Deligne-Lusztig curves as ray class fields

Kristin Lauter

lauter@mpim-bonn.mpg.de

1 Introduction

This paper provides a detailed explanation of Serre's method for using class field theory to construct curves over finite fields with many rational points. This method can be implemented in a systematic way to generate curves over any finite field with many rational points. The power of the method is clear from the fact that it produces or reproduces most of the best existing curves. For example, we give here the ray class field description of the Deligne-Lusztig curves: Hermitian, Suzuki, and Ree. These families are important because each member has the maximum number of points possible for its genus. The ray class field descriptions of these three families are remarkably similar to each other:

Theorem 1 *The Hermitian, Suzuki, and Ree curves can be realized by splitting the q places of degree one different from (∞) of $\mathbb{F}_q(T)$, $q = p^f$, in the ray class field of conductor $D = k(\infty)$, where*

$$k = \begin{cases} p^{\lceil f/2 \rceil} + 2 & \text{if } q \text{ is a square or } p=2 \\ p^{\lceil f/2 \rceil} + 3 & \text{if } p=3 \end{cases}$$

(The Hermitian curves are defined when q is a square; the Suzuki (resp. Ree) curves are defined when q is not a square and the characteristic is 2 (resp. 3).)

From this theorem, we derive interesting results on the order of the group of units of quotitents of polynomial rings.

Corollary 1 *If $q = p^f$ and either q is a square or $p = 2$ or 3, then*

$$|(\mathbb{F}_q[T])/T^k)^*/\mathbb{F}_q^*/\langle 1 - \alpha T | \alpha \in \mathbb{F}_q^* \rangle|$$
$$= \begin{cases} 1 & \text{if } k < p^{\lceil f/2 \rceil} + 2 \\ \sqrt{q} & \text{if } k = p^{\lceil f/2 \rceil} + 2,\ q \text{ is a square} \\ q & \text{if } k = p^{\lceil f/2 \rceil} + 2,\ q \text{ not a square, } p=2 \text{ or } 3 \end{cases}$$

An excellent survey of the progress in constructing curves with many points is contained in the introduction to [9]. These authors use explicit class field theory, and have further demonstrated the power of Serre's method by generating many new examples of curves which come close to the bounds on the number of points.

Section 2 summarizes the known bounds on the number of points. Section 3 consists of a detailed explanation of the application of class field theory to constructing curves with many points. It includes examples of curves constructed via this method which meet the bounds on the number of points. Section 4 gives the ray class field descriptions of the Deligne-Lusztig curves.

Acknowledgements I would like to thank my advisor, Niels Nygaard, for his support for this project. I would also like to thank Rene Schoof for his help and suggestions. This work constitutes a large portion of my thesis at the University of Chicago, and I would like to thank the math department for their support. I would also like to thank the Max Planck Institute for a wonderful place to work.

2 Bounds

This section gives a brief summary of the best known bounds for the number of rational points on a smooth curve of genus g over the field $\mathbb{F}_q$. A rational point is a prime which has residue field isomorphic to $\mathbb{F}_q$. When refering to points, we will always mean rational points. The best-known bound on the number of points is the Hasse-Weil bound:

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

For each g and q, $N_q(g)$ is defined as the maximum number of points on a curve of genus g over $\mathbb{F}_q$. When q is an even power of a prime, $N_q(g)$ can actually be equal to the Hasse-Weil bound. If a curve meets the Hasse-Weil bound, we say it is *Hasse-Weil maximal.* Any curve over $\mathbb{F}_q$ which is *Hasse-Weil maximal* has the property that ([14])

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

Furthermore, [1], either the curve is isomorphic to the Hermitian curve, or else we have $g \leq (\sqrt{q}-1)^2/4$. In the case where q is not a square, the situation is much more difficult to determine.

When q is an odd power of a prime, the Hasse-Weil bound was improved by J.P. Serre to the bound:

$$\#X(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}],$$

where $[x]$ denotes the integer part of x.

Neither of these bounds is effective when the genus is large compared to q, and the improvements on this bound using Weil's "explicit formulae" are significant. To state these bounds, we introduce several auxiliary functions. If $\{c_n\}_{n\geq 1}$ are real numbers, put

$$f(\theta) = 1 + 2\sum_{n=1}^{\infty} c_n \cos(n\theta) = 1 + \sum_{n=1}^{\infty} c_n(e^{in\theta} + e^{-in\theta})$$

for $\theta \in \mathbb{R}$, and

$$\Psi_d(t) = \sum_{n=1}^{\infty} c_{nd} t^{nd}$$

for $d \in \mathbb{N}$, $t \in \mathbb{R}$. Now the bounds arise in the following circumstances: Suppose the $\{c_n\}$ have the following properties:

1. $c_n \geq 0$, not all $c_n = 0$
2. $f(\theta) \geq 0$ for all $\theta \in \mathbb{R}$

Then

$$N \leq \frac{g}{\Psi_1(q^{-\frac{1}{2}})} + \frac{\Psi_1(q^{\frac{1}{2}})}{\Psi_1(q^{-\frac{1}{2}})} + 1$$

This method will yield different bounds depending on the choice of $\{c_n\}$. The Weil bound, for example, is obtained by choosing $c_1 = 1/2$, $c_i = 0$, $i > 1$. It was shown by Oesterle that there exists an optimal choice for the $\{c_n\}$. Oesterle's optimization of this method is described in [13] as follows: "A genus g curve over $\mathbb{F}_q$ with $L+1$ rational points satisfies:

$$g \geq \sup_{\Psi}\{L\Psi(q^{-1/2}) - \Psi(q^{1/2})\} \geq \frac{(L-1)\sqrt{q}\cos\theta_0 + q - L}{q + 1 - 2\sqrt{q}\cos\theta_0}$$

Moreover, if $q \geq 3$ the second inequality is actually an equality, where $\Psi(T) = \sum c_n T^n$ with c_n non-negative and $\Psi(t) + \Psi(\bar{t}) + 1 \geq 0$, for $t \in \mathbb{C}$, $|t| = 1$, as in conditions 1 and 2 above. The value of θ_0 is defined as follows: Let m be the unique integer for which

$$\sqrt{q}^m < L \leq \sqrt{q}^{m+1}.$$

Put

$$u = \frac{\sqrt{q}^{m+1} - L}{L\sqrt{q} - \sqrt{q}^m} \in [0, 1)$$

and let θ_0 denote the unique solution of the equation

$$\cos\frac{m+1}{2}\theta + u\cos\frac{m-1}{2}\theta = 0$$

in the interval $[\frac{\pi}{m+1}, \frac{\pi}{m})$."

Example 1 *Over $\mathbb{F}_4$, a curve with 65 points must have genus $g \geq 32$*

Proof: Since $L = 64$, we find that $m = 5$, $u = 0$. Then $\theta_0 = \pi/6$, and $g \geq 31.9808....$

Example 2 *Over $\mathbb{F}_4$, a curve with 66 points must have genus $g \geq 33$*

Proof: Since $L = 65$, we find that $m = 6$, $u = 63/65$. Then $\theta_0 = 0.522207$, and $g \geq 32.5743....$

Example 3 *Over $\mathbb{F}_4$, a curve with 67 points must have genus $g \geq 34$*

Proof: Since $L = 66$, we find that $m = 6$, $u = 31/34$. Then $\theta_0 = 0.51951$, and $g \geq 33.283....$

These examples establish the following corollary:

Corollary 2 $N_4(33) \leq 66$

This section surveyed the techniques for obtaining upper bounds for $N_q(g)$. To obtain lower bounds for $N_q(g)$, we must construct curves with many points.

