Maximal Artin-Schreier Curves for Coding Theory

A Thesis Presented

by

Grace Brill

to

The Faculty of the College of Engineering and Mathematical Sciences

of

The University of Vermont

In Partial Fulfillment of the Requirements
for the Degree of Bachelor of Science
Specializing in Mathematics

December 13, 2019

Defense Date: December 4, 2019
Thesis Examination Committee:

Christelle Vincent, Ph.D., Advisor
Francois Dorais, Ph.D.
David Darais, Ph.D., Chairperson
Linda Schadler, Ph.D., Dean of College of Engineering and Mathematical Science

Abstract

In the following thesis we explore Artin-Schreier curves and their applications to coding theory and cryptography. We develop an algorithm to compute maximal curves over finite fields working off of *Zeta functions of a class of Artin-Schreier curves with many automorphisms* [1]. We present a list of maximal Artin-Schreier curves useful for coding theory to be further investigated and analyzed.

Acknowledgements

I would like to thank the Mathematics and Computer Science Departments at the University of Vermont for providing me with challenging opportunities to further my education for the past four years. UVM has been a fantastic place to grow as a student and I am grateful for the support I have received from the community. I would also like to thank my thesis committee, Professor Francois Dorais of the Mathematics and Statistics Department, Professor David Darais of the Computer Science Department, and finally my thesis advisor Professor Christelle Vincent, for their time and support. Professor Vincent has provided me with immense encouragement and guidance throughout the process of this thesis as well as the last year of my college career. She has become an amazing mentor to me and I am honored to have had the opportunity to work alongside her. I hope that by working with her I have retained some of her perseverance, patience, and most importantly, sense of humor.

Table of Contents

Chapter 1

Algebraic Curve Background

1.1 Affine and Projective Plane Curves

While we will work with projective curves in this thesis, we will describe them via their associated affine curve. We present this theory here.

Definition 1.1.1. *Let $\mathbb{F}$ be a field. We define the 2-dimensional projective space over $\mathbb{F}$, $\mathbb{P}^2(\mathbb{F})$, to be*

$$\mathbb{P}^2(\mathbb{F}) = \{(X, Y, Z) : X, Y, Z \in \mathbb{F}, (X, Y, Z) \neq (0, 0, 0)\}/\sim$$

where $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ if there exists a $\lambda \neq 0, \lambda \in \mathbb{F}$ with

$$X_2 = \lambda X_1,$$
$$Y_2 = \lambda Y_1,$$
$$Z_2 = \lambda Z_1.$$

Definition 1.1.2. *Let $\mathbb{F}$ be a field, then $\mathbb{A}^2(\mathbb{F}) = \mathbb{F}^2$. We call $\mathbb{A}^2(\mathbb{F})$ the 2-dimensional affine space.*

We can think of $\mathbb{A}^2(\mathbb{F})$ as a subset of $\mathbb{P}^2(\mathbb{F})$ in the following manner: In $\mathbb{P}^2(\mathbb{F})$ consider $(X, Y, Z) \in \mathbb{P}^2(\mathbb{F})$ such that $Z \neq 0$. Then, $(X, Y, Z) \sim (\frac{X}{Z}, \frac{Y}{Z}, 1)$. Letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we get that $(X, Y, Z) \in \mathbb{P}^2(\mathbb{F})$ with $Z \neq 0$ corresponds to a unique point $(x, y) \in \mathbb{A}^2(\mathbb{F})$. We see that

$$\mathbb{P}^2(\mathbb{F}) = \mathbb{A}^2(\mathbb{F}) \cup \{(X, Y, Z) \in \mathbb{P}^2(\mathbb{F}) : Z = 0\}.$$

We call the set of points

$$\{(X, Y, Z) \in \mathbb{P}^2(\mathbb{F}) : Z = 0\}$$

the set of points at infinity.

Definition 1.1.3. *Let $\mathbb{F}$ be a field. Two polynomials $f(x, y), g(x, y) \in \mathbb{F}[x, y]$ are said to be equivalent if there exists a nonzero $\lambda \in \mathbb{F}$ such that $f(x, y) = \lambda g(x, y)$. This forms an equivalence relation on the set of polynomials in $\mathbb{F}[x, y]$. An affine plane curve is an equivalence class of such non-constant polynomials, via*

$$X = \{(x, y) \in \mathbb{A}^2(\mathbb{F}) : f(x, y) = 0\},$$

for any $f(x, y)$ in the equivalence class.

Definition 1.1.4. *Let $\mathbb{F}$ be a field. We associate to any polynomial f of degree d in*

$\mathbb{F}[x, y]$ *the homogenous polynomial* $f^* \in \mathbb{F}[X, Y, Z]$, *given by*

$$f^*(X, Y, Z) = Z^d f(X/Z, Y/Z).$$

We note that in this case, f^* *is homogenous of degree* d.

This homogeneous polynomial allows us to then define a projective plane curve:

Definition 1.1.5. *Let* $f \in \mathbb{F}[x, y]$ *define an affine plane curve. Then the projective plane curve associated to this curve is given by the homogeneous equation* $f^*(X, Y, Z) = 0$ *in* $\mathbb{P}^2(\mathbb{F})$. *In other words, a projective plane curve* C *is given by*

$$X = \{(X, Y, Z) \in \mathbb{P}^2(\mathbb{F}) : f^*(X, Y, Z) = 0\}.$$

We thus see that the points of the affine plane curve $f(x, y)$ are all of the points of the projective plane curve $f^*(X, Y, Z)$ that are not at infinity and are in $\mathbb{A}^2(\mathbb{F})$.

Definition 1.1.6. *Let* X *be an affine plane curve given by the polynomial* $f(x, y) = 0$. *A point* $P = (x, y)$ *on* X *is simple if*

$$\frac{\partial f}{\partial x}(P) \neq 0$$

or

$$\frac{\partial f}{\partial y}(P) \neq 0.$$

A smooth curve is a curve made up of only simple points.

1.2 Properties of Curves

For the sake of this thesis, we will be working with only smooth curves and will not be defining the genus of a curve but will use the following equations.

