu} = \sum_{d=1}^{\infty} a_d \, \frac{-d\,u^{d-1}}{1-u^d},$$

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} d\,a_d \, \frac{u^d}{1-u^d}.$$

Expanding both sides using the geometric series $\displaystyle\sum_{k=1}^{\infty} a^k = \frac{a}{1-a}$, where $|a|<1$, we get

$$\sum_{n=1}^{\infty}(qu)^n = \sum_{d=1}^{\infty} d\,a_d \sum_{k=1}^{\infty} u^{kd},$$

and by comparing coefficients

$$q^n = \sum_{d|n} d\,a_d. \tag{2.1}$$

To find a_d we use the *Möbius inversion formula*, which states that if $f(n) = \sum_{d|n} g(d)$ for all $n \geq 1$ then $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$, where

$$\mu(d) = \begin{cases} (-1)^{\,\omega(d)} & d \text{ square free} \\ 0 & \text{otherwise,} \end{cases} \tag{2.2}$$

and $\omega(d)$ defines the number of distinct prime factors of d.

Now, using the Möbius inversion formula we have

$$\begin{aligned} n\,a_n &= \sum_{d|n} \mu(d)\, q^{\frac{n}{d}}, \\ a_n &= \frac{1}{n}\sum_{d|n} \mu(d)\, q^{\frac{n}{d}} = \frac{q^n}{n} + \frac{1}{n}\sum_{\substack{d|n \\ d\geq 2}} \mu(d)\, q^{\frac{n}{d}}, \\ a_n - \frac{q^n}{n} &= \frac{1}{n}\sum_{\substack{d|n \\ d\geq 2}} \mu(d)\, q^{\frac{n}{d}}. \end{aligned}$$

Then,

$$\begin{aligned}
|a_n - \frac{q^n}{n}| &\leq \frac{1}{n} \sum_{\substack{d|n \\ d\geq 2}} |\mu(d)|\, q^{\frac{n}{d}} \\
&\leq \frac{q^{\frac{n}{2}}}{n} + \frac{1}{n} \sum_{\substack{d|n \\ d\geq 3}} |\mu(d)|\, q^{\frac{n}{d}}, \qquad \text{equality holds when } n \text{ is even} \\
&\leq \frac{q^{\frac{n}{2}}}{n} + \frac{1}{n}\, q^{\frac{n}{3}} \sum_{\substack{d|n \\ d\geq 3}} |\mu(d)| \\
&\leq \frac{q^{\frac{n}{2}}}{n} + \frac{1}{n}\, q^{\frac{n}{3}} \sum_{d|n} |\mu(d)|.
\end{aligned}$$

Now, we want to find a bound for $\sum_{d|n} |\mu(d)|$ which is the number of square free divisors n. Let $n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$, then we see that

$$\sum_{d|n} |\mu(d)| = \text{number of square free divisors of } n = \binom{t}{0} + \binom{t}{1} + \cdots + \binom{t}{t} = \sum_{k=0}^{t} \binom{t}{k} = (1+1)^t = 2^t,$$

where $\binom{t}{k}$ is the number of square free divisors of n in the form of a product of k distinct prime divisors, and since $2^t \leq n$ we have

$$\sum_{d|n} |\mu(d)| \leq n.$$

So, we have

$$\begin{aligned}
|a_n - \frac{q^n}{n}| &\leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}} \\
&= \frac{q^{\frac{n}{2}}}{n} \left(1 + n\, q^{-\frac{n}{6}}\right) \\
&\leq C\, \frac{q^{\frac{n}{2}}}{n},
\end{aligned}$$

since $(1 + n\, q^{-\frac{n}{6}})$ is bounded. Therefore,

$$a_n = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

□

2.3 Counting Monic Square Free Polynomials in the Ring of Polynomials over a Finite Field

Recall that $\mathcal{F}_n$ denote the set of all monic square free polynomials of degree n in $\mathbb{F}_q[x]$. Our goal in this section is to find $b_n = |\mathcal{F}_n|$. We first note that

$$\begin{aligned}\prod_{\substack{P \text{ irreducible}\\ P \text{ monic}}} \left(1+\frac{1}{|P|^s}\right) &= \prod_{i=1}^{\infty}\left(1+\frac{1}{|P_i|^s}\right)\\ &= \left(1+\frac{1}{|P_1|^s}\right)\left(1+\frac{1}{|P_2|^s}\right)\dots\\ &= \sum_{\substack{f \text{ monic}\\ f \text{ SF}}} \frac{1}{|f|^s}\\ &= \sum_{f \text{ monic}} \frac{\delta(f)}{|f|^s},\end{aligned} \tag{2.3}$$

where

$$\delta(f) = \begin{cases} 1 & f \text{ SF}\\ 0 & \text{otherwise.}\end{cases}$$

Also, we can rewrite the product as

$$\prod_{\substack{P \text{ irreducible}\\ P \text{ monic}}} \left(1+\frac{1}{|P|^s}\right) = \prod_{\substack{P \text{ irreducible}\\ P \text{ monic}}} \frac{\left(1-|P|^{-2s}\right)}{\left(1-|P|^{-s}\right)} = \frac{\zeta_q(s)}{\zeta_q(2s)} = \frac{1-q^{1-2s}}{1-q^{1-s}},$$

and since $|f| = q^{\deg(f)} = q^n$, we see that for each degree n there are b_n monic square free polynomials.

So if we let $u = q^{-s}$, (2.3) becomes

$$\frac{1-qu^2}{1-qu} = \sum_{n=0}^{\infty} b_n u^n. \tag{2.4}$$

Expanding the L.H.S. as a geometric series, we get

$$\begin{aligned}\frac{1-qu^2}{1-qu} &= (1-qu^2)\sum_{k=0}^{\infty}(qu)^k \\ &= \sum_{k=0}^{\infty}(qu)^k - \sum_{k=0}^{\infty} q^{k+1}u^{k+2} \\ &= \sum_{k=0}^{\infty} q^k u^k - \sum_{k=2}^{\infty} q^{k-1}u^k \\ &= 1 + qu + \sum_{k=2}^{\infty} q^k(1-q^{-1})u^k,\end{aligned}$$

and replacing in (2.4), this gives

$$1 + qu + \sum_{k=2}^{\infty} q^k(1-q^{-1})u^k = \sum_{n=0}^{\infty} b_n u^n.$$

Finally, by comparing coefficients, we get the following

Lemma 2.1.

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

Chapter 3

The Distribution of $\mathbb{F}_q$-Points of $\mathbb{F}_q$-Hyperelliptic Curves of Genus g

We review in this chapter the work of Kurlberg and Rudnick [1] and Bucur, David, Feigon, and Lalin [2] for the distribution of $\mathbb{F}_q$-points of hyperelliptic curves over $\mathbb{F}_q$ of genus g.

Let C_f be a smooth projective hyperelliptic curve over $\mathbb{F}_q$ of genus g with the affine model

$$C_f : y^2 = f(x),$$

where $f \in \mathbb{F}_q[x]$ is a square free polynomial (not necessarily monic). Therefore, the degree of f is either $2g+1$ or $2g+2$.

The goal is to find the distribution of $\mathbb{F}_q$-points of hyperelliptic curves over $\mathbb{F}_q$ of genus g with the affine model C_f where $f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$ (where $\widehat{\mathcal{F}}_d$ is the set of square free polynomials over $\mathbb{F}_q$ of degree d). Let $\#C_f(\mathbb{F}_q)$ denote the number of $\mathbb{F}_q$-points on C_f for some f.
For any affine point $x \in \mathbb{F}_q$, let

$$\chi(x) = \begin{cases} 1 & x \text{ is a square in } \mathbb{F}_q^\times \\ 0 & x = 0 \\ -1 & x \text{ is not a square in } \mathbb{F}_q^\times. \end{cases}$$

Then,

$$\#C_f(\mathbb{F}_q) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} 1 + \chi(f(x)), \tag{3.1}$$

where the value of f at the point of infinity is given by the value of $x^{2g+2}f(1/x)$ at zero.

The character sum in (3.1) is equal to the number of $\mathbb{F}_q$-points on C_f, since any affine point $x \in \mathbb{F}_q$ corresponds to $1 + \chi(f(x))$ points on the curve C_f. So, we have one point on the curve if x is a root of if $f(x)$, two points if $f(x)$ is a square in $\mathbb{F}_q^\times$ and no corresponding $\mathbb{F}_q$-points on the curve if $f(x)$ is not a square in $\mathbb{F}_q^\times$.

As for the point at infinity, since C_f is a smooth projective hyperelliptic curve over $\mathbb{F}_q$, then C_f consists of two affine pieces

$$y^2 = f(x), \qquad w^2 = v^{2g+2}f(1/v)$$

with the glueing maps

$$(x, y) \longmapsto (1/x, y/x^{g+1}), \qquad (v, w) \longmapsto (1/v, w/v^{g+1}).$$

Then the value of $f(x)$ at the point at infinity is given by the value of $v^{2g+2}f(1/v)$ at zero.

If $f(x) = c_0x^d + c_1x^{d-1} + \cdots + c_d$ where $c_0 \neq 0$, then

$$w^2 = v^{2g+2}f(1/v) = \begin{cases} c_0 + c_1v + \cdots + c_{d-1}v^{d-1} + c_dv^d & d \text{ even} \\ c_0v + c_1v^2 + \cdots + c_{d-1}v^d + c_dv^{d+1} & d \text{ odd.} \end{cases}$$

As a result, if d is odd then we only have one point at infinity. If d is even and c_0 is a square in $\mathbb{F}_q^\times$ then we have two points at infinity on the curve C_f, and finally if d is even and c_0 is not a square in $\mathbb{F}_q^\times$ then there are no points corresponding to infinity on the curve.[1]

Let $x_1, x_2, \ldots, x_{q+1}$ be the points on $\mathbb{P}^1(\mathbb{F}_q)$ such that x_{q+1} denotes the point at infinity, then $\chi(f(x_{q+1}))$ is defined to be

$$\chi(f(x_{q+1})) = \begin{cases} 0 & \text{if } f \in \widehat{\mathcal{F}}_{2g+1} \\ 1 & \text{if } f \in \widehat{\mathcal{F}}_{2g+2} \text{ and the leading coefficient is a square in } \mathbb{F}_q \\ -1 & \text{if } f \in \widehat{\mathcal{F}}_{2g+2} \text{ and the leading coefficient is not a square in } \mathbb{F}_q. \end{cases}$$

Therefore, we can rewrite

$$\#C_f(\mathbb{F}_q) = q + 1 + S(f),$$

[1]For more details on algebraic curves, see [7]. In particular, the above smooth model at infinity for hyperelliptic curves is Exercise 2.14..

where $S(f) = \sum_{x \in \mathbb{F}_q} \chi(f(x)) + \chi(f(x_{q+1}))$.

As we are interested in finding the distribution of $\mathbb{F}_q$-points on curves C_f as f ranges over $f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, we need to evaluate $|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\}|$, where $|s| \leq q+1$.