3 Serre's method

In this section we explain Serre's method for using class field theory for function fields over finite fields to construct curves with many points. We have benefited greatly from the expoosition in [13] to understand Serre's original results [11].

Let K be the function field of a smooth, irreducible curve X over $\mathbb{F}_q$. Abelian covers of X correspond to abelian extensions of K, which correspond by class field theory to subgroups of finite index of C_K, the idele class group of K. Class field theory ensures that for each finite quotient of C_K, there exists an abelian extension of K having this quotient as its Galois group. C_K is the quotient of the idele group $\mathbb{A}_K^*$ by K^*. Let U denote the quotient of the units of $\mathbb{A}_K^*$ by $\mathbb{F}_q^*$. The group of units of $\mathbb{A}_K^*$, $\mathfrak{U}$, consists of all elements of $\mathbb{A}_K^*$ which have valuation zero everywhere.

So in order to construct curves over $\mathbb{F}_q$ as covers of X, it suffices to consider the finite quotients of C_K. To accomplish this, begin by defining a subgroup, U_D, of U, for each divisor D on X.

Definition 1 *If $D = \sum n_\nu \nu$ is a divisor on X, let*

$$U_D = \{(x_\nu) \in U \mid x_\nu \equiv 1 \pmod{t_\nu^{n_\nu}}\}.$$

The definition of $\mathfrak{U}_D$ is analogous.

Definition 2 *A* Ray class field *of conductor D is an extension of K whose Galois group is a finite quotient of C_K/U_D.*

Finite quotients of C_K/U_D are obtained by taking the quotient by the subgroup generated by the uniformizer of at least one place of degree one outside the support of D. This can be seen by considering the following exact sequence:

$$0 \to U/U_D \to C_K/U_D \to Pic(X) \to 0.$$

where the second map sends an element $(x_\nu) \in C_K$ to $\sum v_\nu(x_\nu)\nu$. For any ν, a place of degree one outside the support of D, let K_ν^* denote the multaplicative group of the completion of K at ν, suitably embedded in C_K. Since ν is not in the support of D, the entire unit group $\mathcal{O}_\nu^*$ is trivial in C_K/U_D. Thus the image of K_ν^* in C_K/U_D is generated by a uniformizer at ν, embedded as

$(1, 1, ..., t_\nu, 1, ..)$. It is a copy of $\mathbb{Z}$, which coincides with the infinite factor in $C_K/U_D \cong Pic(X) \times U/U_D$. As we will see below, the quotient of C_K/U_D by K_ν^* is the Galois group of a finite extension in which at least ν is totally split. The next task is to determine the degree and the ramification of the extension, and the outcome of splitting additional places.

The curve constructed via this process depends on the initial choice of three parameters: the base field (or curve) K, the divisor D, which determines the ramification, and the number of places of degree one in the base which we require to be split. In what follows, we will explain how to determine the genus and the number of rational points of the outcome based on the various choices for the input.

3.1 Degree of the extension

The curve corresponding to a finite extension L/K has at least as many points as the degree of the extension, n_L, times the number of places of degree one of the base which are totally split, plus any places of degree one of the base which are totally ramified in the extension:

$$\#X_L(\mathbb{F}_q) \geq n_L(\#\text{ totally split places }) + (\#\text{ totally ramified places})$$

The importance of computing the degree of the extension is clear. If the degree is large, so is the number of rational points, but so also is the genus. Good results are obtained for example when extra places are split without changing the degree. We first consider the situation when D consists of a multiple of just one place, where P_d denotes a place of degree d. We also restrict ourselves to the case where K is the function field of the projective line, $\mathbb{F}_q(T)$. In this case, $Pic(X) \cong \mathbb{Z}$, so if one place of degree one is split, the Galois group is isomorphic to U/U_D, which is described in the following lemma:

Lemma 1 *Let $D = k(P_d)$, $k \in \mathbb{N}$, $d \geq 1$. Then $U/U_D \cong (\mathbb{F}_q[T]/(P_d(T))^k)^*/\mathbb{F}_q^*$.*

Proof: D has only one place in its support, and $\mathfrak{U}_D$ is the entire unit group at every place outside its support, so

$$\mathfrak{U}/\mathfrak{U}_D \cong R^*/(1 + (P_d)^k R)$$

, where R is the completion of $K = \mathbb{F}_q(X)$ at P_d. (We use the symbol P_d to denote both the place and a uniformizer at that place: an irreducible polynomial of degree d.) Now if R is a complete discrete valuation ring with maximal ideal $\mathfrak{M}$ and $k \geq 1$ is an integer, then the group homomorphism:

$$R^* \to (R/\mathfrak{M}^k R)^*$$

is surjective (R^* is the complement of $\mathfrak{M}$), and has kernel $1+\mathfrak{M}^k R$. In our case,

$$R/\mathfrak{M}^k R \cong \mathbb{F}_q[T]/P_d(T)^k,$$

so

$$(R/\mathfrak{M}^k R)^* \cong (\mathbb{F}_q[T]/P_d(T)^k)^*,$$

which quotiented by the global units in U gives the desired result. $\Box$

Remark 1 *When the support of D contains more than one place, we can apply this lemma to each prime separately, and the quotient U/U_D will be the direct sum of the factors obtained in this manner.*

When $K = \mathbb{F}_q(T)$, splitting one place of degree one yields a Galois group which is isomorphic to U/U_D, but splitting more than one place yields a Galois group which is a quotient of U/U_D.

Lemma 2 *Let $D = k(P_d)$, $k \in \mathbb{N}$. Let $K = \mathbb{F}_q(T)$. Then*

$$G \cong (\mathbb{F}_{q^d}[T]/(P_d(T))^k)^*/(\mathbb{F}_q^* \cdot < T - \nu_2, ..., T - \nu_r >)$$

is the Galois group of the extension in which $\nu_1, ..., \nu_r$, r places of degree one of K, are totally split. Here the notation ν_i denotes the place of degree one with uniformizer $(T - \nu_i)$, where ν_i also denotes an element of $\mathbb{F}_q$.

