A formula for constructing curves over finite fields with many rational points

Kristin Lauter

lauter@mpim-bonn.mpg.de

1 Introduction

Over the past fifteen years, mathematicians have been drawn to the problem of constructing curves over finite fields that have many rational points, largely because such curves have been shown to have important applications but also because the construction of such curves is theoretically challenging. The challenge lies in meeting the bounds on the number of points given by Oesterlé's optimization of Weil's explicit formulae. In this paper we prove a formula that can be used to construct curves that come close to these bounds.

In 1983, Serre indicated his method for using class field theory to construct curves over $\mathbb{F}_2$ with many rational points [8]. Since then, class field theory has been responsible for much of the progress on this problem: even families which were found via other methods can be described using Serre's approach, thus unifying the known results under one mantle [3]. Recently, Niederreiter and Xing ([4],[5]) have made remarkable progress in this direction by varying the base field and the ramification for many $\mathbb{F}_q$. In this paper, we complement that work by fixing the base and a place of ramification and increasing the number of points to be split. When attempting to split many points, one is confronted with the problem of computing n_k,

$$n_k = \text{ order of the quotient } (\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*/\langle 1-\alpha T | \alpha \in \mathbb{F}_q^* \rangle.$$

Such quotients appear as the Galois group of abelian extensions of $\mathbb{F}_q(T)$ in which all but one of the places of degree one are totally split. These function fields correspond to curves with $n_k q + 1$ rational points, whose genus can be computed via the conductor-discriminant formula, based on the knowledge of the orders n_l for all $l \leq k$.

Apart from its natural importance for constructing curves with many points, the task of computing n_k is interesting in itself, since it is a measure of the amount of interdependence between decomposition groups at different primes in the extension. A large amount of dependence occurs for example in the case when $q = 9$, $k = 5$, since eight decomposition groups generate a subgroup of the Galois group of the full ray class field extension which is isomorphic to a product of only five of the cyclic factors.

The value of n_k is in general very difficult to compute, since it seems to entail finding the relations between all the degree one polynomials in order to determine the order of the subgroup that they generate. The main result of this paper is a general formula for the order of this quotient for any choice of $q = p^f$ and k.

Theorem 1 *Suppose $q = p^f$, $k > 1$. Then*

$$|(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*/\langle 1-\alpha T|\alpha \in \mathbb{F}_q^*\rangle| = p^{\sum_{j=1}^{k-1}(f-f_j)},$$

where f_j is defined as follows.

First write each j uniquely as $p^\nu i$ for some $i \not\equiv 0 \pmod{p}$. Consider the action of $\mathbb{Z}/f\mathbb{Z}$ on $\mathbb{Z}/(q-1)\mathbb{Z}$ whereby

$$d * i = p^d i.$$

Define the set: $H = \{$the smallest natural number from each of the distinct orbits of $\mathbb{Z}/(q-1)\mathbb{Z}$ under the above action$\}$. Now define

$$f_j = \begin{cases} \text{size of the orbit of } h & \text{if } j = p^\nu h \text{ for some } h \in H \\ 0 & \text{otherwise} \end{cases}$$

For instance, in the case mentioned above when $q = 9$, one has

$$f - f_k = \begin{cases} 0 & \text{if } k = 3^\nu,\ 2\cdot 3^\nu, \text{ or } 5\cdot 3^\nu, \\ 1 & \text{if } k = 4\cdot 3^\nu, \text{ or } 8\cdot 3^\nu, \\ 2 & \text{otherwise,} \end{cases}$$

and then n_{k+1}/n_k is equal to 1, 3, or 9 respectively.

This theorem is proved in Section 2 by transforming the multiplicative structure of this group into an additive one via the isomorphism with the additive group of the ring of generalized Witt vectors. This group can then be decomposed into a direct sum of copies of the usual p-Witt vectors. The subgroup generated by the degree one polynomials is transformed by this isomorphism into the subgroup generated by the image of the Teichmüller lifts of the elements $\{\alpha \in \mathbb{F}_q^*\}$. This subgroup and its order are computed in Proposition 1 of Section 2.

In Section 3, we derive from Theorem 1 expressions for n_k in terms of q for certain special cases of k, which arise from the examples of irreducible Deligne-Lusztig curves. The three Deligne-Lusztig families of irreducible curves, Hermitian, Suzuki, and Ree, are of particular interest because each member of them has the maximum number of points possible for a curve of its genus. These families can all be realized as abelian covers of the projective line with Galois group as in Theorem 1.

