HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS AND THEIR RELATIONS TO ALGEBRAIC CURVES

A Dissertation

by

MARIA VALENTINA VEGA VEGLIO

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2009

Major Subject: Mathematics

HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS AND THEIR RELATIONS TO ALGEBRAIC CURVES

A Dissertation

by

MARIA VALENTINA VEGA VEGLIO

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Matthew Papanikolas
Committee Members,	Daren Cline
	Paula Tretkoff
	Matthew Young
Head of Department,	Albert Boggess

May 2009

Major Subject: Mathematics

ABSTRACT

Hypergeometric Functions over Finite Fields and Their Relations to Algebraic Curves. (May 2009)

María Valentina Vega Veglio, B.S., Universidad de la República, Uruguay;

M.S., Texas A&M University

Chair of Advisory Committee: Dr. Matthew Papanikolas

Classical hypergeometric functions and their relations to counting points on curves over finite fields have been investigated by mathematicians since the beginnings of 1900. In the mid 1980s, John Greene developed the theory of hypergeometric functions over finite fields. He explored the properties of these functions and found that they satisfy many summation and transformation formulas analogous to those satisfied by the classical functions. These similarities generated interest in finding connections that hypergeometric functions over finite fields may have with other objects. In recent years, connections between these functions and elliptic curves and other Calabi-Yau varieties have been investigated by mathematicians such as Ahlgren, Frechette, Fuselier, Koike, Ono and Papanikolas. A survey of these results is given at the beginning of this dissertation. We then introduce hypergeometric functions over finite fields and some of their properties. Next, we focus our attention on a particular family of curves and give an explicit relationship between the number of points on this family over $\mathbb{F}_q$ and sums of values of certain hypergeometric functions over $\mathbb{F}_q$. Moreover, we show that these hypergeometric functions can be explicitly related to the roots of the zeta function of the curve over $\mathbb{F}_q$ in some particular cases. Based on numerical computations, we are able to state a conjecture relating these values in a more general setting, and advances toward the proof of this result are shown in

the last chapter of this dissertation. We finish by giving various avenues for future study.

To Gabriel H. Tucci

ACKNOWLEDGMENTS

There are a number of people whom I would like to thank for having contributed to this dissertation in some way or another.

First and foremost, I would like to thank my advisor Dr. Matthew Papanikolas. Thank you for having provided me with interesting problems to work on and for letting me benefit from your mathematical knowledge and intuition. I am proud to be one of your students.

Thanks also to the other members of my advisory committee, Dr. Daren Cline, Dr. Paula Tretkoff and Dr. Matthew Young, for your time, comments, advice and support.

I would also like to thank the numerous friends and colleagues who, over the years, have inspired, encouraged and guided me. Special thanks goes to Andrea Jedwab, Laura Llobet, Gabriela Pérez, Gimena Rossello and Ana Salvarrey.

Many thanks to the mathematics department at Texas A&M, the administrative staff in particular for all their help.

To my parents Daniel and Gladys and my brother Daniel, I am constantly grateful for your love and support, whether near or far.

And finally, Gabriel, your unabashed love of the art of mathematics is such an inspiration to me. Words cannot express how much your love, support, patience, and comfort through the many ups and downs of graduate school have meant to me. Without your constant support, I truly never would have made it to this day. Gracias!

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

A. General Introduction

Called "the queen of mathematics" by the legendary mathematician Carl Friedrich Gauss, number theory is one of the oldest and largest branches of pure mathematics. It encompasses topics from the study of integers to number fields to solutions of Diophantine equations. In the past few decades, research in number theory has progressed at a rapid rate on many fronts. Recently, important new results have arisen from analytic, geometric, and p-adic methods. These advances had been used to bring about breakthroughs, solve longstanding problems, and inspire questions.

In this dissertation we explore connections between values of hypergeometric functions over finite fields and algebraic curves. In the remainder of this chapter we give an introduction to the problems we are working on together with a brief survey of recent results connecting the previous objects. The second chapter has the purpose of introducing the necessary background material. In particular, in Chapter II Section B we define hypergeometric functions over finite fields and state some of their properties. In Chapter III we introduce a particular family of algebraic curves and study connections that these curves have to hypergeometric functions over $\mathbb{F}_q$. More specifically, in Theorem A.2 we present an explicit relationship between the number of points on these curves over $\mathbb{F}_q$ and values of certain hypergeometric functions over $\mathbb{F}_q$. In Chapter IV we focus on the particular hypergeometric functions that appear in Theorem A.2 and present, in Section B, a conjecture relating values of

---

The journal model is *IEEE Transactions on Automatic Control.*

each one of these hypergeometric functions over $\mathbb{F}_q$ with the roots of the zeta function associated to the curve over $\mathbb{F}_q$. In the remainder of Chapter IV we give proofs of the conjecture in some particular cases and progress toward the proof of the conjecture in the general case is shown in Chapter V. Finally, in Chapter VI, we summarize our work and provide avenues for future study.

The problem of finding the number of solutions over a finite field of a polynomial equation has been of interest to mathematicians for many years. A typical result in this direction is the *Hasse-Weil bound*, which states that a smooth projective curve of genus g defined over a finite field with q elements has between $q+1-2g\sqrt{q}$ and $q+1+2g\sqrt{q}$ points. A natural question to ask is whether there are simple formulas for counting points in terms of interesting mathematical objects.

Classical hypergeometric functions and their relations to counting points on curves over finite fields have been investigated by mathematicians since the beginnings of 1900. Recall that for $a_1, \ldots, a_r, b_1, \ldots, b_s, x \in \mathbb{C}$, the classical hypergeometric series is defined by

$$ {}_rF_s\left(\left.\begin{matrix} a_1, & a_2, & \ldots, & a_r \\ b_1, & b_2, & \ldots, & b_s \end{matrix}\right| x\right) := \sum_{k=0}^{\infty} \frac{(a_1)_k (a_2)_k \cdots (a_r)_k}{(b_1)_k (b_2)_k \cdots (b_s)_k} \frac{x^k}{k!} \tag{1.1} $$

where $(a)_k := a(a+1)\cdots(a+k-1)$ is the Pochhammer symbol.

Many connections between classical hypergeometric series, elliptic curves and modular forms have been discovered. For example, if we consider the Legendre family of elliptic curves given by $y^2 = x(x-1)(x-t)$, $t \neq 0, 1$, and denote

$$ {}_2F_1[a, b; c|t] := {}_2F_1\left(\left.\begin{matrix} a, & b \\ & c \end{matrix}\right| t\right), $$

the specialization ${}_2F_1[\frac{1}{2}, \frac{1}{2}; 1|t]$ is a multiple of an elliptic integral which represents a period of the lattice associated to the previous family, as Kummer showed. For another examples, Beukers [4] related a period of $y^2 = x^3 - x - t$ to the values ${}_2F_1[\frac{1}{12}, \frac{5}{12}; \frac{1}{2}|\frac{27}{4}t^2]$.

In the 1980's, J. Greene [11, 12] initiated a study of finite field hypergeometric functions. Let p be an odd prime, and let $\widehat{\mathbb{F}_p^\times}$ denote the group of multiplicative characters χ on $\mathbb{F}_p^\times$, extended to all of $\mathbb{F}_p$ by setting $\chi(0) = 0$. If $A, B \in \widehat{\mathbb{F}_p^\times}$ and J denotes the Jacobi sum, then define $\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B})$. Greene defined *hypergeometric functions over* $\mathbb{F}_p$, for $A_0, A_1, \ldots, A_n, B_1, B_2, \ldots, B_n \in \widehat{\mathbb{F}_p^\times}$ and $x \in \mathbb{F}_p$ by

$$ {}_{n+1}F_n\left(\left.\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\right| x\right) := \frac{p}{p-1} \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x), $$

where n is a positive integer. (See Chapter II, Section B for more details.)

Greene explored the properties of these functions and found that they satisfy many summation and transformation formulas analogous to those satisfied by the classical functions. For example, classical hypergeometric series have the following inductive integral representation [2]

$$ {}_{n+1}F_1\left(\left.\begin{matrix} a_0, & a_1, & \ldots, & a_n \\ & b_1, & \ldots, & b_n \end{matrix}\right| x\right) = \frac{\Gamma(b_n)}{\Gamma(a_n)\Gamma(b_n - a_n)} \int_0^1 {}_nF_{n-1}\left(\left.\begin{matrix} a_0, & a_1, & \ldots, & a_{n-1} \\ & b_1, & \ldots, & b_{n-1} \end{matrix}\right| tx\right) \cdot t^{a_n}(1-t)^{b_n - a_n} \frac{dt}{t(1-t)}. $$

where $\Gamma(x)$ denotes the Gamma function defined by

$$ \Gamma(x) = \int_0^\infty t^x e^{-t} \frac{dt}{t}. $$

The analogous to this result in the finite field case is

Theorem A.1 ([12] Theorem 3.13)**.** *For characters* $A_0, A_1, \ldots, A_n$, $B_1, \ldots, B_n$ *of* $\mathbb{F}_p^\times$ *and* $x \in \mathbb{F}_p$,

$$ {}_{n+1}F_n\left(\left.\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\right| x\right) = \frac{A_n B_n(-1)}{p} \sum_{y \in \mathbb{F}_p} {}_nF_{n-1}\left(\left.\begin{matrix} A_0, & A_1, & \ldots, & A_{n-1} \\ & B_1, & \ldots, & B_{n-1} \end{matrix}\right| xy\right) \cdot A_n(y)\overline{A_n}B_n(1-y). $$

These similarities generated interest in finding connections that hypergeometric functions over finite fields may have with other objects, for example elliptic curves. In recent years, many results have been proved in this direction and as expected, certain families of elliptic curves are closely related to particular hypergeometric functions over finite fields.

Consider the two families of elliptic curves over $\mathbb{F}_p$ defined by

$$ E_1(t) : y^2 = x(x-1)(x-t), \quad t \neq 0, 1 $$
$$ E_2(t) : y^2 = (x-1)(x^2+t), \quad t \neq 0, -1. $$

Then, define the traces of Frobenius on the above families by

$$ a_1(p,t) = p + 1 - \#E_1(t)(\mathbb{F}_p) $$
$$ a_2(p,t) = p + 1 - \#E_2(t)(\mathbb{F}_p) $$

where, for i=1,2

$$ \#E_i(t)(\mathbb{F}_p) := \#\{(x,y) \in E_i(t) : x, y \in \mathbb{F}_p\} \cup \{P\} $$

denotes the number of points the curve $E_i(t)$ has over the finite field $\mathbb{F}_p$, with $P = [0 : 1 : 0]$ being the point at infinity. Denote by ϕ and ε the quadratic and trivial characters on $\mathbb{F}_p^\times$ respectively, i.e., for $a \in \mathbb{F}_p^\times$

$$\phi(a) = \begin{cases} 1 & \text{if } x^2 = a \text{ is solvable in } \mathbb{F}_p \\ -1 & \text{if } x^2 = a \text{ is not solvable in } \mathbb{F}_p \end{cases}$$

is the Legendre symbol, and

$$\varepsilon(a) = 1.$$

Then, the families of elliptic curves defined above are closely related to particular hypergeometric functions over $\mathbb{F}_p$. For example, ${}_2F_1[\phi, \phi; \varepsilon|t]$ arises in the formula for Fourier coefficients of a modular form associated to $E_1(t)$ [15, 20]. Further, Koike and Ono, respectively, gave the following explicit relationships:

Theorem A.2 ((1) Koike [15], (2) Ono [20])**.** *Let p be an odd prime. Then*

1. *for $t \neq 0, 1$:*

$$p\,{}_2F_1\left(\left.\begin{matrix}\phi, & \phi \\ & \varepsilon\end{matrix}\right| t\right) = -\phi(-1)a_1(p,t)$$

2. *for $t \neq 0, -1$:*

$$p^2\,{}_3F_2\left(\left.\begin{matrix}\phi, & \phi, & \phi \\ & \varepsilon, & \varepsilon\end{matrix}\right| 1 + \frac{1}{t}\right) = \phi(-t)(a_2(p,t)^2 - p).$$

In addition, Frechette, Ono, and Papanikolas [8] gave relations between counting points on more general varieties over $\mathbb{F}_p$ and hypergeometric functions over finite fields. For p and odd prime and $k \geq 4$ even, define three sequences of varieties $\mathcal{U}_k$,

$\mathcal{V}_k$, and $\mathcal{W}_k$ by

$$\begin{aligned}
\mathcal{U}_k : y^2 &= \prod_{i=1}^{k-2}(x_i - 1)(x_i^2 + t), \\
\mathcal{V}_k : y^2 &= \prod_{i=1}^{k-2} x_i(x_i - 1)(x_i - t), \\
\mathcal{W}_k : y^2 &= \prod_{i=1}^{k-2} x_i(x_i - 1)(x_i - t^2).
\end{aligned}$$

Then, the number of points in $\mathcal{U}_k(\mathbb{F}_p)$, $\mathcal{V}_k(\mathbb{F}_p)$ and $\mathcal{W}_k(\mathbb{F}_p)$ are directly related to values of certain hypergeometric functions over $\mathbb{F}_p$. In fact, they are related to the number of points in $E_1(\mathbb{F}_p)$ and $E_2(\mathbb{F}_p)$ which, by Theorem A.2, are related to the hypergeometric functions. Specifically, they showed that:

$$\begin{aligned}
\#\mathcal{U}_k(\mathbb{F}_p) &= p^{k-1} + 2 + \sum_{t=1}^{p-2} a_2(p,t)^{k-2}, \\
\#\mathcal{V}_k(\mathbb{F}_p) &= p^{k-1} + 2 + \sum_{t=2}^{p-1} a_1(p,t)^{k-2}, \\
\#\mathcal{W}_k(\mathbb{F}_p) &= p^{k-1} + 3 + \sum_{t=2}^{p-1} (1 + \phi(t))\, a_1(p,t)^{k-2}.
\end{aligned}$$

Motivated by these types of results, we have explored more relations between hypergeometric functions over finite fields and counting points on varieties over finite fields.

