

A New Construction of Maximal Curves

Abigail Ebin, Deborah Hur, Aaron Katz, and Vladislav Shchogolev

Communicated by Rachel Pries

ABSTRACT. Fuhrmann, Garcia, and Torres [FGT97] proved there is a unique maximal curve of genus $(q-1)^2/4$ defined over \mathbb{F}_{q^2} . We give a new construction of this curve as a pullback of the natural action of $\mathrm{PSL}_2(\mathbb{F}_q)$ on the projective line by a Kummer cover.

CONTENTS

1. Introduction and Preliminaries	1
2. Mathematical Ingredients	3
3. The Construction of the Maximal Curve	8
4. Related Work	10
References	10

1. Introduction and Preliminaries

1.1. Introduction. Maximal curves are of central importance in the development of algebraic coding theory. The correspondence between curves with many points over a finite field and effective error correcting codes is well established. Tsfasman, Vlăduț, and Zink in 1982 [TVZ82] exploited this correspondence to find a sequence of efficient codes which correct many errors. Here we present a new construction of the maximal curve over \mathbb{F}_{q^2} for each odd prime power q studied by Fuhrmann, Garcia, and Torres. Our construction of the curve involves normalizing the fibre product of a Kummer cover and the cover arising from the natural action of $\mathrm{PSL}_2(\mathbb{F}_q)$ on the projective line $\mathbb{P}_{\mathbb{F}_q}^1$. We develop the necessary machinery in depth in Section 2.

1991 *Mathematics Subject Classification.* Primary 14G50; Secondary 11G20, 11T71, 14H30.
Key words and phrases. maximal curve, coding theory, Galois.

The authors were supported by an undergraduate research project in mathematics during summer 2002 at Columbia University sponsored by NSF VIGRE grant DMS-98-10750.

©0000 (copyright holder)

We would like to thank the NSF for their generous support of this VIGRE undergraduate research project during the summer of 2002. Also, the guidance and help of Professor Jeff Achter, Professor Rachel Pries, Sebastian Casalaina-Martin, and Morgan Sherman has been invaluable.

1.2. Coding Theory. We start with the finite field \mathbb{F}_q which will be our *alphabet*. The number of elements q is a power of a prime p . For the purposes of this paper, we will consider only finite fields of characteristic $p > 2$. Any *message word* we wish to encode is an element of \mathbb{F}_q^j for some j . The message word is encoded into a *codeword* in \mathbb{F}_q^n for some $n > j$.

DEFINITION 1.1. For any n , a *code* C of length n over \mathbb{F}_q , is a subset of \mathbb{F}_q^n .

A code C is called *linear* if C is a vector subspace of \mathbb{F}_q^n . The *dimension* k of a linear code C is the dimension of C over \mathbb{F}_q . If $x, y \in C$ are codewords, we define the *Hamming distance* $d_H(x, y) = \#\{i : x_i \neq y_i\}$ and the *Hamming weight* $wt(x) = d_H(0, x)$, which are essential to our understanding of what makes a good code. We define the *minimum distance* $d = \min\{d_H(x, y) : x, y \in C, x \neq y\}$.

PROPOSITION 1.2. *The Hamming distance d_H is a metric on C .*

PROOF. That d_H is symmetric is obvious. Also, $d_H(x, y)$ must be positive for $x \neq y$. Furthermore, for $x, y, z \in C$, we see that if x and z differ in a coordinate, then either x and y differ there or y and z differ there or both. Thus $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$. \square

PROPOSITION 1.3. *For a linear code, d equals the minimum weight wt_{min} .*

PROOF. Since every weight is also a distance, we see $d \leq wt_{min}$. We can choose two code words x and y where $d_H(x, y) = d$. Since C is linear, $x - y$ is also a code word and $wt(x - y) = d$. So, $wt_{min} \leq d$. Thus we conclude, $d = wt_{min}$. \square

The minimum distance is significant because the maximum number of errors a code with minimum distance d can correct is $\lfloor \frac{d-1}{2} \rfloor$. Considering the distance as a metric, this is clear. If the number of errors is greater than $\frac{d-1}{2}$, then there is either not a unique closest code word or the closest code word is not the one intended.

Our goal is to find a code that has both a high information rate, $R = \frac{k}{n}$, and a high relative distance, $\delta = \frac{d}{n}$. This will allow for efficient coding and accurate error correcting.

1.3. Algebraic Geometry and Codes. We see an interesting application of algebraic geometry to coding theory. First, here are some preliminary definitions.