Choosing ε_i from $\{-1, 0, 1\}$ for all $1 \leq i \leq q+1$, we can rewrite

$$\#\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\} = \sum_{\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{q+1} = s} |\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi(f(x_i)) = \varepsilon_i,\ 1 \leq i \leq q+1\}|$$

The results of Bucur, David, Feigon, and Lalin [2] showed that the probability of $\chi(f(x_i)) = \varepsilon_i$ for $1 \leq i \leq q+1$ as f ranges over $\widehat{\mathcal{F}}_{2g+1} \bigcup \widehat{\mathcal{F}}_{2g+2}$ is given by the probability of $q+1$ independent and identically distributed (i.i.d.) trinomial random variables taking the values ε_i for $1 \leq i \leq q+1$ as $g \to \infty$, i.e. $X_i = \varepsilon_i$ where X_i for $1 \leq i \leq q+1$ denote the i.i.d. trinomial random variables taking the values ± 1 with probabilities $1/2(1+q^{-1})$ and the value 0 with probability $1/(q+1)$. More precisely,

Proposition 3.1. *Let $\varepsilon_i \in \{-1, 0, 1\}$ for all $1 \leq i \leq q+1$, and let $m = |\{i \in \{1, 2, \ldots, q+1\} : \varepsilon_i = 0\}|$. Then,*

$$\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \bigcup \widehat{\mathcal{F}}_{2g+2} : \chi(f(x_i)) = \varepsilon_i \ \ \forall\, 1 \leq i \leq q+1\}|}{|\widehat{\mathcal{F}}_{2g+1}| + |\widehat{\mathcal{F}}_{2g+2}|} = \left(\frac{1}{q+1}\right)^m \left(\frac{1}{2(1+q^{-1})}\right)^{q+1-m} (1 + \mathcal{O}(q^{\frac{m}{2}+q-g-1})).$$

As a result of Proposition 3.1, we can find the average number of $\mathbb{F}_q$-points on C_f, denoted by $< \#C_f(\mathbb{F}_q) >_{f \in \mathcal{H}_g}$, where $\mathcal{H}_g = \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$.

Corollary 3.1. *As $g \to \infty$, we have*

$$< \#C_f(\mathbb{F}_q) >_{f \in \mathcal{H}_g} \sim q+1$$

Proof. Since

$$\#C_f(\mathbb{F}_q) = q + 1 + S(f),$$

then, using Proposition 3.1 and taking $g \to \infty$, we get

$$\begin{aligned} < \#C_f(\mathbb{F}_q) >_{f \in \mathcal{H}_g} &\sim q + 1 + \sum_{s=-(q+1)}^{q+1} s \ \text{Prob}(\sum_{i=1}^{q+1} X_i = s) \\ &\sim q + 1 + E(\sum_{i=1}^{q+1} X_i = s), \end{aligned}$$

where $E(Y)$ is the expected value of the random variable Y. Since the expected value is linear and $E(X_i) = 0$ for all $1 \leq i \leq q+1$, we get our result. $\square$

Proposition 3.1 is a corollary of the work of Kurlberg and Rudnick [1], who studied the distribution of the affine $\mathbb{F}_q$-points on hyperelliptic curves of a certain degree over $\mathcal{F}_d$. In the affine case, the number of $\mathbb{F}_q$-points on C_f can be written as $q + \mathcal{R}(f)$, where $\mathcal{R}(f) = \sum_{x \in \mathbb{F}_q} \chi(f(x))$. They showed that $\mathcal{R}(f)$ behaves as the sum of q i.i.d. trinomial random variables as $d \to \infty$ and f ranges over $\mathcal{F}_d$. In more detail,

Proposition 3.2. *Let $\varepsilon_i \in \{-1, 0, 1\}$ for all $1 \leq i \leq q$, and let $m = |\{i \in \{1, 2, \ldots, q\} : \varepsilon_i = 0\}|$. Then,*

$$\frac{|\{f \in \mathcal{F}_d : \chi(f(x_i)) = \varepsilon_i \ \forall 1 \leq i \leq q\}|}{|\mathcal{F}_d|} = \left(\frac{1}{q+1}\right)^m \left(\frac{1}{2(1+q^{-q})}\right)^{q-m} (1 + \mathcal{O}(q^{(3q-d)/2})).$$

So by considering the possible cases of ε_{q+1}, which corresponds to the point at infinity, and using Proposition 3.2 in each affine case we get the result in Proposition 3.1. All the details of Bucur, David, Feigon, and Lalin [2] method will be covered thoroughly later in Chapter 6.

The core of Kurlberg and Rudnick [1] results is the following simple counting lemma. Let $V_d = \{f \in \mathbb{F}_q[x] : f \text{ monic and } \deg(f) = d\}$.

Lemma 3.1. *For $\ell \leq q$ let $x_1, x_2, \ldots, x_\ell \in \mathbb{F}_q$ be distinct elements, and let $c_1, c_2, \ldots, c_\ell \in \mathbb{F}_q$. If $d \geq \ell$, then*

$$|\{f \in V_d : f(x_1) = c_1, \ldots, f(x_\ell) = c_\ell\}| = q^{d-\ell}.$$

The proof of Lemma 3.1 depend on the fact that the evaluation map $g(x) \to (g(x_1), \ldots, g(x_\ell))$ is surjective, where $g \in \widetilde{V}_d = \{g \in \mathbb{F}_q[x] : \deg(g) \leq d-1\}$ and the map $f(x) \to g(x) = f(x) - x^d$ defines a bijection from V_d to $\widetilde{V}_d$.

Chapter 4

Tools & Counting Lemma for $\mathbb{F}_{q^n}$

To find the distribution of $\mathbb{F}_{q^n}$-points on hyperelliptic curves over $\mathbb{F}_q$ of genus g for any $n \geq 1$, we will start in Chapter 5 by generalizing the results of Kurlberg and Rudnick [1] of the affine case to any finite extension of $\mathbb{F}_q$, then in Chapter 6 we will use the method of Bucur, David, Feigon, and Lalin [2] to find the distribution for genus g. However, before proceeding we need to give special care to the representation of the elements of $\mathbb{F}_{q^n}$, which will be covered in Section 4.1. We then can proceed to prove the counting lemma for $\mathbb{F}_{q^n}$ (Lemma 4.2). Also, in Section 4.2 we will find the number of quadratic residues in each subfield of $\mathbb{F}_{q^n}$.

4.1 Representation of the Elements of $\mathbb{F}_{q^n}$

Let $x_1, \ldots, x_{q^n}$ be an enumeration of the elements in the finite field $\mathbb{F}_{q^n}$ and let $c_1, \ldots, c_{q^n}$ be any set of elements in $\mathbb{F}_{q^n}$. Since Lemma 3.1 is the base of Kurlberg and Rudnick [1] work, we are interested in finding the number of elements in $\{f \in V_d : f(x_1) = c_1, \ldots, f(x_{q^n}) = c_{q^n}\}$. Therefore, we need to find a way to represent these q^n elements of $\mathbb{F}_{q^n}$ such that the evaluation map $g(x) \to (g(x_1), \ldots, g(x_{q^n}))$ from $\widetilde{V}_d \to \mathbb{F}_{q^n}^{q^n}$ can be surjective, where $\widetilde{V}_d = \{g \in \mathbb{F}_q[x] : \deg(g) \leq d-1\}$.

Since $\forall\ m|n$ there exists a subfield $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, let $x_0 \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$, then the degree of the minimal polynomial of x_0 over $\mathbb{F}_q$ is m . If there is a prescribed value for $f \in \mathbb{F}_q[x]$ at x_0 , then the values of f at the m Galois conjugates of x_0 over $\mathbb{F}_q$ are prescribed by $f(x_0)$ since f is defined over $\mathbb{F}_q$ and $\sigma(f(x_0)) = f(\sigma(x_0))$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Thus, instead of considering all the elements of $\mathbb{F}_{q^n}$, we will only take into account the number of Galois conjugate classes in each $\mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$ where $m|n$.

If $a_m = |\{P \in \mathbb{F}_q[x] : P \text{ is a monic irreducible polynomial of degree } m\}|$, then we have

Lemma 4.1. *Let $m|n$, then $|\mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}| = ma_m$.*

Proof. Let $m|n$ and $\alpha \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$. Since $\mathbb{F}_{q^m}/\mathbb{F}_q$ is an algebraic extension, there exists an irreducible polynomial $P \in \mathbb{F}_q[x]$ such that $P(\alpha) = 0$, where

$$\deg(P) = [\mathbb{F}_q[x]/(P(x)) : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q].$$

Now, since

$$\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^m} \text{ and } \mathbb{F}_q(\alpha) \not\subseteq \mathbb{F}_{q^k} \ \forall\ k|m, k \neq m,$$

then

$$\deg(P) = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m.$$

Therefore, all the elements of $\mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$ are roots of irreducible polynomials over $\mathbb{F}_q$ of degree m.

On the other hand, let $J \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and β a root of J. Since

$$[\mathbb{F}_q(\beta) : \mathbb{F}_q] = [\mathbb{F}_q[x]/(J(x)) : \mathbb{F}_q] = \deg(J) = m,$$

then $\mathbb{F}_q(\beta) \simeq \mathbb{F}_{q^m}$. As a result, any irreducible polynomial over $\mathbb{F}_q$ of degree m has its roots in $\mathbb{F}_{q^m}$ and not in any subfield of it. Since a_m denote the number of irreducible polynomial of degree m, we get our result.

□

As a result, we can use $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$ for all $m|n$ as a new representation of the initial enumeration $x_1, \ldots, x_{q^n}$ in our case of polynomials with prescribed values at the points of $\mathbb{F}_{q^n}$. Because $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$ for all $m|n$ is a list of the non-Galois conjugate elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $\sum_{m|n} |\mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}| = \sum_{m|n} ma_m = q^n$ as proven in (2.1).

With this representation of the elements of $\mathbb{F}_{q^n}$ we can show that the evaluation map is surjective, as shown in the following essential counting lemma, which is equivalent to Kurlberg and

Rudnick [1] counting lemma in finite extension of $\mathbb{F}_q$.

Lemma 4.2 (Counting Lemma)**.** *For all $m|n$ let $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$ and $c_{m,1}, c_{m,2}, \ldots, c_{m,a_m} \in \mathbb{F}_{q^m}$.*
If $d > q^n$, then

$$|\{f \in V_d : f(x_{m,i}) = c_{m,i} \ \forall \ m|n \text{ and } 1 \leq i \leq a_m\}| = q^{d-q^n}.$$

Proof. Let $\widetilde{V}_d = \{g \in \mathbb{F}_q[x] : \deg(g) \leq d-1\}$. Then there is a bijection between V_d and $\widetilde{V}_d$ defined by the map $f(x) \longmapsto f(x) - x^d = g(x)$. Therefore,

$$|\{f \in V_d : f(x_{m,i}) = c_{m,i}, \forall\, m|n, 1 \leq i \leq a_m\}| = |\{g \in \widetilde{V}_d : g(x_{m,i}) = c_{m,i} - x_{m,i}^d, \forall\, m|n, 1 \leq i \leq a_m\}|. \tag{4.1}$$

Now, the evaluation map $\psi : \widetilde{V}_d \longrightarrow V = \prod_{m|n} (\mathbb{F}_{q^m})^{a_m}$ is a linear map between the vector spaces $\widetilde{V}_d$ and V with d and $\sum_{m|n} m\ a_m = q^n$ as the dimensions over $\mathbb{F}_q$, respectively.

First, we want to show that ψ is a surjective map. Since $\mathrm{Im}\psi \subseteq V$, we only need to prove that $|\mathrm{Im}\psi| = |V|$. The kernel of ψ consists of all $g \in \widetilde{V}_d$ such that

$$g(x) = \prod_{m|n} \prod_{i=1}^{a_m} \prod_{j=0}^{m-1} (x - x_{m,i}^{q^j}) h(x),$$

where $h(x) \in \mathbb{F}_q[x]$ and $\deg(h) \leq d-1-q^n$. Therefore, $\dim_{\mathbb{F}_q} \mathrm{Ker}\psi = d - q^n$.
Since

$$\dim_{\mathbb{F}_q} \widetilde{V}_d = \dim_{\mathbb{F}_q} \mathrm{Ker}\psi + \dim_{\mathbb{F}_q} \mathrm{Im}\psi,$$

we get that

$$\dim_{\mathbb{F}_q} \ \mathrm{Im}\psi = d - (d - q^n) = q^n,$$

and since $\dim_{\mathbb{F}_q} V = q^n$, we find that $|\mathrm{Im}\psi| = q^{q^n} = |V|$.