For the Artin-Schreier curves of the form $y^p - y = f(x)$ considered in this thesis, the genus can be computed as follows:

Lemma 1.2.1 (from section 2 of [2]). *Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}(x)$. Let $y^p - y = f(x)$ define an Artin-Schreier curve in standard form. Suppose $f(x)$ has $r+1$ poles at the points $P_1, \ldots, P_{r+1}$. The genus of the curve $Y : y^p - y - f(x)$ can be expressed as follows:*

$$g_Y = ((\sum_{j=1}^{r+1} d_j + 1) - 2) \cdot \frac{p-1}{2},$$

where d_j is the order of the pole P_j.

In particular if $f \in \mathbb{F}[x]$ the only pole is at infinity and it is of order $d = \deg f$, and the genus is

$$g_Y = (d-1)\frac{p-1}{2}.$$

Definition 1.2.2. *Let $\mathbb{F}$ be a field, and V and W be two projective plane curves defined over $\mathbb{F}$. A map $\varphi : V \to W$ is called a morphism of curves if there are polynomials $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{F}[x_1, x_2, x_3]$ such that*

$$\varphi((a_1, a_2, a_3)) = (\varphi_1(a_1, a_2, a_3), \varphi_2(a_1, a_2, a_3), \varphi_3(a_1, a_2, a_3))$$

for all $(a_1, a_2, a_3) \in V$. The map $\varphi : V \to W$ is an isomorphism of projective plane curves if there is a morphism $\psi : W \to V$ with $\varphi \circ \psi = 1_W$ and $\psi \circ \varphi = 1_V$. A map

φ is called an automorphism if it is an isomorphism of V to itself.

Definition 1.2.3. *Let X be a projective plane curve, then a divisor on X is a finite formal sum of points of X. The divisors form a group under addition denoted* $\mathrm{Div}(X)$

Definition 1.2.4. *Let x be a function on X. Its divisor is*

$$(x) = \sum_{\substack{P \text{ is a} \\ \text{zero of } x}} n_P P - \sum_{\substack{Q \text{ is a} \\ \text{pole of } x}} n_Q Q$$

where n_p is the order of the zero of x at P and n_Q is the order of the pole of x at Q.

Definition 1.2.5. *Let $D_1 = \sum n_i P_i, D_2 = \sum m_i P_i$ be divisors on X. We say $D_1 \leq D_2$ if for all i,*

$$n_i \leq m_i.$$

Definition 1.2.6. *Let X be a curve, for a divisor $A \in \mathrm{Div}(X)$ we define the Riemann-Roch space associated to A by*

$$L(A) := \{x \text{ a function on } X : (x) \geq -A\} \cup \{0\}$$

and its dimension

$$l(A) = \dim L(A).$$

Definition 1.2.7. *Let X be a projective plane curve defined over a finite field $\mathbb{F}_q$, and given by a polynomial $f^* \in \mathbb{F}[X, Y, Z]$. We define its set of rational points to be:*

$$X(\mathbb{F}_q) = \{(X, Y, Z) \in \mathbb{P}^2(\mathbb{F}_q) : f^*(X, Y, Z) = 0\}.$$

Theorem 1.2.8. *Let X be a smooth projective plane curve of genus g defined over a*

finite field $\mathbb{F}_q$. Then we have that

$$|\#X(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

Definition 1.2.9. *We say that X is maximal over $\mathbb{F}_q$ if*

$$\#X(\mathbb{F}_q) - q - 1 = 2g\sqrt{q}.$$

Note that this is only possible if q is a square since $\#X(\mathbb{F}_q) - q - 1$ is an integer.

1.3 Properties of Polynomials

We now introduce some properties of polynomials that will be useful later on.

Definition 1.3.1. *A polynomial P over $\mathbb{F}$ is called separable if it has no multiple roots (i.e. all of its roots are distinct). P is called additive if for any $x, y \in \overline{\mathbb{F}}$, $P(x+y) = P(x) + P(y)$.*

Proposition 1.3.2. *Let P be a separable additive polynomial of degree p^d, defined over a finite field $\mathbb{F}_{p^n}$. Then its roots form a vector space of dimension d over $\mathbb{F}_p$.*

Proof. If the polynomial is additive, then $P(x) = \sum_{i=0}^{d} a_i x^{p^i}$ for some d because $(a+b)^p = a^p + b^p$ in $\mathbb{F}_{p^n}$. Now let $\alpha, \beta \in \mathbb{F}_q$ to be two roots, where $\mathbb{F}_q$ is a field extension of $\mathbb{F}_{p^n}$. Then $P(\alpha+\beta) = P(\alpha) + P(\beta)$ by additivity, and $0+0=0$ so $\alpha+\beta$ is also a root of P. Finally, let $a \in \mathbb{F}_p$ then $P(a\alpha) = \sum_{i=0}^{d} a_i (ax)^{p^i} = a \sum_{i=0}^{d} a_i \alpha^{p^i} = aP(\alpha) = 0$ since $a^p = a$. □

Chapter 2

Code-Based Cryptography

2.1 Coding Theory

Coding theory was developed to help communication over noisy channels. Noisy channels can interfere with sent messages and create errors, meaning that the received message differs from the sent message. Coding theory introduces redundancy in a message by mapping it to a codeword in such a way that when a coded message acquires errors during transmission, the recipient can correct errors, and return the original codeword to be decoded into the original message. All information provided in this section and the next is adapted from Trappe and Washington's *Introduction to Cryptography with Coding Theory* [3].

We begin with some basic definitions:

Definition 2.1.1. *Let $\mathbb{F}$ be a field. A code C is a nonempty subset of $\mathbb{F}^n$ containing allowable strings called codewords. In other words, codewords are strings of length n whose entries are in $\mathbb{F}$. A linear code C is a nonempty set of $\mathbb{F}^n$ that forms a*

k-dimensional vector subspace of $\mathbb{F}^n$. Equivalently, C is closed under addition and scalar multiplication. Thus, if $c_1, c_2 \in C$ then $c_1 + c_2 \in C$ and for every scalar $\alpha \in \mathbb{F}$, and codeword $c \in C$, then $\alpha c \in C$.

