manuscripta math. 98, 87 – 96 (1999)

Kristin Lauter

Deligne–Lusztig curves as ray class fields

Received: 9 July 1998

Abstract. We give ray class field descriptions of the function fields of the Hermitian, Suzuki and Ree curves.

1. Introduction

In this paper we prove that the three families of irreducible Deligne–Lusztig curves all arise from almost the same choice of parameters via Serre's method ([11], [10], [5]) for using class field theory to construct curves over finite fields with many rational points. This serves the dual purpose of (1) highlighting the utility of Serre's method by giving examples of optimal families of curves which arise naturally from it, and (2) emphasizing the underlying similarity of the ramification filtration of the Deligne–Lusztig curves when realized as covers of the projective line. Thus the possible consequences of this work are also two-fold: it points the way to generalizations via class field theory to produce other optimal families of curves (see [7]), and it suggests that we investigate further the ramification structure of the Deligne–Lusztig varieties when considered as covers.

The main theorem of this paper is as follows.

Theorem 1. *The function fields of the Hermitian, Suzuki, and Ree curves are isomorphic to the largest ray class fields of conductor $D = k(\infty)$ in which all places of degree one different from (∞) of $\mathbb{F}_q(x)$ split completely, where*

$$k = \begin{cases} p^{\lceil f/2 \rceil} + 2 \text{ if } q = p^f \text{ is a square or } p = 2 \\ p^{\lceil f/2 \rceil} + 3 \text{ if } q = p^f \text{ is not a square and } p = 3. \end{cases}$$

(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).)

K. Lauter: Department of Mathematics, University of Michigan,
Ann Arbor, MI 48109-1109, USA. e-mail: klauter@math.lsa.umich.edu

Mathematics Subject Classification (1991): 11R37, 20G40, 11R58

From this theorem, we derive interesting results on the interdependence of the decomposition groups at different primes in the extension. This interdependence is expressed by the formula for the order of the Galois groups:

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

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

2. Hermitian curves

Let K be a finite field whose order is a square: $|K| = q^2$. Consider the function field $F = K(x, y)$ with the defining equation

$$y^q + y = x^{q+1}. \tag{1}$$

These fields are the "Hermitian" function fields which were discovered by Leopoldt in the course of his study of the automorphism group of Fermat function fields, and which are characterized in Stichtenoth's thesis [13]. They have a large automorphism group and arise as the Deligne–Lusztig variety associated to the groups of type ${}^2A_2$ (see [1], for example). They are the unique maximal function fields of their genus [9], and later we will need that no function field of higher genus can be maximal [4].

We consider F as an extension of the rational function field $K(x)$. The following facts are well known and can be found in [14].

Fact 1. The field degree is $[F : K(x)] = q$.
Fact 2. The place $x \to \infty$ is the only place of $K(x)$ which is ramified in F. Its ramification degree is q, i.e., it is *totally ramified* in F.
Fact 3. The genus of F is $g = q(q-1)/2$ and the number of rational places is q^3+1, so F is (Hasse-Weil) maximal.
Fact 4. Every finite rational place $x \to a$ with $a \in K$ splits completely in F; its q extensions are given by $(x, y) \to (a, b)$ with $b^q + b = a^{q+1}$.
Fact 5. $F|K(x)$ is abelian; its Galois group G is given by the substitutions $y \to y + b$ with $b^q + b = 0$.

We add the following statement. Let (∞) denote the prime divisor of $K(x)$ corresponding to the place $x \to \infty$.

Fact 6. The conductor of the abelian extension $F|K(x)$ is $\mathfrak{f} = (q+2)\cdot(\infty)$.

Proof. According to Fact 2, the conductor is a multiple of (∞), i.e., $\mathfrak{f} = k \cdot (\infty)$ for some positive integer k. We recall the ramification theory of abelian fields where it is shown how the conductor multiplicity k is computed from the orders of the ramification groups. Let $\mathfrak{p}_\infty$ denote the unique extension of $x \to \infty$ to F, and let $v = v_{\mathfrak{p}_\infty}$ denote its valuation on F. Let us choose a uniformizing element t for $\mathfrak{p}_\infty$, i.e., $v(t) = 1$. Then the i-th ramification group G_i $(i > 0)$ consists of all automorphisms $\sigma \in G$ for which

$$v(t^{\sigma-1} - 1) \geq i\ ,$$

Let $g_i = |G_i|$. Let r denote the largest integer such that $g_r \neq 1$. Then it is known that

$$k = 1 + \frac{1}{g}(g_1 + g_2 + \cdots + g_r) \tag{2}$$

where $g = |G| = q$. So we have to compute the g_i.