In Section 4, we determine the smallest k_0 such that, for $k \geq k_0$, the group $(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*/\langle 1-\alpha T|\alpha \in \mathbb{F}_q^*\rangle$ is *not* of exponent p. When $k > k_0$, we will see that the ratio of the number of points to the genus is better than in the exponent p case which was studied in [9]. In addition, when $k > k_0$, we will observe the existence of characters of conductor $k(T)$, $k = mp + 1$, for many values of m, whereas this is never the case for extensions of exponent p.

In Section 5, we give tables of examples constructed via the formula in Theorem 1 for small values of q and k. For example, when $q = 4$ and $k = 7$, the resulting curve has genus 33 with 65 points. The Weil bound for this genus is 137, whereas the Oesterlé's optimization of the explicit formulae show that no curve over $\mathbb{F}_4$ of this genus can have more than 66 points. This example was already in [2], found via the method of computing relations among the degree one polynomials, but that technique does not highlight the fact that this is the smallest choice of k over $\mathbb{F}_4$ for which the Galois group is not killed by 2, contrary to the case of the examples generated in [9] and the families of Deligne-Lusztig curves.

Acknowledgments: I would like to thank Hendrik Lenstra, Spencer Bloch and J.-P. Serre for their generous help and encouragement. This work was done at the Max Planck Institute in Bonn, and I would like to thank the Institute for a wonderful place to work.

2 Main Theorem

In this section we give the proof of the main theorem of the paper.

Proof of Theorem 1: We want to prove that $n_k = p^{\sum_{j=1}^{k-1}(f-f_j)}$. Clearly $(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*$ has order q^{k-1}, since it consists of all the polynomials of degree less than k with coefficients in $\mathbb{F}_q$ and constant term equal to one. So it suffices to show that the order of the subgroup $\langle 1 - \alpha T | \alpha \in \mathbb{F}_q^* \rangle$ is equal to $p^{\sum_{j=1}^{k-1} f_j}$. To accomplish this, we introduce the following notation. Let

$$I = \{i \in \mathbb{N} \mid 1 \leq i \leq k-1, (i,p) = 1\},$$

and define

$$\gamma_i = \text{ the number of non-negative integers } \nu \text{ such that } ip^\nu \leq k-1.$$

Now we can rewrite the exponent as

$$\sum_{j=1}^{k-1} f_j = \sum_{i \in I} \gamma_i f_i.$$

The proof of the theorem is accomplished in Proposition 1 below via an isomorphism of the principal units in the power series ring in one variable over $\mathbb{F}_q$ with the additive group of the ring of generalized Witt vectors over $\mathbb{F}_q$ and the subsequent decomposition into copies of the usual p-Witt vectors of length γ_i.

Witt decomposition

First note that

$$(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^* \cong (1+T\mathbb{F}_q[[T]])/(1+T^k\mathbb{F}_q[[T]]).$$

Now we have an isomorphism (see [1])

$$\Lambda(\mathbb{F}_q) := (1+T\mathbb{F}_q[[T]]) \cong \mathbb{W}(\mathbb{F}_q)$$

where $\mathbb{W}(\mathbb{F}_q)$ is the ring of generalized Witt vectors over $\mathbb{F}_q$. The map is given by:

$$E(a_1, a_2, ...) = \prod_i (1 - a_i T^i)^{-1}$$

for $(a_1, a_2, ...) \in \mathbb{W}(\mathbb{F}_q)$. The map E^{-1} endows $\Lambda(\mathbb{F}_q)$ with a ring structure.

We need the following decomposition of the generalized Witt vectors into a direct sum of copies of the usual p-Witt vectors. The difference between the generalized Witt vectors, denoted here by $\mathbb{W}(\mathbb{F}_q)$, and the usual p-Witt vectors, denoted here by $\mathbb{W}^p(\mathbb{F}_q)$, is as follows: the operations in either case are defined in terms of polynomials

$$W_n(X_1, X_2, ...) = \sum_{d|n} dX_d^{n/d},$$

but in the case of the usual p-Witt vectors, W_n is replaced by W_{p^n}, and the numbering is shifted to start with 0.

Our presentation here has been distilled from the sources ([7],p.102, and [1]):

$$\mathbb{W}(\mathbb{F}_q) \cong \prod_{I(p)} \mathbb{W}^p(\mathbb{F}_q)$$

where $I(p)$ is the set of positive integers prime to p. This isomorphism is given by the map

$$\vec{c} \to (\vec{a}_i)_{i \in I(p)},$$

where $(\vec{a}_i)_{i \in I(p)}$ satisfies:

$$E(\vec{c}) = \prod_{i \in I(p)} P(\vec{a}_i)^{-1/i}$$

with

$$P(\vec{a}_i) = \prod_{j=0}^{\infty} AH(a_{ij} T^{ip^j})$$

$\vec{a}_i = (a_{i0}, a_{i1}, ...)$, and $AH(T)$ is the Artin-Hasse exponential:

$$AH(T) = \prod_{(n,p)=1} (1 - T^n)^{\mu(n)/n}$$

and μ is the Möbius function.

