COVERS AND INVARIANTS OF DELIGNE-LUSZTIG CURVES

BY

DANE SKABELUND

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2018

Urbana, Illinois

Doctoral Committee:

Professor Scott Ahlgren, Chair
Professor Iwan Duursma, Director of Research
Professor Thomas Nevins
Assistant Professor Patrick Allen

Abstract

This thesis is comprised of three parts, each dealing with one or more of the Hermitian, Suzuki, and Ree curves, which are three families of algebraic curves over finite fields which have pronounced arithmetic and geometric properties.

In the first part, we use a ray class field construction to produce covers of each of these three families of curves which meet the Hasse-Weil bound over suitable base fields. In the Hermitian case, the family of covers constructed coincide with the family of Giulietti-Korchmáros curves.

In the second part, we study a certain linear series $\mathcal{D}$ on the Ree curve which gives an embedding in $\mathbb{P}^{13}$. We compute the orders of vanishing of sections of $\mathcal{D}$, and use this to determine the set of Weierstrass points of $\mathcal{D}$.

The third part is a computational project studying the structure of the 3-torsion group scheme of the Jacobian of the smallest Ree curve, which has genus 3627. This is accomplished by computing the action of the Frobenius and Verschiebung operators on the de Rham cohomology of the curve. As a result, we determine the Ekedahl-Oort type and a decomposition for the Dieudonné module of this curve.

For Marta, Merryweather, Thomas, and ?.

Acknowledgments

Thanks to the Mathematics Department for five years of generous support and to my advisor Iwan Duursma for all his teaching and encouragement over the past several years. I have learned so much from him, and from my other professors and fellow graduate students.

Thanks also to Sue Wood, chimesmaster of the Altgeld Memorial Chime, for welcoming me into a rich tradition of chiming at Illinois and for her example of a life filled with quiet service.

Most of all, thanks to my wife Melinda for coming with me to the midwest to raise our family and for tolerating my “other woman”, mathematics. During our time here, the only things I have done which were of true importance were at home.

Table of Contents

1 Introduction

This thesis is a compilation of three projects, each dealing with specific families of curves which have many points over finite fields. All the curves studies are related in some way to one of the three families of Deligne-Lusztig curves, namely the Hermitian, Suzuki and Ree curves. These curves have received attention for their extreme arithmetic and geometric properties, in particular for the size of their automorphism groups and large number of $\mathbb{F}_q$-rational points relative to their genus. These properties make them interesting mathematically, and useful for creating error-correcting codes with desirable parameters.

We describe here the general outline of the three parts of the thesis. Since the topics of Chapters 3-5 are relatively distinct, however, more thorough introductions are included at the beginning of each chapter. Some background material which is common to all three parts is collected in Chapter 2.

The first project, contained in Chapter 3, deals with covers of the Hermitian, Suzuki, and Ree curves which meet the Hasse-Weil bound. The work in this chapter was motivated by the desire to better understand a family of curves constructed by Giulietti and Korchmáros. It is shown in this chapter that the function field of the Giulietti-Korchmaros curve may be realized as a ray class field over the function field of the Hermitian curve. Moreover, similar extensions of function fields of the Suzuki and Ree curves are constructed and shown to meet the Hasse-Weil bound.

The second two projects involve computing certain geometric invariants of the Ree curves. The originally intended purpose for the work done in Chapter 4 was to obtain a characterization the Ree curve as the only smooth projective curve of its genus defined over $\mathbb{F}_q$ with a certain number of $\mathbb{F}_q$-rational points. This seemed like a natural problem to pursue, as similar characterizations may be shown to hold for the Hermitian and Suzuki curves by using the theory of Stöhr and Voloch. This problem seems difficult, but as a first step in this direction I compute in this chapter the Frobenius orders of a certain linear series on the curve. These are the same invariants which were used to complete the characterization of the Suzuki curve.

The impetus for the work in Chapter 5 was a desire to find an obstruction for covers of the curves found in Chapter 3 by other curves which are known to meet the Hasse-Weil bound. In hindsight, however, I believe that it is more interesting for its own sake than for the intended application. This chapter details a computation of the structure of the de Rham cohomology of the smallest Ree curve, which has genus 3627, as a module under the Frobenius and Verschiebung operators. This is isomorphic to the 3-torsion group scheme of the Jacobian of the curve. This project was motivated by similar work done by Malmskog, Pries, and Weir for the Hermitian and Suzuki curves.

2 Preliminaries

We will assume familiarity with definitions related to algebraic curves and their functions fields which may be found, for example, in [Sti2]. In this chapter, we collect certain facts and results which will be used often in the following chapters. Any background which is specific to a single chapter may be found there.

2.1 Curves and zeta functions

Let X be a smooth, geometrically irreducible, projective algebraic curves defined over a finite field $\mathbb{F}_q$. The *zeta function of X over $\mathbb{F}_q$*, which is given by the power series

$$Z_X(t) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} t^n\right),$$

keeps track of the number of points on X over each finite extension of $\mathbb{F}_q$. Although not obvious from this definition, the function $Z_X(t)$ is a rational function of the form

$$Z_X(t) = \frac{L_X(t)}{(1-t)(1-qt)}.$$

where $L_X(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$. The numerator

$$L_X(t) = (1-t)(1-qt)Z_X(t) = \prod_{j=1}^{2g}(1-\alpha_j t)$$

is called the L-polynomial of X. The following theorem is the analogue of the Riemann hypothesis for curves over finite fields.

Theorem 2.1 (Hasse-Weil Theorem). *The reciprocal roots α_j of $L_X(t)$ satisfy $|\alpha_j| = \sqrt{q}$.*

Unfolding the definitions of $Z_X(t)$ and $L_X(t)$ yields the following formula for the number of points over various extensions of $\mathbb{F}_q$ in terms of the reciprocal roots α_j.

$$\#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} \alpha_j^n \tag{2.1}$$

In this context, the Hasse-Weil Theorem says that

$$q^n + 1 - 2gq^{n/2} \leq \#X(\mathbb{F}_{q^n}) \leq q^n + 1 + 2gq^{n/2}.$$

This is called the Hasse-Weil bound.

The reciprocal of the L-polynomial ,

$$t^{2g}L(1/t) = \prod_{j=1}^{2g}(t - \alpha_j),$$

is the characteristic polynomial of the Frobenius Fr_q acting on the Tate module $T_\ell(\mathrm{Jac}(X))$ [Mum, page 205], making the roots α_j the eigenvalues of this action.

Theorem 2.2 (Riemann-Roch)**.** *Let X be a curve of genus g, and D a divisor on X, and K a canonical divisor on X. Then*

$$\dim L(D) - \dim L(K - D) = d + 1 - g.$$

In particular, if $\deg D > 2g - 2$ *then* $\dim L(D) = d + 1 - g$.

Theorem 2.3 (Hurwitz formula)**.** *If $f\colon X \to Y$ is a finite separable morphism of curves, then*

$$2g_X - 2 = \deg(f) \cdot (2g_Y - 2) + \deg R,$$

where R is the ramification divisor of f.

The ramification divisor R is the same as the different ideal of the extension of function fields induced by f, which may be calculated in terms of ramification groups if the extension is Galois [Sti2, chapter 3], [Ser, chapter 4].

2.2 Hasse-Weil maximal curves

A curve X defined over a finite field $\mathbb{F}_q$ is called *maximal over* $\mathbb{F}_q$, or $\mathbb{F}_q$-*maximal*, if it meets the Hasse-Weil upper bound for the number of $\mathbb{F}_q$-rational points for its genus, that is, if

$$\#X(\mathbb{F}_q) = q + 1 + 2g_X q^{1/2}.$$

Interest in studying these curves was sparked in the 1980s by their application in the theory of algebraic geometry codes. By (2.1), a curve X is maximal over $\mathbb{F}_q$ if and only if each $\alpha_j = -\sqrt{q}$, so that the L-polynomial of X over $\mathbb{F}_q$ is of the form $L_X(t) = (1 + \sqrt{q}t)^{2g}$. In other words, for an $\mathbb{F}_q$-maximal curve the Frobenius acts as multiplication by $-\sqrt{q}$ on the $\mathbb{F}_q$-rational points of $\mathrm{Jac}(X)$, so that $\mathrm{Jac}(X)(\mathbb{F}_q) \cong (\mathbb{Z}/(\sqrt{q}+1)\mathbb{Z})^{2g}$.

In light of this, the following proposition[1] implies that if X is maximal over $\mathbb{F}_q$ and $X \to Y$ is a covering, that Y is also maximal over $\mathbb{F}_q$.

Proposition 2.4 ([AP, Prop 5])**.** *If $X \to Y$ is a finite morphism between two reduced absolutely irreducible smooth projective algebraic curves defined over $\mathbb{F}_q$, then $L_Y(t)$ divides $L_X(t)$ in $\mathbb{Z}[t]$.*

Therefore, the set of $\mathbb{F}_q$-maximal curves, taken up to isomorphism, form a partially ordered set induced by coverings between curves. This motivates the following questions.

- What are the maximal elements of this partially ordered set?
- For fixed q, which g appear as genera of $\mathbb{F}_q$-maximal curves?

The following bound for the genus of a maximal curve follows from (2.1).

Theorem 2.5 ([Iha])**.** *The genus of a curve maximal over $\mathbb{F}_q$ is bounded by*

$$g \leq \frac{\sqrt{q}(\sqrt{q}-1)}{2}.$$

As this bound is attained by the Hermitian curve $H = H_{\sqrt{q}}$ defined by

$$y^{\sqrt{q}} + y = x^{\sqrt{q}+1},$$

[1] In the literature this result is often attributed to Serre (see [Lac, Prop 6]), although I cannot find anywhere where he wrote it down. It is true in much greater generality [Kle, Prop 1.2.4].

the curve H is an example of an $\mathbb{F}_q$-maximal curve which is not covered by any other $\mathbb{F}_q$-maximal curve.

The following theorem characterizing $\mathbb{F}_q$-maximal curves is often referred to in the area as the Natural Embedding Theorem.

Theorem 2.6 ([KT]). *A smooth geometrically irreducible projective curve is maximal over $\mathbb{F}_q$ if and only if it admits an embedding as a curve of degree $\sqrt{q}+1$ on a non-degenerate Hermitian variety defined over $\mathbb{F}_q$.*

Here *Hermitian variety* refers to a projective hypersurface defined by the vanishing of

$$\sum_{0\leq i,j\leq n} a_{ij} X_i^{\sqrt{q}} X_j,$$

for some matrix $A = [a_{ij}]$ defined over $\mathbb{F}_q$ satisfying $A^t = A^\alpha$, where α is the involutive automorphism of $\mathbb{F}_q$ sending $\alpha \mapsto \alpha^{\sqrt{q}}$.

2.3 Deligne-Lusztig curves

There are three particular families of curves which will be of particular interest in this thesis, namely the Hermitian, Suzuki and Ree curves. These three families arise as projectivizations of the Deligne-Lusztig varieties associated to the simple groups of type ${}^2A_2$, ${}^2B_2$, and ${}^2G_2$ [DL]. This is not the main perspective we will take on these curves however, in favor of dealing concrete models which were given for them in years following their more abstract origins [Hen], [HS], [Ped]. For those interested, however, an introduction to these curves considered as Deligne-Lusztig curves may be found in [Han].

While the Hermitian curves exist in all characteristics, the Suzuki and Ree curves are defined only in characteristic 2 and 3, respectively. Each has an optimal number of $\mathbb{F}_q$-rational points for its genus, and becomes maximal over a suitable extension of the base field. These three families curves have extremely large automorphism groups, of the size that cannot occur in characteristic zero because of the Hurwitz bound $\#\operatorname{Aut}(G) \leq 84(g-1)$. The Hermitian and Suzuki curves, along with two specific hyperelliptic curves, are the only curves of genus $g \geq 2$ satisfying $\#\operatorname{Aut}(X) \geq 8g^3$. More similar results may be found in [HKT, chapter 12], [Sti1], [GK1].

The Hermitian curve $H = H_{q_0}$ is defined by

$$y^{q_0} + y = x^{q_0+1},$$

where q_0 is a prime power. The curve H_{q_0} has genus $\frac{1}{2}q_0(q_0 - 1)$ and $q_0^3 + 1$ points defined over $\mathbb{F}_q$, where $q = q_0^2$, so that H_{q_0} is maximal over $\mathbb{F}_q$. As mentioned in the previous section, this is the largest genus that a curve maximal over $\mathbb{F}_q$ may have. The curve H_{q_0} has automorphism group $\mathrm{PGU}(3, q_0)$, which has order $q_0^3(q_0^3 + 1)(q - 1)$ and acts doubly transitively on the $\mathbb{F}_q$-rational points of H_{q_0}.

For $q = 2q_0^2$ an odd power of 2, the Suzuki curve S has an affine model

$$y^q + y = x^{q_0}(x^q + x).$$

The curve S has genus $q_0(q-1)$ and q^2+1 points defined over $\mathbb{F}_q$, which are permuted doubly transitively by the automorphism group $\mathrm{Sz}(q)$, which has order $q^2(q^2 + 1)(q - 1)$. The zeta function of S is

$$Z_S(t) = \frac{(1 + 2q_0t + qt^2)^g}{(1 - t)(1 - qt)},$$

from which it may be seen that S becomes maximal over the field $\mathbb{F}_{q^4}$.

For $q = 3q_0^2$ an odd power of 3, the Ree curve R has an affine model

$$y^q - y = x^{q_0}(x^q - x) \qquad z^q - z = x^{q_0}(y^q - y).$$

The curve R has genus $\frac{3}{2}q_0(q-1)(q+q_0+1)$ and q^3+1 points defined over $\mathbb{F}_q$, which are permuted doubly transitively by the automorphism group $\mathrm{Ree}(q)$ of size $q^3(q^3 + 1)(q - 1)$.

$$Z_R(t) = \frac{(1 + 3q_0t + qt^2)^{q_0(q^2-1)}(1 + qt^2)^{\frac{1}{2}q_0(q-1)(q+3q_0+1)}}{(1 - t)(1 - qt)}$$

from which it follows that the Ree curve becomes maximal over the field $\mathbb{F}_{q^6}$.

The Ree curve admits a smooth embedding in $\mathbb{P}^{13}$, as has been shown independently in [Kan1] and [ED]. The embedding in [Kan1] arises from the description of the curve as a Deligne-Lusztig variety. The embedding in [ED] uses the 14 functions $1, x, y, z, w_1, w_2, \dots, w_{10}$, where the w_i satisfy

$$\begin{aligned} w_1 &= x^{3q_0+1} - y^{3q_0} & w_6 &= xw_4^{3q_0} - w_2^{3q_0} - w_1 z^{3q_0} + w_3 x^{3q_0} \\ w_2 &= xy^{3q_0} - z^{3q_0} & w_7 &= w_2 + xw_3^{q_0} - zw_1^{q_0} \\ w_3 &= xz^{3q_0} - w_1^{3q_0} & w_8 &= w_5^{3q_0} + xw_7^{3q_0} \\ w_4 &= xw_2^{q_0} - yw_1^{q_0} & w_9 &= w_4 w_2^{q_0} - yw_6^{q_0} \\ w_5 &= yw_3^{q_0} - zw_1^{q_0} & w_{10} &= zw_6^{q_0} - w_3^{q_0} w_4. \end{aligned} \tag{2.2}$$

In [ED], a system of 105 symmetrical equations of degrees 2, $q_0 + 1$, and $3q_0 + 1$ is determined which cuts out the image of this embedding.

3 New maximal curves as ray class fields

For many years it was unknown whether there exists an $\mathbb{F}_q$-maximal curve which is not covered by the Hermitian curve $H_{\sqrt{q}}$ [Gar], [TVN, Problem 3.4.9]. An example was found by Garcia and Stichtenoth of a curve maximal over $\mathbb{F}_{27^2}$ which is not Galois-covered by H_{27} [GS]. Around the same time, an unpublished computation of Rains and Zieve demonstrated that the smallest Ree curve, which is also maximal over $\mathbb{F}_{27^2}$, is not Galois-covered by H_{27}. A recent paper of Montanucci and Zini verifies the result of this computation, and in addition proves the analogous result for the smallest Suzuki curve [MZ]. Whether any of these curves are images of the Hermitian curve, however, remains unknown.

In 2008, Giulietti and Korchmáros answered the question positively with their discovery of a new family of curves [GK2]. For $q = q_0^2$ a prime power, the *Giulietti-Korchmáros curve* or *GK-curve* $\widetilde{H} = \widetilde{H}_q$ is maximal over $\mathbb{F}_{q^3}$, but does not admit any covering by the Hermitian curve $H_{q_0^3}$ for $q_0 \geq 3$. To this point, this is the only family of maximal curves which have been proven not to be images of the Hermitian curve. The fact that $\widetilde{H}$ is not covered by the Hermitian curve follows from the Hurwitz formula and the Hasse-Weil bound, which in combination imply that any curve X maximal over $\mathbb{F}_q$ which is covered by the Hermitian curve $H_{\sqrt{q}}$ has genus satsifying

$$\frac{q^{3/2}+1}{q+1+2g_X q^{1/2}} \leq \left\lfloor \frac{q-q^{1/2}-2}{2g_X-2} \right\rfloor .$$

The GK-curve was discovered while searching for maximal curves with large automorphism groups, as described in [GK2]. From the Natural Embedding Theorem (Theorem 2.6), they knew that any maximal curve must lie on a Hermitian variety, and considered a Hermitian surface $\mathcal{H} \subset \mathbb{P}^3$, along with a Hermitian cone $\mathcal{C}$ through a point not lying in $\mathcal{H}$ which is stable un-

The results in this chapter appear in the paper [Ska2].

der a large subgroup of automorphisms of $\mathcal{H}$. The complete intersection of $\mathcal{H}$ and $\mathcal{C}$ breaks into several curves which are permuted transitively by the automorphisms of $\mathcal{H}$, and each of these is isomorphic to a copy of the GK curve.

In section 3.2 we provide an alternate construction for the GK-curve as arising as a ray class field. This was inspired by the following theorem of Lauter, who gave the following uniform description of the Deligne-Lusztig curves as ray class fields.

Theorem 3.1 ([Lau])**.** *The function fields of the Hermitian, Suzuki, and Ree curves are isomorphic to the ray class fields of conductor $D = k(\infty)$ in which all places of degree one different from (∞) of $\mathbb{F}_q(x)$ split completely, where*

$$k = \begin{cases} p^f + 2 & \text{if } q = p^{2f} \\ 2^f + 2 & \text{if } q = 2^{2f+1} \\ 3^f + 3 & \text{if } q = 3^{2f+1}. \end{cases}$$

Rather than arising as a ray class field over $\mathbb{F}_q(x)$, the function field of the GK-curve $\widetilde{H}$ lives over a constant field extension of the function field of a Hermitian curve. Thus, $\widetilde{H}$ may be considered as arising via a two-step ray class field contruction over $\mathbb{P}^1$. First, apply the construction of Lauter, which allows one $\mathbb{F}_q$-rational point to ramify and splits all other $\mathbb{F}_q$-rational points. Then extend the base field before taking another ray class field in which the $\mathbb{F}_q$-rational points are allowed to ramify tamely, while all other points rational over the new base field are caused to split.

This description of $\widetilde{H}$ admits a natural analogue in the case of the Suzuki and Ree curves, which we explore in sections 3.3–3.5. In sections 3.3 and 3.4 we introduce cyclic covers $\widetilde{S}$ and $\widetilde{R}$ of the Suzuki and Ree curves analogous to $\widetilde{H}$, and show that these are maximal over a suitable base field by providing explicit embeddings of these curves in Hermitian varieties in $\mathbb{P}^4$ and $\mathbb{P}^7$. The results in section 3.5 deal with all three Deligne-Lusztig curves simultaneously. For X one of the Hermitian, Suzuki, or Ree curves, we show that $\widetilde{X}$ is is a subcover of a ray class field extension X_{rcf}, and use the maximality of $\widetilde{X}$ to prove that of X_{rcf}. We then show that the cover $X_{\text{rcf}} \to X$ is cyclic of a prescribed form, which allows use to verify computationally that $X_{\text{rcf}} = \widetilde{X}$ for small values of q. We are unable to say whether $X_{\text{rcf}} = \widetilde{X}$ in general, but we give a bound on the degree of the cover $X_{\mathrm{rcf}} \to \widetilde{X}$.

3.1 The Deligne-Lusztig Curves

In this section we collect some facts about the Deligne-Lusztig curves in addition to those in section 2.3 which will be used in this chapter. In particular, we note that the Hermitian, Suzuki, and Ree curves have exactly two short orbits under the action of their full automorphism group, each consisting of all points of certain degrees. These orbits form the sets of points which ramify and split in the covers discussed in sections 3.2–3.4. The results in this section should be well known; we include proofs of some statements for the sake of completeness.

A point of a curve X is fixed by some automorphism of X exactly if it is ramified in the quotient by the full automorphism group. Thus, the Riemann-Hurwitz formula may be applied to the cover $X \to X/\operatorname{Aut}(X)$ to study these points. For G a finite subgroup of automorphisms of X, this formula may be written in the form

$$2g(X) - 2 = \#H \left(2g(X/G) - 2 + \sum_{\mathfrak{p} \in X/G} \frac{d(\mathfrak{p})}{e(\mathfrak{p})} \deg \mathfrak{p} \right),$$

where $d(\mathfrak{p})$ and $e(\mathfrak{p})$ are the different exponent and ramification index of $\mathfrak{p}$ in $X \to X/G$.