As ψ is surjective, we know that for all $b_{m,1}, b_{m,2}, \ldots, b_{m,a_m} \in \mathbb{F}_{q^m}$ and $m|n$ there exists a function $g \in \widetilde{V}_d$ such that $g(x_{m,i}) = b_{m,i}, \forall m|n$ and $1 \leq i \leq a_m$. Thus, the coset $g + \mathrm{Ker}\psi \in \widetilde{V}_d/\mathrm{Ker}\psi$ represent the set of all functions in $\widetilde{V}_d$ with the value $b_{m,i}$ at $x_{m,i}$, $\forall m|n$ and $1 \leq i \leq a_m$.

Since $|g + \mathrm{Ker}\psi| = |\mathrm{Ker}\psi| = q^{d-q^n}$, both sides of (4.1) are equal to q^{d-q^n}.

□

4.2 The Number of Quadratic Residues in Subfields of $\mathbb{F}_{q^n}$

Another point we need to consider is the number of quadratic residues in $\mathbb{F}_{q^n}$ and in each subfield of this finite field. The importance of understanding this fact arises from using the quadratic character of $\mathbb{F}_{q^n}^{\times}$ along with our new enumeration of the non-Galois conjugate elements of $\mathbb{F}_{q^n}$, which will be used in finding the distribution of the $\mathbb{F}_{q^n}-$points on hyperelliptic curves over $\mathbb{F}_q$.

For $m|n$, let $\#QR_n(\mathbb{F}_{q^m})$ denote the number of elements of $\mathbb{F}_{q^m}$ which are squares in $\mathbb{F}_{q^n}$.

Lemma 4.3. *Let $m|n$, then*

$$\#QR_n(\mathbb{F}_{q^m}) = \begin{cases} \dfrac{q^m-1}{2} & 2 \nmid \dfrac{n}{m} \\ q^m - 1 & 2|\dfrac{n}{m}. \end{cases}$$

Proof. First we want to show that the number of squares in $\mathbb{F}_{q^m}^{\times}$, denoted by $\#QR_m(\mathbb{F}_{q^m})$, is equal to $\dfrac{q^m-1}{2}$, for all $m|n$.

Let α be a square in the multiplicative group of the field $\mathbb{F}_{q^m}$, denoted by $\mathbb{F}_{q^m}^{\times}$, such that $\alpha = \beta^2$ for some $\beta \in \mathbb{F}_{q^m}^{\times}$. Then using Lagrange theorem, we have that $\alpha^{\frac{q^m-1}{2}} = \beta^{q^m-1} = 1$, since $|\mathbb{F}_{q^m}^{\times}| = q^m - 1$. Hence, α is a root of $x^{(q^m-1)/2} - 1 \in \mathbb{F}_{q^m}[x]$, which have at most $\dfrac{q^m-1}{2}$ roots, as a result

$$\#QR_m(\mathbb{F}_{q^m}) \leq \frac{q^m-1}{2}.$$

On the other hand, noting that the polynomial $x^2 - \alpha \in \mathbb{F}_{q^m}[x]$ has exactly two roots if α is a square in $\mathbb{F}_{q^m}^{\times}$ we get that

$$q^m - 1 \leq \sum_{\alpha \in QR_m(\mathbb{F}_{q^m})} |\{x \in \mathbb{F}_{q^m}^{\times} : x^2 = \alpha\}| = 2\ \#QR_m(\mathbb{F}_{q^m}),$$

which shows that $\#QR_m(\mathbb{F}_{q^m}) = \dfrac{q^m-1}{2}$.

Now to find $\#QR_n(\mathbb{F}_{q^m})$ for any $m|n$, we will consider two cases based on the parity of n, but first note that if $\alpha \in \mathbb{F}_{q^m}$ is a quadratic residue in $\mathbb{F}_{q^m}$ then it is also a quadratic residue in $\mathbb{F}_{q^n}$,

and as a result we have the lower bound

$$\#QR_n(\mathbb{F}_{q^m}) \geq \frac{q^m - 1}{2}.$$

Let $\alpha \in \mathbb{F}_{q^m}^{\times}$ be a quadratic non-residue in $\mathbb{F}_{q^m}$, then $x^2 - \alpha$ is an irreducible polynomial over $\mathbb{F}_{q^m}$. If β is a root of $x^2 - \alpha$ in $\mathbb{F}_{q^n}$, then $\mathbb{F}_{q^m}(\beta)$ is a subfield of $\mathbb{F}_{q^n}$ such that

$$\begin{aligned}[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] &= [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}(\beta)][\mathbb{F}_{q^m}(\beta) : \mathbb{F}_{q^m}] \\ &= [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}(\beta)] \times 2.\end{aligned}$$

Since $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] = \dfrac{n}{m}$, then we will have two cases :

- If $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}]$ is odd, then
$$\#QR_n(\mathbb{F}_{q^m}) = \frac{q^m - 1}{2}.$$

- If $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}]$ is even, then we will show that for all quadratic non-residues $\alpha \in \mathbb{F}_{q^m}^{\times}$ there exists $\beta \in \mathbb{F}_{q^n}$ such that $\beta^2 = \alpha$.

  let γ be a root of the irreducible polynomial $x^2 - \alpha \in \mathbb{F}_{q^m}[x]$. Since $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^m}(\gamma)$ and $[\mathbb{F}_{q^m}(\gamma) : \mathbb{F}_{q^m}] = 2$, we see that $\mathbb{F}_{q^m}(\gamma) \cong \mathbb{F}_{q^{2m}}$ which is a subfield of $\mathbb{F}_{q^n}$ since $2m|n$ in this case. Therefore, if $\beta \in \mathbb{F}_{q^n}$ corresponded to γ we get our result. Then we have that

$$\#QR_n(\mathbb{F}_{q^m}) = q^m - 1.$$

□

Chapter 5

The Distribution of Affine $\mathbb{F}_{q^n}$-Points on a Family of $\mathbb{F}_q$-Hyperelleptic Curves

In this Chapter, we generalize the work of Kurlberg and Rudnick [1] from $\mathbb{F}_q$ to $\mathbb{F}_{q^n}$. We will find that the parity of n plays an important role.

Let C_f be a smooth projective hyperelleptic curve over $\mathbb{F}_q$ with the affine model

$$C_f : y^2 = f(x),$$

where $f \in \mathbb{F}_q[x]$ is a monic square free polynomial of degree $d \geq 3$. Therefore, the genus is $g = (d-2)/2$ when d is even and $g = (d-1)/2$ when d is odd.

Now, similarly to the discussion in Chapter 3, we get that the number of affine $\mathbb{F}_{q^n}$-points on C_f is given by the character sum

$$\sum_{x \in \mathbb{F}_{q^n}} 1 + \chi_n(f(x)) = q^n + \mathcal{R}(f),$$

where $\mathcal{R}(f) = \sum_{x \in \mathbb{F}_{q^n}} \chi_n(f(x))$, and

$$\chi_n(x) = \begin{cases} 1 & x \text{ is a square in } \mathbb{F}_{q^n}^{\times} \\ 0 & x = 0 \\ -1 & x \text{ is not a square in } \mathbb{F}_{q^n}^{\times}, \end{cases}$$

for any $x \in \mathbb{F}_{q^n}$.

To find the distribution of the affine $\mathbb{F}_{q^n}$-points on C_f as f ranges over $\mathcal{F}_d$, we will start by finding the probability that $\mathcal{R}(f) = s$, where $|s| \leq q^n$ since $\mathcal{R}(f)$ is bounded.

Now, we need to find a way to rewrite $|\{f \in \mathcal{F}_d : \mathcal{R}(f) = s\}|$ using the fact that $\mathcal{R}(f) = \sum_{x \in \mathbb{F}_{q^n}} \chi_n(f(x))$. Since the quadratic character χ_n have the same value at an element of $\mathbb{F}_{q^n}$ and its Galois conjugates, we can use the non-Galois conjugates enumeration of the elements of $\mathbb{F}_{q^n}$ mentioned earlier, as a result

$$\mathcal{R}(f) = \sum_{m|n} m \sum_{i=1}^{a_m} \chi_n(f(x_{m,i})),$$

where $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$ are distinct non-Galois conjugates over $\mathbb{F}_q$ for all $m|n$.

In this chapter we will show that $\mathcal{R}(f)$ behaves as a sum of q^n independent random variables from the set $\{X_{m,i} : m|n, 1 \leq i \leq a_m\}$ as $d \to \infty$, where each random variable $X_{m,i}$ appears m times.

The values each random variable takes depend on the parity of n. When n is odd, each random variable $X_{m,i}$, where $m|n$ and $1 \leq i \leq a_m$, takes the values 0, ± 1 with probabilities $\frac{1}{q^m+1}$, $\frac{q^m}{2(q^m+1)}$ and $\frac{q^m}{2(q^m+1)}$, respectively. On the other hand, when n is even we need to consider two cases depending on the parity of $\frac{n}{m}$ for all $m|n$. If $2 \nmid \frac{n}{m}$, then each $X_{m,i}$, where $1 \leq i \leq a_m$, takes the values 0, ± 1 with the probabilities $\frac{1}{q^m+1}, \frac{q^m}{2(q^m+1)}$ and $\frac{q^m}{2(q^m+1)}$, respectively. Otherwise, i.e. $2|\frac{n}{m}$, each $X_{m,i}$ takes the values 0 with probability $\frac{1}{q^m+1}$ and 1 with probability $\frac{q^m}{q^m+1}$ where $1 \leq i \leq a_m$.

Our result is a version of Kurlberg and Rudnick [1] work in finite extensions of $\mathbb{F}_q$, in the following sense,

Theorem 5.1. *For $d \geq 2$ and $s \in \mathbb{Z}$ with $|s| \leq q^n$, we have*

$$\frac{|\{f \in \mathcal{F}_d : \mathcal{R}(f) = s\}|}{|\mathcal{F}_d|} = Prob(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} = s) + \mathcal{O}(q^{2q^n - \frac{d}{2}}).$$

More precisely, for all $m|n$ let $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$, and let $\varepsilon_{m,i} \in \{-1, 0, 1\}$ such that $1 \leq i \leq a_m$, then

$$\frac{|\{f \in \mathcal{F}_d : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \, \forall \, m|n, \, 1 \leq i \leq a_m\}|}{|\mathcal{F}_d|}$$
$$= \prod_{m|n} \left(\frac{1}{q^m + 1}\right)^{s_m} \left(\frac{q^m}{2^{\lambda_{n,m}}(q^m + 1)}\right)^{a_m - s_m} + \mathcal{O}(q^{q^n - \frac{1}{2}(d + \sum\limits_{m|n} m s_m)}),$$

where $s_m = |\{i \in \{1, \ldots, a_m\} : \varepsilon_{m,i} = 0\}|$ and

$$\lambda_{n,m} = \begin{cases} 1 & n \text{ odd} \\ 1 & n \text{ even and } 2 \nmid \frac{n}{m} \\ 0 & n \text{ even and } 2 | \frac{n}{m}. \end{cases}$$

5.1 The Probability of Taking Nonzero Prescribed Values

To prove Theorem 5.1, we will first start by finding the probability of $f \in \mathcal{F}_d$ taking any prescribed set of nonzero values on all q^n points of $\mathbb{F}_{q^n}$.

