UNIVERSITÀ DEGLI STUDI DI ROMA "TOR VERGATA"

FACOLTÀ DI SCIENZE MM.FF.NN.

DOTTORATO DI RICERCA IN MATEMATICA
XXI CICLO

UNIQUENESS OF OPTIMAL CURVES OVER $\mathbb{F}_2$ OF SMALL GENUS

Alessandra Rigato

A.A. 2008-2009

Advisor: Prof. R. Schoof

To my grandmother,
for her great example
of strength and joyfulness.

Acknowledgements

This work would not have been possible without the precious help of René Schoof: to my advisor above all, I would like to express my gratitude for his patience, his dedication and advice. It is a pleasure to thank Everett Howe for his interesting and constructive comments. I also want to thank Claus Fieker for his MAGMA computation, that helped us to conclude this work. I express my acknowledgements to Jan Denef, for supporting my staying at K.U. Leuven and encouraging me in the final and hardest period of my PhD. I finally would like to thank all of the people that have been by my side in the last few years. Each of them, each in his own way, has indirectly contributed to the great experience behind this work.

Rome, May 2009 Alessandra Rigato

Contents

Introduction

The earliest interest in determining the number of rational points of a curve defined over a finite field can be traced back more than two centuries to the first results of Gauss on solving equations over the integers modulo prime numbers. Though the concepts of field and of curve belong to modern algebra, it is remarkable how the foundations for the study of these geometric objects lay deeply in the arithmetic of numbers. In this direction, after the work of Gauss and Jacobi on characters sums, further development has been made in algebraic number theory by Dirichlet, Dedekind, Kronecker and Weber in the nineteenth century. Though it is only with the work of Artin, Hasse, F.K. Schmidt and A. Weil in the last century that a deep interest in the arithmetic of geometric objects arises.

Among the most interesting tools that have been developed in algebraic number theory there is the Dedekind Zeta function of a numer field K, i.e. a finite field extension of the field of rational numbers $\mathbb{Q}$. This is a function of complex variable $s \in \mathbb{C}$ defined as the series

$$\zeta_K(s) = \sum_{\mathfrak{I} \subseteq \mathcal{O}_K} \left(N_{K/\mathbb{Q}}(\mathfrak{I})\right)^{-s},$$

where $\mathfrak{I}$ ranges through the non-zero ideals of the ring of integers $\mathcal{O}_K$ of the number field K. Here $N_{K/\mathbb{Q}}(\mathfrak{I})$ denotes the norm of $\mathfrak{I}$, i.e. the number of the residue classes of $\mathfrak{I}$ in $\mathcal{O}_K/\mathfrak{I}$. The series converges absolutely only for the complex numbers s such that $\Re e(s) > 1$, but it can be analytically continued to all complex numbers as a meromorphic function with a simple pole at $s = 1$. Moreover, since prime factorization of ideals in $\mathcal{O}_K$ is unique, the Dedekind Zeta function can be expressed as an Euler product

$$\zeta_K(s) = \prod_{\mathfrak{P} \subseteq \mathcal{O}_K} \frac{1}{1 - (N_{K/\mathbb{Q}}(\mathfrak{P}))^{-s}},$$

where $\mathfrak{P}$ is a prime non-zero ideal of $\mathcal{O}_K$.

For the special case $K = \mathbb{Q}$ one gets the well known Riemann Zeta function as the series

$$\zeta(s) = \sum_n \frac{1}{n^s}.$$

Here the sum ranges through all non-negative integers n, generators of the ideals $n\mathbb{Z}$ of the ring of integers $\mathbb{Z}$. The norm of such an ideal is indeed given by the cardinality of $\mathbb{Z}/n\mathbb{Z}$. Also the Riemann Zeta function converges for complex numbers s having $\Re e(s) > 1$ and satisfies the Euler product form

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

It is proved that the analytical continuation of $\zeta(s)$ to all complex numbers $s \neq 1$ has zeros at the negative even integers, the so-called trivial zeros, while the non-trivial zeros are the object of the Riemann hypothesis, that states that they all have real part equal to $1/2$.

In 1924 Artin introduced the Zeta function for a hyperelliptic curve of equation $y^2 = f(x)$ defined over a finite field $\mathbb{F}_q$ for odd q in strict analogy to the Dedekind Zeta function for an algebraic number field. He reformulated Dedekind's Zeta function for number fields in terms of ideals of algebraic function fields in one variable over a finite field $\mathbb{F}_q$ in connections with his work on class field theory. Such a function field F is a finite algebraic field extension of the rational function field $\mathbb{F}_q(x)$, where x is an element of F of trascendece degree 1 over $\mathbb{F}_q$. In this context, the role of a prime ideal of a number field is played by a place P of F, i.e. the maximal ideal $\mathcal{M}_\mathcal{P}$ of a discrete valuation ring $\mathcal{O}_P$ in F. The norm of a prime ideal of a number field is the cardinality $q^{\deg P}$ of the residue class field $\mathcal{O}_P/\mathcal{M}_P$ of a place P. This is a finite extension of $\mathbb{F}_q$ whose index $\deg P$ is called the degree of P. By substitution of variable $t = q^{-s}$, the Euler product form of the Zeta function of a fuction field F looks like

$$Z(t) = \prod_P \frac{1}{(1 - t^{\deg P})} = \prod_{d=1}^{\infty} \frac{1}{(1 - t^d)^{a_d}},$$

where P runs over the places of F and a_d denotes the number of places of degree d of F. Let $D = \sum_P n_P P$ be an effective divisor of a fuction field F, i.e. a formal sum over the places P of F where the integers $n_P \geq 0$ are zero but a finite number. The power series form of the Zeta function $Z(t)$ of a function field F is given by

$$Z(t) = \sum_D \frac{1}{q^{\deg D\, s}} = \sum_D t^{\deg D} = \sum_{d=0}^{\infty} A_d t^d. \tag{1}$$

Here $\deg D = \sum_P n_P \deg P$ is the degree of the divisor D and A_d the number of effetive divisors of F of degree d.

F.K. Schmidt explicitly introduced the Zeta function for a smooth, projective, absolutely irreducible curve C defined over a finite field $\mathbb{F}_q$ in the equivalent suggestive form

$$Z(t) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right).$$

In this form is more evident that the Zeta function encodes information on the number $\#C(\mathbb{F}_{q^n})$ of rational places of C over any degree n extension of the definition field $\mathbb{F}_q$. The function field of C is an algebraic function field over $\mathbb{F}_q$ as described above and this exponential form for the Zeta fuction is obtained taking the logarithm derivative of the Euler product form and considering that

$$\#C(\mathbb{F}_{q^n}) = \sum_{d|n} d a_d.$$

The latter relation comes from the fact that a place of degree d of C corresponds to a conjugacy class of points in $C(\overline{\mathbb{F}_q})$ of cardinality d, given by the action of the Galois group $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, where $\overline{\mathbb{F}_q}$ is a fixed algebraic closure of $\mathbb{F}_q$. Schmidt also proved that the Zeta function of a genus g curve is a rational function

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}, \tag{2}$$

where $L(t)$ is a degree $2g$ polynomial. This is the form we are used to nowadays. The polynomial $L(t)$ can be factored over $\mathbb{C}$ as

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t), \tag{3}$$

where the α_i's are algebraic integers and can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ holds for $i = 1, \ldots, g$ since the polynomial $L(t)$ satisifes the functional equation

$$L(t) = q^g t^{2g} L(1/qt). \tag{4}$$

Moreover the polynomial $L_n(t) = (1-t)(1-q^n t)Z_n(t)$ associated to the curve C defined over $\mathbb{F}_{q^n}$ satisfies

$$L_n(t) = \prod_{i=1}^{2g} (1 - \alpha_i^n t). \tag{5}$$

Artin conjectured the reciprocal roots α_i of the Zeta function of a curve to be complex numbers having absolute value

$$|\alpha_i| = \sqrt{q}.$$

Since $|q^{-s}| = q^{-\Re e(s)}$, this is equivalent to say that the zeros $1/\alpha_i$ of the Zeta function are of the form q^{-s} with $\Re e(s) = 1/2$, in analogy with the conjecture about the zeros of the Riemann Zeta function. Not much later, around 1932, Hasse observed an interesting consequence of Artin's conjecture. Since

$$\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i}), \tag{6}$$

by comparison of the linear terms in (1) and in (3), the number $\#C(\mathbb{F}_q)$ of rational points of a genus g curve C defined over a finite field $\mathbb{F}_q$ can be bounded by

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{7}$$

Hasse proved the conjecture and hence the bound for $g = 1$. But the proof of this conjecture of Artin in the general case is due to Weil in 1948. The Weil Theorem on the zeros of the Zeta function of a curve defined over $\mathbb{F}_q$ can be considered as a milestone in the history of number theory. Moreover, further conjectures due to Weil have been pushing forward investigations for the next twenty-five years, concerning the possibility to extend to Zeta functions of varieties over finite fields the same properties that Weil had proved to hold for Zeta functions of curves over finite fields. A complete proof of Weil's conjectures has finally been achieved by Deligne in 1973.

In the context of curves over finite fields, the bound in (7) is nowadays known as Hasse-Weil bound and it has played an undisputed predominant role until the '80s. Only in 1982, in fact, a sudden revival in the subject takes place, in connection with the studies about error-correcting codes of the Russian mathematician Goppa.

A linear code $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q{}^n$. We denote by k its dimension over $\mathbb{F}_q$. An element of $\mathcal{C}$ is said to be a codeword. Each codeword can be represented as a n-tuple of elements of $\mathbb{F}_q$ in which the first k-entries consist of information that needs to be transmitted through a noisy channel. The rest of the entries is linearly dependent on the previous k and this redundancy allows the receiver of the message to detect errors occured during the transmission, whenever the structure of the received codeword has not been mantained. Sometimes it is even possible to correct the transmission errors: in particular it is possible to correct up to $[(d-1)/2]$ errors in one word, where $d = \min_{v \neq w \in \mathcal{C}}\{i \,|\, v - w$ has a number i of non-zero coordinate$\}$ is the minimal distance of the code. Moreover the lenght n, the dimension k and the minimum distance d of a code are related by the Singleton bound:

$$k + d \leq n + 1.$$

Information and redundancy have to be balanced in order to give a good code: two important parameters that describe the quality of a code are the

transmission rate k/n and the relative distance d/n.
Let C be a genus g curve defined over $\mathbb{F}_q$ and let $D = \sum_P n_P P$ be a rational divisor of C. Consider a set of $\mathbb{F}_q$-rational points $P_1, \ldots, P_n$ of C such that $P_i \notin \operatorname{supp} D$, for all $i = 1, \ldots, n$. Then define the map

$$\begin{aligned} \varphi : L(D) &\to \mathbb{F}_q{}^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)), \end{aligned}$$

from the $\mathbb{F}_q$-vector space $L(D) = \{f \in K^* \,|\, (f) + D \geq 0\} \cup \{0\}$ of elements of the function field K of C. Here $(f) + D \geq 0$ means that for the principal divisor $(f) = \sum_P v_P(f)P$ one has that $v_P(f) + n_P \geq 0$ for every P. In particular f admits a pole in P of order at most n_P and f is well defined in the P_i's. The Goppa code associated to the curve X, and to the divisors D and $\sum_{i=1}^n P_i$ is defined to be the image of φ. The length of a Goppa code is clearly n, while the minimal distance is bounded by $d \geq n - \deg D > 0$. By arguments of algebraic geometry as the Riemann-Roch theorem, one can show that the dimension of the code is at least $k \geq \deg D - g + 1$. From these last two inequalities and the Singleton bound it is easily verified that

$$1 + \frac{1-g}{n} \leq \frac{k}{n} + \frac{d}{n} \leq 1 + \frac{1}{n}.$$

This implies that for a Goppa code it is possible to have both transmission rate k/n and relative minimum distance d/n large, whenever the code is associated to a curve C having small genus g and a large number n of $\mathbb{F}_q$-rational points.

Motivated by the idea that "good codes" could be explicitly constructed by means of curves defined over finite fields having many rational points with respect to their genus, it became of interest to reconsider the study of such curves in order to find explicit examples. Rather unexpectedly, it appeared that Weil's estimates were not best possible for large genus. One can in fact consider the asymptotic behavior of the ratio between the number of $\mathbb{F}_q$-rational points and the genus of all genus g curves C. By means of the Hasse-Weil bound it can be estimated as

$$A(q) = \limsup_{g \to \infty} \frac{\#C(\mathbb{F}_q)}{g} \leq 2\sqrt{q}.$$

Serre gave first a non-trivial improvement to the Hasse-Weil bound when q is not a square

$$|\#C(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}], \tag{8}$$

(here [ ] indicates the integer part). An imediate corollary is $A(q) \leq [2\sqrt{q}]$. The bound (2.1) follows considering the arithmetic-geometric-mean inequality

$$\frac{1}{g} \sum_{i=1}^{g} x_i \geq (\prod_{i=1}^{g} x_i)^{1/g} \geq 1,$$

taken over the totally positive algebraic integers $x_i = [2\sqrt{q}] + 1 + \alpha_i + \overline{\alpha_i}$ for $i = 1, \ldots, g$, where the α_i's are the reciprocal roots of the Zeta function of C. This implies indeed $\sum_{i=1}^{g} x_i \geq g$ and hence the bound.
Generalizing a further improvement due to Ihara [I], in 1983 Drinfeld and Vlăduţ [D-V] achieved the best known asymptotic bound

$$A(q) \leq \sqrt{q} - 1, \tag{9}$$

which has been shown to be attained by Shimura curves when q is a square. The proof relies on some basic ideas from which Serre has obtained information for a particular value of g: the final result is analogous to the use of Weil's explicit formulae for bounding below the discriminant of a number field. Here's the idea that provides new upper bounds for $\#C(\mathbb{F}_q)$. Let $\Psi(t) = \sum_{n=1}^{\infty} c_n t^n$ be a polynomial with non-negative real coefficients c_n satisfying to

$$1 + \Psi(\theta) + \Psi(\theta^{-1}) \geq 0, \qquad \text{for all } \theta \in \mathbb{C},\ |\theta| = 1,$$

and denote by Ψ_d the polynomial $\Psi_d(t) = \sum_{n \equiv 0 \,(\mathrm{mod}\ d)}^{\infty} c_n t^n$. Consider the equalities

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{g} (\alpha_j^n + \overline{\alpha_j}^n) = q^n + 1 - q^{n/2} \sum_{j=1}^{g} (e^{in\theta_j} + e^{-in\theta_j}),$$

where $\alpha_j = \sqrt{q} e^{i\theta_j}$ for $j = 1, \ldots, g$ are the reciprocal roots of the Zeta function of C (the first equality is a generalization of (6) due to (4) and (5)). One has

$$\begin{aligned} 0 \leq \sum_{j=1}^{g} (\Psi(e^{in\theta_j}) + \Psi(e^{-in\theta_j}) + 1) &= g + \sum_{j=1}^{g} \sum_{n \geq 1} c_n (e^{in\theta_j} + e^{-in\theta_j}) \\ &= g + \sum_{n \geq 1} q^{-n/2} c_n (q^n + 1 - \#C(\mathbb{F}_{q^n})) \\ &= g + \Psi(q^{1/2}) + \Psi(q^{-1/2}) - \sum_{d \geq 1} \sum_{d \mid n} q^{-n/2} c_n d a_d. \end{aligned}$$

Then, for any choice of real non-negative coefficients c_n, the following relation holds

$$\sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{1/2}) + \Psi(q^{-1/2}),$$

and in particular

$$\#C(\mathbb{F}_q) \leq \frac{g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}{\Psi(q^{-1/2})},$$

since $\#C(\mathbb{F}_q) = a_1$. Hence any choice of the polynomial $\Psi(t)$ provides an upper bound for the number of $\mathbb{F}_q$-rational points: for example for $\Psi(t) = t/2$ one obtaines the Hasse-Weil bound. But good choices for c_n are those that minimize the corresponding upper bound. For $q = 2$, by choosing $\Psi(t)$ such that

$$1 + \Psi(t) + \Psi(t^{-1}) = \frac{1}{c}(1 + x_1(t + t^{-1}) + x_2(t^2 + t^{-2}) + x_3(t^3 + t^{-3}))^2,$$

where $c = 1+2{x_1}^2+2{x_2}^2+2{x_3}^2$, $x_1 = 1$, $x_2 = 0.7$ and $x_3 = 0.2$, Serre obtained the estimate $\#C(\mathbb{F}_2) \leq 0.83g + 5.35$. For $g \geq 2$ this improves the Hasse-Weil bound. Indeed already for $g = 2$ one has now that $\#C(\mathbb{F}_2) \leq 6$, while the Hasse-Weil bound only predicts $\#C(\mathbb{F}_2) \leq 8$ and Serre's refinement in (2.1) gave $\#C(\mathbb{F}_2) \leq 7$. The improvement is even better as the genus increases: in case $g = 12$, for example, the Hasse-Weil bound is 36, while the new estimate given by $\Psi(t)$ is 15. For more comparisons see Table 2.1. Oesterlé's linear programming method optimized the choice for $\Psi(t)$ in 1982 (the argument has never been published but a sketch of the proof can be found in [S], page Se Th 29, and [E]).

Nevertheless also this estimate failed to be sharp. It became hence of interest to consider the quantity

$$N_q(g) := \max\{\#C(\mathbb{F}_q) \,|\, \text{for a genus } g \text{ curve } C \text{ defined over } \mathbb{F}_q\}, \qquad (10)$$

i.e. the actual maximum number of $\mathbb{F}_q$-rational points that a genus g curve can have, and to define *optimal* a genus g curve defined over $\mathbb{F}_q$ having a number of $\mathbb{F}_q$-rational points equal to $N_q(g)$.

Several methods have been used in order to determine $N_q(g)$ and to provide examples of optimal curves over $\mathbb{F}_q$ for fixed values of the genus g and of the cardinality of the finite field $\mathbb{F}_q$. The progress in characteristic 2 and 3 and for genus $g \leq 50$ is listed in the tables [G-V]: in particular the values of $N_2(g)$ for low genus g have been determined by Serre in [S1] (see also [S], page Se Th 41, for more details), giving examples of curves having a number of $\mathbb{F}_2$-rational points attaining the bounds shown in the row tagged as Serre-Oesterlé of Table 2.1. Most of Serre's examples consist of abelian coverings of curves over $\mathbb{F}_2$, whose algebraic function fields can be constructed as ray class fields. We display Serre's results on $N_2(g)$ in the table below.

Notice that for genus 7 Serre-Oesterlé's estimate in the table is 11. In order to determine $N_2(7) = 10$, Serre gave first an example of a genus 7 curve having 10 rational points and next proved that there is no genus 7 curve with 11 rational points (cf. [S], page Se Th 38a). For genus 12, on the other hand, while it is known that a curve exists having 14 rational points, one still can not prove whether or not there exists a curve attaining the bound of 15

g	0	1	2	3	4	5	6	7	8	9	10	11	12
Hasse - Weil	3	5	8	11	14	17	19	22	25	28	31	34	36
Serre - Oesterlé	5	6	6	7	8	9	10	11	11	12	13	14	15
$N_2(g)$	3	5	6	7	8	9	10	10	11	12	13	14	$14-15$

Table 1: Bounds on the number of $\mathbb{F}_2$-rational points of a genus g curve

rational points over $\mathbb{F}_2$. This means that $N_2(12)$ has not been determined yet.

In this thesis we use class field theoretic methods following Serre to construct optimal curves over $\mathbb{F}_2$. The main idea is to construct as ray class fields suitable abelian extensions of the algebraic function fields of low genus curves over $\mathbb{F}_2$.
The first chapter is an introduction to these methods. One begins by fixing a base curve X over $\mathbb{F}_2$ of genus g_X, a non empty set S of rational points of X and an effective rational divisor $D = \sum_P n_P P$ of X, such that $\operatorname{supp} D \cap S = \emptyset$. Here the sum runs over the places P of the function field K of X. Next one looks for a convenient finite abelian covering $Y \to X$, i.e. a separable surjective map corresponding, by pull back, to a finite abelian Galois extension of the function fields L/K, where all places of K in $\operatorname{supp} D$ ramify over the function field L of Y (D turns out to be the conductor of L/K), and where all places of K in S split completely over L. In this way the curve Y is defined over $\mathbb{F}_2$ and has $|Gal(L/K)|$ rational points lying over each point of X in S and one rational point lying over each rational point of X in the support of D that totally ramifies. The genus g_Y of Y can be determined from the genus of X by a variant of the Hurwitz formula that expresses the different of the abelian extension L/K in terms of the conductors of the cyclic subextensions. Class field theory explains how to determine $Gal(L/K)$ and hence the arithmetic of the curve Y from the arithmetic of X, according to the choices made for S and D.
By means of class field theory it is also possible to study the splitting behavior of places of any degree d of the base curve X in the covering Y, whose function fields extention L/K has been constructed as ray class field. One considers first of all that the places of K that ramify over L are precisely those lying in the support of the conductor D. A not ramifying place P of K splits completely over L if and only if its decomposition group is trivial: the latter is defined to be the subgroup of elements of $Gal(L/K)$ fixing one of the conjugate places Q of L lying over P. Since P is not ramified its decomposition group is cyclic, and, since the extension is abelian, the generator $\mathrm{Frob}P$ of the decomposition group depends only on P. The order of $\mathrm{Frob}P$ can be computed explicitely using class field theory.
A further step in the study of curves defined over finite fields is to consider

their Zeta function as in (2). As seen above this object encodes important arithmetic information on the number of points of the curve over all finite extensions $\mathbb{F}_{q^n}$ of the definition field $\mathbb{F}_q$. On the other hand only a finite piece of information is sufficient to completely determine the Zeta function. For example it is enough to know the numbers a_d of places of the curve of degree $d = 1, \ldots, g$ in order to determine the first $g + 1$ coefficients of the series expansion

$$(1-qt)(1-t)Z(t) = \frac{(1-qt)(1-t)}{\prod_{d=1}^{g}(1-t^d)^{a_d}} + O(t^{g+1}) = 1 + b_1 t + \ldots + b_g t^g + O(t^{g+1}),$$

that coincide with the first $g + 1$ coefficients of the numerator of the Zeta function $L(t) = q^g t^{2g} + b_{2g-1} t^{2g-1} + \ldots + b_1 t + 1$. The rest of the coefficients is determined by $b_{2g-i} = q^{g-i} b_i$ for $i = 1, \ldots, g$, by the functional equation (4) of $L(t)$.

One can recover the number of degree $d = 1, \ldots, g$ places and hence the Zeta function of a curve Y, whose function field has be constructed as ray class field as presented in Section 2.3.

On the other hand one can consider the problem of recovering the Zeta function of an optimal genus g curve C defined over $\mathbb{F}_q$ when only the number of $\mathbb{F}_q$-rational points of C is known (much less that the g numbers a_d of degree d places, for $d = 1, \ldots, g$, we had to consider in the previous part). This is possible following the approach that Serre started by considering the so called real Weil polynomial $h(t)$ associated to the curve C:

$$h(t) = \prod_{i=1}^{g} (t - \mu_i) \ \in \ \mathbb{Z}[t],$$

where $\mu_i = \alpha_i + \overline{\alpha_i}$ for $i = 1, \ldots, g$ and the α_i's are the reciprocal roots of the Zeta function of C. The real Weil polynomial of a curve has hence all roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ and moreover has the property that also the roots of its derivatives lie in the same interval. Since the real Weil polynomial of a genus g curve C is related to the numerator $L(t)$ of the Zeta function of C by

$$t^g L(1/t) = h(t + q/t), \tag{11}$$

the problem of determining the Zeta function of C can be turned into the problem of determining the real Weil polynomial of C. We define a monic degree g polynomial

$$h(t) = t^g + c_{g-1} t^{g-1} + \ldots + c_1 t + c_0 \ \in \ \mathbb{Z}[t]$$

to be a *candidate* real Weil polynomial for a genus g curve C defined over $\mathbb{F}_q$ if it satisfies the following three properties:

1. the trace is $c_{g-1} = \#C(\mathbb{F}_q) - (q+1)$,
2. the polynomial $h(t)$ and all its derivatives have all roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$,
3. the polynomial $L(t) = t^g h(1+qt^2)$, as in (11), satisfies

$$L(t) + O(t^{g+1}) = (1-t)(1-qt)\prod_{i=1}^{g} \frac{1}{(1-t^d)^{a_d}} + O(t^{g+1}),$$

with all $a_d \geq 0$.

