INSTITUTO DE MATEMÁTICA

Universidade Federal do Rio de Janeiro

UFRJ

On algebraic curves with many rational points and Weierstrass semigroups

Erik Antonio Rojas Mendoza

Rio de Janeiro, Brasil

Março 2023

On algebraic curves with many rational points and Weierstrass semigroups

Erik Antonio Rojas Mendoza

Tese de doutorado apresentada ao Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Matemática.

Universidade Federal do Rio de Janeiro

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Supervisor: Luciane Quoos Conte

Rio de Janeiro, Brasil
Março 2023

CIP - Catalogação na Publicação

R741o

Rojas Mendoza, Erik Antonio
On algebraic curves with many rational points and Weierstrass semigroups / Erik Antonio Rojas Mendoza. -- Rio de Janeiro, 2023.
95 f.

Orientadora: Luciane Quoos Conte.
Tese (doutorado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós Graduação em Matemática, 2023.

1. Curvas algébricas. 2. Corpos finitos. 3. Semigrupos de Weierstrass. I. Quoos Conte, Luciane, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

Erik Antonio Rojas Mendoza

On algebraic curves with many rational points and Weierstrass semigroups

Tese de doutorado apresentada ao Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Matemática.

Aprovada em 17/03/2023 por:

Luciane Quoos Conte

Dra. Luciane Quoos Conte - UFRJ
Presidente

Maral Mostafazadehfard

Dra. Maral Mostafazadehfard - UFRJ

Dra. Carolina Araujo - IMPA

Dr. Guilherme Chaud Tizziotti - UFU

Abdón

Dra. Miriam del Milagro Abdón - UFF

Pietro Speziali

Dr. Pietro Speziali - UNICAMP

Dr. Francesco Noseda - UFRJ

Rio de Janeiro, Brasil
Março 2023

Este trabalho é dedicado aos meus pais Felicia e Jesús.

Agradecimentos

À minha família. Aos meus pais Felicia e Jesús por todo o amor incondicional, pela compreensão e apoio durante todos esses anos que estive longe deles. Cada uma das minhas conquistas é por e para eles. Aos meus irmãos Gabriela e Miguel pelo apoio e por sempre cuidarem dos meus pais durante minha ausência.

À minha orientadora Luciane por todos esses anos trabalhando juntos. Pela sua amizade, pela paciência, por sempre me motivar a enfrentar novos desafios, por ter sido parte fundamental da minha formação como matemático e como pessoa, pelos conselhos profissionais e pessoais. Serei sempre grato pela confiança que depositou em mim.

Aos meus amigos Charles, Eric, Alex, Jéssica, Fidel, Brayan, Benazir, Manuel, Paul, Bohr, Abad, Óscar, Roberto, Nádia, Juliana, Maricruz e todos os colegas da sala B-109 do Instituto de Matemática da UFRJ pelo apoio e por fazerem parte desta etapa.

Ao meu amigo e colaborador acadêmico Rohit pelo apoio e pelas produtivas discussões que tivemos na área de Corpos Finitos.

Aos membros da banca por aceitarem avaliar este trabalho, pelos comentários e sugestões.

A cada um dos professores, técnicos e administrativos do Programa de Pós-Graduação do Instituto de Matemática da UFRJ.

À CAPES, CNPq e FAPERJ pelo apoio financeiro, bem como ao Programa de Pós-Graduação do Instituto de Matemática da UFRJ pelo apoio financeiro para participação em eventos.

Resumo

Nos últimos anos, curvas algébricas sobre corpos finitos e semigrupos de Weierstrass têm sido intensamente estudados devido às suas diversas aplicações em outras áreas da Matemática, como a teoria de códigos. Nesta tese, construímos curvas algébricas com muitos pontos racionais de duas maneiras diferentes. Primeiro, beneficiando-se de representações adequadas do grupo de automorfismos da curva BM introduzida por Beelen e Montanucci em [7], construímos equações explícitas para famílias de curvas maximais como subcoberturas de Galois da curva BM. Em segundo lugar, usando polinômios recíprocos e extensões de Kummer, fornecemos um método simples e eficaz para construir curvas algébricas com muitos pontos racionais. Por outro lado, damos uma descrição explícita do semigrupo de Weierstrass no único lugar no infinito Q_∞ de uma curva $\mathcal{X}$ definida pela equação $Y^m = f(X)$, onde $f(X) \in \mathbb{F}_q[X]$ é um polinômio satisfazendo $\gcd(m, \deg f) = 1$ e $\mathrm{Char}(\mathbb{F}_q) \nmid m$. Como consequência, discutimos condições suficientes para que o semigrupo de Weierstrass $H(Q_\infty)$ seja simétrico. Além disso, deduzimos uma fórmula fechada para a cota de Geil-Matsumoto associada ao semigrupo $H(Q_\infty)$ sobre o número de pontos racionais da curva $\mathcal{X}$ e caracterizamos certas curvas Castle maximais do tipo $(\mathcal{X}, Q_\infty)$.

Palavras-chave: Corpos finitos, corpo de funções, curvas algébricas, curvas maximais, curvas quocientes, curvas com muitos pontos racionais, extensões de Kummer, semigrupos de Weierstrass, polinômios recíprocos.

Abstract

In recent years, algebraic curves over finite fields and Weierstrass semigroups have been intensively studied due to their various applications in other areas of mathematics, such as coding theory. In this thesis, we construct algebraic curves with many rational points in two different ways. First, benefiting from suitable representations of the automorphism group of the BM curve introduced by Beelen and Montanucci in [7], we construct explicit equations for families of maximal curves as Galois subcovers of the BM curve. Second, using reciprocal polynomials and Kummer extensions, we provide a simple and effective method for the construction of algebraic curves with many rational points. On the other hand, we give an explicit description of the Weierstrass semigroup at the only place at infinity Q_∞ of a curve $\mathcal{X}$ defined by the equation $Y^m = f(X)$, where $f(X) \in \mathbb{F}_q[X]$ is a polynomial satisfying $\gcd(m, \deg f) = 1$ and $\mathrm{Char}(\mathbb{F}_q) \nmid m$. As a consequence, we discuss sufficient conditions for the Weierstrass semigroup $H(Q_\infty)$ to be symmetric. Furthermore, we deduce a closed formula for the Geil-Matsumoto bound associated to the semigroup $H(Q_\infty)$ on the number of rational points of the curve $\mathcal{X}$ and characterize certain maximal Castle curves of the type $(\mathcal{X}, Q_\infty)$.

Keywords: Finite fields, function fields, algebraic curves, maximal curves, quotient curves, curves with many rational points, Kummer extensions, Weierstrass semigroups, reciprocal polynomials.

List of Figures

List of symbols

$\mathbb{F}_q$	the finite field with q elements;
$\mathbb{F}_q^*$	the nonzero elements of $\mathbb{F}_q$;
K	the algebraic closure of $\mathbb{F}_q$;
$\mathcal{X}(\mathbb{F}_q)$	the set of $\mathbb{F}_q$-rational points of the algebraic curve $\mathcal{X}$;
$\mathbb{F}_q(\mathcal{X})$	the function field of the curve $\mathcal{X}$ with full constant field $\mathbb{F}_q$;
$\mathrm{Aut}(\mathcal{X})$	the full automorphism group of the curve $\mathcal{X}$;
$\mathbb{Z}$	the set of the integers;
$\mathbb{N}$	the set of positive integers;
$\mathbb{N}_0$	the set of non-negative integers.

Contents

Introduction

Algebraic curves over finite fields and their function fields have been a source of great fascination since the seminal work of Hasse and Weil in the 1930s and 1940s. Many important and fruitful ideas have arisen out of this area, where algebra, number theory, and geometry meet. In 1977, Goppa [28] constructed linear error-correcting codes using algebraic curves over finite fields. These are called algebraic geometry codes and usually have good parameters. In order to construct such codes one requires curves with a large number of rational points and explicit equations for such curves. Also, such curves have applications in other areas such as low-discrepancy sequences, stream ciphers, hash functions, and finite geometries. On the other hand, Weierstrass semigroups at one and many rational points on a curve have been shown to have interesting applications. For instance, in [45] and [13] the authors construct algebraic geometry codes with good parameters using Weierstrass semigroups at one and two points respectively. In [39], the authors determine the automorphism group of the cyclotomic function field with modulus X^{n+1} for $n \in \mathbb{N}$ using explicit descriptions of Weierstrass semigroup at one point. In addition, knowing the internal structure of the Weierstrass semigroup allows us to obtain upper bounds for the number of rational points on a curve, see for instance [23] and [38]. These are some of the important reasons that leads the study of algebraic curves over finite fields with many rational points to have been a subject of great interest in recent years.

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p, and K be the algebraic closure of $\mathbb{F}_q$. For a non-singular, projective, absolutely irreducible algebraic curve (or simply curve) $\mathcal{X}$ over $\mathbb{F}_q$ with genus $g(\mathcal{X})$, we denote by $\mathcal{X}(\mathbb{F}_q)$ its set of $\mathbb{F}_q$-rational points. The celebrated Hasse-Weil Theorem states that the number $\#\mathcal{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$ satisfies

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

A curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ is called maximal if the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ attains the Hasse-Weil bound, that is, $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2g(\mathcal{X})q$. One of the most studied maximal curve is the Hermitian curve over $\mathbb{F}_{q^2}$, whose affine model is given by the equation $Y^{q+1} = X^q + X$. It has genus $g = q(q-1)/2$ and a large automorphism group isomorphic to $PGU(3, q)$ compared to its genus, meaning that the order of the automorphism group $\#\mathrm{Aut}(\mathcal{X})$ does not satisfy the classical Hurwitz bound $\#\mathrm{Aut}(\mathcal{X}) \leq 84(g-1)$. It is a well-known result that the Hermitian curve has the highest genus a maximal curve over $\mathbb{F}_{q^2}$ can attain and is, up to isomorphism, the only maximal curve with such a genus.

By a known result of Kleiman [37], any curve $\mathcal{Y}$ over $\mathbb{F}_{q^2}$ which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ is itself $\mathbb{F}_{q^2}$-maximal. This result allows the construction of maximal curves as quotients of known maximal curves. In fact, let $\mathcal{X}$ be a maximal curve over $\mathbb{F}_{q^2}$ and $F = \mathbb{F}_{q^2}(\mathcal{X})$ its function field. Then given a subgroup H of $\mathrm{Aut}(\mathcal{X})$, the curve $\mathcal{Y}$ can be obtained as the fixed field $\mathrm{Fix}(H)$ of F. The genus, the explicit defining equations, and the automorphism group H associated to the quotient curve of a known $\mathbb{F}_{q^2}$-maximal curve, such as the Hermitian curve, the Suzuki curve, the GK curve, the GGS curve and the BM curve are all objects of significant interest (see [2–4, 8, 17, 22, 24, 25] and [27]). However, sometimes it can be hard to give explicit equations for a quotient curve. This problem is relevant for applications to coding theory since maximal curves have been used in the construction of some good linear codes, such as differential and linear algebraic geometry codes (see [12, 13, 40] and references therein). Still another area benefiting from explicit equations of maximal curves is finite geometry, for example in the construction of certain arcs over maximal curves (see [5, 9] and [26]).

On the other hand, several methods, such as class field theory, Drinfeld module, and character theory, to find algebraic curves with many rational points (not necessarily maximal curves) have been studied (see for instance [19,21,33,35,36,52,53,59,62] and [63]). More explicit details about these methods can be found in [61]. However, the computation of the exact number of rational points on a given curve has always been a challenging problem and a general method to do such computations seems out of reach. Nevertheless, for certain very specific curves, some methods, such as evaluation of exponential sums and Kloosterman sums, as well as function field theory, have been helpful. For instance, Coulter [15] used exponential sums to compute the number of rational points on a class of Artin-Schreier curves and Moisio [44] used exponential sums and Kloosterman sums to compute the number of rational points on some families of Fermat curves. In [50, 51], the authors considered fibre products of Kummer covers of the projective line over $\mathbb{F}_q$. In [49], the authors gave a full description of the number of rational points in some extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ in terms of Legendre symbol and quadratic characters for the Artin-Schreier curve $Y^q - Y = XP(X) - \lambda$ where $P(X) = X^{q^i} - X$ and $\lambda \in \mathbb{F}_q$. For more details about these methods, we refer to [8, 15, 44, 50, 51].

With respect to the Weierstrass semigroups at many rational points on algebraic curves, there are several results in the literature. For instance, in [6, 13, 41, 45] the authors determine the Weierstrass semigroup at one and many rational points of specific maximal curves such as the Suzuki curve, the GK curve, the BM curve, and the Hermitian curve. In [48], the authors provide an algorithm to calculate Weierstrass semigroups over an optimal tower of function fields, giving an explicit description of such objects in some cases. In [12], the authors provide an explicit description of the Weierstrass semigroup at one and two totally ramified places of a Kummer extension defined by the equation $Y^m = f(X)^\lambda$, where $p \nmid m$, $\lambda \in \mathbb{N}$, and $f(X) \in K[X]$ is a separable polynomial such that $\gcd(\lambda \deg f, m) = 1$. These results were generalized in [64], where the authors determine the Weierstrass semigroup at many totally ramified places of Kummer extensions defined by the same equation. For Kummer extensions defined by the equation $Y^m = f(X)$, where $f(X) \in K[X]$ has possibly roots with different multiplicities, few results are known.

In this work, we construct algebraic curves with many rational points in two different ways: by constructing quotient curves of known maximal curves, and by using reciprocal polynomials to define Kummer extensions with many rational points. In addition, we study Weierstrass semigroups in Kummer extensions defined by the equation $Y^m = f(X)$, where $f(X) \in K[X]$ is a polynomial such that $\gcd(m, \deg f) = 1$. This thesis compiles the original work contained in the following articles and preprints:

- [43] Mendoza, Erik A. R.; Quoos, Luciane. *Explicit equations for maximal curves as subcovers of the BM curve.* Finite Fields and Their Applications 77 (2022): 101945.
- [32] Gupta, Rohit; Mendoza, Erik A. R.; Quoos, Luciane. *Reciprocal polynomials and curves with many points over a finite field.* arXiv preprint arXiv:2110.10620 (2021).
- [42] Mendoza, Erik A. R. *On Kummer extensions with one place at infinity.* arXiv preprint arXiv:2208.09729 (2022).

The content of this thesis is presented in 4 chapters. In Chapter 1, we present the preliminaries and some previous results on numerical semigroups and algebraic curves. Furthermore, we introduce the notations that will be used throughout the thesis.

In Chapter 2, we apply suitable morphisms to the Beelen-Montanucci curve (BM curve) to provide two new equations for this curve and, benefiting from these models, obtain certain subgroups of $\mathrm{Aut}(BM)$ for which the fixed field and genus can be completely determined. In particular, we obtain a plane model for the BM curve, a generalization of the family of Galois subcovers given in [7, Remark 4.6], a family of subcovers of the curve presented in [7, Corollary 3.7], and generalizations of results in [27]. We finish the chapter by presenting parameters for which some of the curves obtained in this chapter are not covered by the Hermitian curve.

In Chapter 3, we present a family of Kummer covers of the projective line over $\mathbb{F}_{q^2}$ defined by an affine equation of the type

$$Y^m = X^{\epsilon s} f(X) f^*(X)^{\lambda}, \tag{1}$$

where $\epsilon, \lambda \in \{1, -1\}$, s is a non-negative integer, $p \nmid m$, $f(X)$ is a polynomial in $\mathbb{F}_q[X]$ and $f^*(X)$ is the reciprocal polynomial of $f(X)$. We compute the genus of this family of curves and study the particular case $\epsilon = -1$ and $\lambda = 1$, $\epsilon = 1$ and $\lambda = -1$. We provide the exact number of rational points for some families of curves. Finally, we study fibre products of Kummer extensions defined by Equation (1). As a consequence of these constructions, we obtain several improvements on the manYPoints table [60]. More precisely, we obtain 10 new records and 119 new entries.

In Chapter 4, we provide an explicit description of the Weierstrass semigroup $H(Q_\infty)$ and the gap set $G(Q_\infty)$ at the only place at infinity Q_∞ of the Kummer extension defined by the affine equation

$$\mathcal{X}: \quad Y^m = f(X) = \prod_{i=1}^{r}(X - \alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \text{and} \quad 1 \leq \lambda_i < m,$$

where $r \geq 2$ and $m \geq 2$ are integers such that $p \nmid m$, $\alpha_1, \dots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $\gcd(m, \lambda_0) = 1$. As a consequence, we generalize the closed formula for the Geil-Matsumoto bound on the number of rational points of a curve given by Bras-Amorós and Vico-Oton in [11, Theorem 3.2]. Furthermore, we study the Frobenius number and the multiplicity of the semigroup $H(Q_\infty)$ establishing a relationship between them, and we provide sufficient conditions for the semigroup $H(Q_\infty)$ to be symmetric. Finally, we characterize certain $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$.

1 Preliminaries and notations

In this chapter, we introduce the notations that will be used throughout the thesis and present some general results on the theory of numerical semigroups and algebraic curves over finite fields.

We denote by $\mathbb{N}$ the set of positive integers and by $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ the set of non-negative integers. For $c \in \mathbb{R}$ we denote by $\lfloor c \rfloor$, $\lceil c \rceil$ and $\{c\}$ the floor, ceiling and fractional part functions of c respectively, and for $a, b \in \mathbb{Z}$ we denote by (a, b) the greatest common divisor of a and b, and by $b \mod a$ the smallest non-negative integer congruent with b modulo a. Moreover, to differentiate standard sets from multisets (that is, sets that can contain repeated occurrences of elements), we use the usual symbol '$\{\}$' for standard sets and the symbol '$\{\!\!\{\}\!\!\}$' for multisets. For a multiset M, the set of distinct elements of M is called the support of M and is denoted by M^*, the number of occurrences of an element $x \in M^*$ in the multiset M is called the multiplicity of x and is denoted by $m_M(x)$, and the cardinality of the multiset M is defined as the sum of the multiplicities of all elements of M^*. We say that two multisets M_1 and M_2 are equal if $M_1^* = M_2^*$ and $m_{M_1}(x) = m_{M_2}(x)$ for each x in the support. For more on multisets, see [14].

1.1 Numerical semigroups

We start by presenting some known results related to numerical semigroups. For more on numerical semigroups, we refer to the book [55].

Definition 1.1.1. *A numerical semigroup is a subset H of $\mathbb{N}_0$ such that H is closed under addition, H contains the zero, and the complement set $\mathbb{N}_0 \setminus H$ is finite.*

The elements in the complement set $G := \mathbb{N}_0 \setminus H$ are called the gaps of the numerical semigroup H and $g_H := \#G$ is its genus. The largest gap is called the Frobenius number of H and is denoted by F_H, the smallest nonzero element of H is called the multiplicity of the semigroup and is denoted by m_H, and the numerical semigroup H is called symmetric if $F_H = 2g_H - 1$.

A subset $\{a_1, \ldots, a_d\} \subset H$ is called a system of generators of the numerical semigroup H if

$$H = \langle a_1, \ldots, a_d \rangle := \{t_1 a_1 + \cdots + t_d a_d : t_1, \ldots, t_d \in \mathbb{N}_0\}.$$

We say that a system of generators of H is a minimal system of generators if none of its proper subsets generates the numerical semigroup H. The cardinality of a minimal system of generators of H is called the embedding dimension of H and will be denoted by e_H. For the case of numerical semigroups generated by two elements, that is $H = \langle a_1, a_2 \rangle$ with $(a_1, a_2) = 1$, we have that $g_H = (a_1 - 1)(a_2 - 1)/2$, $F_H = a_1 a_2 - a_1 - a_2$ and $e_H = 2$, see [55, Proposition 2.13]. Furthermore, we can characterize the elements of $\langle a_1, a_2 \rangle$ as follows.

Proposition 1.1.2. *[54, Lemma 1] Let $x \in \mathbb{Z}$ and let $a_1, a_2 \geq 2$ be integers such that $(a_1, a_2) = 1$. Then $x \notin \langle a_1, a_2 \rangle$ if and only if $x = a_1 a_2 - n a_1 - m a_2$ for some $n, m \in \mathbb{N}$.*

On the other hand, one of the most useful tools in the theory of numerical semigroups are Apéry sets since many of the properties of numerical semigroups can be characterized by these sets.

Definition 1.1.3. *Let n be a nonzero element of the numerical semigroup H. The Apéry set of n in H is defined by*

$$\mathrm{Ap}(H, n) := \{s \in H : s - n \notin H\}.$$

It is known that the cardinality of $\mathrm{Ap}(H, n)$ is n and that several useful results are associated with the Apéry set as shown in the following results.