The fact that this isomorphism reduces to the following isomorphism for each k can be seen directly or can be found in [7]:

$$\mathbb{W}_{k-1}(\mathbb{F}_q) \cong \bigoplus_I \mathbb{W}^p_{\gamma_i}(\mathbb{F}_q) \quad (*)$$

Both the left and right hand sides indicate copies of truncated Witt vectors, on the left of length $k-1$ and on the right of lengths $\{\gamma_i\}$. (The numbering of components of the Witt vectors starts with 1 on the left hand side and with 0 on the right.) Note that both sides are groups of order q^{k-1}, which is true because

$$\sum_{i \in I} \gamma_i = k-1.$$

For our purposes we will need the images of the Teichmüller representatives of the elements of $\mathbb{F}_q$: $\alpha \in \mathbb{F}_q$ lifts to $\vec{\alpha} = (\alpha, 0, 0, ...)$ in $\mathbb{W}(\mathbb{F}_q)$ and

$$(\alpha, 0, 0, ...) \to ((\alpha, 0, 0, ...), ..., (\alpha^i, 0, 0, ...), ...)_{i \in I(p)}$$

under the isomorphism (*), since

$$E(\vec{\alpha}) = \prod_{i \in I} AH((\alpha T)^i)^{-1/i}.$$

It remains to determine the order of the subgroup, N, of $\bigoplus_I \mathbb{W}^p_{\gamma_i}(\mathbb{F}_q)$ generated by the $\{\alpha^j\}$, where $< \alpha >= \mathbb{F}_q^*$, $j = 1, ...q-1$, and

$$\{\alpha^j\} = ((\alpha^j, 0, 0, ...), ..., (\alpha^{ji}, 0, 0, ...), ...)_{i \in I(p)}$$

(in the ith component, the vector $(\alpha^{ji}, 0, 0, ...)$ has length γ_i). Consider the projection

$$\Pi : \bigoplus_I \mathbb{W}^p_{\gamma_i}(\mathbb{F}_q) \to \bigoplus_H \mathbb{W}^p_{\gamma_i}(\mathbb{F}_q).$$

Note that if some element s of H is not in I, it can only be for the reason that $s \geq k$, in which case $\gamma_s = 0$. Now set N' equal to the projection of N.

Proposition 1

$$N \cong N' \cong \bigoplus_H \mathbb{W}^p_{\gamma_i}(\mathbb{F}_{p^{f_i}})$$

Proof of Proposition:

First we prove the isomorphism $N \cong N'$. Since N' is obtained from N via a projection, it suffices to show that the projection is injective on N. Suppose that for every $i \in H$,

$$\sum_{j=1}^{q-1} c_j(\alpha^{ji}, 0, 0, ...) = (0, 0, 0...).$$

We must show that

$$\sum_{j=1}^{q-1} c_j(\alpha^{ji'}, 0, 0, ...) = (0, 0, 0...)$$

holds for all $i' \in I$. For $i' \in I$, write $i' = ip^h$, $i \in H$. The sum,

$$\sum_{j=1}^{q-1} c_j(\alpha^{ji}, 0, 0, ...)$$

is a Witt vector with entries which are given by polynomials with coefficients in $\mathbb{F}_p$. Thus the entries of the sum $\sum_{j=1}^{q-1} c_j(\alpha^{ji'}, 0, 0, ...)$ are the p^h-th power of the entries of $\sum_{j=1}^{q-1} c_j(\alpha^{ji}, 0, 0, ...)$, which are zero by assumption.

Next we must show that

$$N' \cong \bigoplus_H \mathbb{W}^p_{\gamma_i}(\mathbb{F}_{p^{f_i}}).$$

First remark that the left hand side is contained in the right hand side because α^i and the subgroup it generates are contained in the subfield $\mathbb{F}_{p^{f_i}}$. Now, a subgroup of a finite abelian p-group generates the whole group if and only if it generates the group $\pmod p$. This is an application of Nakayama' s lemma to the group viewed as a $\mathbb{Z}/p^{\gamma_1}\mathbb{Z}$-module. So it suffices to show that the $\mathbb{F}_p$-span of the set $\{(\alpha^j, ..., \alpha^{ji}, ...)_{i\in H}\}_{j=1,...q-1}$ is $\prod_{i\in H} \mathbb{F}_{p^{f_i}}$. Note that the $\mathbb{F}_p$-dimension of this product is exactly the sum of the size of the orbits of the elements of H under multiplication by p, which is exactly all the numbers $\{1, ..., q-1\}$. Thus it suffices to show that the $q-1$ elements $\{(\alpha^j, ..., \alpha^{ji}, ...)_{i\in H}\}_{j=1,...q-1}$ are linearly independent over $\mathbb{F}_p$. Suppose we have a relation:

$$\sum_{j=1}^{q-1} c_j \alpha^{ji} = 0$$

with $c_j \in \mathbb{F}_p$, which holds for all $i \in H$. Then since $c_j \in \mathbb{F}_p$,

$$\sum_{j=1}^{q-1} c_j \alpha^{jip^h} = 0, \quad \text{for all } h \in \mathbb{Z}.$$