3.1.1 The Hermitian Curve

Let $q = q_0^2$ be a prime power. The Hermitian curve $H = H_{q_0}$ has an affine plane model defined by

$$y^{q_0} + y = x^{q_0+1}.$$

It has genus $q_0(q_0-1)/2$ and is maximal over $\mathbb{F}_q$, with $\#X(\mathbb{F}_q) = q^{3/2}+1$. Its automorphism group $\mathrm{PGU}(3, q_0)$ is of size $(q^{3/2}+1)q^{3/2}(q-1)$.

Proposition 3.2 ([GSX]). *The Hermitian curve H_{q_0} has exactly two short orbits under the action of its full automorphism group. One is non-tame of size $q^{3/2}+1$, consisting of the $\mathbb{F}_q$-rational points. The other is tame of size $\frac{1}{3}q^{3/2}(q-1)(q_0+1)$, consisting of all points of degree 3.*

3.1.2 The Suzuki Curve

For $s \geq 1$ and $q = 2q_0^2 = 2^{2s+1}$, the Suzuki curve $S/\mathbb{F}_q$ has an affine model defined by

$$y^q + y = x^{q_0}(x^q + x)$$

and has genus $q_0(q-1)$. Its automorphism group $\mathrm{Sz}(q)$, which has size $(q^2+1)q^2(q-1)$, acts doubly transitively on the q^2+1 rational points. The Suzuki curve is maximal over $\mathbb{F}_{q^4}$.

Proposition 3.3. *The Suzuki curve has exactly two short orbits under the action of its full automorphism group. One is non-tame of size q^2+1, consisting of the $\mathbb{F}_q$-rational points. The other is tame of size $\frac{1}{4}q^2(q-1)(q+2q_0+1)$, consisting of all points of degree 4.*

Proof. The automorphism group $G = \mathrm{Sz}(q)$ transitive on the q^2+1 points of $S(\mathbb{F}_q)$ with point stabilizer of order $q^2(q-1)$. Fix a rational point $\mathfrak{P}_\infty$ on S lying above a point $\mathfrak{p}_\infty$ in $S/G \cong \mathbb{P}^1$. Then

$$\#G_\infty = e(\mathfrak{P}_\infty|\mathfrak{p}_\infty) = q^2(q-1).$$

Let G_i denote the (lower) ramification groups at $\mathfrak{P}_\infty$. Then from [HKT, §12.2], we have

$$\begin{aligned}
&\#G_1 = q^2,\\
&\#G_2 = \cdots = \#G_{2q_0+1} = q,\\
&\#G_{2q_0+2} = 1.
\end{aligned}$$

Therefore, the different exponent at $\mathfrak{p}_\infty$ is

$$\begin{aligned}
d(\mathfrak{p}_\infty) &= (q^2(q-1)-1) + (q^2-1) + 2q_0 \cdot (q-1)\\
&= q^3 + 2qq_0 - 2q_0 - 2.
\end{aligned}$$

From the Hurwitz formula, it follows that

$$\sum_{\mathfrak{p} \neq \mathfrak{p}_\infty} \frac{d(\mathfrak{p})}{e(\mathfrak{p})} \deg \mathfrak{p} = \frac{q-2q_0}{q-2q_0+1} < 1.$$

Now $d(\mathfrak{p}) \geq e(\mathfrak{p}) - 1$, with equality if and only if $\mathfrak{p}$ is tamely ramified. Thus the inequality above implies that there is exactly one place $\mathfrak{p}$ of S/G other than $\mathfrak{p}_\infty$ which is ramified in $S \to S/G$, and that $\deg \mathfrak{p} = 1$. Moreover, $\mathfrak{p}$ is tamely ramified with $e(\mathfrak{p}) = q - 2q_0 + 1$.

Let $\mathfrak{P}$ be a prime of S lying over $\mathfrak{p}$. Then the inertia group $I = I(\mathfrak{P}|\mathfrak{p})$ is cyclic of order $q-2q_0+1$. There is a unique conjugacy class of cyclic subgroups of this order (I is a Singer subgroup, see [HB, page 190]). The decomposition group D of $\mathfrak{P}$ has size $(\deg \mathfrak{P})[G : I]$. Since $N_G(I)$ is the unique maximal subgroup containing I, $D \subset N_G(I)$ and $\deg \mathfrak{P}$ divides $[N_G(I) : I] = 4$. But $\mathfrak{P}$ does not have degree 1 because it is not conjugate to $\mathfrak{P}_\infty$, and S has no points of degree 2, so $\deg \mathfrak{P} = 4$ and $D = N_G(I)$. Thus, the point $\mathfrak{P}$ has orbit of size $[G : D] = \frac{1}{4}q^2(q-1)(q+2q_0+1)$. Since this equal to the number of points on S of degree 4, these points form a single orbit under the action of G. □

3.1.3 The Ree Curve

For $s \geq 1$ and $q = 3q_0^2 = 3^{2s+1}$, the Ree curve $R = R_s$ may be defined by the affine equations

$$y^q - y = x^{q_0}(x^q - x),$$
$$z^q - z = x^{2q_0}(x^q - x).$$

The curve R has $q^3 + 1$ points rational over $\mathbb{F}_q$, genus $\frac{3}{2}q_0(q-1)(q+q_0+1)$, and automorphism group $\mathrm{Ree}(q)$ of size $(q^3+1)q^3(q-1)$. The curve R is maximal over $\mathbb{F}_{q^6}$.

Proposition 3.4. *The Ree curve has exactly two short orbits under the action of its full automorphism group. One is non-tame of size q^3+1, consisting of the $\mathbb{F}_q$-rational points. The other is tame of size $\frac{1}{6}q^3(q-1)(q+1)(q+3q_0+1)$, consisting of all points of degree 6.*

Proof. This can be proved in the same manner as Proposition 3.3. The only pieces of information needed are the sizes of the ramifications groups at a rational point of R in $R \to R/\mathrm{Aut}(R)$, and a list of the maximal subgroups of $\mathrm{Aut}(R)$. These may be found, for example, in [HP] and [HKT, page 648]. □

3.2 The GK-curve

Let $q = q_0^2$. The function field of the GK-curve $\widetilde{H}$ may be defined by the equations

$$y^{q_0} + y = x^{q_0+1}, \qquad t^m = x^q - x,$$

where $m = q - q_0 + 1$. The curve $\widetilde{H}$ has genus $\frac{1}{2}q(q + q_0 - 1)(q_0 - 1)$ and is maximal over $\mathbb{F}_{q^3}$. Let H denote the Hermitian curve $y^{q_0} + y = x^{q_0+1}$. Then the two equations above describe the curve $\widetilde{H}$ as the normalized fiber product of the cover $H \to \mathbb{P}^1_x$ with a Kummer extension of $\mathbb{P}^1_x$ of degree m.

The automorphism group of $\widetilde{H}$ partitions the set of $\mathbb{F}_{q^6}$-rational points of $\widetilde{H}$ into two orbits $\widetilde{\mathcal{O}}_1 = \widetilde{H}(\mathbb{F}_q)$ and $\widetilde{\mathcal{O}}_2 = \widetilde{H}(\mathbb{F}_{q^3}) \setminus \widetilde{H}(\mathbb{F}_q)$ [GK2]. The points of $\widetilde{\mathcal{O}}_1$ are exactly the set of ramification points of the map $\widetilde{H} \to H$. These points are completely ramified, and lie over $\mathcal{O}_1 = H(\mathbb{F}_q)$. The points of $\widetilde{\mathcal{O}}_2$, on the other hand, lie over $\mathcal{O}_2 = H(\mathbb{F}_{q^3}) \setminus H(\mathbb{F}_q)$, and these points split completely in $\widetilde{H} \to H$ (see [FG3, page 5]). By Proposition 3.2, the sets $\mathcal{O}_1$ and $\mathcal{O}_2$ comprise the two short orbits under the action of the automorphism group of H, together forming the set of points of H fixed by some automorphism.

The abelian cover $\widetilde{H} \to H$ is tamely ramified at each point of $\mathcal{O}_1$ and every point of $\mathcal{O}_2$ splits completely in $\widetilde{H}$. Therefore, the function field $K = \mathbb{F}_{q^3}(\widetilde{H})$ is contained in the maximal abelian extension K_{rcf} of $\mathbb{F}_{q^3}(H)$ of conductor $\mathfrak{m} = \sum_{P \in \mathcal{O}_1} P$ in which each point of $\mathcal{O}_2$ splits completely.

The corresponding curve H_{rcf} is also maximal over $\mathbb{F}_{q^3}$ and the function field K_{rcf} is of the form $K((x^q - x)^{1/mk})$ for some $k \geq 1$, as will be proved in section 3.5. With this information we are prepared to show that $\widetilde{H} = H_{\text{rcf}}$.

Theorem 3.5. *The Giulietti-Korchmáros curve $\widetilde{H}$ is equal to H_{rcf}.*

Proof. For $r \geq 1$, let the C_r denote the curve defined by

$$u^r = x^q - x.$$

Then H_{rcf} is the normalized fiber product of $H \to \mathbb{P}^1_x$ and $C_{mk} \to \mathbb{P}^1_x$ for some $k \geq 1$. Since H_{rcf} is maximal over $\mathbb{F}_{q^3}$, so is C_{mk}. But by the following lemma, this implies that $k = 1$. □

Lemma 3.6. *Let $q = q_0^2$ be a square, and let r be a multiple of $m = q - q_0 + 1$ which divides $q^{3/2} + 1 = (q_0 + 1)m$. Then the curve C_r is maximal over $\mathbb{F}_{q^3}$ if and only if $r = m$.*

Proof. The curve C_m is covered by the GK-curve, hence is maximal over $\mathbb{F}_{q^3}$. Let $r = mk$ for some k dividing $q_0 + 1$. Then since $g(C_r) = \frac{1}{2}(r-1)(q-1)$, C_r is maximal over $\mathbb{F}_{q^3}$ only if

$$\#C_r(\mathbb{F}_{q^3}) = q^3 + 1 + (r-1)(q-1)q^{3/2}.$$

Let Tr denote the field trace from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$. Since r divides $q^3 - 1$, the field $\mathbb{F}_{q^3}$ contains the rth roots of unity. Therefore, each $\alpha \in \mathbb{F}_{q^3}^{\times r}$ has exactly r rth roots in $\mathbb{F}_{q^3}$, and the number of solutions of $\alpha = \beta^q - \beta$ is either q or 0, depending on whether $\mathrm{Tr}(\alpha) = 0$ or not. Thus, every element of $\mathbb{F}_{q^3}^{\times r} \cap \ker \mathrm{Tr}$ contributes rq points to $C_r(\mathbb{F}_{q^3})$. Along with the q points corresponding to $u = 0$ and the point at infinity, this gives

$$\#C_r(\mathbb{F}_{q^3}) = q + 1 + rq \cdot \#(\mathbb{F}_{q^3}^{\times r} \cap \ker \mathrm{Tr}).$$

Therefore, C_r is maximal over $\mathbb{F}_{q^3}$ if and only if

$$\#(\mathbb{F}_{q^3}^{\times r} \cap \ker \mathrm{Tr}) = (q-1)(q_0 + 1/k). \tag{3.1}$$

Since the curve C_m is maximal over $\mathbb{F}_{q^3}$, we have $\#(\mathbb{F}_{q^3}^{\times m} \cap \ker \mathrm{Tr}) = (q-1)(q_0+1)$. Let α be an element of $\mathbb{F}_{q^3}^{\times m} \cap \ker \mathrm{Tr}$, so that $\alpha^{(q^3-1)/m} = 1$ and $\mathrm{Tr}(\alpha) = 0$. Then

$$\begin{aligned} 0 &= \alpha^{(q^3-1)/m - q^2}\,\mathrm{Tr}(\alpha) \\ &= \alpha^{(q^3-1)/m - q^2}(\alpha + \alpha^q + \alpha^{q^2}) \\ &= \alpha^{(q-1)q_0} + \alpha^{(q-1)(q_0+1)} + 1, \end{aligned}$$

so there at most $(q-1)(q_0+1)$ such α. We conclude that $\mathbb{F}_{q^3}^{\times m} \cap \ker \mathrm{Tr}$ consists of the roots of the polynomial

$$f(T) = T^{(q-1)(q_0+1)} + T^{(q-1)q_0} + 1.$$

We claim that the trace zero elements of $\mathbb{F}_{q^3}^{\times m}$ are evenly distributed among the cosets of the multiplicative subgroup $W = \mathbb{F}_{q_0^3}^{\times} \subset \mathbb{F}_{q^3}^{\times m}$ of index $q_0 + 1$.

To see this, first note that the polynomial $f(T)$ admits the factorization

$$f(T) = \prod_{\zeta^{q_0+1}=1} (T^{q-1} + \zeta T^{q_0-1} + 1).$$

Fix a generator β of $\mathbb{F}_{q^3}^{\times m}$, so that $\zeta = \beta^{q^{3/2}-1}$ is a primitive (q_0+1)th root of unity. Then we claim that each root of $f(T)$ lying in the coset $\beta^{-i}W$ is a root of $f_i(T) = T^{q-1} + \zeta^i T^{q_0-1} + 1$. For if $\alpha \in \beta^{-i}W$, then $(\alpha\beta^i)^{q_0^3-1} = 1$ and

$$\begin{aligned} \alpha^{(q-1)q_0} f_i(\alpha) &= \alpha^{(q-1)q_0}(\alpha^{q-1} + \zeta^i \alpha^{q_0-1} + 1) \\ &= \alpha^{(q-1)(q_0+1)} + \beta^{(q_0^3-1)i}\alpha^{q_0^3-1} + \alpha^{(q-1)q_0} = f(\alpha). \end{aligned}$$

It follows that $\#(\mathbb{F}_{q^3}^r \cap \ker \mathrm{Tr}) = (q-1)(q_0+1)/k$. Comparing with (3.1), we see that C_r is maximal only if $k = 1$. □

3.3 Suzuki cover

In this section, we introduce a cover $\widetilde{S} \to S$ of the Suzuki curve which is analogous to the GK-curve $\widetilde{H} \to H$ and show that it is maximal over $\mathbb{F}_{q^4}$, where $q = 2q_0^2 = 2^{2s+1}$, $s \geq 1$. Recall that the Suzuki curve S is defined by the affine equation

$$y^q + y = x^{q_0}(x^q + x).$$

Let $\widetilde{S}$ be a smooth model of the curve with function field described by

$$y^q + y = x^{q_0}(x^q + x), \qquad t^m = x^q + x,$$

where $m = q - 2q_0 + 1$. The curve $\widetilde{S}$ may be described as the normalization of the fiber product of the covers $S \to \mathbb{P}_x^1$ and $C_m \to \mathbb{P}_x^1$, where C_m is the curve $t^m = x^q + x$.

Let $F = \mathbb{F}_q(x)$. The function field $\mathbb{F}_q(\widetilde{S})$ is the composite of $\mathbb{F}_q(C_m) = F(t)$ and $\mathbb{F}_q(S) = F(y)$. Each place of F of degree 1 is ramified in $F(t)$, with ramification index m, and no other places are ramified. Also, the place ∞ corresponding to $1/x$ is the only place ramified in $F(y)$, with ramification index q. Therefore, the only places ramified in $F(t,y)/F(y)$ are the q^2+1 rational places, and each is tamely ramified with ramification index m. Thus, the Hurwitz formula gives

$$g_{\widetilde{S}} = 1 + m(g_S - 1) + \frac{1}{2}(q^2+1)(m-1) = \frac{1}{2}(q^3 - 2q^2 + q).$$

Theorem 3.7. *The curve $\widetilde{S}$ is maximal over $\mathbb{F}_{q^4}$.*

We prove this by means of the Natural Embedding Theorem of Korchmáros and Torres (Theorem 2.6). Given an $\mathbb{F}_{\ell^2}$-maximal curve X, there is a concrete construction described in [KT] for producing an embedding of X in a Hermitian variety. First take a basis $f_1, \ldots, f_m$ for the linear series $L((\ell+1)P_0)$, where P_0 is any rational point of X. Then there is a unique point $(z_0 : \cdots : z_m) \in \mathbb{P}^m_{\mathbb{F}_{\ell^2}(X)}$ satisfying

$$z_1^\ell f_1 + \cdots + z_m^\ell f_m = 0.$$

After a linear change of variables, and possibly taking a projection, the functions z_i then give desired embedding.

Define functions $z = y^{2q_0} + x^{2q_0+1}$ and $w = xy^{2q_0} + z^{2q_0}$ on $\widetilde{S}$. These satisfy the relations

$$z^q + z = x^{2q_0}(x^q + x), \qquad w^q + w = y^{2q_0}(x^q + x). \tag{3.2}$$

Moreover, if ∞ denotes the pole of the function x, then

$$\begin{aligned}
-v_\infty(x) &= qm = q^2 - 2qq_0 + q,\\
-v_\infty(y) &= -(1 + \frac{1}{2q_0})v_\infty(x) = q^2 - qq_0 + q_0,\\
-v_\infty(z) &= -(1 + \frac{1}{q_0})v_\infty(x) = q^2 - q + 2q_0,\\
-v_\infty(w) &= -(1 + \frac{1}{q_0} + \frac{1}{q})v_\infty(x) = q^2 + 1,\\
-v_\infty(t) &= -\frac{q}{m}v_\infty(x) = q^2.
\end{aligned}$$

Since the semigroup generated by these numbers has genus $g(\widetilde{S})$, the pole orders of these functions generate the Weierstrass semigroup of $\widetilde{S}$ at ∞. In particular, the linear series $L((q^2+1)\infty)$ has a basis $\mathcal{B}$ of monomials in $1, x, y, z, w, t$. This fact is relevant to the task of finding an equation for the particular Hermitian variety in which we wish to embed $\widetilde{S}$, since it allows a search for the functions z_i mentioned above to be phrased as a linear algebra problem over a vector space with basis $b_i^{q^{2k}} b_j$ with $b_i, b_j \in \mathcal{B}$. Such a computation performed in Magma [BCP] assisted in the discovery of equation (3.3) below.

Lemma 3.8. *Every automorphism of S lifts to an automorphism of $\widetilde{S}$ defined over $\mathbb{F}_{q^4}$.*

Proof. The group $\operatorname{Aut} \mathbb{F}_q(S)$ is generated by the stabilizer of the point ∞, which consists of automorphisms ψ_{abc} taking

$$\begin{aligned} x &\mapsto ax + b \\ y &\mapsto a^{q_0+1} y + b^{q_0} x + c, \end{aligned}$$

for $a \in \mathbb{F}_q^\times$ and $b, c \in \mathbb{F}_q$, along with an involution ϕ defined by $\phi(x) = z/w$ and $\phi(y) = y/w$, which swaps ∞ with another rational point (see [HS] and [Hen]). To extend $\psi = \psi_{abc}$ to $\widetilde{S}$, we need

$$\psi(t)^m = \psi(x)^q - \psi(x) = a(x^q + x).$$

Fix a generator α of $\mathbb{F}_q^\times$ and an mth root β of α which is contained in $\mathbb{F}_{q^4}$ since m divides $q^4 - 1$. Then we may take $\psi(t) = a^{1/m} t$, where $a^{1/m}$ is chosen consistently with the choice of α and β.

The automorphism ϕ may be lifted to an automorphism of $\widetilde{S}$ by $\phi(t) = t/w$. Indeed, ϕ so defined satisfies

$$\phi(t)^m = \phi(x)^q + \phi(x) = (z/w)^q + z/w.$$

To verify this, first multiply the desired equality by w^{q+1} and use (3.2) to obtain

$$\begin{aligned} t^m w^{2q_0} &= z^q w + z w^q \\ &= w(z^q + z) + z(w^q + w) \\ &= w x^{2q_0}(x^q + x) + z y^{2q_0}(x^q + x). \end{aligned}$$

Thus the desired equation is equivalent to $w^{2q_0} = w x^{2q_0} + z y^{2q_0}$, which may now be verified by using the definitions of z and w. □

Lemma 3.9. *The map $\pi = (1 : x : t : z : w)$ defines a smooth embedding of the curve $\widetilde{S}$ in $\mathbb{P}^4$.*

Proof. Let $X_0, \ldots, X_4$ be homogeneous coordinates on $\mathbb{P}^4$. We first check that $\pi(\widetilde{S})$ has no singular points on the affine piece $X_0 = 1$. Here the equations

$$\begin{aligned} z^q + z &= x^{2q_0}(x^q + x) \\ w^q + w &= (x^{2q_0+1} + z)(x^q + x) \\ t^m &= x^q + x \end{aligned}$$

give a matrix of derivatives of rank 3. It remains to check that $\pi(\widetilde{S})$ has no singular points on the hyperplane $X_0 = 0$. Since the function defining π are in $L((q^2 + 1)\infty)$ and

$$v_\infty(w) = -(q^2 + 1) < v_\infty(f)$$

for $f \in \{1, x, z, t\}$, the only point in $\pi(\widetilde{S}) \cap Z(X_0)$ is $P_\infty := \pi(\infty) = (0 : 0 : 0 : 0 : 1)$.