Let X be a nonsingular projective curve defined over the field \mathbb{F}_q .

DEFINITION 1.4. Let D be a divisor on X . The space of rational functions associated to D is

$$L(D) := \{f \in \mathbb{F}_q(X) : \text{div}(f) + D \geq 0\} \cup \{0\}.$$

Goppa's construction of algebraic-geometric codes is as follows:

DEFINITION 1.5. Let $\mathcal{P} = \{P_1, P_2, \dots, P_n\} \subset X(\mathbb{F}_q)$ with $P_i \neq P_j$ for $i \neq j$. Let D be a divisor on X such that $\text{supp}(D) \cap \mathcal{P} = \emptyset$. Then the algebraic geometric code associated to X, \mathcal{P} , and D is

$$C(X, \mathcal{P}, D) := \{(f(P_1), f(P_2), \dots, f(P_n)) : f \in L(D)\} \subset \mathbb{F}_q^n.$$

Recall that a good code is both efficient (high information rate) and corrects many errors (large minimum distance). In terms of Goppa codes, with a little argument, these criteria will be satisfied for a curve with many rational points relative to its genus.

We state the following theorem and refer the reader to [Wei48] for the proof. It is valuable to find curves whose number of points is as close as possible to the following upper bound:

THEOREM 1.6 (Hasse-Weil Bound). *Let X be a nonsingular projective curve of genus g over the field \mathbb{F}_q and set $N = \#X(\mathbb{F}_q)$. Then*

$$|N - (q + 1)| \leq 2g\sqrt{q}.$$

A curve with exactly $q + 1 + 2g\sqrt{q}$ points over \mathbb{F}_q is called *maximal*.

2. Mathematical Ingredients

2.1. The Kummer Cover. Let k be an algebraically closed field of characteristic p . For m relatively prime to p , consider the smooth projective curve Y in $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ given by the equation $f(x, y) = y^m - x$. The ring extension $k[x] \hookrightarrow k[x, y]/(f)$ defines a cover $g : Y \rightarrow \mathbb{P}_k^1$ sending $(x, y) \mapsto x$, whose Galois group G we now compute.

We first consider the automorphism $\sigma(y) = \zeta y$, where ζ is a primitive m^{th} root of unity in k . Since the degree of the extension is m and the order of σ is m , we conclude that the extension is Galois, and the Galois group associated to g is $\mathbb{Z}/m\mathbb{Z}$, generated by the automorphism σ .

To find the branch and ramification points in the (x, y) -affine patch of the curve, we look at which points of the curve are fixed by a nontrivial element τ in the Galois group G . Since σ generates G , we may write $\tau(y) = \sigma^i(y) = \zeta^i y$ for some $i \in \mathbb{Z}$, $m \nmid i$. We see that $y = \zeta^i y$ if and only if $y = 0$. So g is ramified at the point 0_Y where $x = y = 0$. To consider $\infty_{\mathbb{P}^1}$, we use a change of coordinates, $\bar{x} = 1/x$ and $\bar{y} = 1/y$. We similarly conclude that in the (\bar{x}, \bar{y}) -patch of the curve, $\bar{y} = \zeta^i \bar{y}$ if and only if $\bar{y} = 0$. Thus the two ramified points are 0_Y and ∞_Y , which lie above the branch points $0_{\mathbb{P}^1}$ and $\infty_{\mathbb{P}^1}$, respectively.

DEFINITION 2.1. Let $\phi : Y \rightarrow X$ be a Galois cover of curves with Galois group G . Let $P \in X$ and let $Q \in \phi^{-1}(P)$. The *decomposition group* at Q is $D_Q = \{\sigma \in G : \sigma(Q) = Q\}$. The *inertia group* I_Q at Q is the group of automorphisms in D_Q that induce the identity on the residue field of Y at Q . Over an algebraically closed field, the inertia group equals the decomposition group.

Notice for the cover g that above each of the branch points, there is only one point above it in the fibre. Thus the inertia groups of 0_Y and ∞_Y are both $\mathbb{Z}/m\mathbb{Z}$.

We refer the reader to [Har77, IV Corollary 2.4] for the proof of the next theorem.