Since ip^h runs through all elements of $\mathbb{Z} \pmod{q-1}$, putting $a_j = \alpha^j \in \mathbb{F}_q$, we can write

$$\sum_{j=1}^{q-1} c_j a_j^{\nu} = 0, \quad \text{for all } \nu \in \mathbb{Z}.$$

Now it follows from the linear independence of characters that $c_j = 0$ for all j. $\square$

This proposition concludes the proof of our theorem, since the order of this subgroup is seen to be $p^{\sum_{i\in I}\gamma_i f_i}$.

3 Families of Examples: Deligne-Lusztig curves

In [3], the ray class field descriptions of the Deligne-Lusztig curves are given and used to deduce results on the order of quotients of polynomial rings which are quite surprising:

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

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

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

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

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

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

Theorem 3 should be modified slightly to describe the full situation in characteristic 3. The proof of these theorems uses the existence of the Deligne-Lusztig curves, the knowledge of the filtration of the ramification groups, and the theorems of class field theory. It seems natural to try to give a more direct proof. In this section we will show how these theorems can be deduced directly from Theorem 1.

The proofs depend on the following lemma, which was pointed out to me by Hendrik Lenstra. In what follows, the notation $\lceil x \rceil$, (resp. $\lfloor x \rfloor$), will be used to denote the least integer greater than (resp. greatest integer less than) or equal to x.

Lemma 1 *Let $q = p^f$. If $k < p^{\lceil f/2 \rceil} + 2$, then $f_i = f$, for all $i \in I$. When $k = p^{\lceil f/2 \rceil} + 2$, then $k - 1 \in I$, and $f_{k-1} = f/2$ if f is even, or $f_{k-1} = 0$ if f is odd.*

Proof: We will prove these statements in order. To show that $f_i = f$ for all i in I, we must show that the orbit of i has size f, and that i is the smallest element in its orbit. Suppose that $i, i' \leq p^{\lceil f/2 \rceil} - 1$, and

$$p^h i \equiv p^{h'} i' \pmod{q-1}, \quad h, h' < f.$$

Then $p^{h-h'} i \equiv i' \pmod{q-1}$, with $h - h' \leq \lfloor f/2 \rfloor$. Since

$$p^{h-h'} i \leq p^{\lfloor f/2 \rfloor}(p^{\lceil f/2 \rceil} - 1) \leq q - 1$$

and $(i', p) = 1$, we conclude that $h - h' \equiv \pmod{f}$ and $i = i'$. This shows that each of the orbits of the elements $i < p^{\lceil f/2 \rceil} + 1$, $(i, p) = 1$, has size f, and that no two of these elements are in the same orbit, which means exactly that $f_i = f$.

For the next claim, we assume that $k = p^{\lceil f/2 \rceil} + 2$. Then $k-1$ is prime to p, so it belongs to I. When f is even, we must show that the size of the orbit of $k-1$ is $f/2$. But $k-1 = p^{f/2}+1$, and $p^{f/2}(k-1) \equiv (k-1) \pmod{q-1}$. Furthermore, this is the smallest positive power of p which could have this property. We also know that $k-1$ is not in the orbit of any smaller element of I, since all other elements of its orbit are between $p^{f/2}+1$ and $q-1$. ¿From this we conclude that $f_{k-1} = f/2$.

When f is odd, it suffices to show that $k-1$ is in the orbit of a smaller number. But

$$k-1 = p^{\lceil f/2 \rceil} + 1 \equiv p^{\lceil f/2 \rceil}(p^{\lfloor f/2 \rfloor} + 1) \pmod{q-1}.$$