Proof: A place of K is *totally split* if and only if the decomposition group at that place is trivial. Since the decomposition group is generated by the "Frobenius substitution" of the prime, we can ensure that a place of degree one splits by taking the quotient by this element. Locally, we quotient K_ν^* by the prime ideal corresponding to ν, and this is compatible with the embeddings of K_ν^* into C_K and of $D_\mathfrak{p}$ into G. The prime corresponding to a place ν of K is generated by a polynomial of the form $T - \nu$, $\nu \in \mathbb{F}_q$. The first place split will cancel out the factor of $\mathbb{Z}$ from C_K/U_D. From the description of U/U_D given in Lemma 1, we obtain the desired result after taking the quotient by the subgroup generated by the elements $T - \nu_2, ..., T - \nu_r$. $\Box$

3.2 Computation of the genus

It is possible to compute the genus of a curve corresponding to an abelian extension because the information about the ramification of the extension can be extracted from the knowledge of the Galois group. By a theorem of class field theory, a place, ν, is unramified in an extension L/K if and only if $\mathcal{O}_\nu^* \subset N(C_L)$. This translates into the fact that the coefficient of ν is zero in D, the conductor of the extension. In other words, ramification only occurs at the places in the support of D. To understand this, we recall that locally, the conductor of a finite extension $\widehat{L}_\nu/\widehat{K}_\nu$ is defined to be the smallest integer n_ν such that the reciprocity map

$$\theta : \widehat{K}_\nu^* \to Gal(\widehat{L}_\nu/\widehat{K}_\nu)$$

is trivial on U^{n_ν}. Here $U = \mathcal{O}_\nu^*$, and $U^i = \{u \in U \mid u \equiv 1 \pmod{t_\nu^i}\}$ defines a decreasing filtration of U with $U^0 = U$. Since the kernel of θ is $N(\widehat{L}_\nu)$, we see that

$$\mathcal{O}_\nu^* \subset N(C_L) \iff n_\nu = 0.$$

To understand the ramification at places where the reciprocity map is not trivial on $\mathcal{O}_\nu^*$, we introduce the notion of the *Artin conductor* of a character. The Artin conductor of a character coincides with the conductor as defined above when the character has degree one, which is the case here since the extensions are abelian. We give here the definitions of the Artin class function and the local and global Artin conductor and the derivation of a type of Hurwitz genus formula from the conductor-discriminant formula. This presentation has been extracted largely from [12].

3.2.1 Local case

If G is the Galois group of a finite Galois extension L/K, where K is a field *complete* with respect to a discrete valuation, and L/K has separable residue field extension, then the Artin class function, $a_G(s)$, is defined for all $s \in G$ as:

Definition 3

$$a_G(s) = -f \cdot i_G(s), \quad s \neq 1$$
$$a_G(1) = f \sum_{s \neq 1} i_G(s).$$

where $i_G(s) = \nu_L(s(\pi) - \pi)$, π is a uniformizer for L, and f is the residue degree. We can also define a filtration on the inertia group at the prime as follows:

$$G_i = \{s \in G | i_G(s) \geq i + 1\}$$

The ramification is said to be *tame* if $G_1 = \{1\}$.

Definition 4 *The Artin conductor of a character χ of G is given by*

$$\mathfrak{f}(\chi) = (\chi, a_G(s)) = \frac{1}{g} \sum_{s \in G} a_G(s)\chi(s^{-1}),$$

where $g = |G|$. This is equivalent to letting $\mathfrak{f}(\chi)$ be the coefficient of χ in the expression for $a_G(s)$ as a linear combination of irreducible characters.

It is known that a_G is the character of a linear representation of G, called the Artin representation. The proof of this statement relies on the Hasse-Arf theorem and implies that $\mathfrak{f}(\chi)$ is a non-negative integer for every character χ of G.

3.2.2 Global case

The above definitions apply to extensions of function fields after localisation and completion at a prime. If L/K is a Galois extension of a global field with group G, and χ is a character of G, then the *global conductor* of χ is:

$$f(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{f}(\chi, \mathfrak{p})},$$

where $\mathfrak{f}(\chi, \mathfrak{p})$ is defined as follows. If $D_{\mathfrak{P}}$ is the decomposition group of a prime $\mathfrak{P}$ lying over $\mathfrak{p}$, $a_{\mathfrak{P}}$ is the Artin class function associated to this group, and $a_{\mathfrak{p}}$ is the character of G induced by $a_{\mathfrak{P}}$ for any $\mathfrak{P} \mid \mathfrak{p}$, then

$$\mathfrak{f}(\chi, \mathfrak{p}) = (\chi, a_{\mathfrak{p}}) = \mathfrak{f}(\chi \mid D_{\mathfrak{P}})$$

As in the local case, $\mathfrak{f}(\chi, \mathfrak{p}) = 0$ if $\mathfrak{p}$ is unramified, since then $a_{\mathfrak{p}}(s) = 0$, for all $s \in G$.

3.2.3 Genus formulas

The purpose of introducing the Artin conductors is to make use of a relation called the conductor-discriminant formula. If $\mathfrak{d}_{L/K}$ is the discriminant of a Galois extension L/K, then

$$\mathfrak{d}_{L/K} = \prod f(\chi)^{\chi(1)}.$$

If all characters have degree 1, then we have

$$\mathfrak{d}_{L/K} = \prod f(\chi).$$

Now from this relation we obtain a formula for the genus in terms of the Artin conductors of the characters:

Proposition 1 *If L/K is a finite Galois extension with Galois group G, and χ are the irreducible characters of G, then the genus of the cover is related to the genus of the base as follows:*

$$2g_L - 2 = [L : K](2g_K - 2) + \deg(\prod_{\chi} f(\chi)),$$

where the last term indicates the degree of the divisor associated to the prime decompostion of the ideal which is the product of the global conductors over the irreducible characters χ of G:

$$\deg(\prod_{\chi} f(\chi)) = \sum_{\chi} \sum_{\mathfrak{p}} (\deg \mathfrak{p})(\mathfrak{f}(\chi, \mathfrak{p})).$$

Proof: This formula follows directly from the Hurwitz genus formula once we show that $\deg(\prod_{\chi} f(\chi)) = \deg R$, where R is the ramification divisor of the associated cover of curves. If $Y \to X$ is the covering of curves corresponding to the extension L/K, then

$$\deg R = \sum_{Q} (\deg Q)(\ell((\Omega_{Y/X})_Q))$$

where the sum is taken over all points on Y, and $\ell((\Omega_{Y/X})_Q)$ is the length of the stalk at Q of the relative sheaf of Kähler differentials. We claim that $\deg R$ is equal to the degree of the different of the extension. Since both the different and the module of Kähler differentials commute with localisation and completion, we can prove this claim in the case of an extension of a complete discrete valuation ring. If $\mathfrak{P}$ is the prime of L lying over $\mathfrak{p}$, the prime of K, and B and A are the corresponding valuation rings of these primes, then ([12], p. 57) B can be written $B = A[X]/(f)$, where f is a monic polynomial. If $x = \bar{X}$, then dx generates $\Omega_{B/A}$ as a B-module and

$$(f'(x)) = \mathcal{D}_{B/A} = \mathrm{Ann}(\Omega_{B/A}).$$

If $\mathcal{D}_{B/A} = \mathfrak{P}^d$, then we write $d = \nu_{\mathfrak{P}}(\mathcal{D}_{L/K})$, and what we are trying to show is that $d = \ell_B(\Omega_{B/A})$. Since $\Omega_{B/A}$ is generated by one element, we have

$$\Omega_{B/A} \cong B/\mathrm{Ann}(\Omega_{B/A}).$$

So it follows that

$$\ell_B(\Omega_{B/A}) = \ell_B(B/\mathcal{D}_{B/A}) = \ell_B(B/\mathfrak{P}^d) = d.$$