THEOREM 2.2 (Riemann-Hurwitz Formula). *Let $\phi : Y \rightarrow X$ be a non-constant separable morphism of non-singular projective curves defined over k . If p does not divide the order of any inertia group and $\deg(R) = \sum_Q (|I_Q| - 1)$ is the sum over all ramification points $Q \in Y$, then we have*

$$2g_Y - 2 = \deg(\phi)(2g_X - 2) + \deg(R).$$

Applying the Riemann-Hurwitz formula, we see that:

$$2g_Y - 2 = m(2g_X - 2) + \deg(R) = -2m + 2(m - 1).$$

So the genus of Y is 0 and thus $Y \cong \mathbb{P}_k^1$.

2.2. $\mathrm{PSL}_2(\mathbb{F}_q)$. Let $q = p^r$ for some prime p . Let $\mathrm{SL}_2(\mathbb{F}_q)$ be the group of two-by-two matrices whose entries are in \mathbb{F}_q and which have determinant one. Let $H \leq \mathrm{SL}_2(\mathbb{F}_q)$ be the normal subgroup $\{I, -I\}$. Let $\mathrm{PSL}_2(\mathbb{F}_q)$ be the quotient group $\mathrm{SL}_2(\mathbb{F}_q)/H$. Now we would like to compute the size of this group.

LEMMA 2.3. *The order of $\mathrm{GL}_2(\mathbb{F}_q)$ is $(q^2 - 1)(q^2 - q)$.*

PROOF. A matrix is invertible if and only if its column vectors are linearly independent. Given the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, there are $q^2 - 1$ choices such that the first column is a nonzero vector. The number of elements in the span of this vector is q , one for each of its scalar multiples. Since the first and second vector must be linearly independent, our choice for the second column is limited to any of the other $q^2 - q$ vectors in the space. \square

PROPOSITION 2.4. *The order of $\mathrm{PSL}_2(\mathbb{F}_q)$ is $q(q^2 - 1)/2$.*

PROOF. We have

$$|\mathrm{PSL}_2(\mathbb{F}_q)| = (\mathrm{SL}_2(\mathbb{F}_q) : H) = |\mathrm{SL}_2(\mathbb{F}_q)| / 2.$$

Furthermore, $\det : \mathrm{GL}_2(\mathbb{F}_q) \rightarrow \mathbb{F}_q^*$ is a surjective homomorphism with kernel $\mathrm{SL}_2(\mathbb{F}_q)$. Hence $\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q) \cong \mathbb{F}_q^*$ and $|\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q)| = q - 1$. So,

$$|\mathrm{SL}_2(\mathbb{F}_q)| = \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{q - 1} = \frac{(q^2 - 1)(q^2 - q)}{q - 1} = q(q^2 - 1).$$

Combining these two equations we arrive at the desired result. \square

2.3. Subgroups. The set B of lower triangular matrices in $\mathrm{SL}_2(\mathbb{F}_q)$ forms a subgroup under multiplication.

LEMMA 2.5. *The quotient B/H in $\mathrm{PSL}_2(\mathbb{F}_q)$ is isomorphic to a semi-direct product $(\mathbb{Z}/p\mathbb{Z})^r \rtimes \mathbb{Z}/\frac{(q-1)}{2}\mathbb{Z}$.*

PROOF. Let t be a generator of the cyclic group \mathbb{F}_q^* and let T in $\mathrm{SL}_2(\mathbb{F}_q)$ be the subgroup generated by $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$. This matrix has order $q - 1$. This is because $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}^i = \begin{pmatrix} t^i & 0 \\ 0 & t^{-i} \end{pmatrix}$ which is the identity if and only if i is a multiple of $q - 1$. So T is a cyclic group of order $q - 1$.

Now let $A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ where $a \in \mathbb{F}_q$. We have $A^n = \begin{pmatrix} 1 & 0 \\ na & 1 \end{pmatrix}$. Since \mathbb{F}_q has characteristic p , A has order p in $\mathrm{SL}_2(\mathbb{F}_q)$ if $a \neq 0$. Let P be this subset of lower triangular matrices with ones on the diagonal. Then there is a group isomorphism $\phi : P \rightarrow \langle \mathbb{F}_q, + \rangle$ given by the map $\phi : \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mapsto a$. To see this, suppose A is as

defined above and $B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$. Then

$$\phi(AB) = \phi\left(\begin{pmatrix} 1 & 0 \\ a+b & 1 \end{pmatrix}\right) = a+b = \phi(A) + \phi(B).$$

In turn, $\langle \mathbb{F}_q, + \rangle$ is isomorphic to $\langle (\mathbb{Z}/p\mathbb{Z})^r, + \rangle$ if $q = p^r$.