Definition 2.1.2. *A linear code is called a $[n, k]$-code if n is the dimension of the surrounding space and k is the dimension of the space of allowable messages. In this case we call n the length of the code and k its dimension.*

Consider the following example of a $[3, 2]$ repetition code:

Example 2.1.3.

$$C = \{000, 111\} \subseteq \mathbb{F}_2^3$$

where the two codewords correspond to the messages $m = 0, m = 1$ respectively.

Two key characteristics of a code are its Hamming weight and Hamming distance. These quantities are what allow us to measure how well two codewords can be differentiated as well as recovered when there is interference in a noisy channel.

Definition 2.1.4. *Let C be a code over $\mathbb{F}$ and c be a codeword in C. We define the Hamming weight of c to be the number of nonzero digits or entries in c, written as $wt(c)$.*

Definition 2.1.5. *We define the Hamming distance between 2 codewords c_0, c_1 to be the number of entries where c_0 and c_1 differ, written as $d(c_0, c_1)$.*

Proposition 2.1.6. *The Hamming distance is a metric. That is to say that, for all $c_1, c_2, c_3 \in C$ we have*

1. *$d(c_1, c_2) \geq 0$ and*
   $d(c_1, c_2) = 0$ if and only if $c_1 = c_2$,

2. $d(c_1, c_2) = d(c_2, c_1)$, *and*

3. $d(c_1, c_2) \leq d(c_1, c_3) + d(c_3, c_2)$.

Example 2.1.7. We receive a message 001 which we know was encrypted using a repetition code with allowable codewords $\{000, 111\}$. Using the nearest neighbor decoding method, we deduce the sent codeword was 000 since it has the smallest Hamming distance from the received codeword.

The Hamming distance allows us to define an important invariant of a code:

Definition 2.1.8. *Let C be a code with codewords c_n. The minimum distance of C is:*

$$d(C) = min\{d(c_i, c_j) : c_i, c_j \in C \,\text{and}\, c_i \neq c_j\}.$$

Definition 2.1.9. *A linear code is called a $[n, k, d]$-code if n is its length, k is its dimension, and d is the minimum distance of the code.*

By analyzing the repetition code, we can see that there is a limit to the number of errors allowed before our decryption method becomes inaccurate.

Definition 2.1.10 (From chapter 18 of [3])**.** *We say that a code can detect up to s errors if changing a codeword in at most s places cannot change it to another codeword. The code can correct up to t errors if, whenever changes are made at t or fewer places in a codeword c, then the closest codeword is still c.*

We now can see the significance of the minimum distance of a code:

Theorem 2.1.11. *Let C be a code:*

1. *C can detect up to s errors if $d(C) \geq s + 1$.*

2. *C can correct up to t errors if $d(C) \geq 2t + 1$.*

2.2 McEliece Cryptosystem

The McEliece cryptosystem uses coding theory to encrypt and decrypt messages. Its security relies on the hardness of decoding, which for a general linear code is known to be NP-hard. Typically, McEliece's algorithm is used alongside algebraic geometry (AG) codes for their simple decoding algorithm [4]. Before receiving a message, the recipient must generate a private and public key, using the following algorithm:

Algorithm 1 Generating a key

INPUT: a $[n, k]$-linear code C capable of correcting t errors with an efficient decoding algorithm given by a $k \times n$ generator matrix G for the code C
OUTPUT: a public key (G', t) and a private key (S, G, P)
1: select a random $k \times k$ binary non-singular matrix S
2: select a random $n \times n$ permutation matrix P
3: compute the matrix $G' = SGP$

Then anyone who has access to the public key can encrypt a message using the following algorithm:

Algorithm 2 Encryption

INPUT: a message m and a public key (G', t)
OUTPUT: a ciphertext c
1: generate a random error vector e with $wt(e) \leq t$
2: calculate the ciphertext $c = mG' + e$

After receiving the message, the recipient decrypts it with this algorithm:

Algorithm 3 Decryption

INPUT: a ciphertext c and the private key (S, G, P)
OUTPUT: a decoded message m
1: calculate $y = cP^{-1}$
2: utilize the specific decoding algorithm for C to retrieve m'
3: compute the message $m = m'S^{-1}$

The following proof shows that the decoding algorithm recovers the original message:

Proof. Let m be a message, then by the encryption algorithm, our codeword c is

$$c = mG' + e,$$

where $G' = SGP$ and e is our error vector. Thus we substitute to get

$$c = mSGP + e.$$

Following the decoding algorithm,

$$y = cP^{-1} = mSG + eP^{-1}$$

where the weight of eP^{-1} is less than or equal to t, the number of correctable errors, since P is a permutation matrix, so $wt(e) = wt(eP^{-1})$. Then we decode y with the given decoding algorithm to find $m' = mS$. Finally by multiplying by S^{-1} we retrieve the original message m. □

2.3 Algebraic Geometry Codes

We now describe a method to generate codes with an efficient decoding algorithm. We define an algebraic geometry code associated to a curve X:

Definition 2.3.1 ([5]). *Let X be a curve defined over a finite field $\mathbb{F}_q$ and $P_1, \ldots, P_n, P_\infty$ be points defined over $\mathbb{F}_q$. Then we define a code*

$$C(P_1, \ldots, P_n, P_\infty) = \{(x(P_1), ..., x(P_n)) : x \in L(mP_\infty)\} \subseteq \mathbb{F}_q^n$$

where the vector space $L(mP_\infty) := \{f \in \mathbb{F}_q(X) : \deg f \leq m - 1\}$

Theorem 2.3.2 (adapted from [5]). *The code $C(P_1, \ldots, P_n, P_\infty)$ is an $[n, k, d]$-code with $k = l(mP_\infty) - l(mP_\infty - P_1 - P_2 - \ldots - P_\infty)$ and $d \geq n - m$.*

From this theorem we see that it is desirable to choose X to have many $\mathbb{F}_q$-rational points. Indeed, this will give a larger value of n, which will give a larger value of d, which will allow the code to correct more errors. As errors are what make the encryption more secure, the ability to correct more errors is valuable.