Now this establishes the claim that $\deg R = \deg(\mathcal{D}_{L/K})$, since for each prime $\mathfrak{P}$ we have:

$$\nu_{\mathfrak{P}}(\mathcal{D}_{L/K}) = d = \ell_B(\Omega_{B/A}) = \text{ the coefficient of } \mathfrak{P} \text{ in } R.$$

We have the relation between the different and the discriminant of an extension: at each prime $\mathfrak{P}$ lying over $\mathfrak{p}$,

$$\nu_{\mathfrak{P}}(\mathcal{D}_{B/A}) = \frac{1}{f_{\mathfrak{p}}}\nu_{\mathfrak{p}}(N_{B/A}(\mathcal{D}_{B/A})) = \frac{1}{f_{\mathfrak{p}}}\nu_{\mathfrak{p}}(\mathfrak{d}_{B/A}),$$

where the $f_{\mathfrak{p}}$ in this formula denotes the residue degree at this prime. Applying the conductor-discriminant formula and noting that

$$\deg(\mathfrak{P})(\frac{1}{f_{\mathfrak{p}}}) = \deg(\mathfrak{p})$$

we can write

$$\deg R = \sum_{\chi}\sum_{\mathfrak{p}}(\deg \mathfrak{p})(\mathfrak{f}(\chi, \mathfrak{p})). \ \Box$$

As a simple example we compute the Artin conductors in the case $D = P_d$.

Lemma 3 *Let $D = P_d$. Then the Artin conductor of a non-trivial character χ of $G \cong U/U_D$, is equal to f, the residue degree of the extension.*

Proof: In this case, we have $e = |G| = (q^d - 1)/(q - 1)$. Since the order of G is prime to the characteristic, we have no wild ramification, or $G_1 = \{1\}$. Since no non-trivial element of G is in G_1, we have that $i_G(s) = 1$, for all $s \in G$, $s \neq 1$. To compute $\mathfrak{f}(\chi)$ we write:

$$\mathfrak{f}(\chi) = \frac{1}{e}(a_G(1)\chi(1) + \sum_{s\neq 1} a_G(s)\chi(s^{-1}))$$

$$= \frac{1}{e}(f(|G|-1) + \sum_{s\neq 1}(-f)\chi(s)).$$

This implies that $\mathfrak{f}(\chi) = 0$ if χ is the trivial character. If χ is not the trivial character, then we have $\sum_{s\in G}\chi(s) = 0$, so $\sum_{s\neq 1}\chi(s) = -\chi(1) = -1$. Substituting this in to the above formula for $\mathfrak{f}(\chi)$, we get

$$\mathfrak{f}(\chi) = \frac{1}{e}(f(|G|-1) + (-f)(-1)) = f \quad \square$$

Corollary 3 *The degree of the ramification divisor of an extension of degree n with conductor $D = P_d$ is $\deg R = (n-1)df$. If the extension is totally ramified at P_d, then the degree is $(n-1)d$.*

So far we have obtained an expression for the genus of an extension in terms of the conductors of the characters of the Galois group; in the next lemma we will express the genus purely in terms of the degrees of the extension and its subextensions. More precisely,

Lemma 4 *Let $K = \mathbb{F}_q(T)$, $D = kP_d$, $k > 1$. For each $1 \leq i \leq k$, let n_i be the degree of the extension obtained by splitting a fixed set of r places of degree one of the base when $D = iP_d$. Let L be the extension obtained when $i = k$. Then*

$$2g_L - 2 = (-2)n_k + \sum_{i=1}^{k}(n_i - n_{i-1})i$$

Proof: Ramification occurs at only one prime, so we can consider question locally. For any positive integers m, n, with $m < n$ we have the following exact sequence of groups:

$$0 \to U^m/U^n \to U/U^n \to U/U^m \to 0$$

Any character of U/U^m is also a character of U/U^n which happens to be trivial on U^m/U^n and which has conductor m. So it suffices to count the number of non-trivial characters for each $m \leq k$. $\square$

3.3 Examples

It may be useful to give some examples at this point, in order to see how to implement Lemmas 1, 2, and 4. The purpose of this section is to demonstrate the technique. Numerous examples were produced in [6], which contains tables for different choices of q, k, d, and number of places split.

Example 4 *Let $q = 4$, $D = kP_1$, $k = 4$. Then splitting all four of the other rational points of $K = \mathbb{F}_4(T)$, we obtain an extension of degree 2 in which the non-trivial character has conductor 4. This is the elliptic curve with the maximal number of points over $\mathbb{F}_4$: $g = 1$, $N = 9$; it is also the Hermtian curve for $q = 4$, which will be discussed in Section 4.*

Proof: If we choose P_1 to be the place corresponding to 0, or $T+0$, then the four places to be split are the place at infinity and $T+1$, $T+x$, $T+(x+1)$, where 0, 1, x, and $x+1$ are the elements of $\mathbb{F}_4$, and $x^2 = x+1$. If we choose the place at infinity to kill the infinite factor in the product $U/U_D \times \mathrm{Pic}(X)$, then it remains to determine the image of the other three elements in $(\mathbb{F}_4[T]/T^k)^*/\mathbb{F}_4^*$ for each $1 \leq k \leq 4$.

First note that if $J_k = (\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*$, then the order of J_k is q^{k-1}, and the order of an element of the form $1-\alpha T$ in J_k is p^l, where p is the characteristic and l is the smallest power of p such that $p^l \geq k$.

When $k=1$, J_k is already trivial. When $k=2$, J_k has order 4, and each element has order two, so quotienting by all three will leave the trivial group. When $k=3$, J_k has order 16, but each element has order 4, so we are again left with the trivial group. Finally, when $k=4$, J_k has order 64, and each element has order 4, but the second power of the third element is in the group generated by the other two:

$$(T+1)^2(T+x)^2 \equiv (T+(x+1))^2 \pmod{T^4}.$$

Thus the degree of the desired extension is 2. To compute the genus, we know that the only non-trivial character has conductor 4, so the genus formula gives us

$$2g-2 = (-2)2+4,$$

so $g=1$. Since one place is totally ramified and the other four places are totally split, the curve has 9 rational points, which meets the Hasse-Weil bound. When $q=4$, $\frac{\sqrt{q}(\sqrt{q}-1)}{2} = 1$, so this is the highest genus for which the Hasse-Weil bound can be met over $\mathbb{F}_4$.

Example 5 *Let $q=4$, $k=6$. Then splitting all four of the other rational points of $K = \mathbb{F}_q(T)$, we obtain an extension of degree 8 in which one character has conductor 4 and six characters have conductor 6. This extension corresponds to a curve of genus 13 with 33 points, which is the maximum possible according to the Oesterle bound, so $N_4(13) = 33$. This result was also obtained by van der Geer and van der Vlugt [16], who consider equations of Artin-Screier curves.*

Proof: We must first determine if there are any characters of conductor 5. When $k=5$, $|J_k| = 4^4$ and $l=3$, so each element has order no more than 8. We know that the quotient has order at least 2, since it contains the extension corresponding to $k=4$ as a subextension. In fact, the second power of the third element is again contained in the group generated by the other two:

$$(T-(x+1))^2 \equiv (T-1)^6(T-x)^6 \pmod{T^5}.$$

The order of the quotient by these three elements cannot be greater than two. If it were equal to 4, we would have a curve of genus 4 with 17 points, which is not possible according to the Oesterlé bounds. Since the degree of the extension did not increase from $k=4$ to $k=5$, there are no characters of conductor 5.