Since P is normalized by T and $P \cap T = \{I\}$, the group B is isomorphic to a semi-direct product $(\mathbb{Z}/p\mathbb{Z})^r \rtimes \mathbb{Z}/(q-1)\mathbb{Z}$. Also $H \subseteq T$. Thus, $B/H \cong (\mathbb{Z}/p\mathbb{Z})^r \rtimes \mathbb{Z}/\frac{(q-1)}{2}\mathbb{Z}$. \square

2.4. Action of $\mathrm{PSL}_2(\mathbb{F}_q)$ on \mathbb{P}^1 . Next, we examine the action of $\mathrm{PSL}_2(\mathbb{F}_q)$ on the projective line, \mathbb{P}^1 . First, we must verify that we do in fact get an action of this group on \mathbb{P}^1 .

PROPOSITION 2.6. *The group $\mathrm{PSL}_2(\mathbb{F}_q)$ gives an action on the set \mathbb{P}^1 .*

PROOF. We define the action of $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on a choice of coordinates $[x_0 : x_1]$ of a point x in \mathbb{P}^1 like this:

$$M(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} ax_0 + bx_1 \\ cx_0 + dx_1 \end{pmatrix}.$$

First, we show that the action is well defined (i.e., it does not depend on the choice of coordinates for x under the equivalence relation \sim for the projective line).

$$M(tx) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} t \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} atx_0 + btx_1 \\ ctx_0 + dtx_1 \end{pmatrix} = t \begin{pmatrix} ax_0 + bx_1 \\ cx_0 + dx_1 \end{pmatrix} \sim M(x).$$

Hence, the action is well-defined. All matrices in $\mathrm{SL}_2(\mathbb{F}_q)$ are invertible, so none can map an element of \mathbb{P}^1 to the zero-vector, which is not in \mathbb{P}^1 . Next we must check that the subgroup $H = \{I, -I\}$ of $\mathrm{SL}_2(\mathbb{F}_q)$ acts trivially on \mathbb{P}^1 , since we identify elements of H with the identity in $\mathrm{PSL}_2(\mathbb{F}_q)$. This is clear for $I \in H$. For $-I \in H$, we see that $-Ix = -x \sim x$. Thus H acts trivially on \mathbb{P}^1 and we get an action of $\mathrm{PSL}_2(\mathbb{F}_q)$ on \mathbb{P}^1 . \square

Now, we look at the orbit of the point $[0 : 1]$ (i.e., the point at ∞) under the action.

PROPOSITION 2.7. *The stabilizer of $[0 : 1]$ is B/H which has order $q(q-1)/2$. The orbit of $[0 : 1]$ consists of the $q+1$ points in $\mathbb{P}_{\mathbb{F}_q}^1$.*

PROOF.

$$\text{We see } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix} \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ if and only if } b = 0 \text{ and } d \neq 0.$$

Thus $\mathrm{Stab}[0 : 1] = \left\{ \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} : a, c \in \mathbb{F}_q, a \neq 0 \right\} / H$ which is B/H . There are q possibilities for c and $q-1$ possibilities for a , hence there are $q(q-1)$ elements of B . Hence $|B/H| = |B|/2 = q(q-1)/2$.

We see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix} \sim \begin{pmatrix} 1 \\ d/b \end{pmatrix} \text{ for } b \neq 0 \text{ and } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ for } b = 0.$$

If $b = 0$ we get the point at infinity $[0 : 1]$. If $b \neq 0$, we can get any point of \mathbb{F}_q for d/b . Thus the orbit of the point at infinity is $\mathbb{P}_{\mathbb{F}_q}^1$. \square

Now, we look at the other points under the action.

LEMMA 2.8. *The matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixes $[1 : x_1]$ if and only if $bx_1^2 + (a - d)x_1 - c = 0$.*

PROOF. If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixes $[1 : x_1]$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ x_1 \end{pmatrix} = \begin{pmatrix} t \\ tx_1 \end{pmatrix}$ for some $t \in \mathbb{F}_q^*$. So $(a + bx_1)x_1 = tx_1$ and $c + dx_1 = tx_1$. So $(a - d)x_1 + bx_1^2 = c$.