Since $k-1$ is not in H, we conclude that $f_{k-1} = 0$. □

Direct proof of Theorem 2: $q^2 = p^f$, $f = 2m$. By Lemma 1,

$$k < p^m + 2 = q + 2 \Rightarrow f_i = f, \quad \text{for all } i \in I$$

$$\Rightarrow p^{\sum_{i \in I} \gamma_i (f - f_i)} = 1.$$

If $k = p^m + 2$, then $p^{\lceil f/2 \rceil} + 1 \in I$, and $f_{p^m+1} = m$. Since $\gamma_{p^m+1} = 1$, we have

$$p^{\sum_{i \in I} \gamma_i (f - f_i)} = p^{f-m} = q. \quad \square$$

Direct proof of Theorem 3: $q = p^f$, $f = 2m+1$. By Lemma 1,

$$k < p^{\lceil f/2 \rceil} + 2 = p^{m+1} + 2 \Rightarrow f_i = f, \quad \text{for all } i \in I$$

$$\Rightarrow p^{\sum_{i \in I} \gamma_i (f - f_i)} = 1.$$

If $k = p^{m+1} + 2$, then $p^{m+1} + 1 \in I$, and $f_{p^{m+1}+1} = 0$. Since $\gamma_{p^{m+1}+1} = 1$, we have

$$p^{\sum_{i \in I} \gamma_i (f - f_i)} = p^f = q. \quad \square$$

Note that this proof holds for any characteristic, eliminating the assumption $p = 2$ from Theorem 3. When $p = 3$, $m \geq 1$, the quotient in the statement of Theorem 3 corresponds to the first stage of the Ree curve. When k is increased to $3^{m+1}+3$, we obtain the Ree curve which has the maximum number of points for its genus. The fact that the degree of the extension is q^2 when $k = 3^{m+1}+3$ can also be deduced from Theorem 1. In fact, it is a special case of the following proposition:

Proposition 2 *Let $q = p^{2m+1}$, $p > 2$. If $D = (p^{m+1}+i)P_\infty$, $2 \leq i \leq p$, then the ray class field extension of $\mathbb{F}_q(X)$ obtained when the other q places of degree one are totally split has degree q^{i-1}.*

Proof: Taking into consideration what has already been proved in Lemma 1, it suffices to show that $f_{k_i-1} = 0$, $k_i = p^{m+1} + i$, $i = 2, ...p$. In other words, that $p^{m+1} + (i-1)$ is in the orbit of some smaller element of I_{k_i}. But

$$p^{m+1} + i + i(q-1) = p^{m+1} + ip^{m+1}p^m = p^{m+1}(1 + ip^m)$$

$$\Rightarrow p^{m+1} + i \equiv p^{m+1}(1 + ip^m) \pmod{q-1}.$$

This suffices to show that $f_{k_i} = 0$ for $i = 1, ..., p-1$, since $1 + ip^m$ is prime to p and less than $p^{m+1} + i + 1$, so it is an element of $I_{k_{i+1}}$. □

From this proposition, we can produce families of curves in any characteristic which are analogous to the Deligne-Lusztig curves in characteristics 2 and 3. The following simple examples certainly have many points, but it remains to be seen whether they are optimal for their genus. Furthermore, these results also hold for $m = 0$, that is to say over prime fields.

Corollary 1 *Let $q = p^{2m+1}$, $p > 2$. If $D = (p^{m+1} + i)P_\infty$, $2 \le i \le p$, then the ray class field extension of $\mathbb{F}_q(X)$ obtained by splitting the other q places in the base corresponds to a curve with $q^i + 1$ rational points of genus*

$$g = \frac{1}{2}((p^{m+1} + i - 2)q^{i-1} - q^{i-2} - q^{i-3} - ... - q - p^{m+1}).$$

Special cases of this family when $i = 2$ and $i = p$ are:

Corollary 2 *Let $q = p^{2m+1}$, $p > 2$. If $D = (p^{m+1} + 2)P_\infty$, then the ray class field extension of $\mathbb{F}_q(X)$ obtained by splitting the other q places in the base corresponds to a curve with $q^2 + 1$ rational points of genus*

$$g = \frac{1}{2}p^{m+1}(q-1).$$

Corollary 3 *Let $q = p^{2m+1}$, $p > 2$. If $D = (p^{m+1} + p)P_\infty$, then the ray class field extension of $\mathbb{F}_q(X)$ obtained by splitting the other q places in the base corresponds to a curve with $q^p + 1$ rational points of genus*

$$g = \frac{1}{2}((p^{m+1} + p - 2)q^{p-1} - q^{p-2} - q^{p-3} - ... - q - p^{m+1}).$$

These two cases correspond to the first and second stages of the Ree curve. The reason that the behavior of the degree is different when $i \ge p + 1$ is that multiples of p are not in I.

4 Comparison with exponent p

The quotient whose order is computed in Theorem 1 is the Galois group of the maximal abelian extension of $\mathbb{F}_q(T)$ which is

1. unramified outside (T),

2. totally split at all other places of degree one,
3. whose characters have conductor $k'(T)$, with $k' \leq k$.