CHAPTER II

PRELIMINARIES

A. Multiplicative Characters

Let p be a prime and let $\mathbb{F}_q$ be a finite field with q elements, with $q = p^r$ for some positive integer r. We will denote by $\mathbb{F}_q^\times$ the multiplicative group of $\mathbb{F}_q$, i.e., $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$. Recall that $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$. A *multiplicative character* on $\mathbb{F}_q^\times$ is a map $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ that satisfies $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_q^\times$, in other words, χ is a group homomorphism. It is often useful to extend the domain of definition of a multiplicative character χ to all $\mathbb{F}_q$, and we do this by defining $\chi(0) = 0$. Throughout, we let ε denote the trivial character defined by the relation $\varepsilon(a) = 1$ for all $a \in \mathbb{F}_q^\times$. Also, recall that the multiplicative characters on $\mathbb{F}_q^\times$ form a cyclic group of order $q-1$ which will be denoted by $\widehat{\mathbb{F}_q^\times}$. Now we state the *orthogonality relations* for multiplicative characters, of which we will make use in Chapter III. For proofs of these properties and more information on multiplicative characters see Chapter VIII of [13].

Lemma A.1. Let χ be a multiplicative character on $\mathbb{F}_q^\times$. Then

$$(a) \quad \sum_{x \in \mathbb{F}_q} \chi(x) = \begin{cases} q-1 & \text{if } \chi = \varepsilon \\ 0 & \text{if } \chi \neq \varepsilon \end{cases}$$

$$(b) \quad \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} \chi(x) = \begin{cases} q-1 & \text{if } x = 1 \\ 0 & \text{if } x \neq 1. \end{cases}$$

B. Hypergeometric Functions over $\mathbb{F}_q$

The theory of hypergeometric functions over finite fields was developed by Greene [12] in the 1980s. As above, let p be an odd prime and and let $\mathbb{F}_q$ denote the finite field with q elements where $q = p^r$ for some positive integer r.

Definition B.1 ([12] Defn. 2.4)**.** For $A,\ B \in \widehat{\mathbb{F}_q^\times}$, let $J(A,B)$ denote the Jacobi sum $J(A,B) = \sum_{x\in\mathbb{F}_q} A(x)B(1-x)$. Then define the binomial coefficient

$$\binom{A}{B} := \frac{B(-1)}{q} J(A,\overline{B}) = \frac{B(-1)}{q} \sum_{x\in\mathbb{F}_q} A(x)\overline{B}(1-x)$$

where $\overline{\chi}$ is defined by $\chi\overline{\chi} = \varepsilon$ for $\chi \in \widehat{\mathbb{F}_q^\times}$.

Greene defined *Gaussian hypergeometric functions over* $\mathbb{F}_q$ in the following way:

Definition B.2 ([12] Defn. 3.5)**.** For characters $A, B, C \in \widehat{\mathbb{F}_q^\times}$ and $x \in \mathbb{F}_q$

$$ {}_2F_1\left(\left.\begin{matrix} A, & B \\ & C \end{matrix}\right| x\right) := \varepsilon(x)\frac{BC(-1)}{q} \sum_{y\in\mathbb{F}_q} B(y)\overline{B}C(1-y)\overline{A}(1-xy). \tag{2.1}$$

More generally, Greene proved the following theorem which connects these functions to Jacobi sums, and extended the previous definition to a higher number of multiplicative characters.

Theorem B.3 ([12] Theorem 3.6)**.** *For characters* $A, B, C \in \widehat{\mathbb{F}_q^\times}$ *and* $x \in \mathbb{F}_q$*,*

$$ {}_2F_1\left(\left.\begin{matrix} A, & B \\ & C \end{matrix}\right| x\right) = \frac{q}{q-1} \sum_{\chi\in\widehat{\mathbb{F}_q^\times}} \binom{A\chi}{\chi}\binom{B\chi}{C\chi}\chi(x).$$

This leads to the following definition.

Definition B.4 ([12] Defn. 3.10)**.** Let n be a positive integer. For $x \in \mathbb{F}_q$ and characters $A_0, A_1, \ldots, A_n, B_1, B_2, \ldots, B_n \in \widehat{\mathbb{F}_q^\times}$, define the *hypergeometric function over* $\mathbb{F}_q$ by

$$ {}_{n+1}F_n\left(\left.\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\right| x\right) := \frac{q}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^\times}} \binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\cdots\binom{A_n\chi}{B_n\chi}\chi(x). $$

A comprehensive introduction to these functions can be found in Greene's paper [12], where he presented many properties and transformation identities they satisfy. One transformation that is of interest to us is presented in the next theorem, and it allows to replace the arguments $A, B \in \widehat{\mathbb{F}_q^\times}$ by $\overline{A}, \overline{B}$ respectively.

Theorem B.5 ([12] Theorem 4.4)**.** *If $A, B, C \in \widehat{\mathbb{F}_q^\times}$ and $x \in \mathbb{F}_q$, then*

$$ {}_2F_1\left(\left.\begin{matrix} A, & B \\ & C \end{matrix}\right| x\right) = C(-1)C\,\overline{AB}(1-x)\,{}_2F_1\left(\left.\begin{matrix} C\overline{A}, & C\overline{B} \\ & C \end{matrix}\right| x\right) + A(-1)\binom{B}{\overline{A}C}\delta(1-x) \tag{2.2} $$

where $\delta(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0. \end{cases}$

In particular, when A and B are inverses of each other and $C = \varepsilon$ we get the following result.

Corollary B.6. *Let $A \in \widehat{\mathbb{F}_q^\times}$ and $x \in \mathbb{F}_q\backslash\{1\}$. Then*

$$ {}_2F_1\left(\left.\begin{matrix} A, & \overline{A} \\ & \varepsilon \end{matrix}\right| x\right) = {}_2F_1\left(\left.\begin{matrix} \overline{A}, & A \\ & \varepsilon \end{matrix}\right| x\right) $$

Proof. Just notice that, since $x \neq 1$ then the last term in the right hand side of 2.2 vanishes, and $A\overline{A}(1-x) = 1$. □

C. The Zeta Function of a Variety

In this section we introduce the *Zeta function of a projective variety*, which is a generating function for the number of solutions of a set of polynomial equations defined over a finite field $\mathbb{F}_q$, in finite extension fields $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. In this way, we collect all the information about counting points into a single object.

Again, let p be an odd prime and and let $\mathbb{F}_q$ denote the finite field with q elements where $q = p^r$ for some positive integer r. Let $\mathcal{V}$ be a projective variety, so $\mathcal{V}$ is the zero-set

$$f_1(x_0, \ldots, x_N) = \cdots = f_m(x_0, \ldots, x_N) = 0$$

of a collection of homogeneous polynomials with coefficients in $\mathbb{F}_q$. Denote by $\mathcal{V}(\mathbb{F}_{q^n})$ the set of points of $\mathcal{V}$ with coordinates in $\mathbb{F}_{q^n}$, where $\mathbb{F}_{q^n}$ is the field extension of degree n of $\mathbb{F}_q$.

Definition C.1. The zeta function of $\mathcal{V}/\mathbb{F}_q$ is the power series

$$Z(\mathcal{V}/\mathbb{F}_q; T) := \exp\left(\sum_{n=1}^{\infty} \#\mathcal{V}(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

(Here if $F(T) \in \mathbb{Q}[[T]]$ is a power series with no constant term, then $\exp(F(T))$ is the power series $\sum_{i=0}^{\infty} F(T)^i/i!$). Thus, the zeta function $Z(\mathcal{V}/\mathbb{F}_q; T)$ associated to $\mathcal{V}$ contains all the information concerning the number of points of $\mathcal{V}$ over each field extension of $\mathbb{F}_q$ of finite degree. Notice that, once we know $Z(\mathcal{V}/\mathbb{F}_q; T)$, it is not hard to recover the numbers $\#\mathcal{V}(\mathbb{F}_{q^n})$ by the formula

$$\#\mathcal{V}(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(\mathcal{V}/\mathbb{F}_q; T)\Big|_{T=0}.$$

In 1949, André Weil [27] made a series of conjectures concerning the number of points on varieties defined over finite fields. In what follows, we state Weil's conjectures and

apply them to algebraic curves.

Theorem C.2. *(Weil Conjectures). Let $\mathbb{F}_q$ be the field with q elements and $\mathcal{V}/\mathbb{F}_q$ a smooth projective variety of dimension n.*

1. *Rationality*

$$Z(\mathcal{V}/\mathbb{F}_q; T) \in \mathbb{Q}(T).$$

2. *Functional equation: There is an integer ϵ (the Euler characteristic of $\mathcal{V}$) so that*

$$Z(\mathcal{V}/\mathbb{F}_q; 1/q^n T) = \pm\, q^{n\epsilon/2} T^{\epsilon} Z(\mathcal{V}/\mathbb{F}_q; T).$$

3. *Riemann Hypothesis: There is a factorization*

$$Z(\mathcal{V}/\mathbb{F}_q; T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$$

with each $P_i(T) \in \mathbb{Z}[T]$. Further, $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, and for $1 \le i \le 2n-1$, $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \quad \textit{with} \quad |\alpha_{ij}| = q^{i/2}.$$

The polynomial $P(T) := \prod_{i=1}^{n} P_{2i-1}(T)$ is called the L-polynomial of $\mathcal{V}$.

Weil proved these conjectures for curves and abelian varieties, and Dwork [7] in 1960 established the rationality of the zeta function in general. In 1973 Deligne [6] proved the Riemann hypothesis.

Applying these conjectures to a smooth projective curve $\mathcal{V}$ of genus g defined over $\mathbb{F}_q$, we obtain that

$$Z(\mathcal{V}/\mathbb{F}_q; T) = \frac{(1-\alpha_1 T)(1-\overline{\alpha_1} T)\cdots(1-\alpha_g T)(1-\overline{\alpha_g} T)}{(1-T)(1-qT)} \tag{2.3}$$

where $|\alpha_i| = \sqrt{q}$ for all $i = 1, \ldots, g$. Notice that in this case we have a beautiful formula for counting points on $\mathcal{V}$ over $\mathbb{F}_{q^n}$, namely

$$\#\mathcal{V}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{g} (\alpha_i^n + \overline{\alpha_i}^n) \tag{2.4}$$

We will make strong use of formulas (2.3) and (2.4) applied to a particular families of curves to prove the results in Chapter III and IV.

CHAPTER III

HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS AND ALGEBRAIC CURVES

A. Counting Points on Families of Curves over Finite Fields

We consider the problem of connecting the number of points that certain families of curves have over finite fields to values of particular hypergeometric functions over finite fields. Troughout, let $\mathbb{F}_q$ denote the finite field with q elements, where q is some prime power. We start with a result that allows to count the number of solutions of a particular equation by using multiplicative characters on $\mathbb{F}_q$.

Lemma A.1. Let q be a prime and $a \in \mathbb{F}_q \backslash \{0\}$. If $n|(q-1)$ then

$$\#\{x \in \mathbb{F}_q : x^n = a\} = \sum_{\chi^n = \varepsilon} \chi(a)$$

where the sum runs over all characters $\chi \in \widehat{\mathbb{F}_q^\times}$ of order dividing n.

Proof. We start by seeing that there are exactly n characters of order dividing n. Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a character such that $\chi^n = \varepsilon$ and let $g \in \mathbb{F}_q^\times$ be a generator. Since $\chi^n = \varepsilon$, the value of $\chi(g)$ must be an nth root of unity, hence there are at most n such characters. Consider $\chi \in \widehat{\mathbb{F}_q^\times}$ defined by $\chi(g) = e^{2\pi i/n}$ (i.e. $\chi(g^k) = e^{2\pi ik/n}$). It is easy to see that χ is a character and $\varepsilon, \chi, \chi^2, \cdots, \chi^{n-1}$ are n distinct characters of order dividing n. Therefore, there are exactly n characters of order dividing n.

Now let $a \neq 0$ and suppose that $x^n = a$ is solvable; i.e., there is an element $b \in \mathbb{F}_q$ such that $b^n = a$. Since $\chi^n = \varepsilon$ we have that $\chi(a) = \chi(b^n) = \chi(b)^n = 1$. Thus

$$\sum_{\chi^n = \varepsilon} \chi(a) = \sum_{\chi^n = \varepsilon} 1 = n$$

Also notice that in this case, $\#\{x \in \mathbb{F}_q : x^n = a\} = n$ because if $x^n = a \pmod q$ is solvable then there exist exactly $\gcd(n, \varphi(q))$ solutions, where φ denotes the Euler function. But since $\varphi(q) = q - 1$ and $n|(q-1)$ it follows that $\gcd(n, q-1) = n$ (for a proof of this result see [13] Proposition 4.2.1).

To finish the proof we need to consider the case when $x^n = a$ is not solvable, in which case $\#\{x \in \mathbb{F}_q : x^n = a\} = 0$. Call $T := \sum_{\chi^n = \varepsilon} \chi(a)$. Since $x^n = a$ is not solvable, there exist a character ρ such that $\rho^n = \varepsilon$ and $\rho(a) \neq 1$ (take $\rho(g) = e^{2\pi i/n}$ where $< g >= \mathbb{F}_q^\times$). Since the characters of order dividing n form a group, it follows that $\rho(a)T = T$. Then $(\rho(a) - 1)T = 0$ which implies that $T = 0$ since $\rho(a) \neq 1$. $\square$

Similar to the results given in Chapter I, the main theorem of this chapter provides an explicit relation between the number of points on certain family of curves over finite fields and values of particular hypergeometric functions.

Theorem A.2. *Let $a = m/n$ and $b = s/r$ be rational numbers such that $0 < a, b < 1$, and let $z \in \mathbb{F}_q$, $z \neq 0, 1$. Consider the smooth projective algebraic curve with affine equation given by*

$$\mathcal{C}_z^{(a,b)} : y^l = t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}$$

where $l := lcm(n, r)$. If $q \equiv 1 \pmod l$ then:

$$\#\mathcal{C}_z^{(a,b)}(\mathbb{F}_q) = q + 1 + q\sum_{i=1}^{l-1} \eta_q^{ilb}(-1)\, {}_2F_1\left(\begin{matrix} \eta_q^{il(1-a)}, & \eta_q^{il(1-b)} \\ & \varepsilon \end{matrix} \middle| z \right) \tag{3.1}$$

where $\eta_q \in \widehat{\mathbb{F}_q^\times}$ is a character of order l, and $\#\mathcal{C}_z^{(a,b)}(\mathbb{F}_q)$ denotes the number of points that the curve $\mathcal{C}_z^{(a,b)}$ has over $\mathbb{F}_q$.