For a given genus g curve C there are only finitely many candiate real Weil polynomials $h(t) = t^g + (\#C(\mathbb{F}_q) - (q+1))t^{g-1} + \ldots + c_1 t + c_0$. One can compute them explicitly (cf. [S]). In order to determine the coefficients c_i for $i = 0, \ldots, g-2$ one considers the i-th derivatives $h^{(i)}(t)$ of $h(t)$ backwards. The equation $y = h^{(g-2)}(t)$ represents a family of parabolas determined up to translation of the unknown coefficient c_{g-2}. Then $h^{(g-2)}(t)$ has the two roots in $[-2\sqrt{q}, 2\sqrt{q}]$ whenever the corresponding parabola has two intersections with the t-axis in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. Hence c_{g-2} is bounded by the interval of integer values corresponding to the parabolas satisfying the latter property. Each of the values of c_{g-2} determines together with c_{g-1} a value for a_2: if a_2 is negative one discards the corresponding value of c_{g-2}. To each value of c_{g-2} giving a non-negative value of a_2 one associates a branch of a tree and determines $h^{(g-3)}(t)$ and an interval of integer values for c_{g-3} corresponding to non-negative a_3's in a similar way. The procedure can be iterated until one has as leaves of this tree values for the coefficient c_0 for which the all roots of $h(t)$ lie in $[-2\sqrt{q}, \sqrt{q}]$.

Further investigation on the candidate real Weil polynomials of the list sometimes allows to see that there exist no curves associated to some of them. Useful results for further analysis in this direction are due to Serre and more recently to E. Howe and K. Lauter (cf. Section 2.2.3). The idea at the basis of these results is that the factorization of the real Weil polynomial of a genus g curve C encodes some properties of the Jacobian of C.

The main result of the thesis deals with uniqueness up to isomorphism of optimal curves $\mathbb{F}_2$ of genus $g = 1, \ldots, 6$. Indeed two curves having the same Zeta function may not be isomorphic a priori. In Section 2.7 we prove the following results on uniqueness of optimal curves.

- There exists a unique genus g optimal curve over $\mathbb{F}_2$ up to isomorphism for any genus $1 \leq g \leq 5$. The optimal curves constructed by means of class field theory in Section 2.3 are, in this sense, the unique examples of optimal curves.

- There exists a unique genus 6 optimal curve over $\mathbb{F}_2$ for each of the two possible Zeta functions listed in a) and b) of Proposition 2.1.4. In particular, the optimal curve constructed in Section 2.3 is the unique example of genus 6 optimal curve having a) as Zeta function. On the other hand, all genus 6 optimal curves having b) as Zeta function are isomorphic to the curve we describe in Proposition 2.4.3.

We approach to these results in two steps: first we show the following results on uniqueness of the Zeta function of optimal curves

- For $g = 1, \ldots, 5$ the Zeta function of a genus g optimal curve over $\mathbb{F}_2$ is unique and indeed it is the Zeta function of the genus g optimal curve described in Section 2.3. We list these Zeta functions in Proposition 2.1.3.

- Any genus 6 optimal curve over $\mathbb{F}_2$ can have one of two possible Zeta functions. They are listed in Proposition 2.1.4.

In the second step we show how uniqueness up to $\mathbb{F}_2$-isomorphism of an optimal genus g curve follows from its Zeta function.

When the genus increases, the list of candidate real Weil polynomials for a genus g optimal curve defined over $\mathbb{F}_2$ becomes longer and longer. Trying to determine which candidate polynomials do not occur as real Weil polynomial of a curve turns out to be quite hard.

Finally we provide a further example of non-uniqueness by constructing a ray class field having among its subfields the function fields of two genus 7 optimal curves whose Zeta functions are different. We do not know if these are the only examples of genus 7 optimal curves defined over $\mathbb{F}_2$.

Chapter 1

An introduction to class field theory for curves over finite fields

Let X be a projective, smooth absolutely irreducible curve defined over $\mathbb{F}_q$. The function field K of X is defined to be the quotient field of the coordinate ring of any open $\emptyset \neq U \subsetneq X$ and it is an algebraic function field in one variable over $\mathbb{F}_q$ in the sense of Definition 1.1.1. To any separable surjective morphism of curves $Y \to X$ one can associate by pull back the finite separable extension L/K of function fields, where L is the function field of Y. We call such a morphism a *covering* of X of degree n, where n is the extension degree $[L : K]$. If the extension is Galois and the corresponding Galois group is abelian, the extension L/K is said to be an *abelian extension* and the corresponding covering $Y \to X$ is said to be an abelian covering. Most of the results of class field theory that hold for abelian extensions of number fields also hold for these abelian extensions of function fields. In this way it is possible to describe all finite abelian extensions L of the function field K, and hence give a description of the associated coverings $Y \to X$.
We divide this introductory chapter into two sections. In the first we recall some definitions and give results without proof on algebraic function fields and their Galois extensions. A more detailed exposition with proofs and examples can be found in [Sti]. In the second section we present some important results of class field theory for function fields and in particular we focus on ray class fields. More on this subject can be found in [Au], [L1], [N-X], [S], [Sch].

1.1 Algebraic function fields and Galois extensions

Let k be an arbitrary field.

Definition 1.1.1. *An* algebraic function field K of one variable over k *(short* function field*) is a field extension K/k such that there exists an element $x \in K$ of transcendence degree* 1 *over k, such that K is a finite algebraic field extension of the rational function field $k(x)$ (i.e. $[K : k(x)] < \infty$).*

The set $\overline{k} = \{z \in K \mid z \text{ algebraic over } k\}$ is a subfield of K called the *field of constants of K*. Naturally $k \subseteq \overline{k} \subset K$ and $K/\overline{k}$ is itself a function field over k. If $k = \overline{k}$ we say that k is the *full constant field of K*.

1.1.1 Places of a function field and valuations

One of the basics in the theory of algebraic function field is the concept of place. A *discrete valuation ring* is a principal ideal domain with exactly one non-zero maximal ideal, then

Definition 1.1.2. *A* place *of a function field K/k is the maximal ideal $\mathcal{M}_P$ of a valuation ring $\mathcal{O}$ of K/k. Any generator t of $\mathcal{M}_P$, as principal ideal $t\mathcal{O}$, is called* uniformizer *at the place P.*

Let t be a uniformizer at a place P, then every element $0 \neq z \in K$ has a unique representation of the form $z = t^n u$, for some $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$. The discrete valuation ring $\mathcal{O}$ is then uniquely determined by $\mathcal{M}_P$:

$$\mathcal{O} = \{\, z \in K \mid z^{-1} \notin \mathcal{M}_P\}.$$

Hence the notation $\mathcal{O}_P = \mathcal{O}$ makes sense and it is correct to talk about the *discrete valuation ring of the place P*. Moreover one defines

Definition 1.1.3. *A* normalized discrete valuation *of the function field K/k is a surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$ satisfying the following properties:*

i) $v(x) = \infty \iff x = 0$;

ii) $v(xy) = v(x) + v(y)$ *for all* $x, y \in K$;

iii) $v(x + y) \geq min\{\, v(x), v(y)\}$ *for all* $x, y \in K$;

iv) $v(a) = 0$ *for all* $0 \neq a \in k$.

There is a bijective correspondence between the normalized discrete valuations of a function field K and its places defined by associating to any place P the map $v_P : K \to \mathbb{Z} \cup \{\infty\}$ in the following way: let t be a uniformizer at P and consider for any $0 \neq z \in K$ its unique representation $z = t^n u,\ \exists\ n \in \mathbb{Z},\ \exists\ u \in \mathcal{O}_P^*$, one defines $v_P(z) = n$ and $v_P(0) = \infty$. Viceversa, one has

$$\begin{aligned} \mathcal{O}_P &= \{\, z \in K \mid v_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{\, z \in K \mid v_P(z) = 0\}, \\ \mathcal{M}_P &= \{\, z \in K \mid v_P(z) > 0\}, \end{aligned}$$

as further characterization for a place P of K. An element $t \in K$ is a uniformizer at P if and only if $v_P(t) = 1$.

Definition 1.1.4. *Let P be a place of K.*

i) $\mathcal{F}_P = \mathcal{O}_P/\mathcal{M}_P$ *is called the* residue class field of P. *It is a finite extension of k.*

ii) $\deg P = [\mathcal{F}_P : k]$ *is called the* degree *of P.*

For the case when $\deg P = 1$ one has $\mathcal{F}_P = k$ and in this case the place is called a *k-rational place*.

Definition 1.1.5. *Let $z \in K$ and P a place of K, then*

i) P is a zero *of z if and only if $v_P(z) > 0$; if $v_P(z) = m > 0$, P is called a* zero of z of order m.

ii) P is a pole *of z if and only if $v_P(z) < 0$; if $v_P(z) = -m < 0$, P is called a* pole of z of order m.

One can prove that every function field has infinitely many places. On the other hand any non-zero element of a function field has only a finite number of zeros and poles.

1.1.2 Divisors and genus of a function field

The places of a function field generate an additive group as follows.

Definition 1.1.6. *A* divisor *of a function field K/k is a formal sum*

$$D = \sum_P n_P P,$$

where the sum runs over the places of K and all but a finite number of $n_P \in \mathbb{Z}$ are zero.

We define the *support* of a divisor D by $\operatorname{supp} D = \{P \in K \mid n_P \neq 0\}$. The divisors of a function field K form an additive (free abelian) group, generated by the places of the function field itself, called the *divisor group* of K/k and denoted with $Div(K)$. A partial ordering over $Div(K)$ is defined by:

$$D_1 \leq D_2 \;\Leftrightarrow\; v_P(D_1) \leq v_P(D_2) \qquad \forall\ P \text{ place of } K,$$

where $v_P(D) = n_P$. A divisor $D \geq 0$ is called *effective* and the *degree* of a divisor is defined by

$$\deg D = \sum_P v_P(D) \deg P,$$

yielding the group homomorphism $\deg : Div(K) \to \mathbb{Z}$.

Definition 1.1.7. *For any $0 \neq z \in K$ one defines the* principal divisor *of z as the divisor $(z) = \sum_P v_P(z)P$.*

Any principal divisor is the difference $(z) = (z)_0 - (z)_\infty$ of the effective divisors $(z)_0$ and $(z)_\infty$, whose support is respectively the set of zeros of z and the set of poles of z. Moreover $\deg(z)_0 = \deg(z)_\infty$ and hence every principal divisor has degree zero. Since $\forall\ 0 \neq x, y \in K$, $(xy) = (x) + (y)$, the principal divisors of K/k form a subgroup of $Div(K)$, called the *group of principal divisors* of K/k and denoted by

$$\mathcal{P}rinc(K) = \{\ (z) \in Div(K) \mid 0 \neq z \in K\}.$$

The quotient group $Div(K)/Princ(K)$ is called the *divisor class group* of K. To the same divisor class $[D] = D + Princ(K)$ of $D \in Div(K)$ belong all divisors $D' \sim D$ such that $D' = D + (z)$ for some $z \in K\backslash\{0\}$.
The set $Div^0(K)$ consisting of all divisors of degree 0 of K is a subgroup of $Div(K)$ containing $Princ(K)$. It is called the *divisor group of degree zero* of K. The factor group

$$Cl(K) = Div^0(K)/Princ(K)$$

is called the *divisor class group of degree zero* of K. It is a finite group and its cardinality $h(K)$ is called the *divisor class number* of K.

Definition 1.1.8. *For any divisor $D \in Div(K)$ we set*

$$L(D) = \{z \in K \mid (z) + D \geq 0\} \cup \{\,0\}.$$

If $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$ with $n_i > 0,\ m_j > 0$ then $L(D)$ consists of all elements $z \in F$ such that

i) z has zeros of order $\geq m_j$ at Q_j, for $j = i, \ldots, s$, and

ii) z may have poles at the places $P_1, \ldots, P_r$ with pole order at P_i being bounded by n_i $(i = 1, \ldots, r)$.

One can prove that, for all $D \in Div(K)$, $L(D)$ is a finite dimensional vector space over k and that, if $D' \sim D$, then $L(D) \simeq L(D')$ (as vector space over k). The *rank* of a divisor D is $\ell(D) = \dim L(D)$. Therefore equivalent divisors have not only the same degree but also the same rank. So that it makes sense to speak of *degree* and of *rank* of a *divisor class* in the divisor class group.

Definition 1.1.9. *The genus g of a function field K/k can be defined by*

$$g = \max \{\deg D - \ell(D) + 1 \,|\, D \in Div(K)\}.$$

One has the following theorem

Theorem 1.1.10 (Riemann-Roch Theorem)**.** *If D is a divisor of K/k such that $\deg D > 2g - 2$, then*

$$\ell(D) = \deg D + 1 - g.$$

1.1.3 Ramifications in Galois extensions of function fields

Consider now an algebraic function field K and assume its field of constants $k = \mathbb{F}_q$ is finite. We briefly recall some important properties satisfied by a finite separable function field extension L of K.

We say that a place Q of L lies over a place P of K whenever $\mathcal{M}_P = \mathcal{O}_P \cap \mathcal{M}_Q$. We indicate this by $Q|P$. Chosen a uniformizer t_P at P, the positive integer $e(Q|P) = v_Q(t_P)$ is called the *ramification index* of Q over P. We say that Q is *unramified* if $e(Q|P) = 1$, otherwise we say that Q is *ramified*. In particular it is *totally ramified* if $e(Q|P) = [L : K]$. Moreover the ramification of Q can be *wild* or *tame* whenever the characteristic p of $\mathbb{F}_q = \mathbb{F}_{p^n}$ divides the ramification index or not.
Let $\mathcal{F}_Q$ and $\mathcal{F}_P$ the residue fields of Q and P respectively. The extension $\mathcal{F}_Q/\mathcal{F}_P$ is finite and the degree $f(Q/P) = [\mathcal{F}_Q : \mathcal{F}_P]$ is called *relative degree* of Q over P. Ramification indexes and relative degrees of places $R \,|\, Q \,|\, P$ in a function fields tower $K \subseteq L \subseteq L'$ of finite separable extensions, satisfy

$$e(R|P) = e(R|Q)e(Q|P) \qquad \text{and} \qquad f(R|P) = f(R|Q)f(Q|P).$$

Moreover the fundamental relation holds

$$\sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) = [L : K],$$

where Q_i for $i = 1, \ldots, r$ are all places of L lying over P.
We say that a place P of K *splits completely* over L if there are exactly

$[L : K]$ places over it, i.e. if both ramification index and relative degree are trivial for any of the places lying over P.
In particular if the extension L/K is Galois, the Galois group $Gal(L/K)$ acts transitively on the places of L: $\sigma(Q) = \{\sigma(x) : x \in Q\}$ is a conjugate place of Q by $\sigma \in Gal(L/K)$. Thus one can show that for a place P of K all ramification indexes and relatives degrees of the places of L lying over P are equal. Moreover if r is the number of places of L lying over P then one has $re(P)f(P) = [L : K]$.

Ramifications of a function field extension L/K are bounded by the following formula.

Proposition 1.1.11 (Hurwitz genus formula)**.** *Let L/k' be a finite separable extension of K/k. Then*

$$2g_L - 2 = \frac{[L : K]}{[k' : k]}(2g_K - 2) + \deg\mathrm{Diff}(L/K),$$

where g_L and g_K are the genera of L and K respectively.

Here $\mathrm{Diff}(L/K) = \sum_P \sum_{Q|P} d(Q|P)Q$ is the *different* of the extension L/K. It is a divisor of the function field L, where the second sum runs over the places Q of L lying over the places P of K. Only the ramified places of L appear in the support of $\mathrm{Diff}(L/K)$. Indeed the following proposition on the *different exponent* $d(Q|P)$ of Q over P holds

Proposition 1.1.12. *For a place Q of L lying over a place P of K one has*

i) $d(Q|P) = e(Q|P) - 1$ if Q is tamely ramified (or unramified);

ii) $d(Q|P) > e(Q|P) - 1$ if Q is wildly ramified.

1.1.4 Decomposition and inertia groups

Let L/K a finite Galois extension of Galois group $Gal(L/K)$ and let Q a place of L lying over the place P of K.

Definition 1.1.13. *The* decomposition group *of Q is defined as the stabilizer of Q in $Gal(L/K)$*

$$D(Q|P) = \{\sigma \in Gal(L/K) \,|\, \sigma(Q) = Q\}.$$

In the Galois correspondence the fixed field of $D(Q|P)$ is called the *decomposition field* of P.

Each $\sigma \in Gal(L/K)$ provides an isomorphism

$$\begin{array}{rccc} \overline{\sigma}: & \mathcal{O}_Q/\mathcal{M}_Q & \to & \mathcal{O}_{\sigma(Q)}/\mathcal{M}_{\sigma(Q)} \\ & \overline{z} & \mapsto & \overline{\sigma(z)}, \end{array}$$

for any place Q of L. Here $z \in \mathcal{O}_Q$ and $\overline{z}$ is the residue class of z in the residue class field $\mathcal{F}_Q = \mathcal{O}_Q/\mathcal{M}_Q$ of Q. The isomorphism leaves $\mathcal{F}_P$ pointwise fixed, so that we have a map $\sigma \to \overline{\sigma}$ from $Gal(L/K)$ to $Gal(\mathcal{F}_Q|\mathcal{F}_P)$ by identifying the finite fields $\mathcal{F}_Q$ and $\mathcal{F}_{\sigma(Q)}$. This map is a group isomorphism.

Proposition 1.1.14. *Let Q a place of L lying over a place P of K. Then the following sequence is exact*

$$1 \longrightarrow I(Q|P) \longrightarrow D(Q|P) \xrightarrow{\phi} Gal(\mathcal{F}_Q|\mathcal{F}_P) \longrightarrow 1\,.$$

Moreover one has $|D(Q|P)| = e(Q|P)f(Q|P)$ and $|I(Q|P)| = e(Q|P)$.

Definition 1.1.15. *The kernel $I(Q|P)$ of the map ϕ is called the* inertia group *of Q. It is hence a normal subgroup of $D(Q|P)$.*

For any place Q of L lying over P the decomposition groups and the inertia groups of the conjugates places of Q are conjugate. More precisely

$$D(\sigma(Q)|P) = \sigma D(Q|P)\sigma^{-1} \quad \text{and} \quad I(\sigma(Q)|P) = \sigma I(Q|P)\sigma^{-1},$$

for any $\sigma \in Gal(L/K)$ and $Q|P$. In particular if L/K is an abelian extension they are equal.

If Q is an unramified place of L lying over a place P of K, then the exact sequence above gives an isomorphism of groups and the decomposition group $D(Q|P)$ of Q turns out to be a cyclic group. In particular there exists a unique generator $\sigma \in D(Q|P)$ such that $\phi(\sigma)$ is the Frobenius morphism $\overline{\sigma}: x \mapsto x^r$, for any x in the residue field of Q if r is the cardinality of $\mathcal{F}_P$. This element σ is called the *Frobenius automorphism* $\operatorname{Frob} Q$ of Q, and it is characterized by the property that $\sigma(x) \equiv x^r \mod \mathcal{M}_Q$ for all $x \in \mathcal{O}_Q$.

If L/K is an abelian extension, then the Frobenius of Q does not depend on Q but only on the place P of K lying under Q. So we can denote it by $\operatorname{Frob} P$ and finally state a very useful result.

Proposition 1.1.16. *Let L/K be an abelian extension and let K' be a subfield of L/K. An unramified place P of K splits completely over K' if and only its Frobenius automorphism $\operatorname{Frob} P$ belongs to $Gal(L/K')$.*

1.2 Class field theory for function fields

Let K be a algebraic function field defined over the finite field $\mathbb{F}_q$.

1.2.1 Completions and ramification groups

For any place P of the function field K consider the (unique) *completion* K_P of K with respect to the normalized discrete P-adic valuation v_P. We denote by O_P the subring of elements x of K_P for which $v_P(x) \geq 0$. This corresponds to the completion of the discrete valuation ring $\mathcal{O}_P$. Also O_P has a unique maximal ideal generated by a uniformizer t_P at P. One can prove that any element x of K_P can be uniquely expressed by a formal Laurent series expansion

$$x = \sum_{n=r}^{\infty} x_n t_P^n \quad \in \mathbb{F}_{q^d}[[t_P]],$$

where $r \in \mathbb{Z}$. In particular the elements in the ring O_P are formal Taylor series expansions. Viceversa, any such a series with $a_r \neq 0$ represents a non-zero element of K_P such that $v_P(x) = r$. This also gives an isomorphism $O_P/(t_P) \to \mathcal{F}_P$ between the constants of K_P (the elements of valuation zero) and the residue class field $\mathcal{F}_P \simeq \mathbb{F}_q^d$ of the place P, where d is the degree of P.

Let L be a finite Galois extension of K and Q a place of L lying over a place P of K. One can show that the Q-adic valuation on L is the unique extension of the P-adic valuation to a discrete normalized valuation on L. We denote by L_Q the Q-adic completion of L. Since $\sigma(O_Q) = O_{\sigma(Q)}$ for any element $\sigma \in Gal(L/K)$, we have that σ induces a K_P isomorphism $L_Q \to L_{\sigma(Q)}$. If $\sigma \in D(Q|P)$, the decomposition group of Q over P, then σ induces a K_P-automorphism σ_Q on E_Q. One can prove the following proposition

Proposition 1.2.1. *If L/K is a finite Galois extension, the L_Q/K_P is also a finite Galois extension and the map*

$$\begin{array}{rccc} \mu: & D(Q|P) & \to & Gal(L_Q/K_P) \\ & \sigma & \mapsto & \sigma_Q \end{array}$$

is an isomorphism.

Moreover for each integer $i \geq -1$ one can define the *i-th ramification group of L_Q/K_P* as

$$G_i(L_Q/K_P) = \{\sigma \in Gal(L_Q/K_P) \,|\, v_Q(\sigma(x) - x) \geq i+1 \text{ for all } x \in O_Q\}.$$

The group $G_{-1}(L_Q/K_P)$ is just the Galois group $Gal(L_Q/K_P)$, isomorphic to $D(Q|P)$. Similarly, the group $G_0(L_Q/K_P)$ is called the inertia group of L_Q/K_P and one can prove that it is isomorphic to the inertia group $D(Q|P)$.

1.2.2 The idèle class group and the Artin map

Definition 1.2.2. *The ring of* adèles *of the function field K defined by*

$$\mathbb{A}_K = \{(x_P)_P \in \prod_P K_P \,|\, x_P \in O_P \text{ for all but finitely many places } P\},$$

is the restricted product of the completions K_P's with respect to the O_P's.