From Fact 2 we see that $v(x) = -q$, and so from the defining equation (1) we have $v(y) = -(q+1)$. Hence we can take $t = xy^{-1}$. Fact 5 shows that $t^{\sigma-1} = y^{1-\sigma} = y(y+b)^{-1} = 1 + (-b)(y+b)^{-1}$ and thus if $\sigma \neq 1$, i.e., $b \neq 0$:

$$v(t^{\sigma-1} - 1) = v((-b)(y+b)^{-1}) = -v(y+b) = q + 1\,.$$

Hence, every $\sigma \neq 1$ is contained in G_{q+1} but not in G_{q+2} and therefore

$$G = G_1 = \cdots = G_{q+1} \neq G_{q+2} = 1\,.$$

We see: $r = q + 1$ and $g_i = |G| = q$ for $1 \leq i \leq r$. Now (2) shows $k = 1 + r = q + 2$. □

The main theorem for Hermitian fields is the following:

Theorem 2. *F can be characterized as the largest abelian extension of $K(x)$ which has conductor $(q+2)\cdot(\infty)$, and in which all finite places $x \to a$ $(a \in K)$ split completely.*

Proof. Let F' be the largest extension of $K(x)$ with the properties as announced. Then $F \subset F'$. Let $[F' : F] = m$, so that $[F' : K(x)] = mq$. We claim $m = 1$.

Let us count the number N' of K-rational places of F'. In $K(x)$ there are q^2 finite K-rational places $x \to a$ with $a \in K$. Every one of them splits completely in F' which gives a total of $mq \cdot q^2$ K-rational places of F'.

In particular, we see that K is algebraically closed in F' (since otherwise there would not exist K-rational places of F'). In other words: F' is a *regular* field extension of K.

Now consider the infinite place $x \to \infty$. It is *the only place of $K(x)$ which is ramified in F'*, because the conductor of $F'|K(x)$ is a multiple of (∞). We claim that $x \to \infty$ is *totally ramified* in F'. To see this, let us denote by $\mathfrak{p}'_\infty$ an arbitrary extension of $x \to \infty$ to F'. Let T denote its inertia field. Then $T|K(x)$ is unramified with respect to the place induced by $\mathfrak{p}'_\infty$. Now, since $F'|K(x)$ and hence $T|K(x)$ is an *abelian* extension, it follows that $T|K(x)$ is unramified with respect to *every* place extending $x \to \infty$. In other words, $x \to \infty$ is unramified in T. But every other place of $K(x)$ is unramified in T too (because it is unramified in F'). Hence T is an unramified field extension of $K(x)$. Now, there do not exist unramified proper extensions of $K(x)$ which are regular over K. Thus $T = K(x)$ which shows that $x \to \infty$ is indeed totally ramified in F'.

This implies in particular that $\mathfrak{p}'_\infty$ is the only place of F' above $x \to \infty$, and that it is of degree 1, i.e., it is a K-rational place of F'. Hence, besides the $mq \cdot q^2$ K-rational places which we have found already, there is precisely one more above $x \to \infty$. Hence

$$N' = 1 + mq \cdot q^2.$$

Using the Hasse–Weil estimate:

$$N' - q^2 - 1 \leq 2g'q \tag{3}$$

we obtain the estimate:

$$q(mq - 1) \leq 2g'. \tag{4}$$

An estimate in the other direction is obtained as follows. The Riemann–Hurwitz genus formula for $F'|K(x)$ gives

$$2g' = -2(mq - 1) + d' \tag{5}$$

where d' is the degree of the discriminant $\mathfrak{d}'$ of $F'|K(x)$. Since the conductor of $F'|K(x)$ is a multiple of the place (∞), the same holds for the discriminant, i.e., $\mathfrak{d}' = d' \cdot (\infty)$. Now we use the conductor-discriminant formula which shows that $\mathfrak{d}'$ admits a decomposition of the form