Proof. To simplify the notation, we will denote the curve $\mathcal{C}_z^{(a,b)} = \mathcal{C}_z$. Since $\widehat{\mathbb{F}_q^\times}$ is a cyclic group of order $q-1$ and $l|(q-1)$ there exists a character $\eta_q \in \widehat{\mathbb{F}_q^\times}$ of order l.

Recall that $\mathcal{C}_z$ is a projective curve, so adding the point at infinity we have

$$\#\mathcal{C}_z(\mathbb{F}_q) = 1 + \sum_{t\in\mathbb{F}_q} \#\{y \in \mathbb{F}_q : y^l = t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}\}$$

Breaking the sum and applying Lemma A.1 we see that:

$$\begin{aligned}
\#\mathcal{C}_z(\mathbb{F}_q) &= 1 + \sum_{\substack{t\in\mathbb{F}_q \\ t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}\neq 0}} \#\{y \in \mathbb{F}_q : y^l = t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}\} \\
&\quad + \#\{t \in \mathbb{F}_q : t^{l(1-b)}(1-t)^{lb}(1-zt)^{la} = 0\} \\
&= 1 + \sum_{t\in\mathbb{F}_q}\sum_{i=0}^{l-1} \eta_q^i(t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}) \qquad \text{(Lemma A.1)} \\
&\quad + \#\{t \in \mathbb{F}_q : t^{l(1-b)}(1-t)^{lb}(1-zt)^{la} = 0\}.
\end{aligned}$$

Now, by separating the sum according to whether $i = 0$, and collecting the second and last terms into a single one we have

$$\begin{aligned}
\#\mathcal{C}_z(\mathbb{F}_q) &= 1 + \sum_{t\in\mathbb{F}_q} \varepsilon(t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}) + \sum_{t\in\mathbb{F}_q}\sum_{i=1}^{l-1} \eta_q^i(t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}) \\
&\quad + \#\{t \in \mathbb{F}_q : t^{l(1-b)}(1-t)^{lb}(1-zt)^{la} = 0\} \\
&= 1 + q + \sum_{t\in\mathbb{F}_q}\sum_{i=1}^{l-1} \eta_q^i(t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}) \\
&= 1 + q + \sum_{i=1}^{l-1}\sum_{t\in\mathbb{F}_q} \eta_q^{il(1-b)}(t)\,\eta_q^{ilb}(1-t)\,\eta_q^{la}(1-zt). \qquad (3.2)
\end{aligned}$$

The last equality follows from the multiplicativity of η_q and switching the order of summation.

On the other hand, by Definition B.2 in Chapter II, we have

$$q\,{}_2F_1\left(\begin{array}{cc} \eta^{il(1-a)}, & \eta^{il(1-b)} \\ & \varepsilon \end{array}\middle| z\right) = \varepsilon(z)\eta^{il(1-b)}(-1)\sum_{t\in\mathbb{F}_q}\eta^{il(1-b)}(t)\,\overline{\eta^{il(1-b)}}(1-t)\overline{\eta^{il(1-a)}}(1-zt)$$
$$= \varepsilon(z)\eta^{il(1-b)}(-1)\sum_{t\in\mathbb{F}_q}\eta^{il(1-b)}(t)\,\eta^{ilb}(1-t)\,\eta^{ila}(1-zt). \tag{3.3}$$

Since $z \neq 0$, combining (3.2) and (3.3) we get the desired result. □

In he proof of Theorem A.2 we applied Lemma A.1 which requires for q to be a prime number in a particular congruence class modulo l. However, Theorem A.2 is valid over any finite field extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ as we see in the next Corollary.

Corollary A.3. *With same notation as in Theorem A.2, we have that*

$$\#\mathcal{C}_z^{(a,b)}(\mathbb{F}_{q^k}) = q^k + 1 + q^k\sum_{i=1}^{l-1}\eta_{q^k}^{ilb}(-1)\,{}_2F_1\left(\begin{array}{cc} \eta_{q^k}^{il(1-a)}, & \eta_{q^k}^{il(1-b)} \\ & \varepsilon \end{array}\middle| z\right)$$

where $\eta_{q^k} \in \widehat{\mathbb{F}_{q^k}^{\times}}$ *is a character of order* l.

Proof. Again, denote the curve by $\mathcal{C}_z$. First notice that $\widehat{\mathbb{F}_{q^k}^{\times}}$ is a cyclic group of order $q^k - 1$. Then, if $l|(q-1)$ it also divides $q^k - 1$, hence there exists $\eta_{q^k} \in \widehat{\mathbb{F}_{q^k}^{\times}}$ of order l.

Next, we show that Lemma A.1 is also true over $\mathbb{F}_{q^k}$ for any positive integer k. The proof is almost identical. We only need to check that if $a \in \mathbb{F}_{q^k}^{\times}$ and $x^n = a$ is solvable, then $\#\{x \in \mathbb{F}_{q^k} : x^n = a\} = n$. For this recall the following two statements, one of which was already used in the proof of Lemma A.1 (for proofs of them see [13] Propositions 4.2.1 and 4.2.3):

1. If $(a, q) = 1$, then $x^n \equiv a \pmod{q}$ is solvable $\iff$ $a^{\varphi(q)/d} \equiv 1 \pmod{q}$, where $d := \gcd(n, \varphi(q))$. Moreover, if a solution exists then there are exactly d solutions.

2. Let q be an odd prime such that $q \nmid a$ and $q \nmid n$. If $x^n \equiv a \pmod{q}$ is solvable, then $x^n \equiv a \pmod{q^k}$ is also solvable for all $k \geq 1$. Moreover all these congruence have the same number of solutions.

Then, for q prime and in the case $x^n = a$ is solvable we have

$$\#\{x \in \mathbb{F}_{q^k} : x^n = a\} = \#\{x \in \mathbb{F}_q : x^n = a\} = \gcd(n, \varphi(q)) = \gcd(n, q-1) = n$$

since $n|(q-1)$. Hence, Lemma A.1 generalizes over $\mathbb{F}_{q^k}$. The proof of the Corollary now follows analogously to the proof of Theorem A.2.

□

As a consequence of Corollary A.3 we get the following result that relates the number of points of certain curves over finite extensions of $\mathbb{F}_q$.

Corollary A.4. *Let l be a prime, m, m', s, s' be integers satisfying $1 \leq m, m', s, s' < l$ and $m + s = m' + s' = l$, and consider the curves with affine equations given by $\mathcal{C}_z^{(m,s)} : y^l = t^m(1-t)^s(1-zt)^m$ and $\mathcal{C}_z^{(m',s')} : y^l = t^{m'}(1-t)^{s'}(1-zt)^{m'}$ with $z \neq 0, 1$. Then, for a prime q such that $q \equiv 1 \pmod{l}$ we have*

$$\#\mathcal{C}_z^{(m,s)}(\mathbb{F}_{q^k}) = \#\mathcal{C}_z^{(m',s')}(\mathbb{F}_{q^k})$$

for all $k \in \mathbb{N}$.

Proof. Again, we drop the dependency of the curves on the integers m, m', s, s' and denote $\mathcal{C}_z^{(m,s)} = \mathcal{C}_z$ and $\mathcal{C}_z^{(m',s')} = \mathcal{C}'_z$. Let $\eta_{q^k} \in \widehat{\mathbb{F}_{q^k}^\times}$ be a character of order l. If $l = 2$ then $\mathcal{C}_z = \mathcal{C}'_z$ since (m, s) and (m', s') are both $(1, 1)$. Therefore, there is nothing to prove in this case.

Suppose now that l is an odd prime. Then, the order of η_{q^k} is odd and so $\eta_{q^k}(-1) = 1$. Next, consider $a := m/l,\ b := s/l$ and $a' := m'/l,\ b' := s'/l$ in Theorem

A.2. The curves defined by these values are exactly $\mathcal{C}_z$ and $\mathcal{C'}_z$, hence by Corollary A.3 and taking into account that $m+s=l$ and $m'+s'=l$, we have

$$\#\mathcal{C}_z(\mathbb{F}_{q^k}) - (q^k+1) = q^k \sum_{i=1}^{l-1} {}_2F_1\left(\begin{matrix} \eta_{q^k}^{i(l-m)}, & \eta_{q^k}^{im} \\ & \varepsilon \end{matrix} \middle| z \right) \tag{3.4}$$

$$\#\mathcal{C}'_z(\mathbb{F}_{q^k}) - (q^k+1) = q^k \sum_{i=1}^{l-1} {}_2F_1\left(\begin{matrix} \eta_{q^k}^{i(l-m')}, & \eta_{q^k}^{im'} \\ & \varepsilon \end{matrix} \middle| z \right) \tag{3.5}$$

As we can see, the exponents of the characters appearing in the hypergeometric functions in (3.4) and (3.5) add up to $0 \pmod{l}$. Also notice that

- $\#\{(r,t) : 1 \leq r,t \leq l-1, r+t=l\} = l-1$.
- $i(l-m) \equiv j(l-m) \pmod{l} \iff im \equiv jm \pmod{l} \iff l | m(i-j)$. Since l is prime and $0 < m < l$, l must divide $i-j$. But $1 \leq i,j \leq l-1$, then $i(l-m) \equiv j(l-m) \pmod{l} \iff i = j$

By these two observations, we see that the terms appearing in the RHS of (3.4) are the same ones appearing in the RHS of (3.5), therefore we conclude that

$$\#\mathcal{C}_z(\mathbb{F}_{q^k}) = \#\mathcal{C}'_z(\mathbb{F}_{q^k})$$

□

It is not hard to see that the previous result can be generalized to the case when l is an odd integer and $(l,m) = (l,m') = 1$, and the argument is the same done above. However, the result is not true in general if we just ask for $m+s = m'+s'$, as we can see in the following example for $l=5$ and $m+s=4$:

- If $(m,s) = (1,3)$ then $Z(\mathcal{C}_2|\mathbb{F}_{11}, T) = \frac{(11T^2+3T+1)^4}{(1-T)(1-11T)}$ hence

$$|\#\mathcal{C}_2(\mathbb{F}_{11}) - (11+1)| = 12$$

- If $(m', s') = (2, 2)$ then $Z(\mathcal{C}'_2|\mathbb{F}_{11}, T) = \frac{(11T^2-2T+1)^4}{(1-T)(1-11T)}$ hence

$$|\#\mathcal{C}'_2(\mathbb{F}_{11}) - (11+1)| = 8$$

CHAPTER IV

THE MAIN CONJECTURE

A. Introduction

In the previous chapter we proved that we can relate, in an explicit way, the number of points on certain curves over finite fields and values of particular hypergeometric functions. My next interest has been to find a closed formula for hypergeometric functions over finite fields, and more specifically, I have been interested in relating each particular term that appears in the right hand side of sum (3.1) to the curve $\mathcal{C}_z$. First, we recall some basic facts and the Riemann-Hurwitz genus formula, which is extremely useful when trying to compute the genus of an algebraic curve.

Let K be a perfect field (i.e., every algebraic extension of K is separable). We say that a non-constant map of curves $\psi : \mathcal{C}_1 \to \mathcal{C}_2$ is separable if the extension of function fields $K(\mathcal{C}_1)|\psi^*(K(\mathcal{C}_2))$ is a separable extension of fields. Also, ψ has a non-zero degree $n := \deg(\psi)$ that can be defined as the number of points in a generic fiber $\psi^{-1}(Q)$ for $Q \in \mathcal{C}_2$. Now, there is a finite set of points $Q \in \mathcal{C}_2$ for which the inverse image $\psi^{-1}(Q)$ does not have size n, we call these points the ramification points of ψ, and associated to them there is an integer called ramification index (for more details see [9]).

Theorem A.1 (Riemann-Hurwitz genus formula)**.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two smooth curves defined over K of genus g_1 and g_2 respectively. Let $\psi : \mathcal{C}_1 \to \mathcal{C}_2$ be a non-constant and separable map. Then*

$$2g_1 - 2 \geq deg(\psi)(2g_2 - 2) + \sum_{P \in \mathcal{C}_1} (e_\psi(P) - 1)$$

where $e_\psi(P)$ is the ramification index of ψ at P. Moreover, there is equality if and only if either char$(K) = 0$ or char$(K) = p$ and p does not divide $e_\psi(P)$ for all $P \in \mathcal{C}_1$.

Next, we apply the Riemann-Hurwitz formula to compute the genus of the smooth projective curve $\mathcal{C}_z$ with affine equation

$$\mathcal{C}_z : y^l = t^m(1-t)^s(1-zt)^m \tag{4.1}$$

where l is prime and $1 \leq m, s < l$ such that $m + s = l$. For that, we consider the map

$$\psi : \mathcal{C}_z \to \mathbb{P}^1, \qquad [x : y : z] \mapsto [x : z]$$

and notice that $[0 : 1 : 0] \mapsto [1 : 0]$. Generically, every point in $\mathbb{P}^1$ has l preimages, so the degree of this map is l. Now, the genus of $\mathbb{P}^1$ is 0 and ψ is ramified at 4 points, namely $P_1 = [0 : 0 : 1], P_2 = [1 : 0 : 1], P_3 = [z^{-1} : 0 : 1]$ and $P_4 = [0 : 1 : 0]$ the point at infinity, with ramification indices $e_\psi(P_i) = l$ for all $i = 1, \ldots, 4$. Denoting $g := \text{genus}(\mathcal{C}_z)$, we obtain that $2g - 2 = -2l + 4(l-1) = 2l - 4$, hence $g = l - 1$.

Remark A.2. The fact that the curve $\mathcal{C}_z$ has genus $l-1$ can also be seen by noticing that $\mathcal{C}_z$ is a hyperelliptic curve and has model $Y^2 = F(X)$ with $\deg(F(X)) = 2l$ (see Chapter V Theorem A.5). Hence, $2l = 2\,\text{genus}(\mathcal{C}_z) + 2$, therefore, $\text{genus}(\mathcal{C}_z) = l - 1$.