$\mathbb{A}_K$ is an abelian ring with unity $(x_P)_P$, such that $x_P = 1$ for any P, and addition and multiplication are defined componentwise. As in K any $0 \neq x$ has only finitely many poles, it makes sense to define (also for $x = 0$) the adèle all of whose components are equal to x. This is called the *principal adèle* of x. This gives the diagonal embedding

$$\begin{array}{ccc} K & \hookrightarrow & \mathbb{A}_K \\ x & \mapsto & (x)_P. \end{array}$$

Definition 1.2.3. *The unit group of $\mathbb{A}_K^*$ is called the group of* idèles *of K:*

$$\mathbb{A}_K^* = \{(x_P)_P \in \prod_P K_P^* \,|\, x_P \in O_P^* \text{ for all but finitely many places } P\}.$$

The restriction of the above diagonal embedding to $K^* \hookrightarrow \mathbb{A}_K^*$ allows to consider K^* as a subroup of $\mathbb{A}_K^*$ by identification with its image.

Definition 1.2.4. *The quotient group*

$$C_K = \mathbb{A}_K^*/K^*$$

is called the idèle class group *of K.*

The group of idèles admits a natural surjective homomorphism

$$\begin{array}{ccc} \mathbb{A}_K & \to & Div(K) \\ (x_P)_P & \mapsto & \sum_P v_P(x_P)P, \end{array}$$

induced by the valuations maps $v_P : K_P \to \mathbb{Z}$. The kernel U of this morphism consists of the idèles that have trivial valuations at all places. The elements of K^* lying in the kernel are precisely the constants $\mathbb{F}_q^*$. The idèle class group fits hence, in the following commutative diagram.

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{F}_q^* & \longrightarrow & K^* & \longrightarrow & Princ(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U & \longrightarrow & \mathbb{A}_K^* & \longrightarrow & Div(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U/\mathbb{F}_q^* & \longrightarrow & C_K & \longrightarrow & Div(K)/Princ(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & 0 & & \end{array}$$

The idèle class group is the main object of study of class field theory. It is a topological group with respect to the quotient topology, where a base of open neighborhoods of unity for the idèle group $\mathbb{A}_K^*$ is given by the groups $\prod_{P\in T} K_P^* \times \prod_{P\notin T} O_P^*$, where T denotes a finite set of places of K. The main results of class field theory give a correspondence between open subgroups of C_K and abelian extensions of the function field K.

Theorem 1.2.5. *Let K be a function field defined over $\mathbb{F}_q$.*

i) (Artin Reciprocity) For any finite abelian field extension L/K, there is a canonical isomorphism

$$\frac{C_K}{\mathfrak{N}_{L/K}} \to Gal(L/K),$$

given by the surjective homomorphism $\theta : C_K \to Gal(L/K)$ of kernel $\mathfrak{N}_{L/K} = (K^* \cdot N_{L/K}(\mathbb{A}_K^*))/K^*$. Here $N_{L/K} : \mathbb{A}_L^* \to \mathbb{A}_K^*$ is the canonical extension of the norm from L to K and the homomorphism θ is induced by the Artin map $\theta_{L/K}$ in (1.1).

ii) (Existence Theorem) For any open subgroup M of C_K of finite index, there exists a unique (in a fixed algebraic closure of K) finite extension L/K such that $M = \mathfrak{N}_{L/K}$.

Let L_Q be the completion of L with respect to the unique normalized discrete valuation v_Q of L extending v_P. Then the *global Artin map*

$$\begin{aligned} \theta_{L/K} : \quad \mathbb{A}_K^* &\to Gal(L/K) \\ (x_P)_P &\mapsto \prod_P \theta_P(x_P), \end{aligned}$$

is defined as product of *local Artin reciprocity maps*

$$\theta_P : K_P^* \to Gal(L_Q/K_P) \simeq D(P) \hookrightarrow Gal(L/K), \tag{1.1}$$

satisfying the following properties:

i) θ_P is a surjective map and the kernel is given by the norms of L_Q^* in K_P^*;

ii) if K_P is unramified in L_Q then $\theta_P(x) = \mathrm{Frob}\, P^{v_P(x)}$ for any $x \in K_P^*$, where $\mathrm{Frob}\, P$ is the Frobenius automorphism in $Gal(L/K)$;

iii) the unit group O_P^* of K_P^* is mapped onto the inertia group $I(P)$ of P in $Gal(L/K)$.

Each local map θ_P determines hence the global splitting behavior of P over L/K. Thus for a place P of K we have:

i) P is unramified in L/K if and only if $O_P^* \subseteq H$,

ii) P splits completely in L/K if and only if $K_P^* \subseteq H$,

for H a subgroup of $\mathbb{A}_K^*$ containing K^* such that $M = H/K^*$ and $Gal(L/K) \simeq C_K/M$.

Moreover Galois correspondence apply to the subgroups of C_K: given any two finite abelian extensions L/K and L'/K in a fixed algebraic closure of K, one has $L \subseteq L'$ if and only if $\mathfrak{N}_{L'/K} \subseteq \mathfrak{N}_{L/K}$.

1.2.3 Ray class fields

There are some special abelian extensions of a function field K that correspond to particular subgroups of the idèle class group C_K. Let $D = \sum_P n_P P$ a rational effective divisor of K and define

$$U_D = \left\{ (x_P)_P \in U \;\middle|\; x_P \equiv 1 \mod t_P^{n_P} \right\},$$

where t_P is a uniformizer at P. Then U_D is an open subgroup of the idèle group $\mathbb{A}_K^*$. The maximal abelian extension L_D/K where all places in the support of D ramify has Galois group isomorphic to $C_K/(K^* \cdot U_D)$. Moreover, let S be a finite non empty set of places of K disjoint from the support of D. There exists a unique subfield L_D^S of L_D for which the Galois group is isomorphic to the quotient of $C_K/(K^* \cdot U_D)$ by the group generated by the K_P^*'s for any P in S. It is the maximal finite abelian extensions of K over which all places lying in the support of D ramify and all rational places in S split completely. This kind of field is called *ray class field* of conductor D. The corresponding finite quotient of C_K is called the *ray class group*. The field of constants of L_D^S is a cyclic extension of $\mathbb{F}_q$ of degree d equal to the greatest common divisor of the degrees of the places in S. Thus if S consists only of rational places of K, then L_D^S has $\mathbb{F}_q$ as its field of constants.

Theorem 1.2.6 (Conductor Theorem)**.** *Let L/K a finite abelian extension of function fields in a fixed algebraic closure of K and let S be a finite non-empty set of places of K such that all places in S split completely in L/K. Let moreover D be the conductor of the extension L/K, then L is a subfield of L_D^S. If moreover D' is an effective divisor of K such that* $\operatorname{supp} D' \cap S = \emptyset$ *and $L \subseteq L_{D'}^S$, then $D' \geq D$.*

The hardest part is to give an explicit description of the Galois group of a ray class field extension. Let K the function field of a curve X defined over

$\mathbb{F}_q$, and denote by $Pic(X)$ the Picard group of X isomorphic to the divisor class group $Div(K)/Princ(K)$ of K. For any arbitrary divisor D of K one has the exact sequence

$$1 \longrightarrow U/U_D \longrightarrow C_K/U_D \longrightarrow Pic(X) \longrightarrow 0\,. \tag{1.2}$$

For the group U/U_D one can give the following explicit description

$$U/U_D \simeq \bigoplus_{P\,\in\,\mathrm{supp}\,D} \mathbb{F}_q^{\deg P}[[t_P]]^*/\{u\,:\,u\equiv 1 \bmod t_P^{n_P}\}.$$

We want to give a description of the Galois group $Gal(L_D^S/K)$ in a situation which frequently arises in applications. Let

$$O_S^* = \{x \in K \,|\, v_P(x) = 0 \text{ for all } P \notin S\}$$

denote the group of S-units of K. Moreover let π_P denote an idèle all of whose coordinates are equal to 1, but the one at P which is a uniformizer t_P at P. Then we have the following lemma.

Lemma 1.2.7. *Let K the algebraic function field of a curve X defined over $\mathbb{F}_q$, S a finite non empty set of rational places of K and D a rational divisor of K such that $suppD \cap S = \emptyset$. Let L be the maximal ray class field extension of K of conductor D in which all places of S split completely. Under the assumption that the group $Pic(X)$ is generated by the points in S, the following isomorphism holds*

$$Gal(L/K) \simeq U/U_D O_S^*.$$

Proof. Denote by $Div_S(K)$ the subgroup of $Div(K)$ having support disjoint from S. Let $Princ_S(K)$ be the subgroup of principal divisors of $Div_S(K)$. The cokernel $Pic_S(X)$ of the map $Princ_S(K) \to Div_S(K)$ is the quotient of the group $Pic(X)$ modulo the classes of the points in S, which is trivial by assumption. Similarly to what done above one has the following commutative diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & O_S^* & \longrightarrow & K^* & \longrightarrow & Princ_S(K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U\langle\pi_P\rangle_{P\in S} & \longrightarrow & \mathbb{A}_K^* & \longrightarrow & Div_S(K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U\langle\pi_P\rangle_{P\in S}/O_S^* & \longrightarrow & C_K & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

The snake lemma gives an isomorphism map in the bottom row

$$\psi : U\langle \pi_P \rangle_{P\in S}/O_S^* \to \mathbb{A}_K^*/K^* = C_K.$$

The ray class group of conductor D is the quotient of C_K by the subgroup U_D, as in (1.2). Since the points in S have to split in L, the Galois group $Gal(L/K)$ is hence a quotient of the ray class group by $\langle \pi_P \rangle_{P\in S}$. Thus $Gal(L/K) \simeq \mathbb{A}_K^*/(K^* \cdot U_D\langle \pi_P \rangle_{P\in S})$, and by the isomorphism ψ the latter group is isomorphic to $U\langle \pi_P \rangle_{P\in S}/(U_D\langle \pi_P \rangle_{P\in S}O_S^*) \simeq U/U_D O_S^*$. □

Chapter 2

Uniqueness of optimal curves over $\mathbb{F}_2$

2.1 Introduction

Consider a projective, smooth and absolutely irreducible curve C of genus g defined over a finite field $\mathbb{F}_q$. An upper bound for the number of $\mathbb{F}_q$-rational points of C is given by the following (cf. [Sti], Section V.2):

Theorem 2.1.1 (Hasse - Weil Bound)**.**
The number $\#C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational places of a genus g curve is bounded by

$$\#C(\mathbb{F}_q) \leq q + 1 + [2g\sqrt{q}], \tag{2.1}$$

where $[x]$ denotes the integral part of the real number x.

As soon as the genus g of C increases with respect to the cardinality of the finite field $\mathbb{F}_q$, this bound is no more sharp and, as Serre has shown (cf. [S], pg. Se Th 38), better bounds can be obtained adapting Weil's explicit formula to function fields of curves. Indeed let $\Psi(t) = \sum_{n=1}^{\infty} c_n t^n$ be a polynomial such that

$$1 + \Psi(\theta) + \Psi(\theta^{-1}) \geq 0, \qquad \text{for all } \theta \in \mathbb{C},\ |\theta| = 1.$$

For any choice of real non-negative coefficients c_n one has that the the number of rational points of genus g curve defined over $\mathbb{F}_q$ satisfies

$$\#C(\mathbb{F}_q) \leq \frac{g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}{\Psi(q^{-1/2})},$$

Good choices of c_n are those that minimize this upper bound for $\#C(\mathbb{F}_q)$. For example, for $q = 2$, by choosing Ψ such that

$$1 + \Psi(t) + \Psi(t^{-1}) = \frac{1}{c}(1 + x_1(t + t^{-1}) + x_2(t^2 + t^{-2}) + x_3(t^3 + t^{-3}))^2,$$

where $c = 1 + 2{x_1}^2 + 2{x_2}^2 + 2{x_3}^2$, $x_1 = 1$, $x_2 = 0.7$ and $x_3 = 0.2$, one has the estimate $\#C(\mathbb{F}_2) \leq 0.83g + 5.35$. Oesterlé's linear programming method optimizes the choice of $\psi(t)$ (cf. also [S] and [E]). For $g \geq 2$ this improves the Hasse-Weil bound as shown in the row of Table 2.1 marked by Serre-Oesterlé.

Next, it is of interest to consider the quantity

$$N_q(g) := \max\{\#C(\mathbb{F}_q) \,|\, \text{for a genus } g \text{ curve } C \text{ defined over } \mathbb{F}_q\}, \qquad (2.2)$$

i.e. the actual maximum number of $\mathbb{F}_q$-rational points that a genus g curve can have, and give the following definition:

Definition 2.1.2. *A curve C of genus g defined over a finite field $\mathbb{F}_q$ is said to be an* optimal *curve if the number of its $\mathbb{F}_q$-rational points equals $N_q(g)$.*

Several methods have been developed in order to determine $N_q(g)$, improving the Hasse-Weil bound and providing examples of optimal curves over $\mathbb{F}_q$ for fixed values of the genus g and of the cardinality of the finite field $\mathbb{F}_q$. The progress in characteristic 2 and 3 and for genus $g \leq 50$ is listed in the tables [G-V]: in particular the values of $N_2(g)$ for low genus g have been determined by Serre in [S1] (see also [S] for more details), giving examples of curves having exactly a number of $\mathbb{F}_2$-rational points attaining the bounds in the third row of Table 2.1. These examples consist of abelian coverings of curves over $\mathbb{F}_2$, whose algebraic function fields can be constructed as ray class fields. We display Serre's results on $N_2(g)$ in Table 2.1.

g	0	1	2	3	4	5	6	7	8	9	10	11	12
Hasse - Weil	3	5	8	11	14	17	19	22	25	28	31	34	36
Serre - Oesterlé	5	6	6	7	8	9	10	11	11	12	13	14	15
$N_2(g)$	3	5	6	7	8	9	10	10	11	12	13	14	$14-15$

Table 2.1: Bounds on the number of $\mathbb{F}_2$-rational points of a genus g curve

Notice that Serre's estimate for the number of $\mathbb{F}_2$-rational points of a genus 7 curve is 11. Serre has been able to determine $N_2(7)$ by giving first an example of genus 7 curve having 10 rational points and next proving that there is no genus 7 curve with 11 rational points (cf. [S] Se Th 38a). On the other hand for genus 12, while it is known that a curve exists having 14 rational points, one still can not prove whether there exists or not a curve attaining the bound of 15. This means that $N_2(12)$ has not been determined yet.

We focus our attention on optimal curves defined over the finite field $\mathbb{F}_2$ having genus $1 \leq g \leq 6$. In Section 2.3 and in Section 2.8 we present for

completeness Serre's ray class field constructions giving proof of existence of the optimal genus g curves in the table. Moreover we determine the Zeta function associated to each of these curves, by means of the arithmetic information provided by the constructions of their function fields.
In Section 2.4 on the other hand, adapting some results and techniques due to Serre, we completely determine the Zeta function of a general optimal curve of genus $g = 1, \ldots, 5$, i.e. without assuming it is an abelian covering of a given curve.

Proposition 2.1.3. *An optimal curve C of genus $g = 1, \ldots, 5$ has a unique Zeta function and it is as follows:*

1) $g = 1$, *hence* $\#C(\mathbb{F}_2) = 5$*:*

$$Z(t) = \frac{2t^2 + 2t + 1}{(1 - 2t)(1 - t)};$$

2) $g = 2$, *hence* $\#C(\mathbb{F}_2) = 6$*:*

$$Z(t) = \frac{4t^4 + 6t^3 + 5t^2 + 3t + 1}{(1 - 2t)(1 - t)};$$

3) $g = 3$, *hence* $\#C(\mathbb{F}_2) = 7$*:*

$$Z(t) = \frac{8t^6 + 16t^5 + 18t^4 + 15t^3 + 9t^2 + 4t + 1}{(1 - 2t)(1 - t)};$$

4) $g = 4$, *hence* $\#C(\mathbb{F}_2) = 8$*:*

$$Z(t) = \frac{(2t^2 + t + 1)(2t^2 + 2t + 1)(4t^4 + 4t^3 + 2t^2 + 2t + 1)}{(1 - 2t)(1 - t)};$$

5) $g = 5$, *hence* $\#C(\mathbb{F}_2) = 9$*:*

$$Z(t) = \frac{(2t^2 + 1)(2t^2 + 2t + 1)^2(4t^4 + 4t^3 + 2t^2 + 2t + 1)}{(1 - 2t)(1 - t)}.$$

A priori it is not true that there exists a unique possibility for the Zeta function of a genus g curve if we only know the number of its $\mathbb{F}_q$-rational points. The quantity $\#C(\mathbb{F}_q)$ just allows to determine the coefficient of the linear term of the numerator of the Zeta function, which is given by $\#C(\mathbb{F}_q) - (q + 1)$ (see Section 2.2 for more on the Zeta function of a curve). In fact for genus 6 we do not have uniqueness anymore.

Proposition 2.1.4. *An optimal genus 6 curve C defined over $\mathbb{F}_2$ (hence $\#C(\mathbb{F}_2) = 10$) has one of the following Zeta functions:*

$$a) \quad Z(t) = \frac{(2t^2+1)(2t^2+2t+1)(16t^8+40t^7+52t^6+50t^5+39t^4+25t^3+13t^2+5t+1)}{(1-2t)(1-t)},$$

$$b) \quad Z(t) = \frac{(2t^2-t+1)(2t^2+2t+1)(4t^4+6t^3+5t^2+3t+1)^2}{(1-2t)(1-t)}.$$

Moreover two curves having the same Zeta function are in general not isomorphic. Our final results state that the considered optimal curves are unique up to isomorphism:

Proposition 2.1.5. *An optimal curve over $\mathbb{F}_2$ of genus g is unique up to isomorphism, for $g = 1, \ldots, 5$. In particular its function field is always isomorphic to the ray class field of the genus g optimal curve of Section 2.3.*

A slightly more sophisticated approach is needed for the genus $g = 6$ case. Combining recent results due to Howe and Lauter (cf. [H-L]) with methods of Galois theory (see Section 2.5 and Section 2.6), we prove the following result.

Proposition 2.1.6. *There are two optimal curves C_a and C_b over $\mathbb{F}_2$ of genus 6 and each of them is unique up to isomorphism. In particular*

a) the curve C_a, having Zeta function as in a) of Proposition 2.1.4, is isomorphic to the optimal genus 6 curve whose function field is described as ray class field in Proposition 2.3.8;

b) the curve C_b, having Zeta function as in b) of Proposition 2.1.4, is isomorphic to an unramified degree 5 cyclic covering of the unique genus 2 curve Y having Zeta function

$$Z(t) = \frac{(2t^2 - t + 1)(2t^2 + 2t + 1)}{(1 - 2t)(1 - t)},$$

where the two rational places of Y fixed by the hyperelliptic involution split completely.

Finally in Section 2.8 we provide an example of two non-isomorphic genus 7 optimal curves over $\mathbb{F}_2$, by constructing a ray class field having among its subfields the function fields of two genus 7 optimal curves whose Zeta functions are different. We do not know if they are the only examples of genus 7 optimal curves defined over $\mathbb{F}_2$.

2.2 Background

We recall that the curves considered are always projective, smooth and absolutely irreducible curves defined over a finite field $\mathbb{F}_q$, though we refer to them simply as *curves*. In particular we deal with *optimal* curves in the sense of Definition 2.1.2. In this subsection we present some background that is necessary for the rest of the note.

2.2.1 Ray class fields

Serre gives explicit constructions of curves having a number of $\mathbb{F}_2$-rational points that meets the upper bound presented in the row tagged as Serre-Oesterlé in Table 2.1. These constructions give hence a description of optimal curves over $\mathbb{F}_2$. In Section 2.3 and in Section 2.8 these examples for genus $g = 1, \ldots, 7$ are presented. The main idea is to exhibit those curves as abelian coverings over $\mathbb{F}_2$ of low genus curves by constructing the corresponding abelian extensions of function fields as ray class fields. One begins by fixing a base curve X over $\mathbb{F}_2$ of genus g_X, a non empty set S of rational points of X and an effective rational divisor $D = \sum_P n_P P$ of X, such that $\mathrm{supp}D \cap S = \emptyset$. Next one looks for a convenient finite abelian covering $Y \to X$, i.e. a separable surjective map corresponding, by pull back, to a finite abelian Galois extension of the function fields L/K. One wants all places of K in $\mathrm{supp}D$ to ramify over the function field L of Y and all places of K in S to split completely over L. In this way the curve Y turns out to be defined over $\mathbb{F}_2$ and has $|Gal(L/K)|$ rational points lying over each point of X in S and one rational point lying over each rational point of X in the support of D that is totally ramified. The genus g_Y of Y can be determined by a variant of the Hurwitz formula (where the different is replaced by an analogous of the product-discriminant formula for number fields, cf. [G] pg. 128):

$$2g_Y - 2 = |Gal(L/K)|(2g_X - 2) + \sum_{\chi} \deg D(\chi),$$

where $\chi : Gal(L/K) \to \mathbb{C}^*$ is a character of $Gal(L/K)$, i.e. a group homomorphism, and $D(\chi)$ denotes the conductor of the cyclic subextension of L fixed by $\ker \chi$.

Class field theory explains the splitting behavior of the places of X giving a description of these abelian function fields extensions in terms of the idèle class group of K: this is the quotient group $C_K = \mathbb{A}_K^*/K^*$ of the group of idèles of K

$$\mathbb{A}_K^* = \Big\{(x_P) \in \prod_P K_P^* \;\Big|\; x_P \in O_P^* \text{ for all but a finite number of places } P\Big\}.$$

Here K_P denotes the P-adic completion of K and O_P its group of units. The main result of class field theory is that to any open finite index subgroup M of C_K there exists a unique finite abelian extension L/K (in a fixed algebraic closure of K), such that the Galois group $Gal(L/K)$ is isomorphic to the quotient C_K/M. The isomorphism is induced by the global Artin map. For any choice of the rational divisor $D = \sum_P n_P P$, let

$$U_D = \Big\{(x_P) \in \prod_P O_P^* \;\Big|\; x_P \equiv 1 \bmod {t_P}^{n_P}\Big\},$$

an open subgroup of the idèle group $\mathbb{A}_K^*$. Then for a non-empty finite set of rational places S disjoint from the support of D, there exists a finite abelian extension L/K corresponding to a finite quotient of $C_K/(K^* \cdot U_D)$ by the image of the group $\langle K_P^* \rangle_{P \in S}$. This is the maximal finite abelian extension of K where the places in the support of D ramify and the places in S split completely. Such an abelian extension is called ray class field of conductor D. More on the subject can be found in [Au], [L1], [N-X], [S], [Sch].

2.2.2 Zeta function and real Weil polynomial of a curve

We are interested in the study of the Zeta function of a genus g curve C over $\mathbb{F}_q$ in the form of a rational function on $\mathbb{Q}$

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

where

$$\begin{aligned} L(t) &= \prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha_i}t) \\ &= q^g t^{2g} + b_{2g-1}t^{2g-1} + \ldots + b_1 t + 1 \end{aligned}$$

is a polynomial in $\mathbb{Z}[t]$ of degree $2g$. The reciprocal roots $\alpha_i \in \mathbb{C}$ are pairwise conjugate and satisfy $|\alpha_i| = \sqrt{q}$ for all $i = 1, \ldots, 2g$.
We compute the Zeta function of a curve C by determining the numbers $a_d = |\{P \,|\, P \text{ is a place of } C \text{ such that } \deg P = d\}|$ of places of C of degree $d = 1, \ldots, g$. In particular a_1 is equal to the number $\#C(\mathbb{F}_q)$ of rational places the curve C over the field $\mathbb{F}_q$. The first $g+1$ coefficients of the series expansion

$$(1-qt)(1-t)Z(t) = \frac{(1-qt)(1-t)}{\prod_{d=1}^{g}(1-t^d)^{a_d}} + O(t^{g+1}) = L(t)$$

coincide with the first $g+1$ coefficients of $L(t)$. The other coefficients of $L(t)$ are determined by $b_{2g-i} = q^{g-i}b_i$, for $1 \leq i \leq g$.