The order of J_6 is 4^5, and each element has order 8, but again the second power of the third element is in the group generated by the other two, since

$$(T+1)^6(T+x)^6 = (T+(x+1))^2 \pmod{T^6}.$$

Again we cannot have the degree of the extension in which all four points split be any bigger than 8 because if the degree were 16, we would have a curve of genus 29 with 65 points, which violates the bounds. The degree of the extension is 8, so we obtain a curve with $4*8+1=33$ rational points of genus

$$2g-2 = 8(-2)+4+36.$$

Example 6 *Let $q=4$, $k=7$. Then splitting all four of the other rational points of K, we obtain an extension of degree 16 in which one character has conductor 4, six characters have conductor 6, and eight characters have conductor 7. This gives a curve of genus 33 with 65 points. Since the Oesterle bound is 66 in this case (Corollary 1), we obtain: $N_4(33) = 65$ or 66. This was the first example found for this genus over $\mathbb{F}_4$. [6]*

Proof: $|J_7| = 4^6$, and the fourth power of the third element is in the subgroup generated by the other two, since

$$(T+1)^4(T+x)^4 = (x+1)T^4 + x \equiv T^4 + (x+1) = (T+(x+1))^4.$$

The extension has degree 16; if it had degree 32, we would have a genus 73 curve with 129 points, which is not possible. The genus is given by

$$2g-2 = (-2)16 + 4 + 6*6 + 8*7.$$

Since we have only five rational points on K, one of which is in the support of D, we cannot split more than four points. Splitting three points, we obtain at least one example of interest:

Example 7 *For $q=4$, $k=6$, we obtain the best known example of a curve of genus 27. It has 49 points and was also obtained by van der Geer and van der Vlugt [16] via their methods.*

Proof: The first non-trivial characters arise when $k=4$, and the degree is 4. The degree jumps again to 16 when $k=6$. This extension has $3*16+1=49$ rational points, and genus given by:

$$2g-2 = (-2)16 + 3*4 + 12*6.$$

Note: The examples in [16] can always be obtained via Serre's method by choosing the ramification and splitting the appropriate number of places of $\mathbb{F}_q(T)$ and then taking the quotient of the Galois group by the p-th powers. Thus their methods are limited in that they produce only covers of exponent p, which explains why they do not obtain curves of the type in Example 5.

4 Deligne-Lusztig Curves

To attack the problem of finding curves with many rational points compared to the genus Hansen and Stichtenoth focused on families of curves with large automorphism groups, in particular the family of groups giving rise to the Deligne-Lusztig varieties. The curves constructed from the Hermitian, Suzuki, and Ree groups are irreducible and have the maximal number of points for their genus. In this section, we give the ray class field descriptions of these three families.

The Deligne-Lusztig varieties were originally defined as a tool for constructing representations of connected reductive algebraic groups. Hansen introduces these varieties in [3] as follows: "Let G be a connected reductive algebraic group defined over $\mathbb{F}_q$ with Frobenius map $F : G \to G$. Let X_G be the $\mathbb{F}_q$-scheme of all Borel subgroups of G. For $w \in W$ in the Weyl group, define $X(w) \subset X_G$ to be the subscheme of all Borel subgroups B of G such that B and $F(B)$ are in relative position w. If $w = (s_1, ..., s_n)$ is a minimal expression for w, then $\overline{X}(s_1, ..., s_n)$ is the space of sequences such that $B_n = FB_0$ and B_{i-1} and B_i are in relative position e or s_i. The scheme $\overline{X}(s_1, ..., s_n)$ is of dimension n and it is a compactification of $X(w)$. The group of $\mathbb{F}_q$-rational points of $\overline{X}(s_1, ..., s_n)$ is $X(e)$ and the finite group G^F of Lie type acts as $\mathbb{F}_q$-rational automorphisms on $\overline{X}(s_1, ..., s_n)$, $X(w)$, and the $\mathbb{F}_q$-rational points $X(e)$." Much work was done to establish the properties of such varieties, including a criteria for irreducibility. The genus can be computed from the Euler characteristic. The variety constructed from a connected, reductive, algebraic group G is an irreducible variety of dimension one if and only if G is one of the following three groups: (i) G is the projective special unitary group ${}^2A_2(q^2)$; (ii) G is the Suzuki group ${}^2B_2(q)$, $q = 2^{2m+1}$, $m \in \mathbb{N}$; (iii) G is the Ree group ${}^2G_2(q)$, $q = 3^{2m+1}$, $m \in \mathbb{N}$.

4.1 Hermitian Curves

The study of the examples of conductor $k(P_1)$ in Section 3.3 above was motivated by the Hermitian curves, a family of maximal curves described by Stichtenoth. The Hermitian curves are of Artin-Schreier type, defined over fields of even-power order, and meet the Hasse-Weil bound for their genus. They have a large automorphism group and arise as the Deligne-Lusztig variety associated to the groups of type ${}^2A_2$. They are the unique maximal function fields of their genus, and no function field of higher genus can be maximal. Furthermore, Stichtenoth and Garcia [2] were able to use a modification of the equations for these curves to construct function field towers meeting the Drinfeld-Vladut bound over fields of even-power order. The Hermitan curves are characterized by Lemma 5:

Lemma 5 *Let $K = \mathbb{F}_{q^2}(y)$, $q = p^m$, and let L/K be the extension defined by the equation $x^q + x = y^{q+1}$. This extension has degree q, is totally ramified at ∞, totally split at all places of degree one, and has filtration of its ramification group at ∞ as follows:*

$$G = G_1 = G_2 = ... = G_{q+1}$$

$$G_{q+2} = \{1\}$$

This lemma is a special case of the following one, which is valid also for fields of odd-power-order:

Lemma 6 *Let $K = \mathbb{F}_{q^r}(y)$, and let L/K be the extension defined by the equation $x^{q^{r-1}} + ... + x^q + x = y^{q^{r-1}+...q+1}$, $r > 1$. This extension has degree q^{r-1}, is totally ramified at ∞, totally split at all places of degree one, and has filtration of its ramification groups as follows:*

$$G = G_1 = G_2 = ... = G_{q^{r-1}+...q+1}$$

$$G_{q^{r-1}+...q+2} = \{1\}$$

Proof: All but the calculation of the ramification groups is written down in [2], [14]. The preceeding lemma is the special case corresponding to $r = 2$.