Now, applying Theorem A.2 in Chapter III to the curve (4.1), we see that the upper limit in the sum is the genus of the curve. Also, as we mentioned in the previous chapter, since l is prime and $\eta_q \in \widehat{\mathbb{F}_q^\times}$ is a character of order l, we have that

$\eta_q(-1) = 1$. Then,

$$\#\mathcal{C}_z(\mathbb{F}_q) = q + 1 + q \sum_{i=1}^{g} {}_2F_1 \left(\begin{array}{cc} \eta_q^{is}, & \eta_q^{im} \\ & \varepsilon \end{array} \middle| z \right)$$

$$= q + 1 + F_{1,q}(z) + F_{2,q}(z) + \cdots + F_{g,q}(z) \tag{4.2}$$

where $F_{i,q}(z) = q \, {}_2F_1 \left(\begin{array}{cc} \eta_q^{is}, & \eta_q^{im} \\ & \varepsilon \end{array} \middle| z \right)$.

Notice the resemblance between formulas (2.4) and (4.2). With this similarity in mind, we are now interested in finding relations between the terms in these formulas, i.e., relations between the $F_{i,q}(z)$ in formula (4.2) and the $\alpha_{i,q}(z) + \overline{\alpha_{i,q}}(z)$ in formula (2.4).

B. The Main Conjecture

As we mentioned in the previous section, we want to relate the terms $F_{i,q}(z)$ in formula (4.2) to the $\alpha_{i,q}(z) + \overline{\alpha_{i,q}}(z)$ in formula (2.4). Denote $a_{i,q}(z) := \alpha_{i,q}(z) + \overline{\alpha_{i,q}}(z)$. We state next our main conjecture, and in the next sections we prove it in some particular cases.

Conjecture B.1. Let l and q be odd primes such that $q \equiv 1 \pmod{l}$ and let $z \in \mathbb{F}_q$, $z \neq 0, 1$. Consider the smooth projective curve with affine equation given by

$$\mathcal{C}_z^{(m,s)} : y^l = t^m(1-t)^s(1-zt)^m$$

where $1 \leq m, s < l$ are integers such that $m + s = l$. Then, using the notation from previous section and after rearranging terms if necessary

$$F_{i,q}(z) = -a_{i,q}(z) \quad \text{for all } 1 \leq i \leq g.$$

The previous conjecture gives a closed formula for the values of some hypergeometric functions over finite fields in terms of the traces of Frobenius of certain curves. In the next two sections we prove the conjecture for particular values of the prime l.

C. Proof of Conjecture for $l = 3$

Throughout this section fix $l = 3$ and let q be a prime such that $q \equiv 1 \pmod 3$. Let $z \in \mathbb{F}_q$, $z \neq 0, 1$, and consider the smooth projective curve with affine equation given by

$$\mathcal{C}_z^{(1,2)} : y^3 = t(1-t)^2(1-zt) \tag{4.3}$$

Denote $\mathcal{C}_z^{(1,2)} = \mathcal{C}_z$. The idea will be to show that the L-polynomial of the curve $\mathcal{C}_z$ is a perfect square, and from that and formulas (2.4) and (4.2) conclude that the values of the traces of Frobenius must agree with the values of the hypergeometric functions, up to a sign.

Recall that, by the Riemann-Hurwitz formula, $\mathcal{C}_z$ has genus 2. Now, every curve of genus 2 defined over $\mathbb{F}_q$ is birationally equivalent over $\mathbb{F}_q$ to a curve of the form

$$\mathcal{C} : Y^2 = F(X) \tag{4.4}$$

where

$$F(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_6 X^6 \in \mathbb{F}_q[X]$$

is of degree 6 and has no multiple factors (see [5]). This identification is unique up to a fractional linear transformation of X, and associated transformation of Y,

$$X \to \frac{aX+b}{cX+d}, \quad Y \to \frac{eY}{(cX+d)^3} \tag{4.5}$$

where

$$a, b, c, d \in \mathbb{F}_q, \quad ad - bc \neq 0, \quad e \in \mathbb{F}_q^{\times}.$$

In our particular case we have

Lemma C.1. The curve $\mathcal{C}_z : y^3 = t(1-t)^2(1-zt)$ is birationally equivalent to

$$\mathcal{C} : Y^2 = X^6 + 2(1-2z)X^3 + 1. \tag{4.6}$$

Proof. We begin by translating $t \to 1-t$, so the double point is now at the origin. We get:

$$\begin{aligned}\mathcal{C}_{(1)} : y^3 &= (1-t)t^2(1-z(1-t)) \\ &= (1-z)t^2 + (2z-1)t^3 - zt^4.\end{aligned}$$

Since $z \neq 0$, multiply both sides by z^{-1} and define

$$G_2(t,y) := (1-z^{-1})t^2$$

$$G_3(t,y) := z^{-1}y^3 - (2-z^{-1})t^3$$

$$G_4(t,y) := t^4.$$

Then, each G_i is a homogeneous polynomial of degree i in $\mathbb{F}_q[t,y]$ and $\mathcal{C}_z$ is birationally equivalent to

$$\mathcal{C}_{(1)} : G_2(t,y) + G_3(t,y) + G_4(t,y) = 0.$$

Next, put $y = tX$ and complete the square to get:

$$\begin{aligned}\mathcal{C}_{(2)} : 0 &= t^4 + (z^{-1}X^3 + z^{-1} - 2)t^3 + (1-z^{-1})t^2 \\ &= \left(t^2 + \frac{1}{2}(z^{-1}X^3 + z^{-1} - 2)t\right)^2 - \frac{(z^{-1}X^3 + z^{-1} - 2)^2}{4}t^2 + (1-z^{-1})t^2\end{aligned}$$

Multiply by 4 ($\mathrm{char}(\mathbb{F}_q \neq 2)$) and divide by t^2 to get that $\mathcal{C}_z$ is birationally equivalent

to

$$\mathcal{C} : Y^2 = F(X)$$

where

$$Y = 2G_4(1, X)t + G_3(1, X)$$

$$F(X) = G_3(1, X)^2 - 4G_2(1, X)G_4(1, X)$$

By substituting G_2, G_3 and G_4 in $F(X)$, and rescaling $Y \to z^{-1}Y$ we get the desired result, i.e., $\mathcal{C}_z$ is birationally equivalent to

$$\mathcal{C} : Y^2 = X^6 + 2(1 - 2z)X^3 + 1.$$

□

In order to show that the L-polynomial of the curve $\mathcal{C}_z$ over $\mathbb{F}_q$ is a perfect square, we will start by showing that the Jacobian of $\mathcal{C}_z$, $\mathrm{Jac}(\mathcal{C}_z)$, is isogenous to the product of two elliptic curves, i.e., that the $\mathrm{Jac}(\mathcal{C}_z)$ is *reducible*. To do that, it is convenient to find a slightly different model for our curve as we can see in the next criterion. First, we need to introduce the concept of equivalent curves.

Definition C.2. We say that two curves $Y^2 = F(X)$ are equivalent if they are taken into one another by a fractional linear transformation of X and the related transformation of Y given by (4.5).

Theorem C.3 ([5] Theorem 14.1.1)**.** *The following properties of a curve $\mathcal{C}$ of genus 2 are equivalent:*

1. *It is equivalent to a curve*

$$Y^2 = c_3X^6 + c_2X^4 + c_1X^2 + c_0 \tag{4.7}$$

with no terms of odd degree in X.

2. *It is equivalent to a curve*

$$Y^2 = G_1(X)G_2(X)G_3(X) \tag{4.8}$$

where the quadratics $G_j(X)$ are linearly dependent.

3. *It is equivalent to*

$$Y^2 = X(X-1)(X-a)(X-b)(X-ab) \tag{4.9}$$

for some a, b.

If one (and so all) of the previous conditions is satisfied, the Jacobian of $\mathcal{C}$ is reducible.

There are two maps of (4.7) into elliptic curves

$$\mathcal{E}_1 : Y^2 = c_3Z^3 + c_2Z^2 + c_1Z + c_0 \tag{4.10}$$

with $Z = X^2$ and

$$\mathcal{E}_2 : V^2 = c_0U^3 + c_1U^2 + c_2U + c_3 \tag{4.11}$$

with $U = X^{-2}, V = YX^{-3}$. These maps extend to maps of the Jacobian, which is therefore reducible (see [5]).

Hence, to apply Theorem C.3 we find a different model for $\mathcal{C}_z$. In particular we will put our curve in form (4.7).

Lemma C.4. The curve (4.6) is equivalent to the curve

$$Y^2 = (1-z)X^6 + 3(2+z)X^4 + 3(3-z)X^2 + z. \tag{4.12}$$

Proof. Consider the fractional linear transformation given by

$$X \to \frac{X+1}{X-1}$$

$$Y \to \frac{2Y}{(X-1)^3}$$

□

Combining Lemma C.4 and the observation at the end of Theorem C.3, we find two maps from (4.12) to the elliptic curves

$$\mathcal{E}_{1,z} : Y^2 : (1-z)Z^3 + 3(2+z)Z^2 + 3(3-z)Z + z \tag{4.13}$$

$$\mathcal{E}_{2,z} : V^2 = zU^3 + 3(3-z)U^2 + 3(2+z)U + (1-z) \tag{4.14}$$

Notice that $\mathcal{E}_{1,z}$ and $\mathcal{E}_{2,z}$ have discriminant $6912z(1-z)$, which is non-zero since $z \neq 0, 1$. Also, after rescaling, we can write

$$\mathcal{E}_{1,z} : Y^2 : Z^3 + 3(2+z)Z^2 + 3(3-z)(1-z)Z + z(1-z)^2 \tag{4.15}$$

and

$$\mathcal{E}_{2,z} : V^2 = U^3 + 3(3-z)U^2 + 3(2+z)zU + (1-z)z^2 \tag{4.16}$$

As we mentioned above, the existence of these two maps implies that $\mathrm{Jac}(\mathcal{C}_z)$ is isogenous to $\mathcal{E}_{1,z} \times \mathcal{E}_{2,z}$. Next, we see that these elliptic curves are not totally independent of each other. In fact, one is isogenous to a twist of the other as we see in our next result.

Proposition C.5. *The curve $\mathcal{E}_{1,z}$ is isogenous to the twisted curve $(\mathcal{E}_{2,z})_{-3}$.*

Proof. Consider the equation for the twisted curve $(\mathcal{E}_{2,z})_{-3}$:

$$(\mathcal{E}_{2,z})_{-3} : V^2 = U^3 - 9(3-z)U^2 + 27(2+z)zU - 27(1-z)z^2 \tag{4.17}$$

Define $\varphi : \mathcal{E}_{1,z} \to (\mathcal{E}_{2,z})_{-3}$ such that $\varphi[0:1:0] = [0:1:0]$ and

$$\varphi[x:y:1] = \left[\frac{x^3 + Ax^2 + Bx + C}{(x+(z-1))^2} : \frac{(x^3 + Dx^2 + Ex + F)y}{(x+(z-1))^3} : 1\right] \tag{4.18}$$

where
$$\begin{cases} A = 9 \\ B = 3(1-z)(z+9) \\ C = (27-2z)(z-1)^2 \\ D = 3(z-1) \\ E = 3(z+15)(z-1) \\ F = (z-81)(z-1)^2. \end{cases}$$

One can check by hand or with Maple for example, that the map φ is well defined and gives an isogeny between the two curves. □

Denote by $L(\mathcal{C}_z/\mathbb{F}_q, T)$ the L-polynomial of $\mathcal{C}_z$ over $\mathbb{F}_q$. Recall that we want to show that, for $q \equiv 1 \pmod 3$ we have $L(\mathcal{C}_z/\mathbb{F}_q, T) = (1 + aT + qT^2)^2$ for some $a \in \mathbb{R}$. So far, we have seen that

$$L(\mathcal{C}_z/\mathbb{F}_q, T) = (1 + a_{1,q}(z)T + qT^2)(1 + a_{2,q}(z)T + qT^2)$$

where $a_{1,q}(z)$ and $a_{2,q}(z)$ are the traces of Frobenius on the curves $\mathcal{E}_{1,z}$ and $\mathcal{E}_{2,z}$ respectively. Therefore, we need to show that $a_{1,q}(z) = a_{2,q}(z)$, or equivalently, that $\#\mathcal{E}_{1,z}(\mathbb{F}_q) = \#\mathcal{E}_{2,z}(\mathbb{F}_q)$ for $q \equiv 1 \pmod 3$. This is the statement of our next result.

Corollary C.6. *Let q be a prime such that $q \equiv 1 \pmod 3$. Then*

$$\#\mathcal{E}_{1,z}(\mathbb{F}_q) = \#\mathcal{E}_{2,z}(\mathbb{F}_q).$$

Proof. Fix q in the conditions of the corollary. Let $a_{1,q}(z)$ and $a_{2,q}(z)$ be the traces

of Frobenius on the elliptic curves $\mathcal{E}_{1,z}$ and $\mathcal{E}_{2,z}$ respectively, i.e.

$$\#\mathcal{E}_{1,z}(\mathbb{F}_q) = q + 1 - a_{1,q}(z)$$

$$\#\mathcal{E}_{2,z}(\mathbb{F}_q) = q + 1 - a_{2,q}(z)$$

Since $(\mathcal{E}_{2,z})_{-3}$ is a twist of $\mathcal{E}_{2,z}$ we have

$$\#(\mathcal{E}_{2,z})_{-3}(\mathbb{F}_q) = 1 + q - \left(\frac{-3}{q}\right) a_{2,q}(z)$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol.
Now, by Proposition (C.5) we know that

$$\#(\mathcal{E}_{1,z})(\mathbb{F}_q) = \#(\mathcal{E}_{2,z})_{-3}(\mathbb{F}_q)$$

hence

$$a_{2,q}(z) = \left(\frac{-3}{q}\right) a_{1,q}(z).$$

To finish the proof, it only remains to see that $\left(\frac{-3}{q}\right) = 1$ for all primes $q \equiv 1 \pmod 3$. Since the Legendre symbol is completely multiplicative on its top argument, we can decompose $\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right)$. Also

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2} = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{4.19}$$

and

$$\left(\frac{3}{q}\right) = (-1)^{\lceil (q+1)/6 \rceil} = \begin{cases} 1 & \text{if } q \equiv 1, 11 \pmod{12} \\ -1 & \text{if } q \equiv 5, 7 \pmod{12}. \end{cases} \tag{4.20}$$

We will divide the analysis in cases. First notice that since $q \equiv 1 \pmod 3$ then q must be congruent to either 1 or 7 $\pmod{12}$.