Lemma 5.1. *Let $d \geq 2$ be a positive integer.*
For all $m|n$, let $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$ and $c_{m,1}, c_{m,2}, \ldots, c_{m,a_m} \in \mathbb{F}_{q^m}$ be nonzero elements. Then

$$\frac{|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \leq i \leq a_m\}|}{|\mathcal{F}_d|} = q^{-q^n} \prod_{m|n} (1 - q^{-2m})^{-a_m} + \mathcal{O}(q^{-\frac{d}{2}}).$$

Proof. Lets start by finding the following

$$|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \leq i \leq a_m\}| = \sum_{\substack{f \in \mathcal{F}_d \\ f(x_{m,i}) = c_{m,i} \\ \forall m|n, 1 \leq i \leq a_m}} 1 = \sum_{\substack{f \in V_d \\ f(x_{m,i}) = c_{m,i} \\ \forall m|n, 1 \leq i \leq a_m}} \sum_{g^2 | f} \mu(g),$$

since

$$\sum_{g^2|f} \mu(g) = \begin{cases} 1 & \text{if } f \text{ is square free} \\ 0 & \text{otherwise .} \end{cases}$$

Therefore,

$$\begin{aligned} |\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}| \\ &= \sum_{\substack{g \in \mathbb{F}_q[x] \\ g \text{ monic} \\ \deg(g) \le d/2}} \mu(g) \sum_{\substack{f \in V_d \\ g^2|f \\ f(x_{m,i}) = c_{m,i} \\ \forall m|n, 1 \le i \le a_m}} 1 \\ &= \sum_{\substack{g \in \mathbb{F}_q[x] \\ g \text{ monic} \\ \deg(g) \le d/2}} \mu(g) \ |\{f \in V_d : f(x_{m,i}) = g^2(x_{m,i})h(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}| \\ &= \sum_{\substack{g \in \mathbb{F}_q[x] \\ g \text{ monic} \\ \deg(g) \le d/2}} \mu(g) \ |\{h \in V_{d-2 \ \deg(g)} : g^2(x_{m,i})h(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}|. \end{aligned}$$

Since we chose $c_{m,i} \in \mathbb{F}_{q^m}^{\times}$, $\forall m|n, 1 \le i \le a_m$, then there exists a multiplicative inverse for each $g(x_{m,i})$ in $\mathbb{F}_{q^m}$. Another consequence for $f(x_{m,i}) = c_{m,i} \neq 0$ is the fact that we are only counting polynomials in $\mathbb{F}_q[x]$ that are not zero at $x_{m,i}$, $\forall m|n, 1 \le i \le a_m$.

Let $\mathcal{G} = \{f \in \mathbb{F}_q[x] : f(x) \text{ monic }, \ f(x_{m,i}) \neq 0 \ \forall m|n, 1 \le i \le a_m\}$, then

$$\begin{aligned} |\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}| \\ &= \sum_{\substack{g \in \mathcal{G} \\ \deg(g) \le d/2}} \mu(g) \ |\{h \in V_{d-2 \ \deg(g)} : h(x_{m,i}) = c_{m,i} \ g^{-2}(x_{m,i}) \ \forall m|n, 1 \le i \le a_m\}|. \quad (5.1) \end{aligned}$$

Now, to evaluate $|\{h \in V_{d-2 \ \deg(g)} : h(x_{m,i}) = c_{m,i} \ g^{-2}(x_{m,i}) \ \forall m|n, 1 \le i \le a_m\}|$ in equation (5.1), we need to consider different bounds on $d - 2\deg(g)$.

If $d - 2\deg(g) > q^n$, then we can use Lemma 4.2 to get

$$\sum_{\substack{g\in\mathcal{G}\\ \deg(g)<\frac{d-q^n}{2}}} \mu(g)\ |\{h \in V_{d-2\ \deg(g)} : h(x_{m,i}) = c_{m,i}\ g^{-2}(x_{m,i})\ \forall m|n, 1 \le i \le a_m\}|$$

$$= q^{d-q^n} \sum_{\substack{g\in\mathcal{G}\\ \deg(g)<\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)}. \quad (5.2)$$

The other case is when $d - 2\deg(g) \le q^n$, then $\frac{d-q^n}{2} \le \deg(g) \le \frac{d}{2}$ and so there exist at most a unique monic polynomial h in $\mathbb{F}_q[x]$ of degree at most q^n with prescribed values at $x_{m,i}$ for all $m|n$ and $1 \le i \le a_m$. As if there exists two monic polynomials $h_1, h_2 \in \mathbb{F}_q[x]$ such that

$$h_j(x_{m,i}) = c_{m,i}\ \forall m|n, 1 \le i \le a_m,\ j \in \{1, 2\}$$

then $h_1 - h_2$ is a polynomial of degree at most $q^n - 1$ with q^n zeros at $x_{m,i}, \forall m|n, 1 \le i \le a_m$, therefore $h_1 = h_2$.

Accordingly, when $d - 2\deg(g) \le q^n$, we get

$$\sum_{\substack{g\in\mathcal{G}\\ \frac{d-q^n}{2}\le\deg(g)\le\frac{d}{2}}} \mu(g)\ |\{h \in V_{d-2\ \deg(g)} : h(x_{m,i}) = c_{m,i}\ g^{-2}(x_{m,i})\ \forall m|n, 1 \le i \le a_m\}| \le \sum_{\substack{g\in\mathcal{G}\\ \frac{d-q^n}{2}\le\deg(g)\le\frac{d}{2}}} 1$$

$$\le \frac{q}{q-1}\, q^{d/2},$$

and so

$$\sum_{\substack{g\in\mathcal{G}\\ \frac{d-q^n}{2}\le\deg(g)\le\frac{d}{2}}} \mu(g)|\{h \in V_{d-2\ \deg(g)} : h(x_{m,i}) = c_{m,i}\ g^{-2}(x_{m,i})\ \forall m|n, 1 \le i \le a_m\}| = \mathcal{O}(q^{d/2}). \quad (5.3)$$

Now, back to equation (5.2) to evaluate the sum in our main term

$$\sum_{\substack{g\in\mathcal{G}\\ \deg(g)<\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)} = \sum_{g\in\mathcal{G}} \mu(g)\ q^{-2\ \deg(g)} - \sum_{\substack{g\in\mathcal{G}\\ \deg(g)\ge\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)}. \quad (5.4)$$

For the first term of equation (5.4), note that

$$\begin{aligned}\sum_{g\in\mathcal{G}}\mu(g)\ q^{-2\ \deg(g)} = \sum_{g\in\mathcal{G}}\mu(g)|g|^{-2} &= \prod_{\substack{P\in\mathbb{F}_q[x]\\ P\ irreducible\\ P(x_{m,i})\neq 0\\ \forall m|n, 1\leq i\leq a_m}} (1-|P|^{-2}) \\ &= \prod_{\substack{P\in\mathbb{F}_q[x]\\ P\ irreducible}} (1-|P|^{-2}) \prod_{\substack{P\in\mathbb{F}_q[x]\\ P\ irreducible\\ P(x_{m,i})=0\\ \forall m|n, 1\leq i\leq a_m}} (1-|P|^{-2})^{-1} \\ &= \frac{1}{\zeta_q(2)} \prod_{\substack{P\in\mathbb{F}_q[x]\\ P\ irreducible\\ P(x_{m,i})=0\\ \forall m|n, 1\leq i\leq a_m}} (1-|P|^{-2})^{-1} \\ &= \frac{1}{\zeta_q(2)} \prod_{m|n}(1-q^{-2m})^{-a_m},\end{aligned}$$

since the product was running over the minimal polynomials over $\mathbb{F}_q$ of $x_{m,i}$ $\forall m|n, 1\leq i\leq a_m$. As for the second term of equation (5.4), we have

$$|\sum_{\substack{g\in\mathcal{G}\\ \deg(g)\geq\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)}| \leq \sum_{\substack{g\in\mathcal{G}\\ \deg(g)\geq\frac{d-q^n}{2}}} q^{-2\ \deg(g)} \leq \sum_{\substack{g\in\mathbb{F}_q[x]\\ g\ monic\\ \deg(g)\geq\frac{d-q^n}{2}}} q^{-2\ \deg(g)}$$

so

$$|\sum_{\substack{g\in\mathcal{G}\\ \deg(g)\geq\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)}| = \mathcal{O}\Big(\sum_{k=\frac{d-q^n}{2}}^{\infty} q^{-k}\Big) = \mathcal{O}(q^{\frac{q^n-d}{2}}).$$

Replacing in (5.2), we find that

$$q^{d-q^n}\sum_{\substack{g\in\mathcal{G}\\ \deg(g)<\frac{d-q^n}{2}}} \mu(g)\ q^{-2\ \deg(g)} = q^{d-q^n}\Big(\frac{1}{\zeta_q(2)}\prod_{m|n}(1-q^{-2m})^{-a_m} + \mathcal{O}(q^{\frac{q^n-d}{2}})\Big), \tag{5.5}$$

and replacing (5.5) and (5.3) in (5.1) gives

$$|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}| = \frac{q^{d-q^n}}{\zeta_q(2)} \prod_{m|n} (1-q^{-2m})^{-a_m} + \mathcal{O}(q^{\frac{d-q^n}{2}}) + \mathcal{O}(q^{\frac{d}{2}})$$
$$= \frac{q^{d-q^n}}{\zeta_q(2)} \prod_{m|n} (1-q^{-2m})^{-a_m} + \mathcal{O}(q^{\frac{d}{2}}), \tag{5.6}$$

and since $|\mathcal{F}_d| = \frac{q^d}{\zeta_q(2)}$ for $d \ge 2$, we get the result of Lemma 5.1.

□

5.2 The Probability of Taking Any Prescribed Set of Values

Now, we will determine the probability of $f \in \mathcal{F}_d$ to attain any set of prescribed values on all the points of $\mathbb{F}_{q^n}$.

Proposition 5.1. *Let $d \ge 2$ be a positive integer.*
For all $m|n$ and $0 \le s_m \le a_m$, let $x_{m,1}, x_{m,2}, \dots, x_{m,a_m-s_m}, \dots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \ne m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$, and $c_{m,1}, c_{m,2}, \dots, c_{m,a_m-s_m} \in \mathbb{F}_{q^m}^{\times}$, $c_{m,a_m-(s_m-1)} = \cdots = c_{m,a_m} = 0$.
Then

$$|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}| = q^{d-q^n}(1-q^{-1}) \prod_{m|n} \frac{(1-q^{-m})^{s_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}(q^{\frac{\sum_{m|n} m s_m + d}{2}}),$$

and,

$$\frac{|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i} \ \forall m|n, 1 \le i \le a_m\}|}{|\mathcal{F}_d|} = q^{-q^n} \prod_{m|n} \frac{(1-q^{-m})^{s_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}(q^{\frac{\sum_{m|n} m s_m - d}{2}}).$$

Proof. Any polynomial $f \in \mathcal{F}_d$ which vanish on $\mathcal{H} = \bigcup_{m|n} \{x_{m,a_m-(s_m-1)}, \dots, x_{m,a_m}\}$ can be written as

$$f(x) = \prod_{m|n} \prod_{i=a_m-(s_m-1)}^{a_m} \prod_{j=0}^{m-1} (x - x_{m,i}^{q^j}) g(x),$$

where $x_{m,i}, x_{m,i}^q, \ \dots \ , x_{m,i}^{q^{m-1}}$ are the Galois conjugates of $x_{m,i}$ over $\mathbb{F}_q$, and $g(x) \in \mathcal{F}_{d-\sum_{m|n} m s_m}$ is a

non vanishing polynomial on $\mathcal{H}$.