Describing the decoding algorithm for AG codes would take us too far afield for this thesis. There is an efficient decoding algorithm for the dual of this code, given by Duursma [6], building on work of Feng and Rao [7] which itself was built on work of Skorobogatov and Vladut [8]. We note that the connection between a code and its dual is such that computing a parity check matrix for the AG code presented above, gives a generating matrix for the dual code which can easily be decoded. Therefore, the dual is what is most often used, but the theory behind the original code is what allows the dual code to be created.

Chapter 3

Generating Maximal Artin-Schreier Curves

Maximal curves are valuable in code-based cryptography because they, by definition, have the largest possible number of rational points for their genus, which allows us to create codes with a large length n relative to the dimension k. To construct maximal curves, we will restrict our attention to a family of curves called Artin-Schreier curves. Artin-Schreier curves have more structure than a typical curve, which will make it much easier to determine when the curve is maximal.

3.1 A family of Artin-Schreier Curves

We begin by defining a family of curves we will consider.

Definition 3.1.1. *An Artin-Schreier curve is a curve which admits a model of the form* $y^p - y = f(x)$.

Even more specifically, we will be focusing on the family

$$y^p - y = xR(x)$$

where $R(x)$ is an additive polynomial of degree p^h for $h \geq 0$ and p is odd, with coefficients in the field $\mathbb{F}_{p^r}$, or in other words R is of the form

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i}.$$

We can then compute the genus of C_R to be $\frac{p^h(p-1)}{2}$.

Lemma 3.1.2. *The curve C_R has a unique point at infinity.*

Proof. Consider first the case of $h = 0$. Then C_R is of the form $y^p - y = ax^2$ and $p > 2$ since $p \geq 3$. Thus the projective model for the curve is

$$Y^p - Z^{p-1}Y = aX^2Z^{p-2}.$$

If $Z = 0$ then $Y^p = 0$, so $Y = 0$. Since $Y = Z = 0$, $X \neq 0$. Therefore the unique point at ∞ on C_R is $(1, 0, 0)$.
Otherwise if $h > 0$, then C_R is of the form $y^p - y = xR(x)$ and $\deg xR(x) \geq p+1 > p$. So the projective model for the curve is

$$Y^p Z^{p^h-1+1} - YZ^{p^h} = a_h X^{p^h+1} + Zf(X, Z), a_h \neq 0$$

where $f(X, Z)$ is a polynomial in X, Z. Then if $Z = 0$, $0 = a_h X^{p^h+1}$ so $X = 0$. Since $X = Z = 0$, $Y \neq 0$. Therefore the unique point at ∞ on C_R is $(0, 1, 0)$. □

3.2 Automorphisms of C_R

The reason we understand curves in this family is because of their unusually large automorphism group, which we can describe explicitly.

Theorem 3.2.1 (From section 4 of [1]). *Let R be monic and assume that $R(x) \notin \{x, x^p\}$. Then $\mathrm{Aut}(C_R) = \mathrm{Aut}^0(C_R)$, where $\mathrm{Aut}^0(C_R)$ is the subgroup of automorphisms of C_R that fix the unique point at infinity.*

To describe these automorphisms explicitly we will need to define some auxiliary polynomials, the first of which is:

$$E(x) = (R(x))^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \in \mathbb{F}_{p^r}[x].$$

This polynomial will in turn allow us to define a space W which will be crucial to our work.

Definition 3.2.2 (Adapted from [9]). *Given a polynomial in one variable, in this case $E(x)$, with coefficients in $\mathbb{F}_{p^r}$, there is an extension field $\mathbb{F}_q$ of $\mathbb{F}_{p^r}$ such that $E(x) \in \mathbb{F}_q[x]$ splits into a product of linear factors, and $\mathbb{F}_q$ is the smallest extension field of $\mathbb{F}_{p^r}$ with this property. Then, we say that $\mathbb{F}_q$ is the splitting field of the polynomial E over $\mathbb{F}_{p^r}$.*

Then we define $W \subseteq \mathbb{F}_q$ to be the set of roots of $E(x)$.

Lemma 3.2.3. *W is an $\mathbb{F}_p$-vector space of dimension $2h$.*

Proof. Since $\mathbb{F}_q$ is the splitting field of E, and E is separable of degree p^{2h}, $\#W = p^{2h}$.

In addition, since E is an additive polynomial, its roots form an $\mathbb{F}_p$-vector space. An $\mathbb{F}_p$-vector space of size p^{2h} is of dimension $2h$ over $\mathbb{F}_p$ $\square$

We also define a polynomial B_c for each c in W :

$$B_c(x) = \sum_{i=0}^{h-1} b_i x^{p^i}$$

where $b_0 = -ca_0 - R(c)$ and $b_i = -ca_i + b_{i-1}^p$ for $1 \leq i \leq h-1$.

Proposition 3.2.4. *Let $c \in W$ and b be a solution of the equation $x^p - x = cR(c)$. We can then define an automorphism $\sigma_{b,c} : C_R \mapsto C_R$ $(x, y) \mapsto (x + c, y + b + B_c(x))$. This automorphism of C_R fixes the point at ∞.*

These automorphisms in fact give all of the p-power order automorphisms of C_R.

Theorem 3.2.5 (From section 4 of [1])**.** *The group $\mathrm{Aut}^0(C_R)$ has a unique Sylow p-subgroup, which we denote by P. It is the subgroup consisting of all automorphisms $\sigma_{b,c}$, given in Proposition 3.2.4, has cardinality p^{2h+1}, and each of its elements is of order p.*

Remark 3.2.6. We further know that $\mathrm{Aut}^0(C_R)$ is a semi-direct product of P and a cyclic subgroup H containing elements of the form $\sigma(x, y) = (ax, dy)$.

We note that one can show that the center of P is $Z(P) = \langle \sigma_{1,0} \rangle$ where $\sigma_{1,0}(x, y) = (x, y+1)$ is the Artin-Schreier automorphism. By explicit computation, one can show that

$$\sigma_{b_1,c_1}\sigma_{b_2,c_2}\sigma_{b_1,b_1}^{-1}\sigma_{b_2,b_2}^{-1} = \sigma_{1,0}^{B_{c_1}(c_2)+B_{c_2}(c_1)},$$

which gives rise to a symplectic pairing on W given by

$$\epsilon(c_1, c_2) = B_{c_1}(c_2) - B_{c_2}(c_1).$$

As a result, when $\epsilon(c_1, c_2) = 0$ then we know that σ_{b_1,c_1} and σ_{b_2,c_2} commute for any allowable choice of b_1, b_2. This pairing gives W the structure of a symplectic space, and any isotropic subspace has a pre-image in P which gives an abelian subgroup. We now explain the significance of abelian subgroups of P to our understanding of the curve C_R. We begin by stating a result on the structure of a maximal abelian subgroup of P, and some of its distinguished subgroups.