- Suppose $q \equiv 1 \pmod{12}$ and therefore $\left(\frac{3}{q}\right) = 1$ by (4.20). Also, since $q \equiv 1 \pmod{12}$, we have that $q \equiv 1 \pmod 4$, hence $\left(\frac{-1}{q}\right) = 1$ by (4.19). Then $\left(\frac{-3}{q}\right) = 1$ as desired.
- Suppose $q \equiv 7 \pmod{12}$, then $\left(\frac{3}{q}\right) = -1$. Also, in this case $q \equiv 3 \pmod 4$, and so $\left(\frac{-1}{q}\right) = -1$, giving that $\left(\frac{-3}{q}\right) = 1$ as desired.

Hence

$$\#\mathcal{E}_{1,z}(\mathbb{F}_q) = \#\mathcal{E}_{2,z}(\mathbb{F}_q) \text{ for all } q \equiv 1 \pmod 3.$$

□

We have now all the necessary tools to complete the proof of Conjecture B.1 for the case when $l = 3$.

Theorem C.7. *Conjecture B.1 is true for $l = 3$.*

Proof. First notice that when $l = 3$ we have two different cases to consider, namely the curves with $(m, s) = (1, 2)$ and $(m, s) = (2, 1)$. However, by Chapter III Corollary A.4 these two curves have the same number of points over every finite field extension of $\mathbb{F}_q$, therefore they have the same zeta function over $\mathbb{F}_q$. Also, the hypergeometric functions that appear on the right hand side of equation (3.1) are the same for both curves. Because of these, it is enough to prove that the conjecture is true for one of these curves, say $\mathcal{C}_z : y^3 = t(1-t)^2(1-zt)$. As above, write the zeta function of $\mathcal{C}_z$ as

$$\begin{aligned} Z(\mathcal{C}_z/\mathbb{F}_q; T) &= \frac{(1-\alpha_{1,q}(z)T)(1-\overline{\alpha_{1,q}(z)}T)(1-\alpha_{2,q}(z)T)(1-\overline{\alpha_{2,q}(z)}T)}{(1-T)(1-qT)} \\ &= \frac{(1-a_{1,q}(z)T+qT^2)(1-a_{2,q}(z)T+qT^2)}{(1-T)(1-qT)} \end{aligned}$$

where $a_{i,q}(z) = \alpha_{i,q}(z) + \overline{\alpha_{i,q}}(z)$. Using the same notation as in equation (4.2), we

have that

$$F_{1,q}(z) + F_{2,q}(z) = -(a_{1,q}(z) + a_{2,q}(z)) \tag{4.21}$$

Recall that $F_{1,q}(z) = {}_2F_1[\eta_q^2, \eta_q; \varepsilon|z]$ and $F_{2,q}(z) = {}_2F_1[\eta_q, \eta_q^2; \varepsilon|z]$, therefore, Corollary B.6 in Chapter II implies that $F_{1,q}(z) = F_{2,q}(z)$. Also, as we have seen in Corollary C.6, $a_{1,q}(z) = a_{2,q}(z)$, Hence, (4.21) becomes

$$2F_{1,q}(z) = -2a_{1,q}(z)$$

so $a_{1,q}(z) = -F_{1,q}(z)$ and $a_{2,q}(z) = -F_{2,q}(z)$, proving the conjecture for $l = 3$. □

D. Proof of Conjecture for $l = 5$

Our next objective is to prove that Conjecture B.1 also holds when $l = 5$. The proof has some ingredients in common with the previous case, however is not completely analogous and requires some different techniques as we will see.

Consider the smooth projective curve with affine model

$$\mathcal{C}_z : y^5 = t(1-t)^4(1-zt) \tag{4.22}$$

over a finite field $\mathbb{F}_q$ with q prime, $q \equiv 1 \pmod 5$ and $z \in \mathbb{F}_q \backslash \{0, 1\}$. Notice that, by performing the same transformations done in Lemma C.1 and the fractional linear transformation

$$X \to \frac{X+1}{X-1}$$
$$Y \to \frac{2Y}{(X-1)^5}$$

on the curve (4.22) we get the following result.

Lemma D.1. The curve $\mathcal{C}_z : y^5 = t(1-t)^4(1-zt)$ is equivalent to the curve

$$\mathcal{C} : Y^2 = (1-z)X^{10} + (20+5z)X^8 + (110-10z)X^6 + (100+10z)X^4 + (25-5z)X^2 + z. \tag{4.23}$$

Define the curves $\mathcal{H}_{1,z} : y^2 = f(x)$ and $\mathcal{H}_{2,z} : y^2 = g(x)$ where

$$f(x) = (1-z)x^5 + (20+5z)x^4 + (110-10z)x^3 + (100+10z)x^2 + (25-5z)x + z \tag{4.24}$$

and

$$g(x) = zx^5 + (25-5z)x^4 + (100+10z)x^3 + (110-10z)x^2 + (20+5z)x + (1-z). \tag{4.25}$$

Then, by the same argument in the previous section, we can find two maps from $\mathcal{C}$ to $\mathcal{H}_{1,z}$ and $\mathcal{H}_{2,z}$, and extending these maps to the Jacobians of the curves, we conclude that $\mathrm{Jac}(\mathcal{C})$ is isogenous to $\mathrm{Jac}(\mathcal{H}_{1,z}) \times \mathrm{Jac}(\mathcal{H}_{2,z})$. We start by showing that the L-polynomial of $\mathcal{C}_z$ over $\mathbb{F}_q$ with $q \equiv 1 \pmod 5$ is a perfect square. First, we recall some results about abelian varieties.

Let k be a perfect field, which will eventually be finite. Recall that an *abelian variety over* k is a subset of some projective n-space over k which

1. is defined by polynomial equations on the coordinates (with coefficients in k),
2. is connected, and
3. has a group law which is algebraic (i.e., the coordinates of the sum of two points are rational functions of the coordinates of the factors).

We say that an abelian variety over k is *simple* if it has no nontrivial abelian subvarieties. We have the following result.

Theorem D.2. *(Poincaré-Weil) Every abelian variety over k is isogenous to a product of powers of nonisogenous simple abelian varieties over k.*

Consider $\mathcal{C}_z : y^5 = t(1-t)^4(1-zt)$ over the algebraically closed field $\overline{\mathbb{Q}}$ and let $\zeta := e^{2\pi i/5}$ be a fifth root of unity. Then the map $[\zeta] : \mathcal{C}_z \to \mathcal{C}_z$ defined by $[\zeta](t, y) = (t, \zeta y)$ defines an automorphism on the curve $\mathcal{C}_z$. Denote $J_z := \mathrm{Jac}(\mathcal{C}_z)$ and $J_{i,z} := \mathrm{Jac}(\mathcal{H}_{i,z})$, for $i = 1, 2$. The automorphism $[\zeta]$ induces a map from J_z to itself, hence

$$[\zeta] \in \mathrm{End}(J_z).$$

On the other hand, as we mentioned above, we can find an isogeny over $\mathbb{Q}$

$$\phi : J_{1,z} \times J_{2,z} \to J_z.$$

Applying ϕ we get

$$\phi(J_{1,z}) \subseteq J_z$$

where $J_{1,z}$ here denotes $J_{1,z} \times \{0\}$. Similarly

$$\phi(J_{2,z}) \subseteq J_z.$$

We also have

$$[\zeta](\phi(J_{i,z})) \subseteq J_z$$

for $i = 1, 2$.

Consider now the curve $y^5 = t(1-t)^4(1-zt)$ defined over $\overline{\mathbb{Q}(z)}$. We can apply to this curve the same argument we did before, and we can see that $J_{i,z}$ are simple abelian varieties over $\overline{\mathbb{Q}(z)}$. Otherwise, if $J_{i,z}$ is isogenous to the product of two elliptic curves, then, for all z the L-polynomial would have two quadratic factors, which is not the case. (See example in section E at the end of this chapter). Therefore,

we have $\phi(J_{1,z})$ and $[\zeta](\phi(J_{1,z}))$ two simple abelian varieties inside J_z. By Poincaré complete reducibility theorem, we have that either $\phi(J_{1,z}) \cap [\zeta](\phi(J_{1,z}))$ is finite or $\phi(J_{1,z}) = [\zeta](\phi(J_{1,z}))$.

- Case 1: $\phi(J_{1,z}) \cap [\zeta](\phi(J_{1,z}))$ is finite.

  In this case, by dimension count we have

  $$[\zeta](\phi(J_{1,z})) + \phi(J_{1,z}) = J_z.$$

  Then, since $\phi(J_{1,z})$ and $\phi(J_{2,z})$ are simple abelian varieties, the Poincaré -Weil Theorem implies that

  $$[\zeta](\phi(J_{1,z})) \approx \phi(J_{2,z})$$

  over $\mathbb{Q}(\zeta)$, where $\approx$ denotes isogeny. Notice that this isogeny will exist over any field containing a fifth root of unity, therefore, finite fields $\mathbb{F}_q$ with $q \equiv 1 \pmod 5$ are fine. Then, we get that $[\zeta](\phi(J_{1,z}))$ is isogenous to $\phi(J_{2,z})$ over $\mathbb{F}_q$ for $q \equiv 1 \pmod 5$.

- Case 2: $[\zeta](\phi(J_{1,z})) = \phi(J_{1,z})$.

  For this case, we recall first some facts about abelian varieties (for details see [16] or [18]). Suppose $A/\overline{k}$ is a simple abelian variety of dimension g, and denote $\Delta := \mathrm{End}_{\overline{k}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, Poincaré's complete reducibility Theorem implies that Δ is a division algebra. Also, from the theory of division algebras we know that the dimension of a division algebra over its center is a perfect square, hence, if $K = \{x \in \Delta : xa = ax \text{ for all } a \in \Delta\}$ is the center of Δ, we have $[\Delta : K] = d^2$ for some integer d. On the other hand, if $[K : \mathbb{Q}] = e$ then $de|2g$, moreover, in characteristic zero, we have that $d^2e|2g$.

  Now that we have reviewed the results we need we can go back to case 2. In

this case, let $\Delta := \mathrm{End}(\phi(J_{1,z})) \otimes_{\mathbb{Z}} \mathbb{Q}$ and K be its center. Applying the results above, we can assume that $[\Delta : K] = d^2$ and $[K : \mathbb{Q}] = e$, for some integers d and e. Since the dimension of $\phi(J_{1,z}) = 2$ and $\mathrm{char}(\overline{\mathbb{Q}(z)}) = 0$, we have that $d^2 e | 4$.

By assumption, we have that

$$[\zeta] \in \mathrm{End}(\phi(J_{1,z})),$$

hence

$$\mathbb{Q}(\zeta) \subseteq \mathrm{End}(\phi(J_{1,z})) \otimes_{\mathbb{Z}} \mathbb{Q} := \Delta.$$

Now, we have

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \Delta,$$

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$$

and

$$[\Delta : \mathbb{Q}] | 4.$$

Therefore, $4 = 4[\Delta : \mathbb{Q}(\zeta)]$, hence

$$\mathbb{Q}(\zeta) = \Delta$$

i.e., $\mathrm{End}(\phi(J_{1,z})) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a field of degree 4 over $\mathbb{Q}$.

Recall the following definition.

Definition D.3. A totally imaginary quadratic extension of a totally real field is called a CM field (Complex Multiplication).

Then, Δ is a CM field, since it is equal to $\mathbb{Q}(\zeta)$ and every cyclotomic field is a CM field ($\mathbb{Q} \subseteq \mathbb{Q}(\zeta, \overline{\zeta}) \subseteq \mathbb{Q}(\zeta)$).

Theorem D.4 (Shimura [17])**.** *Let k be a field of characteristic zero. Over k there do not exist non-constant families of abelian varieties with full CM (i.e., the endomorphism ring has maximal dimension).*

However, our family $\phi(J_{1,z})$ is non-constant, as it can be computationally checked with Magma using Igusa invariants.

Therefore, only case 1 is possible, and we have

$$[\zeta](\phi(J_{1,z})) \approx \phi(J_{2,z}).$$

We now state and prove our theorem.

Theorem D.5. *Conjecture B.1 holds for $l = 5$ over $\mathbb{F}_q$, for a prime $q \equiv 1 \pmod 5$.*

Proof of Theorem D.5. By the same argument done in the proof of Conjecture B.1 for $l = 3$, it is enough to prove the conjecture for the curve $\mathcal{C}_z : y^5 = t(1-t)^4(1-zt)$. Also, by the previous argument, then the L-polynomial of $\mathcal{C}_z$ is a perfect square, i.e., we can assume, after rearranging terms if necessary, that $a_{1,q}(z) = a_{4,q}(z)$ and $a_{2,q}(z) = a_{3,q}(z)$. We can write then

$$Z(\mathcal{C}_z/\mathbb{F}_q; T) = \frac{(1 - a_1(z)T + qT^2)^2(1 - a_2(z)T + qT^2)^2}{(1-T)(1-qT)}$$

By Corollary B.6 in Chapter II, we know that $F_{1,q}(z) = F_{4,q}(z)$ and $F_{2,q}(z) = F_{3,q}(z)$. At the end, we get that

$$-(a_{1,q}(z) + a_{2,q}(z)) = F_{1,q}(z) + F_{2,q}(z). \tag{4.26}$$

We want to prove that $-a_{1,q}(z) = F_{1,q}(z)$ and $-a_{2,q}(z) = F_{2,q}(z)$. Recall, from (2.4)

that

$$-(a_{1,q}(z)^2 - 2q + a_{2,q}(z)^2 - 2q) = F_{1,q^2}(z) + F_{2,q^2}(z). \tag{4.27}$$

Also, keep in mind that for the hypergeometric functions $F_{1,q}$ and $F_{2,q}$ we are choosing a character $\eta_q \in \widehat{\mathbb{F}_q^\times}$ of order 5, and for the hypergeometric functions F_{1,q^2} and F_{2,q^2} the character we are choosing is in $\widehat{\mathbb{F}_{q^2}^\times}$, also of order 5.