Let ϕ be the automorphism of $\widetilde{S}$ mentioned in the previous lemma, which acts on the image $\pi(\widetilde{S}) \subset \mathbb{P}^4$ via the permutation (04)(13) of homogeneous coordinates on $\mathbb{P}^4$. Since the point $P_0 = (1 : 0 : 0 : 0 : 0) \in \pi(\widetilde{S})$ is nonsingular, so is the point $\phi(P_0) = P_\infty$. □

Proof of Theorem 3.7. We claim that

$$w^{q^2} + w + z^{q^2}x + x^{q^2}z = t^{q^2+1}, \tag{3.3}$$

so that the image of the map $\pi = (1 : x : t : z : w)$ lies on the Hermitian hypersurface

$$X_0X_4^{q^2} + X_0^{q^2}X_4 + X_1^{q^2}X_3 + X_1X_3^{q^2} = X_2^{q^2+1}$$

in $\mathbb{P}^4$. By Theorem 2.6 this will complete the proof of the theorem. Writing $f = x^q + x$ for convenience, we use (3.2) to rewrite the terms on the left hand side of the desired equation as

$$\begin{aligned} w^{q^2} + w &= (y^{2q_0}f)^q + y^{2q_0}f \\ &= (y^{2q_0} + x^{2qq_0+q} + x^{q+2q_0})f^q + y^{2q_0}f \end{aligned}$$

and

$$\begin{aligned} z^{q^2}x + x^{q^2}z &= (z^{q^2}+z)x + (x^{q^2}+x)z \\ &= ((x^{2q_0}f)^q + x^{2q_0}f)x + (f^q+f)(x^{2q_0+1}+y^{2q_0}) \\ &= (x^{2qq_0+1}+x^{2q_0+1}+y^{2q_0})f^q + y^{2q_0}f. \end{aligned}$$

Adding these gives

$$(x^{2qq_0+q}+x^{q+2q_0}+x^{2qq_0+1}+x^{2q_0+1})f^q = f^{q+2q_0+1} = t^{q^2+1},$$

and so the claim is proven. □

3.4 Ree cover

Fix $s \geq 1$, and let $q = 3q_0^2 = 3^{2s+1}$, and recall the definition of the Ree curve R from section 3.1. In this section, we construct a cover $\widetilde{R} \to R$ which is also maximal over $\mathbb{F}_{q^6}$. Let $\widetilde{R}$ be a smooth model of the curve with function field described by

$$\begin{aligned} y^q - y &= x^{q_0}(x^q - x) \\ z^q - z &= x^{2q_0}(x^q - x) \\ t^m &= x^q - x, \end{aligned}$$

where $m = q - 3q_0 + 1$. The curve $\widetilde{R}$ may be described as the normalization of the fiber product of of the covers $R \to \mathbb{P}^1_x$ and $C_m \to \mathbb{P}^1_x$, where C_m is the curve described by the third equation above.

Let $F = \mathbb{F}_q(x)$. The function field $\mathbb{F}_q(\widetilde{R})$ is the composite of $\mathbb{F}_q(C_m) = F(t)$ and $\mathbb{F}_q(S) = F(y,z)$. Each place of F of degree 1 is ramified in $F(t)$ with ramification index m, and no other places are ramified. Also, the place ∞ corresponding to $1/x$ is the only place ramified in $F(y,z)$, with ramification index q^2. Therefore, the only places ramified in $F(t,y,z)/F(y,z)$ are the q^3+1 rational places, and each is tamely ramified with ramification index m. Thus, the Hurwitz formula gives

$$g_{\widetilde{R}} = 1 + m(g_R - 1) + \frac{1}{2}(q^3+1)(m-1)$$

$$= \frac{1}{2}(q^4 + 6q^3q_0 + 2q^3 - 2q^2 - 6qq_0 - 3q + 2).$$

Theorem 3.10. *The curve $\widetilde{R}$ is maximal over $\mathbb{F}_{q^6}$.*

We proceed as in section 3.3 by embedding $\widetilde{R}$ in a Hermitian variety. We recall the functions w_i on the Ree curve introduced in (2.2). From the appendix of [Ped], these satisfy

$$\begin{aligned} w_1^q - w_1 &= x^{3q_0}(x^q - x) & w_4^q - w_4 &= (w_2 - xw_1)^{q_0}(x^q - x) \\ w_2^q - w_2 &= y^{3q_0}(x^q - x) & w_6^q - w_6 &= w_4^{3q_0}(x^q - x) \\ w_3^q - w_3 &= z^{3q_0}(x^q - x) & w_8^q - w_8 &= w_7^{3q_0}(x^q - x). \end{aligned} \tag{3.4}$$

Furthermore, if ∞ denotes the unique pole of x in $\widetilde{R}$, then it follows that

$$\begin{aligned} -v_\infty(x) &= q^3 - 3q^2q_0 + q^2, & -v_\infty(w_6) &= q^3 - q + 3q_0, \\ -v_\infty(w_1) &= q^3 - 2q^2 + 3qq_0, & -v_\infty(w_8) &= q^3 + 1, \\ -v_\infty(w_2) &= q^3 - q^2 + q, & -v_\infty(t) &= q^3. \\ -v_\infty(w_3) &= q^3 - 3qq_0 + 2q, \end{aligned}$$

Lemma 3.11. *Every automorphism of R lifts to an automorphism of $\widetilde{R}$ defined over $\mathbb{F}_{q^6}$.*

Proof. We use the concrete description of $G = \operatorname{Aut} \mathbb{F}_q(R)$ found in [Ped]. The group G is generated by the stabilizer G_∞ of the point ∞ and an involution ϕ which swaps ∞ with another rational point. The stabilizer G_∞ consists of automorphisms ψ_{abcd} taking

$$\begin{aligned} x &\mapsto ax + b \\ y &\mapsto a^{q_0+1}y + ab^{q_0}x + c \\ z &\mapsto a^{2q_0+1}z - a^{q_0+1}b^{q_0}y + ab^{2q_0}x + d, \end{aligned}$$

for $a \in \mathbb{F}_q^\times$ and $b, c, d \in \mathbb{F}_q$. To extend $\psi = \psi_{abcd}$ to $\widetilde{R}$, we need

$$\psi(t)^m = \psi(x)^q - \psi(x) = a(x^q - x).$$

Fix a generator α of $\mathbb{F}_q^\times$ and an mth root β of α which is contained in $\mathbb{F}_{q^6}$ since m divides $q^6 - 1$. Then we may take $\psi(t) = a^{1/m}t$, where $a^{1/m}$ is chosen consistently with the choice of α and β.

The involution $\phi \in \operatorname{Aut} \mathbb{F}_q(R)$ mentioned above sends

$$x \mapsto w_6/w_8, \qquad y \mapsto w_{10}/w_8, \qquad z \mapsto w_9/w_8.$$

We claim that ϕ extends to $\widetilde{R}$ via $\phi(t) = t/w_8$. To verify this, we show that

$$\phi(t)^m = \phi(x)^q - \phi(x) = (w_6/w_8)^q - w_6/w_8.$$

Upon multiplying through by w_8^{q+1}, using (3.4), and then dividing by $x^q - x$, this is seen to be equivalent to

$$w_8^{3q_0} = w_8 w_4^{3q_0} - w_6 w_7^{3q_0}.$$

But this is one of the equations appearing in [ED, Lemma 4.3]. □

Lemma 3.12. *The map* $\pi = (1 : x : w_1 : w_2 : t : w_3 : w_6 : w_8)$ *defines a smooth embedding of the curve* $\widetilde{R}$ *in* $\mathbb{P}^7$*.*

Proof. Let $X_0, \ldots, X_7$ be homogeneous coordinates on $\mathbb{P}^7$. We first check that $\pi(\widetilde{R})$ has no singular points on the affine piece $X_0 = 1$. Here we have, from (2.2) and (3.4),

$$\begin{aligned}
w_1^q - w_1 &= x^{3q_0}(x^q - x)\\
w_2^q - w_2 &= (x^{3q_0+1} - w_1)(x^q - x)\\
w_3^q - w_3 &= (x^{3q_0+2} - xw_1 - w_2)(x^q - x)\\
w_6^q - w_6 &= (x^{3q_0}w_2^q - w_1^q x^{3q_0+1} + w_1^{q+1})(x^q - x)\\
w_8^q - w_8 &= (w_2^{3q_0} + x^{3q_0}w_3^q - x^{6q_0+1}w_1^q + x^{3q_0}w_1^{q+1} + w_2 w_1^q)(x^q - x).
\end{aligned}$$

These equations, along with $t^m = x^q - x$, give a matrix of derivatives of rank 6. It remains to show that $\pi(\widetilde{R})$ has no singular points lying on the hyperplane $X_0 = 0$. Since each of the functions defining π are in $L((q^3+1)\infty)$, and

$$v_\infty(w_8) = -(q^3+1) < v_\infty(f)$$

for $f \in \{1, x, w_1, w_2, w_3, w_6, t\}$, the only point of $\pi(\widetilde{R}) \cap Z(X_0)$ is $P_\infty := \pi(\infty) = (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1)$.

Let ϕ be the involution in $\operatorname{Aut} \mathbb{F}_q(\widetilde{R})$ defined in the previous lemma, which takes $x \mapsto w_6/w_8$ and $t \mapsto t/w_8$. Since the automorphism ϕ also sends

$$\begin{aligned} &w_1 \mapsto w_3/w_8, && w_2 \mapsto w_2/w_8, && w_3 \mapsto w_1/w_8, \\ &w_6 \mapsto x/w_8, && w_8 \mapsto w_8/w_8, \end{aligned}$$

it acts on the image $\pi(\widetilde{R}) \subset \mathbb{P}^7$ via the permutation (07)(16)(25) of homogeneous coordinates on $\mathbb{P}^7$. Since the point $P_0 = (1:0:0:0:0:0:0) \in \pi(\widetilde{R})$ is nonsingular, so is the point $\phi(P_0) = P_\infty$. □

Proof of Theorem 3.10. We show that

$$w_8^{q^3} + w_8 + xw_6^{q^3} + x^{q^3}w_6 + w_1w_3^{q^3} + w_1^{q^3}w_3 + w_2^{q^3+1} = t^{q^3+1},$$

so that the image of the map $\pi = (1 : x : w_1 : w_2 : t : w_3 : w_6 : w_8)$ in $\mathbb{P}^7$ lies on the Hermitian hypersurface

$$X_0X_7^{q^3} + X_0^{q^3}X_7 + X_1X_6^{q^3} + X_1^{q^3}X_6 + X_2X_5^{q^3} + X_2^{q^3}X_5 + X_3^{q^3+1} = X_4^{q^3+1}.$$

The desired result will then follow by Theorem 2.6. Since

$$t^{q^3+1} = (x^q - x)^{\frac{q^3+1}{m}} = (x^q - x)^{q^2+3qq_0+2q+3q_0+1},$$

our verification may be done completely inside of the function field $\mathbb{F}_q(x, y, z)$ of R. Writing $f = x^q - x$ for convenience, we use (3.4) to rewrite the terms on the left hand side of the desired equation as

$$\begin{aligned} w_8^{q^3} + w_8 &= (w_7^{3q_0})^{q^2} f^{q^2} + (w_7^{3q_0})^q f^q + w_7^{3q_0} f - w_8, \\ xw_6^{q^3} + x^{q^3}w_6 &= (w_6^{q^3} - w_6)x + (x^{q^3} - x)w_6 - xw_6 \\ &= ((w_4^{3q_0})^{q^2} x + w_6) f^{q^2} \\ &\quad + ((w_4^{3q_0})^q x + w_6) f^q + (w_4^{3q_0} x + w_6) f - xw_6, \\ w_1w_3^{q^3} + w_1^{q^3}w_3 &= (w_3^{q^3} - w_3)w_1 + (w_1^{q^3} - w_1)w_3 - w_1w_3 \\ &= ((z^{3q_0})^{q^2} w_1 + (x^{3q_0})^{q^2} w_3) f^{q^2} + ((z^{3q_0})^q w_1 + (x^{3q_0})^q w_3) f^q \\ &\quad + (z^{3q_0} w_1 + x^{3q_0} w_3) f - w_1w_3, \\ w_2^{q^3+1} &= (w_2^{q^3} - w_2)w_2 + w_2^2 \\ &= (y^{3q_0})^{q^2} w_2 f^{q^2} + (y^{3q_0})^q w_2 f^q + y^{3q_0} w_2 f + w_2^2. \end{aligned}$$

Collecting terms involving common powers of f gives

$$A_{-1} + A_0 f + A_1 f^q + A_2 f^{q^2},$$

where

$$A_{-1} = -w_8 - xw_6 - w_1 w_3 + w_2^2$$

and

$$A_i = (w_7^{q^i})^{3q_0} + (w_4^{q^i})^{3q_0} x + (z^{q_i})^{3q_0} w_1 + (y^{q_i})^{3q_0} w_2 + (x^{q_i})^{3q_0} w_3 + w_6$$

for $i = 0, 1, 2$. We claim that $A_{-1} = A_0 = A_1 = 0$. Indeed, the quadric A_{-1} and each of the three terms in the expression

$$\begin{aligned} A_0 = (x^{3q_0} w_3 - z^{3q_0} w_1 - w_7^{3q_0} + w_2^{3q_0}) \\ - (w_4^{3q_0} x + z^{3q_0} w_1 - y^{3q_0} w_2) \\ - (w_4^{3q_0} x + w_7^{3q_0} + w_2^{3q_0} - w_6) \end{aligned}$$

are among the relations listed in [ED, Lemma 4.3], so $A_{-1} = 0 = A_0$. Now using (3.4), we obtain

$$\begin{aligned} A_0^q - A_1 &= (w_4^q)^{3q_0}(x^q - x) + (w_6^q - w_6) \\ &\quad + (z^q)^{3q_0}(w_1^q - w_1) + (x^q)^{3q_0}(w_3^q - w_3) + (y^q)^{3q_0}(w_2^q - w_2) \\ &= (w_4^q + w_4 + z^q x + x^q z + y^{q+1})^{3q_0}(x^q - x). \end{aligned}$$

Further simplification reveals that

$$B_1 := w_4^q + w_4 + z^q x + x^q z + y^{q+1} = 0,$$

and so $A_1 = 0$.

It remains to show that $A_2 = (x^q - x)^{3qq_0 + 2q + 3q_0 + 1}$. By (3.4),

$$\begin{aligned} A_1^q - A_2 &= (w_4^{q^2})^{3q_0}(x^q - x) + (w_6^q - w_6) \\ &\quad + (z^{q^2})^{3q_0}(w_1^q - w_1) + (x^{q^2})^{3q_0}(w_3^q - w_3) + (y^{q^2})^{3q_0}(w_2^q - w_2) \\ &= (w_4^{q^2} + w_4 + z^{q^2} x + x^{q^2} z + y^{q^2+1})^{3q_0}(x^q - x). \end{aligned}$$

Thus it suffices to show that

$$B_2 := w_4^{q^2} + w_4 + z^{q^2}x + x^{q^2}z + y^{q^2+1} = -(x^q - x)^{q+2q_0+1}.$$

To do this, we use (3.4) again, obtaining

$$\begin{aligned} B_1^q - B_2 &= (w_4^q - w_4) + z^{q^2}(x^q - x) + x^{q^2}(z^q - z) + y^{q^2}(y^q - y) \\ &= (w_2^{q_0} - w_1^{q_0}x^{q_0} + z^{q^2} + x^{q^2}x^{2q_0} + y^{q^2}x^{q_0})(x^q - x) \\ &= \big[(xy^{3q_0} - z^{3q_0})^{q_0} - (x^{3q_0+1} - y^{3q_0})^{q_0}x^{q_0} \\ &\qquad + z^{q^2} + x^{q^2}x^{2q_0} + y^{q^2}x^{q_0}\big](x^q - x) \\ &= \big[(z^q - z)^q + (y^q - y)^q x^{q_0} + (x^q - x)^q x^{2q_0}\big](x^q - x) \\ &= (x^{2qq_0} + x^{qq_0+q_0} + x^{2q_0})(x^q - x)^{q+1} \\ &= (x^q - x)^{q+2q_0+1}. \end{aligned}$$

□

3.5 Ray class fields

In this section, we let X denote one the Deligne-Lusztig curves H, S, or R, and let $d = 3, 4,$ or 6, respectively. Then $\#X(\mathbb{F}_q) = q^{d/2} + 1$, and $\widetilde{X}$ is maximal over $\mathbb{F}_{q^d}$, and the cover $\widetilde{X} \to X$ is of degree $m = q - \lfloor d/2 \rfloor q_0 + 1$. Moreover, each $\mathbb{F}_q$-rational point of X is totally ramified in $\widetilde{X}$ and these are the only points ramified in $\widetilde{X} \to X$. The following lemma implies then that every point of X of degree d splits completely in $\widetilde{X}$ over $\mathbb{F}_{q^d}$.

Lemma 3.13. *Let X be a curve defined over $\mathbb{F}_q$ which is maximal over $\mathbb{F}_{q^d}$, and let $f\colon Y \to X$ be a tame cover of degree $m > 1$ defined over $\mathbb{F}_q$. Suppose that f is totally ramified at each $\mathbb{F}_q$-rational point of X and unramified elsewhere. Then any two of the following conditions implies the third.*

(i) Y is maximal over $\mathbb{F}_{q^d}$,

(ii) $\#X(\mathbb{F}_q) = q^{d/2} + 1$,

(iii) $\#(f^{-1}(P) \cap Y(\mathbb{F}_{q^d})) = m$ for every $P \in X(\mathbb{F}_{q^d}) \setminus X(\mathbb{F}_q)$.

Proof. Let N_r denote the number of $\mathbb{F}_{q^r}$-rational points of X.. From the Hurwitz genus formula,

$$2g_Y - 2 = m(2g_X - 2) + N_1(m - 1).$$

Also, since X is maximal over $\mathbb{F}_{q^d}$ we have $N_d = q^d + 1 + 2g_X q^{d/2}$. Then

$$\begin{aligned}\#Y(\mathbb{F}_{q^d}) &\le q^d + 1 + 2g_Y q^{d/2} \\ &= q^d + 1 + q^{d/2}\left[m(2g_X - 2) + N_1(m-1) + 2\right] \\ &= N_1 + m(N_d - N_1) + q^{d/2}(m-1)\left[N_1 - (q^{d/2}+1)\right],\end{aligned}$$

If Y is maximal over $\mathbb{F}_{q^d}$ then equality holds above, and so (ii) is satisfied if and only if (iii) is. On the other hand, if both (ii) and (iii) hold, then

$$\#Y(\mathbb{F}_{q^d}) = N_1 + m(N_d - N_1) = q^d + 1 + 2g_Y q^{d/2},$$

and Y is maximal over $\mathbb{F}_{q^d}$. □

Define the modulus $\mathfrak{m}$ as the sum of all $\mathbb{F}_q$-rational points of X and let Σ be the set of the points of X of degree d over $\mathbb{F}_q$. Then there is a curve $X_{\text{rcf}} \to X$ whose function field is the ray class field over $K = \mathbb{F}_{q^d}(X)$ of conductor $\mathfrak{m}$ in which each place in Σ splits completely. Since $\widetilde{K} = \mathbb{F}_{q^d}(\widetilde{X})$ is an abelian extension of K satisfying these ramification and splitting conditions, $\widetilde{K}$ is contained in $K_{\text{rcf}} = \mathbb{F}_{q^d}(X_{\text{rcf}})$ and the cover $X_{\text{rcf}} \to X$ factors through $\widetilde{X}$.

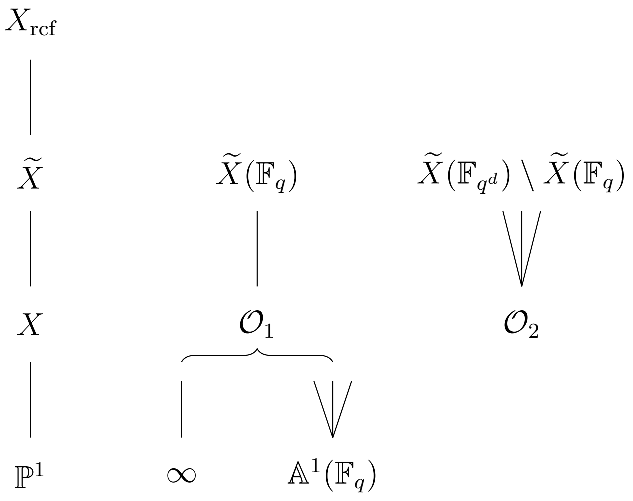

X_{rcf}
$\widetilde{X}$
$\widetilde{X}(\mathbb{F}_q)$
$\widetilde{X}(\mathbb{F}_{q^d}) \setminus \widetilde{X}(\mathbb{F}_q)$
X
$\mathcal{O}_1$
$\mathcal{O}_2$
$\mathbb{P}^1$
∞
$\mathbb{A}^1(\mathbb{F}_q)$

Figure 3.1: Splitting in $\widetilde{X}$

Theorem 3.14. *The curve X_{rcf} is maximal over $\mathbb{F}_{q^d}$.*

Proof. Write $Y = X_{\text{rcf}}$. By Lemma 3.13 it suffices to show that $Y \to X$ is totally ramified at each point of $X(\mathbb{F}_q)$. Let k be the degree of the cover

$Y \to \widetilde{X}$ and write $N = \#\widetilde{X}(\mathbb{F}_q) = q^{d/2} + 1$. For $P \in \widetilde{X}$, let e_P denote the ramification index of P in Y. Then

$$\#Y(\mathbb{F}_{q^d}) = km\#\Sigma + N - r,$$

where r is the number of $\mathbb{F}_q$-rational points of $\widetilde{X}$ with $e_P < k$. On the other hand, the Hasse-Weil bound and Riemann-Hurwitz give

$$\begin{aligned}\#Y(\mathbb{F}_{q^d}) &\leq q^d + 1 + 2g_Y q^{d/2} \\ &= (q^{d/2} + 1)^2 + (2g_Y - 2)q^{d/2} \\ &= N^2 + kq^{d/2}(2g_{\widetilde{X}} - 2) + q^{d/2} \deg \operatorname{Diff} Y/\widetilde{X}.\end{aligned}$$

Now

$$\deg \operatorname{Diff} Y/\widetilde{X} = k \sum_{P \in \widetilde{X}(\mathbb{F}_q)} \left(1 - \frac{1}{e_P}\right) = N(k-1) - \sum_{e_P > 1} \left(\frac{k}{e_P} - 1\right).$$

Combining all this with the facts $m\#\Sigma = q^{d/2}(q-1)N$ and $2g_{\widetilde{X}} - 2 = (q-2)N$ and doing some rearranging yields

$$\sum_{e_P > 1} \left(\frac{k}{e_P} - 1\right) \leq 1 + rq^{-d/2} \leq 2 + q^{-d/2}. \tag{3.5}$$

Since e_P divides k, each nonzero summand on the left hand side of (3.5) is at least 1, so we conclude that $e_P < k$ for at most two $P \in X(\mathbb{F}_q)$. In particular, if $r > 0$ then either $r = 1$ and $e_P = k/3$ for a single P, or $r \in \{1, 2\}$ and $e_P \geq k/2$ for all P. But either of these cases gives a contradiction in (3.5). □

Corollary 3.15. *The cover $X_{\mathrm{rcf}} \to X$ is cyclic. In particular, the function field K_{rcf} is of the form $K((x^q - x)^{1/mk})$ for some k dividing $(q^{d/2} + 1)/m$.*

Proof. The first statement follows from the fact that any tame abelian extension L/K which is totally ramified at some place is cyclic. Indeed, if not then by replacing K with a larger subfield of L we may assume that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/r\mathbb{Z})^2$ for some $r > 1$. Then L is a composite of two cyclic Kummer extensions $K_i = K(v_i)$ with $v_i^r = f_i \in K$. Since L/K is totally ramified at some place P, it follows that $a_i = v_P(f_i)$ is invertible mod r for $i = 1, 2$ (see [Sti2, Prop 3.7.3]). Choose j so that $ja_1 \equiv a_2 \bmod r$. Then $v = v_1^j/v_2 \in L$ is a root of $v^r = f_1^j/f_2$, and $K(v)/K$ is unramified at P since

$v_P(f_1^j/f_2) = ja_1 - a_2 \equiv 0 \bmod r$.