Proposition 3.2.7 (adapted from section 5 of [1])**.** *Let $h \geq 1$.*

1. *Every maximal abelian subgroup $\mathcal{A}$ of P is an elementary abelian group of order p^{h+1}, and is normal in P.*

2. *Let $\mathcal{A} \simeq (\mathbb{Z}/p\mathbb{Z})^{h+1}$ be a maximal abelian subgroup of P. For any subgroup $A = A_p \simeq (\mathbb{Z}/p\mathbb{Z})^h \subset \mathcal{A}$ with $A_p \cap Z(P) = \{1\}$ there exist subgroups $A_1, \ldots, A_{p-1}$ of $\mathcal{A}$ such that*

$$\mathcal{A} = Z(P) \cup A_1 \cup \ldots \cup A_p,$$

$A_i \simeq (\mathbb{Z}/p\mathbb{Z})^h$, $A_i \cap Z(P) = \{1\}$, $A_i \cap A_j = \{1\}$ if $i \neq j$.

Theorem 3.2.8 (from section 7 of [1])**.** *Assume $h \geq 1$. Let $\mathcal{A}$ be a maximal abelian subgroup of P. Any subgroup $A \subset \mathcal{A}$ of order p^h that intersects the center $Z(P)$ of P trivially gives rise to an $\mathbb{F}_q$-isomorphism of the quotient curve $\overline{\mathrm{C}}_A$ onto the smooth projective curve given by the affine equation*

$$y^p - y = a_{\mathcal{A}} x^2,$$

where

$$a_{\mathcal{A}} = \frac{a_h}{2} \prod_{c \in A \setminus \{0\}} c.$$

This theorem, along with a theorem of Kani-Rosen [10] then allows the authors of [1] to connect the point count of the easy-to-understand curve $y^p - y = a_{\mathcal{A}} x^2$ to the point count of the original curve C_R. Since the maximality of the curve $y^p - y = a_{\mathcal{A}} x^2$ depends only on the values of the constant $a_{\mathcal{A}}$, in turn that of C_R also does:

Theorem 3.2.9 (Adapted from section 9 of [1])**.** *If a field $\mathbb{F}_{p^s}$ contains the splitting field $\mathbb{F}_q$ of $E(x)$, then C_R is maximal over $\mathbb{F}_{p^s}$ if and only if one of the following holds:*

- *s is even, $a_{\mathcal{A}}$ is a nonsquare in $\mathbb{F}_q^*$, and $p \equiv 1 \pmod 4$;*
- *$s \equiv 0 \pmod 4$, $a_{\mathcal{A}}$ is a nonsquare in $\mathbb{F}_q^*$, and $p \equiv 3 \pmod 4$;*
- *$s \equiv 2 \pmod 4$, $a_{\mathcal{A}}$ is a square in $\mathbb{F}_q^*$ and $p \equiv 3 \pmod 4$.*

3.3 Computing a Maximal Isotropic Space

Therefore, to determine if C_R is maximal and the smallest field extension over which it is maximal, it suffices to compute a maximal isotropic subspace of W. Then, its nonzero element will allow us to compute the constant $a_{\mathcal{A}}$, which determines if and where C_R is maximal. The algorithm to compute such a space is given in Algorithm 4 below.

Proposition 3.3.1. *Algorithm 4 does yield the nonzero elements of a maximal isotropic subspace of W.*

Algorithm 4 Computing a maximal isotropic subspace

INPUT: polynomial $R(x)$
OUTPUT: the nonzero elements of a maximal isotropic subspace of W

```
compute the list of roots of E(x) in its splitting field (the set W)
place the first non-zero element of W in the isotropic subset
for c_1 in W do
    if ε(c_1, c_2) = 0 for all c_2 in the isotropic subset then
        add c_1 to the subset
    end if
end for
```

Proof. We show that the algorithm always yields a set of size $p^h - 1$ by showing that if at any point we have an isotropic set of size $n < p^h - 1$, we will be able to add an element. Clearly, if $n = p^h - 1$ the set is maximal so no elements can be added and the algorithm terminates.

Suppose first that the set $\{x_1, \ldots, x_n\}$ spans a space of dimension $m < h$. Then the equations

$$\epsilon(x_j, x) = 0$$

$j = 1, \ldots, n$ yield a linear map $\mathbb{F}_q^{2h} \mapsto \mathbb{F}_q^n$ of rank m. Indeed, by the theory of symplectic spaces, there is a basis $c_1, c_2, \ldots, c_h, c'_1, \ldots, c'_h$ of W such that $\epsilon(c_i, c_j) = \epsilon(c'_i, c'_j) = 0$ and $\epsilon(c_i, c'_j) = \delta_{ij}$. Now we write x_j and x in this basis:

$$x_j = \sum_{i=1}^{h} a_{ij} c_i + \sum_{i=1}^{h} b_{ij} c'_i$$

and

$$x = \sum_{i=1}^{h} d_i c_i + \sum_{i=1}^{h} e_i c'_i.$$

Using the properties of the basis $c_1, \ldots, c'_h$ and the linearity of ϵ, we have that

$\epsilon(x_j, x) = 0$ if and only if

$$\sum_{i=1}^{h} a_{ij} e_i + \sum_{i=1}^{h} b_{ij} d_i = 0.$$

Therefore the equations $\epsilon(x_j, x) = 0$ form a set of n linear equations in $2h$ variables. Since $\{x_1, \ldots, x_n\}$ span a set of dimension m, the rank of this map is m. The nullity of this map is thus $2h - m > h > m$ so there is x_{n+1} in the kernel of this map which does not belong to the set $\{x_1, \ldots, x_n\}$ (nor, in fact, its span).