We sum up information on the number a_d of places of degree d of a curve C for $d = 1, 2, 3, \ldots$, in the d-th coordinate of the vector $a(C) = [a_1, a_2, a_3, \ldots]$.

Moreover to a curve C having $L(t)$ as numerator of it Zeta function, we associate the so-called real Weil polynomial

$$h(t) = \prod_{i=1}^{g}(t - \mu_i).$$

This is a polynomial in $\mathbb{Z}[t]$ of degree g, having all real roots $\mu_i = \alpha_i + \overline{\alpha_i} \in [-2\sqrt{q}, 2\sqrt{q}]$ for all $i = 1, \ldots, g$. The real Weil polynomial of a curve has hence the property that all roots of its derivatives also lie in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. The real Weil polynomial of a genus g curve C is related to $L(t)$ by

$$t^g L(1/t) = h(t + q/t).$$

We define a monic degree g polynomial

$$h(t) = t^g + c_{g-1}t^{g-1} + \ldots + c_1 t + c_0 \ \in \ \mathbb{Z}[t]$$

to be a *candidate* real Weil polynomial for a genus g curve defined over $\mathbb{F}_q$ if it satisfies the following three properties:

1. the trace is $c_{g-1} = \#C(\mathbb{F}_q) - (q+1)$,
2. the polynomial $h(t)$ and all its derivatives have all roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$,
3. the polynomial $L(t) = t^g h(1 + qt^2)$ satisfies

$$L(t) + O(t^{g+1}) = (1-t)(1-qt)\prod_{i=1}^{g} \frac{1}{(1-t^d)^{a_d}} + O(t^{g+1}),$$

   with all $a_d \geq 0$.

Following an idea of Serre (cf. [S]), one can turn the problem of determining the Zeta function of C into the problem of determining the real Weil polynomial of C.

2.2.3 Related theorems

Once computed a list of candidate real Weil polynomials for a genus g curve defined over a finite field $\mathbb{F}_q$, there may be some polynomials in the list for which there exists no curve. The following results allow most of the time to discard some of the polynomials in the list that lack of properties that an actual real Weil polynomial of a curve should have. The first theorem is due to Serre:

Theorem 2.2.1. (cf. [S], page *Se 11* and cf. [L], Lemma 1)
Let $h(t)$ be the real Weil polynomial of a curve C over $\mathbb{F}_q$. Then $h(t)$ cannot be factored as $h(t) = h_1(t)h_2(t)$, with $h_1(t)$ and $h_2(t)$ non-constant polynomials in $\mathbb{Z}[t]$ such that the resultant of $h_1(t)$ and $h_2(t)$ is ± 1.

Further generalizations of this Theorem have been proved by Howe and Lauter.

Theorem 2.2.2. (improvement of Theorem 1 *b*) in [H-L] by further unpublished work, cf. [H])
Let $h(t) = h_1(t)h_2(t)$ be the real Weil polynomial of a curve C over $\mathbb{F}_q$, where $h_1(t)$ and $h_2(t)$ are coprime non-constant factors in $\mathbb{Z}[t]$. Let r be the reduced resultant of the radical of $h_1(t)$ and the radical of $h_2(t)$. If $r = \pm 2$. Then, there exists a degree 2 map from C to a curve C' over $\mathbb{F}_q$. The curve C' has either $h_1(t)$ or $h_2(t)$ as real Weil polynomial.

Theorem 2.2.3. (cf. [H-L], Theorem 1 and Proposition 13)
Let $h(t) = (t - \mu)h_2(t)$ be the real Weil polynomial of a curve C over $\mathbb{F}_q$, where $t - \mu$ is the real Weil polynomial of an elliptic curve E and $h_2(t)$ a non-constant polynomial in $\mathbb{Z}[t]$ coprime with $t-\mu$. If $r \neq \pm 1$ is the resultant of $t - \mu$ and the radical of $h_2(t)$, then C admits a map of degree dividing r to an elliptic curve isogenous to E.

We recall that the reduced resultant of two polynomials f_1 and $f_2 \in \mathbb{Z}[x]$ is defined to be the non-negative generator of the ideal $\mathbb{Z} \cap (f_1, f_2)$. To compute the reduced resultant of to coprime polynomials f_1 and f_2 one can compute Bézout's identity $g_1(x)f_1(x) + g_2(x)f_2(x) = 1$ in $\mathbb{Q}[x]$ and then clear denominators.

2.3 Ray class fields constructions of function fields of optimal curves

Let $\mathbb{P}^1$ denote the projective line over $\mathbb{F}_2$. It has 3 rational points: we denote them by P_0, P_1 and P_∞. According to the Hasse-Weil bound this is an example of optimal genus 0 curve. Every optimal genus 0 curve is isomorphic to $\mathbb{P}^1$ since it has $\mathbb{F}_2(x)$ as field of functions. The Zeta function of $\mathbb{P}^1$ is

$$Z(t) = \frac{1}{(1-2t)(1-t)}.$$

2.3.1 On the optimal elliptic curve

We prove in this subsection some properties satisfied by an optimal genus 1 curve over $\mathbb{F}_2$ and by its abelian extensions. In Section 2.4 we also prove that there is a unique optimal genus 1 curve satisfying these properties.

Proposition 2.3.1. *There exists a degree 2 extension of the function field of $\mathbb{P}^1$ of conductor $4P_\infty$, in which the rational places in $S = \{P_0, P_1\}$ split completely. This is the function field of a genus 1 curve having 5 rational points over $\mathbb{F}_2$. The Zeta function of this curve is*

$$Z(t) = \frac{2t^2 + 2t + 1}{(1-2t)(1-t)}. \tag{2.3}$$

Proof. Let $S = \{P_0, P_1\}$ and consider the abelian extension of the the function field of $\mathbb{P}^1$ of conductor $4P_\infty$ in which the points in S are split. By class field theory, the Galois group G of such an extension is isomorphic to the quotient of the group $R = \mathbb{F}_2[[t]]^*/\{u : u \equiv 1 \mod t^4\} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2$ by the image in R of the S-units group O_S^*, where t is a uniformizer at P_∞. Consider the principal divisors

$$\begin{aligned}(x) &= P_0 - P_\infty,\\ (x+1) &= P_1 - P_\infty,\end{aligned}$$

where $x = 1/t$. Then we can take

$$\frac{x}{x+1} = \frac{1}{1+t} = 1 + t + t^2 + t^3 + O(t^4)$$

as generator for O_S^*, which by Dirichlet's Theorem has rank $|S| - 1 = 1$. Its image in R generates a subgroup of order 4. Thus G has order 2 and the corresponding double covering of $\mathbb{P}^1$ is a curve having $N = 2 \cdot |S|2 + 1 = 5$ rational points over $\mathbb{F}_2$. Its genus g, given by the Hurwitz formula $2g - 2 = 2(2\cdot 0 - 2) + 4$, is thus 1. By the Hasse-Weil bound, this construction provides hence an optimal elliptic curve E over $\mathbb{F}_2$.
Since the genus of E is 1, the number of its rational points is enough to determine the Zeta function of E. The numerator is the degree $2g = 2$ polynomial $2t^2 + at + 1$, where a is given by $N = q + 1 + a$ for $q = 2$. Hence $a = 5 - 2 - 1 = 2$ and the Zeta function is as in (2.3). □

Remark 2.3.2. We will often refer to this elliptic curve in the rest of the note, hence for convenience we denote it by E. From the Zeta function it is easy to compute that E has no places of degree two nor three, as well as 5 places of degree four and 4 places of degree five. We sum up this an further information in the vector

$$a(E) = [5, 0, 0, 5, 4, 10, 20, \ldots]. \tag{2.4}$$

We can view E as a smooth cubic in $\mathbb{P}^2$ of affine equation

$$y^2 + y = x^3 + x \tag{2.5}$$

and, in terms of this equation, we denote the 5 rational points of E as

$$P_0 = P_\infty, \quad P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,0), \quad P_4 = (1,1). \tag{2.6}$$

For future reference, we also state here a Lemma concerning some abelian coverings of E.

Lemma 2.3.3. *An abelian covering of E of conductor $4P_\infty$ or $2P_\infty + 2P_1$, in which all points in $S = \{P_2, P_3, P_4\}$ split completely, is necessarily trivial.*

Proof. We begin by factoring some principal divisors of E:

$$\begin{aligned}(x) &= P_1 + P_2 - 2P_\infty, \\ (x+1) &= P_3 + P_4 - 2P_\infty, \\ (y) &= P_1 + 2P_3 - 3P_\infty, \\ (y+1) &= P_2 + 2P_4 - 3P_\infty, \\ (x+y) &= 2P_1 + P_4 - 3P_\infty.\end{aligned} \tag{2.7}$$

Eliminating P_1 and P_∞ from these relations we obtain the following principal divisors, which are generated by S-units:

$$\begin{aligned}\left(\frac{y+1}{y}\frac{x}{x+1}\right) &= 2P_2 + P_4 - 3P_3, \\ \left(\frac{x+y}{y}\frac{x+1}{x}\right) &= 2P_4 - P_3 - P_2.\end{aligned}$$

Choose $t = x/y$ as a uniformizer at P_∞. Then $1/x = t^2 + O(t^3)$ and $1/y = t^3 + O(t^4)$. Dividing the equation of E by x^3 we obtain the equation $1 + 1/x^2 = 1/x^2 \cdot 1/t + 1/x \cdot 1/t^2$. This easily implies that $1/x = t^2 + O(t^4)$. Finally we express the units in terms of the parameter t:

$$\begin{aligned}\frac{y+1}{y}\frac{x}{x+1} &= \left(1+\frac{1}{y}\right)\left(1+\frac{1}{x}\right)^{-1} = (1+t^3)(1+t^2) + O(t^4), \\ \frac{x+y}{y}\frac{x+1}{x} &= \left(1+\frac{x}{y}\right)\left(1+\frac{1}{x}\right) = (1+t)(1+t^2) + O(t^4).\end{aligned} \tag{2.8}$$

By class field theory the Galois group G of an abelian covering of E of conductor $2P_\infty + 2P_1$ is isomorphic to a subgroup of the quotient group $R = \mathbb{F}_2[[t]]^*/\{u : u \equiv 1 \mod t^2\} \times \mathbb{F}_2[[x]]^*/\{u : u \equiv 1 \mod x^2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ modulo the image in R of the S-units. Since the image in R of the unit in 2.8 generates $\mathbb{F}_2[[t]]^*/\{u : u \equiv 1 \mod t^2\}$, the Galois group should have order 2 or be trivial. On the other hand a double covering of E would have genus satisfying $2g - 2 = 4$, hence $g = 3$ and $2 \cdot |S| + 2 = 8$ rational points, which is not allowed by Serre's estimate in Table 2.1. Hence the Galois group is trivial.
Similarly the Galois group G' of a covering of conductor $4P_\infty$ is isomorphic to a subgroup of $R' = \mathbb{F}_2[[t]]^*/\{u : u \equiv 1 \mod t^4\} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2$ modulo the image of the S-units. The computation in 2.8 shows that the image of the S-units generate the whole group R' and hence that G' is trivial. □

2.3.2 On higher genus curves

In this section we give examples of ray class fields that are abelian extensions of the rational function field $\mathbb{F}_2(x)$ or of the function field of the elliptic curve

E defined over $\mathbb{F}_2$. These ray class fields are function fields of optimal curves defined over $\mathbb{F}_2$ of genus $g = 2, \ldots, 6$. By means of class field theory we compute also the Zeta function of these curves.

Proposition 2.3.4. *Let Q be a place of degree three of $\mathbb{P}^1$. There exists a degree 2 extension of the function field of $\mathbb{P}^1$ of conductor $2Q$, in which all points in $S = \{P_0, P_1, P_\infty\}$ are split. This is the function field of a genus 2 curve having 6 rational points over $\mathbb{F}_2$. Its Zeta function is*

$$Z(t) = \frac{4t^4 + 6t^3 + 5t^2 + 3t + 1}{(1-2t)(1-t)}. \tag{2.9}$$

Proof. The projective line $\mathbb{P}^1$ has 2 places of degree three over $\mathbb{F}_2$, one of uniformizer $x^3 + x + 1$ and the other one of uniformizer $x^3 + x^2 + 1$. Let Q be any of these places and let $S = \{P_0, P_1, P_\infty\}$ consist of all rational points of $\mathbb{P}^1$. There exists a degree 2 covering C of $\mathbb{P}^1$ of conductor $2Q$ in which all points in S are split. The curve C has then 6 rational points and its genus g satisfies $2g - 2 = -2 \cdot 2 + 6$, so that $g = 2$.
Indeed, by class field theory, the Galois group of the corresponding function fields extension is isomorphic to the quotient group of $R = \mathbb{F}_{2^3}[[t]]^*/\{u : u \equiv 1 \mod t^2\}$ modulo the image in R of the S-unit group. This quotient is a group of order 2. In order to perform this computation we take $t = x^3 + x + 1$ as uniformizer at Q (the case where $t = x^3 + x^2 + 1$ is similar). The group R is then isomorphic to $\mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$: one write R as $R = \{a + bt \mod t^2 : a \in \mathbb{F}_8^*, b \in \mathbb{F}_8\}$ and take as generators α, a primitive 7-th root of unity and root of $x^3 + x + 1$, $1 + t$, $1 + \alpha t$ and $1 + \alpha^2 t$ respectively. Consider then the principal divisors generated by S-units

$$\begin{aligned} (x) &= P_0 - P_\infty, \\ (x+1) &= P_1 - P_\infty. \end{aligned}$$

Since $x \not\equiv 1$ modulo $x^3 + x + 1$, its image in R generates the 7-part of R and we are just left with the computation of the images of the S-units in the 2-part of R. Elements in the 2-part of R have the form $1 + bt$, with $b \in \mathbb{F}_2[x]/(x^3 + x + 1) \simeq \mathbb{F}_8$. Hence the 2-part image of the S-units in R is the same as the image of their 7-th powers: indeed $(a+bt)^7 \equiv (a+bt)^6(a+bt) \equiv a^6(a + bt) \equiv 1 + a^6 bt \mod t^2$. Thus the images of the 7-th powers of the S-units generate a group isomorphic to a subgroup of the additive group $\mathbb{F}_2[x]/(x^3 + x + 1)$. Here the computation of

$$\begin{aligned} x^7 - 1 &\equiv (x-1)(x^3 + x^2 + 1)(x^3 + x + 1) \\ &\equiv (x+1)(x^2 + x + t)t \\ &\equiv (x+1)(x^2 + x)t \\ &\equiv t \mod t^2 \end{aligned}$$

shows that $x^7 = 1 + t$ in R. In a similar way

$$\begin{aligned}(x+1)^7 - 1 &\equiv x(x^3+x^2+1)(x^3+x+1)\\ &\equiv x(x^2+x+t)t\\ &\equiv x(x^2+x)t\\ &\equiv (x^2+x+1)t \mod t^2\end{aligned}$$

so that $(x+1)^7 = 1 + (x^2+x+1)t$ in R. This shows that the Galois group is isomorphic to the additive group

$$\frac{\mathbb{F}_2[x]/(x^3+x+1)}{\langle 1, x^2+x+1\rangle}, \tag{2.10}$$

which is indeed a group of order 2.
In order to determine the Zeta function of the genus 2 curve C it is enough to determine the number of its degree two places a_2. This depends on the behavior of the only degree two place of $\mathbb{P}^1$. The latter indeed cannot ramify, since it does not appear in the support of the conductor, but it still can either split into 2 points or be inert. If the first case occurs, the image in the ray class group 2.10 of its uniformizer x^2+x+1 has to be trivial. Consider the image of the 7-th power of x^2+x+1:

$$\begin{aligned}(x^2+x+1)^7 &\equiv (x^{16}+x^8+1)/(x^2+x+1)\\ &\equiv (x^2+x^8+1)/(x^2+x+1)\\ &\equiv 1 + (x^8+x)/(x^2+x+1) \mod t^2,\end{aligned}$$

where we used that $x^{16} \equiv x^2$ modulo t^2 (since t divides x^7-1 and hence t^2 divides $x^{14}-1$). Now

$$\begin{aligned}x^8 + x \;=\; x(x^7-1) &\equiv x(x+1)(x^3+x^2+1)t\\ &\equiv x(x+1)(x+x^2)t\\ &\equiv xt \mod t^2,\end{aligned}$$

and hence

$$\begin{aligned}(x^2+x+1)^7 &\equiv 1 + x/(x^2+x+1)\,t\\ &\equiv 1 + (x+1)t \mod t^2.\end{aligned}$$

Now the degree two place of $\mathbb{P}^1$ splits completely if and only if $x+1$ belongs to the additive group $\langle 1, x^2+x+1\rangle$. But this is not the case and hence $a_2 = 0$ and the Zeta function of C is (2.9). □

Proposition 2.3.5. *Let Q be a place of $\mathbb{P}^1$ of degree three. There exists a degree 7 extension of the function field $\mathbb{P}^1$ of conductor Q, in which $S = \{P_\infty\}$*

is split. This is the function field of a genus 3 *curve with* 7 *rational points over* $\mathbb{F}_2$*. Its Zeta function is*

$$Z(t) = \frac{8t^6 + 16t^5 + 18t^4 + 15t^3 + 9t^2 + 4t + 1}{(1-2t)(1-t)}. \tag{2.11}$$

Proof. Let $S = \{P_\infty\}$ and let Q be a place of $\mathbb{P}^1$ of degree three. There exists a degree $7 = \#\mathbb{F}_8^*$ covering C of $\mathbb{P}^1$ of conductor Q in which P_∞ splits completely. Indeed denote by t a uniformizer at one of the 2 places of $\mathbb{P}^1$ of degree three. Then the Galois group of the associated function field extention is isomorphic to the group $\mathbb{F}_{2^3}[[t]]^*/\{u : u \equiv 1 \mod t\} \simeq \mathbb{F}_8^* \simeq \mathbb{Z}_7$, since the group of the S-units is trivial by Dirichlet's unit theorem. The genus g of C satisfies $2g - 2 = -7 \cdot 2 + 6 \cdot 3$, so that $g = 3$. Thus, since Serre's estimate for the upper bound of the number of $\mathbb{F}_2$-rational points of a genus 3 curve is 7, the curve C has at least and hence precisely 7 rational points and it is an optimal genus 3 curve.
In order to compute the Zeta function of C we use class field theory. We represent the Galois group of the above extension as $G = \big(\mathbb{F}_2[x]/(x^3+x+1)\big)^*$ and consider the image in G of uniformizers of places of degree two and three of $\mathbb{P}^1$. In particular we have that a place P having as uniformizer an irreducible polynomial $g(x) \in \mathbb{F}_2[x]$ splits completely over C if and only if $g(x) \equiv 1 \mod x^3 + x + 1$. Since the uniformizer $x^2 + x + 1$ of the only degree two place of $\mathbb{P}^1$ is not 1 modulo $x^3 + x + 1$, we have that $a_2 = 0$. Similarly the uniformizer $x^3 + x^2 + 1$ of the degree three place of $\mathbb{P}^1$ different from Q is not 1 modulo $x^3 + x + 1$. Hence $a_3 = 1$, the only contribution being given by Q itself. The values of $N = a_1 = 7$, $a_2 = 0$ and $a_3 = 1$ determine the Zeta function of C to be as in (2.11). □

Proposition 2.3.6. *There exists a double covering of* E *of conductor* $4P_\infty + 2P_1$*, in which all points in* $S = \{P_2, P_3, P_4\}$ *are split. This is a genus* 4 *curve having* 8 *rational points over* $\mathbb{F}_2$*. Its Zeta function is*

$$Z(t) = \frac{(2t^2 + t + 1)(2t^2 + 2t + 1)(4t^4 + 4t^3 + 2t^2 + 2t + 1)}{(1-2t)(1-t)}. \tag{2.12}$$

Proof. Consider abelian coverings C of E of conductor $4P_\infty + 2P_1$ in which all points in $S = \{P_2, P_3, P_4\}$ are split. The degree of this covering is at least 2 and, by Lemma 2.3.3, exactly 2. Thus one has a curve C with $3 \cdot 2 + 2 = 8$ rational points and genus g satisfying $2g - 2 = 0 + 6$, so that $g = 4$. The curve C is hence an optimal curve of genus 4.
By Remark 2.3.2, we know that E has no places of degree two nor three and 5 places of degree four. Hence, since no rational point of E is inert on C, the curve C does not have any place of degree two nor three either. We consider now the parametric form for the Zeta function of C that can be recovered from the values of $N = a_1 = 8$, $a_2 = 0$, $a_3 = 0$:

$$Z(t) = \frac{16t^8 + 40t^7 + 56t^6 + 56t^5 + \alpha t^4 + 28t^3 + 14t^2 + 5t + 1}{(1-2t)(1-t)}$$

where $\alpha \in \mathbb{Z}$ and the associated real Weil polynomial

$$h(t) = t^4 + 5t^3 + 6t^2 - 2t + (\alpha - 48).$$

Since C is a covering of the curve E, its Zeta function must be divisible by the Zeta function of E (cf. [A-P]). Thus its real Weil polynomial must be divisible by the real Weil polynomial $t + 2$ of E. Hence, since $h(-2) = 0$ implies $\alpha = 44$, the Zeta function of C is precisely (2.12). □

Proposition 2.3.7. *There exists a degree* 8 *abelian covering of* $\mathbb{P}^1$ *of conductor* $4P_0$*, in which* P_∞ *is split. This is a genus* 5 *curve with* 9 *rational points over* $\mathbb{F}_2$*. Its Zeta function is*

$$Z(t) = \frac{(2t^2+1)(2t^2+2t+1)^2(4t^4+4t^3+2t^2+2t+1)}{(1-2t)(1-t)}. \tag{2.13}$$

Proof. Let $S = P_\infty$ and consider abelian coverings of $\mathbb{P}^1$ of conductor kP_0 in which P_∞ is split. The Galois group of these extensions is always isomorphic to the ray class group $\mathbb{F}_2[[x]]^*/\{u : u \equiv 1 \mod x^k\}$ since the groups of S-units is trivial. Then for $k = 2$ one has a covering of degree 2 and for $k = 3$ a covering of degree 4. The Galois group of the function field extension associated to the latter covering is isomorphic to $\mathbb{Z}_4$. Finally for $k = 4$ one has a covering C of degree 8 and in this case the corresponding Galois group is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. In the latter case the genus g of the curve C satisfies then $2g - 2 = -8 \cdot 2 + 2 + 2 \cdot 3 + 4 \cdot 4$, so that $g = 5$. The curve C has at least and hence, by Serre's improvements in Table 2.1, precisely 9 rational points. It is an optimal curve of genus 5.
It is not difficult to determine the Zeta function of C using class field theory. We start considering $x+1$ as uniformizer at P_1. Since the image of $x+1$ has order 4 in the ray class group, the inertia degree of P_1 is 4. In other words, P_1 splits into 2 degree four places over C. Similarly for the only degree two place of $\mathbb{P}^1$: the image in the ray class group of the uniformizer $x^2 + x + 1$ is an element of order 4. Hence the only degree two place of $\mathbb{P}^1$ splits into 2 places of degree eight over C. Consider now the 2 places of degree three of $\mathbb{P}^1$ of uniformizers $x^3 + x^2 + 1$ and $x^3 + x + 1$: the order of their images in the ray class group is 2 and 4 respectively. Hence the first place splits into 4 places of degree six and the second splits into 2 places of degree twelve over C. About the places of degree four of $\mathbb{P}^1$ it is of interest just the number of those splitting completely over C: but since the only degree four polynomial $x^4 + 1$ equivalent to 1 modulo x^4 is not irreducible, there are no places of degree four of $\mathbb{P}^1$ splitting completely over C. Similarly the are no degree five irreducible polynomials congruent to 1 modulo x^4 and hence no degree five places of $\mathbb{P}^1$ splitting completely over C. In conclusion the values $N = a_1 = 9$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$ and $a_5 = 0$ determine completely the Zeta function as in (2.13). □