Claim 1. It is enough to show that

$$F_{i,q^2}(z) = -F_{i,q}(z)^2 + 2q \tag{4.28}$$

for $i = 1, 2$.

Proof of Claim. We will write $a_{i,q} := a_{i,q}(z)$ and $F_{i,q^k} := F_{i,q^k}(z)$ for $i, k = 1, 2$. If (4.28) is true, from (4.26) and (4.27) we get the system of equations in $a_{1,q}$ and $a_{2,q}$

$$\begin{cases} -a_{1,q} - a_{2,q} = F_{1,q} + F_{2,q} \\ a_{1,q}^2 + a_{2,q}^2 = F_{1,q}^2 + F_{2,q}^2. \end{cases}$$

which is equivalent to

$$\begin{cases} -a_{1,q} - a_{2,q} = F_{1,q} + F_{2,q} \\ a_{1,q}a_{2,q} = F_{1,q}F_{2,q}. \end{cases}$$

hence, $a_{1,q} = -F_{1,q}$ and $a_{2,q} = -F_{2,q}$. □

Continuing with the proof of the conjecture for $l = 5$, it only remains to show that (4.28) holds. For that, let's start by writing explicitly the functions we have on the left and right hand side of (4.28). We start with $F_{1,q} = F_{4,q} = 11\,{}_2F_1\left(\begin{matrix} \eta_q, & \eta_q^4 \\ & \varepsilon \end{matrix}\middle| z\right)$. The other case will be the result of a similar argument.

$$
\begin{aligned}
F_{1,q}^2 &= \sum_{x,y\in\mathbb{F}_q} \eta_q^4(xy)\,\eta_q((1-x)(1-y))\,\eta_q^4((1-zx)(1-zy)) \\
&= \sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{x\in\mathbb{F}_q^\times} \eta_q((1-x)(1-s/x))\,\eta_q^4((1-zx)(1-zs/x)) \qquad (xy=s) \\
&= \sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{x\in\mathbb{F}_q^\times} \eta_q(1-x-s/x+s)\,\eta_q^4(1-z(x+s/x)+z^2 s).
\end{aligned}
$$

On the other hand, define $\chi \in \widehat{\mathbb{F}_{q^2}^\times}$ such that $\chi := \eta_q \circ N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}$, i.e., for $\alpha \in \mathbb{F}_{q^2}$, $\chi(\alpha) = \eta_q(N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\alpha)) = \eta_q(\alpha^{q+1})$, where $N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}$ denotes the norm from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$. Since $N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\alpha) \in \mathbb{F}_q$ for all $\alpha \in \mathbb{F}_{q^2}$ then χ is well defined and it actually defines a character of $\mathbb{F}_{q^2}^\times$ (see [13] Chapter 11).. Moreover, since the order of η_q is 5 then the order of χ must divide 5. But if $x \in \mathbb{F}_q$ then $N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(x) = x^{q+1} = x^2$, therefore $\chi|_{\mathbb{F}_q} = \eta_q^2 \neq \varepsilon$. Then $\chi \in \widehat{\mathbb{F}_{q^2}^\times}$ is a character of order 5. We choose this character for our computations and we have

$$
\begin{aligned}
F_{1,q^2} &:= \sum_{c\in\mathbb{F}_{q^2}} \chi^4(c)\chi(1-c)\chi^4(1-zc) \\
&= \sum_{c\in\mathbb{F}_{q^2}} \eta_q^4(c^{q+1})\eta_q((1-c)^{q+1})\eta_q^4((1-zc)^{q+1}) \\
&= \sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{\alpha\in\mathbb{F}_{q^2}^\times,\ \alpha^{q+1}=s} \eta_q(1-\alpha-s/\alpha+s)\eta_q^4(1-z(\alpha+s/\alpha)+z^2 s)
\end{aligned}
$$

where the last equality follows by putting $c^{q+1} = s$ and noting that, since $\mathrm{char}(\mathbb{F}_q) = q$ and $\alpha^{q+1} = s$ then

$$(1-\alpha)^{q+1} = (1-\alpha)^q(1-\alpha) = (1-\alpha^q)(1-\alpha) = 1-\alpha-\alpha^q+\alpha^{q+1} = 1-\alpha-s/\alpha+s.$$

A similar computation gives that

$$(1 - zc)^{q+1} = 1 - z(\alpha + s/\alpha) + z^2 s.$$

For $s \in \mathbb{F}_q^\times$ define $h : \mathbb{F}_{q^2}^\times \to \mathbb{F}_{q^2}$ such that $h(t) = t + s/t$ and let f and g be the restrictions of h to the sets $\mathbb{F}_q^\times$ and $N^{-1}(s) := \{\alpha \in \mathbb{F}_{q^2} : \alpha^{q+1} = s\} \subset \mathbb{F}_{q^2}^\times$ respectively, i.e.,

$$f := h|_{\mathbb{F}_q^\times} : \mathbb{F}_q^\times \to \mathbb{F}_q$$

$$g := h|_{N^{-1}(s)} : N^{-1}(s) \to \mathbb{F}_q$$

Notice that, if $\alpha \in N^{-1}(s)$ then $g(\alpha) = \alpha + s/\alpha = \alpha + \alpha^q = \mathrm{tr}(\alpha) \in \mathbb{F}_q$, hence $\mathrm{Im}(g) \subset \mathbb{F}_q$. Making use of these functions, we can rewrite

$$F_{1,q}^2 = \sum_{s \in \mathbb{F}_q^\times} \eta_q^4(s) \sum_{b \in \mathrm{Im}(f) \subset \mathbb{F}_q} \eta_q(1 - b + s)\eta_q^4(1 - bz + z^2 s)$$

and

$$F_{1,q^2} = \sum_{s \in \mathbb{F}_q^\times} \eta_q^4(s) \sum_{b \in \mathrm{Im}(g) \subset \mathbb{F}_q} \eta_q(1 - b + s)\eta_q^4(1 - bz + z^2 s)$$

Combining both equations, we have

$$F_{1,q}^2 + F_{1,q^2} = \sum_{s \in \mathbb{F}_q^\times} \eta_q^4(s) \sum_{\text{some } b \in \mathbb{F}_q} \eta_q(1 - b + s)\eta_q^4(1 - bz + z^2 s). \tag{4.29}$$

Our next and last step will be to describe over what elements are we summing in the inner sum of (4.29). Fix $s \in \mathbb{F}_q^\times$. Note that h is generically a 2-to-1 map. To see this, suppose $b \in \mathrm{Im}(h)$, therefore there exists $t \in \mathbb{F}_{q^2}^\times$ such that $t + s/t = b$, or equivalently $t^2 - bt + s = 0$. Hence, h is 2-to-1 except when $b^2 - 4s = 0$, i.e., except when s is a perfect square in $\mathbb{F}_q$.

- Case 1: s is not a perfect square in $\mathbb{F}_q^\times$.

  By previous comment, we know that in this case h is 2-to-1 map. Also, is not

too hard to show that h is surjective when restricted to the two domains $\mathbb{F}_q^\times$ and $N^{-1}(s)$. Therefore, in this case every element $b \in \mathbb{F}_q^\times$ will appear exactly twice in the inner sum of (4.29).

- Case 2: s is a perfect square in $\mathbb{F}_q^\times$.

  In this case, let $s = a^2$, then $b = 2a$ or $b = -2a$. As in previous case, every $b \in \mathbb{F}_q$ different from $2a$ and $-2a$ will appear exactly twice in the inner sum of (4.29). What about $b = 2a$ and $b = -2a$? If s is a perfect square then $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{2a, -2a\}$, hence both $2a$ and $-2a$ will also appear twice in the sum, once as part of the sum for $F_{1,q}^2$ and once as part of the sum for F_{1,q^2}.

Summarizing we have

$$\begin{aligned} F_{1,q}^2 + F_{1,q^2} = & \sum_{\substack{s\in\mathbb{F}_q^\times \\ \left(\frac{s}{q}\right)=-1}} \eta_q^4(s) \sum_{\text{some } b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s) \\ & \qquad + \sum_{\substack{s\in\mathbb{F}_q^\times \\ \left(\frac{s}{q}\right)=1}} \eta_q^4(s) \sum_{\text{some } b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s) \\ = & \, 2 \sum_{\substack{s\in\mathbb{F}_q^\times \\ \left(\frac{s}{q}\right)=-1}} \eta_q^4(s) \sum_{b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s). \\ & \qquad + 2 \sum_{\substack{s\in\mathbb{F}_q^\times \\ \left(\frac{s}{q}\right)=1}} \eta_q^4(s) \sum_{b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s) \\ = & \, 2 \sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s). \end{aligned}$$

To finish the proof we need to see that

$$\sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s) = q.$$

We begin by rewriting the inner sum in the above formula, but first recall that the

action of $GL_2(\mathbb{F}_q)$ on $\mathbb{F}_q$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot w := \frac{aw+b}{cw+d}$$

defines an automorphism of $\mathbb{P}^1(\mathbb{F}_q)$. Now, since $\eta_q^5 = \varepsilon$ and $\eta_q(0) = 0$ we get

$$\begin{aligned}\sum_{b\in\mathbb{F}_q} \eta_q(1-b+s)\eta_q^4(1-bz+z^2s) &= \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+zs)}} \eta_q\left(\frac{1-b+s}{1-bz+z^2s}\right) \\ &= \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+zs)}} \eta_q(\gamma\cdot b)\end{aligned}$$

where $\gamma := \begin{pmatrix} -1 & s+1 \\ -z & z^2s+1 \end{pmatrix}$. Now, $\det\gamma = (z-1)(1-sz)$, therefore, since $z \neq 1$ we see that as long as $s \neq z^{-1}$, γ defines an automorphism of $\mathbb{P}^1(\mathbb{F}_q)$. Then, by separating the sums according to whether $s = z^{-1}$ or not, we have:

$$\begin{aligned}\sum_{s\in\mathbb{F}_q^\times} \eta_q^4(s) \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+zs)}} \eta_q(\gamma\cdot b) &= \sum_{\substack{s\in\mathbb{F}_q^\times \\ s\neq z^{-1}}} \eta_q^4(s) \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+zs)}} \eta_q(\gamma\cdot b) \\ &\quad + \eta_q^4(z^{-1}) \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+1)}} \eta_q\left(\frac{1-b+z^{-1}}{1-bz+z}\right) \\ &= A + B\end{aligned}$$

where A and B are set to be the two sums appearing in the previous line. We now

compute A and B. First we have

$$\begin{aligned} B &= \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+1)}} \eta_q^4(z^{-1})\eta_q\left(\frac{1-b+z^{-1}}{1-bz+z}\right) \\ &= \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+1)}} \eta_q\left(\frac{z-bz+1}{1-bz+z}\right) && (\eta_q^4(z^{-1})=\eta_q(z)) \\ &= \sum_{\substack{b\in\mathbb{F}_q \\ b\neq(z^{-1}+1)}} 1 \\ &= q-1. \end{aligned}$$

Now we compute A. Since in this case the action of γ defines an automorphism of $\mathbb{P}^1(\mathbb{F}_q)$, and since $\gamma\cdot b$ runs over $\mathbb{F}_q-\{z^{-1}\}$ as b runs over $\mathbb{F}_q-\{z^{-1}+sz\}$ we see that

$$\begin{aligned} A &= \sum_{\substack{s\in\mathbb{F}_q^\times \\ s\neq z^{-1}}} \eta_q^4(s) \sum_{\substack{u\in\mathbb{F}_q \\ u\neq z^{-1}}} \eta_q(u) \\ &= (-\eta_q^4(z^{-1}))(-\eta_q(z^{-1})) && \text{(orthogonality relations for characters)} \\ &= 1 && (\eta_q^5=\varepsilon) \end{aligned}$$

Therefore, combining our calculations for A and B we see that

$$F_{1,q}^2 + F_{1,q^2} = 2(A+B) = 2q \tag{4.30}$$

finishing the proof. □

E. Example

In this section we illustrate with an example the result of the conjecture. Consider the smooth projective curve with affine model given by

$$\mathcal{C}_3 : y^5 = t^2(1-t)^3(1-3t)^2$$

over the finite field $\mathbb{F}_{11}$. $\mathcal{C}_3$ is a hyperelliptic curve of genus 4, and using Magma we can compute its zeta function. We have that

$$Z(\mathcal{C}_3/\mathbb{F}_{11}, T) = \frac{(121T^4 + 66T^3 + 26T^2 + 6T + 1)^2}{(1-T)(1-11T)}.$$

Therefore, after doing some algebra, we find the values of $a_{i,11}(3)$ for $i = 1, \ldots, 4$. Specifically, if $\zeta_5 := e^{2\pi i/5}$ we have

$$a_{1,11}(3) = a_{4,11}(3) = -4 - 2\zeta_5^2 - 2\zeta_5^3$$
$$a_{2,11}(3) = a_{3,11}(3) = -2 + 2\zeta_5^2 + 2\zeta_5^3.$$

On the other hand, consider the multiplicative character $\eta_{11} \in \widehat{\mathbb{F}_{11}^\times}$ defined by $\eta_{11}(a) := \zeta_5$, where a is a primitive element of $\mathbb{F}_{11}^\times$, i.e., a generates $\mathbb{F}_{11}^\times$, and recall that $F_{i,11}(3) = 11\,{}_2F_1[\eta_{11}^{3i}, \eta_{11}^{2i}; \varepsilon|3]$. Using Magma we get

$$F_{1,11}(3) = F_{4,11}(3) = 4 + 2\zeta_5^2 + 2\zeta_5^3$$
$$F_{2,11}(3) = F_{3,11}(3) = 2 - 2\zeta_5^2 - 2\zeta_5^3.$$

Hence

$$F_{i,11}(3) = -a_{i,11}(3) \quad \text{for all } i = 1, 2, 3, 4.$$

CHAPTER V

ADVANCES TOWARD THE GENERAL CASE

A. The Conjecture in Its Full Generality

Even though it is still work in progress to prove the conjecture in its full generality, some advances have already been made toward it. To show these advances is the purpose of this chapter.