Based on the prescribed values f takes at each $x_{m,\ell}$, $\forall\, m|n, 1 \le \ell \le a_m$, we have that

$$g(x_{m,\ell}) = e_{m,\ell} = \begin{cases} c_{m,\ell} \prod\limits_{m|n} \prod\limits_{i=a_m-(s_m-1)}^{a_m} \prod\limits_{j=0}^{m-1} (x_{m,\ell} - x_{m,i}^{q^j})^{-1} & 1 \le \ell \le a_m - s_m \\ b_{m,\ell} & a_m - (s_m - 1) \le \ell \le a_m, \end{cases}$$

where $b_{m,\ell} \in \mathbb{F}_q^\times$ is arbitrary, and $b_{m,\ell} \neq 0$ since g does not vanish there.

Therefore, we have $\prod\limits_{m|n} (q^m - 1)^{s_m}$ possibilities for g with prescribed values at $x_{m,i}$ for all $m|n\,, 1 \le i \le a_m$, so

$$|\{f \in \mathcal{F}_d : f(x_{m,i}) = c_{m,i}\ \forall m|n, 1 \le i \le a_m\}| = \prod_{m|n} (q^m - 1)^{s_m}\ |\{g \in \mathcal{F}_{d-\sum_{m|n} m s_m} : g(x_{m,i}) = e_{m,i} \neq 0\ \forall m|n, 1 \le i \le a_m\}|. \quad (5.7)$$

Now, using Lemma 5.1, in particular equation (5.6), we see that equation (5.7) is equal to

$$\begin{aligned} &\prod_{m|n} (q^m - 1)^{s_m} \Big(\frac{q^{d-\sum_{m|n} m s_m - q^n}}{\zeta_q(2)} \prod_{m|n} (1 - q^{-2m})^{-a_m} + \mathcal{O}(q^{\frac{d-\sum_{m|n} m s_m}{2}}) \Big) \\ &= q^{\sum_{m|n} m s_m} \prod_{m|n} (1 - q^{-m})^{s_m} \Big(\frac{q^{d-\sum_{m|n} m s_m - q^n}}{\zeta_q(2)} \prod_{m|n} (1 - q^{-2m})^{-a_m} + \mathcal{O}(q^{\frac{d-\sum_{m|n} m s_m}{2}}) \Big) \\ &= \frac{q^{d-q^n}}{\zeta_q(2)} \prod_{m|n} \frac{(1 - q^{-m})^{s_m}}{(1 - q^{-2m})^{a_m}} + \mathcal{O}(q^{\frac{d+\sum_{m|n} m s_m}{2}}), \end{aligned}$$

and since $\zeta_q(2) = \dfrac{1}{(1 - q^{-1})}$, we get the first statement. Dividing by $|\mathcal{F}_d| = \frac{q^d}{\zeta_q(2)}$ for $d \ge 2$, we get the second result.

□

5.3 The Distribution of Points on a Family of Hyperelliptic Curves over $\mathbb{F}_q$ in Finite Extensions

To prove Theorem 5.1, let $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup\limits_{\substack{k|m \\ k \neq m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$, and let $\varepsilon_{m,i} \in \{-1, 0, 1\}$ such that $1 \le i \le a_m$ and $s_m = |\{i \in \{1, \ldots, a_m\} : \varepsilon_{m,i} = 0\}|$, for all $m|n$.

Since Proposition 5.1 shows that the probability of $f \in \mathcal{F}_d$ taking a set of prescribed values

depend only on the number of zeros, then we just need to understand the number of quadratic residues of $\mathbb{F}_{q^n}$ in each subfield $\mathbb{F}_{q^m}$ such that $m|n$. As shown in Lemma 4.3, the number of quadratic residues depend on the parity of $\frac{n}{m}$.

If n is odd, then for all $m|n$ we have that $\frac{n}{m}$ is odd. Therefore, the number of quadratic residues of $\mathbb{F}_{q^n}$ in each subfield $\mathbb{F}_{q^m}$ such that $m|n$, respectively quadratic non-residues, equals $\frac{q^m-1}{2}$. Therefore,

$$\begin{aligned}
&\frac{|\{f \in \mathcal{F}_d : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall m|n, 1 \le i \le a_m\}|}{|\mathcal{F}_d|} \\
&\quad = \prod_{m|n} \left(\frac{q^m-1}{2}\right)^{a_m - s_m} (q^{-q^n} \prod_{m|n} \frac{(1-q^{-m})^{s_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{\frac{1}{2}(\sum_{m|n} m s_m - d)}\right)) \\
&\quad = q^{-\sum_{m|n} m s_m} \ 2^{-\sum_{m|n}(a_m - s_m)} \prod_{m|n} \frac{(1-q^{-m})^{a_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}(q^{q^n - \frac{1}{2}(\sum_{m|n} m s_m + d)}) \\
&\quad = q^{-\sum_{m|n} m s_m} \ 2^{-\sum_{m|n}(a_m - s_m)} \prod_{m|n} \frac{1}{(1+q^{-m})^{a_m}} + \mathcal{O}(q^{q^n - \frac{1}{2}(\sum_{m|n} m s_m + d)}). \qquad (5.8)
\end{aligned}$$

In this case of n odd, let $\{X_{m,i}\}_{\substack{m|n \\ 1 \le i \le a_m}}$ be $\sum_{m|n} a_m$ independent random variables taking the values

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \end{cases}.$$

Then we see that the probability that $X_{m,i} = \varepsilon_{m,i}$ for any choice of $\varepsilon_{m,i} \in \{-1, 0, 1\}$ for all $m|n$ and $1 \le i \le a_m$ is

$$\begin{aligned}
\text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \le i \le a_m\right) &= \prod_{m|n} \prod_{i=1}^{a_m} \text{Prob}\left(X_{m,i} = \varepsilon_{m,i}\right) \\
&= \prod_{m|n} \left(\frac{1}{q^m+1}\right)^{s_m} \left(\frac{q^m}{2(q^m+1)}\right)^{a_m - s_m} \\
&= 2^{-\sum_{m|n} a_m - s_m} \ q^{-\sum_{m|n} m s_m} \prod_{m|n} \frac{1}{(1+q^{-m})^{a_m}},
\end{aligned}$$

which is equal to the main term of equation (5.8). Therefore, as $d \to \infty$

$$\frac{|\{f \in \mathcal{F}_d : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \,\forall\, m|n, 1 \le i \le a_m\}|}{|\mathcal{F}_d|} \sim \text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \le i \le a_m\right). \tag{5.9}$$

On the other hand, if n is even, then the number of quadratic residues of $\mathbb{F}_{q^n}$ in each subfield $\mathbb{F}_{q^m}$ where $m|n$ defer depending on the parity of $\frac{n}{m}$. Thus, by using Lemma 4.3 we get

$$\begin{aligned}
&\frac{|\{f \in \mathcal{F}_d : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \,\forall m|n, 1 \le i \le a_m\}|}{|\mathcal{F}_d|} \\
&= \prod_{\substack{m|n \\ 2\nmid \frac{n}{m}}} \left(\frac{q^m-1}{2}\right)^{a_m - s_m} \prod_{\substack{m|n \\ 2|\frac{n}{m}}} (q^m-1)^{a_m-s_m} \left(q^{-q^n} \prod_{m|n} \frac{(1-q^{-m})^{s_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{\frac{1}{2}(\sum\limits_{m|n} m s_m - d)}\right)\right) \\
&= q^{-\sum\limits_{m|n} m s_m} 2^{-\sum_{\substack{m|n \\ 2\nmid \frac{n}{m}}} a_m - s_m} \prod_{m|n} \frac{1}{(1+q^{-m})^{a_m}} + \mathcal{O}\left(q^{q^n - \frac{1}{2}(\sum\limits_{m|n} m s_m + d)}\right).
\end{aligned} \tag{5.10}$$

Now, let $\{X_{m,i}\}_{\substack{m|n \\ 1\le i\le a_m}}$ be $\sum_{m|n} a_m$ independent random variables, which take different values depending on the parity of $\frac{n}{m}$. So, when $2 \nmid \frac{n}{m}$ we have

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \end{cases}.$$

Otherwise, when $2|\frac{n}{m}$ we have

$$X_{m,i} = \begin{cases} 0 & \text{with probability } \dfrac{1}{q^m+1} \\ 1 & \text{with probability } \dfrac{q^m}{q^m+1} \end{cases}.$$

Then the probability that $X_{m,i} = \varepsilon_{m,i}$ for any $\varepsilon_{m,i} \in \{-1, 0, 1\}$ for all $m|n$ and $1 \le i \le a_m$ is equal

to

$$\begin{aligned}
&\text{Prob}\left(X_{m,i}=\varepsilon_{m,i} \text{ for all } m|n \text{ and } 1\le i\le a_m\right)\\
&\qquad=\prod_{m|n}\prod_{i=1}^{a_m}\text{Prob}\left(X_{m,i}=\varepsilon_{m,i}\right)\\
&\qquad=\prod_{\substack{m|n\\ 2\nmid \frac{n}{m}}}\left(\frac{1}{q^m+1}\right)^{s_m}\left(\frac{q^m}{2(q^m+1)}\right)^{a_m-s_m}\prod_{\substack{m|n\\ 2\mid \frac{n}{m}}}\left(\frac{1}{q^m+1}\right)^{s_m}\left(\frac{q^m}{q^m+1}\right)^{a_m-s_m}\\
&\qquad=2^{-\sum\limits_{\substack{m|n\\ 2\nmid\frac{n}{m}}}a_m-s_m}\,q^{-\sum\limits_{m|n}ms_m}\prod_{m|n}\frac{1}{(1+q^{-m})^{a_m}}. \qquad (5.11)
\end{aligned}$$

Since equation (5.11) is equal to the main term of equation (5.10), we get

$$\frac{|\{f\in\mathcal{F}_d:\chi_n(f(x_{m,i}))=\varepsilon_{m,i}\,\forall m|n,1\le i\le a_m\}|}{|\mathcal{F}_d|}\sim\text{Prob}\left(X_{m,i}=\varepsilon_{m,i}\text{ for all } m|n \text{ and } 1\le i\le a_m\right), \qquad (5.12)$$

as $d\to\infty$.

Now, to prove the first statement in Theorem 5.1 we can rewrite

$$\frac{|\{f\in\mathcal{F}_d:\mathcal{R}(f)=s\}|}{|\mathcal{F}_d|}=\sum_{\sum\limits_{m|n}m\sum\limits_{i=1}^{a_m}\varepsilon_{m,i}=s}\frac{|\{f\in\mathcal{F}_d:\chi_n(f(x_{m,i}))=\varepsilon_{m,i}\,\forall m|n\ ,1\le i\le a_m\}|}{|\mathcal{F}_d|}. \qquad (5.13)$$

Using the results in (5.9) and (5.12), which shows that for any $n\ge 1$ the summand of (5.13) can be represented by the probability of $\sum_{m|n}a_m$ independent random variables taking specific values as $d\to\infty$, we get

$$\begin{aligned}
&\frac{|\{f\in\mathcal{F}_d:\mathcal{R}(f)=s\}|}{|\mathcal{F}_d|}\\
&\qquad=\sum_{\sum\limits_{m|n}m\sum\limits_{i=1}^{a_m}\varepsilon_{m,i}=s}\left(\text{Prob}\left(X_{m,i}=\varepsilon_{m,i}\text{ for all } m|n \text{ and } 1\le i\le a_m\right)+\mathcal{O}\left(q^{q^n-\frac{1}{2}(\sum\limits_{m|n}ms_m+d)}\right)\right)\\
&\qquad=\text{Prob}\left(\sum_{m|n}m\sum_{i=1}^{a_m}X_{m,i}=s\right)+\mathcal{O}\left(q^{2q^n-\frac{d}{2}}\right). \qquad (5.14)
\end{aligned}$$

Therefore, (5.14) shows that $\mathcal{R}(f)$ behaves as a sum of q^n independent random variables from the set $\{X_{m,i} : m|n, 1 \leq i \leq a_m\}$ as $d \to \infty$, where each random variable $X_{m,i}$ appears m times, which conclude the proof of Theorem 5.1 .