Proposition 2.3.8. *Let Q be a place of degree five of E. There exists a double covering of E of conductor $2Q$, in which all 5 rational points of E split completely. This is a genus 6 curve having 10 rational points over $\mathbb{F}_2$. Its Zeta function is*

$$Z(t) = \frac{(2t^2+1)(2t^2+2t+1)(16t^8+40t^7+52t^6+50t^5+39t^4+25t^3+13t^2+5t+1)}{(1-2t)(1-t)}. \qquad (2.14)$$

Proof. Let Q denote a place of degree five of E. There is a quadratic cover C of E of conductor $2Q$ in which all 5 rational points of E split completely. As a consequence, the curve C has 10 rational points and it genus g satisfies $2g-2 = 0 + 2\cdot 5$ by the Hurwitz formula, so that $g = 6$.
By class field theory the Galois group of the associated abelian function fields extension is isomorphic to the ray class group $R = \mathbb{F}_{2^5}[[t]]^*/\{u : u \equiv 1 \mod t^2\}$ modulo the group generated by the image of the S-unit group in R. Here t is a uniformizer at Q and S denotes the set of 5 rational places of E. The S-units x, $x+1$, y and $x+y$, whose effective divisors are listed in (2.7), generate the whole S-unit group. We first choose a degree five place Q of E. Let α be a zero of x^5+x^3+1. Then the $\mathbb{F}_{2^5}$-rational point of coordinates $P = (\alpha, \alpha^4)$ is a point of E. The prime ideal of the coordinate ring $\mathbb{F}_2[x,y]/(y^2+y+x^3+x)$ corresponding to P is $\mathfrak{p} = (x^5+x^3+1, y+x^4)$. Considering the divisor $(x^5+x^3+1) = P+P'-10P_\infty$, where P' is the point of E of coordinate (α, α^4+1), we can take the function $t = x^5+x^3+1$ as uniformizer at Q. Actually there are 4 places of degree five over E, but a different choice for Q would lead to the same results.
Next consider again the S-units: since the image of x in the ray class group R is not trivial modulo t, it generates the 31-part of R. Thus we compute the 2-part of R generated by the image of the S-units similarly to the genus 2 case. We consider the 31-st power modulo t^2 of each generator: this is an element of R of the form $1+at$, where a is in the additive group $\mathbb{F}_2[x]/(x^5+x^3+1)$. A computer calculation shows that the first two uniformizers x and $x+1$ satisfy

$$\begin{aligned} x^{31} &\equiv 1+t \mod t^2, \\ (x+1)^{31} &\equiv 1+(x^4+x^3+1)t \mod t^2. \end{aligned}$$

For the S-unit y we first consider that from the equation of E one has $y^{31} = y^{32}/y = (v+y)/y = 1+v/y$, where $v = \mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(x^3+x) = (x^3+x)^{16}+(x^3+x)^8+(x^3+x)^4+(x^3+x)^2+(x^3+x) \equiv 0 \mod t$. Since $y \equiv x^4$ modulo t, we compute

$$(y^{31}-1)/t \equiv \frac{v}{x^4 t} \equiv x^4+1 \mod t.$$

In a similar way

$$\begin{aligned} (y+x)^{31} &= (y+x)^{32}/(y+x) = (y^{32}+x^{32})/(y+x) \\ &= (v+y+x^{32})/(y+x) \\ &= 1+(v+x^{32}+x)/(y+x), \end{aligned}$$

so that a computer calculation yields

$$((y+x)^{31}-1)/t \equiv \frac{v+x^{32}+x}{(x^4+x)t} \equiv x^2+1 \mod t.$$

Hence the images of the four S-units in $K = \mathbb{F}_2[x]/(x^5+x^3+1)$ are 1, x^4+x^3+1, x^4+1, x^2+1 and they are $\mathbb{F}_2$-independent. These polynomials generate the hyperplane of polynomials of K having no linear term. Hence the Galois group has order 2 and a place of E splits completely over C if and only if the image of Frobenius in K has linear term equal to zero.

We want to determine the Zeta function of C: we already know that $N = a_1 = 10$ and that $a_2 = a_3 = 0$ because E does not have any place of degree two nor three. We perform computations now to determine the images in K of the uniformizers of degree four and five places of E and hence a_4 and a_5 using class field theory. A computer calculation shows all factorizations of $g(x)^2+g(x)+x^3+x$ for all polynomials $g(x) \in \mathbb{F}_2[x]$ of degree $d \leq 3$. This allows us to determine the coordinates of representatives of the 5 places of degree four of E as:

i) $Q_1 = (a, a^3)$ and $Q_2 = (a, a^3+1)$, where $a^4+a^3+a^2+a+1 = 0$;

ii) $Q_3 = (b, b^2+b^3)$ and $Q_4 = (b, b^2+b^3+1)$, where $b^4+b^3+1 = 0$;

iii) $Q_5 = (c, d)$, where $c^2+c+1 = 0$ and $d^4+d+1 = 0$;

while the corresponding prime ideals are

i) $(x^4+x^3+x^2+x+1, y+x^3)$ and $(x^4+x^3+x^2+x+1, y+x^3+1)$;

ii) $(x^4+x^3+1, y+x^3+x^2)$ and $(x^4+x^3+1, y+x^3+x^2+1)$;

iii) (x^2+x+1, y^4+y+1).

As uniformizers we can take $y+x^3$, $y+x^3+1$, $y+x^3+x^2$, $y+x^3+x^2+1$ and x^2+x+1 respectively and compute their images in $\mathbb{F}_2[x]/(x^5+x^3+1)$. For the first 4 places we consider in general

$$\begin{aligned}(y+f(x))^{31} &= (y^{32}+f(x)^{32})/(y+f(x)) \\ &= 1+(v+f(x)^{32}+f(x))/(y+f(x)), \end{aligned} \tag{2.15}$$

and compute $((v+f(x)^{32}+f(x))/t)/(y+f(x))$ modulo t. For $f(x) = x^3$ and $f(x) = x^3+1$ we have that the images of the two places in $i)$ are x^2+x and $x+1$ respectively. While for $f(x) = x^3+x^2$ and $f(x) = x^3+x^2+1$ we compute the images of the two places in $ii)$ to be x^4+x^3+x and x^3+x^2+x respectively. Still we have to deal with the place of uniformizer x^2+x+1. We have

$$((x^2+x+1)^{31}-1)/t \equiv x^4+x+1 \mod t,$$

in other words $(x^2+x+1)^{31} \equiv 1+(x^4+x+1)t \mod t^2$. Since all polynomials x^2+x, $x+1$, x^4+x^3+x, x^3+x^2+x and x^4+x+1 have a linear term, none of them lies in the group generated by the image of the S-units in K. Hence none of the degree four places of E splits over C and $a_4(C)=0$.
Consider now the 4 places of degree five of E. They are the places of coordinates

i) (a, a^4) and (a, a^4+1), where $a^5+a^3+1=0$;

ii) (b, b^4+b) and (b, b^4+b+1), where $b^5+b^4+b^3+b^2+1=0$.

The corresponding prime ideals are

i) $(x^5+x^3+1, y+x^4)$ and $(x^5+x^3+1, y+x^4+1)$;

ii) $(x^5+x^4+x^3+x^2+1, y+x^4+x)$ and $(x^5+x^4+x^3+x^2+1, y+x^4+x+1)$.

The first place in $i)$ is the place Q that ramifies in C by definition. As uniformizer of the second place in $i)$ we take $y+x^4+1$. Since $y \equiv x^4$ modulo t, this time $y+x^4+1 \equiv 1$ modulo t, so that it is already in the 2-part of the ray class group R and it is not necessary to compute its 31-st power. Hence we have

$$\begin{aligned} y+x^4+1 &\equiv 1+(y+x^4)(y+x^4+1)/(y+x^4+1) \\ &\equiv 1+(x^3+x+x^8+x^4)/(y+x^4+1) \\ &\equiv 1+\frac{(x^3+x)t}{y+x^4+1} \mod t^2. \end{aligned}$$

Since $y \equiv x^4$ modulo t we have that $(y+x^4)/t \equiv x^3+x$ modulo t and hence $y+x^4+1 \equiv 1+(x^3+x)t$ modulo t^2: the polynomial x^3+x has a linear term and hence the degree five place of E of uniformizer y^4+x+1 is not split over C.
As uniformizers of the places in $ii)$ we take $y+x^4+x$ and $y+x^4+x+1$ respectively and a computation similar to (2.15) leads to their images in K: x^2 and $x^4+x^3+x^2+x+1$. Having no linear term, only the first of them splits. Thus $a_5=3$.
Now we consider the parametric form for the Zeta function of C that can be recovered from the values of $N=a_1=10$, $a_2=a_3=a_4=0$ and $a_5=3$:

$$Z(t) = \frac{64t^{12}+9600t^{11}+2640t^{10}+600t^9+108t^8+14t^7+\alpha t^6+300t^5+165t^4+75t^3+27t^2+7t+1}{(1-2t)(1-t)}$$

and the associated real Weil polynomial

$$h(t) = t^6+7t^5+15t^4+5t^3-15t^2-10t+(\alpha-460).$$

Since C is a covering of the curve E, the Zeta function of E divides the Zeta function of C. In other words the real Weil polynomial $t+2$ of E must divide the real Weil polynomial of C. Hence, since $h(-2)=0$ leads to $\alpha=460$, the Zeta function of C is precisely (2.14). □

2.4 Uniqueness of the Zeta function of an optimal curve

The previous section shows the Zeta function of an optimal curve C over $\mathbb{F}_2$ arising as an abelian covering of $\mathbb{P}^1$ or of the elliptic curve E and having genus $1 \leq g \leq 6$. In this section we consider again optimal curves over $\mathbb{F}_2$ of genus $1 \leq g \leq 6$ and we compute their Zeta functions in a general setting. This prevents us to recover information on the number of places of degree $d = 1, \ldots, g$ of the optimal curve using class field theory. To determine Zeta functions we start following the idea of Serre in [S] (cf. pages Se Th 38 and following) in order to get a list of candidate real Weil polynomials for a genus g curve over $\mathbb{F}_2$. Since we know that for each genus g an optimal curve always exists, one of the candidate real Weil polynomials in the list has to correspond to the Zeta function we found in Section 2.3. We use Theorems of Subsection 2.2.3 to determine for which polynomials among the remaining ones there exists no curve.

Proposition 2.4.1. *The real Weil polynomial of any optimal curve X defined over $\mathbb{F}_2$ of genus $g = 1, \ldots, 5$ is as follows.*

1) $g = 1$*:*

$$h(t) = t + 2, \qquad a(X) = [5, 0, 0, 5, 4, 10, \ldots],$$

2) $g = 2$*:*

$$h(t) = t^2 + 3t + 1, \qquad a(X) = [6, 0, 1, 1, 6, 12, \ldots],$$

3) $g = 3$*:*

$$h(t) = t^3 + 4t^2 + 3t - 1, \qquad a(X) = [7, 0, 1, 0, 7, 7, \ldots],$$

4) $g = 4$*:*

$$h(t) = (t + 1)(t + 2)(t^2 + 2t - 2), \qquad a(X) = [8, 0, 0, 2, 4, 8, \ldots],$$

5) $g = 5$*:*

$$h(t) = t(t + 2)^2(t^2 + 2t - 2), \qquad a(X) = [9, 0, 0, 2, 0, 12, \ldots],$$

The vector $a(X) = [a_1, a_2, a_3, \ldots]$ sums up the number a_d of degree d places of X in the d-th entry.

Proof. For genus $g = 1$, the number of rational points $N = 5$ is indeed sufficient to determine completely the real Weil polynomail of X: this is a degree 1 polynomial $h(t) = t - a$, where $N = q + 1 - a$, hence $h(t) = t + 2$. For genus $g = 2, \ldots, 5$, searching for candidate real Weil polynomials of degree g we find only two or three possibilities for each degree. We do with the help of computer calculation implementing the algorithm explained in the introduction on page 17:

$g = 2$:

1. $h_1(t) = t^2 + 3t + 1$, $a(X) = [6, 0, \ldots]$
2. $h_2(t) = (t + 1)(t + 2)$, $a(X) = [6, 1, \ldots]$

$g = 3$:

1. $h_1(t) = t^3 + 4t^2 + 3t - 1$, $a(X) = [7, 0, 1, \ldots]$
2. $h_2(t) = (t + 2)(t^2 + 2t - 1)$, $a(X) = [7, 0, 0, \ldots]$

$g = 4$:

1. $h_1(t) = (t + 1)(t + 2)(t^2 + 2t - 2)$, $a(X) = [8, 0, 0, 2, \ldots]$
2. $h_2(t) = (t^2 + 2t - 1)(t^2 + 3t + 1)$, $a(X) = [8, 0, 1, 0, \ldots]$

$g = 5$:

1. $h_1(t) = t(t + 2)^2(t^2 + 2t - 2)$, $a(X) = [9, 0, 0, 2, 0, \ldots]$
2. $h_2(t) = (t+1)(t^4 + 5t^3 + 5t^2 - 5t - 5)$, $a(X) = [9, 0, 0, 0, 7, \ldots]$
3. $h_3(t) = (t^2 + 3t + 1)(t^3 + 3t^2 - 3)$, $a(X) = [9, 0, 0, 1, 3, \ldots]$

In all cases one can check that all polynomials but the $h_1(t)$'s can not occur by Serre's Theorem 2.2.1: indeed in every case the resultant of the two factors is 1 or -1. □

The Zeta functions related to each real Weil polynomial can now be easily computed from the vectors $a(X)$'s. For convenience they have been listed in Proposition 2.1.3.

The two possibilities for the Zeta functions of a genus 6 optimal curve listed in Proposition 2.1.4 follow from the following result.

Proposition 2.4.2. *An optimal genus* 6 *curve* X *defined over* $\mathbb{F}_2$ *has one of the following real Weil polynomials:*

a) $h(t) = t(t + 2)(t^4 + 5t^3 + 5t^2 - 5t - 5)$, $a(X) = [10, 0, 0, 0, 3, 10, \ldots]$;

b) $h(t) = (t - 1)(t + 2)(t^2 + 3t + 1)^2$, $a(X) = [10, 0, 0, 0, 2, 15, \ldots]$.

Proof. A computer calculation as in the proof of Proposition 2.4.1 reveals that the candidate real Weil polynomials of an optimal genus 6 curve X are the following:

1. $h_1(t) = (t-1)(t+2)(t^2+3t+1)^2$, $a(X) = [10, 0, 0, 0, 2, 15, \dots]$;
2. $h_2(t) = t(t+2)(t^4+5t^3+5t^2-5t-5)$, $a(X) = [10, 0, 0, 0, 3, 10, \dots]$;
3. $h_3(t) = (t^3+3t^2-3)(t^3+4t^2+3t-1)$, $a(X) = [10, 0, 0, 0, 4, 6, \dots]$;
4. $h_4(t) = (t+1)(t+2)(t^2+2t-2)(t^2+2t-1)$, $a(X) = [10, 0, 0, 1, 0, 12, \dots]$.

We consider the list backwards.

a) Polynomial number 4 cannot occur. Since the resultant of the polynomials $t+2$ and $(t+1)(t^2+2t-2)(t^2+2t-1)$ is -2, applying Theorem 2.2.3, we deduce that the genus $g = 6$ curve X admits a degree 2 map to the elliptic curve E that has real Weil polynomial equal to $t+2$. By Remark 2.3.2 the elliptic curve E has 5 places of degree four and X has only one. This means that one of the degree four places of E must ramify in X. In other words the different of the covering $X \to E$ is divisible by $2Q$ for some degree four place Q of E (where the coefficient 2 is forced by wild ramification). By the Hurwitz formula we have that the degree of the different has to be equal to $2g - 2 = 10$. Since $2Q$ already gives a contribution of 8 to the degree of the different, the only possibility for the different is to be equal to $2Q + 2R$, where R is a rational point of E. But this gives a contradiction since all the points of E must be totally split in order to get 10 rational points on X.

b) Number 3 can not occur either by Theorem 2.2.1 since the resultant of the two factors is 1.

c) Of the two remaining polynomials we recognize polynomial number 2 as the real Weil polynomial associated to the genus 6 curve given by the class field theory construction in Proposition 2.3.8: since the double covering $X \to E$ is ramified at precisely one place Q of degree five, the number of places of degree five of X has to be odd. In fact places of degree five of E that are totally split, resp. inert, always give a contribution of 2 places, resp. no points, of degree five on X. Since polynomial number 1 gives $a_5(X) = 2$ and polynomial number 2 gives $a_5(X) = 3$, the right one has hence to be the second. This confirms the computations performed in the proof of Proposition 2.3.8.

d) In Proposition 2.4.3 we construct a genus 6 optimal curve having polynomial number 1 as real Weil polynomial.

□

Proposition 2.4.3. *Let C the genus 2 projective curve defined over $\mathbb{F}_2$ of affine equation $y^2+xy = x^5+x^4+x^2+x$. There exists an unramified cyclic degree 5 covering X of C in which the place at infinity P_∞ and the rational place $P_0 = (0,0)$ of C split completely. The curve X is an optimal genus 6 curve defined over $\mathbb{F}_2$. The Zeta function of X is*

$$Z(t) = \frac{(2t^2-t+1)(2t^2+2t+1)(4t^4+6t^3+5t^2+3t+1)^2}{(1-2t)(1-t)}.$$

Proof. The curve C is a smooth curve defined over $\mathbb{F}_2$, whose equation has the form $y^2+h(x)y = f(x)$, where $h(x)$, $f(x) \in \mathbb{F}_2[x]$ are polynomials of degree $\deg h(x) < g$ and $\deg f(x) = 2g+1$ respectively, for $g = 2$. This kind of curve is called a hyperelliptic curve over $\mathbb{F}_2$ and its genus is precisely $g = 2$ (cf. for example the brief introduction in [M-N]). The curve C has a unique place at infinity P_∞ and 3 more rational places over $\mathbb{F}_2$ of coordinates

$$P_0 = (0,0), \qquad P_1 = (1,0), \qquad P_2 = (1,1).$$

Over $\mathbb{F}_4$ there are 4 more points satisfying the equation of C, namely those of coordinates (a,a), $(a,a+1)$, $(a+1,a)$ and $(a+1,a+1)$, for a such that $a^2+a+1 = 0$. Hence C has 2 places of degree two. From the parameters $a(C) = [4,2,\ldots]$ one can compute the real Weil polynomial of C to be $h(t) = (t-1)(t+2)$ and the numerator of the Zeta function of C to be $L(t) = 4t^4+2t^3+2t^2+t+1$. One has that the class group divisor $Pic^0(C) = Div^0(C)/Princ(C)$ of C has order $L(1) = 10$ and hence $Pic^0(C) \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$.
Consider now the unramified extension of the function field of C where the place P_∞ splits completely. This is a Hilbert class field, i.e. a ray class field of conductor $D = 0$. By class field theory one has the following exact sequence

$$1 \longrightarrow U \longrightarrow C_K \xrightarrow{\psi} Pic(C) \longrightarrow 0\,, \tag{2.16}$$

where ψ is induced by the map $\mathbb{A}_K^* \to Div(C)$, $(x_P)_P \mapsto \sum_P v_P(x_P)P$. By taking quotiens by $U = \ker\psi$ one gets the isomorphism $C_K/U \to Pic(C)$. The quotient of this class group by the subgroup $\langle \mathrm{Frob}P_\infty \rangle \simeq K_{P_\infty}^*/O_{P_\infty}^*$ generated by the Frobenius automorphism $\mathrm{Frob}P_\infty$ of P_∞, is the class group of the maximal non-ramified abelian extension X' of C in which P_∞ splits completely. Indeed one has the following diagram

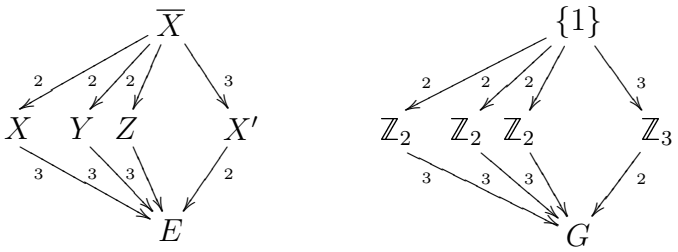
$$\begin{array}{ccccccccc}
 & & 1 & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
1 & \longrightarrow & K^*_{P_\infty}/O^*_{P_\infty} & \xrightarrow{v_{P_\infty}} & & & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
1 & \longrightarrow & C_K/U & \xrightarrow{\psi} & & & Pic(C) & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
1 & \longrightarrow & C_K/U\langle \mathrm{Frob} P_\infty\rangle & \longrightarrow & Pic^0(C) \simeq \mathbb{Z}_2 \times \mathbb{Z}_5 & \longrightarrow & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & 1 & & & & 1 & &
\end{array}$$

Thus the class group associated to the morphism $X' \to C$ is isomorphic to $Pic^0(C) \simeq \mathbb{Z}_5 \times \mathbb{Z}_2$. By class field theory this is also the Galois group of the corresponding finite function fields extension. Now by the Galois correspondence there exists a degree 5 cyclic covering X of C such that the Galois group G of the function fields extension is isomorphic to $\mathbb{Z}_5$ as quotient of $Pic^0(C)$ by its order 2 subgroup. We show that in the function field of X also the rational place P_0 splits completely. This is equivalent to show that the Frobenius of P_0 lies in the subgroup of order 2 of $Pic^0(C)$, so that $\mathrm{Frob}P_0$ is trivial in G. The map $C_K/U\langle \mathrm{Frob}\ P_\infty\rangle \to Pic^0(C)$ sends an idèle class in the class of the associated divisor. Hence if t_{P_0} is a uniformizer at P_0, then the idèle $(\ldots, 1, 1, 1, t_{P_0}, 1, 1, \ldots) \in K^*_{P_0}/O^*_{P_0}$ is sent in the class of $P_0 - P_\infty$. Since $2(P_0 - P_\infty) = (x)$ is a principal divisor it is hence trivial in $Pic^0(C)$. Thus $\mathrm{Frob}P_0$ corresponding to the image of $P_0 - P_\infty$ in the quotient group of order 5 is trivial.
By the Hurwitz formula the curve X has genus g satisfiying $2g-2 = 5(2\cdot 2-2)$. Hence X is a genus 6 curve and it has at least, and by Serre's estimate hence exactly, 10 rational places over $\mathbb{F}_2$. In other words X is an optimal genus 6 curve over $\mathbb{F}_2$. By Proposition 2.4.2 there are only two possibilities for the real Weil polynomial of X. Since X is a covering of the curve C, the real Weil polynomial of C has to divide the real polynomial of X [A-P]. Hence the Zeta function of X is the one corresponding to the real Weil polynomial b) of Proposition 2.4.2. □

2.5 Some remarks on the Galois closure of a degree 3 non-Galois covering of E

This section is an auxiliary section. We present in a more general context some useful results for the proof of Proposition 2.1.6 on genus 6 optimal curves defined over $\mathbb{F}_2$.