Suppose now that l and q are odd primes, with $q \equiv 1 \pmod{l}$, and let $z \in \mathbb{F}_q \backslash \{0, 1\}$. Recall that our conjecture relates values of certain hypergeometric functions over $\mathbb{F}_q$ to counting points on certain curves over $\mathbb{F}_q$. Recall also, that the curves we are interested in are smooth projective curves of genus $l-1$ with affine model

$$\mathcal{C}_z^{(m,s)} : y^l = t^m(1-t)^s(1-zt)^m$$

where $1 \leq m, s < l$ are integers such that $m + s = l$. Now, as we mentioned in the previous chapter, Corollary A.4 in Chapter III states that the curves $\mathcal{C}_z^{(m,s)}$ have all the same number of points over every finite extension of $\mathbb{F}_q$ as (m, s) varies over all pairs of positive integers with $m + s = l$, hence they all have the same zeta function over $\mathbb{F}_q$. This, together with the fact that the hypergeometric functions that appear on the right hand side of equation (3.1) are the same for all these curves imply that it is enough to prove the conjecture for only one of them, say

$$\mathcal{C}_z^{1,l-1} : y^l = t(1-t)^{l-1}(1-zt). \tag{5.1}$$

Throughout this chapter, we will denote this curve by $\mathcal{C}_z$.

So, the question is: what results would be enough to know in order to prove the

conjecture for all primes l and q with $q \equiv 1 \pmod{l}$? Recall that, by equations (2.4) and (4.2) we have that

$$F_{1,q^n}(z) + F_{2,q^n}(z) + \cdots + F_{l-1,q^n}(z) = -\sum_{i=1}^{l-1}(\alpha_{i,q}^n(z) + \overline{\alpha_{i,q}^n}(z)) \tag{5.2}$$

where $F_{i,q^n}(z) = q^n\, {}_2F_1\left(\begin{array}{cc} \eta_{q^n}^i, & \eta_{q^n}^{i(l-1)} \\ & \varepsilon \end{array}\middle| z\right)$ with $\eta_{q^n} \in \widehat{\mathbb{F}_{q^n}^{\times}}$ a character of order l, and $\alpha_{i,q}(z)$ are the reciprocals of the roots of the zeta function of $\mathcal{C}_z$ over $\mathbb{F}_q$, i.e.,

$$Z(\mathcal{C}_z/\mathbb{F}_q;T) = \frac{(1-\alpha_{1,q}(z)T)(1-\overline{\alpha_{1,q}(z)}T)\cdots(1-\alpha_{l-1,q}(z)T)(1-\overline{\alpha_{l-1,q}(z)}T)}{(1-T)(1-qT)}.$$

From now on we will omit the dependency on z of the hypergeometric functions and the roots of the zeta function, therefore, we will denote $F_{i,q^n} := F_{i,q^n}(z)$ and $\alpha_{i,q} := \alpha_{i,q}(z)$. Also, as in the previous chapter, denote $a_{i,q} := \alpha_{i,q} + \overline{\alpha_{i,q}}$, for $i = 1, \cdots, l-1$. Since we want to relate the hypergeometric functions above with the values $a_{i,q}$, first we are going to express the values $\alpha_{i,q}^n + \overline{\alpha_{i,q}^n}$ in terms of $a_{i,q}$ and q. We have the following theorem:

Lemma A.1. For $\alpha \in \mathbb{C}$ such that $|\alpha| = \sqrt{q}$ denote $\alpha + \overline{\alpha} := a$, and let n be a non-negative integer. Then:

$$\alpha^n + \overline{\alpha}^n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^i\, T(n,i)\, q^i\, a^{n-2i} \tag{5.3}$$

where $T(0,0) := 2$, $T(n,0) := 1$ for $n > 0$ and

$$T(n,i) := \frac{n(n-i-1)!}{i!(n-2i)!}, \quad \text{for } n > 0,\ i \geq 0.$$

Proof. We will prove the result by induction on n. For $n = 0$ and $n = 1$ is clear. Now suppose the result is true for all $k \leq n$. We want to show then that is also true

for $n+1$. Notice that

$$\begin{aligned}(\alpha^n+\overline{\alpha}^n)(\alpha+\overline{\alpha}) &= \alpha^{n+1}+\overline{\alpha}^{n+1}+\alpha^n\overline{\alpha}+\overline{\alpha}^n\alpha \\ &= \alpha^{n+1}+\overline{\alpha}^{n+1}+\alpha\overline{\alpha}(\alpha^{n-1}+\overline{\alpha}^{n-1}) \\ &= \alpha^{n+1}+\overline{\alpha}^{n+1}+q(\alpha^{n-1}+\overline{\alpha}^{n-1}) \qquad (\alpha\overline{\alpha}=q)\end{aligned}$$

Hence, since $a=\alpha+\overline{\alpha}$, we have

$$\alpha^{n+1}+\overline{\alpha}^{n+1} = (\alpha^n+\overline{\alpha}^n)\,a - q\,(\alpha^{n-1}+\overline{\alpha}^{n-1}). \tag{5.4}$$

Combining equation (5.4) and the inductive hypothesis we have

$$\begin{aligned}\alpha^{n+1}+\overline{\alpha}^{n+1} &= \sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\,T(n,i)\,q^i\,a^{n+1-2i} - \sum_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}(-1)^i\,T(n-1,i)\,q^{i+1}\,a^{n-1-2i} \\ &= a^{n+1}+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\,T(n,i)\,q^i\,a^{n+1-2i} \\ &\qquad - \sum_{j=1}^{\lfloor\frac{n-1}{2}\rfloor+1}(-1)^{j-1}\,T(n-1,j-1)\,q^j\,a^{n+1-2j} \qquad (5.5)\end{aligned}$$

after breaking apart the $i=0$ contribution in the first sum, and making the change of variables $i+1=j$ in the second sum.

Now we separate in two cases.

- Case 1: n is even.

  Notice that, in this case we have that $\lfloor\frac{n}{2}\rfloor = \lfloor\frac{n-1}{2}\rfloor + 1$. Then, equation (5.5) becomes

$$\begin{aligned}\alpha^{n+1}+\overline{\alpha}^{n+1} = a^{n+1}+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}(-1)^i\left(\frac{n}{i!(n-2i)!}+\frac{(n-1)}{(i-1)!(n+1-2i)!}\right) \\ \cdot\,(n-1-i)!\,q^i\,a^{n+1-2i}\end{aligned}$$

$$= a^{n+1} + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \, T(n+1,i) \, q^i \, a^{n+1-2i}$$
$$= \sum_{i=0}^{\lfloor \frac{n+1}{2} \rfloor} (-1)^i \, T(n+1,i) \, q^i \, a^{n+1-2i}$$

after replacing $T(n,k)$ by its definition, doing some algebra, and noticing that, if n is even then $\lfloor \frac{n}{2} \rfloor = \lfloor \frac{n+1}{2} \rfloor$. This proves the lemma for n even.

- Case 2: n is odd.

  In this case we have $\lfloor \frac{n}{2} \rfloor = \lfloor \frac{n-1}{2} \rfloor$ and $\lfloor \frac{n+1}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + 1$. Combining these, breaking apart the contribution of $i = \lfloor \frac{n}{2} \rfloor + 1$ in the second sum, and using the previous computation, equation (5.5) becomes

$$\alpha^{n+1} + \overline{\alpha}^{n+1} = a^{n+1} + \sum_{i=1}^{\lfloor \frac{n+1}{2} \rfloor - 1} (-1)^i \, T(n+1,i) \, q^i \, a^{n+1-2i}$$
$$+ (-1)^{\lfloor \frac{n+1}{2} \rfloor} \frac{(n-1)(n-1-\lfloor \frac{n+1}{2} \rfloor)!}{(\lfloor \frac{n+1}{2} \rfloor) - 1)!(n+1-2\lfloor \frac{n+1}{2} \rfloor)!} \, q^{\lfloor \frac{n+1}{2} \rfloor} \, a^{n+1-2\lfloor \frac{n+1}{2} \rfloor}.$$

  To finish the proof, we need to see that

$$\frac{(n-1)(n-1-\lfloor \frac{n+1}{2} \rfloor)!}{(\lfloor \frac{n+1}{2} \rfloor) - 1)!(n+1-2\lfloor \frac{n+1}{2} \rfloor)!} = T(n+1, \lfloor \frac{n+1}{2} \rfloor). \tag{5.6}$$

  This is not a hard computation. Write $n = 2m+1$ for some $m \in \mathbb{N}$, then $\lfloor \frac{n+1}{2} \rfloor = m+1$. Substituting this in equation (5.6) we get $2 = 2$ finishing the proof for n odd.

□

Now, equation (5.2) and Lemma A.1 allow us to relate explicitly the hypergeometric functions with the traces of Frobenius, giving

$$F_{1,q^n} + F_{2,q^n} + \cdots + F_{l-1,q^n} = -\sum_{i=1}^{l-1} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^j \, T(n,j) \, q^j \, a_{i,q}^{n-2j}. \tag{5.7}$$

Since in Conjecture B.1 we want to prove that $F_{i,q} = -a_{i,q}$ for all $i = 1, \ldots, l-1$, then we have the following result.

Proposition A.2. *If for all $i, n = 1, \ldots, l-1$ we have that*

$$F_{i,q^n} = (-1)^{n+1} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^j \, T(n,j) \, q^j \, F_{i,q}^{n-2j} \tag{5.8}$$

then Conjecture B.1 is true.

Proof. Assume equation (5.8) is true. Then, substituting into equation (5.7) for $n = 1, \ldots, l-1$ we get a system of equations relating sums of the hypergeometric functions $F_{i,q}$ and their powers to sums of the traces of Frobenius $a_{i,q}$ and their powers. After simplifying this system of equations, we get an equivalent one of the form

$$\begin{cases} F_{1,q} + F_{2,q} + \cdots + F_{l-1,q} = -(a_{1,q} + a_{2,q} + \cdots + a_{l-1,q}) \\ F_{1,q}^2 + F_{2,q}^2 + \cdots + F_{l-1,q}^2 = a_{1,q}^2 + a_{2,q}^2 + \cdots + a_{l-1,q}^2 \\ \qquad\qquad\qquad\qquad \vdots \\ F_{1,q}^n + F_{2,q}^n + \cdots + F_{l-1,q}^n = (-1)^n (a_{1,q}^n + a_{2,q}^n + \cdots + a_{l-1,q}^n) \\ \qquad\qquad\qquad\qquad \vdots \\ F_{1,q}^{l-1} + F_{2,q}^{l-1} + \cdots + F_{l-1,q}^{l-1} = a_{1,q}^{l-1} + a_{2,q}^{l-1} + \cdots + a_{l-1,q}^{l-1}. \end{cases} \tag{5.9}$$

This fact can be seen by induction. For $n = 1$ there is nothing to prove. Suppose now that $F_{1,q}^k + F_{2,q}^k + \cdots + F_{l-1,q}^k = (-1)^k (a_{1,q}^k + a_{2,q}^k + \ldots + a_{l-1,q}^k)$ for all $k < n$. Now,

by equation (5.8) we have

$$\begin{aligned} F_{1,q^n} + \cdots + F_{l-1,q^n} &= (-1)^{n+1} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^j \, T(n,j) \, q^j \, \left(F_{1,q}^{n-2j} + \cdots + F_{l-1,q}^{n-2j} \right) \\ &= (-1)^{n+1} (F_{1,q}^n + \cdots + F_{l-1,q}^n) \\ &\quad + (-1)^{n+1} \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^j \, T(n,j) \, q^j \, \left(F_{1,q}^{n-2j} + \cdots + F_{l-1,q}^{n-2j} \right) \\ &= (-1)^{n+1} (F_{1,q}^n + \cdots + F_{l-1,q}^n) \\ &\quad + (-1)^{n+1} \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^{n-j} \, T(n,j) \, q^j \, \left(a_{1,q}^{n-2j} + \cdots + a_{l-1,q}^{n-2j} \right) \end{aligned} \tag{5.10}$$

where the last equality follows from the inductive hypothesis.

On the other hand, by breaking apart the contribution of $j = 0$ in equation (5.7) we have

$$F_{1,q^n} + \cdots + F_{l-1,q^n} = -(a_{1,q}^n + \ldots + a_{l-1,q}^n) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^{j+1} \, T(n,j) \, q^j \, (a_{1,q}^{n-2j} + \ldots + a_{l-1,q}^{n-2j}). \tag{5.11}$$

Therefore, combining equations (5.10) and (5.11) and noticing that $(-1)^{2n+1-j} = (-1)^{j+1}$ we get

$$F_{1,q}^n + \cdots + F_{l-1,q}^n = (-1)^n \left(a_{1,q}^n + \ldots + a_{l-1,q}^n \right)$$

as desired.

Next, by using the Newton-Girard formulas, which give relations between elementary symmetric polynomials and power sums, we see that the system (5.9) is equivalent

to

$$\begin{cases} F_{1,q} + \cdots + F_{l-1,q} = -(a_{1,q} + a_{2,q} + \cdots + a_{l-1,q}) \\ \sum_{1 \le i < j \le l-1} F_{i,q}F_{j,q} = \sum_{1 \le i < j \le l-1} a_{i,q}a_{j,q} \\ \vdots \\ F_{1,q} \dots F_{l-1,q} = a_{1,q} \dots a_{l-1,q} \end{cases}$$

i.e., the elementary symmetric polynomials in the variables $F_{1,q}, \dots, F_{l-1,q}$ equal (up to a sign) the elementary symmetric polynomials in $a_{1,q}, \dots, a_{l-1,q}$. Then, we can think of these values as being roots of the same polynomial, therefore, after rearranging terms, we have that

$$F_{i,q} = -a_{i,q} \quad \text{for all } i = 1, \dots, l-1$$

and Conjecture B.1 follows. □

Remark A.3. Notice that it is enough to prove equation (5.8) only for prime powers of q, i.e., only for $1 \le n \le l-1$ with n prime. Otherwise, if $n = mr$ then $\mathbb{F}_{q^n} | \mathbb{F}_{q^m} | \mathbb{F}_q$ is a tower of extensions, and we can use the relation for these extensions of lower degree.