It is an abelian p-group, but it is not necessarily of exponent p (killed by p). Taking the quotient of this group by the subgroup of its pth powers, we obtain the Galois group of the maximal abelian extension of exponent p with properties (1),(2),(3). In this section, we compare the degrees of these two extensions, which we call the maximal p-extension and the maximal p-extension of exponent p.

4.1 Comparison of the degrees

First note that the degree of the maximal p-extension of exponent p is given by the formula:

$$p^{\sum_{i\in I}(f-f_i)}.$$

This follows from the proof of proposition 1, where we computed the subgroup $N' \pmod p$. All of the families described in Section 5 are of exponent p. In fact, we can determine exactly the smallest k for which the Galois group of the extension will not be killed by p:

Proposition 3 *Let $q = p$. Then the degrees of the maximal p-extension and the maximal p-extension of exponent p are equal when $k < (p+1)p+1$. For $k \geq (p+1)p+1$, the degrees differ, and the quotient in Theorem 1 is not of exponent p.*

Proof: It is clear that $p^{\sum_{i\in I}(f-f_i)} = p^{\sum_{i\in I}\gamma_i(f-f_i)}$ whenever

$$f_i \neq f \Rightarrow \gamma_i = 1, \text{ for all } i \in I.$$

In this case, since $f_i = f = 1, \quad$ for all $i \in H$, the only contribution to the degree in either of the formulas comes when $i \notin H$. Each element of the set $\{1, ..., p-1\}$ constitutes a distinct orbit under multiplication by $p \pmod{p-1}$, so they all belong to H. The first element of I which is not in H is $p+1$, and the first k for which $\gamma_{p+1} > 1$ is $(p+1)p+1$. □

When q is a power of a prime, the situation is similar. Proposition 3 is a special case of the following:

Proposition 4 *When $q = p^f$, the smallest k for which the extension is not of exponent p occurs for $k = p^{\lceil f/2\rceil+1} + p + 1$.*

Proof: This follows from Lemma 1 since the first $i \in I$ for which $f_i \neq f$ occurs when $i = p^{\lceil f/2\rceil+1} + 1$, and it is not until $k > ip$ that $\gamma_i > 1$. □

4.2 Example: $q = 2$

As an example of the difference between these two types of extensions, we consider the formulas for the degrees in terms of k when $q = 2$:

Proposition 5 *Let $K = \mathbb{F}_2(X)$. Then the degree of L_k, the maximal p-extension of K of conductor $D = kP_1$ in which the other two rational points of K are totally split, depends on k in the following way:*

$$\deg(L_k/K) = 2^{k-p-m^*}$$

where

$$m^* = \#\{\text{ positive powers of } p \leq k-1\} = \lfloor \log_p(k-1) \rfloor.$$

Proof: Since $q = p$ is a prime and $f = 1$, the only contribution to the degree is p^{γ_i} for each $i \in I - H$. In this situation, $H = \{1\}$. Beginning with $k = 4$, which is the first time when $k-1$ produces an element of I which is not in H, remark that the degree of the extension increases by a power of two for every increase of the conductor by one, except when $k-1$ is a power of the prime. In fact, if k is even, then $k-1$ gives a new element of $I \setminus H$, with $\gamma_{k-1} = 1$; if k is odd, then γ_i increases by one, for some $i \in I$: this will increase the degree by one unless $i \in H$, which in this case happens exactly when $k-1$ is a power of the prime. □

Compare this with the formula for the maximal p-extension of exponent p and conductor kP_1:

Proposition 6 *Let L_k^p denote the maximal p-extension of exponent p of K of conductor $D = kP_1$ in which the other two rational points of K are totally split. If $k = 2m + r$, $r = 0, 1$, then*

$$\deg(L_k^p/K) = 2^{m-1}.$$

Proof: The degree increases by one power of p for each new element of I which is not in H, which are exactly all odd numbers bigger than one and less than k. □

The point of this comparison is that for a given k the degree of the maximal p-extension will be roughly $2^{k-2}/(k-1)$, while the degree of the maximal exponent p p-extension will be roughly $\sqrt{2}^{k-2}$, which means that the examples of the former type will have a much better ratio of number of points to genus. For example, the extension of K with 33 rational points is obtained when $k = 8$, but as an exponent p extension when $k = 10$, so the genus of the exponent p extension is 47 instead of 39. Similarly, in the table for $\mathbb{F}_4$, the example over $\mathbb{F}_4$ of a curve with 65 points which is not of exponent p has genus 33, whereas the curve with this same number of points which is of exponent p has genus 37. □

4.3 New characters from maximal p-extensions

We can interpret a jump in the degree of the extension when k is increased by 1 as implying the existence of new characters with conductor $(k+1)P_1$. The formula we obtained in Theorem 1 shows that when considering the maximal p extension, one will obtain characters of conductor a multiple of p plus one in many cases, whereas this will never occur in the exponent p case. The degree of the maximal p-extension of exponent p does not change when k is increased from a multiple of p, mp, to $mp+1$, since mp is not prime to p, so it is not an element of I. However, the expression for the degree of the maximal p-extension may change under these circumstances, if $mp = ip^{\gamma_i}$, for some $i \in I$. This is due to the fact that when k is increased to $mp+1$, γ_i will increase by one.