To simplify notation, we set $n_r = q^{r-1} + q^{r-2} + ... + q + 1$. We need to show that $\nu_L(s(z) - z) = n_r + 1$, for all $s \in G$, $s \neq 1$, where z is a uniformizer at the place of L which lies over ∞. First we must determine z. Let $T = \frac{1}{y}$ denote a uniformizer at the place at ∞. Then $\nu_K(T) = 1$ and $\nu_L(T) = q^{r-1}$. From the equation defining the extension we deduce that

$$q^{r-1}\nu_L(x) = q^{r-1}\nu_L(y^{n_r})$$

which implies that

$$\nu_L(x) = -n_r.$$

Now since $(n_r, q^{r-1}) = 1$, there exist $a, b \in \mathbb{Z}$ such that $a(-n_r)+b(q^{r-1}) = 1$. Then $\nu_L(x^aT^b) = 1$ and we can set $z = x^aT^b$. Now for any $s \in G$, we must determine $\nu_L(s(x^aT^b) - x^aT^b)$. We have

$$\nu_L(s(x^aT^b) - x^aT^b) = \nu_L((s(x^aT^b) - x^aT^b)x^{-a}T^{-b}) - \nu_L(x^{-a}T^{-b})$$

$$= \nu_L((x+\beta)^aT^bx^{-a}T^{-b} - 1) + 1$$

where $\beta \in \mathbb{F}_{q^r}$ is an element whose trace in $\mathbb{F}_q$ is zero. Each $s \in G$ corresponds to such a β. Then

$$\nu_L(s(x^aT^b) - x^aT^b) = \nu_L(\frac{(x+\beta)^a - x^a}{x^a}) + 1$$

$$= \nu_L((x+\beta)^a - x^a) - \nu_L(x^a) + 1$$

We treat the cases $a < 0$ and $a > 0$ separately. First suppose $a > 0$. Then

$$\nu_L((x+\beta)^a - x^a) - \nu_L(x^a) + 1 = \nu_L(x^{a-1}\beta + x^{a-2}\beta^2 + ... + \beta^a) - \nu_L(x^a) + 1$$

$$= \nu_L(x^{a-1}\beta) - \nu_L(x^a) + 1$$

since $\nu_L(\beta) = 0$ and $\nu_L(x) < 0$, so

$$= \nu_L(x^{a-1}) + \nu_L(\beta) - \nu_L(x^a) + 1$$

$$= (a - 1 - a)\nu_L(x) + 1 = -\nu_L(x) + 1 = n_r + 1.$$

The case where $a < 0$ is similar:

$$\nu_L((x+\beta)^a - x^a) - \nu_L(x^a) + 1 = \nu_L(\frac{1 - (x+\beta)^{-a}x^a}{(x+\beta)^{-a}} - \nu_L(x^a) + 1$$

$$= \nu_L(1 - (x+\beta)^{-a}x^a) - \nu_L((x+\beta)^{-a}) - \nu_L(x^a) + 1$$

$$= \nu_L(x^1\beta + ... + x^a\beta^{-a}) + a\nu_L(x+\beta) - a\nu_L(x) + 1$$

Since $a < 0$, we have $\nu_L(x^{-1}) < \nu_L(x^a)$, so

$$= \nu_L(x^{-1}) + 1 = n_r + 1$$

Thus we conclude that $\nu_L(s(z) - z) = n_r + 1$ for all $s \in G$. $\square$

These curves will be referred to as trace-norm curves because of their definition. Note that the proof of Lemma 5 by itself would be much simpler because in that case we have: $a = -1$, $b = -1$. Lemma 5 will be needed to prove the following theorem, which gives the ray class field characterization of the Hermitian curves.

Theorem 2 *Let $K = \mathbb{F}_{q^2}(y)$, $D = (q+2)(\infty)$ Then the abelian extension of K obtained by splitting all other places of degree one of K has degree q. The corresponding curve is the Hermitian curve; it has genus $q(q-1)/2$ and the maximal number of points for this genus: $q^3 + 1$.*

Proof: Let L/K be the Hermitian curve defined by the Artin-Schreier-type equation above. To find D minimal s.t. $U_D \subset N(C_L)$, first note that from [14], we know that all places of K are unramified in L except ∞. As explained in Section 3.2 above, this implies that the conductor D is of the form $D = k(\infty)$, for some k. It remains to determine k. We conclude from the characterization of the ramification groups at ∞ in Lemma 5 that all characters have conductor $q+2$ and k must be $q+2$. This is due to the fact that the reciprocity map must be trivial on U_∞^{q+2} since it maps into G_{q+2}, which is trivial. No non-trivial character can have conductor less than $q+2$ or the genus would be too small. We claim that the quotient of C_K/U_D by the Frobenius at the q^2 places of degree one is isomorphic to the Galois group of L/K, $C_K/N(C_L)$, which has order q. In fact, we know that $U_D K^*_{\nu_1} K^*_{\nu_2} ... K^*_{\nu_{q^2}}$ is contained in $N(C_L)$, and if it were strictly smaller than $N(C_L)$, then we would have

$$|C_K/U_D K^*_{\nu_1} K^*_{\nu_2} ... K^*_{\nu_{q^2}}| = q * p^r, \quad r \geq 1,$$

which would lead to a contradiction to the fact that there are no maximal function fields over $\mathbb{F}_{q^2}$ of genus greater than $\frac{q(q-1)}{2}$, where "maximal" here means attaining the Weil bound. In fact, if the extension were of degree $q * p^r$, then the number of points would be $N = q^2(q * p^r) + 1$, and the genus would be $g = \frac{q(q*p^r-1)}{2}$. Over $\mathbb{F}_{q^2}$ the Weil bound for this genus is

$$N \leq q^2 + 1 + 2gq = q^2 + 1 + q^2(q * p^r - 1) = q^2(q * p^r) + 1.$$

Since our curve would meet this bound we must have $g \leq \frac{q(q-1)}{2}$, which implies $r = 0$. □

Corollary 4 *Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, q a power of a prime. Let $k = q + 2$. Then*

$$|(\mathbb{F}_{q^2}[T]/T^k)^*/\mathbb{F}_{q^2}^* / < 1 - \alpha T | \alpha \in \mathbb{F}_{q^2}^* > | = q.$$

Furthermore, this quotient is trivial if $k < q + 2$, in which case all polynomials split completely into factors of degree one.

Example 8 *When $q^2 = 4$, $k = 4$, we obtain the example of the elliptic curve with 9 points. The fact that the extension has degree* 2 *was determined in Section 2.3 above by computing the order of the quotient of* $(\mathbb{F}_4[T]/T^4)^*$ *by* $T+1$, $T+x$, *and* $T + x + 1$, *where* $0, 1, x, x+1$ *are the elements of* $\mathbb{F}_4$.

The computations for larger square fields would almost have to be done by computer, since it is necessary to split all q^2 points for each conductor up to $q+2$ and to determine the order of the quotient at each stage. The theorem, however, implies immediately that the degree of $(\mathbb{F}_{q^2}[T]/T^{q+2})^*/\mathbb{F}_{q^2}^*$ after quotienting by the other q^2 places is q.

The Hermitian curves are only maximal over fields of order an even power of a prime. When the order of the finite field is not a square the trace-norm curves are a natural generalisation. However, they are not maximal. Their ray class field descriptions can be determined using the computation of their ramification groups from Lemma 6 above. They arise from splitting all places of degree one when $D = (q^{r-1} + q^{r-2} + ... + q + 2)(\infty)$.