Proposition 1.1.4. *[55, Proposition 2.12] Let H be a numerical semigroup and $S \subseteq H$ be a subset that consists of n elements that form a complete set of representatives for the congruence classes of $\mathbb{Z}$ modulo $n \in H$. Then*

$$S = \mathrm{Ap}(H, n) \quad \textit{if and only if} \quad g_H = \sum_{a \in S} \left\lfloor \frac{a}{n} \right\rfloor.$$

Proposition 1.1.5. *[55, Proposition 4.10] Let H be a numerical semigroup and let n be a nonzero element of H. Let $\mathrm{Ap}(H, n) = \{a_0 < a_1 < \cdots < a_{n-1}\}$ be the Apéry set of n in H. Then H is symmetric if and only if*

$$a_i + a_{n-1-i} = a_{n-1} \ \textit{for each } i = 0, \ldots, n-1.$$

1.2 Algebraic curves over finite fields

Let q be the power of a prime p, $\mathbb{F}_q$ the finite field with q elements, and K the algebraic closure of $\mathbb{F}_q$. For a nonsingular, projective, absolutely irreducible algebraic curve (or simply curve) $\mathcal{X}$ with genus $g(\mathcal{X})$, we denote by $F = K(\mathcal{X})$ its function field, by $\mathcal{P}_F$ the set of places of F, and by ν_P the discrete valuation of F associated to the place $P \in \mathcal{P}_F$. Also, we denote by $\mathrm{Div}(F)$ the group of divisors of F, and for a function $z \in F$ we let $(z)_F, (z)_\infty$ and $(z)_0$ stand for the principal, pole and zero divisors of the function z in F respectively. Furthermore, when the curve $\mathcal{X}$ is defined over $\mathbb{F}_q$, we denote by $\mathcal{X}(\mathbb{F}_q)$ its set of $\mathbb{F}_q$-rational points and, due to the one-to-one correspondence between algebraic function fields of one variable and algebraic curves, we consider a rational point on the curve is the same as a rational place (place of degree one) on the function field of the curve.

One of the main objects to study in this thesis are the Weierstrass semigroups associated to a place, which are defined below.

Definition 1.2.1. *Let $P \in \mathcal{P}_F$ be a place of F. The Weierstrass semigroup associated to P is defined by the set*

$$H(P) = \{n \in \mathbb{N}_0 : (z)_\infty = nP \text{ for some } z \in F\}$$

and the complementary set $G(P) := \mathbb{N}_0 \setminus H(P)$ is called the gap set at P.

As a consequence of Riemann-Roch Theorem [56, Theorem 1.5.15], we obtain that the gap set at a place is finite and therefore Weierstrass semigroups are numerical semigroups. More specifically, we have the following result.

Theorem 1.2.2. *[56, Theorem 1.6.8] Let $F = K(\mathcal{X})$ be the function field of the curve $\mathcal{X}$ with genus $g(\mathcal{X}) > 0$ and $P \in \mathcal{P}_F$ be a place. Then $\#G(P) = g(\mathcal{X})$ and*

$$G(P) = \{1 = i_1 < i_2 < \cdots < i_{g(\mathcal{X})} \leq 2g(\mathcal{X}) - 1\}.$$

It is a well-known fact that for all but finitely many places $P \in \mathcal{P}_F$, the gap set is always the same. This set is called the gap sequence of $\mathcal{X}$. The places for which the gap set is not equal to the gap sequence of $\mathcal{X}$ are called Weierstrass places.

Now, let $\mathcal{X}$ and $\mathcal{Y}$ be algebraic curves with function fields $F = K(\mathcal{X})$ and $F' = K(\mathcal{Y})$ respectively. Assume that $F \subseteq F'$ and F'/F is an algebraic extension. Next, we present some results about extensions of function fields.

Definition 1.2.3. *A place $P \in \mathcal{P}_{F'}$ is said to lie over $P \in \mathcal{P}_F$ if $P \subseteq P'$. We also say that P' is an extension of P and we write $P'|P$.*

Proposition 1.2.4. *[56, Proposition 3.1.4] Let $P \in \mathcal{P}_F$ and $P' \in \mathcal{P}_{F'}$. Then the following statements are equivalents:*

i) $P'|P$.

ii) There exists a positive integer $e(P'|P)$ called ramification index of the extension $P'|P$ satisfying $\nu_{P'}(x) = e(P'|P)\nu_P(x)$ for all $x \in F$.

Since for each $P' \in \mathcal{P}_{F'}$ there exists a unique $P \in \mathcal{P}_F$ such that $P'|P$, then for simplicity we will often denote by $e(P')$ the ramification index of the extension $P'|P$ in F'/F. In the case that the extension $[F' : F]$ is finite, we say that a place $P \in \mathcal{P}_F$

is totally ramified in the extension F'/F if there is a place $P' \in \mathcal{P}_{F'}$ with $P'|P$ and $e(P'|P) = [F' : F]$, and we say that P splits completely in F'/F if there are exactly $[F' : F]$ distinct places $P' \in \mathcal{P}_{F'}$ with $P'|P$.

Definition 1.2.5. *For a place $P \in \mathcal{P}_F$, we define the conorm of P with respect to the extension F'/F as*

$$\mathrm{Con}_{F'/F}(P) := \sum_{\substack{P' \in \mathcal{P}_{F'} \\ P'|P}} e(P'|P)P'.$$

Note that the conorm can be extended to a group homomorphism from $\mathrm{Div}(F)$ to $\mathrm{Div}(F')$ by setting

$$\mathrm{Con}_{F'/F}\left(\sum n_P P\right) := \sum n_P \mathrm{Con}_{F'/F}(P).$$

Furthermore, one of the most interesting properties of the conorm is that it preserves principal divisors.

Proposition 1.2.6. *[56, Proposition 3.1.9] For a function $0 \neq z \in F$, we have that*

$$\mathrm{Con}_{F'/F}((z)_F) = (z)_{F'}.$$

In the theory of algebraic curves, the Riemann-Hurwitz formula is one of the fundamental theorems. This result relates, by means of a closed formula, the genus of the algebraic curves $\mathcal{X}$ and $\mathcal{Y}$ when $K(\mathcal{Y})/K(\mathcal{X})$ is a finite separable extension. Here we present a particular case of the Riemann-Hurwitz formula that will be useful in the development of the thesis. For a more general version see [56, Theorem 3.4.13].

Theorem 1.2.7 (Riemann-Hurwitz formula)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be algebraic curves with function fields $F = K(\mathcal{X})$ and $F' = K(\mathcal{Y})$ respectively. Suppose that F'/F is a finite separable extension and assume that $p \nmid e(P'|P)$ for all extensions of places $P'|P$ in the extension F'/F. Then*

$$2g(\mathcal{Y}) - 2 = (2g(\mathcal{X}) - 2)[F' : F] + \sum_{P \in \mathcal{P}_F} \sum_{\substack{P' \in \mathcal{P}_{F'} \\ P'|P}} (e(P'|P) - 1).$$

Next, we introduce a special type of extension of function fields called Kummer extensions. These types of extensions are a fundamental part of this thesis.

Proposition 1.2.8. *[56, Proposition 3.7.3] Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$ and $F = \mathbb{F}_q(\mathcal{X})$ be its function field. Suppose that $\mathbb{F}_q$ contains a primitive m-th root of unity where $m > 1$ and $p \nmid m$, and that $u \in F$ is an element satisfying*

$$u \neq w^d \text{ for all } w \in F \text{ and } d \mid m,\ d > 1.$$

Let

$$F' = F(y) \quad \text{with} \quad y^m = u.$$

Such an extension F'/F is said to be a Kummer extension of F. This extension is Galois of degree $[F' : F] = m$ and for $P \in \mathcal{P}_F$ and $P' \in \mathcal{P}_{F'}$ an extension of P, the ramification index of $P'|P$ is given by

$$e(P'|P) = \frac{m}{(m, \nu_P(u))}.$$

Now, to finish this chapter, we present some preliminary results with respect to the number of rational points on a curve over a finite field.

Several upper bounds for the number of rational points of algebraic curves are available in the literature. Next, we present some of these upper bounds starting with the best known, the Hasse Weil bound [56, Theorem 5.2.3].

Theorem 1.2.9 (Hasse-Weil bound)**.** *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$ with genus $g(\mathcal{X})$. Then*

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

Definition 1.2.10. *A curve $\mathcal{X}$ defined over $\mathbb{F}_q$ with genus $g(\mathcal{X})$ is called $\mathbb{F}_q$-maximal if equality holds in the Hasse-Weil bound, that is,*

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

Due to the following result given by Kleiman [37], we can construct new maximal curves as quotients of known maximal curves.

Theorem 1.2.11. *Let $\mathcal{X}$ and $\mathcal{Y}$ be algebraic curves defined over $\mathbb{F}_q$. If $\mathcal{X}$ is $\mathbb{F}_q$-maximal and $\mathcal{Y}$ is an $\mathbb{F}_q$-subcover of $\mathcal{X}$, that is $\mathbb{F}_q(\mathcal{Y}) \subseteq \mathbb{F}_q(\mathcal{X})$, then $\mathcal{Y}$ is also $\mathbb{F}_q$-maximal.*

Among other upper bounds for the number of rational points we have the Lewittes bound [38], and the Geil-Matsumoto bound [23] that improved the bound given by Lewittes.

Theorem 1.2.12 (Lewittes bound)**.** *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$ and let P be an $\mathbb{F}_q$-rational place of $\mathcal{X}$. Then*

$$\#\mathcal{X}(\mathbb{F}_q) \leq q m_{H(P)} + 1,$$

where $m_{H(P)}$ is the multiplicity of the Weierstrass semigroup $H(P)$.

Theorem 1.2.13 (Geil-Matsumoto bound)**.** *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$ and let P be an $\mathbb{F}_q$-rational place of $\mathcal{X}$. Then*

$$\#\mathcal{X}(\mathbb{F}_q) \leq GM_q(H(P)) := 1 + \#(H(P) \setminus (qH^*(P) + H(P))),$$

where $H^*(P) = H(P) \setminus \{0\}$ and $qH^*(P) + H(P) = \{qa + b : a \in H^*(P), b \in H(P)\}$.

In general, there is no closed formula for the Geil-Matsumoto bound. However, for Weierstrass semigroups generated by two elements, Bras-Amorós and Vico-Oton [11] provided the following closed formula for the Geil-Matsumoto bound.

Theorem 1.2.14. *[11, Theorem 3.2] The Geil-Matsumoto bound for the Weierstrass semigroup generated by two elements a and b with $a < b$ is given by*

$$GM_q(\langle a, b\rangle) = 1 + \sum_{n=0}^{a-1} \min\left\{q, \left\lceil \frac{q-n}{a} \right\rceil b\right\}.$$

On the other hand, the Lewittes bound allows us to define a new class of algebraic curves: the Castle curves. The notion of Castle curves were introduced by Munuera, Sepúlveda, and Torres in [47], and have been studied due to their interesting properties related to the construction of algebraic geometry codes with good parameters and its duals, see [46, 47].

Definition 1.2.15. *A pointed algebraic curve $(\mathcal{X}, P)$ over $\mathbb{F}_q$, where P is an $\mathbb{F}_q$-rational place of $\mathcal{X}$, is called a Castle curve if the semigroup $H(P)$ is symmetric and equality holds in the Lewittes bound.*

Finally, we present the following remark that will be useful for the calculation of the number of rational points of a curve defined by a Kummer extension. For a more general version see [50, Theorems 3 and 4].

Remark 1.2.16. *Let $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ be a Kummer extension of degree m defined by the equation $Y^m = h(X)$, where m is a divisor of $q - 1$ and $h \in \mathbb{F}_q(X)$. For each $\alpha \in \mathbb{F}_q$, we write*

$$h(X) = (X - \alpha)^{k_\alpha} h_\alpha(X),$$

where $k_\alpha \in \mathbb{Z}$, $h_\alpha \in \mathbb{F}_q(x)$, and α is neither a zero nor a pole of h_α. Then there exist either no or exactly (m, k_α) $\mathbb{F}_q$-rational places of $\mathbb{F}_q(x, y)$ over P_α. In fact, there exists an $\mathbb{F}_q$-rational place of $\mathbb{F}_q(x, y)$ over P_α if and only if $g_\alpha(\alpha)$ is a (m, k_α)-power in $\mathbb{F}_q^*$. Moreover, suppose

$$h(X) = c_\infty \frac{g_1(X)}{g_2(X)}$$

where $c_\infty \in \mathbb{F}_q^*$ and g_1, g_2 are monic polynomials in $\mathbb{F}_q[X]$ with $(g_1, g_2) = 1$. Then there exist either no or exactly $(m, \deg\, g_2 - \deg\, g_1)$ $\mathbb{F}_q$-rational places of $\mathbb{F}_q(x, y)$ over P_∞. In the case of P_∞, there exists an $\mathbb{F}_q$-rational place of $\mathbb{F}_q(x, y)$ over P_∞ if and only if c_∞ is a $(m, \deg\, g_2 - \deg\, g_1)$-power in $\mathbb{F}_q^*$.

For more on function fields and algebraic curves, we refer to the books [18] and [56].

2 Maximal curves as subcovers of the Beelen-Montanucci curve

For decades many of the known maximal curves were obtained as, or proved to be, Galois subcovers of the Hermitian curve. This raised the question of whether any maximal curve could be covered by the Hermitian curve. In 2009, Giulietti and Korchmáros introduced the first example of a maximal curve not covered by the Hermitian curve, see [24]. This curve is defined over $\mathbb{F}_{q^6}$ by the affine equations

$$GK : \begin{cases} Z^{q^2-q+1} = Y \sum_{i=0}^{q} (-1)^{i+1} X^{i(q-1)} \\ Y^{q+1} = X^q + X \end{cases} . \tag{2.1}$$

In the following years, two generalizations of the GK curve were presented, that is, maximal curves over $\mathbb{F}_{q^{2n}}$ for $n \geq 3$ odd and isomorphic to the GK in the case $n = 3$. The first such generalization is the so-called GGS curve, described in [20] by Garcia, Güneri and Stichtenoth

$$GGS : \begin{cases} Z^{\frac{q^n+1}{q+1}} = Y^{q^2} - Y \\ Y^{q+1} = X^q + X \end{cases} . \tag{2.2}$$

This curve is maximal over $\mathbb{F}_{q^{2n}}$ with genus $g(GGS) = (q-1)(q^{n+1} + q^n - q^2)/2$, and for $n \geq 5$ its full automorphism group over $\mathbb{F}_{q^{2n}}$ has size $\#\mathrm{Aut}(GGS) = q^3(q-1)(q^n+1)$, see [30, Theorem 3.10].

Applying a suitable $\mathbb{F}_{q^2}$-projectivity, a new equation for the GK curve over $\mathbb{F}_{q^6}$ was introduced in [27] by Giulietti, Quoos, and Zini. It is defined by the complete intersection

$$GQZ : \begin{cases} Z^{q^2-q+1} = Y \frac{X^{q^2}-X}{X^{q+1}-1} \\ Y^{q+1} = X^{q+1} - 1 \end{cases} . \tag{2.3}$$

This new equation allowed the determination of some explicit equations of maximal curves covered by the GK curve, as well as that of the Galois group corresponding to the cover in some cases.

For $n \geq 3$ odd, a natural generalization of the GQZ curve was investigated in [7] by Beelen and Montanucci, and we denote it by BM. It is defined by the affine equations

$$BM : \begin{cases} Z^{\frac{q^n+1}{q+1}} = Y \left(\frac{X^{q^2}-X}{X^{q+1}-1} \right) \\ Y^{q+1} = X^{q+1} - 1 \end{cases} . \tag{2.4}$$

The BM curve can also be seen as a generalization of the GK curve since it is maximal over $\mathbb{F}_{q^{2n}}$ with genus satisfying $g(BM) = g(GGS)$ for $n \geq 3$. Surprisingly, despite being maximal and having the same genus as the GGS curve, the BM curve is not isomorphic to GGS

for $n \geq 5$. In fact, for $n \geq 5$, the full automorphism group $\mathrm{Aut}(BM) \cong SL(2,q) \rtimes C_{q^n+1}$ has order $q(q^2-1)(q^n+1)$, see [7, Theorem 4.3].

In [8], Beelen and Montanucci determined genera of Galois subcovers of the BM curves for $n \geq 5$. They work from the point of view of finite group theory, using the classification of maximal subgroups of $\mathrm{PGU}(3,q)$ and studying the action of the automorphism group on the rational points on the curve. For the cases $(n, q+1) = 1$ and q a power of 2, or $(n, q+1) = 1$ and $q \equiv 1 \pmod 4$, they obtain all the genera.

From the point of view of applications, our goal in this chapter is to provide a number of explicit equations for Galois subcovers of the BM curve over $\mathbb{F}_{q^{2n}}$. These curves are obtained as fixed field of certain subgroups of the automorphism group of the BM curve for n odd and $n \geq 3$. The genus, as well an explicit description of the Galois subgroup of $\mathrm{Aut}(BM)$ associated to the covering are provided.

Throughout the chapter we let p be a prime number, q a power of p, and for $n \geq 3$ an odd integer we write $m = (q^n+1)/(q+1)$. For $k \geq 1$ we let $\mathcal{C}_k$ stand for the cyclic group of order k. Moreover, for H a subgroup of the automorphism group $\mathrm{Aut}(\mathcal{X})$ of a curve $\mathcal{X}$ defined over $\mathbb{F}_q$, we denote by $\mathrm{Fix}(H) \subset \mathbb{F}_q(\mathcal{X})$ the field fixed by H. Then we have that the extension $\mathbb{F}_q(\mathcal{X})/\mathrm{Fix}(H)$ is Galois and the function field $\mathrm{Fix}(H)$ corresponds to the quotient curve $\mathcal{X}/H$ of $\mathcal{X}$ with respect to the automorphism subgroup H.

2.1 Quotient curves from the first new model of the BM curve

In this section, we present two families of maximal curves over $\mathbb{F}_{q^{2n}}$ depending on certain parameters given by divisors of $q+1, q-1, m$, and q^n+1.

Applying the morphism $\varphi(X,Y,Z) = (\frac{X}{Y}, \frac{1}{Y}, \frac{Z}{Y})$ to the curve (2.3) defined by the equations

$$\begin{cases} Z^{q^2-q+1} = Y\frac{X^{q^2}-X}{X^{q+1}-1} \\ Y^{q+1} = X^{q+1}-1 \end{cases},$$

we obtain a birationally equivalent curve

$$\mathcal{X} : \begin{cases} Z^{q^2-q+1} = X^{q^2}Y - XY^{q^2} \\ Y^{q+1} = X^{q+1}-1 \end{cases},$$

which will prove useful for dealing with subgroups of the automorphism group of the curve explicitly. For $n \geq 3$ odd, it is natural to consider the following generalization of the curve $\mathcal{X}$ given by

$$\mathcal{X}_n : \begin{cases} Z^{m} = X^{q^2}Y - XY^{q^2} \\ Y^{q+1} = X^{q+1}-1 \end{cases}. \tag{2.5}$$

We now show that the curves $\mathcal{X}_n$ and BM in (2.4) are in fact isomorphic. Let x, y, w be functions in the function field $\mathbb{F}_{q^{2n}}(BM)$ satisfying $w^m = y\left(\frac{x^{q^2}-x}{x^{q+1}-1}\right)$ and $y^{q+1} = x^{q+1}-1$;

and $x, y, z \in \mathbb{F}_{q^{2n}}(\mathcal{X}_n)$ be such that $z^m = x^{q^2}y - xy^{q^2}$ and $y^{q+1} = x^{q+1} - 1$. Then

$$\begin{aligned} z^m = x^{q^2}y - xy^{q^2} &= xy(x^{q^2-1} - y^{q^2-1}) \\ &= xy(x^{q^2-1} - (x^{q+1}-1)^{q-1}) \\ &= xy\left(x^{q^2-1} - \frac{x^{q^2+q}-1}{x^{q+1}-1}\right) \\ &= -xy\left(\frac{x^{q^2-1}-1}{x^{q+1}-1}\right) = -w^m = (-w)^m, \end{aligned} \tag{2.6}$$

and we conclude that $w = -\zeta z$, for some $\zeta \in \mathbb{F}_{q^{2n}}, \zeta^m = 1$. This yields equality of the function fields $\mathbb{F}_{q^{2n}}(\mathcal{X}_n)$ and $\mathbb{F}_{q^{2n}}(BM)$. In particular, the automorphisms groups $\mathrm{Aut}(\mathcal{X}_n)$ and $\mathrm{Aut}(BM)$ are isomorphic. It is easy to check that the full automorphism group $\mathrm{Aut}(BM)$ as described in [8, Section 2] acts on the curve $\mathcal{X}_n$, so

$$\mathrm{Aut}(\mathcal{X}_n) = \{\sigma_{a,c,\xi} : a^{q+1} - c^{q+1} = 1,\ \xi^{q^n+1} = 1\}, \tag{2.7}$$

where

$$\sigma_{a,c,\xi} : (X, Y, Z) \mapsto (aX + c^q\xi^m Y, cX + a^q\xi^m Y, \xi Z).$$

Let d_1 and d_2 be divisors of $q+1$, and d be a divisor of q^n+1. Consider the functions

$$u := x^{(q+1)/d_1}, \quad v := y^{(q+1)/d_2} \quad \text{and} \quad w := z^{(q^n+1)/d}.$$

From Equation (2.5), we conclude the functions u, v and w satisfy the following algebraic relations

$$\begin{aligned} \bullet\, v^{d_2} &= u^{d_1} - 1, \text{ and} \\ \bullet\, w^d &= x^{q+1}y^{q+1}((x^{q+1})^{q-1} - (y^{q+1})^{q-1})^{q+1} \\ &= x^{q+1}(x^{q+1}-1)((x^{q+1})^{q-1} - (x^{q+1}-1)^{q-1})^{q+1} \\ &= x^{q+1}(x^{q+1}-1)\left((x^{q+1})^{q-1} - \frac{(x^{q+1})^q - 1}{x^{q+1}-1}\right)^{q+1} \\ &= \frac{x^{q+1}(1-(x^{q+1})^{q-1})^{q+1}}{(x^{q+1}-1)^q} \\ &= \frac{u^{d_1}(1-u^{d_1(q-1)})^{q+1}}{(u^{d_1}-1)^q} \\ &= u^{d_1}(u^{d_1}-1)\left(\frac{u^{d_1(q-1)}-1}{u^{d_1}-1}\right)^{q+1}. \end{aligned}$$

Thus, we can present the following result.