As we have seen above, proving equation (5.8) for prime powers of q would be enough to prove Conjecture B.1 in the general case. However, equation (5.8) gets complicated as n grows, so it would be helpful if this equation is needed for even fewer values of n in order to prove the conjecture. This might be possible; in fact, this is what we did to prove cases $l = 3$ and $l = 5$ in Chapter IV. Hence, looking at the proofs in previous chapter, we see that

Proposition A.4. *If the L-polynomial of the smooth projective curve of genus $l-1$ with affine model $\mathcal{C}_z : y^l = t(1-t)^{l-1}(1-zt)$ is a perfect square, and equation (5.8)*

is verified for all primes n such that $1 \leq n \leq (l-1)/2$, then Conjecture B.1 holds..

Proof. Recall that

$$L(\mathcal{C}_z/\mathbb{F}_q; T) = \prod_{i=1}^{l-1}(1 - a_{i,q}T + qT^2).$$

Hence, if the proposition is true, we would have

$$L(\mathcal{C}_z/\mathbb{F}_q; T) = \prod_{i=1}^{(l-1)/2}(1 - a_{i,q}T + qT^2)^2$$

therefore, after rearranging terms, we have $a_{i,q} = a_{l-i,q}$, for all $i = 1, \cdots, l-1$.
On the other hand, recall that by Corollary B.6 in Chapter II the hypergeometric functions $F_{i,q}$ come in pairs, i.e., $F_{i,q} = F_{l-i,q}$ for $i = 1, \cdots, l-1$. Hence, system (5.9) gets reduced to half of it, having only $(l-1)/2$ unknowns. Then, it is enough to prove relation (5.8) only for primes n up to $(l-1)/2$ in order to prove Conjecture B.1. □

Now, the question is how can we determine if the L-polynomial of $\mathcal{C}_z$ over $\mathbb{F}_q$ is a perfect square. One possible way is to do an argument similar to the one done for the cases $l = 3$ and $l = 5$. First, notice that we have the following result, analogous to Lemma C.1.

Theorem A.5. *The curve $\mathcal{C}_z : y^l = t(1-t)^{l-1}(1-zt)$ is birationally equivalent to*

$$\mathcal{C} : Y^2 = X^{2l} + 2(1-2z)X^l + 1. \tag{5.12}$$

Proof. The proof is analogous to the proof of Lemma C.1. □

Also, analogous to Lemma C.4, by considering the fractional linear transformation

$$X \to \frac{X+1}{X-1}$$
$$Y \to \frac{Y}{(X-1)^l}$$

we see that the curve (5.12) is equivalent to a curve of the form

$$Y^2 = c_l X^{2l} + c_{l-1} X^{2(l-1)} + \cdots + c_1 X^2 + c_0$$

with no terms of odd degree in X, where the coefficients c_i are polynomial equations in z. Then, as in previous chapter, we can conclude that the jacobian of $\mathcal{C}_z$ is isogenous to the product of the jacobians of two curves of genus $(l-1)/2$, call them $\mathcal{H}_{1,z}$ and $\mathcal{H}_{2,z}$. Therefore, by Proposition A.4, we have

Theorem A.6. *Let $q \equiv 1 \pmod{l}$. If $\#\mathcal{H}_{1,z}(\mathbb{F}_{q^i}) = \#\mathcal{H}_{2,z}(\mathbb{F}_{q^i})$ for all $i = 1, \ldots, (l-1)/2$, and equation (5.8) holds for all primes n such that $1 \leq n \leq (l-1)/2$, then Conjecture B.1 holds.*

Proof. Notice that the fact that $\#\mathcal{H}_{1,z}(\mathbb{F}_{q^i}) = \#\mathcal{H}_{2,z}(\mathbb{F}_{q^i})$ for all $i = 1, \ldots, (l-1)/2$ implies that the curves $\mathcal{H}_{1,z}$ and $\mathcal{H}_{1,z}$ have the same L-polynomial over $\mathbb{F}_q$, then, as we mentioned above, the system (5.9) gets reduced to half of it, having only $(l-1)/2$ unknowns. The rest of the proof follows from Proposition A.4. □

Remark A.7. Notice that, if Proposition A.2 holds (i.e. Conjecture B.1 is true over $\mathbb{F}_q$), using Lemma A.1 we can get a result similar to Conjecture B.1 over $\mathbb{F}_{q^n}$, for $n \in \mathbb{N}$.

CHAPTER VI

CONCLUSIONS AND FUTURE RESEARCH

The main objective of this dissertation is to find connections hypergeometric functions over finite fields have to algebraic curves. In particular, we focused our attention to a specific family of curves. For $a = m/n$ and $b = s/r$ rational numbers such that $0 < a, b < 1$, and $z \in \mathbb{F}_q$, $z \neq 0, 1$ we considered the smooth projective algebraic curve with affine equation

$$\mathcal{C}_z^{(a,b)} : y^l = t^{l(1-b)}(1-t)^{lb}(1-zt)^{la}$$

where $l := \operatorname{lcm}(n, r)$. If q is prime and $q \equiv 1 \pmod{l}$, we showed in Chapter III Theorem A.2, an explicit formula for the number of points on $\mathcal{C}_z^{(a,b)}$ over $\mathbb{F}_q$ in terms of sums of hypergeometric functions ${}_2F_1\left(\begin{array}{cc} \eta_q^{il(1-a)}, & \eta_q^{il(1-b)} \\ & \varepsilon \end{array} \middle| z\right)$, where $\eta_q \in \widehat{\mathbb{F}_q^\times}$ is a character of order l. Moreover, we showed that this result can be extended to any finite extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. Next, we restricted our attention to the family of curves $\mathcal{C}_z^{(a,b)}$ where $a = m/l$ and $b = s/l$ with l a prime and $m+s = l$, and showed, in Chapter III Corollary A.4 that, if $q \equiv 1 \pmod{l}$ and $\mathcal{C}_z^{(a,b)}$, $\mathcal{C}_z^{(a',b')}$ are two such curves, then

$$\#\mathcal{C}_z^{(a,b)}(\mathbb{F}_{q^k}) = \#\mathcal{C}_z^{(a',b')}(\mathbb{F}_{q^k})$$

for all $k \in \mathbb{N}$.

Then, in Chapter IV, we were interested in relating each particular hypergeometric function ${}_2F_1\left(\begin{array}{cc} \eta_q^{il(1-a)}, & \eta_q^{il(1-b)} \\ & \varepsilon \end{array} \middle| z\right)$ to the curve $\mathcal{C}_z^{(a,b)}$. We proved that we can relate explicitly each one of these hypergeometric functions to the roots of the zeta function of $\mathcal{C}_z^{(a,b)}$ over $\mathbb{F}_q$ for $q \equiv 1 \pmod{l}$ when $l = 3$, and in many cases when

$l = 5$. The proof of these results involved studying properties of the Jacobian variety associated to the curve together with relations between hypergeometric functions over finite fields and their extensions. Based on numerical computations, we conjectured that the previous relations between the hypergeometric functions and the roots of the zeta function of the curve over $\mathbb{F}_q$ hold for all prime l, and $q \equiv 1 \pmod{l}$, and this is the statement of Conjecture B.1 in Chapter IV. We are currently working on proving Conjecture B.1 in its full generality and some progress has already been made in this direction. These advances toward the general case are the content of Chapter V.

We plan to continue the work of the previous chapters to future research. Another project is to study what kind of relations, maybe similar to the ones presented in this dissertation, can be found in the case when $m + s$ is not a prime l. We have already started to investigate in this direction, and have collected some data that suggests there might be some relation between the values in this more general setting. For example, over $\mathbb{F}_{11}$, consider the curve with affine equation

$$\mathcal{C}_z : y^5 = t^2(1-t)^3(1-zt).$$

Notice that in this case we are considering $l = 5$ and $(m, s) = (1, 3)$ in Theorem A.2 of Chapter III, so $m + s \neq l$.

- In the case that $z = 2$ we obtain $a_{i,11}(2) = -3$ and $F_{i,11}(2) = 3$ for all $1 \leq i \leq 4$. This might mislead to think that the hypothesis of $m + s = l$ is not needed in Conjecture B.1. However, one more computation shows that this is not the case, as we see next.

- When $z = 6$, for $\zeta_5 := e^{2\pi i/5}$ a fifth root of unity, we obtain that

$$a_{1,11}(6) = 5 + \zeta_5 + \zeta_5^4 \quad , \quad a_{2,11}(6) = 5 + \zeta_5^2 + \zeta_5^3,$$

$$a_{3,11}(6) = -5 + \zeta_5^2 + \zeta_5^3 \quad , \quad a_{4,11}(6) = -5 + \zeta_5 + \zeta_5^4.$$

On the other hand, we get that

$$F_{1,11}(6) = 1 + \zeta_5 + \zeta_5^3 \quad , \quad F_{2,11}(6) = 1 + \zeta_5 + \zeta_5^2,$$

$$F_{3,11}(6) = 1 + \zeta_5^3 + \zeta_5^4 \quad , \quad F_{4,11}(6) = 1 + \zeta_5^2 + \zeta_5^4.$$

Manipulating these values we can have

$$F_{1,11}(6) = -\zeta_5^3(a_{1,11} - 5) \quad , \quad F_{2,11}(6) = -\zeta_5(a_{2,11} - 5),$$

$$F_{3,11}(6) = -\zeta_5^4(a_{3,11} + 5) \quad , \quad F_{4,11}(6) = -\zeta_5^2(a_{4,11} + 5).$$

As we can see in this example, the data suggests that some connection can be made between these values. However, it is more subtle than the case $m + s = l$.

In addition to these previous ongoing projects, the problem can be generalized even more, to finding relations when l in Chapter III Theorem A.2 is any composite number, and not necessarily a prime.

REFERENCES

[1] S. Ahlgren and K. Ono, "Modularity of a certain Calabi-Yau threefold," *Monatsh. Math.*, vol. 129, pp. 177-190, 2000.

[2] R. Askey, *Orthogonal Polynomials and Special Functions*. Philadelphia, PA: SIAM, 1975.

[3] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*. New York, NY: J. Wiley & Sons, Inc., 1998

[4] F. Beukers, "Algebraic values of G-functions," *J. Reine Angew. Math.*, vol. 434, pp. 45-65, 1993.

[5] J. W. S. Cassels, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Cambridge, UK: Cambridge University Press, London Mathematical Society Lecture Note Series 230, 1996.

[6] P. Deligne, "La conjecture de Weil," *Publ. Math. IHES*, vol. 43, pp. 273-307, 1974.

[7] B. Dwork, "On the rationality of the zeta function of an algebraic variety," *Amer. J. of Math.*, vol. 82, pp. 631-648, 1960.

[8] S. Frechette, K. Ono, and M. Papanikolas, "Gaussian hypergeometric functions and traces of Hecke operators," *Int. Math. Res. Not.*, pp. 3233-3262, 2004.

[9] W. Fulton, *Algebraic Curves, An Introduction to Algebraic Geometry*. New York, NY: W. A. Benjamin, Inc, 1969.

[10] J.G. Fuselier, "Hypergeometric functions over finite fields and relations to modular forms and elliptic curves," Ph.D. dissertation, Texas A&M University, 2007.

[11] J. Greene, "Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields," Ph.D. dissertation, University of Minnesota, 1984.

[12] J. Greene, "Hypergeometric functions over finite fields," *Trans. Amer. Math. Soc.*, vol. 301, pp. 77-101, 1987.

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York, NY: Springer-Verlag, 1990, 2nd. ed.

[14] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*. New York, NY: Springer-Verlag, 1993, 2nd. ed.

[15] M. Koike, "Hypergeometric series over finite fields and Apéry numbers," *Hiroshima Math. J.*, vol. 22, pp. 461-467, 1992.

[16] S. Lang, *Complex Multiplication*. New York, NY: Springer-Verlag, 1983.

[17] J. S. Milne, "Introduction to Shimura varieties" in *Harmonic analysis, the trace formula and Shimura varieties*. Cambridge, MA: Clay Math. Proc., vol. 4, pp. 265-378.

[18] D. Mumford, *Abelian Varieties*. Bombay, India: Tata Inst. Fund. Research and Oxford University Press, 1985, 2nd. ed.

[19] I. Niven, H.S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*. New York, NY: John Wiley & Sons, Inc., 1991, 5th. ed.

[20] K. Ono, "Values of Gaussian hypergeometric series," *Trans. Amer. Math. Soc.*, vol. 350, pp. 1205-1223, 1998.

[21] M. Papanikolas, "A formula and a congruence for Ramanujan's τ-function," *Proc. Amer. Math. Soc.*, vol. 134, pp. 333-341, 2006.

[22] R. Schoof, "Nonsingular plane cubic curves over finite fields," *J. Combin. Theory*, Ser. A vol. 46, pp. 183-211, 1987.

[23] J.H. Silverman, *The Arithmetic of Elliptic Curves*. New York, NY: Springer-Verlag, 1986.

[24] L. Slater, *Generalized Hypergeometric Functions*. Cambridge: Cambridge Univ. Press, 1966.

[25] P.F. Stiller, "Classical automorphic forms and hypergeometric functions," *J. Number Theory*, vol. 28, pp. 219-232, 1988.

[26] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields," *Proc. Symp. Pure Math.*, vol. 20, pp. 53-64, 1971.

[27] A. Weil, "Number of solutions of equations in finite fields," *Bull. AMS*, vol. 55, pp. 497-508, 1949.

[28] C. Xing, "Zeta-functions of curves of genus 2 over finite fields," *Journal of Algebra*, vol. 308, pp. 734-741, 2007.

VITA

Name: María Valentina Vega Veglio

Education:

- Ph.D. in Mathematics, Texas A&M University, College Station, 2009
- M.S. in Mathematics, Texas A&M University, College Station, 2006
- B.S. in Mathematics, Universidad de la República, Montevideo, Uruguay, 2004

Address: Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, TX 77843-3368

e-mail: vvega@math.tamu.edu