$$\mathfrak{d}' = \sum_{\chi} \mathfrak{f}(\chi)$$

where χ ranges over the characters of the Galois group of $F'|K(x)$ and $\mathfrak{f}(\chi)$ is the corresponding conductor via class field theory. If we write $\mathfrak{f}(\chi) = f(\chi) \cdot (\infty)$ we obtain

$$d' = \sum_{\chi} f(\chi).$$

Since $F'|K(x)$ is supposed to have the conductor $(q+2)\cdot(\infty)$, we conclude that $f(\chi) \leq q+2$ for all $\chi \neq 1$; for the trivial character $\chi = 1$ we have of course $f(1) = 0$. It follows $d' \leq (mq-1)(q+2)$ and therefore in view of the Riemann–Hurwitz formula (5):

$$2g' \leq -2(mq-1) + (mq-1)(q+2) = q(mq-1)\,.$$

Comparing with (4) we conclude

$$2g' = q(mq-1)\,. \tag{6}$$

At the same time we see that equality holds not only in (4) but also in (3):

$$N' - (q^2+1) = 2g'q\,.$$

This means that the number of rational places of $F'|K$ meets the maximal bound as permitted by the Hasse–Weil estimate. In other words: F' is a *maximal* function field.

Now, Ihara [4] has proved that every maximal function field over the field with q^2 elements has genus $g' \leq q(q-1)/2 = g$. Comparison with (6) gives $m = 1$. □

Corollary 2. *Let $k = q+2$, K as above. Then*

$$|(K[T]/T^k)^*/K^*/\langle 1-\alpha T|\alpha \in K^*\rangle| = q.$$

Furthermore, this quotient is trivial if $k < q+2$.

Proof. Via class field theory, this quotient is exactly the Galois group of $F|K(x)$, and thus it has order q. The second statement follows from the fact proved above that all non-trivial characters χ of G satisfy $f(\chi) = q+2$. □

3. Suzuki curves

The Suzuki curves are the Deligne–Lusztig varieties constructed from the linear algebraic group ${}^2B_2$ ([1]). Let $K = \mathbb{F}_q$, where $q = 2^{2m+1}$. Then the Suzuki curve is the curve associated to the function field $F = K(x,y)$ with defining equation:

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

with $q_0 = 2^m$. We consider F as an extension of the rational function field $K(x)$ and again we have the following well-known facts: ([3])

Fact 1. The field degree is $[F : K(x)] = q$.

Fact 2. The place $x \to \infty$ is the only place of $K(x)$ which is ramified in F. Its ramification degree is q, i.e., it is *totally ramified* in F.

Fact 3. The genus of F is $g = q_0(q-1)$ and the number of rational places is q^2+1. F has the maximum possible number of rational places for its genus. This is shown by choosing the trigonometric polynomial

$$h_1(\theta) = 1 + 2(\frac{\sqrt{2}}{2}\cos(\theta) + \frac{1}{4}\cos(2\theta)),$$

to obtain a bound on the number of places from the explicit formulae method. This method for obtaining bounds from different choices of trigonometric polynomials is described in [11], [10], or [1].

Fact 4. Every finite rational place $x \to a$ with $a \in K$ splits completely in F.

Fact 5. $F|K(x)$ is abelian; its Galois group G is given by the substitutions $y \to y + \alpha$ with $\alpha \in K$.

Fact 6. The conductor of the abelian extension $F|K(x)$ is $\mathfrak{f} = (2q_0+2)\cdot(\infty)$.