Theorem 2.1.1. *Let d_1 and d_2 be divisors of $q+1$, and d be a divisor of q^n+1 such that $\left(d_2, d, \frac{dd_1}{(d,2d_1)}\right) = 1$. Then the affine equations*

$$\begin{cases} W^d = U^{d_1}(U^{d_1}-1)\left(\frac{U^{d_1(q-1)}-1}{U^{d_1}-1}\right)^{q+1} \\ V^{d_2} = U^{d_1}-1 \end{cases} \tag{2.8}$$

define an $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{Y}_{d_1,d_2,d}$ of genus

$$g = 1 + \frac{1}{2}(dd_1d_2(q-1) - d_1d_2(q-2)(d,q+1) - d_2(d,d_1) - d_1(d,d_2) - (2d_1d_2, dd_1, dd_2)).$$

Moreover, the curve $\mathcal{Y}_{d_1,d_2,d}$ is the quotient curve $\mathcal{X}_n/H_{d_1,d_2,d}$, where the subgroup $H_{d_1,d_2,d}$ is given by

$$H_{d_1,d_2,d} = \left\{\sigma_{a,0,\xi} : (X,Y,Z) \mapsto (aX, a^q\xi^mY, \xi Z) : a^{\frac{q+1}{d_1}} = 1,\, (a^q\xi^m)^{\frac{q+1}{d_2}} = 1,\, \xi^{\frac{q^n+1}{d}} = 1\right\}.$$

Proof. We start by proving that $H_{d_1,d_2,d}$ is a $\mathbb{F}_{q^{2n}}$-automorphism subgroup of $\mathrm{Aut}(\mathcal{X}_n)$ and $\mathbb{F}_{q^{2n}}(u,v,w) \subseteq \mathrm{Fix}(H_{d_1,d_2,d})$. It is clear that $H_{d_1,d_2,d} \neq \emptyset$ is a finite subset of $\mathrm{Aut}(\mathcal{X}_n)$, therefore to prove that $H_{d_1,d_2,d}$ is a subgroup of $\mathrm{Aut}(\mathcal{X}_n)$ it is enough to prove that $H_{d_1,d_2,d}$ is closed under multiplication. For $\sigma_{a_1,0,\xi_1}, \sigma_{a_2,0,\xi_2} \in H_{d_1,d_2,d}$, we have that

$$\begin{aligned}\sigma_{a_2,0,\xi_2}\sigma_{a_1,0,\xi_1} &= \begin{pmatrix} a_2 & 0 & 0 \\ 0 & a_2^q\xi_2^m & 0 \\ 0 & 0 & \xi_2 \end{pmatrix}\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_1^q\xi_1^m & 0 \\ 0 & 0 & \xi_1 \end{pmatrix} \\ &= \begin{pmatrix} a_1a_2 & 0 & 0 \\ 0 & (a_1a_2)^q(\xi_1\xi_2)^m & 0 \\ 0 & 0 & \xi_1\xi_2 \end{pmatrix} \\ &= \sigma_{a_1a_2,0,\xi_1\xi_2}\end{aligned}$$

and

$$(a_1a_2)^{\frac{q+1}{d_1}} = [(a_1a_2)^q(\xi_1\xi_2)^m]^{\frac{q+1}{d_2}} = (\xi_1\xi_2)^{\frac{q^n+1}{d}} = 1.$$

This implies that $H_{d_1,d_2,d}$ is subgroup of $\mathrm{Aut}(\mathcal{X}_n)$. On the other hand, it is clear the functions $u = x^{(q+1)/d_1}, v = y^{(q+1)/d_2}$, and $w = z^{(q^n+1)/d} \in \mathbb{F}_{q^{2n}}(\mathcal{X}_n)$ satisfy Equation (2.8). Furthermore, for $\sigma_{a,0,\xi} \in H_{d_1,d_2,d}$,

$$\begin{aligned}\sigma_{a,0,\xi}(U) &= \sigma_{a,0,\xi}(X^{\frac{q+1}{d_1}}) = (aX)^{\frac{q+1}{d_1}} = a^{\frac{q+1}{d_1}}X^{\frac{q+1}{d_1}} = U, \\ \sigma_{a,0,\xi}(V) &= \sigma_{a,0,\xi}(Y^{\frac{q+1}{d_2}}) = (a^q\xi^mY)^{\frac{q+1}{d_2}} = (a^q\xi^m)^{\frac{q+1}{d_2}}Y^{\frac{q+1}{d_2}} = V, \text{ and} \\ \sigma_{a,0,\xi}(W) &= \sigma_{a,0,\xi}(Z^{\frac{q^n+1}{d}}) = (\xi Z)^{\frac{q^n+1}{d}} = \xi^{\frac{q^n+1}{d}}Z^{\frac{q^n+1}{d}} = W.\end{aligned}$$

This implies that $\mathbb{F}_{q^{2n}}(u,v,w) \subseteq \mathrm{Fix}(H_{d_1,d_2,d})$.

Now, consider the double extension of function fields

$$\mathbb{F}_{q^{2n}}(u,v,w) \subseteq \mathrm{Fix}(H_{d_1,d_2,d}) \subseteq \mathbb{F}_{q^{2n}}(x,y,z) = \mathbb{F}_{q^{2n}}(\mathcal{X}_n).$$

As $\mathbb{F}_{q^{2n}}(\mathcal{X}_n)/\mathrm{Fix}(H_{d_1,d_2,d})$ is Galois, we have $[\mathbb{F}_{q^{2n}}(\mathcal{X}_n) : \mathrm{Fix}(H_{d_1,d_2,d})] = \# H_{d_1,d_2,d}$. From (2.6) we get $y \in \mathbb{F}_{q^{2n}}(x,z)$. So

$$[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(u,v,w)] = [\mathbb{F}_{q^{2n}}(x,z) : \mathbb{F}_{q^{2n}}(u,v,w)] = \frac{[\mathbb{F}_{q^{2n}}(x,z) : \mathbb{F}_{q^{2n}}(u,w)]}{[\mathbb{F}_{q^{2n}}(u,v,w) : \mathbb{F}_{q^{2n}}(u,w)]} \leq \frac{(q+1)(q^n+1)}{d_1 d_2 d}.$$

To conclude that $\mathbb{F}_{q^{2n}}(u,v,w) = \mathrm{Fix}(H_{d_1,d_2,d})$, it remains to show that the subgroup $H_{d_1,d_2,d}$ has cardinality $\frac{(q+1)(q^n+1)}{d_1 d_2 d}$. Let $\tau \in \mathbb{F}_{q^{2n}}$ be a primitive (q^n+1)-th root of unity. For each $a \in \mathcal{C}_{\frac{q+1}{d_1}}$, let $i \in \mathbb{Z}$ be such that $a = \tau^{imd_1}$ and R_a be the set defined by $R_a := \left\{ \xi \in \mathcal{C}_{\frac{q^n+1}{d}} : (a^q \xi^m)^{\frac{q+1}{d_2}} = 1 \right\}$, then $\# H_{d_1,d_2,d} = \sum_{a \in \mathcal{C}_{(q+1)/d_1}} \# R_a$. We notice that

$$\left(d, \frac{dd_1}{(d,2d_1)}\right) = \begin{cases} d, & \text{if } d \text{ is odd,} \\ \frac{d}{2}\left(2, \frac{2d_1}{(d,2d_1)}\right), & \text{if } d \text{ is even.} \end{cases}$$

Therefore, from the condition $\left(d_2, d, \frac{dd_1}{(d,2d_1)}\right) = 1$, we deduce that $(d,d_2) = 1$ or $(d,d_2) = 2$. Now we analyze both cases.

Case 1: $(d,d_2) = 1$. We prove that $\# R_a = \frac{q^n+1}{d_2 d}$ for any a. For this, it is sufficient to prove that R_a is not empty, since if $\gamma \in R_a$, then $R_a = \gamma \mathcal{C}_{\frac{q^n+1}{d_2 d}}$. Also, since $(d_2, d) = 1$, there are $k, j \in \mathbb{Z}$ such that $kd_2 - jd = iqd_1$. Thus, $\varrho = \tau^{jd} \in \mathcal{C}_{\frac{q^n+1}{d}}$ and

$$(a^q \varrho^m)^{\frac{q+1}{d_2}} = (\tau^{iqmd_1} \tau^{jmd})^{\frac{q+1}{d_2}} = (\tau^{m(iqd_1+jd)})^{\frac{q+1}{d_2}} = \tau^{(q^n+1)k} = 1.$$

This implies $\varrho = \tau^{jd} \in R_a$.

Case 2: $(d,d_2) = 2$. Note that necessarily q and d_1 are odd, and $\frac{q+1}{d_1}$ is even. In this case, we prove that

$$\# R_a = \begin{cases} \frac{2(q^n+1)}{d_2 d}, & \text{if } i \text{ is even,} \\ 0, & \text{if } i \text{ is odd.} \end{cases}$$

Suppose that i is odd and $R_a \neq \emptyset$, then there exists $\xi \in R_a$ and $j \in \mathbb{Z}$ such that $\xi = \tau^{jd}$. Thus,

$$1 = (a^q \xi^m)^{\frac{q+1}{2}} = (\tau^{iqmd_1} \tau^{jdm})^{\frac{q+1}{d_2}} = \tau^{\frac{(iqd_1+jd)(q^n+1)}{d_2}}$$

and therefore d_2 divides $iqd_1 + jd$. This is a contradiction since $iqd_1 + jd$ is odd and d_2 is even.

Now suppose that i is even. For this, it is sufficient to prove that R_a is not empty, since if $\gamma \in R_a$, then $R_a = \gamma \mathcal{C}_{\frac{2(q^n+1)}{d_2 d}}$. Also, since i is even and $(d,d_2) = 2$, then there are $k, j \in \mathbb{Z}$ such that $kd_2 - jd = iqd_1$. Using an argument analogous to the one used in the case $(d,d_2) = 1$ it is easy to show that $R_a \neq \emptyset$. We conclude that $\# H_{d_1,d_2,d} = \sum_{a \in \mathcal{C}_{(q+1)/d_1}} \# R_a = \frac{(q+1)(q^n+1)}{d_1 d_2 d}$.

Let $\mathbb{F}_{q^{2n}}(\mathcal{Y}_{d_1,d_2,d}) = \mathbb{F}_{q^{2n}}(u,v,w)$. Denote by $\alpha_1, \alpha_2, \ldots, \alpha_{d_1(q-1)}$ the roots in K of the separable polynomial $f(U) = U^{d_1(q-1)} - 1$, where the first d_1 elements $\alpha_1, \alpha_2, \ldots, \alpha_{d_1}$

are the roots of the polynomial $g(U) = U^{d_1} - 1$. We compute the following principal divisor in $K(u)$:

$$\begin{aligned}\left(\frac{u^{d_1} f(u)^{q+1}}{g(u)^q}\right)_{K(u)} &= d_1(u)_{K(u)} + (q+1)(f(u))_{K(u)} - q(g(u))_{K(u)} \\ &= d_1 P_0 + \sum_{i=1}^{d_1} P_{\alpha_i} + (q+1) \sum_{i=d_1+1}^{d_1(q-1)} P_{\alpha_i} - d_1 q(q-1) P_\infty,\end{aligned}$$

where P_{α_i}, P_0, and P_∞ are the places corresponding to α_i, 0, and the pole of u respectively. We conclude that $K(u,w)/K(u)$ is a Kummer extension of degree d. For P a place in $\mathcal{P}_{K(u,w)}$, the ramification indices of the ramified places in the extension $K(u,w)/K(u)$ are given by

$$e(P) = \begin{cases} d/(d,d_1), & \text{if } P \text{ is over } P_0, \\ d, & \text{if } P \text{ is over } P_{\alpha_i} \text{ for } i = 1,\dots,d_1, \\ d/(d,q+1), & \text{if } P \text{ is over } P_{\alpha_i} \text{ for } i = d_1+1,\dots,d_1(q-1), \\ d/(d,2d_1), & \text{if } P \text{ is over } P_\infty. \end{cases}$$

By the Riemann-Hurwitz formula, the genus of the function field $K(u,w)$ is given by

$$g(K(u,w)) = \frac{dd_1(q-1) - d_1 - d_1(q-2)(d,q+1) - (d,d_1) - (d,2d_1) + 2}{2}.$$

We now show that the extension $K(u,w,v)/K(u,w)$ is a Kummer extension and compute the genus of $K(\mathcal{Y}_{d_1,d_2,d})$. We start by computing the principal divisor of $u^{d_1} - 1$ in $K(u,v)$

$$(u^{d_1} - 1)_{K(u,w)} = d \sum_{i=1}^{d_1} Q_{\alpha_i} - \frac{dd_1}{(d,2d_1)} \sum_{i=1}^{(d,2d_1)} Q_{\infty,i},$$

where Q_{α_i} and $Q_{\infty,i}$ are the extensions of the places P_{α_i} and P_∞, respectively. From the condition $\left(d_2, d, \frac{dd_1}{(d,2d_1)}\right) = 1$, we conclude the extension $K(u,w,v)/K(u,w)$ is a Kummer extension of degree d_2 with ramification indices given by

$$e(P) = \begin{cases} d_2/(d_2,d), & \text{if } P \text{ is over } Q_{\alpha_i}, \\ d_2(2d_1,d)/(2d_1d_2, dd_1, dd_2), & \text{if } P \text{ is over } Q_{\infty,i}, \\ 1, & \text{in the other cases.} \end{cases}$$

Thus we conclude that Equation (2.8) defines an absolutely irreducible curve. The calculation of the genus g of the function field $K(u,v,w)$ follows from the Riemann-Hurwitz formula

$$2g - 2 = d_2(2g(K(u,w)) - 2) + d_1d_2 - d_1(d_2,d) + d_2(d,2d_1) - (2d_1d_2, dd_1, dd_2).$$

□

Remark 2.1.2. *In Theorem 2.1.1, for $n = 3$ (d_1 and d_2 divisors of $q+1$, and d a divisor of q^2-q+1), we obtain quotient curves of the GK curve defined by*

$$\begin{cases} W^d = U^{d_1}V^{d_2}\left(\frac{U^{d_1(q-1)}-1}{U^{d_1}-1}\right)^{q+1} \\ V^{d_2} = U^{d_1}-1 \end{cases}$$

corresponding to the subgroup

$$H_{d_1,d_2,d} = \left\{\sigma_{a,0,\xi} : a^{\frac{q+1}{d_1}} = 1,\ (a^q\xi^{q^2-q+1})^{\frac{q+1}{d_2}} = 1,\ \xi^{\frac{q^3+1}{d}} = 1\right\} < \mathrm{Aut}(\mathcal{X}_3).$$

These quotient curves were studied in [27], where the genus was computed for $d = d_3(q^2-q+1)$ and d_3 is a divisor of $q+1$, see [27, Theorem 3.3]. Moreover, assuming

$$(d_1, d_2, d) = 1,$$

the corresponding subgroups were provided for two particular cases: (1) $d_1 \mid 3d_3$ and $(d_1, d_2) = 1$, and (2) $d_1 \mid d_2$ and $(d_1, d) = 1$, see [27, Section 4].

Theorem 2.1.1 generalizes this result, providing the genus and the corresponding subgroups for all values of d_1, d_2 and d satisfying the condition $\left(d_2, d, \frac{dd_1}{(d,2d_1)}\right) = 1$. Also the families of curves provided in [27, Section 5] for d_4 a divisor of q^2-q+1 given by

$$\mathcal{Z} : \begin{cases} W_1^{d_4} = V_1(1 + U_1^{d_1} + U_1^{2d_1} + \cdots + U_1^{(q-2)d_1}) \\ V_1^{q+1} = U_1^{2d_1} - U_1^{d_1} \end{cases}$$

are covered by the curve in Theorem 2.1.1. To see this, notice that the functions w_1 and u_1 satisfy

$$\begin{aligned} w_1^{d_4(q+1)} &= (v_1(1 + u_1^{d_1} + u_1^{2d_1} + \cdots + u_1^{(q-2)d_1}))^{q+1} \\ &= v_1^{q+1}\left(\frac{u_1^{d_1(q-1)}-1}{u_1^{d_1}-1}\right)^{q+1} \\ &= u_1^{d_1}(u_1^{d_1}-1)\left(\frac{u_1^{d_1(q-1)}-1}{u_1^{d_1}-1}\right)^{q+1}. \end{aligned}$$

Thus $\mathbb{F}_{q^6}(\mathcal{Z}) = \mathbb{F}_{q^6}(u_1, v_1, w_1) = \mathbb{F}_{q^6}(u_1, w_1) = \mathbb{F}_{q^6}(\mathcal{Y}_{d_1,1,d_4(q+1)})$. Moreover, the curve defined by the second equation $W^{d_4(q+1)} = U^{d_1}(U^{d_1}-1)\left(\frac{U^{d_1(q-1)}-1}{U^{d_1}-1}\right)^{q+1}$ also appears in [7, Remark 4.6] and corresponds to the subgroup

$$H_{d_1,1,d_4(q+1)} = \left\{\sigma_{a,0,\xi} : (X,Y,Z) \mapsto (aX, a^qY, \xi Z) : a^{\frac{q+1}{d_1}} = 1,\ \xi^{\frac{m}{d_4}} = 1\right\}.$$

As a direct consequence of Theorem 2.1.1, we provide a plane model for the curve $\mathcal{X}_n$.

Corollary 2.1.3. *The curve $\mathcal{X}_n$ is birationaly equivalent over $\mathbb{F}_{q^{2n}}$ to the plane curve with affine equation*

$$Z^{q^n+1} = X^{q+1}(X^{q+1}-1)((X^{q+1}-1)^{q-1} - X^{q^2-1})^{q+1}. \tag{2.9}$$

Proof. In Theorem 2.1.1, for $d_1 = q+1$, $d_2 = 1$, and $d = q^n + 1$ we get

$$\begin{aligned} w^{q^n+1} &= u^{q+1}(u^{q+1}-1)\left(\frac{u^{q^2-1}-1}{u^{q+1}-1}\right)^{q+1} \\ &= u^{q+1}(u^{q+1}-1)((u^{q+1}-1)^{q-1} - u^{q^2-1})^{q+1} \end{aligned}$$

and $g(K(u,w)) = g(\mathcal{X}_n)$. □

Now consider the $\mathbb{F}_{q^{2n}}$-automorphism subgroup of $\mathrm{Aut}(\mathcal{X}_n)$ defined by

$$H = \left\{ \sigma_{a,c,\xi} \in \mathrm{Aut}(\mathcal{X}_n) : a^{q+1} - c^{q+1} = 1, \xi^m = 1 \right\}$$

of order $q(q-1)(q^n+1)$. In the following, we provide a family of quotient curves corresponding to subgroups of H.