Chapter 6

The Distribution of $\mathbb{F}_{q^n}$-Points on $\mathbb{F}_q$-Hyperelliptic Curves of Genus g

Our goal in this chapter is to generalize Bucur, David, Feigon, and Lalin [2] method, briefly mentioned in Chapter 3, to find the distribution of points on hyperelliptic curves over $\mathbb{F}_q$ of genus g in finite extensions of $\mathbb{F}_q$, by using the results of Chapter 5 for the distribution of affine $\mathbb{F}_{q^n}$-points on hyperelliptic curves C_f as f ranges over $\mathcal{F}_d$ for some $d \geq 3$.

We then need to consider taking $f \in \widehat{\mathcal{F}}_d$, and adding the points at infinity on these curves. Depending in the parity of d, we see that there is only one point at infinity on C_f when d is odd, and when d is even there are either two points at infinity, or no points at infinity, which rely on whether the leading coefficient of f is a square or not, and the parity of n.

Let C_f be a a smooth projective hyperelleptic curve over $\mathbb{F}_q$ of genus g with the affine model

$$C_f : y^2 = f(x),$$

where $f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, and let $\#C_f(\mathbb{F}_{q^n})$ denote the number of $\mathbb{F}_{q^n}$-points on C_f.
Then, in view of the discussion of Chapter 3, we can write

$$\#C_f(\mathbb{F}_{q^n}) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_{q^n})} 1 + \chi_n(f(x)),$$

where χ_n is the quadratic character of $\mathbb{F}_{q^n}^\times$ for any $x \in \mathbb{F}_{q^n}$, and the value of χ_n at the point at infinity is given by the value of $x^{2g+2} f(1/x)$ at zero.

Let $x_{m,1}, x_{m,2}, \ldots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k\neq m}} \mathbb{F}_{q^k}$ for all $m|n$ be an enumeration of the non-Galois conjugate elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ in each subfield $\mathbb{F}_{q^m}$, and let x_{q^n+1} denote the point at infinity, then

$$\begin{aligned}\#C_f(\mathbb{F}_{q^n}) &= \sum_{m|n} m \sum_{i=1}^{a_m} (1+\chi_n(f(x_{m,i}))) + 1 + \chi_n(f(x_{q^n+1})) \\ &= q^n + 1 + S(f),\end{aligned}$$

where $S(f) = \sum\limits_{m|n} m \sum\limits_{i=1}^{a_m} \chi_n(f(x_{m,i})) + \chi_n(f(x_{q^n+1}))$, and

$$\chi_n(f(x_{q+1})) = \begin{cases} 0 & \text{if } f \in \widehat{\mathcal{F}}_{2g+1} \\ 1 & \text{if } f \in \widehat{\mathcal{F}}_{2g+2} \text{ and the leading coefficient is a square in } \mathbb{F}_{q^n} \\ -1 & \text{if } f \in \widehat{\mathcal{F}}_{2g+2} \text{ and the leading coefficient is not a square in } \mathbb{F}_{q^n}. \end{cases}$$

Since we are interested in finding the distribution of $\mathbb{F}_{q^n}$-points on curves C_f as f ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, we will start by finding the probability that $S(f) = s$ where $|s| \leq q^n + 1$, and as before we need to understand $|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\}|$.

As χ_n takes the values $0, \pm 1$, let $\varepsilon_{m,i}, \varepsilon_{q^n+1} \in \{-1, 0, 1\}$ for all $m|n$ and $1 \leq i \leq a_m$. Then for some $s \in \mathbb{Z}$ such that $|s| \leq q^n + 1$ we have

$$\begin{aligned}&|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\}| = \\ &\sum_{\sum\limits_{m|n} m \sum\limits_{i=1}^{a_m} \varepsilon_{m,i} + \varepsilon_{q^n+1} = s} |\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \,\forall\, m|n \,,\, 1 \leq i \leq a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|.\end{aligned} \tag{6.1}$$

Now, to evaluate (6.1) we will consider two cases depending on the parity of n, but first lets make the following notation, for any $m|n$ let

$$r_m = \begin{cases} |\{i \in \{1, \ldots, a_m\} : \varepsilon_{m,i} = 0\}| & m \neq 1 \\ |\{i \in \{1, \ldots, a_m\} : \varepsilon_{m,i} = 0\}| & m = 1, \varepsilon_{q^n+1} \neq 0 \\ |\{i \in \{1, \ldots, a_m\} : \varepsilon_{m,i} = 0\}| + 1 & m = 1, \varepsilon_{q^n+1} = 0, \end{cases}$$

and let $r = \sum_{m|n} r_m$.

6.1 n Odd

To evaluate (6.1) we will consider two cases depending on the possible values of ε_{q^n+1}, and since n is odd, $\varepsilon_{q^n+1} = \chi_n(f(x_{q^n+1}))$ can take all possible values $0, \pm 1$, as these values depend on the leading coefficient of f in $\mathbb{F}_q^\times$.

i. $\boldsymbol{\varepsilon_{q^n+1} = 0}$:

In this case the number of zeros among $\varepsilon_{m,1}, \ldots, \varepsilon_{m,a_m}$ for all $m|n$ is $r-1$, and there are no polynomials in $f \in \widehat{\mathcal{F}}_{2g+2}$ such that $\chi_n(f(x_{q^n+1})) = 0$ and for all polynomials in $f \in \widehat{\mathcal{F}}_{2g+1}$ we see that $\chi_n(f(x_{q^n+1})) = 0$, then

$$\begin{aligned} &|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}| \\ &\quad = |\{f \in \widehat{\mathcal{F}}_{2g+1} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m\}| \\ &\quad = \sum_{\alpha \in \mathbb{F}_q^\times} |\{g \in \mathcal{F}_{2g+1} : \chi_n(\alpha)\chi_n(g(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m\}|\ . \end{aligned} \tag{6.2}$$

Now, to evaluate (6.2) we need to take into account that since n is odd, there are $\dfrac{q^m-1}{2}$ quadratic residues, and the same number of quadratic non-residues, in each subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$, and since there are $q-1$ possibilities for the leading coefficient, we see that by using the first statement of Proposition 5.1, (6.2) can be written as

$$\begin{aligned} &(q-1)\left(\frac{q-1}{2}\right)^{q-(r_1-1)} \prod_{\substack{m|n \\ m\neq 1}} \left(\frac{q^m-1}{2}\right)^{a_m-r_m} \left[(1-q^{-1})q^{2g+1-q^n}\frac{(1-q^{-1})^{r_1-1}}{(1-q^{-2})^q}\right. \\ &\left.\prod_{\substack{m|n \\ m\neq 1}} \frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{(2g+1+r_1-1+\sum_{\substack{m|n \\ m\neq 1}} mr_m)/2}\right)\right] \\ &\quad = 2^{-(q-(r_1-1)+\sum_{\substack{m|n \\ m\neq 1}}(a_m-r_m))}\, q^{1-(r_1-1)+q^n-\sum_{\substack{m|n \\ m\neq 1}} mr_m}\, (1-q^{-1})^{1+q-(r_1-1)} \prod_{\substack{m|n \\ m\neq 1}} (1-q^{-m})^{a_m-r_m} \\ &\times \left[(1-q^{-1})\, q^{2g+1-q^n}\frac{(1-q^{-1})^{r_1-1}}{(1-q^{-2})^q} \prod_{\substack{m|n \\ m\neq 1}} \frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{(2g+1+r_1-1+\sum_{\substack{m|n \\ m\neq 1}} mr_m)/2}\right)\right], \end{aligned}$$

$$= 2^{-(q-(r_1-1)+\sum_{\substack{m|n\\ m\neq 1}}(a_m-r_m))}\, q^{2g+3-r_1-\sum_{\substack{m|n\\ m\neq 1}} mr_m} \frac{(1-q^{-1})^2}{(1+q^{-1})^q} \prod_{\substack{m|n\\ m\neq 1}} \frac{1}{(1+q^{-m})^{a_m}}$$
$$+ \mathcal{O}\left(q^{q^n+g+2-\frac{1}{2}(r_1+\sum_{\substack{m|n\\ m\neq 1}} mr_m)}\right). \tag{6.3}$$

ii. $\boldsymbol{\varepsilon_{q^n+1} = \pm 1}$:

In this case there are r zeros among $\varepsilon_{m,1}, \ldots, \varepsilon_{m,a_m}$ for all $m|n$, and we only consider polynomials in $\widehat{\mathcal{F}}_{2g+2}$, since $\chi_n(f(x_{q^n+1})) = 0$ for all $f \in \widehat{\mathcal{F}}_{2g+1}$. As there are $\dfrac{q-1}{2}$ leading coefficients such that $\chi_n(f(x_{q^n+1})) = 1$, and the same number such that $\chi_n(f(x_{q^n+1})) = -1$, we have

$$|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i}\ \forall\ m|n\ ,\ 1 \le i \le a_m, \chi_n(f(x_{q^n+1})) = \pm 1\}|$$
$$= \frac{q-1}{2}\ |\{g \in \mathcal{F}_{2g+2} : \varepsilon_{q^n+1}\ \chi_n(g(x_{m,i})) = \varepsilon_{m,i}\ \forall\ m|n\ ,\ 1 \le i \le a_m\}|. \tag{6.4}$$

Using Proposition 5.1 and Lemma 4.3, we get that (6.4) is equal to

$$\left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}\right)^{q-r_1} \prod_{\substack{m|n\\ m\neq 1}} \left(\frac{q^m-1}{2}\right)^{a_m-r_m} \left[(1-q^{-1})q^{2g+2-q^n} \prod_{m|n} \frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}}\right.$$
$$\left. + \mathcal{O}\left(q^{\frac{1}{2}(2g+2+\sum_{m|n} mr_m)}\right)\right]$$
$$= 2^{-(1+q-r_1+\sum_{\substack{m|n\\ m\neq 1}} a_m-r_m)}\, q^{1-r_1+q^n-\sum_{\substack{m|n\\ m\neq 1}} mr_m} (1-q^{-1})^{1+q-r_1} \prod_{\substack{m|n\\ m\neq 1}} (1-q^{-m})^{a_m-r_m}$$
$$\times \left[(1-q^{-1})q^{2g+2-q^n} \prod_{m|n} \frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{\frac{1}{2}(2g+2+\sum_{m|n} mr_m)}\right)\right]$$
$$= 2^{-(1+q-r_1+\sum_{\substack{m|n\\ m\neq 1}} a_m-r_m)}\, q^{2g+3-\sum_{m|n} mr_m} \frac{(1-q^{-1})^2}{(1+q^{-1})^q} \prod_{\substack{m|n\\ m\neq 1}} \frac{1}{(1+q^{-m})^{a_m}}$$
$$+ \mathcal{O}\left(q^{g+2+q^n-\frac{1}{2}\sum_{m|n} mr_m}\right). \tag{6.5}$$