Let $J_{\mathfrak{m}}$ denote the ray class group over K of conductor $\mathfrak{m}$. Then $J_{\mathfrak{m}}$ fits into an exact sequence

$$1 \to \mathbb{F}_{q^d}^\times \to \mathcal{O}_{\mathfrak{m}}^\times \to J_{\mathfrak{m}} \to J \to 1,$$

where $J = \mathrm{Jac}(X)(\mathbb{F}_{q^d})$ and

$$\mathcal{O}_{\mathfrak{m}}^\times = \prod_{P \in \mathfrak{m}} (\mathcal{O}_P/\mathfrak{m}_P)^\times \cong (\mathbb{F}_{q^d}^\times)^{\#X(\mathbb{F}_{q^2})} \cong (\mathbb{Z}/(q^d-1)\mathbb{Z})^{q^{d/2}+1}.$$

Furthermore, we have $J \cong (\mathbb{Z}/(q^{d/2}+1)\mathbb{Z})^{2g_X}$ since X is maximal over $\mathbb{F}_{q^d}$. Thus $J_{\mathfrak{m}}$ has exponent dividing $q^d - 1$, and so does its quotient $\mathrm{Gal}(K_{\mathrm{rcf}}/K)$. From the discussion above, $L = K((x^q - x)^{1/(q^d-1)})$ is the largest abelian extension of K of exponent dividing $q^d - 1$ in which each $\mathbb{F}_q$-rational place of K is totally ramified. Since K_{rcf} is such an extension, we have $\widetilde{K} \subset K_{\mathrm{rcf}} \subset L$, and so K_{rcf} is of the form $K((x^q - x)^{1/mk})$ for some k dividing $(q^d - 1)/m$.

This shows that X_{rcf} covers the curve C_{mk} given by $u^{mk} = x^q - x$. Since X_{rcf} is maximal over $\mathbb{F}_{q^d}$, so is C_{mk}. But a theorem of Garcia and Tazafolian [GT, Theorem 1.2] implies that a curve of the form $u^r = x^q - x$ may be maximal over $\mathbb{F}_{q^d}$ only for r dividing $q^{d/2} + 1$. Thus k divides $(q^{d/2} + 1)/m$, as desired. □

It follows from the proof of Corollary 3.15 that a sufficient condition for X_{rcf} to be equal to $\widetilde{X}$ is that none of the curves C_r defined by $u^r = x^q - x$ are maximal over $\mathbb{F}_{q^d}$ for r a proper multiple of m. This is the case when $X = H$, as was shown in section 3.2. The analogue of Lemma 3.6 does not hold in the situation corresponding to S_{rcf} and R_{rcf}, however. Indeed, in the Suzuki case $q^{d/2} + 1 = q^2 + 1 = (q + q_0 + 1)m$, and the curve $u^{q^2+1} = x^q + x$ is covered by the Hermitian curve $u^{q^2+1} = x^{q^2} + x$, hence is maximal over $\mathbb{F}_{q^4}$. In the Ree case, there are also proper multiplies r of m such that the curve $u^r = x^q - x$ is maximal over $\mathbb{F}_{q^6}$.

In any case, Corollary 3.15 allows one to verify computationally that $X_{\mathrm{rcf}} = \widetilde{X}$ for small values of q by checking that $K((x^q - x)^{1/m\ell})$ is not maximal over $\mathbb{F}_{q^d}$ for any prime ℓ dividing $(q^{d/2} + 1)/m$. Our computations in Magma have shown that $S_{\mathrm{rcf}} = \widetilde{S}$ for $q = 2^{2s+1}$ with $1 \le s \le 6$, and that $R_{\mathrm{rcf}} = \widetilde{R}$ for $q = 27$. We leave as an open problem the question of whether $X_{\mathrm{rcf}} = \widetilde{X}$ in general. The following bound on the degree of the cover $X_{\mathrm{rcf}} \to \widetilde{X}$ follows from Theorem 3.14.

Corollary 3.16. *The degree k of the cover $X_{\mathrm{rcf}} \to \widetilde{X}$ satisfies*

$$k \leq \frac{q^{d/2} - 3}{q - 2}.$$

Proof. Since the curve X_{rcf} is maximal over $\mathbb{F}_{q^d}$ its genus is at most $q^{d/2}(q^{d/2} - 1)/2$ [Iha]. The desired bound follows immediately by combining this with the Hurwitz formula applied to the cover $X_{\mathrm{rcf}} \to \widetilde{X}$, and the fact that $2g_{\widetilde{X}} - 2 = (q-2)(q^{d/2} + 1)$. □

Remark. This bound is slightly better than the bound $k \leq (q^{d/2} + 1)/m$ from Corollary 3.15. When X is the Suzuki or Ree curve, it gives

$$\begin{aligned} k &\leq q + 2, \\ k &\leq q^2 + 2q + 4, \end{aligned}$$

respectively. Current results on the genus spectrum of maximal curves may be used to reduce these bounds by a factor of 3.

4 The orders of an embedding of the Ree curve

Let X be a smooth, geometrically irreducible, projective algebraic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, and let

$$m(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{Z}[t]$$

be the square-free part of the characteristic polynomial of the Frobenius endomorphism Fr_q on the Jacobian of X. Then for any $P, P_0 \in X$ with P_0 an $\mathbb{F}_q$-rational point, we have the fundamental linear equivalence [HKT]

$$m(\mathrm{Fr}_q)(P) = \mathrm{Fr}_q^n(P) + \cdots + a_1 \mathrm{Fr}_q(P) + a_0 P \sim m(1)P_0. \tag{4.1}$$

Thus for $m = |m(1)|$, the linear series $\mathcal{D}_X := |mP_0|$, sometimes called the *Frobenius linear series*, is independent of the choice of rational point P_0.

The linear series $\mathcal{D}_X$ is a useful tool for studying curves with many rational points, especially in the context of the theory of Stöhr and Voloch, which we introduce in section 4.1. The series $\mathcal{D}_X$ has been used extensively to study $\mathbb{F}_q$-maximal curves, since it is intimately related to the embedding given in Theorem 2.6. See for example [FGT], [AT], [FG1], [FG2], and has also been used to study $\mathbb{F}_q$-optimal curves [FT].

The Hermitian, Suzuki, and Ree curves are each characterized among curves over $\mathbb{F}_q$ by their genus, number of rational points, and automorphism group [HP]. Moreover, it can be shown using Stöhr-Voloch theory applied to $\mathcal{D}_X$ that the genus and number of rational points alone are sufficient to characterize the Hermitian and Suzuki curves [RS], [FT]. Whether this is also the case for the Ree curve remains an open question—one which was the initial motivation for the work in the current chapter.

The results in this chapter appear in the paper [Ska1].

In this chapter, we let X denote the Ree curve

$$y^q - y = x^{q_0}(x^q - x), \qquad z^q - z = x^{q_0}(y^q - y), \tag{4.2}$$

where $q = 3q_0^2 = 3^{2s+1}$, $s \geq 1$, and consider X as a curve over $\mathbb{F}_q$. Recall that X has genus $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$ and $N = q^3+1$ points defined over $\mathbb{F}_q$. Weil–Serre's explicit formulas can be used to show that X is $\mathbb{F}_q$-optimal, and that any curve defined over $\mathbb{F}_q$ with this g and N has L-polynomial

$$L_X(t) = (1 + 3q_0 t + qt^2)^{q_0(q^2-1)}(1+qt^2)^{\frac{1}{2}q_0(q-1)(q+3q_0+1)}. \tag{4.3}$$

Since the characteristic polynomial of Fr_q is $t^{2g}L_X(1/t)$, we obtain

$$\begin{aligned} m(t) &= (t^2 + 3q_0 t + q)(t^2+q) \\ &= t^4 + 3q_0 t^3 + 2qt^2 + 3qq_0 t + q^2, \end{aligned}$$

and $\mathcal{D}_X = |mP_0|$ with $m = m(1) = 1 + 3q_0 + 2q + 3qq_0 + q^2$.

There is a subseries $\mathcal{D} \subset \mathcal{D}_X$ of projective dimension 13 which is invariant under $\mathrm{Aut}(X)$. In [ED], Duursma and Eid show that $\mathcal{D}$ is very ample, giving a smooth embedding of X in $\mathbb{P}^{13}$. They also find 105 equations describing the image of this embedding, and use these to compute the Weierstrass semigroup at a rational point when $s = 1$. In this case, it follows from their work that $\mathcal{D} = \mathcal{D}_X$ is a complete linear series. Whether or not $\mathcal{D}$ is complete for $s \geq 2$ is unknown at present.

In this chapter we determine the order sequence of $\mathcal{D}$, that is, the orders of vanishing of sections of $\mathcal{D}$ at a general point. Equivalently, these are the intersection multiplicities of hyperplane sections of X embedded in $\mathbb{P}^{13}$ at a general point. We prove the following theorem.

Theorem 4.1. *The orders of $\mathcal{D}$ are*

$$0,\ 1,\ q_0,\ 2q_0,\ 3q_0,\ q,\ q+q_0,\ 2q,\ qq_0,\ qq_0+q_0,\ qq_0+q,\ 2qq_0,\ 3qq_0,\ q^2.$$

Since $\mathcal{D} \subset \mathcal{D}_X$, these form a subset of the orders of $\mathcal{D}_X$.

As a consequence, we show in Corollary 4.9 that the Weierstrass points of $\mathcal{D}$ consist of the $\mathbb{F}_q$-rational points of X.

4.1 Weierstrass points and Stöhr-Voloch theory

The theory of Weierstrass points in characteristic p was developed first by F.K. Schmidt [Sch]. We briefly give the necessary definitions and results on the subject following the presentation in the paper of Stöhr and Voloch [SV].

Given a base-point-free linear series $\mathcal{D}$ on X of dimension r and degree d, and P a point of X, the $(\mathcal{D}, P)$-*orders* consist of the sequence

$$0 = j_0(P) < j_1(P) < \cdots < j_r(P) \leq d$$

of integers j_i such that there is a hyperplane in $\mathcal{D}$ intersecting P with multiplicity equal to j_i. These are the same for all but finitely many points $P \in X$, called $\mathcal{D}$-*Weierstrass points*. The generic values of the $j_i(P)$ are the $\mathcal{D}$-*orders*

$$0 = \epsilon_0 < \epsilon_1 < \cdots < \epsilon_r.$$

This order sequence may be computed by choosing the ϵ_i lexicographically smallest so that

$$(D_x^{\epsilon_i} f_0 : D_x^{\epsilon_i} f_1 : \cdots : D_x^{\epsilon_i} f_r), \qquad i = 1, \ldots, r,$$

are linearly independent in $\mathbb{P}^r_{\mathbb{F}_q(X)}$, where $f_0, f_1, \ldots, f_r$ is a basis for $\mathcal{D}$, and the D_x^i are Hasse derivatives taken with respect to some fixed separating variable x.

The Hasse derivatives D_x^i are defined on $\mathbb{F}_q(x)$ by

$$D_x^i x^j = \binom{j}{i} x^{j-i},$$

and extend uniquely to derivations on $\mathbb{F}_q(X)$ satisfying the properties

$$D_x^k(fg) = \sum_{i+j=k} (D_x^i f)(D_x^j g), \qquad D_x^k f^p = \begin{cases} (D_x^{k/p} f)^p & \text{if } p \mid k \\ 0 & \text{if } p \nmid k \end{cases}$$

for any $f, g \in \mathbb{F}_q(X)$. In view of this second property, it will be often be convenient to write $D_x^{k/q}$ for k/q is a rational number with denominator a power of p, adopting the convention that $D_x^{k/q} = 0$ when k/q is not an integer.

Furthermore, when the choice of separating variable x is clear from context, we omit the subscript and write simply D^i.

The following "p-adic criterion" for $\mathcal{D}$-orders is quite useful.

Lemma 4.2 ([SV, Corollary 1.9]). *If ϵ is a $\mathcal{D}$-order and $\binom{\epsilon}{\mu} \not\equiv 0 \bmod p$, then μ is also a $\mathcal{D}$-order.*

By Lucas's Theorem, the condition $\binom{\epsilon}{\mu} \not\equiv 0 \bmod p$ in the lemma is equivalent to saying that the coefficients in the p-adic expansion of ϵ are greater than or equal to those in the expansion of μ. When this is the case we write $\mu \leq_p \epsilon$. This defines a partial order on the nonnegative integers.

The (q-)*Frobenius orders* $0 = \nu_0 < \nu_1 < \cdots < \nu_{r-1}$ of $\mathcal{D}$ form a subsequence of the order sequence $\{\epsilon_i\}$, and are defined lexicographically smallest so that

$$\begin{aligned}
&(f_0^q : f_1^q : \cdots : f_r^q),\\
&(D_x^{\nu_0} f_0 : D_x^{\nu_0} f_1 : \cdots : D_x^{\nu_0} f_r),\\
&\qquad\vdots\\
&(D_x^{\nu_{r-1}} f_0 : D_x^{\nu_{r-1}} f_1 : \cdots : D_x^{\nu_{r-1}} f_r)
\end{aligned}$$

are linearly independent in $\mathbb{P}^r_{\mathbb{F}_q(X)}$. There is exactly one $\mathcal{D}$-order ϵ_I which is omitted by the sequence $\{\nu_i\}$. The geometric significance of the index I is as follows: it is the smallest $i \geq 0$ such that, for general P, the image of P under the Frobenius endomorphism lies in the ith osculating space at P. The Frobenius orders are closely connected with the $\mathbb{F}_q$-rational points of X, and are used in Stöhr and Voloch's proof of the Riemann Hypothesis for curves over finite fields.

Lemma 4.3 ([SV, page 10]). *Let $(1 : f_1 : \cdots : f_r)$ be the morphism associated to $\mathcal{D}$. Then the Frobenius orders of $\mathcal{D}$ which are less than q are the first several orders of the morphism $(f_1 - f_1^q : \cdots : f_r - f_r^q)$.*

4.2 Derivatives on the Ree Curve

The function field of the Ree curve X is $\mathbb{F}_q(x, y, z)$, where y and z satisfy (4.2). The linear series $\mathcal{D}$ we wish to study corresponds to the $\overline{\mathbb{F}}_q$-vector space $V_{\mathcal{D}}$ spanned by the 14 functions

$$\mathcal{B} = \{1,\ x,\ y,\ z,\ w_1,\ w_2,\ \ldots,\ w_{10}\},$$

where w_i are defined as in (2.2). The functions in $\mathcal{B}$ have distinct orders at the pole P_∞ of x, hence are linearly independent. We will use the separating variable x for computing all Hasse derivatives on the Ree curve.

To compute the orders of $\mathcal{D}$, we will need to obtain closed form expressions for the derivatives of the functions $f \in \mathcal{B}$. In addition to the relations in (4.2), the following equations derived by Pedersen will be useful for computing the derivatives of the w_i.

$$\begin{aligned}
w_1^q - w_1 &= x^{3q_0}(x^q - x) & w_4^q - w_4 &= w_2^{q_0}(x^q - x) - w_1^{q_0}(y^q - y) \\
w_2^q - w_2 &= y^{3q_0}(x^q - x) & w_5^q - w_5 &= w_3^{q_0}(y^q - y) - w_2^{q_0}(z^q - z) \\
w_3^q - w_3 &= z^{3q_0}(x^q - x) & w_7^q - w_7 &= w_2^{q_0}(y^q - y) - w_3^{q_0}(x^q - x) \\
w_6^q - w_6 &= w_4^{3q_0}(x^q - x) & w_9^q - w_9 &= w_2^{q_0}(w_4^q - w_4) - w_6^{q_0}(y^q - y) \\
w_8^q - w_8 &= w_7^{3q_0}(x^q - x) & w_{10}^q - w_{10} &= w_6^{q_0}(z^q - z) - w_3^{q_0}(w_4^q - w_4)
\end{aligned} \tag{4.4}$$

We have separated these equations into groups of similar form. We call the w_i which appear on the left hand side of (4.4) of type 1 and the w_i on the right hand side of type 2.

We give an example to show how the expressions in (4.4) are useful for computing derivatives. To compute the derivatives of y, we let $h = x^{q_0}(x^q - x)$. Since $y^q - y = h$, we may expand y as a series in h whose tail is contained in the kernel of any of the derivations we wish to apply. To compute $D^i y$ for $i < q^2$, we consider

$$y = -h - h^q + y^{q^2} \equiv -h - h^q \mod \overline{\mathbb{F}}_q(X)^{q^2},$$

since $\overline{\mathbb{F}}_q(X)^{q^2} = \bigcap_{i=1}^{q^2-1} \ker D^i$. Then

$$D^i y = -D^i h - (D^{i/q} h)^q.$$

In this manner, the derivatives of y are written in terms of derivatives of h, which can be determined using the basic properties of Hasse derivatives.

Each equation in (4.4) is of a similar form, with each new function written in terms of previous ones. Therefore, one may in principle write down any derivative $D^i f$ with $f \in \mathcal{B}$ as an element of $\mathbb{F}_q[x, y, z]$ using this method.

For each $f \in \mathcal{B}$, we construct a set S_f containing all indices $0 \leq i \leq q^2$ such that $D^i f \neq 0$, which we refer to as the *support* of f. We make no claims that $D^i f \neq 0$ for all i in S_f. By direct calculation as in the example above, the sets

$$\begin{aligned}
S_{x^q-x} &= \{0, 1, q\} \\
S_{y^q-y} &= \{0, 1, q_0, q_0 + 1, q, q + q_0\} \\
S_y &= \{0, 1, q_0, q_0 + 1, q, q + q_0, qq_0, qq_0 + q, q^2\} \\
S_{z^q-z} &= \{0, 1, q_0, q_0 + 1, 2q_0, 2q_0 + 1, q, q + q_0, q + 2q_0\} \\
S_z &= \{0, 1, q_0, q_0 + 1, 2q_0, 2q_0 + 1, q, \\
&\qquad q + q_0, q + 2q_0, qq_0, qq_0 + q, 2qq_0, 2qq_0 + q, q^2\}
\end{aligned}$$

satisfy the desired conditions.

Now we construct S_{w_i} for $i = 1, \ldots, 10$. For $n \geq 1$ and $A, B \subset \{0, \ldots, q^2\}$ we use the notation

$$\begin{aligned}
nA &= \{na : a \in A\} \cap [0, q^2], \\
A + B &= \{a + b : a \in A, b \in B\} \cap [0, q^2].
\end{aligned}$$

Since $w_1^q - w_1 = x^{3q_0}(x^q - x)$, we define

$$\begin{aligned}
S_{w_1^q-w_1} &= 3q_0 S_x + S_{x^q-x} \\
&= \{0, 3q_0\} + \{0, 1, q\} = \{0, 1, 3q_0, 3q_0 + 1, q, q + 3q_0\}
\end{aligned}$$

and

$$\begin{aligned}
S_{w_1} &= S_{w_1^q-w_1} \cup qS_{w_1^q-w_1} \\
&= \{0, 1, 3q_0, 3q_0 + 1, q, q + 3q_0, 3qq_0, 3qq_0 + q, q^2\}.
\end{aligned}$$

Similarly, we define $S_{w_2^q-w_2} = 3q_0 S_y + S_{x^q-x}$ and $S_{w_2} = S_{w_2^q-w_2} \cup qS_{w_2^q-w_2}$, and so on, using the equations in (4.4) as a guide.