Proof. We apply the same argument as for the Hermitian case above, using the fact proved in [3] that the ramification groups are as follows:

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

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

The main theorem for the function fields of the Suzuki curves is then:

Theorem 3. *F can be characterized as the largest abelian extension of $K(x)$ which has conductor $(2q_0+2)\cdot(\infty)$, and in which all finite places $x \to a$ $(a \in K)$ split completely.*

Proof. Again let F' be the largest extension of $K(x)$ with the properties as announced. Then $F \subset F'$. Let $[F' : F] = m$, so that $[F' : K(x)] = mq$. We claim $m = 1$. By the same argument as in the Hermitian case, F' has $N' = q^2 \cdot m + 1$ rational places. Now we carry through that argument except that in this case, we use the method of explicit formulae to obtain a bound on N' in terms of g', the genus of F. Using the trigonometric polynomial h_1 given above, we find that

$$N' \le \alpha \cdot g' + \beta, \tag{7}$$

where

$$\alpha = \frac{4q}{4q_0+1}, \qquad \beta = \frac{4q_0q + q^2}{4q_0+1} + 1.$$

Formula (5) for the genus, combined with the estimate $f(\chi) \le 2q_0 + 2$ for all non-trivial characters of the Galois group of $F'|K(x)$ lead to the following upper bounds:

$$d' \le (mq-1)(2q_0+2),$$

and therefore

$$g' \le q_0(mq - 1)\,.$$

So formula (7) becomes:

$$q^2 \cdot m + 1 \le q^2 \cdot \frac{4q_0 m + 1}{4q_0 + 1} + 1,$$

which can happen only if $m \le 1$. □

Corollary 3. *Let $K = \mathbb{F}_q$ be the finite field with $q = 2^{2m+1} = 2q_0^2$ elements. Let $k = 2q_0 + 2$. Then*

$$|(K[T]/T^k)^*/K^*/\langle 1 - \alpha T | \alpha \in K^* \rangle| = q.$$

Furthermore, this quotient is trivial if $k < 2q_0 + 2$.

4. Ree curves

The Deligne–Lusztig varieties arising from the Ree group ${}^2G_2(q)$ when $q = 3^{2m+1}$ are irreducible curves defined over $\mathbb{F}_q$. Let $K = \mathbb{F}_q$, where $q = 3^{2m+1}$. Then the Ree curve is the curve associated to the function field $F = K(x, y_1, y_2)$ with defining equations:

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

and

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

with $q_0 = 3^m$. We consider F as an extension of the rational function field $K(x)$ and again we have the following well-known facts: ([2], [8])

Fact 1. The field degree is $[F : K(x)] = q^2$.

Fact 2. The place $x \to \infty$ is the only place of $K(x)$ which is ramified in F. Its ramification degree is q^2, i.e., it is *totally ramified* in F.

Fact 3. The genus of F is $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$, and the number of rational places is $q^3 + 1$. F has the maximum possible number of rational places for its genus. The trigonometric polynomial which is chosen to show that the Ree curves are maximal is

$$h_2(\theta) = 1 + 2\sum c_n \cos(n\theta),$$

where

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

Fact 4. Every finite rational place $x \to a$ with $a \in K$ splits completely in F.

Fact 5. The Galois group of $F|K(x)$ is abelian; it is a subgroup of the full Ree group.

Fact 6. The conductor of the abelian extension $F|K(x)$ is $\mathfrak{f} = (3q_0+3)\cdot(\infty)$.

Proof. From the work of Hansen and Pedersen [2], we can extract the following lemma, changing their notation to agree with [12] and to be consistent with the notation in this paper.

Lemma 1. *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:*

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

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

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

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

Applying Lemma 1 to calculate k in formula (2) yields:

$$k = 1 + \frac{1}{q^2}((3q_0+1)q^2 + q \cdot q) = 3q_0 + 3,$$

which is the desired result. □

The main theorem for the function fields of the Ree curves is then:

Theorem 4. *F can be characterized as the largest abelian extension of $K(x)$ which has conductor $(3q_0+3)\cdot(\infty)$, and in which all finite places $x \to a$ $(a \in K)$ split completely.*

Proof. As before, we need only show that $m = 1$, where $m = [F' : F]$ and F' is the largest extension of $K(x)$ with the properties as announced. Again we observe that F' has $N' = q^3 \cdot m + 1$ rational places. In this case we use the trigonometric polynomial h_2 to get a bound on N' in terms of the genus of F'. As in formula (7) above, the bound can be written as

$$N' \leq \alpha \cdot g' + \beta,$$

where

$$\alpha = \frac{12q^2}{18qq_0 + 7q + 6q_0 + 1}, \qquad \beta = \frac{q^2(18q_0 + 7q + 6qq_0 + q^2)}{18qq_0 + 7q + 6q_0 + 1} + 1.$$