Let E be an optimal elliptic curve over $\mathbb{F}_2$ as in Remark 2.3.2 and X a curve over $\mathbb{F}_2$ of genus g such that there exists a morphism $X \to E$ of degree 3, but the function field extension X/E is not normal and hence non-Galois. Consider the curve $\overline{X}$ whose function field is the normal closure of the function field of X with respect to the fucntion field of E. The function field of $\overline{X}$ is now a Galois extension of the function field of E and the corresponding Galois group G isomorphic to S_3. In the Galois correspondence the function field extension associated to the covering $X \to E$ corresponds to one of the 3 non-normal subgroups of S_3 of index three. This also means that there are 2 more curves Y and Z, isomorphic to X, between $\overline{X}$ and E, each of them corresponding to the other 2 subgroups of S_3 of order two. Moreover there is a unique quadratic extension K of $\mathbb{F}_2(E)$, function field of the curve X' which is a double covering $X' \to E$, which correspons to $A_3 \simeq \mathbb{Z}_3$, the unique (normal) subgroup of S_3 of index two. The situation can be described in the following picture:



In the rest of the section we assume that X satisfies two conditions:

1. X is unramified out of the $\mathbb{F}_2$-rational places of E,
2. X doesn't have any place of degree two nor three.

Under the latter hypothesis all places P' of X lying over a rational place P of E must have relative degree $f(P' \,|\, P) = 1$, i.e. their residue field is $\mathbb{F}_2$. Therefore there are only three possibilities for each $\mathbb{F}_2$-rational point P in E:

a) P splits completely over X,

b) P splits into 2 points, one unramified and the other one with ramification index two,

c) P is totally ramified with ramification index three.

In the following we refer to these points as the a-points, the b-points and the c-points of E and denote by a, b, c the number of a-points, b-points and c-points of E respectively. The following lemma describes their splitting behavior over $\overline{X}$ and over X'.

Lemma 2.5.1.

a) The a-points of E split completely over $\overline{X}$ and over X' as well,

b) over each b-point of E there are 3 points over $\overline{X}$ each with ramification index two and 1 point over X' which is totally ramified,

c) the c-points of E are inert over X' giving rise to a degree two place that totaly ramifies over $\overline{X}$.

Proof.

a) Consider one of the a-points P of E. It is totally split over X. Since there are other 2 curves Y and Z, such that their function fields are isomorphic to the function field of X and are subfield of the function field of $\overline{X}$, P is totally split in Y and Z as well. Hence the splitting field of P has to be a subfield of the function field of $\overline{X}$ containing all 3 function fields of the curves X, Y and Z. In other words it has to contain their compositum as well, which is indeed the function field of $\overline{X}$, i.e. the a-points of E split completely over $\overline{X}$. On the other hand, also the function field of the curve X' is contained in the function field of $\overline{X}$ which is the splitting field of P, hence the a-points of E split completely over X'.

b) A b-point P of E has inertia group of order two: indeed one of the two splitting points of X lying over P has ramification index two, and if it ramifies further in $\overline{X}$, then the places of $\overline{X}$ lying over P would have different ramification indices. This is not possible since $\overline{X}$ is a Galois extension of E. Now since the inertia group is a normal subgroup of the decomposition group, also the decomposition group has order two and we can conlude that, over each point of this type, there are 3 points in $\overline{X}$, each with ramificaton index two. Hence P has to be totally ramified over X'.

c) A c-point P of E has inertia group of order three. Indeed it is totally ramified with ramification indeces $e_P(X|E)$ and $e_P(Y|E)$ equal to 3 both in X and in Y. Since the ramification is tame, P ramifies in $\overline{X}$, the compositum of X and of Y, with ramification index $e_P(\overline{X}|E) = lcm\,(e_P(X|E), e_P(Y|E)) = 3$ as well (Abhyankar's Lemma, cf. [Sti] pag. 125). Hence the order of the decomposition group of P can be either six or three. In the first case there is only one place Q in $\overline{X}$ lying over P having relative degree $f(Q|P) = 2$. In the second case there are 2 places Q and Q' in $\overline{X}$ lying over P having residue class field $\mathbb{F}_2$. We show that the second case is impossible. We have $e(Q|P) = e_P(\overline{X}|E) = 3$. This is the order of the inertia group $I(P) = G_0(Q|P)$

of P. Consider now the residue class field of Q and denote it by $\mathcal{F}_Q$. The map

$$\begin{aligned} \psi : \ G_0(Q|P) &\to \mathcal{F}_Q^* \\ \sigma &\to \frac{\sigma(t)}{t} \mod Q \end{aligned}$$

where t is a uniformizer at Q, is a group homomorphism from $G_0(Q|P)$ to the moltiplicative group of $\mathcal{F}_Q$ and the kernel is the 1-th ramification group $G_1(Q|P) := \{\sigma \in Gal(\overline{X}/E) \,|\, v_Q(\sigma(z) - z) \geq 2 \text{ for all } z \in \mathcal{O}_Q\}$ of P (cf. [Sti], page 122-123). In our case the map ψ is injective since the ramification of P is tame. Indeed, since $e(Q|P) = 3$, we have that the different exponent $d(Q|P) = 2$. But the different exponent can be expressed by Hilbert's different formula (cf. [Sti], Theorem III.8.8) as

$$d(Q|P) = \sum_{i=0}^{\infty} (G_i(Q|P) - 1).$$

Since the order of $G_0(Q|P)$ is already 3, its contribution is the only one which is non-trivial, while all G_i's must have order one for $i \geq 1$. Thus $G_0(Q|P)$ is isomorphic to a subgroup of $\mathcal{F}_Q^*$. Since $G_0(Q|P)$ has order three, the residue class field of Q has to be $\mathbb{F}_4$. Hence $f(Q|P) = 2$ and Q is the only place lying over P in $\overline{X}$ and P is inert over X'.

□

Lemma 2.5.2. *The extension X'/E ramifies exactly at the b-points ramifying in X/E.*

Proof. We know from the previous lemma that the a-points and the c-points of E do not ramify over X'. Consider now a place Q of E of degree $d > 1$. X/E is unramified out of the rational places by hypothesis (2) and the same holds for the isomorphic covering Y/E. Since $\overline{X}$ is the compositum of X and Y, Q does not ramify in $\overline{X}$ either (cf. [Sti], Corollary III.8.4 b)). Thus Q is unramified in X' as well. □

Proposition 2.5.3. *Let X be a degree three non-normal covering of E of genus g, unramified out of the $\mathbb{F}_2$-rational places of E, having no places of degree two nor three and such that $b \neq 0$ then the field of functions of X' has constant field equal to $\mathbb{F}_2$ and X' has genus $g' = g - c$.*

Proof. Let K be the field of functions of X'. Suppose the constant field of K is not $\mathbb{F}_2$, then K is a degree 2 constant field extension of $\mathbb{F}_2(E)$ and hence the field of functions of X' has to be $\mathbb{F}_4$. Since by hypothesis there is always at least one b-point P of E which totally ramifies, the residue field of the $\mathbb{F}_2$-rational point of X' lying over P has to be $\mathbb{F}_2$. Now since the residue field

of a place of a function field always contains the constant function field, we have that $\mathbb{F}_2 \supseteq \mathbb{F}_4$. This is a contradiction.
Since locally at any of these b-points the covering $X' \to E$ is isomorphic to $X \to E$, we can compute the different of $X' \to E$ by looking at the extension $X \to E$. We have $2g-2 = \deg \mathrm{Diff}(X/E) = \deg(\mathrm{Diff}(X/E)_{tame}) + \deg(\mathrm{Diff}(X/E)_{wild})$. The contribution to $\mathrm{Diff}(X/E)$ given by the c tame ramified points is $2c$, while the contribution given by the b wildly ramified points is hence $2g-2-2c$. Since X' is not ramified out of the b-points by Lemma 2.5.2, it follows that $2g'-2 = \deg(\mathrm{Diff}(X'/E)) = \deg(\mathrm{Diff}(X/E)_{wild})$, so that $g' = g - c$. □

2.6 Further remarks on genus 6 non-Galois coverings of E

Through the whole section we let X be a genus 6 optimal curve defined over $\mathbb{F}_2$ having Zeta function as in b) of Proposition 2.1.4. We give a series of results on X in terms of Section 2.5 in order to finally prove uniqueness results on genus 6 optimal curves in section 2.7.

Proposition 2.6.1. *The curve X is a non-Galois extension of degree 3 of the optimal elliptic curve E, unramified out of the $\mathbb{F}_2$-rational places of E.*

Proof. We recall that the real Weil polynomial of X is $h(t) = (t-1)(t+2)(t^2+3t+1)^2$ and the parameters of X are $a(X) = [10,0,0,0,2,15,\dots]$. Since the resultant of the polynomials $t+2$ and $(t-1)(t^2+3t+1)$ is equal to 3, by Theorem 2.2.3 the curve X admits a morphism of degree 3 to the usual optimal elliptic curve E. Since X has no points of degree two nor three, all places P' of X lying over a rational place P of E must have relative degree $f(P'|P) = 1$, i.e. their residue field is $\mathbb{F}_2$. Therefore, according to the notations of Section 2.5, each of the $\mathbb{F}_2$-rational points in E can be either an a-point, or a b-point or a c-point. Then we have

$$\begin{aligned} a+b+c &= 5 \\ 3a+2b+c &= 10 \end{aligned}$$

and hence

$$2a+b=5 \quad \text{and} \quad a=c.$$

This leaves us with the following three cases:

	a	b	c
I	0	5	0
II	1	3	1
III	2	1	2

In each case the covering $X \to E$ is not a Galois covering. Indeed, since b is never zero, the extension can never be Galois. We show that moreover it has to be unramified outside the $\mathbb{F}_2$-rational places of E. Consider the degree of the different of the function fields extension corresponding to the covering $X \to E$: by the Hurwitz formula the degree of the different has to be $2g-2 = 10$, where $g = 6$ is the genus of X. The a-points of E are unramified by definition. Over each b-point of E lies precisely one ramified point with ramification index 2. Hence the ramification is wild and its contribution to the different is therefore at least 2. Finally the c-points of E are tamely ramified. The contributions to the different that come from the rational points of E are therefore at least $db + 2c$ wiht $d \geq 2$, i.e. at least $5 \cdot 2 = 10$ in case I, at least $3 \cdot 2 + 2 = 8$ in case II and at least $1 \cdot 2 + 2 \cdot 2 = 6$ in case III. Since there are no points of degree two, three nor four on X, any other non-rational ramified place of E should have degree strictly larger than 4. But this gives a too large contribution to the different. Hence there are no other places of E ramifying in X but those of degree one. □

The parameters of X are $a(X) = [10, 0, 0, 0, 2, 15, \dots]$. Hence, by the previous Proposition, we have that X is a genus 6 non-Galois covering of E of degree 3 satisfying the two conditions (1) and (2) of Section 2.5.

We can consider now the curve $\overline{X}$ whose function field is the Galois closure of the function field of X with respect to the function field of E.

Lemma 2.6.2. *The behavior of the places of $\overline{X}$ and of the places of X' depends on the behavior of the rational points of E as follows:*

$$\begin{array}{lcll} a_1(\overline{X}) & = & 6a + 3b, & a_1(X') = 2a + b; \\ a_2(\overline{X}) & = & c, & a_2(X') = c; \\ a_3(\overline{X}) & = & 0, & a_3(X') = 0; \\ a_4(\overline{X}) & = & 0, & a_4(X') = 10; \\ a_5(\overline{X}) & = & 0. & \end{array}$$

Proof. By Lemma 2.5.1, the computation of the number of $\mathbb{F}_2$-rational points $a_1(\overline{X})$ and $a_1(X')$ is easily done. The places in X' of degree two are precisely the ones lying over the c-points of E and they are themselves totally ramified in $\overline{X}$. This gives

$$a_2(\overline{X}) = c \qquad \text{and} \qquad a_2(X') = c.$$

Consider now the vectors of the a_i's of E and X, they are:

$$a(E) = [5, 0, 0, 5, 4, ...] \qquad \text{and} \qquad a(X) = [10, 0, 0, 0, 2, 15, ...]$$

It follows at once that $a_3(X') = a_3(\overline{X}) = 0$. Since X has no places of degree two nor four, we have $a_4(\overline{X}) = 0$, which means that the places of degree four

of E are inert in X. Since they are not ramified, their decomposition group has to be cyclic and hence of order 3. Therefore they are split in X' and we have

$$a_4(X') = 2a_4(E) = 2 \cdot 5 = 10.$$

If $a_5(\overline{X})$ is not zero, then one of the points of degree five of E splits completely in $\overline{X}$. This implies that X has at least 3 places of degree five, which is not the case. This proves the lemma. □

More precisely, the following proposition holds:

Proposition 2.6.3. *Let X be a genus 6 optimal curve defined over $\mathbb{F}_2$ having Zeta function*

$$Z(t) = \frac{(2t^2 - t + 1)(2t^2 + 2t + 1)(4t^4 + 6t^3 + 5t^2 + 3t + 1)^2}{(1 - 2t)(1 - t)}.$$

Consider the degree 3 non-Galois morphism $X \to E$, where E is an optimal elliptic curve defined over $\mathbb{F}_2$. Denote by $\overline{X}$ the curve whose function field is the Galois closure of the function field of X with respect to $\mathbb{F}_2(E)$ and by X' the curve whose function field is the quadratic subfield of $\mathbb{F}_2(\overline{X})$. There are two possibilities for the splitting behavior of the $\mathbb{F}_2$-rational points of E and in each case we can determine genus and real Weil poynomial of X' and of $\overline{X}$. They are as follows:

I) All 5 rational points of E are b-points, i.e. they split over X into 2 rational points such that one has ramification index 2 and the other one is unramified.

• The double covering $X' \to E$ is a genus $g' = 6$ curve having parameters

$$a(X') = [5, 0, 0, 10, 4, 20, \ldots]$$

and real Weil polynomial

$$h(t) = t(t + 2)(t^2 - 5)^2.$$

• The Galois closure $\overline{X}$ of X over E is a genus $\overline{g} = 16$ curve having parameters

$$a(\overline{X}) = [15, 0, 0, 0, 0, 30, 0, 30, 60, 96, 120, 340, 720, 1200, 2164, 3960, \ldots]$$

and real Weil polynomial

$$h(t) = t(t + 2)(t - 1)^2(t^2 - 5)^2(t^2 + 3t + 1)^4.$$

II) Of the 5 rational points of E, one is an a-point, i.e. it splits completely over X; 3 are b-points, i.e. they split over X into 2 rational points

such that one has ramification index two and the other one is unramified; one is a c-point, i.e. it is totally ramified over X.

• *The double covering $X' \to E$ is a genus $g' = 5$ curve having parameters*

$$a(X') = [5, 1, 0, 10, 4, \ldots]$$

and real Weil polynomial

$$h(t) = (t+2)(t^2-5)(t^2-2).$$

• *The Galois closure $\overline{X}$ of X over E is a genus $\overline{g} = 15$ curve having parameters*

$$a(\overline{X}) = [15, 1, 0, 0, 0, 18, 0, 42, 60, 108, 120, 334, 720, 1164, 2164, \ldots]$$

and real Weil polynomial

$$h(t) = (t+2)(t-1)^2(t^2-5)(t^2-2)(t^2+3t+1)^4.$$

Proof. Consider the curve X'. From Proposition 2.5.3 we have that its genus $g' = g - c$ and from Proposition 2.6.2 we have that $a(X') = [2a+b, c, 0, 10, \ldots]$. Hence according to the three cases described above:

	a	b	c	g'	$a(X')$
I	0	5	0	6	$[5, 0, 0, 10, \ldots]$
II	1	3	1	5	$[5, 1, 0, 10, \ldots]$
III	2	1	2	4	$[5, 2, 0, 10, \ldots]$

We can easily eliminate case number III since X' would be a genus 4 curve having $N_4 = N + 2a_2 + 4a_4 = 5 + 2 \cdot 2 + 4 \cdot 10 = 49$ rational points over $\mathbb{F}_{2^4}$, while $N_4(4) = 45$ according to the tables [G-V].
A computer calculation implementing the algorithm on page 17, allows us to determine that there is only one candidate real Weil polynomial possible in each case and precisely

I $\quad h(t) = t(t+2)(t^2-5)^2$,

II $\quad h(t) = (t+2)(t^2-5)(t^2-2)$

From the real Weil polynomials of X and X' we can recover the real Weil polynomial of $\overline{X}$ in both cases I and II. We first of all consider the following relation among the Zeta function $Z_{\overline{X}}(t)$ of $\overline{X}$ and the Zeta functions $Z_X(t)$ and $Z_{X'}(t)$ of the curves X and X' respectively:

$$Z_{\overline{X}}(t) = L_X(t)^2 L_{X'}(t) Z_E(t),$$

where here

$$L_X(t) = \frac{Z_X(t)}{Z_E(t)} \quad \text{and} \quad L_{X'}(t) = \frac{Z_{X'}(t)}{Z_E(t)}$$

denote the Artin L-functions of X and X' respectively (cf. for example [R] Chapter 9, in particular Remark 4, pg. 130).
Similarly, for the real Weil polynomials we obtain

$$h_{\overline{X}}(t) = \frac{h_X^2(t)h_{X'}(t)}{h_E^2(t)},$$

from which the genus and the real Weil polynomial of $\overline{X}$ follow as stated. □

2.7 Uniqueness of low genus optimal curves

Proposition 2.4.1 shows the only possible form of a Zeta function of an optimal genus g curve for $1 \leq g \leq 5$. But two curves having the same Zeta function are not isomorphic a priori.
In this section we show that for $g = 1, \ldots, 5$ an optimal genus g curve defined over $\mathbb{F}_2$ is unique up to isomorphism. In particular it is isomorphic to the genus g optimal curve of the construction of Section 2.3. This is what is stated in Proposition 2.1.5. In order to prove this Proposition, we first state and prove some other lemmas that are useful for the genus 3 case.

Lemma 2.7.1. *Let C be a genus 3 curve having 7 rational points over $\mathbb{F}_2$, then*

a) $\mathcal{J}ac(C)$ has an automorphism τ of order 7,

b) τ preserves the polarization of $\mathcal{J}ac(C)$.

Proof. For a curve X defined over $\mathbb{F}_q$ we denote by $\mathcal{J}ac(X)$ the Jacobian variety of X and by V_ℓ the Tate module attached to $\mathcal{J}ac(X)$, where ℓ is a prime number different from the characteristic of $\mathbb{F}_q$. Let $F : V_\ell \to V_\ell$ be the Frobenius map and by $V : V_\ell \to V_\ell$ the Verschiebung map This is the unique map such that $V \circ F = q$. The ring $\mathbb{Z}[F, V]$ is a subring of the endomorphism ring of $\mathcal{J}ac(X)$. Next we let ϕ be the canonical polarization on $\mathcal{J}ac(X)$. Then ϕ can be represented as a non-degenerate alternating form $\phi : V_\ell \times V_\ell \to \mathbb{Q}_\ell$, with values in the ℓ-adic completion of $\mathbb{Q}$. Since $\phi(F(x), F(y)) = q\phi(x, y)$ for every x and y in V_ℓ, by bilinearity of ϕ we have that $\phi(F(x), F(y)) = q\phi(x, y) = \phi(qx, y) = \phi(V(F(x)), y)$. Comparing the first and the latter member of the equality we have that $\phi(z, F(y)) = \phi(V(z), y)$ for any y and z in V_ℓ. In other words V is left adjoint to F with respect to ϕ.

a) We show that for the genus 3 curve C defined over $\mathbb{F}_2$ the ring $\mathbb{Z}[F, V]$ generated by F and V is isomorphic to $\mathbb{Z}[\zeta_7]$, the ring of integers of $\mathbb{Q}(\zeta_7)$. Thus $\mathbb{Z}[\zeta_7]$ is isomorphic to a subring of the endomorphism ring of $\mathcal{J}ac(C)$ and in particular $\mathcal{J}ac(C)$ has an automorphism τ of order

7 corresponding to ζ_7.
By Proposition 2.4.1 the real Weil polyomial of C is $h(t) = t^3 + 4t^2 + 3t - 1$, which is the minimal polynomial of $F + V$. Its discriminant is 49. Hence the corresponding number field is the subfield $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ of degree 3 of $\mathbb{Q}(\zeta_7)$ (cf. [Wa], pg. 16). This can be seen as follows: put $\mu = \zeta_7 + \zeta_7^{-1}$. Now $-\mu - \mu^2 \in \mathbb{Z}[\mu]$ is a root of the polynomial $h(t)$. Since the discriminant of the minimal polynomial $p(t) = x^3 + x^2 - 2x - 1$ of μ is 49 as well, we have that $\mathbb{Z}[-\mu - \mu^2] \simeq \mathbb{Z}[F + V] \simeq \mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$. Now consider the ring generated by Frobenius F and Verschiebung V: the minimal polynomial of F over $\mathbb{Q}[\zeta_7 + \zeta_7^{-1}]$ is the polynomial $t^2 - at + 2$, with $a = -\mu - \mu^2$. Since $1 - \zeta_7 - \zeta_7^5$ is a root of this polynomial, we can conclude that $\mathbb{Z}[F, V] \subseteq \mathbb{Z}[\zeta_7]$. On the other hand $\zeta_7 + \zeta_7^5 = \zeta_7^3(\zeta_7^{-2} + \zeta_7^2)$ is in the ring generated by F and V and $\zeta_7^{-2} + \zeta_7^2 = \mu^2 - 2$ is a unit of $\mathbb{Z}[\mu]$: indeed $(\zeta_7^{-2} + \zeta_7^2)^{-1} = \zeta_7^5 + \zeta_7^2 = -1 - \zeta_7 - \zeta_7^{-1} = -1 - \mu$. Hence $\zeta_7^3 \in \mathbb{Z}[F, V]$ and $\zeta_7 = (\zeta_7^3)^5 \in \mathbb{Z}[F, V]$. This shows that the ring $\mathbb{Z}[F, V]$ is isomorphic to $\mathbb{Z}[\zeta_7]$ the ring of integers of $\mathbb{Q}(\zeta_7)$ as wanted.

b) Let ϕ be a fixed polarization on $\mathcal{J}ac(C)$ as above. Now by bilinearity of ϕ and since V is the complex conjugate of F, the left adjoint to an element τ in $\mathbb{Z}[F, V]$ is its complex conjugate $\overline{\tau}$. Hence in particular we have $\phi(\tau(x), y) = \phi(x, \overline{\tau}(y)) = \phi(x, \tau^{-1}(y))$ for every x, y in V_ℓ and τ the automorphism of $\mathcal{J}ac(C)$ of order 7, since τ is an element of $\mathbb{Z}[F, V]$ of absolute value 1 by point *a*). This implies that $\phi(\tau(x), \tau(y)) = \phi(x, y)$ for every x and y in V_ℓ, i.e. τ preserves the polarization ϕ of $\mathcal{J}ac(C)$.

□

Theorem 2.7.2. ***Torelli Theorem*** *(cf. [W])*
Let X and X' be two curves over a perfect field k.
Let $\sigma : \mathcal{J}ac(X) \to \mathcal{J}ac(X')$ be an isomorphism compatible with the canonical polarizations. Then

a) if X is hyperelliptic, there exists a unique isomorphism $f : X \to X'$ which gives σ;

b) if X is not hyperelliptic, there exists a unique isomorphism $f : X \to X'$ and a unique $\varepsilon \in \{\pm 1\}$ such that f gives $\varepsilon\sigma$.

Corollary 2.7.3. If σ is an automorphism of $\mathcal{J}ac(X)$ preserving the polarization, then either σ or $-\sigma$ comes from an automorphism of X.