Let S denote the union of the S_f with $f \in \mathcal{B}$. Since we will use these sets later, we collect their values in Tables 4.2 and 4.3 at the end of current chapter. In these tables, an asterisk in row i and column f indicates that i

is in the set S_f. In particular, $D^i f = 0$ wherever there is a blank entry in the table. Note in particular that

$$S_x \subset S_{w_1} \subset S_{w_2} \subset S_{w_3} \subset S_{w_6} = S_{w_8}$$

and

$$S_y \subset S_z \subset S_{w_4} \subset S_{w_7} \subset S_{w_5} \subset S_{w_9} \subset S_{w_{10}}.$$

For $s = 1$, the indices appearing in the tables are not all distinct, since for example $3q = qq_0$. To avoid any complications this may cause, we assume going forward that $s \geq 2$. Computations performed in Magma [BCP] have verified the statements of all our results for $s = 1$.

4.3 Computation of Orders

In this section we compute the orders of $\mathcal{D}$.

Theorem 4.1. *The orders of $\mathcal{D}$ are*

$$0,\ 1,\ q_0,\ 2q_0,\ 3q_0,\ q,\ q+q_0,\ 2q,\ qq_0,\ qq_0+q_0,\ qq_0+q,\ 2qq_0,\ 3qq_0,\ q^2.$$

Since $\mathcal{D} \subset \mathcal{D}_X$, these form a subset of the orders of $\mathcal{D}_X$.

Lemma 4.4. *The orders of $\mathcal{D}$ which are less than q are 0, 1, q_0, $2q_0$, and $3q_0$.*

Proof. That $\epsilon_0(\mathcal{D}) = 0$ and $\epsilon_1(\mathcal{D}) = 1$ is clear. The rest follows from Lemma 4.3. Indeed, the orders of the morphism

$$\begin{aligned}(x^q - x : y^q - y : z^q - z : w_1^q - w_1 : w_2^q - w_2 : \cdots)\\ = (1 : x^{q_0} : x^{2q_0} : x^{3q_0} : y^{3q_0} : \cdots)\end{aligned}$$

which are less than q are 0, q_0, $2q_0$, and $3q_0$, so these are the Frobenius orders of $\mathcal{D}$ which are less than q. There is only one order of $\mathcal{D}$ which is not a Frobenius order, and this is $\epsilon_1(\mathcal{D})$. □

In light of Lemma 3, the fact that $\nu_1(\mathcal{D}) = \epsilon_2(\mathcal{D}) > 1$ means that the matrix

$$\begin{pmatrix} x^q - x & y^q - y & z^q - z & \cdots & w_{10}^q - w_{10} \\ 1 & D^1 y & D^1 z & \cdots & D^1 w_{10} \end{pmatrix}$$

has rank 1, so that

$$f^q - f = (x^q - x)D^1 f \tag{4.5}$$

holds for all $f \in \mathcal{B}$. Applying the derivatives D^q and D^{kq_0} for $k = 1, 2, 3$ to the previous equation gives the identities

$$D^{kq_0} f = -(x^q - x)D^{kq_0+1} f, \qquad k = 1, 2, 3 \tag{4.6}$$

$$D^q(f^q - f) = D^1 f + (x^q - x)D^{q+1} f \tag{4.7}$$

which hold for all $f \in \mathcal{B}$. These will be used extensively in what follows.

From (4.1), we have for any $P \in X$ a linear equivalence

$$\mathrm{Fr}^4(P) + 3q_0\,\mathrm{Fr}^3(P) + 2q\,\mathrm{Fr}^2(P) + 3qq_0\,\mathrm{Fr}(P) + q^2 P \sim mP_\infty.$$

If $P \notin X(\mathbb{F}_q)$, then the terms on the left hand side involve distinct points since X has no places of degrees 2, 3, or 4 over $\mathbb{F}_q$. By applying some multiple of the Frobenius to this equivalence, we obtain each of 1, $3q_0$, $2q$, $3qq_0$, and q^2 as orders of $\mathcal{D}_X$, as in [FT, Lemma 3.2]. By the p-adic criterion it follows that q is also an order of $\mathcal{D}_X$. That said, it is not immediately clear that these are orders of the linear series $\mathcal{D}$. We show now that these are in fact the orders of the subseries $\mathcal{E} \subset \mathcal{D}$ corresponding to $V_{\mathcal{E}} = \overline{\mathbb{F}}_q\langle 1, x, w_1, w_2, w_3, w_6, w_8\rangle$, and hence are orders of $\mathcal{D}$.

Theorem 4.5. *The orders of* $\mathcal{E}$ *are* 0, 1, $3q_0$, q, $2q$, $3qq_0$, *and* q^2.

For ease of notation we write $\ell = x^q - x$ in the proof of the next lemma and throughout the rest of this chapter.

Lemma 4.6. *The image in* $\mathbb{P}^6$ *of the map* $\phi_{\mathcal{E}} = (1 : x : w_1 : w_2 : w_3 : w_6 : w_8)$ *lies on the hypersurface*

$$\sum_{i+j=6} X_i^{q^2} X_j = 0.$$

Proof. By using (4.4) one finds that

$$\begin{aligned}
w_8^{q^2} + w_8 &= (w_7^{3q_0})^q \ell^q + w_7^{3q_0}\ell - w_8\\
xw_6^{q^2} + x^{q^2} w_6 &= ((w_4^{3q_0})^q x + w_6)\ell^q + (w_4^{3q_0} x + w_6)\ell - xw_6\\
w_1 w_3^{q^2} + w_1^{q^2} w_3 &= ((z^{3q_0})^q w_1 + (x^{3q_0})^q w_3)\ell^q\\
&\qquad + (z^{3q_0} w_1 + x^{3q_0} w_3)\ell - w_1 w_3
\end{aligned}$$

$$w_2^{q^2+1} = (y^{3q_0})^q w_2 \ell^q + y^{3q_0} w_2 \ell + w_2^2.$$

Summing these and collecting terms involving common powers of ℓ gives an expression of the form

$$A_{-1} + A_0 \ell + A_1 \ell^q.$$

That each $A_i = 0$ on X may be verified using (2.2) and (4.4), along with some of the 105 equations found in [ED]. This calculation is carried out explicitly as a part of the proof of Lemma 3.12. □

Lemma 4.7. *The largest order of $\mathcal{E}$ is q^2.*

Proof. Because the coefficients a_i of $m(t) = t^4 + 3q_0 t^3 + 2qt^2 + 3qq_0 t + q^2$ satisfy $a_0 \geq a_2 \geq \cdots \geq a_4$ and $\#X(\mathbb{F}_q) > q(m - a_0) + 1$, it follows from [FGT, Prop 3.4] that the largest order of $\mathcal{D}_X$ is q^2 (our numbering of the coefficients a_i is opposite that found in the reference). Since each order of $\mathcal{E}$ is an order of $\mathcal{D}_X$, no order of $\mathcal{E}$ is greater than q^2. We exhibit a family of functions g_P in $V_{\mathcal{E}}$ parameterized by P in X which vanish to order at least q^2 at P.

Write $(1, x, w_1, w_2, w_3, w_6, w_8) = (f_0, \ldots, f_6)$. Then by Lemma 4.6, the function

$$G(P, Q) = \sum_{i+j=6} f_i^{q^2}(P) f_j(Q)$$

vanishes on the diagonal of $X \times X$. Choose any $P \in X \smallsetminus \{P_\infty\}$. Then $g_P = G(P, \cdot)$ and $h_P = G(\cdot, P)$ are functions on X which vanish at P, and g_P is in $V_{\mathcal{E}}$. Since

$$h_P = \sum_{i+j=6} f_j(P) f_i^{q^2} = \left(\sum_{i+j=6} f_j(P)^{1/q^2} f_i \right)^{q^2},$$

the function h_P vanishes at P to order at least q^2. But

$$\begin{aligned} g_P - h_P &= \sum_{i+j=6} f_i^{q^2}(P) f_j - f_j(P) f_i^{q^2} \\ &= \sum_{i+j=6} (f_i^{q^2}(P) - f_i^{q^2})(f_j(P) + f_j) + f_i^{q^2} f_j - f_i^{q^2}(P) f_j(P) \\ &= \sum_{i+j=6} (f_i(P) - f_i)^{q^2} (f_j(P) + f_j) \end{aligned}$$

also vanishes at P to order at least q^2, hence so does g_P. Since P was chosen in an open subset of X, q^2 is an order of $\mathcal{E}$. □

Remark. The proof of the preceding lemma shows that

$$\sum_{i+j=6} f_i^{q^2}(P)X_j = 0$$

is the equation of the osculating hyperplane at P, and that the function $X \to \mathrm{Div}(X)$ taking $P \mapsto \mathrm{div}(g_P)$ assigns to P the corresponding hyperplane section.

Proof of Theorem 4.5. Let M be the matrix of derivatives $[D^i f_j]$ with $i \in \{0, 1, 3q_0+1, q+3q_0+1, 2q+3q_0+1\}$ and $f_j \in \{1, x, w_1, w_2, w_3\}$. By referring to Table 4.2 we see that the matrix M is upper triangular. Moreover, one may check by hand that each diagonal entry is equal to 1. Thus, there are at least 5 orders ϵ of $\mathcal{E}$ with $\epsilon \le 2q + 3q_0 + 1$.

Let $I_{\mathcal{E}} = \{0, 1, 3q_0, q, 2q, 3qq_0, q^2\}$ be the proposed set of orders. The subset of $S_{w_8} \smallsetminus I_{\mathcal{E}}$ of elements minimal with respect to the partial order $\le_3$ is

$$J = \{3q_0 + 1, q + 1, q + 3q_0, 3q, 3qq_0 + 1, 3qq_0 + 3q_0, 3qq_0 + q, 6qq_0\}.$$

By the p-adic criterion, to prove the theorem it will suffice to show that no $j \in J$ is an order of $\mathcal{E}$. In fact, it will be enough to show that no $j \in \{3q_0 + 1, q + 1, q + 3q_0, 3q\}$ is an order. For then we will already know that the six elements of $I_{\mathcal{E}} \smallsetminus \{3qq_0\}$ are orders. Then exactly one of the remaining elements of J is the seventh and final order of $\mathcal{E}$. But each of the remaining elements satisfies $j \ge_3 3qq_0$, so this final order is $3qq_0$.

That $3q_0 + 1$ is not an order follows from (4.6). Let w be one of the functions w_1, w_2, w_3, w_6, w_8. Each of these is of the form

$$w \equiv -h - h^q \mod \overline{\mathbb{F}}_q(X)^{q^2},$$

where $h = f^{3q_0}(x^q - x)$ and $f \in \{x, y, z, w_4, w_7\}$. Then $D^k w = -D^k h -$

$(D^{k/q}h)^q$ and

$$\begin{aligned} D^k h &= \sum_{3q_0 i + j = k} (D^i f)^{3q_0} D^j (x^q - x) \\ &= (x^q - x)(D^{\frac{k}{3q_0}} f)^{3q_0} - (D^{\frac{k-1}{3q_0}} f)^{3q_0} + (D^{\frac{k-q}{3q_0}} f)^{3q_0}. \end{aligned}$$

We calculate

$$\begin{aligned} D^{3q_0+1} w &= (D^1 f)^{3q_0} \\ D^{q+3q_0} w &= -(D^1 f)^{3q_0} - \ell (D^{q_0+1} f)^{3q_0} \\ D^q w &= (f^q - f)^{3q_0} - \ell (D^{q_0} f)^{3q_0} \\ D^{2q} w &= -(D^{q_0} f)^{3q_0} - \ell (D^{2q_0} f)^{3q_0} \\ D^{q+1} w &= (D^{q_0} f)^{3q_0} \\ D^{3q} w &= -(D^{2q_0} f)^{3q_0}. \end{aligned} \tag{4.8}$$

Then by using these along with (4.5) and (4.6), one immediately verifies that

$$\begin{aligned} \ell D^{q+1} w + D^q w &= \ell^{3q_0} D^{3q_0+1} w \\ \ell^{3q_0} D^{q+3q_0} w + D^q w &= 0 \\ \ell D^{3q} w &= D^{2q} w + D^{q+1} w, \end{aligned}$$

and so $q+1$, $q+3q_0$, and $3q$ are not orders of $\mathcal{D}$. This completes the proof. □

Up to this point we have shown that the nine numbers

$$0,\ 1,\ q_0,\ 2q_0,\ 3q_0,\ q,\ 2q,\ 3qq_0,\ q^2$$

are orders of $\mathcal{D}$, and it remains to show that $q + q_0$, qq_0, $qq_0 + q_0$, $qq_0 + q$, and $2qq_0$ are orders.

Proof of Theorem 4.1. Let $I_{\mathcal{D}}$ be the list of orders of $\mathcal{D}$ proposed in the statement of the theorem. Let M be the 12 by 12 matrix of derivatives $[D^i f_j]$ with i in

$$\{0, 1, q_0 + 1, 2q_0 + 1, 3q_0 + 1, q + 3q_0 + 1, 2q + 3q_0 + 1, qq_0 + 2q + q_0, \\ qq_0 + q + 2q_0 + 1, qq_0 + 2q + 3q_0, qq_0 + 3q + 3q_0, 2qq_0 + 3q_0 + 1\}$$

and f_j in $\{1, x, y, z, w_1, w_2, w_3, w_4, w_7, w_5, w_9, w_{10}\}$. Tables 4.2 and 4.3 assure that M is upper triangular. Moreover, one may check by hand that each diagonal entry is equal to 1, except the last, which is x^{2q}. Thus there are at least 11 orders which are less than $2qq_0$, and 12 orders which are at most $2qq_0 + 3q_0 + 1$. Since there are 14 orders in total, and we already know that $3qq_0$ and q^2 are among them, to prove the theorem it will be enough to show that no element of $(S \smallsetminus I_{\mathcal{D}}) \cap [0, 2qq_0 + 3q_0 + 1]$ is an order.

By the p-adic criterion, it suffices to check elements of this set which are minimal with respect to $\leq_3$. These elements comprise the set

$$\begin{aligned} J = \{&q_0 + 1, 3q_0 + 1, q + 1,\ q + 2q_0,\ q + 3q_0,\ 2q + q_0,\ 3q,\ qq_0 + 1, \\ &qq_0 + 2q_0,\ qq_0 + 3q_0,\ qq_0 + q + q_0,\ qq_0 + 2q,\ 2qq_0 + q_0\}. \end{aligned} \tag{4.9}$$

In fact, it will be enough to demonstrate that each element of $J \smallsetminus \{2qq_0 + q_0\}$ is not an order, since $2qq_0 \leq_3 2qq_0 + q_0$.

That $q_0 + 1$ and $3q_0 + 1$ are not orders follows from Lemma 4.4. To deal with each remaining ten elements $j \in J$, we give a differential equation

$$c_j D^j f + \sum_{i<j} c_i D^i f = 0, \qquad c_i \in \mathbb{F}_q(X)$$

which is satisfied by all $f \in \mathcal{B}$. These are listed in the following lemma, and proven in the next section. This will complete the proof of the theorem. □

Lemma 4.8. *The following differential equations are satisfied by each $f \in \mathcal{B}$:*

(A1) $\ell^{q_0} D^{q_0+1} f + \ell^{2q_0} D^{2q_0+1} f + \ell^{3q_0} D^{3q_0+1} f = D^q f + \ell D^{q+1} f$

(A2) $\ell^{q_0}(D^{q+2q_0} f + D^{2q_0+1}) f = D^{q+q_0} f + D^{q_0+1} f$

(A3) $D^q f + \ell^{q_0} D^{q+q_0} f + \ell^{2q_0} D^{q+2q_0} f + \ell^{3q_0} D^{q+3q_0} f = 0$

(A4) $\ell D^{2q+q_0} f = D^{q_0+1} f + D^{q+q_0} f$

(A5) $\ell D^{3q} f = D^{2q} f + D^{q+1} f$

(A6) $\ell D^{qq_0+1} f + D^{qq_0} f = \ell^q(\ell^{q_0} D^{2q_0+1} f - D^{q_0+1} f)$

(A7) $\ell^{2q_0} D^{qq_0+2q_0} f - \ell^{q_0} D^{qq_0+q_0} f = \ell^q(D^{q_0+1} f + D^{q+q_0} f)$

(A8) $\ell^{q_0} D^{qq_0+q_0} f + \ell^{2q_0} D^{qq_0+2q_0} f + \ell^{3q_0} D^{qq_0+3q_0} f = \ell D^{qq_0+1} f$

(A9) $\ell^{q+q_0+1}D^{qq_0+q+q_0}f = (\ell^q - \ell)\ell^{q_0}D^{qq_0+q_0}f$

(A10) $\ell^{2q}(\ell D^{qq_0+2q}f - D^{qq_0+1}f) = (\ell^q - \ell)(\ell^q D^{qq_0+q}f + D^{qq_0}f)$.

Proof. The fact that x, y, and z satisfy these equations may be verified without difficulty by hand. If f is of type 1, then by consulting Tables 4.2 and 4.3 we see that the only equations among (A1)–(A10) in which nonzero derivatives of f appear are (A1), (A3), and (A5), and, keeping in mind that some of the terms are zero for f of type 1, these are the equations which were verified in the proof of Theorem 4.5. The proof for functions of type 2 is contained in the next section. □

4.4 Verification of Some Differential Equations

Before proceeding to verify equations (A1)–(A10) for functions of type 2, we first list a few identities for w of type 1 which will be useful for this task. For w of type 1, write $w^q - w = f^{3q_0}(b^q - b)$ as in the proof of Theorem 4.5. Then $D^{2q+1}w = (D^{2q_0}f)^{3q_0}$, and so by (4.8), we have

$$\ell D^{2q+1}w + D^{2q}w + D^{q+1}w = 0. \tag{4.10}$$

Also, from the proof of Theorem 4.5 we recall that

$$D^q w + \ell D^{q+1}w = \ell^{3q_0}D^{3q_0+1}w, \tag{4.11}$$

$$\ell^{3q_0}D^{q+3q_0}w + D^q w = 0. \tag{4.12}$$

Now let w be of type 2. From (4.4), w may be written in the form $w = t_1 - t_2$, where t_i satisfies

$$t_i^q - t_i = h_i = f_i^{q_0}(b_i^q - b_i),$$

for some $f_i \in \{w_1, w_2, w_3, w_6\}$ and $b_i \in \{x, y, z, w_4\}$. Thus, if one of the desired equations holds for all t_i of this form, then it also holds for w. This will be the case for some but not all of the equations we wish to verify.

Let t, h, f, b be as above. Then

$$D^k h = \sum_{q_0 i + j = k} (D^i f)^{q_0} D^j (b^q - b)$$

and

$$D^i t = -D^i h - (D^{i/q} h)^q.$$

Taking into account the supports of f and b and using (4.5) and (4.6) to make simplifications, we compute the derivatives of t which appear in equations (A1)–(A10).

$$\begin{aligned}
D^{kq_0+1} t &= f^{q_0} D^{kq_0+1} b + (D^1 f)^{q_0} D^{(k-1)q_0+1} b, \qquad k = 1, 2, 3 \\
D^q t &= f^{q_0} D^q b + (D^1 f)^{q_0} \ell^{q_0} D^q (b^q) + (D^{3q_0+1} f)^{q_0} \ell^{q_0+1} D^1 b \\
D^{q+1} t &= f^{q_0} D^{q+1} b - (D^{3q_0+1} f)^{q_0} \ell^{q_0} D^1 b \\
D^{q+q_0} t &= f^{q_0} D^{q+q_0} b - (D^1 f)^{q_0} D^q (b^q - b) \\
&\quad + (D^{3q_0+1} f)^{q_0} (\ell^{q_0+1} D^{q_0+1} b - \ell D^1 b) \\
D^{q+2q_0} t &= f^{q_0} D^{q+2q_0} b + (D^1 f)^{q_0} D^{q+q_0} b \\
&\quad + (D^{3q_0+1} f)^{q_0} (\ell^{q_0+1} D^{2q_0+1} b - \ell D^{q_0+1} b) \\
D^{q+3q_0} t &= f^{q_0} D^{q+3q_0} b + (D^1 f)^{q_0} D^{q+2q_0} b - (D^{3q_0+1} f)^{q_0} \ell D^{2q_0+1} b \\
D^{2q} t &= f^{q_0} D^{2q} b + (D^{3q_0+1} f)^{q_0} \ell^{q_0} D^q (b^q - b) \\
D^{2q+q_0} t &= f^{q_0} D^{2q+q_0} b + (D^1 f)^{q_0} D^{2q} b \\
&\quad - (D^{3q_0+1} f)^{q_0} (\ell^{q_0} D^{q+q_0} b + D^q (b^q - b)) \\
D^{3q} t &= f^{q_0} D^{3q} b - (D^{3q_0+1} f)^{q_0} \ell^{q_0} D^{2q} b \\
D^{qq_0} t &= f^{q_0} D^{qq_0} b + (D^1 f)^{q_0} \ell^{q_0} D^{qq_0} (b^q) \\
&\quad - (D^q f)^{q_0} \ell D^1 b - (D^q f^q)^{q_0} \ell^q D^q (b^q) \\
D^{qq_0+1} t &= f^{q_0} D^{qq_0+1} b + (D^q f)^{q_0} D^1 b \\
D^{qq_0+q_0} t &= f^{q_0} D^{qq_0+q_0} b - (D^1 f)^{q_0} D^{qq_0} (b^q - b) \\
&\quad - (D^q f)^{q_0} \ell D^{q_0+1} b - (D^{q+1} f)^{q_0} \ell D^1 b \\
D^{qq_0+2q_0} t &= f^{q_0} D^{qq_0+2q_0} b + (D^1 f)^{q_0} D^{qq_0+q_0} b \\
&\quad - (D^q f)^{q_0} \ell D^{2q_0+1} b - (D^{q+1} f)^{q_0} \ell D^{q_0+1} b. \\
D^{qq_0+3q_0} t &= f^{q_0} D^{qq_0+3q_0} b - (D^{q+1} f)^{q_0} \ell D^{2q_0+1} b
\end{aligned}$$

$$\begin{aligned}
D^{qq_0+q}t &= f^{q_0}D^{qq_0+q}b + (D^1 f)^{q_0}\ell^{q_0}D^{qq_0+q}(b^q) \\
&\quad - (D^{3q_0+1}f)^{q_0}\ell^{q_0}(D^{qq_0}b - D^{qq_0}(b^q)) - (D^q f)^{q_0}D^q(b^q - b) \\
&\quad - (D^{q+3q_0}f)^{q_0}\ell D^1 b + (D^q f^q)^{q_0}D^q(b^q) \\
D^{qq_0+q+q_0}t &= f^{q_0}D^{qq_0+q+q_0}b - (D^1 f)^{q_0}D^{qq_0+q}(b^q - b) \\
&\quad - (D^{3q_0+1}f)^{q_0}(\ell^{q_0}D^{qq_0+q_0}b + D^{qq_0}(b^q - b)) + (D^q f)^{q_0}D^{q+q_0}b \\
&\quad - (D^{q+1}f)^{q_0}D^q(b^q - b) + (D^{q+3q_0}f)^{q_0}D^{q_0}b - (D^{q+3q_0+1}f)^{q_0}\ell D^1 b \\
D^{qq_0+2q}t &= f^{q_0}D^{qq_0+2q}b + (D^{3q_0+1}f)^{q_0}\ell^{q_0}D^{qq_0+q}(b^q - b) \\
&\quad - (D^q f)^{q_0}D^{2q}(b^q - b) - (D^{q+3q_0}f)^{q_0}D^q(b^q - b).
\end{aligned}$$

We will also use a few of the values $D^i b$, which are collected in the following table.