The Riemann–Hurwitz genus formula takes the form

$$2g' = -2(mq^2 - 1) + d',$$

so an upper bound on g' can be obtained by analyzing

$$d' = \sum_{\chi} f(\chi)$$

as follows. Since F is a subextension of F', characters of the Galois group of $F|K(x)$ have the same Artin conductor when considered as characters of G, the Galois group of $F'|K(x)$ ([12], p. 101). Thus, there are at least $(q-1)$ characters χ of G with $f(\chi) \leq (3q_0+2)$. By assumption, the remaining characters satisfy $f(\chi) \leq (3q_0+3)$. So

$$d' \leq (q^2m - q)(3q_0+3) + (q-1)(3q_0+2),$$

which leads to the upper bound

$$2g' \leq (3q_0+1)(q^2m-1) - (q-1).$$

Now the upper bound on N' becomes:

$$\begin{aligned} N' &\leq \frac{\frac{1}{2}[(q^2m-1)(3q_0+1)-(q-1)]12q^2+q^2(18q_0+7q+6qq_0+q^2)}{18qq_0+7q+6q_0+1}+1 \\ &= 1+q^3\Big(\frac{18qq_0m+(6m+1)q+6q_0+1}{18qq_0+7q+6q_0+1}\Big), \end{aligned}$$

but the number of rational places of F' is $1+q^3m$, which does not satisfy this inequality unless $m \leq 1$. □

Corollary 4. *Let K be the finite field with $q = 3^{2m+1} = 3q_0^2$ elements. Let $k = 3q_0+3$. Then*

$$|(K[T]/T^k)^*/K^*/\langle 1-\alpha T | \alpha \in K^* \rangle| = q^2.$$

Furthermore, this quotient is trivial if $k < 3q_0+2$.

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 [9] and [2]). The uniformity of the descriptions indicates that it would be interesting to study the correspondence between the Deligne–Lusztig construction of these varieties and the ramification structure of their equations as covers of $\mathbb{P}^1$. Also, the ray class field description of these curves lends itself to generalization in other characteristics, for which it is necessary to have an analog of the corollary stated in the introduction which is valid when q is not a square and the characteristic is not equal to 2 or 3. The reader can verify directly that computing the order of the quotients appearing in the statement of the corollaries is a non-trivial matter which is greatly facilitated here by the use of the existence of the Deligne–Lusztig curves. A general solution for the order of such quotients for any q and k is presented in [7] using direct methods.

Acknowledgements. This paper comprises some of my dissertation work, and I would like to thank my advisor, Niels Nygaard for his support, Rene Schoof for his suggestions, and the referee for significant help in rewriting this paper.

References

[1] Hansen, J.P.: *Deligne–Lusztig Varieties and Group Codes*. In: Lecture Notes in Mathematics **1518**, Coding Theory and Algebraic Geometry, Proceedings, Luminy, 1991, p. 63–81

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

[3] Hansen, J.P. and Stichtenoth, H.: 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. In: Appl. Algebra Engrg. Comm. Comput. **1** no. 1, 67–77 (1990)

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

[5] Lauter, K.: 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**, Berlin: Springer, 1996, pp. 187–195

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

[7] Lauter, K.: A formula for constructing curves over finite fields with many rational points. Max Planck Institut Preprint 97–64, to appear in J. Number Theory

[8] Pedersen, J.P.: A Function Field Related to the Ree Group. In: *Lecture Notes in Mathematics* **1518***, Coding Theory and Algebraic Geometry, Proceedings, Luminy, 1991*, pp. 122–131

[9] Rück, H.-G. and Stichtenoth, H.: A characterization of Hermitian function fields over finite fields. J. reine angew. Math. **457**, 185–188 (1994)

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

[11] Serre, J.-P.: Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. C.R. Acad. Sc. Paris Sér. I Math. **296**, 397–402 (1983)

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

[13] Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. Arch. Math. Vol. **24**, 527–544 (1973)

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