Dividing both (6.3) and (6.5) by

$$|\widehat{\mathcal{F}}_{2g+1}| + |\widehat{\mathcal{F}}_{2g+2}| = q^{2g+3}(1-q^{-1})(1-q^{-2}), \tag{6.6}$$

since $|\widehat{\mathcal{F}}_d| = (q-1)|\mathcal{F}_d|$ and using Lemma 2.1 for any $d \geq 2$, we get that the probability that χ_n takes the values $\varepsilon_{m,1}, \ldots, \varepsilon_{m,a_m}, \varepsilon_{q^n+1}$ for all $m|n$ as f ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$ is

$$\begin{aligned}&\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \leq i \leq a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \\ &= 2^{-(1+\sum_{m|n} a_m - r_m)} q^{-\sum_{m|n} m r_m} \frac{1}{(1+q^{-1})^{q+1}} \prod_{\substack{m|n \\ m\neq 1}} \frac{1}{(1+q^{-m})^{a_m}} + \mathcal{O}\left(q^{-g-1+q^n-\frac{1}{2}\sum_{m|n} m r_m}\right).\end{aligned} \tag{6.7}$$

Now, let $\{X_{m,i}\}_{\substack{m|n \\ 1\leq i\leq a_m}} \cup \{X_{q^n+1}\}$ be $\sum_{m|n} a_m + 1$ independent random variables taking the values

$$X_{m,i} = \begin{cases} 1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \\ 0 & \text{with probability } \dfrac{1}{q^m+1} \\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)} \end{cases},$$

and

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

Then the probability that $X_{m,i} = \varepsilon_{m,i}, X_{q^n+1} = \varepsilon_{q^n+1}$ for any $\varepsilon_{m,i}, \varepsilon_{q^n+1} \in \{-1,0,1\}$ for all $m|n$ and $1 \leq i \leq a_m$ is equal to

$$\begin{aligned}&\text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \leq i \leq a_m, X_{q^n+1} = \varepsilon_{q^n+1}\right) \\ &\quad = \prod_{m|n} \prod_{i=1}^{a_m} \text{Prob}\left(X_{m,i} = \varepsilon_{m,i}\right) \times \text{Prob}\left(X_{q^n+1} = \varepsilon_{q^n+1}\right) \\ &\quad = \left(\frac{1}{q+1}\right)^{r_1} \left(\frac{q}{2(q+1)}\right)^{q+1-r_1} \prod_{\substack{m|n \\ m\neq 1}} \left(\frac{1}{q^m+1}\right)^{r_m} \left(\frac{q^m}{2(q^m+1)}\right)^{a_m - r_m}\end{aligned}$$

$$= 2^{-(q+1-r_1+\sum_{\substack{m|n\\ m\neq 1}} a_m - r_m)} \; q^{1-r_1+q^n-\sum_{\substack{m|n\\ m\neq 1}} mr_m} \frac{1}{(q+1)^{q+1}} \prod_{\substack{m|n\\ m\neq 1}} \frac{1}{(q^m+1)^{a_m}}$$

$$= 2^{-(q+1-r_1+\sum_{\substack{m|n\\ m\neq 1}} a_m - r_m)} \; q^{-\sum_{m|n} mr_m} \frac{1}{(1+q^{-1})^{q+1}} \prod_{\substack{m|n\\ m\neq 1}} \frac{1}{(1+q^{-m})^{a_m}},$$

which is equal to the main term in (6.7). Then we have that

$$\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall \ m|n \ , \ 1 \leq i \leq a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|}$$

$$= \text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{for all } m|n \text{ and } 1 \leq i \leq a_m, X_{q^n+1} = \varepsilon_{q^n+1}\right) + \mathcal{O}\left(q^{-g-1+q^n-\frac{1}{2}\sum_{m|n} mr_m}\right). \tag{6.8}$$

6.2 n Even

As we did in the case of n odd, we will investigate two cases depending on the possible values of ε_{q^n+1}. Since n is even, $\varepsilon_{q^n+1} = \chi_n(f(x_{q^n+1}))$ will only take the values $0, 1$, as all the elements of $\mathbb{F}_q^\times$ are squares in $\mathbb{F}_{q^n}^\times$, hence the leading coefficient of f is always a square.

i. $\boldsymbol{\varepsilon_{q^n+1} = 0}$:

In this case the number of zeros among $\varepsilon_{m,1}, \ldots, \varepsilon_{m,a_m}$ for all $m|n$ is $r-1$, and only the polynomials in $\widehat{\mathcal{F}}_{2g+1}$ will contribute. Taking into account that since n is even, the number of quadratic residues in each subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ rely on the parity of $\frac{n}{m}$, as proven in Lemma 4.3. Using the same notation of Lemma 4.3, If $2|\frac{n}{m}$, then all the elements of $\mathbb{F}_{q^m}^\times$ are quadratic residues in $\mathbb{F}_{q^n}$. Otherwise, if $2 \nmid \frac{n}{m}$ then there are $\dfrac{q^m-1}{2}$ quadratic residues, and the same number of quadratic non-residues, in $\mathbb{F}_{q^m}$. Using Proposition 5.1, we get that

$$|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall \ m|n \ , \ 1 \leq i \leq a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|$$

$$= |\{f \in \widehat{\mathcal{F}}_{2g+1} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall \ m|n \ , \ 1 \leq i \leq a_m\}|,$$

$$
\begin{aligned}
&= (q-1)(q-1)^{q-(r_1-1)} \prod_{\substack{m|n \\ m\neq 1 \\ 2|\frac{n}{m}}} (q^m-1)^{a_m-r_m} \prod_{\substack{m|n \\ 2\nmid\frac{n}{m}}} \left(\frac{q^m-1}{2}\right)^{a_m-r_m} \\
&\left[(1-q^{-1})q^{2g+1-q^n}\frac{(1-q^{-1})^{r_1-1}}{(1-q^{-2})^q}\prod_{\substack{m|n \\ m\neq 1}}\frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{\frac{1}{2}(2g+\sum_{m|n} mr_m)}\right)\right] \\
&= 2^{-(\sum_{\substack{m|n \\ 2\nmid\frac{n}{m}}} a_m-r_m)} q^{2+q^n-\sum_{m|n} mr_m}(1-q^{-1})^{1+q-(r_1-1)} \prod_{\substack{m|n \\ m\neq 1}} (1-q^{-m})^{a_m-r_m} \\
&\left[q^{2g+1-q^n}\frac{(1-q^{-1})^{r_1}}{(1-q^{-2})^q}\prod_{\substack{m|n \\ m\neq 1}}\frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}} + \mathcal{O}\left(q^{\frac{1}{2}(2g+\sum_{m|n} mr_m)}\right)\right] \\
&= 2^{-(\sum_{\substack{m|n \\ 2\nmid\frac{n}{m}}} a_m-r_m)} q^{2g+3-\sum_{m|n} mr_m}\frac{(1-q^{-1})^{q+2}}{(1-q^{-2})^q}\prod_{\substack{m|n \\ m\neq 1}}\frac{(1-q^{-m})^{a_m}}{(1-q^{-2m})^{a_m}} \\
&+ \mathcal{O}\left(q^{g+2+q^n-\frac{1}{2}\sum_{m|n} mr_m}\right).
\end{aligned} \tag{6.9}
$$

ii. $\boldsymbol{\varepsilon_{q^n+1}=1}$:

Since $\varepsilon_{q^n+1}=1$, there are r zeros in between $\varepsilon_{m,1},\ldots,\varepsilon_{m,a_m}$ for all $m|n$, and in this case we will consider only polynomials in $\widehat{\mathcal{F}}_{2g+2}$. As n is even, all the elements of $\mathbb{F}_q^\times$ are possible leading coefficients of $f\in\widehat{\mathcal{F}}_{2g+2}$ such that $\chi_n(f(x_{q^n+1}))=1$, thus

$$
\begin{aligned}
&|\{f\in\widehat{\mathcal{F}}_{2g+1}\cup\widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i}))=\varepsilon_{m,i}\ \forall\ m|n\ ,\ 1\le i\le a_m, \chi_n(f(x_{q^n+1}))=\varepsilon_{q^n+1}\}| \\
&= |\{f\in\widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i}))=\varepsilon_{m,i}\ \forall\ m|n\ ,\ 1\le i\le a_m\}| \\
&= q-1|\{g\in\mathcal{F}_{2g+2} : \varepsilon_{q^n+1}\ \chi_n(g(x_{m,i}))=\varepsilon_{m,i}\ \forall\ m|n\ ,\ 1\le i\le a_m\}|.
\end{aligned} \tag{6.10}
$$

Using Proposition 5.1 and Lemma 4.3, we get that (6.10) is equal to

$$\begin{aligned}
&(q-1)(q-1)^{q-r_1}\prod_{\substack{m|n\\ m\neq 1\\ 2|\frac{n}{m}}}(q^m-1)^{a_m-r_m}\prod_{\substack{m|n\\ 2\nmid\frac{n}{m}}}\left(\frac{q^m-1}{2}\right)^{a_m-r_m}\\
&\times\left[(1-q^{-1})q^{2g+2-q^n}\frac{(1-q^{-1})^{r_1}}{(1-q^{-2})^q}\prod_{\substack{m|n\\ m\neq 1}}\frac{(1-q^{-m})^{r_m}}{(1-q^{-2m})^{a_m}}+\mathcal{O}\left(q^{\frac{1}{2}(2g+2+\sum_{m|n}mr_m)}\right)\right]\\
&=2^{-(\sum_{m|n}a_m-r_m)}_{2\nmid\frac{n}{m}}q^{2g+3-\sum_{m|n}mr_m}\frac{(1-q^{-1})^{2+q}}{(1-q^{-2})^q}\prod_{\substack{m|n\\ m\neq 1}}\frac{(1-q^{-m})^{a_m}}{(1-q^{-2m})^{a_m}}\\
&+\mathcal{O}\left(q^{g+2+q^n-\frac{1}{2}\sum_{m|n}mr_m}\right).
\end{aligned}\tag{6.11}$$

Since $|\widehat{\mathcal{F}}_{2g+1}|+|\widehat{\mathcal{F}}_{2g+2}|=q^{2g+3}(1-q^{-1})(1-q^{-2})$, we conclude from (6.9) and (6.11) that the probability of χ_n to take the values $\varepsilon_{m,1},\dots,\varepsilon_{m,a_m}$ for all $m|n$ as f ranges over $\widehat{\mathcal{F}}_{2g+1}\cup\widehat{\mathcal{F}}_{2g+2}$ is

$$\begin{aligned}
&\frac{|\{f\in\widehat{\mathcal{F}}_{2g+1}\cup\widehat{\mathcal{F}}_{2g+2}:\chi_n(f(x_{m,i}))=\varepsilon_{m,i}\ \forall\ m|n\ ,\ 1\le i\le a_m,\chi_n(f(x_{q^n+1}))=\varepsilon_{q^n+1}\}|}{|\widehat{\mathcal{F}}_{2g+1}\cup\widehat{\mathcal{F}}_{2g+2}|}\\
&=2^{-\sum_{m|n}a_m-r_m}_{2\nmid\frac{n}{m}}q^{-\sum_{m|n}mr_m}\frac{1}{(1+q^{-1})^{q+1}}\prod_{\substack{m|n\\ m\neq 1}}\frac{1}{(1+q^{-m})^{a_m}}+\mathcal{O}\left(q^{-g-1+q^n-\frac{1}{2}\sum_{m|n}mr_m}\right)
\end{aligned}\tag{6.12}$$