Table 4.1: Select derivatives $D^i b$

i	$D^i y$	$D^i z$	$D^i w_4$
1	x^{q_0}	x^{2q_0}	$-x^{2q_0+1} - x^{q_0}y - z$
q_0+1	1	$-x^{q_0}$	$x^{q_0+1} - y$
$2q_0+1$	0	1	$-x^q$
$q+1$	0	0	$-\ell^{2q_0}$
$q+q_0$	-1	x^{q_0}	$\ell^{q_0+1} - x^{q_0+1} + y$
$2q$	0	0	ℓ^{2q_0}
qq_0+1	0	0	$-\ell^{q+q_0}$
qq_0+q_0	0	0	$-\ell^{q+1}$

Now we verify each of the equations (A1)–(A10) in turn. Since each b_i associated with w appears before w in the list

$$x,\ y,\ z,\ w_4,\ w_5,\ w_7,\ w_9,\ w_{10},$$

and since each of (A1)–(A10) has already been verified for x, y, and z, we may assume by induction that these equations are satisfied by each b_i which appears in the proof.

Proof of (A1). We show that the desired equation holds for all t. Since $D^{3q_0+1}b = 0$, we have

$$\begin{aligned}
\sum_{k=1}^{3}\ell^{kq_0}D^{kq_0+1}t &= f^{q_0}\sum_{k=1}^{3}\ell^{kq_0}D^{kq_0+1}b + (D^1 f)^{q_0}\ell^{q_0}(D^1 b + \sum_{k=1}^{3}\ell^{kq_0}D^{kq_0+1}b) \\
&= f^{q_0}(\ell D^{q+1}b + D^q b) + (D^1 f)^{q_0}\ell^{q_0}(D^1 b + D^q b + \ell D^{q+1}b)
\end{aligned}$$

$$\begin{aligned} &= f^{q_0}(\ell D^{q+1}b + D^q b) + (D^1 f)^{q_0}\ell^{q_0} D^q(b^q) \\ &= D^q t + \ell D^{q+1} t, \end{aligned}$$

where we used (4.7) in the third line. □

Proof of (A2). Let

$$\Delta_t := \ell^{q_0}(D^{q+2q_0}t + D^{2q_0+1}t) - (D^{q+q_0}t + D^{q_0+1}t).$$

Here it is not the case that $\Delta_t = 0$ for all t, so we need to show that $\Delta_{t_1} = \Delta_{t_2}$ for each $w = t_1 - t_2$. The contribution to Δ_t of those terms involving f^{q_0} is zero by our assumption on b. Moreover, by (4.7) the contributed coefficient of $(D^1 f)^{q_0}$ is

$$\begin{aligned} &\ell^{q_0} D^{q+q_0}b + \ell^{q_0} D^{q_0+1}b + D^q(b^q - b) - D^1 b \\ &\quad = \ell^{q_0} D^{q+q_0}b + \ell^{q_0} D^{q_0+1}b + \ell D^{q+1}b, \end{aligned}$$

which is zero by Table 4.1. Therefore, the only terms giving a contribution to Δ_t are those involving $(D^{3q_0+1}f)^{q_0}$. The coefficient of $(D^{3q_0+1}f)^{q_0}$ in Δ_t is

$$\sum_{k=0}^{2} \ell^{kq_0+1} D^{kq_0+1}b = \ell(D^1 b + D^q b + D^{q+1}b) = \ell D^q(b^q),$$

where we have used the fact that $D^{3q_0+1}b = 0$, along with (4.7) and (A1). With the exception of $w = w_7$ we have $f_i^q - f_i = b_j^{3q_0}(x^q - x)$ for $i \neq j$, so that

$$(D^{3q_0+1}f_i)^{q_0} = (D^{3q_0}(b_j^{3q_0}))^{q_0} = D^q(b_j^q).$$

Therefore, for $w \neq w_7$ we have

$$\Delta_{t_i} = D^q(b_j^q) \cdot \ell D^q(b_i^q),$$

and so $\Delta_{t_1} = \Delta_{t_2}$ as desired. Finally, for $w = w_7$ we check that

$$D^q(y^q) \cdot \ell D^q(y^q) = x^{2qq_0}\ell = D^q(z^q) \cdot \ell D^q(x^q). \qquad \square$$

Proof of (A3). We show that the desired equation holds for all t. Since

$D^{q+3q_0}b = 0$, we have

$$\sum_{k=0}^{3} \ell^{kq_0} D^{q+kq_0} t = f^{q_0} \sum_{k=0}^{3} \ell^{kq_0} D^{q+kq_0} b \\ + (D^1 f)^{q_0} \ell^{q_0} \sum_{k=0}^{3} \ell^{kq_0} D^{q+kq_0} b + (D^{3q_0+1} f)^{q_0} \cdot 0 = 0. \square$$

Proof of (A4). We show that the desired equation holds for all t. The contribution of the terms involving f^{q_0} is zero by our assumption on b. By considering the contribution of terms involving $(D^1 f)^{q_0}$ and $(D^{3q_0+1} f)^{q_0}$, it will suffice to show that the equations

$$D^q(b^q - b) + D^1 b = \ell D^{2q} b$$
$$\ell^{q_0} D^{q_0} b + \ell D^1 b = \ell^{q_0+1} D^{q+q_0} b + \ell D^q(b^q - b)$$

hold for $b = x, y, z, w_4$. These may be rewritten using (4.7) as

$$D^{2q} b + D^{q+1} b = 0$$
$$\ell^{q_0} D^{q+q_0} b + \ell D^{q+1} b + \ell^{q_0} D^{q_0+1} b = 0,$$

and these follow from Table 4.1. □

Proof of (A5). We show that the desired equation holds for all t. By our assumption on b, the contribution of all terms involving f^{q_0} is zero. By comparing the coefficients of $(D^{3q_0+1} f)^{q_0}$ and using (4.7), it suffices to show that

$$\ell D^{2q} b = D^1 b - D^q(b^q - b) = -\ell D^{q+1} b.$$

This follows from Table 4.1. □

Proof of (A6). Let

$$\Delta_t = \ell D^{qq_0+1} t + D^{qq_0} t - \ell^q(\ell^{q_0} D^{2q_0+1} t - D^{q_0+1} t).$$

By our assumption on b, the terms in Δ_t involving f^{q_0} sum to zero. Moreover, the terms involving $(D^q f)^{q_0}$ also give no contribution to Δ_t. After some simplification, the sum of the remaining terms is ℓ^q times

$$(D^1 f)^{q_0} D^1 b - ((D^1 f)^{q_0} D^1 b)^q - (D^1 f)^{q_0} \ell^{q_0} (D^{q_0+1} b + (D^{q_0+1} b)^q).$$

Note that $(D^1 f)^{q_0} = c^q$, where $f^q - f = c^{3q_0}(x^q - x)$ and $c \in \{x, y, z, w_4\}$. Thus, Δ_t is ℓ^q times

$$c^q D^1 b - (c^q D^1 b)^q - c^q \ell^{q_0}(D^{q_0+1} b + (D^{q_0+1} b)^q).$$

That $\Delta_1 = \Delta_2$ may now be checked in each case by using Table 4.1. □

Proof of (A7). Let

$$\Delta_t = \ell^{2q_0} D^{qq_0+2q_0} t - \ell^{q_0} D^{qq_0+q_0} t - \ell^q D^{q_0+1} t - \ell^q D^{q+q_0} t.$$

By our assumption on b, the contribution to Δ_t of those terms involving f^{q_0} is zero. The contribution of the terms involving $(D^1 f)^{q_0}$ is

$$\begin{aligned} &\ell^{2q_0} D^{qq_0+q_0} b + \ell^{q_0} D^{qq_0}(b^q - b) + \ell^q D^q(b^q - b) - \ell^q D^1 b \\ &\quad = \ell^{2q_0} D^{qq_0+q_0} b + \ell^{q_0+1} D^{qq_0+1} b + \ell^{q+1} D^{q+1} b. \end{aligned}$$

This is also zero by Table 4.1. Then using (4.11), we may rewrite the sum of the remaining terms as

$$\begin{aligned} \Delta_t = (\ell^{3q_0} D^{3q_0+1} f)^{q_0} \ell^{q_0} D^{q_0} b \\ - (\ell^{3q_0} D^{3q_0+1} f)^{q_0}(\ell^{2q_0} D^{2q_0} b + \ell^{q_0} D^{q_0} b - \ell D^1 b) \\ + (\ell D^{q+1} f)^{q_0}(\ell^{2q_0} D^{2q_0} b + \ell^{q_0} D^{q_0} b - \ell D^1 b). \end{aligned}$$

As in the proof of (A2), we have

$$\ell^{2q_0} D^{2q_0} b + \ell^{q_0} D^{q_0} b - \ell D^1 b = \ell D^q(b^q).$$

Furthermore, if $c \in \{x, y, z, w_4\}$ with $f^q - f = c^{3q_0}(x^q - x)$, then $(D^{3q_0+1} f)^{q_0} = D^q(c^q)$ and $(D^{q+1} f)^{q_0} = (D^{q_0} c)^q$. Therefore,

$$\Delta_t = \ell^{q_0} D^q(c^q) D^{q_0} b - \ell D^q(c^q) D^q(b^q) + \ell (D^{q_0} c)^q D^q(b^q).$$

Now Table 4.1 may be used to verify in each case that $\Delta_{t_1} = \Delta_{t_2}$. □

Proof of (A8). By using (4.11), the terms on the left hand side of the desired equation may be written as

$$\begin{aligned}\ell^{q_0}D^{qq_0+q_0}t &= f^{q_0}\ell^{q_0}D^{qq_0+q_0}b-(D^1f)^{q_0}\ell^{q_0}D^{qq_0}(b^q-b)\\ &\quad-(\ell^{3q_0}D^{3q_0+1}f)^{q_0}\ell D^1b+(D^qf)^{q_0}(\ell^{q_0}D^{q_0}b+\ell D^1b)\\ \ell^{2q_0}D^{qq_0+2q_0}t &= f^{q_0}\ell^{2q_0}D^{qq_0+2q_0}b+(D^1f)^{q_0}\ell^{2q_0}D^{qq_0+q_0}b\\ &\quad+(\ell^{3q_0}D^{3q_0+1}f)^{q_0}\ell^{q_0}D^{q_0}b+(D^qf)^{q_0}(\ell^{2q_0}D^{2q_0}b-\ell^{q_0}D^{q_0}b)\\ \ell^{3q_0}D^{qq_0+3q_0}t &= f^{q_0}\ell^{3q_0}D^{qq_0+3q_0}b\\ &\quad+(\ell^{3q_0}D^{3q_0+1}f)^{q_0}\ell^{2q_0}D^{2q_0}b-(D^qf)^{q_0}\ell^{2q_0}D^{2q_0}b.\end{aligned}$$

By our assumption on b, the contribution of the terms involving f^{q_0} is zero. The terms involving $(D^qf)^{q_0}$ sum to zero. The sum of the terms involving $(D^{3q_0+1}f)^{q_0}$ is ℓ^q times the quantity which was dealt with (A2), so by the same argument these give no contribution to $\Delta_{t_1}-\Delta_{t_2}$. It remains only to show that the terms involving $(D^1f)^{q_0}$ sum to zero, i.e., that

$$\ell^{2q_0}D^{qq_0+q_0}b=\ell^{q_0}D^{qq_0}(b^q-b)=\ell^{q_0+1}D^{qq_0+1}b.$$

But this follows from Table 4.1. □

Proof of (A9). We show that the desired equation holds for all t. Use (4.11) and (4.12) to write each side of the desired equation as

$$\begin{aligned}\ell^{q_0}D^{qq_0+q_0}t &= f^{q_0}\ell^{q_0}D^{qq_0+q_0}b-(D^1f)^{q_0}\ell^{q_0}D^{qq_0}(b^q-b)\\ &\quad-\ell^q(D^{3q_0+1}f)^{q_0}(b^q-b)+(D^qf)^{q_0}(\ell^{q_0}D^{q_0}b+(b^q-b))\end{aligned}$$

and

$$\begin{aligned}\ell^{q+q_0}D^{qq_0+q+q_0}t &= f^{q_0}\ell^{q+q_0}D^{qq_0+q+q_0}b-(D^1f)^{q_0}\ell^{q+q_0}D^{qq_0+q}(b^q-b)\\ &\quad-\ell^q(D^{3q_0+1}f)^{q_0}(\ell^{2q_0}D^{qq_0+q_0}b\\ &\qquad+\ell^{q_0}D^{qq_0}(b^q-b)+\ell^qD^q(b^q-b)-\ell D^1b)\\ &\quad+(D^qf)^{q_0}\left(\ell^{q+q_0}D^{q+q_0}b+\ell^qD^q(b^q-b)-\ell^{q_0}D^{q_0}b-\ell D^1b\right).\end{aligned}$$

By our assumption on b, the contribution of the terms involving f^{q_0} is zero. After using (4.5) to rewrite the coefficients of $(D^1f)^{q_0}$, $\ell^q(D^{3q_0+1}f)^{q_0}$, and $(D^qf)^{q_0}$ completely in terms of derivatives of b and doing some simplification, it will suffice to show that the equations

$$\begin{aligned}
D^{qq_0+1}b + \ell^q D^{qq_0+q+1}b &= 0 \\
\ell^{q+1}D^{q+1}b + \ell^{2q_0}D^{qq_0+q_0}b + \ell^{q_0+1}D^{qq_0+1}b &= 0 \\
\ell^{q_0}D^{q_0+1}b + \ell D^{q+1}b + \ell^{q_0}D^{q+q_0}b &= 0
\end{aligned}$$

hold for $b = x, y, z, w_4$. This is easily verified by consulting Table 4.1. □

Proof of (A10). We show that the desired equation holds for all t. By using (4.12) to replace occurrences of $D^{qq_0+3q_0}f$ with $D^q f$, we find that

$$\begin{aligned}
\ell^q D^{qq_0+q}t = {}& f^{q_0}\ell^q D^{qq_0+q}b - (D^1 f)^{q_0}\ell^{q_0}D^{qq_0}(b^q) \\
&+ (D^{3q_0+1}f)^{q_0}\ell^{q+q_0}D^{qq_0}(b^q - b) \\
&- (D^q f)^{q_0}(\ell^q D^q(b^q - b) - \ell D^1 b) + (D^q f^q)^{q_0}\ell^q D^q(b^q) \\
\ell^{2q}D^{qq_0+2q}t = {}& f^{q_0}\ell^{2q}D^{qq_0+2q}b + (D^{3q_0+1}f)^{q_0}\ell^{2q+q_0}D^{qq_0+q}(b^q - b) \\
&+ (D^q f)^{q_0}(\ell^q D^q(b^q - b) - \ell^{2q}D^{2q}(b^q - b)).
\end{aligned}$$

By our assumption on b, the contribution of the terms involving f^{q_0} is zero. The terms involving $(D^1 f)^{q_0}$ and $(D^q f^q)^{q_0}$ also give no contribution.

By comparing the coefficients of $(D^{3q_0+1}f)^{q_0}$ and $(D^q f)^{q_0}$ and doing some minor simplification, it will suffice to show that the equations

$$\begin{aligned}
\ell^{q+1}D^{qq_0+q}(b^q - b) &= (\ell^q - \ell)D^{qq_0}(b^q - b) \\
\ell D^{2q}(b^q - b) + D^1 b &= D^q(b^q - b)
\end{aligned}$$

hold for $b = x, y, z, w_4$. Each of these is easily verified using (4.5) and Table 4.1. □

This completes the proof of Lemma 4.8, and hence of Theorem 4.1.

4.5 Weierstrass points

As a consequence of Theorem 4.1, we determine the Weierstrass points of $\mathcal{D}$. Recall that the $\mathcal{D}$-Weierstrass points are those $P \in X$ satisfying $j_i(P) \neq \epsilon_i(P)$ for some i. These points make up the support of a divisor $R_{\mathcal{D}}$ with

$$\deg R_{\mathcal{D}} = (2g-2)\sum \epsilon_i + (13+1)m.$$

Since the sequence $\nu_i(\mathcal{D})$ of Frobenius orders differs from $\epsilon_0, \ldots, \epsilon_{13}$, [SV, Cor 2.10] implies that every rational point of X is a $\mathcal{D}$-Weierstrass point. We claim that in fact $\operatorname{Supp} R_{\mathcal{D}} = X(\mathbb{F}_q)$.

Corollary 4.9. *The set of Weierstrass points of $\mathcal{D}$ consists of the $\mathbb{F}_q$-rational points of X.*

Proof. By Theorem 4.1, we have

$$\deg R_{\mathcal{D}} = (2g-2)\sum \epsilon_i + (13+1)m = (3qq_0 + 9q + 23q_0 + 12)N,$$

and so it will suffice to show that $v_P(R) = 3qq_0 + 9q + 23q_0 + 12$ for $P \in X(\mathbb{F}_q)$. This will follow from the inequality

$$v_P(R_{\mathcal{D}}) \geq \sum_{i=0}^{r} (j_i(P) - \epsilon_i). \tag{4.13}$$

Since the automorphism group acts doubly transitively on the $\mathbb{F}_q$-rational points of X, it will suffice to show this for the point P_0 with $x = y = z = 0$. By expanding out the functions in $\mathcal{B}$ as power series in x, or by simply using the equations in 2.2, we find that they vanish at P_0 to the orders

$$\begin{aligned}
j_0 &= 0, & j_7 &= 1 + 3q_0 + 2q,\\
j_1 &= 1, & j_8 &= 1 + 2q_0 + q + qq_0,\\
j_2 &= 1 + q_0, & j_9 &= 1 + 3q_0 + q + qq_0,\\
j_3 &= 1 + 2q_0, & j_{10} &= 1 + 3q_0 + 2q + qq_0,\\
j_4 &= 1 + 3q_0, & j_{11} &= 1 + 3q_0 + 2q + 2qq_0,\\
j_5 &= 1 + 2q_0 + q, & j_{12} &= 1 + 3q_0 + 2q + 3qq_0,\\
j_6 &= 1 + 3q_0 + q, & j_{13} &= 1 + 3q_0 + 2q + 3qq_0 + q^2.
\end{aligned}$$

Inserting these values into (4.13) completes the proof. □

The same argument shows that the $\mathcal{E}$-Weierstrass points are exactly the $\mathbb{F}_q$-rational points as well. In this case, $v_P(R_{\mathcal{E}}) = 3qq_0 + 4q + 12q_0 + 5$ for $P \in X(\mathbb{F}_q)$.