Theorem 2.1.4. *Let d_1 and d be divisors of $q-1$ and m respectively. The equation*

$$W^d = \frac{1 - U^{d_1(q+1)}}{U^{d_1}} \tag{2.10}$$

defines an $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{Y}_{d_1,d}$ covered by the curve $\mathcal{X}_n$ of genus $g = \frac{d_1(d-1)(q+1)}{2}$. This curve is the quotient curve $\mathcal{X}_n/H_{d_1,d}$, where

$$H_{d_1,d} = \left\{ \sigma_{a(b^q+1),ab,\xi} : (b^q + b + 1)a^2 = 1,\ a^{\frac{q-1}{d_1}} = 1,\ \xi^{\frac{m}{d}} = 1 \right\}$$

and

$$\sigma_{a(b^q+1),ab,\xi} : (X,Y,Z) \mapsto (a(b^q+1)X + ab^qY, abX + a(b+1)Y, \xi Z).$$

Proof. Note that $H_{d_1,d} \neq \emptyset$ is a finite subset of $\mathrm{Aut}(\mathcal{X}_n)$ and for $\sigma_{a_1(b_1^q+1),a_1b_1,\xi_1}, \sigma_{a_2(b_2^q+1),a_2b_2,\xi_2}$ elements in $H_{d_1,d}$,

$$\begin{aligned} \sigma_{a_2(b_2^q+1),a_2b_2,\xi_2}\sigma_{a_1(b_1^q+1),a_1b_1,\xi_1} &= \begin{pmatrix} a_2(b_2^q+1) & a_2b_2^q & 0 \\ a_2b_2 & a_2(b_2+1) & 0 \\ 0 & 0 & \xi_2 \end{pmatrix} \begin{pmatrix} a_1(b_1^q+1) & a_1b_1^q & 0 \\ a_1b_1 & a_1(b_1+1) & 0 \\ 0 & 0 & \xi_1 \end{pmatrix} \\ &= \begin{pmatrix} A(B^q+1) & AB^q & 0 \\ AB & A(B+1) & 0 \\ 0 & 0 & \xi_1\xi_2 \end{pmatrix} \\ &= \sigma_{A(B^q+1),AB,\xi_1\xi_2}, \end{aligned}$$

where $A = a_1a_2$ and $B = b_2a_1^{-2} + b_1$. Since $A^{\frac{q-1}{d_1}} = (\xi_1\xi_2)^{\frac{m}{d}} = 1$ and

$$\begin{aligned} (B^q + B + 1)A^2 &= ((b_2^q + b_2)a_1^{-2} + b_1^q + b_1 + 1)a_1^2a_2^2 \\ &= (b_2^q + b_2)a_2^2 + a_2^2 \\ &= (b_2^q + b_2 + 1)a_2^2 \\ &= 1, \end{aligned}$$

we conclude that $H_{d_1,d}$ is a subgroup of $\mathrm{Aut}(\mathcal{X}_n)$ of order $\frac{q(q-1)m}{d_1 d}$.

Now, consider the functions $u := (x+y)^{(q-1)/d_1}$ and $w := z^{m/d}$ in $\mathbb{F}_{q^{2n}}(\mathcal{X}_n)$. For $\sigma_{a(b^q+1),ab,\xi} \in H_{d_1,d}$, we have that

$$\sigma_{a(b^q+1),ab,\xi}(U) = (a(b^q+b+1)(X+Y))^{\frac{q-1}{d_1}} = (a^{-1}(X+Y))^{\frac{q-1}{d_1}} = U \text{ and}$$
$$\sigma_{a(b^q+1),ab,\xi}(W) = \sigma_{a(b^q+1),ab,\xi}(Z^{\frac{m}{d}}) = (\xi Z)^{\frac{m}{d}} = \xi^{\frac{m}{d}} Z^{\frac{m}{d}} = W.$$

Thus, $\mathbb{F}_{q^{2n}}(u,w) \subseteq \mathrm{Fix}(H_{d_1,d})$. Furthermore, from Equation (2.5) we deduce that the functions x and y satisfy the following relation

$$\begin{aligned}(x^{q+1}-1)((x+y)-(x+y)^{q^2}) &= (x^{q+1}-1)(x-x^{q^2}) + (x^{q+1}-1)(y-y^{q^2})\\ &= y^{q+1}x(1-x^{q^2-1}) + y(x^{q+1}-1)(1-(x^{q+1}-1)^{q-1})\\ &= y^{q+1}x(1-x^{q^2-1}) + yx^{q+1}(1-x^{q^2-1})\\ &= xy(x+y)^q(1-x^{q^2-1})\\ &= xy(x+y)^q((x^{q+1}-1)x^{q^2-1} - (x^{q^2+q}-1)),\end{aligned}$$

that is,

$$(x+y)-(x+y)^{q^2} = xy(x+y)^q \left(x^{q^2-1} - \frac{x^{q^2+q}-1}{x^{q+1}-1}\right). \tag{2.11}$$

Hence, we conclude

$$\begin{aligned} w^d = z^m = x^{q^2}y - xy^{q^2} = xy\left(x^{q^2-1} - \frac{x^{q^2+q}-1}{x^{q+1}-1}\right) &\qquad \text{from Equation (2.6)}\\ = \frac{(x+y)-(x+y)^{q^2}}{(x+y)^q} &\qquad \text{from Equation (2.11)}\\ = \frac{1-(x+y)^{q^2-1}}{(x+y)^{q-1}} &\\ = \frac{1-u^{d_1(q+1)}}{u^{d_1}}. &\end{aligned}$$

From this algebraic relation, we conclude that the extension $\mathbb{F}_{q^{2n}}(u,w)/\mathbb{F}_{q^{2n}}(u)$ is a Kummer extension of degree d. By Theorem 2.1.1 we have $[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(x,y)] = m$ and by [7, Lemma 3.1], $[\mathbb{F}_{q^{2n}}(x,y) : \mathbb{F}_{q^{2n}}(x+y)] = q$. Therefore $[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(x+y)] = qm$ and we get that

$$[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(u,w)] = \frac{[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(x+y)][\mathbb{F}_{q^{2n}}(x+y) : \mathbb{F}_{q^{2n}}(u)]}{[\mathbb{F}_{q^{2n}}(u,w) : \mathbb{F}_{q^{2n}}(u)]} \leq \frac{q(q-1)m}{d_1 d}.$$

This implies $\mathrm{Fix}(H_{d_1,d}) = \mathbb{F}_{q^{2n}}(u,w)$. In order to calculate the genus of $K(u,w)$ we compute the principal divisor

$$\left(\frac{1-u^{d_1(q+1)}}{u^{d_1}}\right)_{K(u)} = \sum_{i=1}^{d_1(q+1)} P_{\alpha_i} - d_1 P_0 - d_1 q P_\infty,$$

where $\alpha_1, \ldots, \alpha_{d_1(q+1)}$ are the roots of the separable polynomial $U^{d_1(q+1)} - 1$. Thus all the places over P_{α_i}, P_0 or P_∞ are totally ramified in the extension $K(u,w)/K(u)$.

The genus g of $K(u,w)$ follows from the Riemann-Hurwitz formula, $g = d_1(d-1)(q+1)/2$. □

In particular, for $d_1 = q-1$ and $d = m$ in Theorem 2.1.4, we obtain the quotient curve $W^m = \frac{1-U^{q^2-1}}{U^{q-1}}$ corresponding to the subgroup $H_{q-1,m} = \{\sigma_{b^q+1,b,1} : b^q + b = 0\}$. This curve already appeared in [7, Corollary 3.7] where it played an important role in the proof of the maximality of the BM curve.

2.2 Quotient curves from a second new model for the BM curve

In this section, we apply a morphism to the curve $\mathcal{X}_n$ in order to obtain new subgroups of $\mathrm{Aut}(\mathcal{X}_n)$. Consider $\mathbb{F}_{q^{2n}}(\mathcal{X}_n) = \mathbb{F}_{q^{2n}}(x,y,z)$, the function field of the curve $\mathcal{X}_n$, and let $\rho \in \mathbb{F}_{q^{2n}}$ be such that $\rho^{q^n+1} = 1$ and $\rho^m \neq 1$. Applying the morphism

$$\phi(X,Y,Z) = \left(\frac{\rho^m}{\rho^m - 1}(X-Y), X - \rho^m Y, \rho Z\right) \tag{2.12}$$

to the curve

$$\mathcal{X}_n : \begin{cases} Z^m = X^{q^2}Y - XY^{q^2} \\ Y^{q+1} = X^{q+1} - 1 \end{cases}$$

we have that the functions $u := \frac{\rho^m}{\rho^m-1}(x-y)$, $v := x - \rho^m y$, and $w := \rho z$ in $\mathbb{F}_{q^{2n}}(\mathcal{X}_n)$ satisfy

$$\begin{aligned} u^q v + u v^q &= \frac{\rho^{mq}}{\rho^{mq}-1}(x^q - y^q)(x - \rho^m y) + \frac{\rho^m}{\rho^m - 1}(x-y)(x^q - \rho^{mq}y^q) \\ &= \frac{\rho^{mq}}{\rho^{mq}-1}(x^{q+1} - \rho^m x^q y - xy^q + \rho^m y^{q+1}) + \\ &\quad \frac{\rho^m}{\rho^m-1}(x^{q+1} - \rho^{mq}xy^q - x^q y + \rho^{mq}y^{q+1}) \\ &= \left(\frac{\rho^{mq}}{\rho^{mq}-1} + \frac{\rho^m}{\rho^m-1}\right)x^{q+1} + \left(\frac{1}{\rho^{mq}-1} + \frac{1}{\rho^m-1}\right)y^{q+1} \\ &\quad - \left(\frac{\rho^{mq}}{\rho^{mq}-1} + \frac{1}{\rho^m-1}\right)xy^q - \left(\frac{1}{\rho^{mq}-1} + \frac{\rho^m}{\rho^m-1}\right)x^q y \\ &= x^{q+1} - y^{q+1} \end{aligned}$$

and

$$\begin{aligned}
v^{q^2}u - u^{q^2}v &= \frac{\rho^m}{\rho^m - 1}(x^{q^2} - \rho^m y^{q^2})(x - y) - \frac{\rho^m}{\rho^m - 1}(x^{q^2} - y^{q^2})(x - \rho^m y) \\
&= \frac{\rho^m}{\rho^m - 1}(x^{q^2+1} - x^{q^2}y - \rho^m x y^{q^2} + \rho^m y^{q^2+1} - x^{q^2+1} + \rho^m x^{q^2} y \\
&\quad + x y^{q^2} - \rho^m y^{q^2+1}) \\
&= \rho^m(x^{q^2}y - xy^{q^2}) \\
&= \rho^m z^m \\
&= w^m.
\end{aligned}$$

Thus, we obtain an isomorphic curve with equations

$$\mathcal{F}_n : \begin{cases} Z^m = Y^{q^2}X - X^{q^2}Y \\ X^qY + XY^q = 1 \end{cases} . \tag{2.13}$$

Recall that

$$\mathrm{Aut}(\mathcal{X}_n) = \left\{\sigma_{a,c,\xi} : a^{q+1} - c^{q+1} = 1,\ \xi^{q^n+1} = 1\right\},$$

where

$$\sigma_{a,c,\xi} : (X, Y, Z) \mapsto (aX + c^q\xi^m Y, cX + a^q\xi^m Y, \xi Z).$$

By conjugation, we retrieve a representation for the automorphism group of the curve $\mathcal{F}_n$

$$\mathrm{Aut}(\mathcal{F}_n) = \phi\mathrm{Aut}(\mathcal{X}_r)\phi^{-1} = \left\{\tilde{\tau}_{a,c,\xi} : a^{q+1} - c^{q+1} = 1,\ \xi^{q^n+1} = 1\right\},$$

where

$$\tilde{\tau}_{a,c,\xi} : \begin{cases} X \mapsto \frac{\rho^m}{\rho^m-1}\left((a-c) - (a-c)^q\xi^m\rho^{mq}\right)X - \frac{\rho^m}{(\rho^m-1)^2}((a-c) - (a-c)^q\xi^m)Y, \\ Y \mapsto ((a - c\rho^m) - (a - c\rho^m)^q\xi^m)X - \frac{1}{\rho^m-1}((a - c\rho^m) - (a - c\rho^m)^q\xi^m\rho^m)Y, \\ Z \mapsto \xi Z. \end{cases}$$

From the equality

$$(X - Y)^q(X - Y\rho^m) - \rho^m(X - Y\rho^m)^q(X - Y) = (1 - \rho^m)(X^{q+1} - Y^{q+1})$$

we can represent

$$\mathrm{Aut}(\mathcal{F}_n) = \left\{\tau_{a,c,\xi} : a^qc - \rho^m ac^q = 1 - \rho^m,\ \xi^{q^n+1} = 1\right\},$$

where

$$\tau_{a,c,\xi} : \begin{cases} X \mapsto \frac{\rho^m}{\rho^m-1}\left(a - a^q\xi^m\rho^{mq}\right)X - \frac{\rho^m}{(\rho^m-1)^2}(a - a^q\xi^m)Y, \\ Y \mapsto (c - c^q\xi^m)X - \frac{1}{\rho^m-1}(c - c^q\xi^m\rho^m)Y, \\ Z \mapsto \xi Z. \end{cases}$$

The equations defining the curve $\mathcal{F}_n$ allow to obtain, by simple inspection, automorphisms that had not been previously considered, yielding new quotient curves. In the following theorem, we provide a quotient curve of the curve $\mathcal{F}_n$ corresponding to the subgroup generated by a single automorphism.

Theorem 2.2.1. *Let d_1 and d_2 be divisors of $q-1$ and m respectively. The following equations define an $\mathbb{F}_{q^{2n}}$-maximal curve which is a subcover of the curve $\mathcal{F}_n$:*

$$\mathcal{Y}_{d_1,d_2} : \begin{cases} W^{d_2} = \frac{1-VU^{d_1}-(VU^{d_1})^q}{V^q} \\ V^q = U^{d_1} - VU^{2d_1} \end{cases} . \tag{2.14}$$

The curve $\mathcal{Y}_{d_1,d_2}$ has genus

$$g = \frac{d_1(q+1)(d_2(q+1)-q) - (d_1(q+1,2), q-1)}{2}$$

and corresponds to the quotient curve $\mathcal{F}_n/L$, where L is the subgroup of $\mathrm{Aut}(\mathcal{F}_n)$ *generated by the automorphism*

$$\tau_{\theta^{d_1},\theta^{-d_1},\epsilon} : (X,Y,Z) \mapsto \left(\theta^{-d_1}X, \theta^{d_1}Y, \epsilon Z\right),$$

where θ is a primitive element of $\mathbb{F}_q$ and ϵ is a primitive (m/d_2)-th root of unity.

Proof. First of all, note that the functions $u := x^{(q-1)/d_1}$, $v := xy$ and $w = z^{m/d_2}$ are in the fixed field $\mathrm{Fix}(L)$. In fact, we have that

$$\begin{aligned}
\tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(U) &= \tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(X^{\frac{q-1}{d_1}}) = (\theta^{-d_1}X)^{\frac{q-1}{d_1}} = X^{\frac{q-1}{d_1}} = U, \\
\tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(V) &= \tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(XY) = (\theta^{-d_1}X)(\theta^{d_1}Y) = XY = V, \text{ and} \\
\tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(W) &= \tau_{\theta^{d_1},\theta^{-d_1},\epsilon}(Z^{\frac{m}{d_2}}) = (\epsilon Z)^{\frac{m}{d_2}} = Z^{\frac{m}{d_2}} = W.
\end{aligned}$$

Furthermore, since $\tau^i_{\theta^{d_1},\theta^{-d_1},\epsilon}(X,Y,Z) = (\theta^{-id_1}X, \theta^{id_1}Y, \epsilon^i Z)$ for $i \in \mathbb{N}$, θ is a primitive element of $\mathbb{F}_q$, and ϵ is a primitive (m/d_2)-th root of unity, we have that L is a subgroup of $\mathrm{Aut}(\mathcal{F}_n)$ of order $\frac{(q-1)m}{d_1d_2}$. Moreover, since

$$[\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(u,v,w)] = [\mathbb{F}_{q^{2n}}(x,xy,z) : \mathbb{F}_{q^{2n}}(u,v,w)] \leq \frac{(q-1)m}{d_1d_2} = \#L,$$

we conclude that $\mathrm{Fix}(L) = \mathbb{F}_{q^{2n}}(u,v,w)$.

In order to provide irreducible equations for $\mathcal{Y}_{d_1,d_2} \cong \mathcal{F}_n/L$, we use Equation (2.13) to conclude that the functions u, v and w satisfy the relations

$$v^q = (xy)^q = x^{q-1}(xy^q) = x^{q-1}(1-yx^q) = x^{q-1} - (xy)x^{2(q-1)} = u^{d_1} - vu^{2d_1}$$

and

$$\begin{aligned}
w^{d_2} = z^m = xy((y^{q-1})^{q+1} - (x^{q-1})^{q+1}) &= xy\left(\left(\frac{1}{xy} - x^{q-1}\right)^{q+1} - (x^{q-1})^{q+1}\right) \\
&= \frac{1-(xy)x^{q-1} - ((xy)x^{q-1})^q}{(xy)^q} \\
&= \frac{1-vu^{d_1} - (vu^{d_1})^q}{v^q}.
\end{aligned}$$

This implies that the equations given in (2.14) define a quotient curve of $\mathcal{F}_n$. For convenience, in order to calculate the genus of the algebraic function field $K(u,v,w)$, we write $t = vu^{d_1}$. Consider the following extensions of function fields:

$$K(t) \subseteq K(t,v) \subseteq K(t,v,w) \subseteq K(t,v,w,u) = K(u,v,w).$$

From (2.14), the functions t, v and w satisfy the relations

$$w^{d_2} = (1-t-t^q)/v^q \quad \text{and} \quad v^{q+1} = t(1-t).$$

We conclude that the function field extension $K(t,v)/K(t)$ is a Kummer extension of degree $q+1$ of genus

$$g(K(t,v)) = (q+1-(q+1,2))/2.$$

Moreover, if P_0 and P_1 are the zeros of t and $t-1$ respectively, and P_∞ the pole of t in $K(t)$, then P_0 and P_1 are totally ramified, P_∞ has $(q+1,2)$ extensions and the other places are completely split in $K(t,v)/K(t)$.

On the other hand, for $\alpha_1, \alpha_2, \ldots, \alpha_q$ the roots of the separable polynomial $f(T) = 1-T-T^q$ in K, let P_{α_j} be the place in $K(t)$ associated to the function $t-\alpha_j$. After some computations, we get the principal divisors

$$(t-\alpha_j)_{K(t,v)} = \sum_{i=1}^{q+1} Q_{\alpha_j,i} - \frac{q+1}{(q+1,2)} \sum_{i=1}^{(q+1,2)} Q_{\infty,i}$$

and

$$(v)_{K(t,v)} = Q_0 + Q_1 - \frac{2}{(q+1,2)} \sum_{i=1}^{(q+1,2)} Q_{\infty,i},$$

where $Q_{\alpha_j,i}$, Q_i and $Q_{\infty,i}$ are extensions of P_{α_j}, P_i and P_∞ in $K(t,v)$ respectively. Hence, we obtain the following divisor in $K(t,v)$:

$$\left(\frac{f(t)}{v^q}\right)_{K(t,v)} = \sum_{j=1}^{q}\sum_{i=1}^{q+1} Q_{\alpha_j,i} - q(Q_0+Q_1) - \frac{q(q-1)}{(q+1,2)} \sum_{i=1}^{(q+1,2)} Q_{\infty,i}.$$

Therefore the extension $K(t,v,w)/K(t,v)$ is also a Kummer extension of degree d_2, and all the ramified places in the extension are totally ramified.

By the Riemann-Hurwitz formula, we obtain

$$g(K(t,v,w)) = \frac{d_2(q+1)^2 - (q^2+q+(q+1,2))}{2}.$$

To conclude the proof, we prove that $K(t,v,w,u)/K(t,v,w)$ is a Kummer extension and compute the genus of $K(t,v,w,u) = K(u,v,w)$. We have $u^{d_1} = t/v$ and start by computing the divisors of the functions t and v:

$$(t)_{K(t,v,w)} = d_2(q+1)R_0 - \frac{d_2(q+1)}{(q+1,2)} \sum_{i=1}^{(q+1,2)} R_{\infty,i},$$

$$(v)_{K(t,v,w)} = d_2 \left(R_0 + R_1 - \frac{2}{(q+1,2)} \sum_{i=1}^{(q+1,2)} R_{\infty,i} \right).$$

Therefore

$$(t/v)_{K(t,v,w)} = d_2 q R_0 - d_2 R_1 - \frac{d_2(q-1)}{(q+1,2)} \sum_{i=1}^{(q+1,2)} R_{\infty,i},$$

where R_i and $R_{\infty,i}$ are the unique extensions in $K(t,v,w)$ of the places Q_i and $Q_{\infty,i}$ respectively. Since $(d_1, d_2) = 1$, we conclude that $K(t,v,w,u)/K(t,v,w)$ is a Kummer extension of degree d_1. For S a place in $\mathcal{P}_{K(t,v,w,u)}$ we have the following ramification indices

$$e(S) = \begin{cases} d_1, & \text{if } S \text{ is over } R_i, \\ d_1(q+1,2)/(d_1(q+1,2), q-1), & \text{if } S \text{ is over } R_{\infty,i}, \\ 1, & \text{in the other cases.} \end{cases}$$

By the Riemman-Hurwitz formula, we can finally obtain the genus

$$g(K(u,v,w)) = g(K(t,v,w,u)) = \frac{d_1(q+1)(d_2(q+1)-q) - (d_1(q+1,2), q-1)}{2}.$$

□

Choosing $d_2 = 1$ in Theorem 2.2.1 we obtain a family of quotient curves $V^q = U^{d_1} - VU^{2d_1}$ of the Hermitian curve over $\mathbb{F}_{q^2}$ defined by $X^qY + XY^q = 1$. This quotient curve has genus

$$g = \frac{d_1(q+1) - (d_1(q+1,2), q-1)}{2} = \begin{cases} \frac{d_1(q+1)-(2d_1,q-1)}{2}, & \text{if } q \text{ is odd}, \\ d_1 \frac{q}{2}, & \text{if } q \text{ is even}, \end{cases}$$

and corresponds to the subgroup generated by the automorphism $\tau : (X,Y) \mapsto \left(\theta^{-d_1}X, \theta^{d_1}Y\right)$.