If $\{x_1, \ldots, x_n\}$ spans a space of dimension h, but $n < p^h - 1$, then there is a nonzero element x_{n+1} in the span of $\{x_1, \ldots, x_n\}$ (and thus in the kernel), but not in the set $\{x_1, \ldots, x_n\}$ so we can add this element to our isotropic set.

□

Chapter 4

Results

In this chapter we present maximal Artin-Schreier curves defined over $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$ and $\mathbb{F}_9$ to be further explored in future work. For each polynomial R, such that C_R becomes maximal, we give the splitting field $\mathbb{F}_q$ of E and the degree of the smallest extension of $\mathbb{F}_q$ such that C_R is maximal over this extension. The following families of polynomials were explored for each field where a, b are both elements of the respective field:

- $ax^p + bx$
- $ax^{p^2} + bx^p$
- $ax^{p^2} + bx$

$\mathbb{F}_3$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_3$	x	4
$\mathbb{F}_3$	$2x$	2
$\mathbb{F}_{3^6}$	$x^3 + x$	6
$\mathbb{F}_{3^3}$	$2x^3 + x$	12
$\mathbb{F}_{3^3}$	$x^3 + 2x$	6
$\mathbb{F}_{3^6}$	$2x^3 + 2x$	6
$\mathbb{F}_{3^{18}}$	$x^9 + x^3$	18
$\mathbb{F}_{3^9}$	$2x^9 + x^3$	18
$\mathbb{F}_{3^{18}}$	$x^9 + 2x^3$	36

$\mathbb{F}_5$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{5^4}$	x^5	4
$\mathbb{F}_{5^4}$	$2x^5$	4
$\mathbb{F}_{5^4}$	$3x^5$	4
$\mathbb{F}_{5^4}$	$4x^5$	4
$\mathbb{F}_{5^{10}}$	$x^5 + x$	10
$\mathbb{F}_{5^3}$	$2x^5 + x$	6
$\mathbb{F}_{5^6}$	$3x^5 + x$	6
$\mathbb{F}_5$	$2x$	2
$\mathbb{F}_{5^6}$	$x^5 + 2x$	6
$\mathbb{F}_{5^{10}}$	$2x^5 + 2x$	10

$\mathbb{F}_5$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{5^5}$	$3x^5 + 2x$	10
$\mathbb{F}_5$	$3x$	2
$\mathbb{F}_{5^5}$	$2x^5 + 3x$	10
$\mathbb{F}_{5^{10}}$	$3x^5 + 3x$	10
$\mathbb{F}_{5^6}$	$4x^5 + 3x$	6
$\mathbb{F}_{5^6}$	$2x^5 + 4x$	6
$\mathbb{F}_{5^3}$	$3x^5 + 4x$	6
$\mathbb{F}_{5^{10}}$	$4x^5 + 4x$	10
$\mathbb{F}_{5^8}$	x^{25}	8
$\mathbb{F}_{5^8}$	$2x^{25}$	8
$\mathbb{F}_{5^8}$	$3x^{25}$	8
$\mathbb{F}_{5^8}$	$4x^{25}$	8
$\mathbb{F}_{5^{30}}$	$x^{25} + x^5$	30
$\mathbb{F}_{5^{13}}$	$2x^{25} + x^5$	26
$\mathbb{F}_{5^{26}}$	$3x^{25} + x^5$	26
$\mathbb{F}_{5^{26}}$	$x^{25} + 2x^5$	26
$\mathbb{F}_{5^{30}}$	$2x^{25} + 2x^5$	30
$\mathbb{F}_{5^{15}}$	$3x^{25} + 2x^5$	30
$\mathbb{F}_{5^{15}}$	$2x^{25} + 3x^5$	30
$\mathbb{F}_{5^{30}}$	$3x^{25} + 3x^5$	30
$\mathbb{F}_{5^{26}}$	$4x^{25} + 3x^5$	26
$\mathbb{F}_{5^4}$	$4x^5$	4

$\mathbb{F}_5$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{5^{26}}$	$2x^{25} + 4x^5$	26
$\mathbb{F}_{5^{13}}$	$3x^{25} + 4x^5$	26
$\mathbb{F}_{5^{30}}$	$4x^{25} + 4x^5$	30
$\mathbb{F}_{5^{20}}$	$x^{25} + x$	20
$\mathbb{F}_{5^6}$	$2x^{25} + x$	6
$\mathbb{F}_{5^{12}}$	$3x^{25} + x$	12
$\mathbb{F}_{5^{10}}$	$4x^{25} + x$	10
$\mathbb{F}_{5^{12}}$	$x^{25} + 2x$	12
$\mathbb{F}_{5^{20}}$	$2x^{25} + 2x$	20
$\mathbb{F}_{5^{10}}$	$3x^{25} + 2x$	10
$\mathbb{F}_{5^6}$	$4x^{25} + 2x$	6
$\mathbb{F}_{5^6}$	$x^{25} + 3x$	6
$\mathbb{F}_{5^{10}}$	$2x^{25} + 3x$	10
$\mathbb{F}_{5^{20}}$	$3x^{25} + 3x$	20
$\mathbb{F}_{5^{12}}$	$4x^{25} + 3x$	12
$\mathbb{F}_{5^{10}}$	$x^{25} + 4x$	10
$\mathbb{F}_{5^{12}}$	$2x^{25} + 4x$	12
$\mathbb{F}_{5^6}$	$3x^{25} + 4x$	6
$\mathbb{F}_{5^{20}}$	$4x^{25} + 4x$	20
End of Table		