4.2 Suzuki Curves

It remains to determine the correct generalization of Hermitian curves to fields of odd-power-order in order to obtain families of curves meeting the Oesterle bounds. As a partial solution, in characteristics 2 and 3, we have the Suzuki and the Ree curves which are maximal for their genus. Their ray class field descriptions are remarkably similar to the description for the Hermitian curves. While the Hermitian curves are obtained by splitting all $q = p^{2m}$ points of the projective line with conductor $D = (p^m + 2)P_\infty$, the Suzuki curves and the first stage of the Ree curves are obtained by splitting all q points when $q = p^{2m+1}$ and $D = (p^{m+1} + 2)P_\infty$.

The Suzuki curves are the Deligne-Lusztig varieties constructed from the linear algebraic group ${}^2B_2$. They are defined over $\mathbb{F}_q$, where $q = 2^{2m+1}$, by the equation:

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

with $q_0 = 2^m$ [5]. They are irreducible of genus $q_0(q-1)$, having $1+q^2$ rational points, the maximum possible number for this genus according to the bounds from the explicit formulae. The fact that this is the maximum number possible is shown by chosing the trigonometric polynomial

$$f(\theta) = 1 + 2(\frac{\sqrt{2}}{2}\cos(\theta) + \frac{1}{4}\cos(2\theta)).$$

Theorem 3 *Let $K = \mathbb{F}_q(x)$, $D = (p^{m+1}+2)(\infty)$, where $q = 2^{2m+1}$. Then the abelian extension of K obtained by splitting all q other places of degree one of K inside the ray class field of conductor D has degree q. This is a curve of genus $q_0(q-1)$ having the maximal number of points for this genus: q^2+1.*

Proof: This proof is similar to the proof for the Hermitian curves. We use an analog of Lemma 5 which was calculated by Hansen and Stichtenoth in [5].

Lemma 7 *Let $K = \mathbb{F}_q(x)$, $q = 2^{2m+1}$, and let L/K be the extension defined by the equation $y^q - y = x^{q_0}(x^q - x)$, $\quad q_0 = 2^m$. This extension has degree q, is totally ramified at ∞, totally split at all places of degree one, and has filtration of its ramification group at ∞ as follows:*

$$G = G_1 = G_2 = \ldots = G_{2q_0+1},$$

$$G_{2q_0+2} = \{1\}.$$

Let L/K be the extension defined by this equation. It is an abelian extension, and we need to find D minimal s.t. $U_D \subset N(C_L)$ We know from the lemma that the only ramification occurs at ∞, so the coefficient which is minimal at all other places is zero and $D = k(\infty)$. To determine k, we conclude from the characterization of the ramification groups that all characters have conductor $2^{m+1}+2$, so $k = 2^{m+1}+2$. We claim that the quotient of C_K/U_D by the q places of degree one is isomorphic to the Galois group of the extension, $C_K/N(C_L)$, which has order q. We know that $U_D K^*_{\nu_1} K^*_{\nu_2} \ldots K^*_{\nu_q}$ is contained in $N(C_L)$. If the two were not equal, we would again have an extension whose genus and number of points would contradict the known bounds. Indeed, suppose the order of the extension were $q2^s$, $s \geq 1$. Then we would have an extension with $N = q^2 2^s + 1$ points, of genus no greater than $g \leq q_0(q2^s - 1)$. (If all non-trivial characters had conductor k we would have equality; if some conductors were less than k, the genus would be smaller.) Now we can show that this is impossible by using the polynomial f which was chosen to show the maximality of the Suzuki curves,

$$f(\theta) = 1 + 2(\frac{\sqrt{2}}{2}\cos(\theta) + \frac{1}{4}\cos(2\theta))$$

The bound we obtain from this choice is a line with slope

$$\frac{4q}{2\sqrt{2q}+1}$$

and intercept

$$\frac{2q\sqrt{2q}+q^2}{2\sqrt{2q}+1}+1$$

so it follows that for $q = 2^{2m+1}$, $g \leq q_0(q2^s - 1)$, and $s \geq 1$, we must have $N < q^2 2^s + 1$. $\Box$

Corollary 5 *Let $\mathbb{F}_q$ be the finite field with $q = 2^{2m+1} = 2q_0^2$ elements. Let $k = 2q_0 + 2$. Then*

$$|(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*/ < 1 - \alpha T | \alpha \in \mathbb{F}_q^* > | = q$$

Furthermore, this quotient is trivial if $k < 2q_0 + 2$, in which case all polynomials split completely into factors of degree one.

Example 9 *When $q = 8$, $q_0 = 2$, we have the degree 8 cover of $\mathbb{P}^1$ in the ray class field of conductor $D = 6(\infty)$ in which all 8 points are split. The curve is of genus 14 with 65 rational points.*

4.3 Ree Curves

The Deligne-Lusztig varieties arising from the Ree group ${}^2G_2(q)$ when $q = 3^{2m+1}$ are irreducible curves defined over $\mathbb{F}_q$. They can be viewed as abelian covers of $\mathbb{P}^1$ of degree q^2. They have genus

$$g = \frac{3}{2}q_0(q-1)(q+q_0+1),$$

where $q_0 = 3^m$, and $q^3 + 1$ rational points, which is maximal for this genus [3]. The trigonometric polynomial which is chosen to show that this is maximal is

$$f(\theta) = 1 + 2\sum c_n \cos(n\theta),$$

where

$$c_1 = \frac{\sqrt{3}}{2}, c_2 = \frac{7}{12}, c_3 = \frac{\sqrt{3}}{6}, c_4 = \frac{1}{12}, \quad c_i = 0, \quad i > 4.$$

Based on our findings in the previous two cases, we might expect that the Ree curve be obtained when splitting all q points in the ray class field of conductor $D = (3^{m+1} + 2)(\infty)$ over $\mathbb{P}^1$. In the previous cases, however, we obtained an extension of $\mathbb{P}^1$ of degree q from this process, and what we need here is an extension of degree q^2. In fact, Pedersen [10] determined the equations for the function field corresponding to the Ree curve: $F = \mathbb{F}_q(x, y_1, y_2)$, with equations

$$y_1^q - y_1 = x^{q_0}(x^q - x)$$

and

$$y_2^q - y_2 = x^{q_0}(y_1^q - y_1).$$

We refer to $F_1 = \mathbb{F}_q(x, y_1)$, as defined by the first equation, as the first stage of the Ree function field. It is a cover of $\mathbb{P}^1$ of degree q and genus

$$g = \frac{3}{2}q_0(q-1).$$

From the work of Hansen and Pedersen [4], we can extract the following lemma, changing the notation to agree with [12].

Lemma 8 *If F is the function field of the Ree curve as defined in the paragraph above, then the filtration of its ramification group at ∞ is as follows:*

$$G_0 = G_1 = G_2 = \ldots = G_{3q_0+1},$$

$$G_{3q_0+2} = \ldots = G_{q+3q_0+1},$$

$$G_{q+3q_0+2} = \{1\},$$

$$|G_0| = q^2 \text{ and } |G_{3q_0+2}| = q.$$

Lemma 8 leads us to the following characterization of F as an abelian cover of $\mathbb{P}^1$ of degree q^2.