Now we consider a second automorphism of the curve $\mathcal{F}_n$ given by

$$\tau_d : (X,Y,Z) \mapsto (Y,X,-\epsilon Z),$$

where d is a divisor of m and ϵ is a primitive (m/d)-th root of unity. We provide the quotient curve corresponding to the subgroup L_d of $\mathrm{Aut}(\mathcal{F}_n)$ generated by τ_d. For this, it is necessary to distinguish between the two cases of odd and even characteristic. We start with the case of odd characteristic.

Consider the functions $u := x + y$ and $w := z^{2m/d}$. We start by determining an algebraic relation between these functions. From Equation (2.13) we have

$$(x-y)^{q+1} = (x+y)^{q+1} - 2 \tag{2.15}$$

and, after some calculations,

$$y^{q^2}x - x^{q^2}y = -(x-y)\left(\frac{(x+y)^{q^2} - (x+y)}{(x+y)^{q+1} - 2}\right). \tag{2.16}$$

Thus,

$$\begin{aligned} w^{d(q+1)/2} = z^{q^n+1} &= (y^{q^2}x - x^{q^2}y)^{q+1} \\ &= (x-y)^{q+1}\left(\frac{(x+y)^{q^2}-(x+y)}{(x+y)^{q+1}-2}\right)^{q+1} && \text{from Equation (2.16)} \\ &= ((x+y)^{q+1}-2)\left(\frac{(x+y)^{q^2}-(x+y)}{(x+y)^{q+1}-2}\right)^{q+1} && \text{from Equation (2.15)} \\ &= \frac{(x+y)^{q+1}((x+y)^{q^2-1}-1)^{q+1}}{((x+y)^{q+1}-2)^q} \\ &= \frac{u^{q+1}(u^{q^2-1}-1)^{q+1}}{(u^{q+1}-2)^q}. \end{aligned}$$

Therefore the functions u and w satisfy the irreducible equation

$$W^{d(q+1)/2} = \frac{U^{q+1}(U^{q^2-1}-1)^{q+1}}{(U^{q+1}-2)^q}. \tag{2.17}$$

Furthermore, it is clear that $\mathbb{F}_{q^{2n}}(u,w) \subseteq \text{Fix}(L_d) \subseteq \mathbb{F}_{q^{2n}}(x,y,z)$. From Equation (2.16), $x-y \in \mathbb{F}_{q^{2n}}(x+y,z)$ and therefore

$$\begin{aligned} [\mathbb{F}_{q^{2n}}(x,y,z) : \mathbb{F}_{q^{2n}}(u,w)] &= [\mathbb{F}_{q^{2n}}(x+y, x-y, z) : \mathbb{F}_{q^{2n}}(u,w)] \\ &= [\mathbb{F}_{q^{2n}}(x+y, z) : \mathbb{F}_{q^{2n}}(u,w)] \leq \frac{2m}{d}. \end{aligned}$$

Since $\#L_d = 2m/d$, we conclude that $\mathbb{F}_{q^{2n}}(u,w) = \text{Fix}(L_d)$ and therefore the curve defined by the Equation (2.17) corresponds to the quotient curve $\mathcal{F}_n/L_d$. This curve is isomorphic to the curve $\mathcal{Y}_{q+1,1,d(q+1)/2}$ given in Theorem 2.1.1. In fact, $\nu(U,W) = (\alpha^{-1}U, W)$, where $\alpha \in \mathbb{F}_{q^{2n}}$ such that $\alpha^{q+1} = 2$, is a morphism between the curves defined by Equation (2.17) and $\mathcal{Y}_{q+1,1,d(q+1)/2}$.

For the case q even, we first need the following result.

Lemma 2.2.2. *Suppose $q = 2^s$. Then we have the following polynomial identity in $K[X,Y]$:*

$$\sum_{m=0}^{s-1} (XY)^{2^m}(X+Y)^{2^s-2^{m+1}+1} = X^{2^s}Y + XY^{2^s}.$$

Proof. We prove this identity by induction. For $s = 1$, the identity is trivial. Assume the validity of the identity for $s \geq 1$. Then,

$$\begin{aligned}
&(X+Y)\left(\sum_{m=0}^{s}(XY)^{2^m}(X+Y)^{2^{s+1}-2^{m+1}+1}\right)\\
&=\sum_{m=0}^{s}(XY)^{2^m}(X+Y)^{2^{s+1}-2^{m+1}+2}\\
&=XY(X+Y)^{2^{s+1}}+\sum_{m=1}^{s}(XY)^{2^m}(X+Y)^{2^{s+1}-2^{m+1}+2}\\
&=XY(X+Y)^{2^{s+1}}+\sum_{m=0}^{s-1}(XY)^{2^{m+1}}(X+Y)^{2^{s+1}-2^{m+2}+2}\\
&=XY(X+Y)^{2^{s+1}}+\left(\sum_{m=0}^{s-1}(XY)^{2^m}(X+Y)^{2^s-2^{m+1}+1}\right)^2\\
&=XY(X+Y)^{2^{s+1}}+(X^{2^s}Y+XY^{2^s})^2\\
&=YX^{2^{s+1}+1}+XY^{2^{s+1}+1}+X^{2^{s+1}}Y^2+X^2Y^{2^{s+1}}\\
&=(X+Y)(X^{2^{s+1}}Y+XY^{2^{s+1}}).
\end{aligned}$$

□

Theorem 2.2.3. *Suppose $q = 2^s$ and let d be a divisor of m. The equations*

$$\begin{cases} W^d = \frac{U^{q^2-1}+1}{U^{q-1}} \\ \sum_{m=0}^{s-1} V^{2^m}U^{2^s-2^{m+1}+1} = 1 \end{cases} \tag{2.18}$$

define an $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{Y}_d$ covered by the curve $\mathcal{F}_n$. Moreover, the curve $\mathcal{Y}_d$ corresponds to the quotient curve $\mathcal{F}_n/L_d$ and has genus $g = \frac{d(q+1)(q^2-2)-(q^3-2)}{4}$.

Proof. We start defining the functions $u := x + y$, $v := xy$ and $w := z^{m/d}$. By Lemma 2.2.2, the functions u and v satisfy the algebraic relation

$$\sum_{m=0}^{s-1} v^{2^m}u^{2^s-2^{m+1}+1} = 1.$$

Moreover, from the defining equations of the curve $\mathcal{F}_n$ in (2.13) it follows that

$$y^q(x+y)+y(x+y)^q = y^qx+yx^q = 1.$$

So,

$$\left(\frac{y}{x+y}\right)^q+\left(\frac{y}{x+y}\right)=\left(\frac{1}{x+y}\right)^{q+1}, \tag{2.19}$$

$$\left(\frac{y}{x+y}\right)^{q^2}+\left(\frac{y}{x+y}\right)^q=\left(\frac{1}{x+y}\right)^{q^2+q}$$

and therefore, after some computations, we conclude

$$\left(\frac{y}{x+y}\right)^{q^2}+\left(\frac{y}{x+y}\right)=\left(\frac{1}{x+y}\right)^{q+1}+\left(\frac{1}{x+y}\right)^{q^2+q}.$$

Since

$$z^m = y^{q^2}x + yx^{q^2} = (x+y)^{q^2}y + (x+y)y^{q^2}$$

we get that

$$\frac{z^m}{(x+y)^{q^2+1}} = \left(\frac{y}{x+y}\right) + \left(\frac{y}{x+y}\right)^{q^2} = \left(\frac{1}{x+y}\right)^{q+1} + \left(\frac{1}{x+y}\right)^{q^2+q}$$

and therefore

$$w^d = z^m = \frac{(x+y)^{q^2} + (x+y)}{(x+y)^q} = \frac{u^{q^2-1}+1}{u^{q-1}}.$$

Thus, the functions u, v and w satisfy the equations given in (2.18). On the other hand, to calculate the genus of the function field $K(u,v,w)$ note that, from the second equation of (2.18), we have

$$\left(\frac{v}{u^2}\right)^{2^{s-1}} + \left(\frac{v}{u^2}\right)^{2^{s-2}} + \cdots + \left(\frac{v}{u^2}\right)^2 + \frac{v}{u^2} = \frac{1}{u^{q+1}}. \tag{2.20}$$

By [56, Proposition 3.7.10], the extension $\mathbb{F}_{q^{2n}}(u^{-1}, vu^{-2})/\mathbb{F}_{q^{2n}}(u^{-1})$ is an Artin-Schreier extension of degree $q/2$ and has genus $g(K(u^{-1}, vu^{-2})) = \frac{q(q-2)}{4}$. If $P_\infty \in \mathcal{P}_{K(u^{-1})}$ is the pole of u^{-1}, then P_∞ is the unique place totally ramified and the other places are completely split in such extension. Also, since

$$\frac{u^{q^2-1}+1}{u^{q-1}} = \frac{(u^{-1})^{q^2-1}+1}{(u^{-1})^{q^2-q}},$$

we have

$$\left(\frac{u^{q^2-1}+1}{u^{q-1}}\right)_{K(u^{-1})} = -q(q-1)P_0 + \sum_{\alpha\in\mathbb{F}_{q^2}\setminus\{0\}} P_\alpha - (q-1)P_\infty$$

and therefore

$$\left(\frac{u^{q^2-1}+1}{u^{q-1}}\right)_{K(u^{-1},vu^{-2})} = -q(q-1)\sum_{i=1}^{q/2} Q_{0,i} + \sum_{i=1}^{q/2}\sum_{\alpha\in\mathbb{F}_{q^2}\setminus\{0\}} Q_{\alpha,i} - \frac{q(q-1)}{2}Q_\infty,$$

where $Q_{0,i}$, $Q_{\alpha,i}$ and Q_∞ are the extensions in $\mathcal{P}_{K(u^{-1},vu^{-2})}$ of the places P_0, P_α and P_∞ respectively. This implies that the extension $K(u^{-1}, vu^{-2}, w)/K(u^{-1}, vu^{-2})$ is a Kummer extension of degree d. For R a place in $\mathcal{P}_{K(u^{-1},vu^{-2},w)}$, the ramification indices are given by

$$e(R) = \begin{cases} d, & \text{if } R \text{ is over } Q_{0,i}, Q_{\alpha,i} \text{ or } Q_\infty, \\ 1, & \text{in the other cases,} \end{cases}$$

and therefore the genus of $K(u^{-1}, vu^{-2}, w)$ satisfies

$$2g(K(u^{-1}, vu^{-2}, w)) - 2 = d\left(\frac{q(q-2)}{2} - 2\right) + (d-1)\left(\frac{q}{2} + \frac{q}{2}(q^2-1) + 1\right).$$

This yields

$$g(K(u,v,w)) = g(K(u^{-1}, vu^{-2}, w)) = \frac{d(q+1)(q^2-2) - (q^3-2)}{4}.$$

To show that the curve (2.18) is a quotient curve of $\mathcal{F}_n$, note that by (2.19) we have $[\mathbb{F}_{q^{2n}}(x,y):\mathbb{F}_{q^{2n}}(u)]=q$ and therefore

$$[\mathbb{F}_{q^{2n}}(x,y,z):\mathbb{F}_{q^{2n}}(u)]=[\mathbb{F}_{q^{2n}}(x,y,z):\mathbb{F}_{q^{2n}}(x,y)][\mathbb{F}_{q^{2n}}(x,y):\mathbb{F}_{q^{2n}}(u)]=qm.$$

Thus,

$$[\mathbb{F}_{q^{2n}}(x,y,z):\mathbb{F}_{q^{2n}}(u,v,w)]=\frac{[\mathbb{F}_{q^{2n}}(x,y,z):\mathbb{F}_{q^{2n}}(u)]}{[\mathbb{F}_{q^{2n}}(u,v,w):\mathbb{F}_{q^{2n}}(u,v)][\mathbb{F}_{q^{2n}}(u,v):\mathbb{F}_{q^{2n}}(u)]}=\frac{2m}{d}.$$

Since u, v and w are elements of the fixed field $\mathrm{Fix}(L_d)$ and the subgroup L_d has order $\frac{2m}{d}$, we conclude that $\mathrm{Fix}(L_d)=\mathbb{F}_{q^{2n}}(u,v,w)$. □

For q even, the curve $\mathcal{Y}_{q-1,d}$ presented in Theorem 2.1.4 is covered by the curve $\mathcal{Y}_d$ presented in Theorem 2.2.3, and $\mathcal{Y}_{q-1,d}\cong\mathcal{Y}_d$ if and only if $q=2$.

The curves in Theorem 2.2.1 for q even, and the ones in Theorem 2.2.3 are not isomorphic for $q\neq 4$. In fact, if the genera obtained in Theorems 2.2.1 and 2.2.3 were equal, we could conclude that

$$-(q^3-2)\equiv -2d_1 \pmod{q+1},$$

that is $-2d_1\equiv 3 \pmod{q+1}$, which implies $q=4$ and $d_1=1$.

We also notice that, in the particular case of $d=1$ in Theorem 2.2.3 and $q=2^s$, we obtain a curve defined by

$$\sum_{i=1}^{s} Y^{q/2^i}=X^{q+1}$$

of genus $g=q(q-2)/4$. This curve first appeared in a paper of Abdón and Torres [3], where it was proved that any maximal curve in characteristic 2 such that $q/2$ is a Weierstrass non-gap at a certain point of the curve and has genus $q(q-2)/4$ is isomorphic to it.

The genus of the explicit quotient curve $\mathcal{Y}_d$ given in Theorem 2.2.3 appears in the classification given by Beelen and Montanucci [8]. In fact, following the same notations introduced in [8], let $\pi:\mathrm{Aut}(\mathcal{X}_n)\to\mathrm{Aut}(\mathcal{H})$ be the group homomorphism given by natural restriction to the Hermitian curve $\mathcal{H}$ and $C_m:=\mathrm{Ker}(\pi)=\{\sigma_{1,0,\xi}\in\mathrm{Aut}(\mathcal{X}_n):\xi^m=1\}$. In even characteristic, for L_d the subgroup of $\mathrm{Aut}(\mathcal{F}_n)$ considered in Theorem 2.2.3 and $\phi:\mathcal{X}_n\to\mathcal{F}_n$ the morphism defined in (2.12), we consider the subgroup $\mathcal{C}_2$ of $\mathrm{Aut}(\mathcal{H})$ and note that $\pi\circ\phi^{-1}(L_d)\cong\mathcal{C}_2$. By [8, Lemma 4.1],

$$N=\frac{q^3+2}{2}\quad\text{and}\quad g_{\pi\circ\phi^{-1}(L_d)}=\frac{q(q-2)}{4},$$

where N is the number of orbits in the set $\mathcal{X}_n(\mathbb{F}_{q^2})$ under the action of $\phi^{-1}(L_d)$, and $g_{\pi\circ\phi^{-1}(L_d)}$ is the genus of the fixed field $\mathrm{Fix}(\pi\circ\phi^{-1}(L_d))\subseteq K(\mathcal{H})$. Also, since $\phi^{-1}(L_d)\cap C_m\cong\mathcal{C}_{\frac{m}{d}}$, by [8, Theorem 2.1], we conclude

$$g(\mathcal{Y}_d)=\frac{m}{\#\mathcal{C}_{\frac{m}{d}}}(g_{\pi\circ\phi^{-1}(L_d)}-1)+\frac{N}{2}\left(\frac{m}{\#\mathcal{C}_{\frac{m}{d}}}-1\right)+1=\frac{d(q+1)(q^2-2)-(q^3-2)}{4}.$$

Now we present parameters for which some curves provided in this chapter are not covered by the Hermitian curve. For this note that, by Equation (1.2.7), it easily follows that the degree $\deg\phi$ of a subcover $\mathcal{Y}$ of a maximal curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ given by an $\mathbb{F}_{q^2}$-rational map $\phi : \mathcal{X} \to \mathcal{Y}$ must satisfy the relation

$$\lceil \mathcal{L}_{\mathcal{X},\mathcal{Y}} \rceil \leq \deg\phi \leq \lfloor \mathcal{U}_{\mathcal{X},\mathcal{Y}} \rfloor, \tag{2.21}$$

where $\mathcal{L}_{\mathcal{X},\mathcal{Y}} = \frac{\#\mathcal{X}(\mathbb{F}_{q^2})}{\#\mathcal{Y}(\mathbb{F}_{q^2})}$ and $\mathcal{U}_{\mathcal{X},\mathcal{Y}} = \frac{2g(\mathcal{X})-2}{2g(\mathcal{Y})-2}$. With this argument, we have that the quotient curve $\mathcal{Y}_{d_1,d_2}$ defined in Theorem 2.2.1 does not satisfy the condition (2.21) for $n = 3$, $d_1 = q-1$ and $d_2 = \frac{q^2-q+1}{k}$, where $k \mid q^2-q+1$ and $1 \leq k \leq \sqrt{q}-1$. In this case, we obtain the following family of genus corresponding to curves not covered by the Hermitian curve

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

Comparing the obtained genus with the genus of maximal curves not covered by the Hermitian curve over $\mathbb{F}_{q^2}$ given in [24, 27] and [57], we obtain for $k = 3$ the following new genera over the indicated finite field:

- $\mathbb{F}_{2^{30}}$: 50.136.579,
- $\mathbb{F}_{17^6}$: 2.100.744,
- $\mathbb{F}_{23^6}$: 9.582.309, and
- $\mathbb{F}_{29^6}$: 30.621.654.

3 Curves with many points and reciprocal polynomials

For a curve $\mathcal{X}$ defined over $\mathbb{F}_q$ with genus $g(\mathcal{X}) \leq 50$, the webpage `www.manypoints.org` [60] collects the current intervals in which the number of $\mathbb{F}_q$-rational points $\#\mathcal{X}(\mathbb{F}_q)$ of the curve $\mathcal{X}$ is known to lie for some values of q. For a pair (q, g), the tables record an interval $[a, b]$ where b is the best upper bound for the maximum number of points of a curve over $\mathbb{F}_q$ with genus g, and a gives a lower bound obtained from an explicit example of a curve defined over $\mathbb{F}_q$ with a (or at least a) $\mathbb{F}_q$-rational points. At some places in manYPoints table in [60], the lower bound a of the interval $[a, b]$ is replaced by the symbol '$-$' where '$-$' represents the lower bound $L(q, g)$ given in Remark 3.0.1.

In this chapter, we improve upon the lower bounds of many of the intervals in [60] by constructing new examples of curves with many rational points. We provide a simple and effective construction of Kummer extensions and fibre products of Kummer extensions over finite fields with many rational points using reciprocal polynomials. We give a general lower bound for the number of rational points under certain hypothesis and we calculate the exact number of rational points for some particular constructions. As a consequence of these constructions, we obtain several improvements on the manYPoints table [60]. More precisely, we obtain 10 new records and 119 new entries. All the examples were obtained using the software Magma [10].

Given a polynomial f in $\mathbb{F}_q[X]$ and a subset $\mathcal{A} \subseteq \mathbb{F}_{q^2}$, we let $N_f(\mathcal{A}) := \#\{\alpha \in \mathcal{A} : f(\alpha) = 0\}$ stand for the number of roots of f in $\mathcal{A}$, and for polynomials $f_1, f_2 \in K[X]$ we denote by (f_1, f_2) the greatest common divisor of f_1 and f_2. Furthermore, we denote by ξ_q a primitive element of $\mathbb{F}_q$. Next, we set some notation about curves with many points in the following remark.

Remark 3.0.1. *We say that a curve $\mathcal{X}$ over $\mathbb{F}_q$ with genus g has many points if the number of $\mathbb{F}_q$-rational points of $\mathcal{X}$, denoted by $\#\mathcal{X}(\mathbb{F}_q)$, satisfies*

$$\#\mathcal{X}(\mathbb{F}_q) \geq L(q, g) := \left\lfloor \frac{U(q, g) - q - 1}{\sqrt{2}} \right\rfloor + q + 1, \tag{3.1}$$

where $U(q, g)$ denotes the upper bound given in manYPoints table [60] for the number of $\mathbb{F}_q$-rational points of a curve over $\mathbb{F}_q$ with genus g. In particular, for a pair (q, g) and a curve $\mathcal{X}$ over $\mathbb{F}_q$ with genus g, we say that $\mathcal{X}$ gives a **new record** *(resp.* **meets the record***) if the number $\#\mathcal{X}(\mathbb{F}_q)$ is strictly larger than (resp. is equal to) the lower bound registered in manYPoints table corresponding to (q, g). Further, we say that a curve $\mathcal{X}$ over*

$\mathbb{F}_q$ with genus g is a **new entry** *if there was no earlier lower bound entry in manYPoints table corresponding to (q, g) and $\#\mathcal{X}(\mathbb{F}_q)$ satisfies the relation (3.1).*

In Subsections 3.1.1 and 3.1.2, and in Section 3.2, we provide tables of curves with many rational points. In the tables where we provide a new record, the notation OLB (old lower bound) stands for the lower bound on the number $\#\mathcal{X}(\mathbb{F}_q)$ of rational points for a curve over $\mathbb{F}_q$ with genus g registered in the table [60]. Instead, when we provide a new entry, the notation OLB stands for the lower bound given in (3.1). Moreover, the symbol † indicates a maximal curve over $\mathbb{F}_{q^2}$.