Proof of Proposition 2.1.5. We divide the proof into five parts, each for a different value of the genus of the curve.

1) A genus 1 curve C over $\mathbb{F}_2$ is an elliptic curve. This means that there is a separable morphism $C \to \mathbb{P}^1$ of degree 2. Since C has 5 rational

points the only possibility is that 2 of the three rational points of $\mathbb{P}^1$ splits completely and one of them ramifies over C. Hence this is an abelian extension of degree 2 and the conductor has to be $2P + D$, where P is the wildly ramified point of C and D a rational divisor of C. By the Hurwitz formula $\deg D = 2$. Since the ramification of the only degree two place of $\mathbb{P}^1$ would not be tame and no other rational point of C but P ramifies, we have $D = 2P$. Hence C is an abelian extension of $\mathbb{P}^1$ of conductor $4P$, where the other two rational points of $\mathbb{P}^1$ are split.
If $P = P_\infty$ we have the construction of Proposition 2.3.1. We can always reduce to this case choosing for P any of the other two rational points of $\mathbb{P}^1$: in fact $\mathbb{P}^1$ has an automorphism group acting doubly transitively on its 3 rational points.

It is possible to determine the equation of C supposing, for example, it is the point at infinity of $\mathbb{P}^1$ the ramifying one. First of all such an equation has to be of the form $y^2 + a(x)y = f(x)$, where $a(x)$ and $f(x)$ are polynomials in $\mathbb{F}_2[x]$, the first of degree 0 or 1 and the latter of degree 3. In order to let ramify only the point at infinity, $a(x)$ has to be 1, hence the equation has the form $y^2 + y = f(x)$. Since the points of $\mathbb{P}^1$ of coordinate $x = 0$ and $x = 1$ have to split, we have that $f(0) = f(1) = 0$ and hence $f(x) = x(x + 1)(x + a)$, where $a \in \mathbb{F}_2$. If $a = 1$ we find the equation $y^2 + y = x^3 + x$ and if $a = 0$ the equation is $y^2 + y = x^3 + x^2$. The two curves indeed turn out to be isomorphic over $\mathbb{F}_2$ by changing coordinates through the map $(x, y) \mapsto (x + 1, y)$.

2) A genus 2 curve C over $\mathbb{F}_2$ is a hyperelliptic curve. Hence we know that there exists a separable double covering $C \to \mathbb{P}^1$. For C to have 6 rational points, all three $\mathbb{F}_2$-rational points of $\mathbb{P}^1$ have to split completely in C. Since, by Proposition 2.4.1, the curve C has only one place of degree three, only 1 of the 2 degree three places Q of $\mathbb{P}^1$ totally ramifies in C. Hence the conductor D of the covering is divided by $2Q$. Moreover by the Hurwitz formula we have $2 \cdot 2 - 2 = 2(2 \cdot 0 - 2) + \deg D$. This implies that the degree of the conductor has to be 6. Thus any genus 2 curve having 6 rational points over $\mathbb{F}_2$ is a double covering of $\mathbb{P}^1$ of conductor $2Q$, where Q is a place of $\mathbb{P}^1$ of degree three, in which all rational points of $\mathbb{P}^1$ are split. This is the class field theory construction we described in Proposition 2.3.4.
The choice of which of the 2 places of degree three of $\mathbb{P}^1$ has to ramify leads to two isomorphic curves. Indeed the $\mathbb{F}_2$-automorphism τ of $\mathbb{P}^1$ sending $x \mapsto 1/x$, sends in particular $Q = (x^3 + x^2 + 1)$ into $Q' = (x^3 + x + 1)$.

3) By Lemma 2.7.1 and by the above Corollary of Torelli's Theorem the

curve C admits an automorphism f of order 7. Indeed if f does not induce τ of order 7 as in the Lemma, but f induces $-\tau$, we can take $f \circ f$ as automorphism of order 7 of C. Then C is a cyclic covering of degree 7 and conductor D of a curve X, that by the Hurwitz formula can only be $\mathbb{P}^1$. Indeed if the genus of X would be $g \geq 2$ one had

$$2 \cdot 3 - 2 = 7(2g-2) + 6 \deg D \geq 14 + 6 \deg D$$

and hence a different of degative degree, which is not possible. If X would be a genus 1 curve than $\deg D = 2/3$, which is not possible since it is not an integer value. By the Hurwitz formula the degree of the conductor D of the cyclic covering over $\mathbb{P}^1$ is then given by $2\,g(C)-2 = 7\,(2\,g(\mathbb{P}^1)-2)+6\deg D$, that is $\deg D = 3$. Since there are 7 points on C, one rational place of $\mathbb{P}^1$ splits completely over C. Hence C has to be a degree 7 covering of $\mathbb{P}^1$ of conductor a place Q of $\mathbb{P}^1$ of degree three where one of the rational points R of $\mathbb{P}^1$ splits completely. It is not difficult to check that different choices for the splitting point R and for the degree three place Q give rise to isomorphic curves. Indeed first we can always reduce to the case $R = P_\infty$ as in Proposition 2.3.5 because the automorphisms group of $\mathbb{P}^1$ acts transitively on the rational points. Next the automorphism $x \mapsto x+1$ fixes the point at infinity and maps one degree 3 place of $\mathbb{P}^1$ into the other one.

4) By Proposition 2.4.1 the real Weil polynomial of an optimal genus 4 curve C over $\mathbb{F}_2$ is $(t+1)(t+2)(t^2+2t-2)$. Since the resultant of the polynomials $t+2$ and $(t+1)(t^2+2t-2)$ is 2, by Theorem 2.2.3, there exists a double covering $C \to E$, where E is the optimal elliptic curve of equation $y^2+y = x^3+x$ we have been dealing with above. The comparison between the two vectors $a(C) = [8,0,0,2,\ldots]$ and $a(E) = [5,0,0,5,4,\ldots]$ gives some additional information on the behavior of the rational points of E in C. Since C has no places of degree two, no rational point of E can be inert in C. To get 8 rational points on C, then, there is only one possibility for the 5 rational points of E: 3 points are split and 2 are totally ramified. Denoting by P and P' the two wildly ramified points, the contribution to the different is at least $2P+2P'$. By the Hurwitz formula we know that the degree of the different has to be 6. Since $\deg(2P+2P') = 4$ and since there are no other rational places of E ramifying, the different, and hence the conductor of the abelian extension, has to be $4P+2P'$ (or $2P+4P'$). Thus any optimal genus 4 curve over $\mathbb{F}_2$ is a double covering of the optimal elliptic curve E of conductor $4P+2P'$, where P and P' are 2 rational points of E, in which the other 3 rational points of E are split. This is the class field theory construction we described in Proposition 2.3.6 when $P = P_\infty$ and $P' = P_1$.

Uniqueness up to isomorphism of C follows (and the case $2P + 4P'$ reduces to the case $4P + 2P'$) from the fact that we can choose for P and P' any two points of E, having E an endomorphism group acting doubly transitively on its 5 rational points: one can map any two rational places of E to any other pair of rational places by an element of the group generated by τ and σ, where $\tau : (x, y) \mapsto (x + 1, x + y + 1)$ is an automorphism of order 4 and σ the endomorphisms of order 5 corresponding to the addition by P_1.

5) By Proposition 2.4.1 a genus 5 optimal curve C defined over $\mathbb{F}_2$ has real Weil polynomial $h(t) = t(t + 2)^2(t^2 + 2t - 2)$. One has moreover that $2 = t(t + 2) - (t^2 + 2t - 2)$ is the generator of the principal ideal $(t(t + 2), t^2 + 2t - 2) \cap \mathbb{Z}$. Hence, by Theorem 2.2.2, a genus 5 optimal curve C is a double covering of a curve Y having real Weil polynomial either $t(t + 2)^2$ or $t^2 + 2t - 2$. But a curve having real Weil polynomial $t(t+2)^2$ would be a genus 3 curve having 7 rational points over $\mathbb{F}_2$: this is impossible by Proposition 2.4.1. Hence Y is a genus 2 curve having 5 rational places and no place of degree two. Every genus 2 curve defined over $\mathbb{F}_2$ is a hyperelliptic curve Y, i.e. it admits a separable $\mathbb{F}_2$-morphism $Y \to \mathbb{P}^1$ of degree 2. Up to $\mathbb{F}_2$-isomorphism there exists a unique hyperelliptic curve having real Weil polynomial $t^2 + 2t - 2$. One can find for example in Maisner and Nart' paper [M-N] (pg. 327) a classification of hyperelliptic curves up to $\mathbb{F}_2$-isomorphisms. In particular for a hyperelliptic curve Y over $\mathbb{F}_2$ having 5 rational points the different of the function fields extension associated to the double covering $Y \to \mathbb{P}^1$ has to be $6P$, where P is a rational point of $\mathbb{P}^1$. By taking $P = P_\infty$ any hyperelliptic curve over $\mathbb{F}_2$ having real Weil polynomial $h(t) = t^2 + 2t - 2$ turns out to be $\mathbb{F}_2$-isomorphic to a projective curve of affine equation $y^2 + y = x^5 + ax^3 + bx^2 + c$ with $a, b, c \in \mathbb{F}_2$. Of the 8 possible equations arising from the choice of the parameters a, b, c, only the equation $y^2 + y = x^5 + x^3$ is the equation of a projective curve having 5 rational points and no place of degree two over $\mathbb{F}_2$.
Since there are 9 rational places over C, only one of the 5 rational places of Y ramifies and the other 4 split completely over C. On the other hand the different of the corresponding function fields extension has degree 4 by the Hurwitz formula. Since ramification is wild the only possibility for the different, and hence for the conductor of the extension, has to be $4P$, where P is the only rational point of Y ramifying over C. Let X' be a curve such that its function field $\mathbb{F}_2(X')$ is the maximal abelian extension of the function field $\mathbb{F}_2(Y)$ of Y of conductor $4P_\infty$ where all other rational places of Y split completely. If $Gal(\mathbb{F}_2(X')/\mathbb{F}_2(Y)) \simeq \mathbb{Z}_2$, then X coincides with X' since X' is unique by class field theory. The class group of conductor $4P$ is isomorphic

to $R = \left(\mathbb{F}_2[[t]]/(t^4)\right)^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$, where t is a uniformizer at the rational place P. By class field theory, the group $Gal(\mathbb{F}_2(X')/\mathbb{F}_2(Y))$ is isomorphic to a quotient of R by the group generated by the Frobenius elements of the splitting rational places. Denote by $P_0 = (0,0)$, $P_0' = (0,1)$, $P_1 = (1,0)$ and $P_1' = (1,1)$ the affine rational places of the curve Y of equation $y^2 + y = x^5 + x^3$. We consider all possible choices for P and show that for $P = P_\infty$ the curve X is indeed unique, while for any other rational P the group $Gal(\mathbb{F}_2(X')/\mathbb{F}_2(Y))$ is trivial.

i) Let $P = P_\infty$ and $t = \frac{y}{x^3}$ a uniformizer at P_∞. Let $S = \{P_0, P_0', P_1, P_1'\}$. Consider the principal divisors

$$\begin{aligned}(y + x^3) &= 5P_0 + P_1 - 6P_\infty,\\ (x^3) &= 3P_0 + 3P_0' - 6P_\infty.\end{aligned}$$

Then the S-unit $g_{P_1} = \frac{y+x^3}{x^3}$ generating the following principal divisor

$$\left(\frac{y + x^3}{x^3}\right) = 2P_0 + P_1 - 3P_0',$$

is a uniformizer at P_1. Its image in R is

$$\frac{y + x^3}{x^3} = 1 + t \bmod t^4.$$

This generates a subgroup of order 4 in R. Consider now the order 4 automorphism σ of Y

$$\begin{aligned}\sigma : Y &\to Y\\ (x, y) &\mapsto (x + 1, y + x^2 + 1),\end{aligned}$$

fixing P_∞ and acting transitively on S. Then $\sigma(g_{P_1})$, $\sigma^2(g_{P_1})$ are S-units and uniformizers at $P_0 = \sigma(P_1)$ and $P_1' = \sigma^2(P_1)$ respectively. Hence their image in R also generates the same subgroup of order 4. Hence the quotient group of R by the S-units group generated by the image of the three linearly independent S-units g_{P_1}, $\sigma(g_{P_1})$ and $\sigma^2(g_{P_1})$ is a group of order 2. It cannot be trivial since also the image of the uniformizer $\sigma^3(g_{P_1})$ of P_0' is in the image of the S-units g_{P_1}, $\sigma(g_{P_1})$ and $\sigma^2(g_{P_1})$.

ii) Let $P = P_0$ and x a uniformizer at P_0. Let $S = \{P_\infty, P_0', P_1, P_1'\}$. Consider the principal divisors

$$\begin{aligned}(y + x^3) &= 5P_0 + P_1 - 6P_\infty,\\ (y + x^2) &= 2P_0 + 3P1 - 5P_\infty,\\ (y + 1) &= 3P_0' + 2P_1' - 5P_\infty,\\ (y) &= 3P_0 + 2P_1 - 5P_\infty.\end{aligned}$$

By means of Hensel lemma, we compute the local expansion of y at P_0: this is $y = x^5 + x^3 + O(x^6)$. Then the image of the S-unit $y+1$ in R is given by $x^5 + x^3 + 1 + O(x^6) \equiv x^3 + 1 \bmod x^4$. This generates a subgroup R' of order 2 of R. Consider the S-unit h_{P_0} generating the principal divisor

$$(h_{P_0}) = \Big(\frac{y(y+x^2)}{y+x^3}\Big) = 4(P_1 - P'_\infty).$$

Its image in R is the element

$$\begin{aligned} h_{P_0} = \frac{y(y+x^2)}{y+x^3} &\equiv \frac{(x^5+x^3)(x^5+x^3+x^2)}{x^5+x^3+x^3} \\ &\equiv (x^2+1)(x^3+x+1) \equiv x^2+x+1 \bmod x^4 \end{aligned}$$

generating the complement subgroup of R' in R of order 4. Hence the image of $y+1$ and h_{P_0} generate the whole ray class group R and the corresponding ray class field extension is trivial.

The other possibilities for P reduce to the case *ii*) by applying the automorphism σ. □

We finally give a proof of Proposition 2.1.6 dealing with uniqueness of optimal genus 6 curves.

Proof of Proposition 2.1.6. *a*) Let C be a genus 6 optimal curve defined over $\mathbb{F}_2$ having Zeta function as in *a*). The real Weil polynomial of such a curve C is $t(t+2)(t^4+5t^3+5t^2-5t-5)$. The resultant of the polynomials $t+2$ and $t(t^4+5t^3+5t^2-5t-5)$ is -2, hence, by Theorem 2.2.3, there exists a covering $C \to E$ of degree 2. For C to have 10 rational points, all of the 5 rational points of E have to split completely. Moreover by the Hurwitz formula the degree of the different has to be 10. Now, since $a_2(C) = a_3(C) = a_4(C) = 0$, the only possibility for a place Q of E to ramify is to have degree at least five. This allows us to conclude that, since the ramification has to be wild, the different has to be precisely $2Q$, where Q is a degree five point of E. Thus any optimal genus 6 curve is a double covering of E of conductor $2Q$, where Q is a place of E of degree five, in which all rational points of E are split. This is the class field theory construction we described in Proposition 2.3.8.

The elliptic curve E has actually 4 points of degree five. If we choose a different degree five ramifying point of E for the construction, this gives us an isomorphic genus 6 curve C' having the same Zeta function. Indeed the elliptic curve has an $\mathbb{F}_2$-automorphism τ of order 4 acting transitively on the four places of degree five, which in particular fixes

the point at infinity and acts transitively on the other 4 rational points of E:

$$\begin{array}{rccc} \tau: & E & \to & E \\ & (x,y) & \mapsto & (x+1, x+y+1) \\ & P_1 & \mapsto & P_4 \\ & P_2 & \mapsto & P_3 \\ & P_3 & \mapsto & P_1 \\ & P_4 & \mapsto & P_2. \end{array} \tag{2.17}$$

b) Let C be an optimal curve of genus 6 defined over $\mathbb{F}_2$ such that its Zeta function is as in *b*). The real Weil polynomial of C is hence given by $(t-1)(t+2)(t^2+3t+1)^2$ and the parameters of C are $a(X) = [10, 0, 0, 0, 2, 15, \dots]$. Hence C satisfies all properties described in Section 2.6. By Proposition 2.6.1 it is a non-Galois extension of degree 3 of the optimal elliptic curve E. Consider as in the previous setting, the curve $\overline{C}$ whose function field $\overline{L}$ is the Galois closure of the function field L of C with respect to the function field K of E. The Galois group $Gal(\overline{L}/K)$ is isomorphic to the symmetric group S_3. By Proposition 2.6.3 we have the following two cases:

I) All 5 rational points of E are *b*-points, i.e. they split over C into 2 rational points such that one has ramification index 2 and the other one is unramified. Consider the morphism $\tau + 2 : E \to E$, where $\tau \in Aut(E)$ as in (2.17). It is a surjective morphism of degree 5 whose kernel consists of the $\mathbb{F}_2$-rational places of E. Let C' be the curve whose function field is the quadratic subfield of the function field of $\overline{C}$. By Proposition 2.6.3 the curve C' has genus 6. Hence by the Hurwitz formula the double covering $C' \to E$ must have conductor $\sum_{i=0}^{4} P_i$, where the P_i's are all 5 rational places of E. They must ramify in C' by hypothesis. Moreover C' has 10 places of degree four. Hence all 5 places of degree four of E split complitely over C'. Consider now the covering $C' \to E \to E$. It is stable under permutation of the rational places of E. Hence it is Galois. The curve $\overline{C}$ has genus 16 by Proposition 2.6.3, hence the degree 3 covering $\overline{C} \to C'$ is unramified. Moreover since $\overline{C}$ has 15 rational places, all rational places of C' split completely. There is a unique degree 3 such covering of C': indeed since $|Pic^0(C')| = L(1) = 2^4 \cdot 3 \cdot 5$, there is a unique degree 3 subgroup in the ray class group. Here $L(t) = (2t^2+1)(2t^2+2t+1)(4t^4-t^2+1)^2$ denotes the numerator of the Zeta function of C' computed in Proposition 2.6.3. Thus also the morphism $\overline{C} \to E \to E$ corresponds to a Galois extension of algebraic function fields. The Galois group G

of this extension has a normal subgroup S_3 of order 6 coprime to the order 5 of the quotient group $G/S_3 \simeq \mathbb{Z}_5$. The G fits in the following split exact sequence

$$0 \longrightarrow S_3 \longrightarrow G \longrightarrow \mathbb{Z}/5\mathbb{Z} \longrightarrow 0,$$

by Schur-Zassenhaus Theorem. In other words G is a semidirect product of S_3 and $\mathbb{Z}_5$. In this way one also has another tower of function fields corresponding to the morphisms of curves $\overline{C} \to Z \to E$, such that the Galois group G' of the function fields extension corresponding to the morphism $Z \to E$ satisfies $G' \simeq S_3$. Let $\tau \in S_3$ be a generator of the Galois group corresponding to the covering $\overline{C} \to C$ and consider invariant fields. We obtain a Galois covering $C \to Z'$ of degree 5. This covering has to be unramified. Indeed if a place Q of X lying over a place P of Z' ramifies, then it is totally ramified since the corresponding function field extension is cyclic. Thus any other ramification index in the covering $X \to E \to E$ has to be divided by 5. But this is impossible since $E \to E$ is unramified by construction and $X \to E$ has degree 3. The curve Z' has genus $g_{Z'} = 2$ by the Hurwitz formula $2 \cdot 6 - 2 = 5(2g_{Z'} - 2) + 0$. Thus the real Weil polynomial of Z' has to be a degree 2 factor of the real Weil polynomial of X. Since Z' is also a degree 3 covering of E, the real Weil polynomial of Z' is divisible by the real Weil polynomial $t + 2$ of E (cf. [A-P]). Hence the only possibility for the real Weil polynomial of Z' is to be $h(t) = (t + 2)(t - 1)$. The curve Z' is thus a genus 2 curve having 4 rational places and 2 places of degree two over $\mathbb{F}_2$. Over $\mathbb{F}_2$ any genus 2 smooth curve is a hyperelliptic curve. We show that up to $\mathbb{F}_2$-isomorphism there exists a unique hyperelliptic curve having real Weil polynomial $(t+2)(t-1)$. For a genus 2 hyperelliptic curve Z' over $\mathbb{F}_2$ having 4 rational points the different of the function fields extension associated to the double covering $Z' \to \mathbb{P}^1$ has to be $4P + 2Q$, where P and Q are rational points of $\mathbb{P}^1$. Indeed by Hurwitz formula the degree of the different is 6 and since Z' has 4 rational points, 2 of the rational points of $\mathbb{P}^1$ are wildly ramified and one splits completely. By taking $P = P_\infty$ and $Q = (0, 0)$ any hyperelliptic curve over $\mathbb{F}_2$ is $\mathbb{F}_2$-isomorphic to a projective curve of affine equation $y^2 + y = x^3 + ax + 1/x + b$ with $a, b \in \mathbb{F}_2$, according to the classification of Maisner and Nart in [M-N] (pg. 327). There are 4 possibilities for the parameters a and b but only the equation $y^2 + y = x^3 + x + 1/x + 1$ is the equation of a projective curve having 4 rational points and 2 places of degree two over $\mathbb{F}_2$. This curve is $\mathbb{F}_2$-isomorphic to the projective curve of affine equation $y^2 + xy = x^5 + x^4 + x^2 + x$, appearing in Proposition

2.4.3. The isomorphism is given by $(x, y) \mapsto (x, (y + x^2)/x)$.
Consider now the covering $C \mapsto Z'$. Since C has 10 rational points, two of the rational points of Z' have to split completely. If we choose P_∞ and $P_0 = (0, 0)$ of Z' to split completely we get the same construction as in Proposition 2.4.3. On the other hand this choice is the only possible one. Suppose one of the two splitting rational places of Z' is not P_∞. Then there are three possibilities for the splitting pairs of points:

i) The points $(1, 0)$ and $(1, 1)$ are split. This is equivalent to say that the divisor $2(1, 0) - 2(1, 1)$ is principal. Consider now the principal divisor $(x + 1) = 2(1, 0) + 2(1, 1) - 4P_\infty$, then $2(1, 0) - 2(1, 1) + (x + 1) = 4(1, 0) - 4P_\infty$ is principal as well. But this leads to a contradiction since P_∞ would also be split.

ii) If the points $(1, 0)$ and $(0, 0)$ are split, then $2(1, 0) - 2(0, 0)$ is principal. Similarly to the previous case, by adding the principal divisor $(x) = 2(0, 0) - 2P_\infty$, then $2(1, 0) - 2P_\infty$ is principal and a contradiction follows.

iii) Symmetrically with $(1, 1)$ and $(0, 0)$ by supposing $2(1, 1) - 2(0, 0)$ is principal and adding (x).

If P_∞ splits, then also does P_0. On the other hand, if we assume that the divisor $2P_\infty - 2(1, 0)$, resp. $2P_\infty - 2(1, 1)$, is principal, by adding $(x + 1)$ we find three rational splitting places, which is a contradiction.