Now, let $\{X_{m,i}\}_{\substack{m|n\\ 1\le i\le a_m}}\cup\{X_{q^n+1}\}$ be $\sum_{m|n}a_m+1$ independent random variables taking different values depending on the parity of $\frac{n}{m}$, so when $2\nmid\frac{n}{m}$ we have

$$X_{m,i}=\begin{cases}1 & \text{with probability } \dfrac{q^m}{2(q^m+1)}\\ 0 & \text{with probability } \dfrac{1}{q^m+1}\\ -1 & \text{with probability } \dfrac{q^m}{2(q^m+1)}\end{cases},$$

and when $2|\frac{n}{m}$ we have

$$X_{m,i}=\begin{cases}0 & \text{with probability } \dfrac{1}{q^m+1}\\ 1 & \text{with probability } \dfrac{q^m}{q^m+1}\end{cases},$$

and

$$X_{q^n+1} = \begin{cases} 1 & \text{with probability } \dfrac{q}{q^+1} \\ 0 & \text{with probability } \dfrac{1}{q+1} \end{cases}.$$

Then,

$$\begin{aligned}
&\text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \le i \le a_m, X_{q^n+1} = \varepsilon_{q^n+1}\right) \\
&\quad = \prod_{m|n} \prod_{i=1}^{a_m} \text{Prob}\left(X_{m,i} = \varepsilon_{m,i}\right) \times \text{Prob}\left(X_{q^n+1} = \varepsilon_{q^n+1}\right) \\
&\quad = \left(\frac{1}{q+1}\right)^{r_1} \left(\frac{q}{q+1}\right)^{q+1-r_1} \prod_{\substack{m|n \\ m\neq 1 \\ 2\nmid \frac{n}{m}}} \left(\frac{1}{q^m+1}\right)^{r_m} \left(\frac{q^m}{q^m+1}\right)^{a_m-r_m} \prod_{\substack{m|n \\ 2\nmid \frac{n}{m}}} \left(\frac{1}{q^m+1}\right)^{r_m} \left(\frac{q^m}{2(q^m+1)}\right)^{a_m-r_m} \\
&\quad = 2^{-\left(\sum_{\substack{m|n \\ 2\nmid \frac{n}{m}}} a_m - r_m\right)} q^{-\sum_{m|n} m r_m} \frac{1}{(1+q^{-1})^{q+1}} \prod_{\substack{m|n \\ m\neq 1}} \frac{1}{(1+q^{-m})^{a_m}}, \qquad (6.13)
\end{aligned}$$

which is equal to the main term of (6.12). As a result, we have that

$$\begin{aligned}
&\frac{\left|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}\right|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \\
&= \text{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \le i \le a_m, X_{q^n+1} = \varepsilon_{q^n+1}\right) + \mathcal{O}\left(q^{-g-1+q^n-\frac{1}{2}\sum_{m|n} m r_m}\right). \qquad (6.14)
\end{aligned}$$

6.3 Main Result

After studying each case of n, we see that the distribution of $S(f)$ as f ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, behaves as the sum of q^n+1 independent random variables, where their possible values depend on the parity of n.

In more detail, let $s \in \mathbb{Z}$ such that $|s| \le q^n+1$, then with the results we obtained in (6.8) and

(6.14), we see that

$$\begin{aligned}
&\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \\
&= \sum_{\sum_{m|n} m \sum_{i=1}^{a_m} \varepsilon_{m,i} + \varepsilon_{q^n+1} = s} \frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \\
&= \sum_{\sum_{m|n} m \sum_{i=1}^{a_m} \varepsilon_{m,i} + \varepsilon_{q^n+1} = s} \Big[\mathrm{Prob}\left(X_{m,i} = \varepsilon_{m,i} \text{ for all } m|n \text{ and } 1 \le i \le a_m, X_{q^n+1} = \varepsilon_{q^n+1}\right) \\
&+ \mathcal{O}\left(q^{-g-1+q^n-\frac{1}{2}\sum_{m|n} m r_m}\right)\Big] \\
&= \mathrm{Prob}\left(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} + X_{q^n+1} = s\right) + \mathcal{O}\left(q^{-g+2q^n}\right).
\end{aligned}$$

We can summaries all of the previous cases and results in the following theorem, which is basically a generalization of Bucur, David, Feigon, and Lalin [2] results to any finite extension of $\mathbb{F}_q$. Using the notation we defined earlier we have

Theorem 6.1. *For $g \ge 1$ and $s \in \mathbb{Z}$ with $|s| \le q^n + 1$, we have*

$$\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \mathcal{S}(f) = s\}|}{| \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} = Prob(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} + X_{q^n+1} = s) + \mathcal{O}(q^{-g+2q^n}).$$

More precisely, for all $m|n$ let $x_{m,1}, x_{m,2}, \dots, x_{m,a_m} \in \mathbb{F}_{q^m} \setminus \bigcup_{\substack{k|m \\ k \ne m}} \mathbb{F}_{q^k}$ be distinct non-Galois conjugates over $\mathbb{F}_q$ and x_{q^n+1} denote the point at infinity, and let $\varepsilon_{m,i}, \varepsilon_{q^n+1} \in \{-1, 0, 1\}$ such that $1 \le i \le a_m$, then

$$\begin{aligned}
&\frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_n(f(x_{m,i})) = \varepsilon_{m,i} \ \forall\ m|n\ ,\ 1 \le i \le a_m, \chi_n(f(x_{q^n+1})) = \varepsilon_{q^n+1}\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \\
&= \left(\frac{q}{2^{\lambda_{n,1}}(q+1)}\right)^{q+1-r_1} \prod_{\substack{m|n \\ m \ne 1}} \left(\frac{q^m}{2^{\lambda_{n,m}}(q^m+1)}\right)^{a_m - r_m} \prod_{m|n} \left(\frac{1}{q^m+1}\right)^{r_m} + \mathcal{O}\left(q^{\,q^n - g - 1 - \frac{1}{2}\sum_{m|n} m r_m}\right),
\end{aligned}$$

where

$$r_m = \begin{cases} |\{i \in \{1, \dots, a_m\} : \varepsilon_{m,i} = 0\}| & m \ne 1 \\ |\{i \in \{1, \dots, a_m\} : \varepsilon_{m,i} = 0\}| & m = 1, \varepsilon_{q^n+1} \ne 0 \\ |\{i \in \{1, \dots, a_m\} : \varepsilon_{m,i} = 0\}| + 1 & m = 1, \varepsilon_{q^n+1} = 0, \end{cases}$$

and

$$\lambda_{n,m} = \begin{cases} 1 & n \text{ odd} \\ 1 & n \text{ even and } 2 \nmid \frac{n}{m} \\ 0 & n \text{ even and } 2 | \frac{n}{m}. \end{cases}$$

As an application of Theorem 6.1, we can find the average number of $\mathbb{F}_{q^n}$-point for any $n \geq 1$ on hyperelliptic curves over $\mathbb{F}_q$ of genus g as $g \to \infty$, denoted by $< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g}$ where $\mathcal{H}_g = \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$.

Corollary 6.1. *For $n \geq 1$, we have that*

$$< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} \sim \begin{cases} q^n + 1 & n \text{ odd} \\ q^n + q^{n/2} + 1 - \sum\limits_{\substack{m | \frac{n}{2} \\ m \neq 1}} \dfrac{m a_m}{q^m + 1} & n \text{ even}, \end{cases}$$

as $g \to \infty$.

Proof. We can write the average as

$$\begin{aligned} < \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} &= q^n + 1 + \frac{1}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|} \sum_{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}} S(f) \\ &= q^n + 1 + \sum_{s=-(q^n+1)}^{q^n+1} s \, \frac{|\{f \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : S(f) = s\}|}{|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}|}. \end{aligned}$$

Using Theorem 6.1, we get

$$\begin{aligned} < \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} &= q^n + 1 + \sum_{s=-(q^n+1)}^{q^n+1} s \left[Prob(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} + X_{q^n+1} = s) + \mathcal{O}(q^{-g+2q^n}) \right] \\ &= q^n + 1 + E\left(\sum_{m|n} m \sum_{i=1}^{a_m} X_{m,i} + X_{q^n+1} \right) + \mathcal{O}(q^{-g+2q^n+2n}) \\ &= q^n + 1 + \sum_{m|n} m \sum_{i=1}^{a_m} E(X_{m,i}) + E(X_{q^n+1}) + \mathcal{O}(q^{-g+2q^n+2n}), \end{aligned}$$

as the expected value is linear.

Depending on the parity of n, we will have two cases :

i ***n odd***: for all $m|n$ and $1 \leq i \leq a_m$ we have $E(X_{m,i}) = 0$ and $E(X_{q^n+1}) = 0$

ii ***n even***: for all $m|n$ and $1 \leq i \leq a_m$ we have

$$E(X_{m,i}) = \begin{cases} 0 & 2 \nmid \frac{n}{m} \\ \dfrac{q^m}{q^m+1} & 2|\frac{n}{m}, \end{cases}$$

and $E(X_{q^n+1}) = \dfrac{q}{q+1}$.

Then, as a result when n is odd and $g \to \infty$ we get

$$< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} \sim q^n + 1.$$

On the other hand, when n is even we have

$$\begin{aligned} < \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{H}_g} &= q^n + 1 + \sum_{\substack{m|n \\ 2|\frac{n}{m}}} m a_m \frac{q^m}{q^m+1} + \frac{q}{q+1} + \mathcal{O}(q^{-g+2q^n+2n}) \\ &= q^n + q + 1 + \sum_{\substack{m|\frac{n}{2} \\ m \neq 1}} m a_m \frac{q^m}{q^m+1} + \mathcal{O}(q^{g+2q^n+2n}) \\ &= q^n + q + 1 + \sum_{\substack{m|\frac{n}{2} \\ m \neq 1}} m a_m - \sum_{\substack{m|n/2 \\ m \neq 1}} \frac{m a_m}{q^m+1} + \mathcal{O}(q^{g+2q^n+2n}), \end{aligned}$$

since $\sum_{\substack{m|\frac{n}{2} \\ m \neq 1}} m a_m = q^{n/2} - q$, we get our result when $g \to \infty$. □

As we mentioned in the introduction, the average number of points we get is different than the result obtained by Rudnick in [3], since he consider only the set of curves

$$C_f : y^2 = f(x),$$

where $f \in \mathcal{F}_{2g+1}$ (square free monic of degree $2g+1$). As $g \to \infty$, Rudnick[3] obtains the following

$$< \#C_f(\mathbb{F}_{q^n}) >_{f \in \mathcal{F}_{2g+1}} \sim \begin{cases} q^n + 1 & n \text{ odd} \\ q^n + q^{n/2} + 1 - \sum\limits_{m|\frac{n}{2}} \dfrac{m\, a_m}{q^m+1} & n \text{ even.} \end{cases}$$

Bibliography

[1] Kurlberg, P., & Rudnick, Z. (2009). The fluctuations in the number of points on a hyperelliptic curve over a finite field. Journal Of Number Theory, 129(3), 580-587. doi:10.1016/j.jnt.2008.09.004.

[2] Bucur, A., David, C., Feigon, B., & Lalin, M. (2009). Statistics for Traces of Cyclic Trigonal Curves over Finite Fields. *International Mathematics Research Notices*. doi:10.1093/imrn/rnp162.

[3] Rudnick, Z. (2010). Traces of high powers of the Frobenius class in the hyperelliptic ensemble. *Acta Arith.*, 143(1), 81-99. doi:10.4064/aa143-1-5.

[4] Chinis, I. (2015). Traces of high powers of the Frobenius for the moduli space of hyperelliptic curves.

[5] Dummit, D., & Foote, R. (2004). *Abstract algebra*. New Jersey: Wiley.

[6] Rosen, M. (2002). *Number theory in function fields*. New York: Springer.

[7] Silverman, J. (2009). *The Arithmetic of Elliptic Curves* (2nd ed.). New York: Springer-Verlag.