3.1 A construction of curves over $\mathbb{F}_{q^2}$.

In this section, we propose a construction of algebraic curves over $\mathbb{F}_{q^2}$ using reciprocal polynomials. We will see that certain specific polynomials provide interesting algebraic curves with many points. This idea is explored in more detail in the subsequent sections.

Given a polynomial $f(X) = a_0 + a_1X + \cdots + a_dX^d \in \mathbb{F}_q[X]$ of degree d, denote by $f^*(X) = X^d f(1/X)$ the reciprocal polynomial of f. For $m \geq 2$ an integer not divisible by p and s a non-negative integer, consider the algebraic curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ defined by the affine equation

$$\mathcal{X}: \quad Y^m = X^{\epsilon s} f(X) f^*(X)^{\lambda} \text{ where } \epsilon, \lambda \in \{1, -1\}. \tag{3.2}$$

With some assumptions on f, we compute the genus of these curves in the following proposition.

Proposition 3.1.1. *Let $d > 0$ and let $f(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$ be a separable polynomial of degree d satisfying $f(0) \neq 0$. Let s be a non-negative integer, d_1 be the degree of (f, f^*) and $m \geq 2$ be such that $p \nmid m$. If $d_1 < d$, then the algebraic function field $K(x, y)$ defined by the affine equation*

$$Y^m = X^{\epsilon s} f(X) f^*(X)^{\lambda}, \quad \textit{where } \epsilon, \lambda \in \{1, -1\},$$

has genus

$$g = (m-1)d + 1 - \frac{(m, s) + (m, \epsilon s + d + \ d\lambda) + d_1(m, \lambda + 1) + d_1(m-2)}{2}.$$

Proof. At first, we write

$$X^{\epsilon s} f(X) f^*(X)^{\lambda} = X^{\epsilon s}(f(X)/h(X))(f^*(X)/h(X))^{\lambda} h(X)^{1+\lambda}$$

where $h = (f, f^*)$. The polynomials h, f/h and f^*/h are separable and $\alpha \in K$ is a root of f if and only if α^{-1} is a root of f^*. So, without loss of generality, we can suppose that

$$f/h = \beta_1 \prod_{i=1}^{d-d_1} (X - \alpha_i), \quad f^*/h = \beta_2 \prod_{j=1}^{d-d_1} (X - \gamma_j) \quad \text{and} \quad h = \beta \prod_{k=d-d_1+1}^{d} (X - \alpha_k),$$

where β_1, β_2, β are in K, $\alpha_1, \alpha_2, \ldots, \alpha_d$ are the roots of the polynomial f, $\gamma_j = \alpha_i^{-1}$ for some $1 \leq i \leq d$, and $\alpha_i, \gamma_j, \alpha_k$ are pairwise distinct for all $1 \leq i, j \leq d - d_1$ and $d - d_1 + 1 \leq k \leq d$. The principal divisor of the function $x^{\epsilon s} f(x) f^*(x)^\lambda$ in $K(x)$ is given by

$$\begin{aligned}(x^{\epsilon s} f(x) f^*(x)^\lambda)_{K(x)} &= \epsilon s(P_0 - P_\infty) + \sum_{i=1}^{d-d_1} P_{\alpha_i} - (d - d_1)P_\infty + \lambda \sum_{j=1}^{d-d_1} P_{\gamma_j} \\ &\quad - \lambda(d - d_1)P_\infty + (\lambda + 1) \sum_{k=d-d_1+1}^{d} P_{\alpha_k} - d_1(\lambda + 1)P_\infty \\ &= \epsilon s P_0 + \sum_{i=1}^{d-d_1} P_{\alpha_i} + \lambda \sum_{j=1}^{d-d_1} P_{\gamma_j} + (\lambda + 1) \sum_{k=d-d_1+1}^{d} P_{\alpha_k} \\ &\quad - (\epsilon s + d + \lambda d)P_\infty.\end{aligned}$$

This implies that the extension $K(x, y)/K(x)$ is a Kummer extension of degree m and, for a place P of $K(x, y)$, the ramification index is given by

$$e(P) = \begin{cases} m/(m, s), & \text{if } P \text{ is over } P_0, \\ m, & \text{if } P \text{ is over } P_{\alpha_i} \text{ or } P_{\gamma_i}, \text{ for } i = 1, \ldots, d - d_1, \\ m/(m, \lambda + 1), & \text{if } P \text{ is over } P_{\alpha_i}, \text{ for } i = d - d_1 + 1, \ldots, d, \\ m/(m, \epsilon s + d + \ d\lambda), & \text{if } P \text{ is over } P_\infty, \\ 1, & \text{otherwise.} \end{cases}$$

By the Riemann-Hurwitz formula, the genus g of $K(x, y)$ satisfies

$$2g - 2 = -2m + m - (m, s) + 2(m - 1)(d - d_1) + d_1(m - (m, \lambda + 1)) + m - (m, \epsilon s + d + \ d\lambda),$$

which gives

$$g = (m - 1)d + 1 - \frac{(m, s) + (m, \epsilon s + d + \ d\lambda) + d_1(m, \lambda + 1) + d_1(m - 2)}{2}.$$

□

In the subsequent subsections, we investigate the number of $\mathbb{F}_{q^2}$-rational points on the curve (3.2) for the cases $\epsilon = -1$ and $\lambda = 1$, and $\epsilon = 1$ and $\lambda = -1$ separately. Note that the curves $\mathcal{X}$ for $\epsilon = \lambda = 1$ and $\epsilon = \lambda = -1$ are isomorphic to the curves with $\epsilon = -1$ and $\lambda = 1$, and $\epsilon = 1$ and $\lambda = -1$ respectively.

3.1.1 The case of $\epsilon = -1$ and $\lambda = 1$.

In this subsection, we restrict ourselves to the curve $\mathcal{X}$ in (3.2) with $\epsilon = -1$ and $\lambda = 1$. We impose certain conditions on the polynomial $f \in \mathbb{F}_q[X]$ to provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points on the curve $\mathcal{X}$. Moreover, for some of these algebraic curves, we compute the exact number of $\mathbb{F}_{q^2}$-rational points.

Theorem 3.1.2. *Let $m \geq 2$ be a divisor of $q+1$, $f \in \mathbb{F}_q[X]$ be a separable polynomial of degree d satisfying $f(0) \neq 0$ and $(f, f^*) = 1$, and s be an integer such that $0 \leq s < m$. Then the algebraic curve defined by*

$$\mathcal{X}: \quad Y^m = \frac{f(X)f^*(X)}{X^s} \tag{3.3}$$

has genus

$$g = (2md - 2(d-1) - (m,s) - (m, 2d-s))/2.$$

Further if $(f, X^{q+1}-1) = 1$, then the number of rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ over $\mathbb{F}_{q^2}$ satisfies

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m[(q+1, 2(d-s)) + q - 3 - 2N_f(\mathbb{F}_q^*)] + 2N_f(\mathbb{F}_{q^2}).$$

In particular, for $s = d$, we have $\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2m(q-1-N_f(\mathbb{F}_q^*)) + 2N_f(\mathbb{F}_{q^2})$.

Proof. A direct application of Proposition 3.1.1 gives the genus of the curve defined in (3.3). We now provide an expression for the number of $\mathbb{F}_{q^2}$-rational points on this curve. Let $\alpha \in \mathbb{F}_{q^2}^*$ be such that $f(\alpha)f^*(\alpha) \neq 0$. Then $\frac{f(\alpha)f^*(\alpha)}{\alpha^s}$ is a m-th power in $\mathbb{F}_{q^2}$ if and only if $\left(\frac{f(\alpha)f^*(\alpha)}{\alpha^s}\right)^{\frac{q^2-1}{m}} = 1$, which is equivalent to

$$\left(\left(\frac{f(\alpha)f^*(\alpha)}{\alpha^s}\right)^{q-1} - 1\right)\left(\sum_{i=0}^{\frac{q+1}{m}-1}\left(\frac{f(\alpha)f^*(\alpha)}{\alpha^s}\right)^{(q-1)i}\right) = 0,$$

that is,

$$((f(\alpha)f^*(\alpha))^{q-1} - \alpha^{s(q-1)})\left(\sum_{i=0}^{\frac{q+1}{m}-1}(f(\alpha)f^*(\alpha))^{(q-1)i}\alpha^{s(q-1)\left(\frac{q+1}{m}-1-i\right)}\right) = 0.$$

Let

$$h_1(X) = (f(X)f^*(X))^{q-1} - X^{s(q-1)}$$

and

$$h_2(X) = \sum_{i=0}^{\frac{q+1}{m}-1}(f(X)f^*(X))^{(q-1)i}X^{s(q-1)\left(\frac{q+1}{m}-1-i\right)}.$$

Then h_1 and h_2 are coprime polynomials. In fact, if α is a root of h_1, then $(f(\alpha)f^*(\alpha))^{q-1} = \alpha^{s(q-1)}$ and

$$\begin{aligned} h_2(\alpha) &= \sum_{i=0}^{\frac{q+1}{m}-1}(f(\alpha)f^*(\alpha))^{(q-1)i}\alpha^{s(q-1)\left(\frac{q+1}{m}-1-i\right)} \\ &= \sum_{i=0}^{\frac{q+1}{m}-1}\alpha^{s(q-1)i}\alpha^{s(q-1)\left(\frac{q+1}{m}-1-i\right)} \\ &= \left(\frac{q+1}{m}\right)\alpha^{s(q+1)\left(\frac{q+1}{m}-1\right)} \neq 0. \end{aligned}$$

It is also clear that $(h_1, ff^*) = (h_2, ff^*) = 1$. We conclude that

$$\begin{aligned}&\#\left\{\alpha \in \mathbb{F}_{q^2}^* : f(\alpha)f^*(\alpha) \neq 0 \text{ and } \frac{f(\alpha)f^*(\alpha)}{\alpha^s} \text{ is a } m\text{-th power in } \mathbb{F}_{q^2}^*\right\}\\ &= N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2}).\end{aligned}$$

From Remark 1.2.16, each $\alpha \in \mathbb{F}_{q^2}$ such that $f(\alpha)f^*(\alpha) = 0$ gives one rational point on the curve. From Remark 1.2.16, we also conclude that each one of $x = 0$ and $x = \infty$ (that is, each one of the places P_0 and P_∞ of $\mathbb{F}_q(x)$) contributes (m, s) and $(m, 2d - s)$ rational points on the curve, respectively. So the number of rational points on the curve $\mathcal{X}$ is

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = (m, s) + (m, 2d - s) + 2N_f(\mathbb{F}_{q^2}) + m(N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2})). \tag{3.4}$$

Now we assume that $(f, X^{q+1} - 1) = 1$. Note that, for $\beta \in \{\omega \in \mathbb{F}_{q^2} : \omega^{(q+1,2(d-s))} = 1\}$, we have $\beta^q = \beta^{-1}$, and thus we write

$$\begin{aligned}h_1(\beta) &= (f(\beta)f^*(\beta))^{q-1} - \beta^{s(q-1)} = \frac{(f(\beta)f^*(\beta))^q}{f(\beta)f^*(\beta)} - \beta^{-2s}\\ &= \frac{f(\beta^q)f^*(\beta^q)}{f(\beta)f^*(\beta)} - \beta^{-2s} = \frac{f(1/\beta)f^*(1/\beta)}{f(\beta)f^*(\beta)} - \beta^{-2s}\\ &= \frac{f(\beta)f^*(\beta)}{\beta^{2d}f(\beta)f^*(\beta)} - \beta^{-2s} = \beta^{-2d} - \beta^{-2s} = 0.\end{aligned}$$

Also, for $\beta \in \mathbb{F}_q^*$ such that $f(\beta)f^*(\beta) \neq 0$, we have $h_1(\beta) = 0$. Therefore

$$N_{h_1}(\mathbb{F}_{q^2}) \geq (q + 1, 2(d - s)) + q - 1 - 2N_f(\mathbb{F}_q^*) - (q - 1, 2).$$

Hence we get

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2N_f(\mathbb{F}_{q^2}) + m[(q + 1, 2(d - s)) + q - 3 - 2N_f(\mathbb{F}_q^*)].$$

□

In what follows we compute the genus and the exact number of rational points for some families of algebraic curves as constructed in (3.3).

Theorem 3.1.3. *Let $b \in \mathbb{F}_q^*$ be such that $b^2 \neq 1$, and d be a positive divisor of $q + 1$. Then the algebraic curve defined by*

$$\mathcal{X} : Y^{q+1} = \frac{bX^{2d} + (b^2 + 1)X^d + b}{X^d}$$

has genus

$$g = d(q - 1) + 1$$

and its number of $\mathbb{F}_{q^2}$-rational points is given by

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = d(q^2 - 1) + (d, 2)(q + 1)^2 + 4d - d(q + 1)((q - 1, 2) + 2).$$

In particular, if $q \geq 17$ is odd and $d = 2$, then this curve has many points.

Proof. The curve $\mathcal{X}$ corresponds to the construction in (3.3) for $f(X) = X^d + b$, $s = d$, and $m = q+1$. Since $b^2 \neq 1$, we have $(f, f^*) = 1$. The genus of the curve follows from Theorem 3.1.2. Now we compute the number of $\mathbb{F}_{q^2}$-rational points on the curve following the proof and notation as in Theorem 3.1.2. Since $b \in \mathbb{F}_q^*$ and d is a divisor of $q+1$, each one of f and f^* has d distinct roots in $\mathbb{F}_{q^2}^*$ and therefore $N_{ff^*}(\mathbb{F}_{q^2}) = 2d$. Note that each root of ff^* contributes one rational point on the curve. From Remark 1.2.16, we also conclude that each one of $x = 0$ and $x = \infty$ contributes $(q+1, d) = d$ rational points on the curve, respectively.

On the other hand, we have that

$$\begin{aligned}&\#\left\{\alpha \in \mathbb{F}_{q^2}^* : f(\alpha)f^*(\alpha) \neq 0 \text{ and } \frac{f(\alpha)f^*(\alpha)}{\alpha^d} \text{ is a } (q+1)\text{-th power in } \mathbb{F}_{q^2}^*\right\}\\ &= N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2}),\end{aligned}$$

where

$$h_1(X) = (f(X)f^*(X))^{q-1} - X^{d(q-1)} = \frac{b(X^{d(q+1)}-1)(X^{d(q-1)}-1)}{f(X)f^*(X)} \quad \text{and} \quad h_2(X) \equiv 1.$$

Clearly $N_{h_2}(\mathbb{F}_{q^2}) = 0$. Next we show that the polynomial $h_1 \in \mathbb{F}_q[X]$ has $d(q-1) + 2(q+1) - 4d$ distinct roots in $\mathbb{F}_{q^2}^*$. In fact, since

$$\begin{aligned}(X^{d(q+1)} - 1, X^{q^2-1} - 1) &= X^{(d,2)(q+1)} - 1,\\ (X^{d(q-1)} - 1, X^{q^2-1} - 1) &= X^{d(q-1)} - 1, \text{ and}\\ (X^{(d,2)(q+1)} - 1, X^{d(q-1)} - 1) &= X^{d(q-1,2)} - 1,\end{aligned}$$

we obtain $d(q-1) + (d,2)(q+1) - d(q-1,2)$ distinct roots of $(X^{d(q+1)}-1)(X^{d(q-1)}-1)$ in $\mathbb{F}_{q^2}^*$. Since $N_{ff^*}(\mathbb{F}_{q^2}) = 2d$, we conclude that h_1 has $d(q-1)+(d,2)(q+1)-d(q-1,2)-2d$ distinct roots in $\mathbb{F}_{q^2}^*$. Hence the number of $\mathbb{F}_{q^2}$-rational points on the curve $\mathcal{X}$ is given by

$$\begin{aligned}\#\mathcal{X}(\mathbb{F}_{q^2}) &= 4d + (q+1)(d(q-1) + (d,2)(q+1) - d(q-1,2) - 2d)\\ &= d(q^2-1) + (d,2)(q+1)^2 + 4d - d(q+1)((q-1,2)+2).\end{aligned}$$

Next we show that for $q \geq 17$ odd and $d = 2$, this curve has many points. By Remark 3.0.1, a curve is considered to have many points if and only if $L(q^2, g) \leq \#\mathcal{X}(\mathbb{F}_{q^2})$. From the Hasse-Weil bound, we have

$$L(q^2, g) \leq \left\lfloor \frac{q^2+1+2gq-q^2-1}{\sqrt{2}} \right\rfloor + q^2 + 1 = \left\lfloor \sqrt{2}gq \right\rfloor + q^2 + 1.$$

In particular, algebraic curves satisfying $\sqrt{2}gq + q^2 + 1 \leq \#\mathcal{X}(\mathbb{F}_{q^2})$ have many points. Therefore the curve $\mathcal{X}$ has many points if

$$\sqrt{2}q(d(q-1)+1) + q^2 + 1 \leq d(q^2-1) + (d,2)(q+1)^2 + 4d - d(q+1)((q-1,2)+2). \quad (3.5)$$

The condition (3.5) is never satisfied when q is even or when q is odd and $d \neq 2$. For q odd and $d = 2$, this condition is satisfied if and only if $q \geq 17$. □

Note that for $b^2 = 1$ the curve $\mathcal{X}$ in Theorem 3.1.3 is isomorphic to the curve with affine equation $Y^{q+1} = (X^d + b)^2/X^d$. In order to complete the analysis of the curve $\mathcal{X}$, we study in Proposition 3.1.4 an absolutely irreducible component of the curve $Y^{q+1} = (X^d + b)^2/X^d$ obtained when d is even, and in Proposition 3.1.5 we study this curve for d odd.

Proposition 3.1.4. *Assume q is odd. Let $d \geq 1$ be a positive integer such that $4d$ divides $q^2 - 1$, and let $b \in \mathbb{F}_q$ be such that $b^2 = 1$. Then the algebraic curve $\mathcal{X}$ defined by the affine equation*

$$Y^{(q+1)/2} = \frac{X^{2d} + b}{X^d} \tag{3.6}$$

has genus

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

and its number of $\mathbb{F}_{q^2}$-rational points is given by

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = \frac{(q+1)^2(2d, q-1) + (q^2+1)(2d, q+1) - 2d(3q+1)}{2}.$$

In particular, this curve is maximal over $\mathbb{F}_{q^2}$ if and only if $(2d, q+1) + (2d, q-1) = 2(d+1)$.

Proof. By Remark 1.2.16, each one of the points $x = 0$ and $x = \infty$ contributes with $(d, \frac{q+1}{2})$ rational points on the curve. Now we consider the roots of $X^{2d} + b$. Since $4d \mid q^2 - 1$, we have $\#\{\alpha \in \mathbb{F}_{q^2} : \alpha^{2d} + b = 0\} = 2d$ and each root of $X^{2d} + b$ contributes with one rational point. On the other hand, for $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{2d} + b \neq 0$, we have

$$\begin{aligned} \frac{\alpha^{2d}+b}{\alpha^d} \text{ is a } \frac{(q+1)}{2}\text{-th power in } \mathbb{F}_{q^2}^* \quad &\Leftrightarrow \quad \left(\frac{\alpha^{2d}+b}{\alpha^d}\right)^{2(q-1)} = 1 \\ &\Leftrightarrow \quad (\alpha^{2d(q+1)} - 1)(\alpha^{2d(q-1)} - 1) = 0. \end{aligned} \tag{3.7}$$

Since

$$\begin{aligned} &(X^{2d(q+1)} - 1, X^{q^2-1} - 1) = X^{(q+1)(2d,q-1)} - 1, \\ &(X^{2d(q-1)} - 1, X^{q^2-1} - 1) = X^{(q-1)(2d,q+1)} - 1, \text{ and} \\ &(X^{(q+1)(2d,q-1)} - 1, X^{(q-1)(2d,q+1)} - 1) = X^{4d} - 1, \end{aligned}$$

we obtain that there are $(q+1)(2d, q-1) + (q-1)(2d, q+1) - 4d$ elements $\alpha \in \mathbb{F}_{q^2}^*$ satisfying (3.7). Also, since

$$X^{2d} + b \mid (X^{2d(q+1)} - 1)(X^{2d(q-1)} - 1),$$

we conclude that the polynomial $(X^{2d(q+1)} - 1)(X^{2d(q-1)} - 1)$ has $(q+1)(2d, q-1) + (q-1)(2d, q+1) - 6d$ distinct roots in $\mathbb{F}_{q^2}^* \setminus \{\alpha \in \mathbb{F}_{q^2}^* : \alpha^{2d} + b = 0\}$. Consequently,

$$\begin{aligned} \#\mathcal{X}(\mathbb{F}_{q^2}) &= 2d + 2\left(d, \frac{q+1}{2}\right) + \frac{q+1}{2}((q+1)(2d, q-1) + (q-1)(2d, q+1) - 6d) \\ &= \frac{(q+1)^2(2d, q-1) + (q^2+1)(2d, q+1) - 2d(3q+1)}{2}. \end{aligned}$$

Finally, we note that

$$\#\mathcal{X}(\mathbb{F}_{q^2}) - q^2 - 1 - 2gq = \frac{(q+1)^2}{2}((2d, q-1) + (2d, q+1) - 2 - 2d).$$

This completes the proof. □

Proposition 3.1.5. *Assume q is odd. Let $d \geq 1$ be an odd integer such that $p \nmid d$, and let $b \in \mathbb{F}_q$ be such that $b^2 = 1$. Then the algebraic curve $\mathcal{X}$ defined by the equation*

$$Y^{q+1} = \frac{(X^d + b)^2}{X^d} \tag{3.8}$$

has genus

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

and its number of $\mathbb{F}_{q^2}$-rational points is given by

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = (q^2+1)(d, q+1) + (q+1)^2(d, q-1) - (3q+1)(d, q^2-1).$$

In particular, for a divisor d of $q^2 - 1$, the curve $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal if and only if either $(d, q+1) = 1$ or $(d, q-1) = 1$.