If $bx_1^2 + (a - d)x_1 - c = 0$ then $(c + dx_1)/(a + bx_1) = x_1$. So

$$M \begin{pmatrix} 1 \\ x_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ x_1 \end{pmatrix} = \begin{pmatrix} a + bx_1 \\ c + dx_1 \end{pmatrix} \sim \begin{pmatrix} 1 \\ x_1 \end{pmatrix}.$$

\square

PROPOSITION 2.9. *The set F of all x which are not in the orbit of $[0 : 1]$ and which are fixed by some matrix $M \in PSL_2(\mathbb{F}_q)$ is $\mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1$.*

PROOF. Suppose $x \in F$. Without any loss of generality, we write $x = [1 : x_1]$. If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixes $[1 : x_1]$ then $bx_1^2 + (a - d)x_1 - c = 0$. Hence x_1 satisfies a quadratic equation with coefficients in \mathbb{F}_q , so it is contained in \mathbb{F}_{q^2} . Recalling that x is not in the orbit of the point at ∞ , we see $F \subseteq \mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1$.

Conversely, given $x \in \mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1$, we show that x is fixed by some matrix, $M \in PSL_2(\mathbb{F}_q)$. Again without a loss of generality, we can write $x = [1 : x_1]$ where $x_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. From the lemma, we want to find a, b, c, d so that $bx_1^2 + (a - d)x_1 - c = 0$. Consider the unique monic irreducible polynomial $x^2 + \alpha x + \beta$, with $\alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$, which has x_1 as a root. Equating coefficients, we need

$$\begin{aligned} a - d &= b\alpha, \\ \text{and } -c &= \beta b. \end{aligned}$$

These equations give us a matrix M , but its determinant is not necessarily one. Let $M' = (1/\det M)M^2$. Notice that

$$\det(M') = \det\left(\frac{1}{\det M}M^2\right) = \frac{1}{(\det M)^2}(\det M)^2 = 1.$$

If $M \in GL_2(\mathbb{F}_q)$ fixes x , then M^2 fixes x . Multiplying by a scalar (in this case, $1/(\det M)^2$) also fixes x because of the equivalence relation on the projective line. Thus $M' \in SL_2(\mathbb{F}_q)$ and fixes x whenever M fixes x .

We only need to find one $M \in SL_2(\mathbb{F}_q)$ (which fixes x) so that M' is not the identity matrix. If $\alpha \neq 0$, we let $a = 0$ and $b = 1$. From the above equations, we get:

$$\begin{aligned} M' &= \frac{1}{\beta} \begin{pmatrix} 0 & 1 \\ -\beta & -\alpha \end{pmatrix}^2 = \begin{pmatrix} -1 & -\alpha\beta^{-1} \\ \alpha & \alpha^2\beta^{-1} - 1 \end{pmatrix} \\ \text{and } \det(M') &= 1 - \alpha^2\beta^{-1} + \alpha^2\beta^{-1} = 1. \end{aligned}$$

If $\alpha = 0$, then $\beta \neq -1$ since $x_1^2 + \beta$ is irreducible. We let $a = b = 1$. Then $M' = \frac{1}{1+\beta} \begin{pmatrix} 1-\beta & 2 \\ -2\beta & 1-\beta \end{pmatrix}$.

After identifying M' with its coset, we end up with a non-trivial element of $\mathrm{PSL}_2(\mathbb{F}_q)$ which fixes x . Thus $\mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1 \subseteq F$. \square

Now we wish to compute the stabilizer and orbit of an element $x = [1 : x_1]$ of F . Let $x^2 + \alpha x + \beta$ be the irreducible polynomial for x_1 over \mathbb{F}_q . Before we can do this we need to define the following group:

$$D_x = \left\{ M = \begin{pmatrix} a & b \\ -b\beta & a - b\alpha \end{pmatrix}, a, b \in \mathbb{F}_q \text{ not both zero} \right\}.$$

These are all the matrices that fix a given $x \in F$. To see that $D_x \subset \mathrm{GL}_2(\mathbb{F}_q)$, notice that $\det M = a^2 - ab\alpha + b^2\beta$. If $b = 0$ then $a \neq 0$ so $\det M \neq 0$. If $b \neq 0$ and $\det M = 0$, then $(a/b)^2 - (a/b)\alpha + \beta = 0$. This equation has the same discriminant as $x^2 + \alpha x + \beta$ which is irreducible over \mathbb{F}_q . So $(a/b) \notin \mathbb{F}_q$ which gives a contradiction.

To pick out the matrices with determinant one, we construct the homomorphism:

$$f : D_x \longrightarrow \mathbb{F}_q^*$$

where $f(M) = \det M$ for all $M \in D_x$.