Table 4.2: The supports S_f for f of type 1.

i	x	w_1	w_2	w_3	w_6	w_8
0	$*$	$*$	$*$	$*$	$*$	$*$
1	$*$	$*$	$*$	$*$	$*$	$*$
$3q_0$		$*$	$*$	$*$	$*$	$*$
$3q_0 + 1$		$*$	$*$	$*$	$*$	$*$
q		$*$	$*$	$*$	$*$	$*$
$q + 1$			$*$	$*$	$*$	$*$
$q + 3q_0$		$*$	$*$	$*$	$*$	$*$
$q + 3q_0 + 1$			$*$	$*$	$*$	$*$
$2q$			$*$	$*$	$*$	$*$
$2q + 1$				$*$	$*$	$*$
$2q + 3q_0$			$*$	$*$	$*$	$*$
$2q + 3q_0 + 1$				$*$	$*$	$*$
$3q$				$*$	$*$	$*$
$3q + 3q_0$				$*$	$*$	$*$
$3qq_0$		$*$	$*$	$*$	$*$	$*$
$3qq_0 + 1$			$*$	$*$	$*$	$*$
$3qq_0 + 3q_0$					$*$	$*$
$3qq_0 + 3q_0 + 1$					$*$	$*$
$3qq_0 + q$		$*$	$*$	$*$	$*$	$*$
$3qq_0 + q + 1$			$*$	$*$	$*$	$*$
$3qq_0 + q + 3q_0$					$*$	$*$
$3qq_0 + q + 3q_0 + 1$					$*$	$*$
$3qq_0 + 2q$			$*$	$*$	$*$	$*$
$3qq_0 + 2q + 1$				$*$	$*$	$*$
$3qq_0 + 2q + 3q_0$					$*$	$*$
$3qq_0 + 2q + 3q_0 + 1$					$*$	$*$
$3qq_0 + 3q$				$*$	$*$	$*$
$3qq_0 + 3q + 3q_0$					$*$	$*$
$6qq_0$					$*$	$*$
$6qq_0 + 1$					$*$	$*$
$6qq_0 + q$					$*$	$*$
$6qq_0 + q + 1$					$*$	$*$
$6qq_0 + 2q$					$*$	$*$
$6qq_0 + 2q + 1$					$*$	$*$
$6qq_0 + 3q$					$*$	$*$
q^2		$*$	$*$	$*$	$*$	$*$

Table 4.3: The supports S_f for f of type 2.

i	y	z	w_4	w_7	w_5	w_9	w_{10}
0	*	*	*	*	*	*	*
1	*	*	*	*	*	*	*
q_0	*	*	*	*	*	*	*
$q_0 + 1$	*	*	*	*	*	*	*
$2q_0$		*	*	*	*	*	*
$2q_0 + 1$		*	*	*	*	*	*
$3q_0$					*	*	*
$3q_0 + 1$					*	*	*
q	*	*	*	*	*	*	*
$q + 1$			*	*	*	*	*
$q + q_0$	*	*	*	*	*	*	*
$q + q_0 + 1$			*	*	*	*	*
$q + 2q_0$		*	*	*	*	*	*
$q + 2q_0 + 1$			*	*	*	*	*
$q + 3q_0$					*	*	*
$q + 3q_0 + 1$					*	*	*
$2q$			*	*	*	*	*
$2q + 1$						*	*
$2q + q_0$			*	*	*	*	*
$2q + 2q_0$			*	*	*	*	*
$2q + 3q_0$					*	*	*
$2q + 3q_0 + 1$						*	*
$3q$						*	*
$3q + 3q_0$						*	*
qq_0	*	*	*	*	*	*	*
$qq_0 + 1$			*	*	*	*	*
$qq_0 + q_0$			*	*	*	*	*
$qq_0 + q_0 + 1$			*	*	*	*	*
$qq_0 + 2q_0$				*	*	*	*
$qq_0 + 2q_0 + 1$				*	*	*	*
$qq_0 + 3q_0$					*	*	*
$qq_0 + 3q_0 + 1$					*	*	*
$qq_0 + q$	*	*	*	*	*	*	*
$qq_0 + q + 1$			*	*	*	*	*
$qq_0 + q + q_0$			*	*	*	*	*
$qq_0 + q + q_0 + 1$			*	*	*	*	*
$qq_0 + q + 2q_0$				*	*	*	*
$qq_0 + q + 2q_0 + 1$				*	*	*	*
$qq_0 + q + 3q_0$					*	*	*
$qq_0 + q + 3q_0 + 1$					*	*	*
$qq_0 + 2q$			*	*	*	*	*
$qq_0 + 2q + 1$						*	*
$qq_0 + 2q + q_0$			*	*	*	*	*
$qq_0 + 2q + 2q_0$				*	*	*	*
$qq_0 + 2q + 3q_0$					*	*	*
$qq_0 + 2q + 3q_0 + 1$						*	*
$qq_0 + 3q$						*	*
$qq_0 + 3q + 3q_0$						*	*
$2qq_0$		*	*	*	*	*	*
$2qq_0 + 1$			*	*	*	*	*
$2qq_0 + q_0$				*	*	*	*
$2qq_0 + q_0 + 1$				*	*	*	*
$2qq_0 + 2q_0$					*	*	*
$2qq_0 + 2q_0 + 1$					*	*	*
$2qq_0 + 3q_0$							*
$2qq_0 + 3q_0 + 1$							*

5 de Rham cohomology of the Ree curve

For A a principally polarized abelian variety over an algebraically closed field k of characteristic $p > 0$, the p-torsion group scheme $A[p]$ can be understood in terms of the interaction between the Frobenius and Verschiebung morphisms, into which the multiplication-by-p map $[p] = V \circ F$ factors. In particular, the isomorphism type of $A[p]$ is characterized the structure of the mod p-reduction of the Dieudonné module of $A[p]$ as a $k[F, V]$-module. This information can also be captured in the Ekedahl-Oort type, which is a combinatorial invariant giving a stratification of the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties [Oor2] [EvdG].

For X a curve over k, there is an isomorphism of $k[F, V]$-modules between the p-torsion group scheme $\mathrm{Jac}(X)[p]$ and the de Rham cohomology $H^1_{\mathrm{dR}}(X)$ [Oda], which is a more concrete object. In [PW] and [MPW], de Rham cohomology is used to study the $k[F, V]$-module structure and Ekedahl-Oort types of the Hermitian and Suzuki curves. In this paper, we begin a similar analysis of the Ree curve, which is defined in characteristic $p = 3$.

There are two main difficulties in dealing with the Ree curves which are not present with the other two families of curves mentioned. The first is that, unlike for the other two families, no general explicit basis is known for the space of holomorphic differentials on the Ree curve. The second is sheer size, which makes it difficult to explore the problem computationally. The smallest Ree curve has genus 3627 and the second smallest has genus 826551. Because of this, we content ourselves at present with computing the structure of $H^1_{\mathrm{dR}}(X)$ for the smallest Ree curve. One might hope that familiarity with the structure of this first example may lead to insight into the general case.

The computations described in this chapter were implemented using the computer algebra system Magma [BCP]; all of our code is available upon request.

The results in this chapter have been submitted in a joint paper with Iwan Duursma.

5.1 Background

5.1.1 The Ree curve

Here recall definition and relevant properties of the Ree curve. For $s \geq 1$, the Ree curve R_s is the smooth projective curve over $\mathbb{F}_3$ defined by the affine equations

$$y^q - y = x^{q_0}(x^q - x) \qquad z^q - z = x^{q_0}(y^q - y), \tag{5.1}$$

where $q_0 = 3^s$ and $q = 3q_0^2 = 3^{2s+1}$. The automorphism group of R_s, which has order $(q^3+1)q^3(q-1)$ and acts doubly transitively on the $\mathbb{F}_q$-rational points of R_s, is exceptionally large in comparison to the genus $g_s = \frac{3}{2}q_0(q-1)(q+q_0+1)$. The curve R_s has no places of degrees 2, 3, 4, or 5 over $\mathbb{F}_q$, but over $\mathbb{F}_{q^6}$ it meets the Hasse-Weil upper bound.

By examining the L-polynomial

$$L_{R_s}(t) = (1 + 3q_0t + qt^2)^{q_0(q^2-1)}(1+qt^2)^{\frac{1}{2}q_0(q-1)(q+3q_0+1)},$$

it can be seen that the curve R_s is supersingular. Equivalently, the Jacobian $\mathrm{Jac}(R_s)$ is isogenous over the algebraic closure to a product of supersingular elliptic curves [Oor1, Theorem 4.2], and has no nontrivial 3-torsion points over $\overline{\mathbb{F}}_3$.

The embedding of R_s in $\mathbb{P}^{13}$ given in [ED] uses the 14 functions in

$$\mathcal{B} = \{1, x, y, z, w_1, \ldots, w_{10}\},$$

where the w_i are defined in 2.2. The functions in $\mathcal{B}$ are regular away from the pole P_∞ of x, where they have distinct pole orders. The function w_8 has divisor $\mathrm{div}(w_8) = m(P_0 - P_\infty)$ where $m = (q+1)(q+3q_0+1)$ is the exponent of the group of $\mathbb{F}_q$-rational points of $\mathrm{Jac}(R_s)$, and P_0 is the point $(x, y, z) = (0, 0, 0)$.

There are two particular subgroups of automorphisms of R_s which will prove useful in our computations. The first is the stabilizer of the two points P_0 and P_∞. This subgroup is isomorphic to $\mathbb{F}_q^\times = \langle \zeta \rangle$, and acts on the curve via

$$\phi_\zeta(x, y, z) = (\zeta x, \zeta^{q_0+1}y, \zeta^{2q_0+1}z).$$

This action breaks the function field $\mathbb{F}_q(x, y, z)$ into isotypic subspaces, that is, eigenspaces for the linear transformation induced by ϕ_ζ. Note that each of the functions in $\mathcal{B}$ is an eigenvector, so that $\mathbb{F}_q^\times$ acts diagonally on R_s embedded in $\mathbb{P}^{13}$.

The second automorphism of interest is an involution τ which interchanges the points P_0 and P_∞. It acts on the function field by

$$\tau(x, y, z) = (w_6/w_8, w_{10}/w_8, w_9/w_8).$$

The map τ also acts linearly on the image of R_s in $\mathbb{P}^{13}$. Up to sign, it acts on the functions in $\mathcal{B}$ by permuting them and then dividing by w_8 (see [ED, page 268]).

5.1.2 Dieudonné modules

Let $\mathbb{E}$ denote the non-commutative ring $k[F, V]$ generated by semi-linear operators F and V subject to the relations $FV = VF = 0$ and $F\lambda = \lambda^p F$ and $\lambda V = V\lambda^p$ for all $\lambda \in k$. This is the mod p reduction of the Dieudonné ring, which has coefficients a ring of Witt vectors instead of k. There is an equivalence of categories between p-torsion group schemes of principally polarized abelian varieties of dimension g and symmetric $\mathbb{E}$-modules of dimension $2g$ over k. We will refer to the $\mathbb{E}$-module corresponding to $\mathrm{Jac}(X)[p]$ as the *Dieudonné module* of X.

In the following, let $N = \mathrm{Jac}(X)[p]$. Then N is a symmetric BT_1 group scheme over k, as defined in [Oor2]. Let

$$0 = N_0 \subset N_1 \subset \cdots N_r = V(N) \subset \cdots \subset N_s = N,$$

be the smallest filtration of N stable under the action of V and F^{-1}, called the *canonical filtration*. This filtration may be obtained by iteratively refining by elements $F^{-i}V^j(N')$ where N' runs over terms in the existing filtration. In other words, it consists of $w(N)$ as w runs over all possible words in V and F^{-1}.

Let $B_i = N_{i+1}/N_i$ for $i = 0, \ldots, s-1$, which we call the *blocks* of the canonical filtration. Then for each i, exactly one of V and F^{-1} is zero on B_i and the other is an isomorphism of B_i onto another block, which we call $B_{\pi(i)}$. This defines a permutation π of $\{0, 1, \ldots, s-1\}$.

The canonical filtration may be refined to a *final filtration* of length $2g$

which is again stable under V and F^{-1}. The *final type* or *Ekedahl-Oort type* of N is the sequence $\nu = [\nu_1, \dots, \nu_g]$, where the ν_i are the dimensions of the image under V of the terms of dimensions $1 \leq i \leq g$ in a final filtration. The ν_i are nondecreasing and satisfy the condition $\nu_{i+1} \leq \nu_i + 1$, so the final type breaks into alternating intervals with slope 0 and 1, and is characterized by the *break points* ν_i where either $\nu_{i-1} = \nu_i \neq \nu_{i+1}$ or $\nu_{i-1} \neq \nu_i = \nu_{i+1}$. The final type characterizes N up to isomorphism.

5.1.3 de Rham cohomology

It was shown by Oda that there is an isomorphism of $\mathbb{E}$-modules between the Dieudonné module of $\mathrm{Jac}(X)[p]$ and the de Rham cohomology group $H^1_{\mathrm{dR}}(X)$. In the latter setting it is easier to do concrete calculations. In this section we recall the following description of $H^1_{\mathrm{dR}}(X)$ which may be found in [Oda, chapter 5]. We use the open cover $\mathcal{U} = \{U_0, U_\infty\}$ where $U_i = X \smallsetminus \{P_i\}$.

The space we are interested in studying is

$$H^1_{\mathrm{dR}}(X) \cong H^1_{\mathrm{dR}}(\mathcal{U}) = Z^1_{\mathrm{dR}}(\mathcal{U})/B^1_{\mathrm{dR}}(\mathcal{U}),$$

where the $Z^1_{\mathrm{dR}}(\mathcal{U})$ and $B^1_{\mathrm{dR}}(\mathcal{U})$ are as follows. The closed de Rham cocycles in $Z^1_{\mathrm{dR}}(\mathcal{U})$ consist of pairs the form $(f, (\omega_0, \omega_\infty))$ where $f \in \Gamma(U_0 \cap U_\infty, \mathcal{O})$ and $\omega_i \in \Gamma(U_i, \Omega^1)$ satisfy $df = \omega_0 - \omega_\infty$. The de Rham coboundaries in $B^1_{\mathrm{dR}}(\mathcal{U})$ are elements of the form $(f_0 - f_\infty, (df_0, df_\infty))$ with $f_i \in \Gamma(U_i, \mathcal{O})$.

There is a short exact sequence of $\mathbb{E}$-modules

$$0 \longrightarrow H^0(X, \Omega^1) \xrightarrow{\lambda} H^1_{\mathrm{dR}}(X) \xrightarrow{\gamma} H^1(X, \mathcal{O}_X) \longrightarrow 0,$$

where the map λ sends $\omega \mapsto (0, \omega) = (0, (\omega|_{U_0}, \omega|_{U_\infty}))$ and γ sends $(f, \omega) \mapsto f$. The Frobenius F and Verschiebung V on $H^1_{\mathrm{dR}}(X)$ by $F(f, \omega) = (f^p, 0)$ and $V(f, \omega) = (0, \mathcal{C}\omega)$, where $\mathcal{C}$ is the Cartier operator on the sheaf Ω^1 [Car]. The operator F is p-linear, while the operator V is $1/p$-linear. Moreover, $\ker F = H^0(X, \Omega^1) = \mathrm{im}\, V$.

The Cartier operator $\mathcal{C}$ is characterized by the properties that it annihilates exact differentials, preserves logarithmic differentials, and is $1/p$-linear. Locally, the operator $\mathcal{C}$ may be defined as follows. Let t be a separating variable for $k(X)$, so that any differential ω may be written in the form $\omega = (f_0^p + f_1^p t + \cdots + f_{p-1}^p t^{p-1})dt$. Then $\mathcal{C}(\omega) = f_{p-1} dt$. If ω is regular at P, then $\mathcal{C}(\omega)$ is also regular at P, so $\mathcal{C}$ preserves the space $H^0(X,\Omega^1)$.

In process of our computation, we make a choice of a section ψ of γ. To do this, for each f in a basis of $H^1(X,\mathcal{O}_X)$ we decompose df as $df = \omega_0 - \omega_\infty$ where $\omega_i \in \Gamma(U_i,\Omega^1)$, and set $\psi(f) = (f,(\omega_0,\omega_\infty))$. Note that in such a decomposition of df, the ω_i are defined only up to a holomorphic differential.

5.2 The Cartier operator on H^0

Since the curve R_s is supersingular, it has p-rank zero and the Frobenius $\mathcal{F}$ acts nilpotently on $H^1(R_s,\mathcal{O})$. Therefore, by the duality of $\mathcal{C}$ and $\mathcal{F}$, the Cartier operator is nilpotent on $H^0(R_s,\Omega^1)$. The goal of this section is to compute the invariant factors of $\mathcal{C}$ for $s = 1,2$. As a result, we determine dimension of the kernel of $\mathcal{C}$ on $H^0(R_s,\Omega^1)$ for $s = 1,2$. This is equal to the *a-number* of $\mathrm{Jac}(R_s)$, which is defined as the dimension of $\mathrm{Hom}_{\overline{\mathbb{F}}_p}(\alpha_p, \mathrm{Jac}(R_s)[p])$, where α_p is the kernel of Frobenius on the additive group $\mathbb{G}_a$ [LO, 5.2.8] [FGM+] [DF].

Each element of $H^0(R_s,\Omega^1)$ is a linear combination of differentials of the form $\omega = x^i y^j z^k dx$. In our calculations by hand, it will suffice to consider only the 27 differentials ω with $0 \le i,j,k \le 2$ since $\mathcal{C}$ is 1/3-linear. For convenience, we let T denote the operator $T(f) = \mathcal{C}(f dx)/dx$. From

$$y = x^{q_0}(x - x^q) + y^q = -w_1^{q_0} + x^{q_0}x$$
$$z = x^{2q_0}(x - x^q) + z^q = -(xw_1 + w_2)^{q_0} + x^{2q_0}x$$

we obtain the values $T(f)$ for the 9 monomials $f = x^i y^j z^k$ with $0 \le i \le 2$ and $0 \le j + k \le 1$.

(i,j,k)	$T(x^i y^j z^k)$
$(0,0,0)$	0
$(1,0,0)$	0
$(2,0,0)$	1
$(0,1,0)$	0
$(1,1,0)$	$x^{q_0/3}$
$(2,1,0)$	$-w_1^{q_0/3}$
$(0,0,1)$	0
$(1,0,1)$	$x^{2q_0/3}$
$(2,0,1)$	$-(xw_1 + w_2)^{q_0/3}$

Along with the following formula, these may be used to obtain the remaining 18 values of $T(x^iy^jz^k)$ with $0 \leq i,j,k \leq 2$.

Lemma 5.1. *For $0 \leq i \leq p-1$,*

$$T(x^ifg) = \sum_{i+j+k=p-1} T(x^{p-1-j}f)T(x^{p-1-k}g) \\ + \sum_{i+j+k=2p-1} xT(x^{p-1-j}f)T(x^{p-1-k}g).$$

Proof. This is a simple exercise. Write each of f and g in the form $\sum a_ix^i$ with $a_i \in k(X)^p$, expand, and use the $1/p$-linearity of $\mathcal{C}$. □

In particular, for $p = 3$ we have

$$\begin{aligned} T(fg) &= T(x^2f)T(g) + T(xf)T(xg) + T(f)T(x^2g) \\ T(xfg) &= T(xf)T(x^2g) + T(x^2f)T(xg) + xT(f)T(g) \\ T(x^2fg) &= T(x^2f)T(x^2g) + xT(xf)T(g) + xT(f)T(xg). \end{aligned}$$

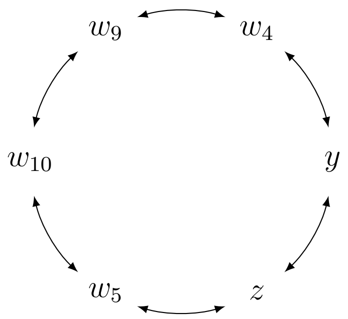
For a basis for $V = H^0(R_s, \Omega^1)$ we use a collection of g linearly independent differentials $\omega = fdx$, where the f are monomials in the 14 functions of $\mathcal{B}$ satisfying $-v_{P_\infty}(f) \leq 2g-2$. Since

$$\frac{2g-2}{\operatorname{ord}_{P_\infty}(w_8)} = 3q_0 - 2 < 3q_0 = \left\lfloor \frac{2g-2}{\operatorname{ord}_{P_\infty}(x)} \right\rfloor,$$

a naive search for linearly independent monomials of this form involves going through between 3^{3q_0-2} and 3^{3q_0} terms, which is prohibitively large for $s = 2$. In order to reduce the search space for a basis, we use the fact that the image of R_s in $\mathbb{P}^{13}$ lies on many quadrics. In particular, we have the equations

$$\begin{aligned} y^2 &= w_4 + xz & z^2 &= w_5 + yw_1 \\ w_4^2 &= xw_9 + yw_3 & w_5^2 &= zw_6 + w_1w_{10} \\ w_9^2 &= w_3w_{10} + w_4w_8 & w_{10}^2 &= w_5w_8 + w_6w_9 \\ w_2^2 &= w_8 + xw_6 + w_1w_3 & w_7^2 &= w_8 + xw_6 + yw_{10}. \end{aligned}$$

In each of these equations, the square of one of the 8 functions w_2, w_7, y, z, w_4, w_5, w_9, and w_{10} appears as one of the monomials with greatest pole order at P_∞. The first six equations form a cycle



If the square of one of these six variables appears in a monomial, then reducing by the equation involving its square yields two new terms, one for each neighboring variable, in which the neighbor appears with degree one greater than before, but the original variable appears with degree two less. Moreover, the last two equations allow w_2^2 and w_7^2 to be written in terms of other variables. This shows that the space of monomials in the functions of $\mathcal{B}$ is spanned by monomials in which each of the 8 functions above appear with degree at most 1. Using this, the size of the search space for $s = 2$ becomes at most

$$\sum_{i=0}^{8} \binom{27 - i + 6 - 1}{6 - 1} 2^i \approx 10^{7.4},$$

which is within a reasonable range.