Proof. The computation of the genus is analogous to the one in Proposition 3.1.1 and the computation of the number of $\mathbb{F}_{q^2}$-rational points on the curve is analogous to the proof of Proposition 3.1.4. For a divisor d of $q^2 - 1$, we have

$$\begin{aligned}
\#\mathcal{X}(\mathbb{F}_{q^2}) - q^2 - 1 - 2gq &= (q^2+1)(d, q+1) + (q+1)^2(d, q-1) - (3q+1)d - q^2 - 1 \\
&\quad - dq(q+1) + 2dq + 2q(d, q+1) - 2q \\
&= (q+1)^2((d, q+1) + (d, q-1) - 1) - d(q+1)^2 \\
&= (q+1)^2((d, q+1) + (d, q-1) - 1 - d) \\
&= -(q+1)^2((d, q+1) - 1)((d, q-1) - 1).
\end{aligned}$$

□

Remark 3.1.6. *The curve in Proposition 3.1.5 is isomorphic to $Y^{q+1} = X^{q+1-d}(X^d + b)^2$. We point out that for some values of d (for instance, when d is a divisor of $q+1$), this curve has appeared in [22, Example 6.4 (case 2)] as a subcover of the Hermitian curve over $\mathbb{F}_{q^2}$ given by*

$$Y^{m_1} = (-1)^k X^{bm}(X^m + 1)^k,$$

where m, m_1 are divisors of $q+1$, and k, b are positive integers.

We now provide examples of curves with many points from the constructions obtained in this subsection. For this, we use the notation given in Remark 3.0.1.

Example 3.1.7. *Let $f(X) = X + b$ where $b \in \mathbb{F}_q^*$ is such that $b^2 \neq 1$. In the following tables, we list q, m, b, s, g and $\#\mathcal{X}(\mathbb{F}_{q^2})$ where $m, s, \mathcal{X}$ and f satisfy the hypotheses of Theorem 3.1.2.*

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
3^2	5	$\xi_{3^2}^2$	3	4	$154^\dagger$
3^2	10	$\xi_{3^2}^2$	4	8	$226^\dagger$
5	6	2	4	4	$66^\dagger$
5^2	13	ξ_{5^2}	0	6	$926^\dagger$
5^2	13	2	1	12	$1226^\dagger$
5^2	26	2	4	24	$1826^\dagger$
7	4	2	3	3	$92^\dagger$
7^2	5	$\xi_{7^2}^3$	1	4	$2794^\dagger$
7^2	10	3	4	8	$3186^\dagger$
7^2	25	ξ_{7^2}	0	12	$3578^\dagger$
7^2	50	$\xi_{7^2}^{12}$	10	44	$6714^\dagger$
7^2	50	$\xi_{7^2}^{12}$	4	48	$7106^\dagger$
13	14	2	0	6	$326^\dagger$

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
13	14	5	4	12	$482^\dagger$
13^2	10	$\xi_{13^2}^4$	3	9	31504
13^2	34	8	4	32	$39378^\dagger$
17	18	2	0	8	$562^\dagger$
17	18	4	6	14	$766^\dagger$
17	18	4	4	16	$834^\dagger$
19	5	2	0	2	$438^\dagger$
19	20	2	0	9	$704^\dagger$

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	*OLB*
7^2	50	$\xi_{7^2}^4$	5	47	5708	5658

Example 3.1.8. *Let $f(X) = X^2 + b$ where $b \in \mathbb{F}_q^*$ such that $b^2 \neq 1$. We list q, m, b, s, g and $\#\mathcal{X}(\mathbb{F}_{q^2})$ in the following tables where $m, s, \mathcal{X}$ and f satisfy the hypotheses of Theorem 3.1.2. We note that if $m = q + 1$ and $s = 2$ in the following tables, then the genus g and the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ satisfies Theorem 3.1.3.*

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
3^2	5	ξ_{3^2}	0	6	$190^\dagger$
3^2	10	ξ_{3^2}	2	17	288
5	6	2	5	10	$126^\dagger$
5^2	26	ξ_{5^2}	2	49	2400
7^2	5	$\xi_{7^2}^3$	0	6	$2990^\dagger$
7^2	25	3	0	36	$5930^\dagger$
11	2	3	1	2	$166^\dagger$
11	3	3	2	4	$210^\dagger$
11	6	3	5	10	$342^\dagger$
13	2	5	1	2	$222^\dagger$
13	14	2	2	25	624

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
13	14	5	9	26	$846^\dagger$
13^2	5	8	2	8	$31266^\dagger$
13^2	10	5	2	17	34208
17	2	3	1	2	$358^\dagger$
17	3	3	2	4	$426^\dagger$
17	6	3	5	10	$630^\dagger$
17	9	5	0	12	$698^\dagger$
17^2	5	4	2	8	$88146^\dagger$
19	5	4	0	6	$590^\dagger$
19	10	14	5	16	$970^\dagger$

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
7^2	25	$\xi^3_{7^2}$	5	46	$6910^\dagger$	5589
13^2	34	$\xi^5_{13^2}$	0	49	41112	40273
17	18	2	2	33	1088	1083
17^2	10	5	2	17	92928	90470
19	20	2	2	37	1368	1356

New record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
7^2	10	$\xi^3_{7^2}$	0	13	3576	3258
7^2	10	$\xi^3_{7^2}$	2	17	3968	3808

Example 3.1.9. *Let $f(X) = X^3 + b \in \mathbb{F}_q[X]$, $m \geq 2$ be a divisor of $q + 1$, and s be an integer such that $0 \leq s < m$. We consider the algebraic curve defined by*

$$\mathcal{X} : \quad Y^m = \frac{f(X)f^*(X)}{X^s}.$$

The following tables consists of q, m, b, s, g and $\#\mathcal{X}(\mathbb{F}_{q^2})$ which leads to meet record/new entry in the manYPoints table in [60]. Further, if $m = q + 1$, $s = 3$ and $b^2 = 1$, then the genus g and the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ satisfies Proposition 3.1.5.

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
17	18	4	0	40	$1650^\dagger$

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
5^2	13	1	3	18	$1526^\dagger$	1262
5^2	26	1	3	36	$2426^\dagger$	1898
7^2	10	$\xi^2_{7^2}$	8	26	4444	4203
7^2	10	$\xi^3_{7^2}$	3	27	4748	4273
13^2	10	$\xi^2_{13^2}$	8	26	36604	34776

Remark 3.1.10. *For $q = 5^2$ in Example 3.1.9, we obtain an explicit equation for a maximal curve of genus 36 over $\mathbb{F}_{5^4}$ given by $Y^{26} = \frac{(X^3+1)^2}{X^3}$. The covered curve $Y^{13} = \frac{(X^3+1)^2}{X^3}$ of genus 18 also provides a maximal curve. Moreover, in Example 3.1.8 we get a new maximal curve over $\mathbb{F}_{7^4}$ of genus 46. These genera already appeared in [16] as the genus of a curve covered by the Hermitian curve.*

These three examples of explicit maximal curves are new entries in the manYPoints table [60] and rise a natural question, to decide if these curves are or not covered by the Hermitian curve.

Example 3.1.11. *Let $f(X) = X^4 + b$ where $b \in \mathbb{F}_q^*$ is such that $b^2 \neq 1$. In the following table, we list q, m, b, s, g and $\#\mathcal{X}(\mathbb{F}_{q^2})$ where $m, s, \mathcal{X}$ and f satisfy the hypotheses of Theorem 3.1.2.*

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
3^2	10	$\xi_{3^2}^{2}$	9	36	$730^\dagger$
5^2	2	2	1	4	$826^\dagger$
5^2	13	2	4	48	$3026^\dagger$
11^2	2	$\xi_{11^2}^{30}$	1	4	$15610^\dagger$
17	3	4	4	8	$562^\dagger$
17	9	4	4	32	$1378^\dagger$

Next, we provide some more examples of curves with many points.

Example 3.1.12. *In the following tables, we list* q, m, f, s, g *and* $\#\mathcal{X}(\mathbb{F}_{q^2})$ *where* $m, s, \mathcal{X}$ *and* $f \in \mathbb{F}_q[X]$ *satisfy the hypotheses of Theorem 3.1.2.*

Meet record

q	m	f	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
2	3	X^3+X+1	0	4	$15^\dagger$
3	4	X^2+2X+2	0	3	$28^\dagger$
3^2	5	X^4+X^2+2	4	16	$370^\dagger$
7	4	X^4+X^2+5	0	5	$120^\dagger$
7	8	X^2+3X+3	6	9	$176^\dagger$
7^2	5	X^4+2X^2+3	4	16	$3970^\dagger$
11	6	$X^2+3X+10$	0	7	$276^\dagger$
11	6	$X^2+3X+10$	2	9	$320^\dagger$
11	12	$X^2+3X+10$	0	15	$452^\dagger$
11	12	$X^2+3X+10$	8	19	$540^\dagger$
19	10	$X^2+6X+18$	0	13	$856^\dagger$
19	10	$X^2+6X+18$	2	17	$1008^\dagger$
19	20	$X^2+6X+18$	8	35	$1692^\dagger$
19	10	X^4+X^2+7	9	36	$1730^\dagger$

New entry

q	m	f	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	*OLB*
7^2	10	$X^2+\xi_{7^2}X+\xi_{7^2}^{39}$	3	18	3726	3649
7^2	10	$X^4+\xi_{7^2}X^2+\xi_{7^2}^{29}$	4	25	4272	4134
7^2	10	X^4+2X^2+3	4	35	5052	4827
17	6	X^4+6X^2+16	1	20	826	770
17	18	$X^3+14X+2$	3	23	892	842
19	10	X^4+2X^2+16	4	25	1072	1033

Inspired by the previous constructions, we present some improvements obtained by using Artin-Schreier extensions.

Example 3.1.13. *Let $\mathcal{X}$ be the curve defined by the equation*

$$\mathcal{X}: \quad Y^q + Y = \frac{f(X)f^*(X)}{X^s},$$

where $f \in \mathbb{F}_q[X]$ and $s \geq 0$ is an integer. We have the following improvements in the manYPoints table [60].

New entry

q	f	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	*OLB*
7	X^2+1	2	12	170	165
11	X^2+1	2	20	442	430
13	X^2+1	2	24	626	611

3.1.2 The case of $\epsilon = 1$ and $\lambda = -1$

In this subsection, we consider the curve $\mathcal{X}$ in (3.2) with $\epsilon = 1$ and $\lambda = -1$. As in Subsection 3.1.1, we provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points on the curve $\mathcal{X}$ when the polynomial $f \in \mathbb{F}_q[X]$ satisfies certain conditions. We also provide some examples of curves with many points.

Theorem 3.1.14. *Let $m \geq 2$ be a divisor of $q-1$, $f \in \mathbb{F}_q[X]$ be a separable polynomial of degree d satisfying $f(0) \neq 0$ and $(f, f^*) = 1$, and s be an integer such that $0 \leq s < m$. Then the algebraic curve defined by the affine equation*

$$\mathcal{X}: \quad Y^m = \frac{X^s f(X)}{f^*(X)} \tag{3.9}$$

has genus

$$g = d(m-1) + 1 - (m, s).$$

Further if $(f, X^{q+1} - 1) = 1$, then the number of rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ over $\mathbb{F}_{q^2}$ satisfies

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2N_f(\mathbb{F}_{q^2}) + m(q+1).$$

Proof. A direct application of Proposition 3.1.1 gives the genus of the curve defined in (3.9). To obtain an expression for the number of rational points for this curve, we observe that for $\alpha \in \mathbb{F}_{q^2}^*$ with $f(\alpha)f^*(\alpha) \neq 0$, we have that $\frac{\alpha^s f(\alpha)}{f^*(\alpha)}$ is a m-th power in $\mathbb{F}_{q^2}$ if and only if $\left(\frac{\alpha^s f(\alpha)}{f^*(\alpha)}\right)^{\frac{q^2-1}{m}} = 1$, which is equivalent to

$$\left((\alpha^s f(\alpha))^{q+1} - f^*(\alpha)^{q+1}\right) \left(\sum_{i=0}^{\frac{q-1}{m}-1} (\alpha^s f(\alpha))^{(q+1)i} f^*(\alpha)^{(q+1)\left(\frac{q-1}{m}-1-i\right)} \right) = 0.$$

Let

$$h_1(X) = (X^s f(X))^{q+1} - f^*(X)^{q+1}$$

and

$$h_2(X) = \sum_{i=0}^{\frac{q-1}{m}-1} (X^s f(X))^{(q+1)i} f^*(X)^{(q+1)\left(\frac{q-1}{m}-1-i\right)}.$$

Then h_1 and h_2 are coprime. In fact, if α is a root of h_1 we have $(\alpha^s f(\alpha))^{q+1} = f^*(\alpha)^{q+1}$ and

$$\begin{aligned} h_2(\alpha) &= \sum_{i=0}^{\frac{q-1}{m}-1} (\alpha^s f(\alpha))^{(q+1)i} f^*(\alpha)^{(q+1)\left(\frac{q-1}{m}-1-i\right)} = \sum_{i=0}^{\frac{q-1}{m}-1} f^*(\alpha)^{(q+1)i} f^*(\alpha)^{(q+1)\left(\frac{q-1}{m}-1-i\right)} \\ &= \sum_{i=0}^{\frac{q-1}{m}-1} f^*(\alpha)^{(q+1)\left(\frac{q-1}{m}-1\right)} = \left(\frac{q-1}{m}\right) f^*(\alpha)^{(q+1)\left(\frac{q-1}{m}-1\right)} \neq 0. \end{aligned}$$

Also, since $(h_1, ff^*) = (h_2, ff^*) = 1$, we obtain

$$\#\left\{\alpha \in \mathbb{F}_{q^2}^* : f(\alpha)f^*(\alpha) \neq 0 \text{ and } \frac{\alpha^s f(\alpha)}{f^*(\alpha)} \text{ is a } m\text{-th power in } \mathbb{F}_{q^2}^*\right\} = N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2}).$$

On the other hand, from Remark 1.2.16, we know that each root in $\mathbb{F}_{q^2}$ of the polynomial ff^* gives one rational point on the curve. Thus

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2N_f(\mathbb{F}_{q^2}) + m(N_{h_1}(\mathbb{F}_{q^2}) + N_{h_2}(\mathbb{F}_{q^2})). \tag{3.10}$$

Next we assume $(f, X^{q+1} - 1) = 1$. Then for $\beta \in \mathbb{F}_{q^2}$ such that $\beta^{q+1} = 1$, we have

$$\begin{aligned} h_1(\beta) &= (\beta^s f(\beta))^{q+1} - f^*(\beta)^{q+1} \\ &= \beta^{s(q+1)} f(\beta)^{q+1} - \beta^{d(q+1)} f(\beta)^{q+1} \\ &= 0. \end{aligned}$$

Therefore $N_{h_1}(\mathbb{F}_{q^2}) \geq q + 1$. Hence the assertion on the number of rational points follows from (3.10). □

From the constructions given in Theorem 3.1.14, we obtain the following examples of curves with many points.

Example 3.1.15. *Let $f(X) = X + b \in \mathbb{F}_q[X]$ be such that $b \neq 0$ and $b^2 \neq 1$, and $m, s, \mathcal{X}$ be as defined in Theorem 3.1.14. Then $(f, f^*) = (f, X^{q+1} - 1) = 1$ and the curve $\mathcal{X}$ has genus $g = m - (m, s)$. We obtain the following tables of curves with many points.*

Meet record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$
7	6	2	4	4	102
11^2	8	$\xi_{11^2}^{30}$	4	4	$15610^{\dagger}$
11^2	8	$\xi_{11^2}^{37}$	3	7	16308
13	12	2	4	8	362

New record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
17	16	3	9	15	708	692
11^2	15	$\xi_{11^2}^{26}$	5	10	16952	16942
19	18	2	3	15	866	782

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
5^2	24	$\xi_{5^2}^{3}$	8	16	1202	1191
5^2	24	2	4	20	1450	1333
5^2	24	2	9	21	1400	1368
7^2	16	$\xi_{7^2}^{3}$	6	14	3558	3372
7^2	16	$\xi_{7^2}^{5}$	7	15	3684	3441
7^2	24	$\xi_{7^2}^{13}$	5	23	4276	3995
11^2	15	$\xi_{11^2}^{2}$	4	14	17674	17037
11^2	24	$\xi_{11^2}^{25}$	8	16	18050	17379
11^2	24	5	3	21	18968	18235
11^2	24	$\xi_{11^2}^{21}$	7	23	19204	18577
11^2	30	$\xi_{11^2}^{9}$	3	27	19988	19262
11^2	30	$\xi_{11^2}^{2}$	4	28	20106	19433
11^2	40	$\xi_{11^2}^{7}$	4	36	20962	20802

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
11^2	40	$\xi_{11^2}^{13}$	6	38	22246	21144
13^2	12	$\xi_{13^2}^{23}$	5	11	31972	31191
13^2	14	$\xi_{13^2}^{10}$	9	13	32260	31669
13^2	21	$\xi_{13^2}^{2}$	5	20	34318	33342
13^2	24	$\xi_{13^2}^{23}$	5	23	35428	34059
13^2	28	$\xi_{13^2}^{5}$	9	27	35452	35015
13^2	42	$\xi_{13^2}^{11}$	7	35	37550	36927
17^2	12	$\xi_{17^2}^{4}$	9	9	87938	87200
17^2	12	$\xi_{17^2}^{6}$	5	11	88828	88017
17^2	16	$\xi_{17^2}^{7}$	5	15	91044	89652
17^2	24	$\xi_{17^2}^{4}$	5	23	94996	92922
17^2	32	$\xi_{17^2}^{7}$	5	31	97604	96191
17^2	48	$\xi_{17^2}^{4}$	5	47	105124	102731

Example 3.1.16. *Let $f(X) = X^2 + b \in \mathbb{F}_q[X]$ be such that $b \neq 0$ and $b^2 \neq 1$, and $m, s, \mathcal{X}$ be as defined in Theorem 3.1.14. Then $(f, f^*) = 1$ and the curve $\mathcal{X}$ has genus $g = 2m - 1 - (m, s)$. For this case, we have the following tables.*

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
5^2	8	ξ_{5^2}	2	13	1128	1085
5^2	24	ξ_{5^2}	10	45	2216	2216
7^2	12	$\xi_{7^2}^{6}$	2	21	4040	3857
7^2	16	$\xi_{7^2}^{13}$	2	29	4552	4411
7^2	24	$\xi_{7^2}^{5}$	6	41	5380	5243
7^2	24	$\xi_{7^2}^{3}$	4	43	5476	5381
7^2	24	$\xi_{7^2}^{10}$	10	45	5672	5520
11	10	3	2	17	408	386
11^2	8	$\xi_{11^2}^{18}$	4	11	16940	16524
11^2	8	$\xi_{11^2}^{7}$	2	13	17480	16866
11^2	10	$\xi_{11^2}^{19}$	2	17	18128	17551
11^2	12	$\xi_{11^2}^{43}$	4	19	18436	17893
11^2	15	$\xi_{11^2}^{2}$	5	24	18964	18748
11^2	15	$\xi_{11^2}^{31}$	3	26	19564	19091
11^2	30	ξ_{11^2}	0	29	19684	19604