Theorem 4 *Let $K = \mathbb{F}_q(x)$, $D = (3^{m+1}+3)(\infty)$, where $q = 3^{2m+1}$. Then the abelian extension of K obtained by splitting all q other places of degree one of K inside the ray class field of conductor D has degree q^2. This is a curve of genus*

$$g = \frac{3}{2}q_0(q-1)(q+q_0+1)$$

having the maximal number of points for this genus: q^3+1.

Proof: This proof is similar to the proof for the Hermitian and Suzuki curves. As in those cases, we show that the Ree curve must have the stated description as a ray class field. Let $G = \mathrm{Gal}(F/K)$, $H = \mathrm{Gal}(F/F_1) < G$. Then $G/H = \mathrm{Gal}(F_1/K)$. Actually, the subgroup G_{3q_0+2} has F_1 as its fixed field, so $G = G_0$, and $H = G_{3q_0+2}$. We need an argument to show that the characters of G have Artin conductor at most $3q_0+3$. We use the formula for the transitivity of the discriminant:

Proposition 2 (Transitivity of the discriminant)

$$\mathfrak{d}_{F/K} = (\mathfrak{d}_{F_1/K})^{[F:F_1]} N_{F_1/K}(\mathfrak{d}_{F/F_1})$$

Applying the conductor discriminant formula, we get the relation

$$\prod_{\chi\in\hat{G}} f(\chi) = (\prod_{\chi\in\widehat{G}/H} f(\chi))^{[F:F_1]} N_{F_1/F}(\prod_{\chi\in\hat{H}} f(\chi))$$

For $\chi \in \widehat{G/H}$, $\chi \neq 1$, we know that $f(\chi) = 3q_0 + 2$, and each character of G/H is also a character of G of the same conductor. We also know that $|H| = [F : F_1] = q$, and that all the non-trivial characters of H have conductor $q + 3q_0 + 2$. Putting this information in to the last formula, we see that the other $q^2 - q$ characters of G cannot have conductor greater than $3q_0 + 3$, or the left hand side would be greater than the right hand side. The formula becomes:

$$(q-1)(3q_0+2) + (q^2-q)(3q_0+3) = q(q-1)(3q_0+2) + (q-1)(q+3q_0+2)$$

Next we need to show that the degree of the ray class field extension with this splitting and ramification cannot be greater than q^2, the degree of the Ree extension. This is achieved again by means of the polynomial which was chosen to show that the Ree curves are maximal.

$$f(\theta) = 1 + 2(\frac{\sqrt{3}}{2}\cos(\theta) + \frac{7}{12}\cos(2\theta) + \frac{\sqrt{3}}{6}\cos(3\theta) + \frac{1}{12}\cos(4\theta))$$

so in this case

$$\Psi_1(q^{-\frac{1}{2}}) = \frac{18qq_0 + 7q + 6q_0 + 1}{12q^2}$$

$$\Psi_1(q^{\frac{1}{2}}) = \frac{1}{12}(18q_0 + 7q + 6qq_0 + q^2)$$

and

$$N \leq \frac{g}{\Psi_1(q^{-\frac{1}{2}})} + \frac{\Psi_1(q^{\frac{1}{2}})}{\Psi_1(q^{-\frac{1}{2}})} + 1$$

Suppose that the degree of the extension is equal to $q^2 3^r$, $r \geq 1$. Still we have only $q-1$ characters of conductor $3q_0 + 2$, and the other $q^2 3^r - q$ must have conductor $3q_0 + 3$. So the genus is determined by:

$$2g - 2 = (-2)q^2 3^r + (q-1)(3q_0+2) + (q^2 3^r - q)(3q_0+3)$$

or

$$2g = (q^2 3^r - 1)(3q_0 + 1) - (q - 1)$$

Then we must have:

$$N \leq \frac{\frac{1}{2}[(q^2 3^r - 1)(3q_0+1) - (q-1)]12q^2 + q^2(18q_0 + 7q + 6qq_0 + q^2)}{18qq_0 + 7q + 6q_0 + 1} + 1$$

$$1 + q^3(\frac{18qq_0 3^r + (6p^r + 1)q + 6q_0 + 1}{18qq_0 + 7q + 6q_0 + 1}$$

But the number of points on the curve is $1 + q^3 3^r$, which does not satisfy this inequality unless $r = 0$. $\square$

This completes the ray class field descriptions of the Deligne-Lusztig curves and thus the proof of the main theorem of the paper as stated in the introduction. It should be noted that we used only the existence, not the uniqueness of the Hermitian, Suzuki, and Ree curves (as discussed in [4]). The uniformity of the descriptions indicates that it would be interesting to study the correspondance between the Deligne-Lusztig construction of these varieties and the ramification structure of their equations as covers of $\mathbb{P}^1$. It is natural to ask whether we can obtain further families of maximal curves via the Deligne-Lusztig construction from some of the other connected, reductive, algebraic groups. None of them give rise to irreducible curves, but the irreducible components could be studied. Finally, the ray class field description of these curves lends itself to generalization in other characteristics, which may produce other families of maximal curves.

References

[1] R. Fuhrmann and F. Torres, *A note on the genus of certain curves over finite fields*, to appear.

[2] A. Garcia and H. Stichtenoth, *A Tower of Artin-Schreier Extensions of Function Fields Attaining the Drinfeld-Vladut Bound*, Inv. Math. **121** (1995), p.211-222.

[3] J. P. Hansen, *Deligne-Lusztig Varieties and Group Codes*, Proceedings from the Conference at Luminy, 1991, p.63-81.

[4] J. P. Hansen and Jens Peter Pedersen, *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields*, J. reine angew. Math. **440** (1993), 99-109.

[5] J. P. Hansen and H. Stichtenoth, *Group Codes on Algebraic Curves Associated to the Sylow-2-Subgroups of the Suzuki Groups*, Preprint Series, Matematisk Institut, Aarhus Universitet, 1988/89, No. 7.

[6] K. Lauter, *Ray class field constructions of curves over finite fields with many rational points*, in Algorithmic Number Theory (ed. by H. Cohen), Lecture Notes in Computer Science 1122, p.187-195. Springer, Berlin 1996.

[7] K. Lauter, *Ray class field constructions of curves over finite fields with many rational points*, PhD Dissertation, University of Chicago, June 1996.

[8] H. Niederreiter and C. Xing, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C.R. Acad. Sc. Paris Sér. I Math.322 (1996), 651-654.

[9] H. Niederreiter and C. Xing, *Algebraic curves over finite fields with many rational points*, submitted to Proc. Number Theory Conf. (Eger, 1996), de Gruyter, Berlin.

[10] J. P. Pedersen, *A Function Field Related to the Ree Group*, Proceedings from Conference at Luminy, 1991, p.122-131.

[11] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*, C.R. Acad. Sc. Paris, t. 296, (7 mars 1983).

[12] J.-P. Serre, *Local Fields*, Springer-Verlag New York Inc., 1979.

[13] R. Schoof, *Algebraic curves and coding theory*, UTM 336, Univ. of Trento, 1990.

[14] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer, Berlin-Heidelberg-New York 1993.

[15] C. Xing and H. Stichtenoth, *The Genus of Maximal Function Fields over Finite Fields*, manuscripta math. 86, 217-224 (1995).

[16] G. van der Geer and M. van der Vlugt, *How to Construct Curves over Finite Fields with Many Points*, to appear.