5 Examples

In this section, we give tables for different $q = p^f$ of curves obtained by splitting all q rational points of $\mathbb{P}^1_{\mathbb{F}_q}$ different from a given one, P_1, in the ray class field of conductor $D = kP_1$, where $k \geq p^{\lceil f/2 \rceil} + 2$.

All entries in these tables are computed directly from the main theorem of this paper via the ray class field method of Serre which is detailed in [6],[3]. Some of these entries correspond to examples from [9], [5], [8], and [2]. Optimality of an example is determined relative to the Oesterlé bounds. Examples not contained in previous tables in the above sources are denoted with a star (*).

5.1 characteristic 2

5.1.1 q=2

For all entries in this table, $H = \{1\}$.

Table 1: Splitting q Points, $D = kP_1$, $q = 2$

k	n_k	genus	N	exponent p?	Notes
$k=4$ $=p+2$	2	$g=1$	5	yes	optimal (Serre) $k-1=3 \notin H$
$k=5$	2				no new element of I $\gamma_1 = 3$, no difference
$k=6$	2^2	$g=5$	9	yes	optimal (Serre) $\gamma_3 = 1$, $\gamma_5 = 1$
$k=7$	2^3	$g=15$	17	no	optimal (Serre) $\gamma_3 = 2$, $\gamma_5 = 1$
$k=8$	2^4	$g=39$	33	no	optimal (Serre)
$k=9$	2^4				$\gamma_1 = 4$
$k=10$	2^5	$g=103$	65	no	
$k=11$	2^6	$g=247$	129	no	$\gamma_5 = 2$

5.1.2 q=4

For all entries in this table, $H = \{1, 3\}$ since the orbits modulo $(q-1)$ are: $\{1, 2\}$ and $\{3\}$.

Table 2: Splitting q Points, $D = kP_1$, $q = 4 = 2^2$

k	n_k	genus	N	exp p?	Notes
$k = 4$ $= p + 2$	2	$g = 1$	9	yes	optimal (Hermitian) $k - 1 = 3 \in H$, $f_3 = 1$
$k = 5$	2				no new element of I $\gamma_1 = 3$, no difference
$k = 6$	2^3	$g = 13$	33	yes	optimal $f_5 = 0$
$k = 7$	2^4	$g = 33$	65	no	Oesterlé bound is 66 $\gamma_3 = 2$
$* \ k = 8$	2^6	$g = 177$	257	no	$f_7 = 0$ Oesterlé bound 269

5.1.3 q=8

Orbits for $q = 2^3 = 8$:

$\{1, 2, 4\}$
$\{3, 6, 5\}$
$\{7\}$
$H = \{1, 3, 7\}$

Table 3: Splitting q Points, $D = kP_1$, $q = 8 = 2^3 = 2^{2m+1}$

k	n_k	genus	N	exp p?	Notes
$k = 6$ $= p^{m+1} + 2$	2^3	$g = 14$	65	yes	Suzuki curve (optimal) $k - 1 = p^{m+1} + 1$ first time an element appears in a previous orbit
$k = 7$	2^3				$\gamma_3 = 2$, $f_3 = 3$
$* \ k = 8$	2^5	$g = 86$	257	yes	$f_7 = 1$, Oesterlé: 266 Weil: 495
$k = 9$	2^5				$\gamma_1 = 4$, no change
$* \ k = 10$	$2^8 = 256$	$g = 982$	$2,049$	yes	$f_9 = 0$ Oesterlé: $2,372$ Weil: $5,281$
$* \ k = 11$	2^{11}	$g = 9,046$	$16,385$	no	$\gamma_5 = 2$, Oesterlé:$19,673$ Weil: $51,181$

First k for which the extension is not of exponent p is 11.