PROPOSITION 2.10. *Given $x = [1 : x_1] \in F$ with irreducible polynomial $x^2 + \alpha x + \beta = 0$, $\mathrm{Stab}[1 : x_1] = (\ker f)/H$. This group is cyclic of order $(q+1)/2$.*

PROOF. By the fundamental homomorphism theorem,

$$\frac{|D_x|}{|\ker f|} = |\mathrm{Im} f| = \frac{q-1}{(\mathbb{F}_q^* : \mathrm{Im} f)}.$$

The cardinality of D_x is $q^2 - 1$ since a and b cannot both be zero. Thus,

$$|\ker f| = \frac{|D_x|}{q-1} (\mathbb{F}_q^* : \mathrm{Im} f) = (q+1)(\mathbb{F}_q^* : \mathrm{Im} f).$$

To get an upper bound for $|\ker f|$, suppose

$$\det M = a^2 - ab\alpha + b^2\beta = 1.$$

Using the quadratic formula gives an equation for a in terms of b . Thus, for every one of the q choices for b , there are at most 2 choices for a . So there are at most $2q$ elements in $\ker f$.

This gives

$$(q+1)(\mathbb{F}_q^* : \mathrm{Im} f) = |\ker f| \leq 2q.$$

Since the index is a natural number, by the inequality above, the only choice is $(\mathbb{F}_q^* : \mathrm{Im} f) = 1$. Therefore, $|\ker f/H| = (q+1)/2$. Since $\mathrm{Stab}[1 : x_1]$ is the inertia group at x and p does not divide $(q+1)/2$, the inertia group is cyclic. \square

PROPOSITION 2.11. *The group $\mathrm{PSL}_2(\mathbb{F}_q)$ acts transitively on F .*

PROOF. If $x, y \in F$, we need to show there is some $M \in \mathrm{PSL}_2(\mathbb{F}_q)$ such that $Mx = y$. Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and let $x \in \mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1$. We can write $x = [1 : x_1]$. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Now we show that $Mx \in F$ by contradiction. Suppose $Mx \in \mathbb{P}_{\mathbb{F}_q}^1$. Notice that $a + bx_1 \neq 0$ since $x_1 \notin \mathbb{F}_q$. So,

$$Mx = \begin{pmatrix} 1 \\ \frac{c+dx_1}{a+bx_1} \end{pmatrix} \Rightarrow \frac{c+dx_1}{a+bx_1} = \gamma \in \mathbb{F}_q.$$

$$\begin{aligned} \text{It follows that } c + dx_1 &= \gamma(a + bx_1) \\ \text{and } (d - \gamma b)x_1 &= \gamma a - c. \end{aligned}$$

Since $a, b, c, d, \gamma \in \mathbb{F}_q$, then $x_1 = (\gamma a - c)/(d - \gamma b) \in \mathbb{F}_q$. This is a contradiction. Thus $G \cdot x \subseteq F$. Furthermore, we see

$$|G \cdot x| = \frac{|G|}{|\mathrm{Stab}(x)|} = \frac{q(q^2 - 1)/2}{(q + 1)/2} = q(q - 1) = q^2 - q = |F|.$$

Thus, $\mathrm{PSL}_2(\mathbb{F}_q)$ acts transitively on F . \square

3. The Construction of the Maximal Curve

3.1. The Construction of the Maximal Curve. Let $f : W \rightarrow \mathbb{P}_k^1$ be the quotient cover $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1/\mathrm{PSL}_2(\mathbb{F}_q)$ and $g : Y \rightarrow \mathbb{P}_k^1$ be the Kummer cover given by the equation $y^m = x$. Let $m = (q + 1)/2$. Let Z be the fibre product $W \times_{f,g} Y$:

$$\begin{array}{ccc} Z := W \times_{f,g} Y & \xrightarrow{\pi_2} & Y \\ \downarrow \pi_1 & & \downarrow g \\ W & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

Recall that f and g have the following properties:

	f		g	
Galois Group	$\mathrm{PSL}_2(\mathbb{F}_q)$		$\mathbb{Z}/m\mathbb{Z}$	
Branch Points	$\mathbf{0}_{\mathbb{P}^1}$	$\infty_{\mathbb{P}^1}$	$\mathbf{0}_{\mathbb{P}^1}$	$\infty_{\mathbb{P}^1}$
Ramification Points	$\mathbb{P}_{\mathbb{F}_{q^2}}^1 \setminus \mathbb{P}_{\mathbb{F}_q}^1$	$\mathbb{P}_{\mathbb{F}_q}^1$	$\mathbf{0}_Y$	∞_Y
Number of Ramification Points	$q^2 - q$ points	$q + 1$ points	1	1
Order of Inertia Group	$\frac{q+1}{2}$	$\frac{q(q-1)}{2}$	$\frac{q+1}{2}$	$\frac{q+1}{2}$