Once a basis is found, we perform the linear algebra by evaluating the functions ω/dx and $\mathcal{C}(\omega)/dx$ at sufficiently many $\mathbb{F}_q$-rational points. In order to reduce the size of this computation, the space V may be broken into $q-1$ isotypic components V_n under the action of $\mathbb{F}_q^\times$. Let V_n denote the subspace of V satisfying $\phi_\zeta^*(\omega) = \zeta^n\omega$. Then since the Cartier operator commutes with automorphisms, it follows that $\mathcal{C}(V_{3n}) \subset V_n$. Indeed, for $\omega \in V_{3n}$ we have

$$\phi_\zeta^*\mathcal{C}(\omega) = \mathcal{C}(\phi_\zeta^*\omega) = \mathcal{C}(\zeta^{3n}\omega) = \zeta^n\mathcal{C}(\omega).$$

The components V_n may be described explicitly as follows. Given a multi-index $I = (i, j, k)$, let ω_I denote $x^i y^j z^k dx$, and write $|I| = 1 + i + (q_0 + 1)j + (2q_0 + 1)k$. Then $\phi_\zeta^*\omega_I = \zeta^{|I|}\omega_I$, and any $\omega = \sum_I a_I\omega_I$ in $H^0(R_s, \Omega^1)$ may be decomposed as

$$\omega = \sum_{n \bmod q-1} \sum_{|I| \equiv n \bmod q-1} a_I \omega_I = \sum_{n \bmod q-1} \omega_n.$$

Note that the terms in each of the defining equations $y^q - y = x^{q_0}(x^q - x)$ and $z^q - z = x^{q_0}(y^q - y)$ have equal weights modulo $q-1$ and moreover, that $|I| = 1 + v_{P_0}(\omega_I)$. It follows that the decomposition into ω_n is unique, and breaks ω into isotypic components.

The dimensions of the V_n may be determined by applying a theorem of Bouw, which she credits as a special case of a result of Kani [Kan2], which gives a formula for the dimensions of the isotypic subspaces W_n of $H^1(X, \mathcal{O}_X)$ under the action of a cyclic group of automorphism in terms of the ramification data of the induced cover [Bou, Theorem 4.3]. The dimensions of V_n follow from Serre duality since $\dim V_n = \dim W_{q-1-n}$.

Consider the cover $R_s \to R_s/\mathbb{F}_q^\times = Y$. The points P_0 and P_∞ are fixed by every element of $\mathbb{F}_q^\times$, and so they are ramified with index $q-1$. Since 1 and $2q_0 + 1$ are both coprime to $q-1$, the only other points fixed by some element of $\mathbb{F}_q^\times$ are the $q-1$ points of the form $P_\beta = (0, \beta, 0)$ with $\beta \neq 0$. Since $\gcd(q-1, 2q_0+1) = 2$, there are two orbits of these points each with ramification index 2. From the Hurwitz theorem we conclude that $g_Y = (3qq_0 + q + 3q_0 - 1)/2$. Inserting this information into the theorem of Bouw gives the following.

Lemma 5.2. *The spaces V_n have dimension*

$$\dim V_n = \begin{cases} g_Y & n \text{ even,} \\ g_Y + 1 & n \text{ odd.} \end{cases}$$

Our computations performed in Magma yield the following.

Proposition 5.3. *The invariant factor decomposition of $H^0(R_1, \Omega^1)$ under the action of $\mathcal{C}$ is*

$$\begin{aligned} H^0(R_1, \Omega^1)/\mathcal{C} \cong & (k[x]/x)^7 \oplus (k[x]/x^2)^{79} \oplus (k[x]/x^3)^{139} \\ & \oplus (k[x]/x^4)^{49} \oplus (k[x]/x^5)^{343} \oplus (k[x]/x^6)^{189}. \end{aligned}$$

In particular, the a-number of $\mathrm{Jac}(R_1)$ *is* $\frac{2}{9} g_1 = 801$.

Proposition 5.4. *The invariant factor decomposition of $H^0(R_2, \Omega^1)$ under the action of $\mathcal{C}$ is*

$$\begin{aligned} H^0(R_2,\Omega^1)/\mathcal{C} \cong &(k[x]/x)^{7463} \oplus (k[x]/x^2)^{350} \oplus (k[x]/x^3)^{25886} \oplus (k[x]/x^4)^{9147} \\ &\oplus (k[x]/x^5)^{24018} \oplus (k[x]/x^6)^{21952} \oplus (k[x]/x^7)^{5047} \\ &\oplus (k[x]/x^8)^{353229} \oplus (k[x]/x^9)^{9261} \oplus (k[x]/x^{10})^{5103}. \end{aligned}$$

In particular, the a-number of $\mathrm{Jac}(R_2)$ *is 143556.*

Remark. It is interesting that the last two factors $k[x]/x^{4s+1}$ and $k[x]/x^{4s+2}$ appear with multiplicities $27^{s-1} \cdot 7^3$ and $27^s \cdot 7$ for $s = 1, 2$.

5.3 Computation of F and V

In this section, we describe the setup for our computation of F and V on $H^1_{\mathrm{dR}}(R_1)$, which we completed using Magma. For a basis of $H^1(R_1, \mathcal{O})$ we use a set of functions $\{f_i\}$ whose pole orders at P_∞ realize all g Weierstrass gaps at P_∞. An explicit description of the Weierstrass semigroup is not known for the Ree curves in general, but for $s = 1$ it has been determined in [ED]. The gap functions f_i necessarily have poles away from P_∞, but it is sufficient to introduce a pole at a single other point P_0, since for $a, b \geq 2g$ Riemann-Roch implies that

$$H^1(R_1, \mathcal{O}) \cong L(aP_0 + bP_\infty)/(L(aP_0) + L(bP_\infty)).$$

This allows us to do all our computations inside a space L of the form $L = L(AP_0 + BP_\infty)$, provided that A and B are large enough that L contains f^3 and df/dx for all f in our basis. The reasons for these conditions are as follows:

- To choose a section ψ of $\gamma\colon H^1_{\mathrm{dR}}(R_1) \to H^1(R_1, \mathcal{O})$, we decompose each df_i/dx as $df_i/dx = g_{i,0} - g_{i,\infty}$ with $g_{i,j} \in \Gamma(U_j, \mathcal{O})$ to get $\psi(f_i) = (f_i, \mathbf{g}_i) = (f_i, (g_{i,0}dx, g_{i,\infty}dx))$.
- To compute F on $H^1(R_1, \mathcal{O})$, we decompose each f_i^3 as

$$f_i^3 = \sum_j a_{ij} f_j + h_{i,0} + h_{i,\infty}, \qquad h_{i,j} \in \Gamma(U_j, \mathcal{O}).$$

To compute $V|_{H^1(R_1,\mathcal{O})}$, we apply the Cartier operator to each $\mathbf{g}_i$ and express this in terms of our basis for $H^0(R_1,\Omega^1)$. Furthermore, the coefficients a_{ij} give us the entries of the matrix of F acting on $H^1(R_1,\mathcal{O})$. Since $(h_0,(dh_0,0))$ and $(h_\infty,(0,dh_\infty))$ are coboundaries, we obtain the $H^0(R_1,\Omega^1)$ component of $F(\psi(f_i))$ from

$$(f_i^3,\mathbf{0})-\sum_j a_{ij}\psi(f_j)=-\sum_j a_{ij}(0,\mathbf{g}_j)-(0,(dh_{i,0},0))-(0,(0,dh_{i,\infty})).$$

Our basis for L is composed of monomials in the functions $\mathcal{B}\cup\{w_8^{-1}\}$. The benefit of dealing with functions of this form is that they are eigenvectors for the action of ϕ_ζ and are easy to transform under τ. First we find monomials in $\mathcal{B}$ with pole orders at P_∞ covering each residue class modulo m. From these, we form a basis for $H^1(R_1,\mathcal{O})$ by dividing by appropriate powers of w_8 to get each nongap as a pole order at P_∞. These functions end up living in $L(aP_0+(2g-1)P_\infty)$ where $a=8198\approx 2.26g$, and the space L we use for the main computation is $L(3aP_0+(6g-3)P_\infty)$. To obtain a basis for L, we find monomials in $\mathcal{B}$ spanning $L((6g-3)P_\infty)$ and $L(3aP_\infty)$ and apply the involution τ to obtain a basis for $L(3aP_0)$.

The space L has dimension 42727, which is too large if we wish to deal with the functions in L as vectors evaluated at $\mathbb{F}_q$-rational points, of which there are only $q^3+1=19684$. Therefore, we break L into $q-1=26$ isotypical components L_n under the action of $\mathbb{F}_q^\times$, each of dimension about 1640, keeping in mind that $f\mapsto f^3$ sends L_n to L_{3n} and $f\mapsto df/dx$ sends L_n to L_{i-1}. Even after breaking L into isotypical components, however, the $\mathbb{F}_q$-rational points still do not impose enough independent conditions on the L_n, so in order to complete the step where we compute ψ and F on $H^1(R_1,\mathcal{O})$, we evaluate at carefully chosen $\mathbb{F}_{q^6}$-rational points, and perform the linear algebra over a field of order $q^6=3^{18}$.

5.4 Decomposition of the Dieudonné module

The computations in the previous section yield two $2g\times 2g$ matrices with coefficients in $\mathbb{F}_3$ which describe the action of the semilinear operators F and V on our basis of $N=H^1_{\mathrm{dR}}(R_1)$. Since these matrices have entries in $\mathbb{F}_3$, each term in the canonical filtration of N is defined over $\mathbb{F}_3$.

Upon computing the canonical filtration for N, we find that it has 75 terms including 0 and N. Let $B_i = N_{i+1}/N_i$, $i = 0, \dots, 73$, be the blocks in the canonical filtration. Recall from that for each i, either V is zero on B_i or V gives an isomorphism $B_i \to B_{\pi(i)}$. The Ekedahl-Oort type can be read off of the sizes of the B_i and the permutation π.

Proposition 5.5. *The Ekedahl-Oort type $\nu = [\nu_1, \dots, \nu_g]$ of the curve R_1 has the following break points:*

$$532, 721, 770, 1302, 1392, 1441, 1490, 2022, 2029, 2078, 2150, 2884, 2891, 3627.$$

In [Oor2, §9.1], there are explicit instructions that allow one to reconstruct a finite group scheme N, along with a non-degenerate alternating pairing on the Dieudonné module of N, given the Ekedahl-Oort type of N. We are interested, however, in decomposing the Dieudonné module into indecomposable factors, which can be obtained by examining the permutation π of the blocks B_i.

In our case, we find that the blocks B_i are broken into seven orbits under the permutation π induced by V and F^{-1}. We list the cycles of π in the table below. Each cycle is associated to a distinct isotypic component of the Dieudonné module. The dimension of any block in a given orbit is the orbit's *multiplicity*, which corresponds to the multiplicity of the corresponding factor in the Dieudonné module. If $\pi(i) < i$ then $V\colon B_i \to B_{\pi(i)}$ is an isomorphism, and if $\pi(i) > i$, then $F^{-1}\colon B_i \to B_{\pi(i)}$ is an isomorphism. Collecting these isomorphisms, one obtains a word in V and F^{-1} associated to each orbit, which is defined up to a cyclic permutation. For example, the cycle below containing 3 corresponds to the word $w = F^{-3}V^2F^{-3}V^4$.

Table 5.1: Cycles of π

cycle	mult.
(0, 37, 50, 62, 68, 71, 73, 36, 23, 11, 5, 2)	189
(1, 38, 51, 63, 69, 72, 35, 22, 10, 4)	343
(3, 39, 52, 64, 31, 18, 48, 60, 67, 33, 20, 8)	49
(6, 40, 53, 65, 70, 34, 21, 9, 42, 55, 25, 13)	49
(7, 41, 54, 66, 32, 19)	41
(12, 43, 56, 26, 14, 44, 57, 27, 49, 61, 30, 17, 47, 59, 29, 16, 46, 24)	7
(15, 45, 58, 28)	2

For a word w in F^{-1} and V, we denote by $\mathbb{E}(w)$ the Dieudonné module of the corresponding group scheme, as in [Oor2, §9.8]. The structure of $\mathbb{E}(w)$ can be written out simply in terms of generators and relations if desired. This is explained in [PW, §5.2] in terms of the orbits of π [1].

To see how this works, consider the following example. The orbit of the block B_3, which has corresponding word $w = F^{-3}V^2F^{-3}V^4$, is depicted in Figure 5.1. The module $\mathbb{E}(w)$ can be written as the quotient of the left $\mathbb{E}$-module generated by variables X_1 and X_2 corresponding to the "peak" blocks B_{64} and B_{67} of the orbit by the left ideal of relations corresponding to the "valley" blocks B_3 and B_{18} of the orbit. Specifically, we have

$$\mathbb{E}(w) = (\mathbb{E}X_1 + \mathbb{E}X_2)/\mathbb{E}(V^2X_1 + F^3X_2, V^4X_2 + F^3X_1),$$

and this module occurs in $H^1_{\mathrm{dR}}(X)$ with multiplicity $\dim B_3 = 49$.

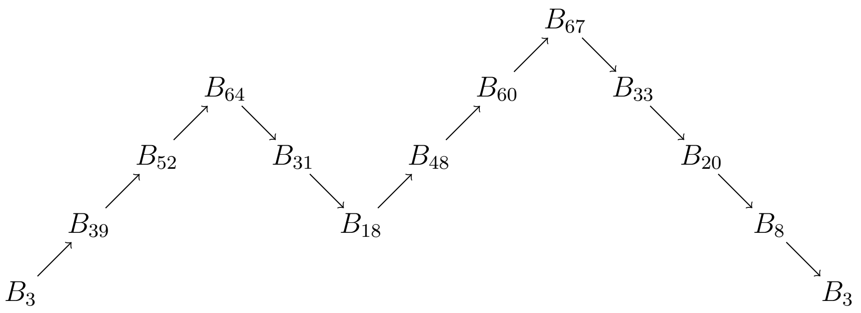


Figure 5.1: Orbit of block B_3, $w = F^{-3}V^2F^{-3}V^4$

In summary, we obtain the following decomposition of $H^1_{\mathrm{dR}}(R_1)$. Consider the words

$$\begin{aligned} w_1 &= F^{-3}V^2F^{-3}V^4 \\ w_1' &= F^{-4}V^3F^{-2}V^3 \\ w_2 &= F^{-2}V^2F^{-1}V^2F^{-2}V^2F^{-2}VF^{-2}V^2, \end{aligned}$$

which correspond to the cycles in Table 5.4 of containing blocks 3, 6, and 12.

[1] Although [PW, §5.2] deals with a specific class of curves, the approach works more generally.

Theorem 5.6. *As an $\mathbb{E}$-module, $H^1_{\mathrm{dR}}(R_1)$ decomposes as*

$$\begin{aligned} H^1_{\mathrm{dR}}(R_1) \cong& \left(\mathbb{E}/\mathbb{E}(F^2+V^2)\right)^2 \oplus (\mathbb{E}(w_2))^7 \\ &\oplus \left(\mathbb{E}/\mathbb{E}(F^3+V^3)\right)^{41} \oplus (\mathbb{E}(w_1) \oplus \mathbb{E}(w_1'))^{49} \\ &\oplus \left(\mathbb{E}/\mathbb{E}(F^5+V^5)\right)^{343} \oplus \left(\mathbb{E}/\mathbb{E}(F^6+V^6)\right)^{189}. \end{aligned}$$

References

[AT] M. Abdón and F. Torres. On $\mathbf{F}_{q^2}$-maximal curves of genus $\frac{1}{6}(q-3)q$. *Beiträge Algebra Geom.*, 46(1):241–260, 2005.

[AP] Y. Aubry and M. Perret. Divisibility of zeta functions of curves in a covering. *Arch. Math. (Basel)*, 82(3):205–213, 2004.

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

[Bou] I. I. Bouw. The p-rank of ramified covers of curves. *Compositio Math.*, 126(3):295–322, 2001.

[Car] P. Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244:426–428, 1957.

[DL] P. Deligne and G. Lusztig. Representations of reductive groups over finite fields. *Ann. of Math. (2)*, 103(1):103–161, 1976.

[DF] N. Dummigan and S. Farwa. Exact holomorphic differentials on a quotient of the Ree curve. *J. Algebra*, 400:249–272, 2014.

[ED] A. Eid and I. Duursma. Smooth embeddings for the Suzuki and Ree curves. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 251–291. Amer. Math. Soc., Providence, RI, 2015.

[EvdG] T. Ekedahl and G. van der Geer. Cycle classes of the E-O stratification on the moduli of abelian varieties. In *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I*, volume 269 of *Progr. Math.*, pages 567–636. Birkhäuser Boston, Inc., Boston, MA, 2009.

[FG1] S. Fanali and M. Giulietti. On maximal curves with Frobenius dimension 3. *Des. Codes Cryptogr.*, 53(3):165–174, 2009.

[FG2] S. Fanali and M. Giulietti. On some open problems on maximal curves. *Des. Codes Cryptogr.*, 56(2-3):131–139, 2010.

[FG3] S. Fanali and M. Giulietti. Quotient curves of the GK curve. *Adv. Geom.*, 12(2):239–268, 2012.

[FGM$^+$] H. Friedlander, D. Garton, B. Malmskog, R. Pries, and C. Weir. The a-numbers of Jacobians of Suzuki curves. *Proc. Amer. Math. Soc.*, 141(9):3019–3028, 2013.

[FGT] R. Fuhrmann, A. Garcia, and F. Torres. On maximal curves. *J. Number Theory*, 67(1):29–51, 1997.

[FT] R. Fuhrmann and F. Torres. On Weierstrass points and optimal curves. *Rend. Circ. Mat. Palermo (2) Suppl.*, (51):25–46, 1998.

[Gar] A. Garcia. On curves with many rational points over finite fields. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 152–163. Springer, Berlin, 2002.

[GS] A. Garcia and H. Stichtenoth. A maximal curve which is not a Galois subcover of the Hermitian curve. *Bull. Braz. Math. Soc. (N.S.)*, 37(1):139–152, 2006.

[GSX] A. Garcia, H. Stichtenoth, and C.-P. Xing. On subfields of the Hermitian function field. *Compositio Math.*, 120(2):137–170, 2000.

[GT] A. Garcia and S. Tafazolian. On additive polynomials and certain maximal curves. *J. Pure Appl. Algebra*, 212(11):2513–2521, 2008.

[GK1] M. Giulietti and G. Korchmáros. Algebraic curves with a large non-tame automorphism group fixing no point. *Trans. Amer. Math. Soc.*, 362(11):5983–6001, 2010.

[GK2] M. Giulietti and G. Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.*, 343(1):229–245, 2009.

[Han] J. P. Hansen. Deligne-Lusztig varieties and group codes. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 63–81. Springer, Berlin, 1992.

[HP] J. P. Hansen and J. P. Pedersen. Automorphism groups of Ree type, Deligne-Lusztig curves and function fields. *J. Reine Angew. Math.*, 440:99–109, 1993.

[HS] J. P. Hansen and H. Stichtenoth. Group codes on certain algebraic curves with many rational points. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):67–77, 1990.

[Hen] H.-W. Henn. Funktionenkörper mit grosser Automorphismengruppe. *J. Reine Angew. Math.*, 302:96–115, 1978.

[HKT] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[HB] B. Huppert and N. Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1982.

[Iha] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[Kan1] D. M. Kane. Canonical projective embeddings of the Deligne-Lusztig curves associated to ${}^2A_2$, ${}^2B_2$, and ${}^2G_2$. *Int. Math. Res. Not. IMRN*, (4):1158–1189, 2016.

[Kan2] E. Kani. The Galois-module structure of the space of holomorphic differentials of a curve. *J. Reine Angew. Math.*, 367:187–206, 1986.

[Kle] S. L. Kleiman. Algebraic cycles and the Weil conjectures. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 359–386. North-Holland, Amsterdam, 1968.

[KT] G. Korchmáros and F. Torres. Embedding of a maximal curve in a Hermitian variety. *Compositio Math.*, 128(1):95–113, 2001.

[Lac] G. Lachaud. Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(16):729–732, 1987.

[Lau] K. Lauter. Deligne-Lusztig curves as ray class fields. *Manuscripta Math.*, 98(1):87–96, 1999.

[LO] K.-Z. Li and F. Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[MPW] B. Malmskog, R. Pries, and C. Weir. The de Rham cohomology of the Suzuki curves. Oct 2017. arXiv:1719.08544v1.

[MZ] M. Montanucci and G. Zini. Some Ree and Suzuki curves are not Galois covered by the Hermitian curve. *Finite Fields Appl.*, 48:175–195, 2017.

[Mum] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[Oda] T. Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)*, 2:63–135, 1969.

[Oor1] F. Oort. Subvarieties of moduli spaces. *Invent. Math.*, 24:95–119, 1974.

[Oor2] F. Oort. A stratification of a moduli space of abelian varieties. In *Moduli of abelian varieties (Texel Island, 1999)*, volume 195 of *Progr. Math.*, pages 345–416. Birkhäuser, Basel, 2001.

[Ped] J. P. Pedersen. A function field related to the Ree group. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 122–131. Springer, Berlin, 1992.

[PW] R. Pries and C. Weir. The Ekedahl-Oort type of Jacobians of Hermitian curves. *Asian J. Math.*, 19(5):845–869, 2015.

[RS] H.-G. Rück and H. Stichtenoth. A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.*, 457:185–188, 1994.

[Sch] F. K. Schmidt. Zur arithmetischen Theorie der algebraischen Funktionen. II. Allgemeine Theorie der Weierstraßpunkte. *Math. Z.*, 45(1):75–96, 1939.

[Ser] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ska1] D. Skabelund. On the order sequence of an embedding of the Ree curve. 2017. Pre-print, arXiv:1705.04268.

[Ska2] D. C. Skabelund. New maximal curves as ray class fields over Deligne-Lusztig curves. *Proc. Amer. Math. Soc.*, 146(2):525–540, 2018.

[Sti1] H. Stichtenoth. über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. *Arch. Math. (Basel)*, 24:527–544, 1973.

[Sti2] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer Publishing Company, Incorporated, 2nd edition, 2008.

[SV] K.-O. Stöhr and J. F. Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1):1–19, 1986.

[TVN] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.