$\mathbb{F}_7$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_7$	x	2
$\mathbb{F}_{7^{14}}$	$x^7 + x$	14
$\mathbb{F}_{7^3}$	$2x^7 + x$	12
$\mathbb{F}_{7^6}$	$5x^7 + x$	6
$\mathbb{F}_{7^7}$	$6x^7 + x$	14
$\mathbb{F}_7$	$2x$	2
$\mathbb{F}_{7^{14}}$	$2x^7 + 2x$	14
$\mathbb{F}_{7^6}$	$3x^7 + 2x$	6
$\mathbb{F}_{7^3}$	$4x^7 + 2x$	12
$\mathbb{F}_{7^7}$	$5x^7 + 2x$	14
$\mathbb{F}_7$	$3x$	4
$\mathbb{F}_{7^6}$	$x^7 + 3x$	6
$\mathbb{F}_{7^{14}}$	$3x^7 + 3x$	14
$\mathbb{F}_{7^7}$	$4x^7 + 3x$	28
$\mathbb{F}_{7^3}$	$6x^7 + 3x$	6
$\mathbb{F}_7$	$4x$	2
$\mathbb{F}_{7^3}$	$x^7 + 4x$	12
$\mathbb{F}_{7^7}$	$3x^7 + 4x$	14
$\mathbb{F}_{7^{14}}$	$4x^7 + 4x$	14
$\mathbb{F}_{7^6}$	$6x^7 + 4x$	6
$\mathbb{F}_7$	$5x$	4
$\mathbb{F}_{7^7}$	$2x^7 + 5x$	28

$\mathbb{F}_7$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{7^3}$	$3x^7 + 5x$	6
$\mathbb{F}_{7^6}$	$4x^7 + 5x$	6
$\mathbb{F}_{7^{14}}$	$5x^7 + 5x$	14
$\mathbb{F}_7$	$6x$	4
$\mathbb{F}_{7^7}$	$x^7 + 6x$	28
$\mathbb{F}_{7^6}$	$2x^7 + 6x$	6
$\mathbb{F}_{7^3}$	$5x^7 + 6x$	6
$\mathbb{F}_{7^{14}}$	$6x^7 + 6x$	14
$\mathbb{F}_{7^{42}}$	$x^{49} + x^7$	42
$\mathbb{F}_{7^{25}}$	$2x^{49} + x^7$	50
$\mathbb{F}_{7^{50}}$	$5x^{49} + x^7$	50
$\mathbb{F}_{7^{21}}$	$6x^{49} + x^7$	84
$\mathbb{F}_{7^{42}}$	$2x^{49} + 2x^7$	42
$\mathbb{F}_{7^{50}}$	$3x^{49} + 2x^7$	50
$\mathbb{F}_{7^{25}}$	$4x^{49} + 2x^7$	50
$\mathbb{F}_{7^{21}}$	$5x^{49} + 2x^7$	84
$\mathbb{F}_{7^{50}}$	$x^{49} + 3x^7$	50
$\mathbb{F}_{7^{42}}$	$3x^{49} + 3x^7$	42
$\mathbb{F}_{7^{21}}$	$4x^{49} + 3x^7$	42
$\mathbb{F}_{7^{25}}$	$6x^{49} + 3x^7$	100
$\mathbb{F}_{7^{25}}$	$x^{49} + 4x^7$	50
$\mathbb{F}_{7^{21}}$	$3x^{49} + 4x^7$	84

$\mathbb{F}_7$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{7^{42}}$	$4x^{49} + 4x^7$	42
$\mathbb{F}_{7^{50}}$	$6x^{49} + 4x^7$	50
$\mathbb{F}_{7^{21}}$	$2x^{49} + 5x^7$	42
$\mathbb{F}_{7^{25}}$	$3x^{49} + 5x^7$	100
$\mathbb{F}_{7^{50}}$	$4x^{49} + 5x^7$	50
$\mathbb{F}_{7^{42}}$	$5x^{49} + 5x^7$	42
$\mathbb{F}_{7^{21}}$	$x^{49} + 6x^7$	42
$\mathbb{F}_{7^{50}}$	$2x^{49} + 6x^7$	50
$\mathbb{F}_{7^{25}}$	$5x^{49} + 6x^7$	100
$\mathbb{F}_{7^{42}}$	$6x^{49} + 6x^7$	42
$\mathbb{F}_{7^6}$	$2x^{49} + x$	6
$\mathbb{F}_{7^{14}}$	$6x^{49} + x$	14
$\mathbb{F}_{7^2}$	$4x^{49} + 2x$	6
$\mathbb{F}_{7^{14}}$	$5x^{49} + 2x$	14
$\mathbb{F}_{7^{14}}$	$4x^{49} + 3x$	14
$\mathbb{F}_{7^6}$	$6x^{49} + 3x$	6
$\mathbb{F}_{7^6}$	$x^{49} + 4x$	6
$\mathbb{F}_{7^{14}}$	$3x^{49} + 4x$	14
$\mathbb{F}_{7^{14}}$	$2x^{49} + 5x$	14
$\mathbb{F}_{7^6}$	$3x^{49} + 5x$	6
$\mathbb{F}_{7^{14}}$	$x^{49} + 6x$	14
$\mathbb{F}_{7^6}$	$5x^{49} + 6x$	6

$\mathbb{F}_7$		
Splitting Field	Polynomial R	Deg of Ext
End of Table		

$\mathbb{F}_9$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{3^2}$	$(a+1)x^3$	2
$\mathbb{F}_{3^8}$	$(2a+2)x^3$	2
$\mathbb{F}_{3^2}$	ax	4
$\mathbb{F}_{3^6}$	$(a+1)x$	2
$\mathbb{F}_{3^6}$	$ax^3+(a+1)x$	12
$\mathbb{F}_{3^6}$	$(2a+1)x^3+(a+1)x$	12
$\mathbb{F}_{3^6}$	$2x^3+(a+1)x$	6
$\mathbb{F}_{3^6}$	$2ax^3+(a+1)x$	12
$\mathbb{F}_{3^6}$	$(a+2)x^3+(a+1)x$	12
$\mathbb{F}_{3^6}$	$x^3+(a+1)x$	6
$\mathbb{F}_{3^2}$	$(2a+1)x$	4
$\mathbb{F}_{3^2}$	$2x$	2
$\mathbb{F}_{3^6}$	ax^3+2x	12
$\mathbb{F}_{3^6}$	$(2a+1)x^3+2x$	12
$\mathbb{F}_{3^6}$	$2x^3+2x$	6
$\mathbb{F}_{3^6}$	$2ax^3+2x$	12
$\mathbb{F}_{3^6}$	$(a+2)x^3+2x$	12
$\mathbb{F}_{3^6}$	x^3+2x	6