II) Of the 5 rational points of E, one is an a-point, i.e. it splits completely over C; 3 are b-points, i.e. they split over C into 2 rational points such that one has ramification index two and the other one is unramified; one is a c-point, i.e. it is totally ramified over X. The double covering $C' \to E$ is a genus $g' = 5$ curve having parameters $a(C') = [5, 1, 0, 10, 4, \ldots]$ and real Weil polynomial $h(t) = (t+2)(t^2-5)(t^2-2)$ by Proposition 2.6.3. There are three rational places P, P' and P'' of E that ramify in C', one rational place Q splitting completely, and one rational place R which is inert by Proposition 2.5.1. By comparing the parameters of E and C' one also has that all 5 places Q_i, for $i = 1, \ldots, 5$, of E of degree four have to split completely over C'. One can always assume $Q = P_\infty$ by translating by P_1. Moreover one can also assume $R = P_1 = (1, 1)$ applying the order 4 automorphism τ of E in (2.17) that fixes P_∞ and permutes the other rational places of E. Both automorphisms fix the set of degree four places of E. By the Hurwitz formula the degree of the discriminant has to be 8. Hence the covering $C' \to E$ has conductor $4P + 2P' + 2P''$, where $\{P, P', P''\} = \{P_1, P_2, P_3\}$ with $P_1 = (0, 0)$, $P_2 = (0, 1)$ and

$P_3 = (1, 0)$. Let C'' be a curve such that its function field $\mathbb{F}_2(C'')$ is the maximal abelian extension of the function field $\mathbb{F}_2(E)$ of E of conductor $4P+2P'+2P''$ where P_∞ and all degree four places of E split completely. If $Gal(\mathbb{F}_2(C'')/\mathbb{F}_2(E)) \simeq \mathbb{Z}_2$, then C' coincides with C'', since C'' is unique by class field theory. The class group of conductor $4P+2P'+2P''$ is isomorphic to $R = \left(\mathbb{F}_2[[t_P]]/(t_P^4)\right)^* \oplus \left(\mathbb{F}_2[[t'_P]]/({t'_P}^2)\right)^* \oplus \left(\mathbb{F}_2[[t''_P]]/({t''_P}^2)\right)^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, where t_P, t'_P and t''_P are uniformizers at P, P' and P'' respectively. By class field theory, the group $Gal(\mathbb{F}_2(C'')/\mathbb{F}_2(E))$ is isomorphic to a quotient of R by the group generated by the images of the S-units, where S is the set of splitting places. We consider all possible choices for P, P' and P'' and show that for $P = P_2$ the curve C' is unique since $Gal(\mathbb{F}_2(C'')/\mathbb{F}_2(E))$ has order 2, while for $P = P_1$ or $P = P_3$ the group $Gal(\mathbb{F}_2(X')/\mathbb{F}_2(Y))$ is trivial.

Let $S = \{Q_1, Q_2, Q_3, Q_4, Q_5, P_\infty\}$, where the Q_i's are the 5 places of degree four of E as listed at page 48, for $i = 1, \ldots, 5$. The divisors generated by the uniformizers of the Q_i's are as follows

$$\begin{aligned}
(y + x^3) &= Q_1 + P_1 + P_4 - 8P_\infty, \\
(y + x^3 + 1) &= Q_2 + P_2 + P_3 - 8P_\infty, \\
(y + x^3 + x^2) &= Q_3 + P_1 + P_3 - 8P_\infty, \\
(y + x^3 + x^2 + 1) &= Q_4 + P_2 + P_4 - 8P_\infty, \\
(x^2 + x + 1) &= Q_5 - 4P_\infty.
\end{aligned}$$

Form these and the divisors listed in (2.7) we compute the divisors

$$\begin{aligned}
(u_1) &= (x^4 + x^3 + x^2 + x + 1) = Q_1 + Q_2 - 8P_\infty, \\
(u_2) &= (x^4 + x^3 + 1) = Q_3 + Q_4 - 8P_\infty, \\
(u_3) &= (x^2 + x + 1) = Q_5 - 4P_\infty, \\
(u_4) &= \left(\frac{(y + x^3)(y + x^3 + x^2)^2}{y(y + x)(x^2 + x + 1)^3}\right) = Q_1 + 2Q_3 - 3Q_5, \\
(u_5) &= \left(\frac{(y + x^3)^2(y + x^3 + x^2 + 1)}{(y + 1)(y + x)(x^2 + x + 1)^3}\right) = Q_4 + 2Q_1 - 3Q_5.
\end{aligned}$$

generated by S-units u_i, for $i = 1, \ldots, 5$. The u_i's are $\mathbb{F}_2$-linearly independent. Moreover by Hensel lemma we compute the local expansion y_{P_i} of y at P_i for $i = 1, 2, 3$:

$$\begin{aligned}
y_{P_1} &= x + x^2 + x^3 + x^4 + x^6 + O(x^7), \\
y_{P_2} &= 1 + x + x^2 + x^3 + x^4 + x^6 + O(x^7), \\
y_{P_3} &= t^2 + t^3 + t^4 + t^6 + O(t^7), \text{ where } t = x + 1.
\end{aligned}$$

i) Let $P = P_2$. We compute the images of the S-units in R. One has that

$$u_1 = x^4+x^3+x^2+x+1 \equiv \begin{cases} 1+x & \mod x^2, \\ 1+x+x^2+x^3 \equiv (1+x)^3 & \mod x^4, \\ 1 & \mod t^2; \end{cases}$$

$$u_2 = \ x^4 + x^3 + 1 \ \equiv \begin{cases} 1 & \mod x^2, \\ 1+x^3 & \mod x^4, \\ 1+t & \mod t^2; \end{cases}$$

$$u_3 = \ x^2 + x + 1 \ \equiv \begin{cases} 1+x & \mod x^2, \\ 1+x+x^2 \equiv (1+x)^3(1+x^3) & \mod x^4, \\ 1+t & \mod t^2; \end{cases}$$

and hence the images of u_1, u_2 and u_3 are $(1+t_{P_1})(1+t_{P_2})^3$, $(1+t_{P_2}^3)(1+t_{P_3})$ and $(1+t_{P_1})(1+t_{P_2})^3(1+t_{P_2}^3)(1+t_{P_3})$ respectively. Moreover

$$u_4 \equiv \begin{cases} 1 & \mod x^2, \\ 1+x+x^2 \equiv (1+x)^3(1+x^3) & \mod x^4, \\ 1 & \mod t^2; \end{cases}$$

$$u_5 \equiv \begin{cases} 1 & \mod x^2, \\ 1+x^3 & \mod x^4, \\ 1+t & \mod t^2; \end{cases}$$

so that the images of u_4 and u_5 are $(1+t_{P_2})^3(1+t_{P_2}^3)$ and $(1+t_{P_2}^3)(1+t_{P_3})$ respectively. The subgroup of R generated by the images of the u_i's for $i = 1, \ldots, 5$ is hence a subgroup of index 2. It coincides with the group generated by the images of the S-units u_1, u_2 and u_3.

ii) Let $P = P_1$. Similarly to the previous case one can compute the images of the S-units u_i's in the class group R. In particular, since they depend only on the variable x, the images of u_i for $i = 1, 2, 3$, are easily computed as $(1+t_{P_1})^3(1+t_{P_2})$, $(1+t_{P_1}^3)(1+t_{P_3})$ and $(1+t_{P_1})^3(1+t_{P_1})(1+t_{P_2})(1+t_{P_3})$ respectively, by replacing P_1 by P_2 and viceversa. On the other hand one has

$$u_4 \equiv \begin{cases} 1+x^2+x^3 & \mod x^4, \text{ at } P_1, \\ 1+x \equiv (1+x)^3(1+x^3) & \mod x^2, \text{ at } P_2, \\ 1 & \mod t^2; \end{cases}$$

$$u_5 \equiv \begin{cases} 1 & \mod x^4, \text{ at } P_1, \\ 1 & \mod x^2, \text{ at } P_2, \\ 1+t & \mod t^2; \end{cases}$$

Hence the images of u_4 and u_5 are $(1+t_{P_1})^2(1+t_{P_1}^3)(1+t_{P_2})$ and $(1+t_{P_3})$ respectively. The images of u_1, u_2, u_4 and u_5 are independent generators of R. The first has order 4, while the images of u_2, u_4, u_5 have order 2. Thus they generate the whole class group R.

iii) In case $P = P_3$ we have

$$u_1 = x^4+x^3+x^2+x+1 \equiv \begin{cases} 1+x & \mod x^2, \\ 1+t^3 & \mod t^4; \end{cases}$$

$$u_2 = \ x^4+x^3+1 \ \equiv \begin{cases} 1 & \mod x^2, \\ 1+t+t^2+t^3 \equiv (1+t)^3 & \mod t^4; \end{cases}$$

$$u_3 = \ x^2+x+1 \ \equiv \begin{cases} 1+x & \mod x^2, \\ 1+t+t^2 \equiv (1+t)^3(1+t^3) & \mod t^4; \end{cases}$$

and hence the images of u_1, u_2 and u_3 are $(1+t_{P_1})(1+t_{P_3}^3)(1+t_{P_2})$, $(1+t_{P_3})^3$ and $(1+t_{P_1})(1+t_{P_3})^3(1+t_{P_3}^3)(1+t_{P_2})$ respectively. Moreover

$$u_4 \equiv \begin{cases} 1 & \mod x^2, \text{ at } P_1, \\ 1+x & \mod x^2, \text{ at } P_2, \\ 1 & \mod t^4; \end{cases}$$

$$u_5 \equiv \begin{cases} 1 & \mod x^2, \text{ at } P_1, \\ 1 & \mod x^2, \text{ at } P_2, \\ 1+t+t^2 \equiv (1+t)^3(1+t^3) & \mod t^4; \end{cases}$$

so that the images of u_4 and u_5 are $(1+t_{P_2})$ and $(1+t_{P_3})^3(1+t_{P_3}^3)$ respectively. The images of u_1, u_2, u_4 and u_5 generate the whole ray class group R.

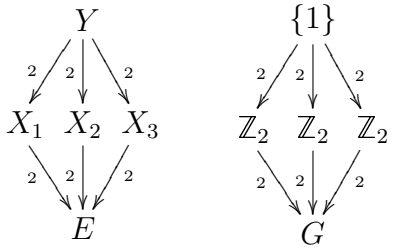
The rational place $P_4 = (1,1)$ of E is inert in C'. Let P_4' denote the place of degree 2 of C' lying over P_4. Then the genus 15 curve $\overline{C}$, having parameters $a(\overline{C}) = [15,1,0,0,0,\ldots]$ by Proposition 2.6.3, is a degree 3 Galois covering of C' where all rational places of C' are split and the degree two place P_4' ramifies. Then by the Hurwitz formula the different has to be $2P_4'$ and the function field of $\overline{C}$ is the ray class field of conductor $2P_4'$ where all rational places of C' split completely. A computer calculation performed by Claus Fieker in MAGMA shows that the associated ray class group is always trivial. Hence the curve C does not exists.

□

2.8 An example of two genus 7 optimal curves having different Zeta functions

In this last section we want to present a construction of a ray class field having among its subfields the algebraic function fields of two genus 7 optimal curves. We combine methods of the previous sections in order to compute the Zeta functions associated to these curves: they turn out to be different, providing existence of two non-isomorphic genus 7 optimal curves.

Example 2.8.1. *Let Q denote a degree six place of uniformizer $t = x^6+x^5+1$ of the optimal elliptic curve E defined over $\mathbb{F}_2$. The maximal ray class field L of conductor $2Q$, in which all 5 rational points of the function field K of E are totally split, is an extension of K with Galois group $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The three subgroups of G of order 2 correspond to three genus 7 coverings X_1, X_2 and X_3 of E having 10 rational points over $\mathbb{F}_2$:*



The Zeta function of X_i has the form

$$Z(t) = \frac{(2t^2+2t+1)P_i(t)}{(1-2t)(1-t)},$$

for $i = 1, 2, 3$, where

$$\begin{aligned} P_1(t) = P_3(t) &= 64t^{12} + 160t^{11} + 240t^{10} + 280t^9 + 276t^8 + 238t^7 \\ &\quad +180t^6 + 119t^5 + 69t^4 + 35t^3 + 15t^2 + 5t + 1, \end{aligned} \tag{2.18}$$

while

$$\begin{aligned} P_2(t) &= (4t^4 + 6t^3 + 5t^2 + 3t + 1)(16t^8 + 16t^7 + 16t^6 \\ &\quad +14t^5 + 10t^4 + 7t^3 + 4t^2 + 2t + 1). \end{aligned} \tag{2.19}$$

Proof. Remark 2.3.2 states that the elliptic curve E has 10 places of degree six. Repeating the construction of Proposition 2.3.8 with the place Q of degree six rather than five, we obtain a degree 4 extension L of the function field K of E. By class field theory, the Galois group of L/K isomorphic to $R = \mathbb{F}_{2^6}[[t]]^*/\{u : u \equiv 1 \mod t^2\}$ modulo the image of the S-unit group $O_S^* = \langle x, x+1, y, y+x\rangle$ of E, where S is the set of 5 rational points of

E. Similarly to Proposition 2.3.8, we let α be a root of x^6+x^5+1. Then $P=(a,a^4+a^3+a^2+1)$ and $P'=(a,a^4+a^3+a^2)$ are $\mathbb{F}_{2^6}$-rational points of E. The prime ideal of the coordinate ring of E corresponding to P is $\mathfrak{p}=(x^6+x^5+1, y+x^4+x^3+x^2+1)$. Consider the divisor $(x^6+x^5+1)=P+P'-12P_\infty$ and take $t=x^6+x^5+1$ as uniformizer at Q, the place of which the point P is representative. In order to compute the image of the S-units in R, we first observe that the image of the S-unit x has order 63 modulo t and hence it generates the 63-part of R. Thus we compute

$$\begin{aligned} x^{63}-1 &\equiv (x+1)t && \bmod t^2,\\ (x+1)^{63}-1 &\equiv xt && \bmod t^2,\\ y^{63}-1 &\equiv (x^5+x^2)t && \bmod t^2,\\ (y+x)^{63}-1 &\equiv (x^5+x^4+x^3+x^2)t && \bmod t^2, \end{aligned}$$

and the Galois group of L/K is isomorphic to the quotient group $\mathbb{F}_2[x]/(x^6+x^5+1)H$, where $H=\langle x+1, x, x^5+x^2, x^5+x^4+x^3+x^2\rangle$ is a subgroup of index 4. Since all elements in this quotient group have order 2, the Galois group of L/K is isomorphic to $\mathbb{Z}_2\oplus\mathbb{Z}_2$. Its three subgroups of order 2 correspond to three coverings X_1, X_2 and X_3 of E having each 10 rational points over $\mathbb{F}_2$ since all five rational places of S split completely over each curve. They all have genus $g=7$: indeed by the Hurwitz formula one has $2g-2=2(2\cdot 1-2)+2\deg Q$, since each of the three non-trivial characters of $\mathbb{Z}_2\times\mathbb{Z}_2$ has conductor $2Q$. Hence we have three genus 7 curves over $\mathbb{F}_2$ with 10 rational places. They are optimal by Serre's estimate.
We compute the Zeta function of each curve X_i. To this end we consider the places of degree $d=2,\dots,7$ of E. Since the rational points of E are all split and E has no places of degree two nor three, none of the three X_i has places of degree two or three either. In each curve X_i a place of degree four must lie over one of the places of degree four of E that split completely. Similarly for a place of X_i of degree five. By class field theory, a place P of E splits completely over X_i if and only if the image of the uniformizer of P is trivial in the ray class group corresponding to the covering $X_i\mapsto E$. We start considering uniformizers for the degree four places of E as in the proof of Proposition 2.3.8 and computing their images in $\mathbb{F}_2[x]/(x^6+x^5+1)$ as done above for the S-units of E. One has

$$\begin{aligned} (y+x^3)^{63}-1 &\equiv (x^5+x)t && \bmod t^2,\\ (y+x^3+1)^{63}-1 &\equiv x^4t && \bmod t^2,\\ (y+x^3+x^2)^{63}-1 &\equiv (x^5+x^3+x)t && \bmod t^2,\\ (y+x^3+x^2+1)^{63}-1 &\equiv (x^4+x^2)t && \bmod t^2,\\ (x^2+x+1)^{63}-1 &\equiv (x^5+x^3+x^2)t && \bmod t^2. \end{aligned}$$

Similarly for the places of degree five we take uniformizers as follows and

compute

$$\begin{aligned}
(y+x^4)^{63}-1 &\equiv (x^3+x+1)t && \bmod t^2,\\
(y+x^4+1)^{63}-1 &\equiv (x^5+x^4+x)t && \bmod t^2,\\
(y+x^4+x)^{63}-1 &\equiv (x^4+x^3+x^2+1)t && \bmod t^2,\\
(y+x^4+x+1)^{63}-1 &\equiv (x^5+x^4+x^3+1)t && \bmod t^2.
\end{aligned}$$

We consider now the index two subgroups $H_1 = H \cdot \langle x^3 \rangle$, $H_2 = H \cdot \langle x^2 \rangle$ and $H_3 = H \cdot \langle x^3 + x^2 \rangle$ of $\mathbb{F}_2[x]/(x^6 + x^5 + 1)$, for which the ray class groups associated to the genus 7 curve X_i is isomorphic to $\mathbb{F}_2[x]/(x^6+x^5+1)H_i$, for $i = 1, \ldots, 3$. The images in $\mathbb{F}_2[x]/(x^6 + x^5 + 1)H_i$ of the above uniformizers are the following:

1) Among the places of degree four only the images x^4 and $x^5 + x^3 + x^2$ of the places of uniformizers $y + x^3 + 1$ and $x^2 + x + 1$ respectively lie in H_1. Hence the curve X_1 has 4 places of degree four. Of the places of degree five only the place of uniformizer $y + x^4$ has image $x^3 + x + 1$ lying in H_1: the curve X_1 has hence 2 places of degree five. We sum up the recovered information in the vector $a(X_1) = [10, 0, 0, 4, 2, \ldots]$.

2) In the case $i = 2$, there is only one place of degree four whose uniformizer $y + x^3$ has image $x^5 + x$ lying in H_2. Among the places of degree five, the places of uniformizers $y+x^4+x$ and $y+x^4+x+1$ split completely over X_2: indeed these are the only two places for which the images $x^4 + x^3 + x^2 + 1$ and $x^5 + x^4 + x^3 + 1$ of their uniformizers lie in H_2. The curve X_2 has hence 2 places of degree four and 4 places of degree five. Summing up $a(X_2) = [10, 0, 0, 2, 4, \ldots]$.

3) Also in the case $i = 3$ there are 2 places of degree four, namely the places of uniformizers $y + x^3 + x^2 + 1$ and $y + x^3 + x^2$, and only one place of degree five, having uniformizer $y + x^4 + 1$, whose images lie in H_3. Hence the curve X_3 has $a(X_3) = [10, 0, 0, 4, 2, \ldots]$, the same as X_1 up to the 5-th entry.

Since the degree six place Q of E ramifies in every curve X_i for all $i = 1, \ldots, 3$, the number $a_6(X_i)$ of degree six places of X_i has to be odd, while the number $a_7(X_i)$ of degree seven places of X_i, has to be even. We can now determine a parametric form for the real Weil polynomial of each curve X_i from the information we have:

i) For the curves X_1 and X_3 the common values of $N = a_1 = 10$, $a_2 = a_3 = 0$, $a_4 = 4$ and $a_5 = 2$ allow to determine a parametric form common to the real Weil polynomials of both curves:

$$h_{\alpha,\beta}(t) = t^7 + 7t^6 + 13t^5 - 9t^4 - 45t^3 - 21t^2 + \alpha t + \beta.$$

One can check that only for the values of $(\alpha, \beta) = (26, 16)$ and $(\alpha, \beta) = (27, 18)$ both $h_{\alpha,\beta}(t)$ and its derivative have all roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$. But while the first pair of values $(26, 16)$ gives $a_6(X_i) = 5$ and $a_7(X_i) = 18$, the second pair gives $a_6(X_i) = 6$, which is even. Hence both X_1 and X_3 have the same Zeta function an it is determined by the polynomial (2.18).

ii) For the curve X_2 the values $a(X_2) = [10, 0, 0, 2, 4, \ldots]$ give the parametric real Weil polynomial

$$h_{\alpha,\beta}(t) = t^7 + 7t^6 + 13t^5 - 9t^4 - 47t^3 - 33t^2 + \alpha t + \beta.$$

In this case there are three pairs of values of (α, β) for which both $h_{\alpha,\beta}(t)$ and its derivative have all roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$:

i) the pair $(3, 2)$, which gives $a_6 = 10$,

ii) the pair $(4, 4)$, which gives $a_6 = 11$ and a_7=12,

iii) and the pair $(5, 7)$, for which $a_6 = 12$.

Hence the Zeta fuction of X_2 corresponds to the only pair $(\alpha, \beta) = (4, 4)$ for which a_6 is non even. This Zeta function is hence determined by the polynomial (2.18).

□

Bibliography

[A-P] Y.Aubry and M.Perret, Divisibility of zeta functions of curves in a covering , *Arch. Math.* **82** (2004), 205-213.

[Au] R. Auer, Ray class fields of global function fields with many rational places, *Acta Arith.* **95** (2000), 97-122.

[D-V] V.G. Drinfeld and S.G. Vlăduţ, The number of points of an algebraic curve, *Funct. Anal. i Ego Pril.* **17** (1983), 68-69; (=*Functional Analysis* **17** (1983), 53-54).

[E] A. Edouard, Formules explicites et nombre de points des courbes sur les corps finis: le théorème d'Oesterlé, Thèse de Doctorat, Université de la Méditerranée Aix-Marseille II, (1998).

[G] G. Gras, Class field Theory: from theory to practice, Springer-Verlag, Berlin, 2003. .

[G-V] G. van der Geer and M. van der Vlugt, Tables of curves with many points, *Math. Comp.* **69** (2000), 797-810. Updates at `http://www.manypoints.org/`

[H] H. Howe, Even sharper upper bounds on the number of points on curves, slides based on work in progress with Kristin Lauter available at `http://alumnus.caltech.edu/~however/talks.html`.

[H-L] H. Howe and K. Lauter, Improved upper bounds for the number of points on curves over finite fields, *Ann. Inst. Fourier* **53** (2003), 1677-1737.

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

[L] K. Lauter, Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points, *Proc. Amer. Math. Soc.* **128** (2000), 369-374.

[L1] K. Lauter, Ray class field constructions of curves over finite fields with many rational points, *Algorithmic Number Theory*, H. Cohen (ed.), *Lecture Notes in Comput. Sci.* **1122**, Springer, (1996), 187-195.

[M-N] D. Maisner and E. Nart, with an appendix by E. Howe, Abelian surfaces over finite fields as Jacobians, *Experimental Math.* **11** (2002), 321-337.

[N-X] H. Niederreiter and C.P. Xing, Rational points on curves over finite fields: Theory and Applications, London Mathematical Society Lecture Note Series 285, Cambridge, 2001.

[R] M. Rosen, Number theory in function fields, Springer-Verlag, New York, 2002.

[S] J.-P. Serre, Rational points on curves over finite fields, unpublished notes by Fernando Q. Gouvéa of lectures at Harvard University, 1985.

[S1] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris, Sér I Math.* **296** (1983), 397-402; (= *Oeuvres III*, No. 128, 397-402).

[S2] J.-P. Serre, Nombres de points des courbes algébiriques sur $\mathbb{F}_q$, *Sém. Théor. Nombres Bordeaux*, **22**, (1982/83); (= *Oeuvres III*, No. 129, 664-668).

[S3] J-P. Serre, Résumé des cours de 1983-1984, *Ann. Collége France*, (1984), 79-83; (= *Oeuvres III*, No. 132, 701-705).

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

[Sti] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

[W] A. Weil, Zum Beweis des Torellischen Satzes, *Nachr. Akad. Göttingen, Math.-Phys. Kl.*, (1957), 33-53.

[Wa] L.C. Washington, Introduction to cyclotomic fields, Springer-Verlag, New-York, 1982.