By Abhyankar's Lemma, [Gro71, Lemma X 3.6], the fiber product Z is singular at the $q^2 - q$ points above $\mathbf{0}$ since f and g are both ramified over $\mathbf{0}_{\mathbb{P}^1}$ with order $(q + 1)/2$. Let \tilde{Z} denote the normalization of Z . Let f_1 be the map that takes \tilde{Z} to Y , and let g_1 be the map that takes \tilde{Z} to W . The degree of f_1 is $q(q^2 - 1)/2$ and g_1 has degree m . The Galois groups associated with the maps f_1 and g_1 are the same as the Galois groups associated with f and g .

Let $F : \tilde{Z} \rightarrow \mathbb{P}_k^1$. Then $F = f \circ g_1 = g \circ f_1$. Also F has degree $q(q^2 - 1)m/2$ and Galois group $\mathrm{PSL}_2(\mathbb{F}_q) \times \mathbb{Z}/m\mathbb{Z}$.

$$\begin{array}{ccc}
 \tilde{Z} & \xrightarrow{f_1} & Y \\
 \downarrow g_1 & \searrow F & \downarrow g \\
 W & \xrightarrow{f} & \mathbb{P}^1
 \end{array}$$

The normalization of Z replaces each singular point with $(q+1)/2$ points. The cover g_1 is then unramified at the $(q+1)(q^2-q)/2$ points in $F^{-1}(\mathbf{0})$.

The order of the ramification of $g^{-1}(\infty)$ is $(q^2-q)/2$, which is relatively prime to $(q+1)/2$. So g_1 is ramified at the points in $F^{-1}(\infty)$ with inertia group $\mathbb{Z}/m\mathbb{Z}$. Thus, there are $q+1$ points in $f_1^{-1}(\infty)$ and one point in $g_1^{-1}(\infty)$, so there are $q+1$ points in \tilde{Z} above ∞ , ramified with order $(q+1)/2$.

3.2. Genus of \tilde{Z} . We will use the Riemann-Hurwitz formula to determine the genus of \tilde{Z} . For a nonconstant separable morphism of projective curves $\varphi : Y \rightarrow X$ with X of genus g_X , the Riemann-Hurwitz formula 2.2 states that

$$2g_Y - 2 = \deg(\varphi)(2g_X - 2) + \deg R.$$

If $\deg \varphi$ is relatively prime to the characteristic of the base field (which it is here), then $\deg R = \sum_Q (|I_Q| - 1)$, where the sum is over all the ramification points $Q \in Y$.

THEOREM 3.1. *The genus of \tilde{Z} is $(q-1)^2/4$.*

PROOF. We apply Riemann-Hurwitz to the map $g_1 : \tilde{Z} \rightarrow W$, recalling that W is \mathbb{P}^1 :

$$2g_{\tilde{Z}} - 2 = \deg(g_1)(2g_{\mathbb{P}^1} - 2) + \deg R.$$

As we have shown before, g_1 is ramified at $q+1$ points and the inertia group for each one is $\mathbb{Z}/m\mathbb{Z}$. Hence $|I_Q| - 1 = m - 1$, and $\deg R = (q+1)(m-1) = (q+1)(q-1)/2$. Furthermore, the genus of the projective line, \mathbb{P}^1 , is zero. We have

$$g_{\tilde{Z}} = [-(q+1) + \frac{(q+1)(q-1)}{2} + 2]/2 = (q-1)^2/4. \quad \square$$

The computation of the genus can also be made using the map $f_1 : \tilde{Z} \rightarrow Y$. It is considerably more complicated since p divides the orders of the inertia groups, but it verifies this result.

3.3. Points on \tilde{Z} .

THEOREM 3.2. *The curve \tilde{Z} is maximal over \mathbb{F}_{q^2} .*

PROOF. First, we look at the \mathbb{F}_q -rational points on \tilde{Z} . All of the \mathbb{F}_q -rational points in W map to ∞ by f and only the point at ∞ itself maps from Y to ∞ . In the fibre product $W \times_{f,g} Y$, there are $q+1$ points over ∞ , so there are $q+1$ \mathbb{F}_q -rational points on \tilde{Z} .