5.2 characteristic 3

5.2.1 q=3

For all entries in this table, $H = \{1, 2\}$

Table 4: Splitting q Points, $D = kP_1$, $q = 3$

k	n_k	genus	N	exp p?	Notes
$k = 5$ =p+2	3	$g = 3$	10	yes	optimal $k - 1 = 4 \notin H$
$k = 6$	$3^2 = 9$	$g = 15$	28	yes	optimal
$k = 7$	3^2				no new element of I
$k = 8$	3^3	$g = 69$	82	yes	Oesterlé bound is 88
$* \; k = 9$	3^4	$g = 258$	244	yes	$k - 1 \notin H$ Oesterlé: 276
$k = 10$	3^4				
$* \; k = 11$	3^5	$g = 987$	730	yes	$k - 1 \notin H$ Oesterlé: 940
$* \; k = 12$	3^6	$g = 3417$	2188	yes	$k - 1 \notin H$
$* \; k = 13$	3^7	$g = 11,436$	$6,562$	no	$\gamma_4 = 2, 4 \notin H$
$* \; k = 14$	3^8	$g = 37,680$	$19,684$	no	$k - 1 \notin H$
$* \; k = 15$	3^9	$122,973$	$59,050$	no	$k - 1 \notin H$

5.2.2 q=9

Orbits for $q = 3^2 = 9$:

$\{1, 3\}$

$\{2, 6\}$

$\{4\}$

$\{5, 7\}$

$\{8\}$

$H = \{1, 2, 4, 5, 8\}$

Table 5: Splitting q Points, $D = kP_1$, $q = 9 = 3^2$

k	n_k	genus	N	exp p?	Notes
$k=5$ =p+2	3	$g=3$	28	yes	Hermitian curve orbit of 4 size 1
$k=6$	3				orbit of 5 size $f=2$
$k=7$	3				$I_7 = I_6$ $\gamma_2 = 2$
$* \ k=8$	3^3	$g=75$	244	yes	7 is in orbit of 5 Oesterlé: 263
$* \ k=9$	3^4	$g=264$	730	yes	orbit of 8 size 1 Oesterlé: 784
$k=10$	3^4				I,H same, $\gamma_1 = 3$
$* \ k=11$	3^6	$g=3180$	6561	yes	$k > q$, so $k-1 \notin H$
$* \ k=12$	3^8	$g=32,340$	$59,049$	yes	$k-1 \notin H$
$* \ k=13$	3^9	$g=104,511$	$177,147$	no	$\gamma_4 = 2$, $f_4 = 1$
$* \ k=14$	3^{11}	$g=1,049,295$	$1,594,323$	no	$k-1 \notin H$

5.2.3 q=27

Orbits for $q = 3^3 = 27$:

$\{1,3,9\}$
$\{2,6,18\}$
$\{4,12,10\}$
$\{5,15,19\}$
$\{7,21,11\}$
$\{8,24,20\}$
$\{13\}$
$\{14,16,22\}$
$\{17,25,23\}$

Table 6: Splitting q Points, $D = kP_1$, $q = 27 = 3^3 = 3^{2m+1}$

k	n_k	genus	N	exponent p?	Notes
$k=11$ $=p^{m+1}+2$	$3^3 = 27$	$g=117$	730	yes	first stage of Ree curve $k-1 = p^{m+1}+1$ first time an element appears in a previous orbit
$k=12$	$3^6 = q^2 = 729$	$g=3,627$	$19,684$	yes	Ree curve
$k=13$	3^6				I same, $\gamma_4 = 2$
$* \ k=14$	$3^8 = 6561$	$g=38,619$	$177,148$	yes	$f_{13} = 1$

Table 7: Splitting q Points, $D = kP_1$, $q = 5$

k	n_k	genus	N	ratio	Notes
$k = 7$	5	$g = 10$	26	2.6	$N \leq 34$
$k = 8$	25	$g = 70$	126	1.8	$N \leq 150$
$k = 9$	125	$g = 420$	626	1.49048	$g \geq 359$
$k = 10$	625	$g = 2420$	3126	1.29174	$g \geq 2018$
$k = 32$	5^{22}	$g = 3.56936 \times 10^{16}$	11,920,928,955,078,126	0.333979	
$k = 33$	5^{22}	$g = 3.66473 \times 10^{16}$	$11,920,928,955,078,126$	0.325288	exponent p

Note: The last entry in the last table is meant to be compared with the second-to-last entry, to show that curves arising from the main theorem have a much better ratio than those of exponent p.

References

[1] P. Cartier, *Groupes formels associés aux anneaux de Witt généralisés*, C.R.Acad.Sc. Paris, t.265 (10 juillet 1967), Serie A, p. 49-52.

[2] 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.

[3] K. Lauter, *Deligne-Lusztig curves as ray class fields*, Max Planck Institut Preprint 97-63.

[4] 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.

[5] 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.

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

[7] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann Paris, 1959.

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

[9] G. van der Geer and M. van der Vlugt, *How to Construct Curves over Finite Fields with Many Points*, Proc. Conf. Algebraic Geometry (Cortona, 1995), to appear.

[10] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. reine angew. Math. **176** (1936) p.126-140.