$\mathbb{F}_9$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{3^2}$	$2ax$	4
$\mathbb{F}_{3^2}$	$(2a+2)x$	2
$\mathbb{F}_{3^6}$	$ax^3+(2a+2)x$	12
$\mathbb{F}_{3^6}$	$(2a+1)x^3+(2a+2)x$	12
$\mathbb{F}_{3^6}$	$2x^3+(2a+2)x$	6
$\mathbb{F}_{3^6}$	$2ax^3+(2a+2)x$	12
$\mathbb{F}_{3^6}$	$(a+2)x^3+(2a+2)x$	12
$\mathbb{F}_{3^6}$	$x^3+(2a+2)x$	6
$\mathbb{F}_{3^2}$	$(a+2)x$	4
$\mathbb{F}_{3^2}$	x	2
$\mathbb{F}_{3^6}$	ax^3+x	12
$\mathbb{F}_{3^6}$	$(2a+1)x^3+x$	12
$\mathbb{F}_{3^6}$	$2x^3+x$	6
$\mathbb{F}_{3^6}$	$2ax^3+x$	12
$\mathbb{F}_{3^6}$	$(a+2)x^3+x$	12
$\mathbb{F}_{3^6}$	x^3+x	6
$\mathbb{F}_{3^{10}}$	ax^9+2x^3	20
$\mathbb{F}_{3^{18}}$	$(a+1)x^9+2x^3$	18
$\mathbb{F}_{3^{10}}$	$(2a+1)x^9+2x^3$	20
$\mathbb{F}_{3^{18}}$	$2x^9+2x^3$	18
$\mathbb{F}_{3^{10}}$	$2ax^9+2x^3$	20
$\mathbb{F}_{3^{10}}$	$(2a+2)x^9+2x^3$	18

$\mathbb{F}_9$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{3^{10}}$	$(a+2)x^9 + 2x^3$	20
$\mathbb{F}_{3^{18}}$	$x^9 + 2x^3$	18
$\mathbb{F}_{3^{10}}$	$ax^9 + x^3$	20
$\mathbb{F}_{3^{18}}$	$(a+1)x^9 + x^3$	18
$\mathbb{F}_{3^{10}}$	$(2a+1)x^9 + x^3$	20
$\mathbb{F}_{3^{18}}$	$2x^9 + x^3$	18
$\mathbb{F}_{3^{10}}$	$2ax^9 + x^3$	20
$\mathbb{F}_{3^{18}}$	$(2a+2)x^9 + x^3$	18
$\mathbb{F}_{3^{10}}$	$(a+2)x^9 + x^3$	20
$\mathbb{F}_{3^{18}}$	$x^9 + x^3$	18
$\mathbb{F}_{3^{10}}$	$(a+1)x^9 + ax$	10
$\mathbb{F}_{3^{10}}$	$2x^9 + ax$	10
$\mathbb{F}_{3^6}$	$2ax^9 + ax$	12
$\mathbb{F}_{3^{10}}$	$(2a+1)x^9 + (a+1)x$	20
$\mathbb{F}_{3^{10}}$	$2ax^9 + (a+1)x$	20
$\mathbb{F}_{3^6}$	$(2a+2)x^9 + (a+1)x$	6
$\mathbb{F}_{3^{10}}$	$2x^9 + (2a+1)x$	10
$\mathbb{F}_{3^{10}}$	$(2a+2)x^9 + (2a+1)x$	10
$\mathbb{F}_{3^6}$	$(a+2)x^9 + (2a+1)x$	12
$\mathbb{F}_{3^{10}}$	$2ax^9 + 2x$	20
$\mathbb{F}_{3^{10}}$	$(a+2)x^9 + 2x$	20
$\mathbb{F}_{3^6}$	$x^9 + 2x$	6

$\mathbb{F}_9$		
Splitting Field	Polynomial R	Deg of Ext
$\mathbb{F}_{3^6}$	$ax^9 + 2ax$	12
$\mathbb{F}_{3^{10}}$	$(2a+2)x^9 + 2ax$	10
$\mathbb{F}_{3^{10}}$	$x^9 + 2ax$	10
$\mathbb{F}_{3^{10}}$	$ax^9 + (2a+2)x$	20
$\mathbb{F}_{3^6}$	$(a+1)x^9 + (2a+2)x$	6
$\mathbb{F}_{3^{10}}$	$(a+2)x^9 + (2a+2)x$	20
$\mathbb{F}_{3^{10}}$	$(a+1)x^9 + (a+2)x$	10
$\mathbb{F}_{3^6}$	$(2a+1)x^9 + (a+2)x$	12
$\mathbb{F}_{3^{10}}$	$x^9 + (a+2)x$	10
$\mathbb{F}_{3^{10}}$	$ax^9 + x$	20
$\mathbb{F}_{3^{10}}$	$(2a+1)x^9 + x$	20
$\mathbb{F}_{3^6}$	$2x^9 + x$	6
End of Table		

Bibliography

[1] Irene Bouw, Wei Ho, Beth Malmskog, Renate Scheidler, Padmavathi Srinivasan, and Christelle Vincent. Zeta functions of a class of Artin-Schreier curves with many automorphisms. In *Directions in number theory*, volume 3 of *Association for Women in Mathematics Series*, pages 87–124. Springer, 2016.

[2] Shawn Farnell. *Artin-Schreier Curves*. PhD thesis, Colorado State University, 2010.

[3] Wade Trappe and Lawrence Washington. *Introduction to cryptography with coding theory*. Pearson, 2006.

[4] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. In *DSN Progress Report*, volume 44, pages 114–116. 1978.

[5] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 2009.

[6] Iwan M. Duursma. Majority coset decoding. *IEEE Transactions on Information Theory*, 39(3):1067–1070, 1993.

[7] Gui Liang Feng and T.R.N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 39(1):37–45, 1993.

[8] Sergei G. Vladut and Alexei N. Skorobogatov. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 36(5):1051–1060, 1990.

[9] Neil Koblitz. *Algebraic Aspects of Cryptography*. Springer, 1999.

[10] Ernst Kani and Michael Rosen. Idempotent relations and factors of Jacobians. *Mathematische Annalen*, 284(2):307–327, 1989.