Next, we look at the number of \mathbb{F}_{q^2} -rational points that are not \mathbb{F}_q -rational points. The $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ -rational points of \tilde{Z} map to zero by F . The curve Z is singular at 0 , but when we normalize to \tilde{Z} , we get m distinct points. Each of these points is \mathbb{F}_{q^2} -rational since m divides $q^2 - 1$ and so the m th roots of unity are in \mathbb{F}_{q^2} . Thus there are $m(q^2 - q)$ \mathbb{F}_{q^2} -rational points that are not \mathbb{F}_q -rational points. Note that

$$m(q^2 - q) = (q+1)(q-1)q/2 = (q^3 - q^2)/2.$$

Let N be the total number of points over \mathbb{F}_{q^2} . We see that N is $(q^3 - q^2)/2 + q + 1$. We compare this to the Hasse-Weil bound:

$$|N - (q^2 + 1)| = \left| \frac{q^3 - q^2}{2} + q + 1 - (q^2 + 1) \right| \leq 2g\sqrt{q^2}.$$

In fact we have $|N - (q^2 + 1)| = |q(q-1)^2/2| = 2gq$. So \tilde{Z} meets the Hasse-Weil bound, i.e., it is maximal over \mathbb{F}_{q^2} . \square

4. Related Work

Fuhrmann, Garcia, and Torres [FGT97] proved there is a unique maximal curve of genus $(q-1)^2/4$ defined over \mathbb{F}_{q^2} . We refer the reader to [FGT97, Theorem 3.1] for the proof.

THEOREM 4.1 (Fuhrmann, Garcia, Torres). *Let X be a maximal curve over \mathbb{F}_{q^2} of genus $g = (q-1)^2/4$. Then the curve X is \mathbb{F}_{q^2} -isomorphic to the one given by*

$$y^q + y = x^{(q+1)/2}.$$

So the curve \tilde{Z} is \mathbb{F}_{q^2} -isomorphic to the curve with equation $y^q + y = x^{(q+1)/2}$. We can find another equation for \tilde{Z} using the cover $g_1 : \tilde{Z} \rightarrow W$. The curve W is \mathbb{P}^1 and g_1 is branched at $f^{-1}(\infty_{\mathbb{P}^1})$ (which are the \mathbb{F}_q -rational points of \mathbb{P}^1) with inertia group $\mathbb{Z}/m\mathbb{Z}$. So \tilde{Z} has equation $z^m = \prod_{i \in \mathbb{F}_q} (y - i)$ which simplifies to $z^{(q+1)/2} = y^q - y$. These two equations are isomorphic over \mathbb{F}_{q^2} but not over \mathbb{F}_q .

Ihara [Iha81] and Tsfasman, Vlăduț, and Zink [TVZ82] used modular curves to construct a sequence of codes over \mathbb{F}_q that have a high information rate and a high relative distance. These codes are efficient and have good error-correcting capabilities. It turns out that the curve \tilde{Z} is related to these codes. The cover $f_1 : \tilde{Z} \rightarrow Y$ has Galois group $\mathrm{PSL}_2(\mathbb{F}_q)$ and is branched at only one point $g^{-1}(\infty_{\mathbb{P}^1}) = \infty_Y$. When $q = p$, there is only one cover like this so that \tilde{Z} has genus $(p-1)^2/4$ and it comes from the reduction of the modular curve $X(p)$, [BW04, Proposition 5.3].

References

- [BW04] I. Bouw and S. Wewers. Stable reduction of modular curves. In *Modular curves and abelian varieties (Barcelona, 2002)* Cremona et al eds, pages 1–22. Progress in Math, vol 224, Birkhäuser, 2004.
- [FGT97] R. Fuhrmann, A. Garcia, and F. Torres. On maximal curves. *J. Number Theory*, 67(1):29–51, 1997.
- [Gro71] A. Grothendieck. *Revêtements étales et groupe fondamental*. Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.
- [Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [Iha81] 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.
- [TVZ82] M. Tsfasman, S. Vlăduț, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.
- [Wei48] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

DEPARTMENT OF MATHEMATICS, COLUMBIA UNIVERSITY, NEW YORK, NEW YORK 10027

E-mail address: `ace2001@columbia.edu`

E-mail address: `dhur@math.upenn.edu`

E-mail address: `amk156@columbia.edu`

E-mail address: `vs299@columbia.edu`