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
11^2	20	$\xi_{11^2}^{26}$	5	34	20644	20460
11^2	20	$\xi_{11^2}^{37}$	8	35	20964	20631
11^2	20	$\xi_{11^2}^{13}$	2	37	21528	20973
11^2	24	$\xi_{11^2}^{25}$	4	43	22372	22000
11^2	24	$\xi_{11^2}^{21}$	2	45	22472	22342
13	12	2	8	19	532	519
13^2	12	$\xi_{13^2}^{5}$	4	19	33748	33103
13^2	12	$\xi_{13^2}^{44}$	1	22	34374	33820
13^2	14	$\xi_{13^2}^{8}$	2	25	35400	34537
13^2	21	8	3	38	38314	37644
13^2	24	$\xi_{13^2}^{23}$	10	45	40136	39317
17	16	2	4	27	972	939
17^2	8	ξ_{17^2}	6	13	89224	88835
17^2	18	ξ_{17^2}	7	34	97494	97418
19	18	2	6	29	1156	1141

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
19^2	6	ξ_{19^2}	1	10	136782	135427
19^2	12	ξ_{19^2}	0	11	136612	135937
19^2	9	ξ_{19^2}	3	14	138208	137469
19^2	9	ξ_{19^2}	2	16	139650	138490
19^2	24	ξ_{19^2}	0	23	142372	142064

New record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
17	8	4	2	13	648	612

Example 3.1.17. *Let $f(X) = X^3 + b \in \mathbb{F}_q[X]$ be such that $b \neq 0$ and $b^2 \neq 1$, and $m, s, \mathcal{X}$ be as defined in Theorem 3.1.14. Then $(f, f^*) = 1$ and the curve $\mathcal{X}$ has genus $g = 3m - 2 - (m, s)$. In this case, we obtain the following tables.*

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
7^2	12	$\xi_{7^2}^{2}$	3	31	4680	4550
11^2	8	$\xi_{11^2}^{15}$	4	18	18486	17722
11^2	12	$\xi_{11^2}^{2}$	0	22	19080	18406
11^2	12	$\xi_{11^2}^{9}$	3	31	20820	19946
11^2	15	$\xi_{11^2}^{30}$	6	40	22242	21486
11^2	24	$\xi_{11^2}^{2}$	0	46	22608	22513
13^2	7	$\xi_{13^2}^{4}$	3	18	33980	32864
13^2	12	$\xi_{13^2}^{23}$	3	31	36792	35971
13^2	14	$\xi_{13^2}^{21}$	7	33	37568	36449
13^2	14	$\xi_{13^2}^{3}$	3	39	38732	37883
19	9	4	6	22	972	953

New record

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
11^2	5	$\xi_{11^2}^{6}$	0	8	16566	16546

Example 3.1.18. *Let $f(X) = X^4 + b \in \mathbb{F}_q[X]$ be such that $b \neq 0$ and $b^2 \neq 1$, and $m, s, \mathcal{X}$ be as defined in Theorem 3.1.14. Then $(f, f^*) = 1$ and the curve $\mathcal{X}$ has genus $g = 4m - 3 - (m, s)$. We have the following tables of curves with many points.*

New entry

q	m	b	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
7^2	8	3	5	28	4522	4342
11^2	6	$\xi_{11^2}^{20}$	0	15	17672	17208
11^2	8	$\xi_{11^2}^{7}$	4	25	19456	18919
11^2	12	$\xi_{11^2}^{14}$	6	39	22184	21315
13	6	2	1	20	554	537
13^2	6	$\xi_{13^2}^{22}$	0	15	32216	32147
13^2	8	$\xi_{13^2}^{4}$	0	21	34584	33581
13^2	12	$\xi_{13^2}^{23}$	8	41	38784	38361
17^2	6	ξ_{17^2}	5	20	91826	91696

We finish this section by giving some additional improvements in the manYPoints table [60].

Example 3.1.19. *In the following tables, we list q, m, f, s, g and $\#\mathcal{X}(\mathbb{F}_{q^2})$ where $m, s, \mathcal{X}$ and $f \in \mathbb{F}_q[X]$ satisfy the hypotheses of Theorem 3.1.14.*

New entry

q	m	f	s	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
5^2	4	$X^4 + \xi_{5^2} X^2 + \xi_{5^2}^7$	4	9	984	944
5^2	8	$X^2 + 2X + \xi_{5^2}^7$	4	11	1092	1014
5^2	8	$X^2 + \xi_{5^2}^3 X + 2$	7	14	1206	1120
5^2	6	$X^4 + X^2 + \xi_{5^2}^{14}$	6	15	1160	1156
5^2	12	$X^2 + \xi_{5^2}^2 X + \xi_{5^2}^8$	6	17	1252	1227
5^2	6	$X^4 + X^2 + \xi_{5^2}^7$	4	19	1308	1297
7^2	6	$X^4 + \xi_{7^2}^{44} X^2 + 5$	4	19	3780	3718
7^2	8	$X^6 + \xi_{7^2}^6$	3	42	5486	5312
11^2	5	$X^8 + \xi_{11^2}^{14}$	2	32	20482	20117
11^2	5	$X^{12} + \xi_{11^2}^4$	0	44	22800	22171
13^2	6	$X^7 + 2$	0	30	35966	35732

3.2 Curves with many points from fibre products

In this section, we construct new curves with many rational points by considering the fibre product of the curves constructed in Subsections 3.1.1 and 3.1.2. To provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points for these new constructions, we use a generalization of Remark 1.2.16 given in [50, Theorem 4] for fibre products of Kummer extensions.

Theorem 3.2.1. *For $i \in \{1, 2\}$, let $m_i \geq 2$ be a divisor of $q+1$, s_i be an integer with $0 \leq s_i < m_i$, and f_i be a separable polynomial in $\mathbb{F}_q[X]$ of degree d_i satisfying $f_i(0) \neq 0$ and $(f_i, f_i^*) = (f_1 f_1^*, f_2 f_2^*) = 1$. Then the curve $\mathcal{X}$ defined by the affine equations*

$$\mathcal{X} : \begin{cases} Y_2^{m_2} = \frac{f_2(X) f_2^*(X)}{X^{s_2}} \\ Y_1^{m_1} = \frac{f_1(X) f_1^*(X)}{X^{s_1}} \end{cases} \tag{3.11}$$

has genus

$$g = m_1 m_2 (d_1 + d_2) - d_1 m_2 - d_2 m_1 + 1 - \frac{\kappa + (m_1 m_2, m_2(2d_1 - s_1), m_1(2d_2 - s_2))}{2}$$

where $\kappa = (m_1 m_2, s_1 m_2, s_2 m_1)$. Further, if $\mathbb{F}_{q^2}$ is the full constant field of $\mathbb{F}_{q^2}(\mathcal{X})$, $[\mathbb{F}_{q^2}(\mathcal{X}), \mathbb{F}_{q^2}(x)] = m_1 m_2$, and $(f_i, X^{q+1} - 1) = 1$ for $i \in \{1, 2\}$, then the number of

$\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ of the curve $\mathcal{X}$ satisfies

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1m_2((q+1, 2(d_1-s_1), 2(d_2-s_2)) + q - 3 - 2N_{f_1f_2}(\mathbb{F}_q^*)) \\ + 2m_2N_{f_1}(\mathbb{F}_q^*) + 2m_1N_{f_2}(\mathbb{F}_q^*).$$

In particular, for $s_1 = d_1$ and $s_2 = d_2$, we have

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq 2m_1m_2(q-1-N_{f_1f_2}(\mathbb{F}_q^*)) + 2m_2N_{f_1}(\mathbb{F}_q^*) + 2m_1N_{f_2}(\mathbb{F}_q^*).$$

Proof. We start by computing the genus of the function field $K(x, y_1, y_2)$. By Theorem 3.1.2, we have $g(K(x, y_1)) = (2m_1d_1 - 2(d_1-1) - (m_1, s_1) - (m_1, 2d_1 - s_1))/2$. Also, for the roots $\gamma_1, \ldots, \gamma_{d_1}$ of f_1 in K, we have the following ramification indices $e(P)$ in the extension $K(x, y_1)/K(x)$.

$$e(P) = \begin{cases} m_1/(m_1, s_1), & \text{if } P \text{ is over } P_0, \\ m_1, & \text{if } P \text{ is over } P_{\gamma_i} \text{ or } P_{\gamma_i^{-1}}, \\ m_1/(m_1, 2d_1 - s_1), & \text{if } P \text{ is over } P_\infty, \\ 1, & \text{otherwise.} \end{cases}$$

Now we show that the extension $K(x, y_1, y_2)/K(x, y_1)$ is a Kummer extension. Let $\alpha_1, \ldots, \alpha_{d_2} \in K$ be the roots of f_2. The principal divisor of the function $x^{-s_2}f_2(x)f_2^*(x)$ in $K(x)$ is given by

$$(x^{-s_2}f_2(x)f_2^*(x))_{K(x)} = \sum_{i=1}^{d_2}(P_{\alpha_i} + P_{\alpha_i^{-1}}) - s_2P_0 - (2d_2 - s_2)P_\infty,$$

and consequently

$$(x^{-s_2}f_2(x)f_2^*(x))_{K(x,y_1)} = \sum_{j=1}^{m_1}\sum_{i=1}^{d_2}(Q_{\alpha_i,j} + Q_{\alpha_i^{-1},j}) - \frac{s_2m_1}{(m_1, s_1)}\sum_{i=1}^{(m_1,s_1)} Q_{0,i} \\ - \frac{m_1(2d_2 - s_2)}{(m_1, 2d_1 - s_1)}\sum_{i=1}^{(m_1,2d_1-s_1)} Q_{\infty,i},$$

where $Q_{\alpha_i,j}$, $Q_{\alpha_i^{-1},j}$, $Q_{0,i}$, and $Q_{\infty,i}$ are the extensions in $K(x, y_1)$ of the places P_{α_i}, $P_{\alpha_i^{-1}}$, P_0, and P_∞ respectively. Thus the ramification indices in the extension $K(x, y_1, y_2)/K(x, y_1)$ are given by

$$e(R) = \begin{cases} \dfrac{m_2(m_1, s_1)}{\kappa}, & \text{if } R \text{ is over } Q_{0,i}, \\ \dfrac{m_2(m_1, 2d_1 - s_1)}{(m_1m_2, m_1(2d_2 - s_2), m_2(2d_1 - s_1))}, & \text{if } R \text{ is over } Q_{\infty,i}, \\ m_2, & \text{if } R \text{ is over } Q_{\alpha_i,j} \text{ or } Q_{\alpha_i^{-1},j}, \\ 1, & \text{otherwise.} \end{cases}$$

We conclude that the equations (3.11) define an absolutely irreducible curve. Its genus follows from the Riemann-Hurwitz formula applied to $K(x, y_1, y_2)/K(x, y_1)$.

Next, we provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points. From [50, Theorem 4], it follows that:

- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_1f_1^*f_2f_2^*(\alpha) \neq 0$, the curve $\mathcal{X}$ has m_1m_2 points with coordinate $x = \alpha$ if and only if $\frac{f_i(\alpha)f_i^*(\alpha)}{\alpha^{s_i}}$ is a m_i-th power in $\mathbb{F}_{q^2}^*$ for $i \in \{1, 2\}$,
- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_1f_1^*(\alpha) = 0$, the curve $\mathcal{X}$ has m_2 points with coordinate $x = \alpha$ if and only if $\frac{f_2(\alpha)f_2^*(\alpha)}{\alpha^{s_2}}$ is a m_2-th power in $\mathbb{F}_{q^2}^*$,
- for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_2f_2^*(\alpha) = 0$, the curve $\mathcal{X}$ has m_1 points with coordinate $x = \alpha$ if and only if $\frac{f_1(\alpha)f_1^*(\alpha)}{\alpha^{s_1}}$ is a m_1-th power in $\mathbb{F}_{q^2}^*$.

From the proof of Theorem 3.1.2, for $i \in \{1, 2\}$, we have

$$\left(\frac{f_i(\alpha)f_i^*(\alpha)}{\alpha^{s_i}}\right)^{\frac{q^2-1}{m_i}} = 1 \quad \Leftrightarrow \quad \alpha \text{ is a root of } h_{i,1}h_{i,2},$$

where

$$h_{i,1}(X) = (f_i(X)f_i^*(X))^{q-1} - X^{s_i(q-1)}$$

and

$$h_{i,2}(X) = \sum_{j=0}^{\frac{q+1}{m_i}-1} (f_i(X)f_i^*(X))^{(q-1)j} X^{s_i(q-1)\left(\frac{q+1}{m_i}-1-j\right)}.$$

From the proof of Theorem 3.1.2, we also have that if $\beta \in \mathbb{F}_{q^2}$ satisfies $\beta^{(q+1,2(d_1-s_1),2(d_2-s_2))} = 1$, then $h_{i,1}(\beta) = 0$. Further, for $i \in \{1, 2\}$, if $\beta \in \mathbb{F}_q^*$ and $f_i(\beta)f_i^*(\beta) \neq 0$, then $h_{i,1}(\beta) = 0$. Hence,

$$\begin{aligned}\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1m_2((q+1, 2(d_1-s_1), 2(d_2-s_2)) + q - 3 - 2N_{f_1f_2}(\mathbb{F}_q^*))\\ + 2m_2N_{f_1}(\mathbb{F}_q^*) + 2m_1N_{f_2}(\mathbb{F}_q^*).\end{aligned}$$

□

Example 3.2.2. *For polynomials $f_1, f_2 \in \mathbb{F}_q[X]$ satisfying the conditions of Theorem 3.2.1 and the curve $\mathcal{X}$ as defined in (3.11), we have the following table.*

New entry

q	m_1	m_2	s_1	s_2	f_1	f_2	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
19	2	4	4	4	X^4+2	X^4+7	33	1280	1248

Also, for a self-reciprocal polynomial $f_1 \in \mathbb{F}_q[X]$, we have the following improvements in the manYPoints table [60].

New entry

q	m_1	m_2	s_1	s_2	f_1	f_2	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
11	3	3	2	2	X^2+1	X^2+7	16	402	370
11	3	6	0	1	X^2+1	X^2+10	22	462	459
17	3	6	2	2	X^2+1	X^2+3	37	1224	1179

New record

q	m_1	m_2	s_1	s_2	f_1	f_2	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	*OLB*
5	3	6	2	5	X^2+1	X^2+4	22	174	168

Analogously to Theorem 3.2.1, we have the following result corresponding to another type of fibre product.

Theorem 3.2.3. *For $i \in \{1,2\}$, let $m_i \geq 2$ be a divisor of $q-1$, s_i be an integer such that $0 \leq s_i < m_i$, and f_i be a separable polynomial in $\mathbb{F}_q[X]$ of degree d_i satisfying $f_i(0) \neq 0$ and $(f_i, f_i^*) = (f_1 f_1^*, f_2 f_2^*) = 1$. Then the curve $\mathcal{X}$ defined by the affine equations*

$$\mathcal{X} : \begin{cases} Y_2^{m_2} = \frac{X^{s_2} f_2(X)}{f_2^*(X)} \\ Y_1^{m_1} = \frac{X^{s_1} f_1(X)}{f_1^*(X)} \end{cases} \tag{3.12}$$

has genus

$$g = m_1 m_2(d_1+d_2) - d_1 m_2 - d_2 m_1 + 1 - \kappa$$

where $\kappa = (m_1 m_2, s_1 m_2, s_2 m_1)$. Furthermore, if $\mathbb{F}_{q^2}$ is the full constant field of $\mathbb{F}_{q^2}(\mathcal{X})$, $[\mathbb{F}_{q^2}(\mathcal{X}), \mathbb{F}_{q^2}(x)] = m_1 m_2$, and $(f_i, X^{q+1}-1) = 1$ for $i \in \{1,2\}$, then the number of $\mathbb{F}_{q^2}$-rational points $\#\mathcal{X}(\mathbb{F}_{q^2})$ of the curve $\mathcal{X}$ satisfies

$$\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1 m_2(q+1).$$

Proof. We start by computing the genus of the function field $K(x, y_1, y_2)$. By Theorem 3.1.14, we have that $g(K(x,y_1)) = (m_1-1)d_1 + 1 - (m_1, s_1)$. Also, for $\gamma_1, \ldots, \gamma_{d_1} \in K$ the roots of f_1, we have the following ramification indices in the extension $K(x,y_1)/K(x)$

$$e(P) = \begin{cases} m_1/(m_1,s_1), & \text{if } P \text{ is over } P_0 \text{ or } P_\infty, \\ m_1, & \text{if } P \text{ is over } P_{\gamma_i} \text{ or } P_{\gamma_i^{-1}}, \\ 1, & \text{otherwise.} \end{cases}$$

Now we show that the extension $K(x,y_1,y_2)/K(x,y_1)$ is a Kummer extension and obtain its genus. Let $\alpha_1, \ldots, \alpha_{d_2} \in K$ be the roots of f_2. The principal divisor of the function $x^{s_2} f_2(x) f_2^*(x)^{-1}$ in $K(x)$ is given by

$$(x^{s_2} f_2(x) f_2^*(x)^{-1})_{K(x)} = s_2(P_0 - P_\infty) + \sum_{i=1}^{d_2} (P_{\alpha_i} - P_{\alpha_i^{-1}}),$$

and consequently

$$(x^{s_2} f_2(x) f_2^*(x)^{-1})_{K(x,y_1)} = \frac{s_2 m_1}{(m_1,s_1)} \sum_{i=1}^{(m_1,s_1)} (Q_{0,i} - Q_{\infty,i}) + \sum_{j=1}^{m_1} \sum_{i=1}^{d_2} (Q_{\alpha_i,j} - Q_{\alpha_i^{-1},j}),$$

where $Q_{\alpha_i,j}$, $Q_{\alpha_i^{-1},j}$, $Q_{0,i}$, and $Q_{\infty,i}$ are the extensions in $K(x,y_1)$ of the places P_{α_i}, $P_{\alpha_i^{-1}}$, P_0, and P_∞ respectively. Thus, the ramification indices in the extension $K(x,y_1,y_2)/K(x,y_1)$

are given by

$$e(R) = \begin{cases} m_2(m_1, s_1)/\kappa, & \text{if } R \text{ is over } Q_{0,i} \text{ or } Q_{\infty,i}, \\ m_2, & \text{if } R \text{ is over } Q_{\alpha_i,j} \text{ or } Q_{\alpha_i^{-1},j}, \\ 1, & \text{otherwise.} \end{cases}$$

We conclude that the equations (3.12) define an absolutely irreducible curve. Its genus follows from the Riemann-Hurwitz formula applied to $K(x, y_1, y_2)/K(x, y_1)$.

To provide a lower bound for the number of $\mathbb{F}_{q^2}$-rational points, note that, by [50, Theorem 4], we have that for $\alpha \in \mathbb{F}_{q^2}^*$ such that $f_1 f_1^* f_2 f_2^*(\alpha) \neq 0$, the curve $\mathcal{X}$ has $m_1 m_2$ points with coordinate $x = \alpha$ if and only if $\alpha^{s_i} f_i(\alpha)/f_i^*(\alpha)$ is a m_i-th power in $\mathbb{F}_{q^2}^*$ for $i = 1, 2$, and by Theorem 3.1.14,

$$\left(\frac{\alpha^{s_i} f_i(\alpha)}{f_i^*(\alpha)}\right)^{\frac{q^2-1}{m_i}} = 1 \quad \text{for} \quad i = 1, 2 \quad \Leftrightarrow \quad \alpha \text{ is a root of } (h_{1,1}h_{1,2}, h_{2,1}h_{2,2}),$$

where

$$h_{j,1}(X) = (X^{s_j} f_j(X))^{q+1} - f_j^*(X)^{q+1}$$

and

$$h_{j,2}(X) = \sum_{i=0}^{\frac{q-1}{m_j}-1} (X^{s_j} f_j(X))^{(q+1)i} f_j^*(X)^{(q+1)\left(\frac{q-1}{m_j}-1-i\right)}.$$

From the same Theorem 3.1.14, we have that if $\beta \in \mathbb{F}_{q^2}$ satisfies $\beta^{q+1} = 1$ then $h_{j,1}(\beta) = 0$ for $j = 1, 2$. Thus, $\#\mathcal{X}(\mathbb{F}_{q^2}) \geq m_1 m_2(q + 1)$. □

Example 3.2.4. *For polynomials $f_1, f_2 \in \mathbb{F}_q[X]$ satisfying the conditions of Theorem 3.2.3, and the curve $\mathcal{X}$ as defined in (3.12), we have the following tables.*

New entry

q	m_1	m_2	s_1	s_2	f_1	f_2	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
13	3	3	0	2	X^2+3X+3	$X+4$	16	558	464
13	4	4	1	1	$X+2$	$X+6$	21	568	556
17	4	4	1	1	$X+3$	$X+8$	21	808	794

New record

q	m_1	m_2	s_1	s_2	f_1	f_2	g	$\#\mathcal{X}(\mathbb{F}_{q^2})$	OLB
13	2	4	0	2	X^2+4	$X+5$	11	444	400
13	2	6	0	2	$X+3$	$X+6$	13	444	438

4 Weierstrass semigroup in Kummer extensions

Let K be the algebraic closure of the finite field $\mathbb{F}_q$. In this final chapter, we investigate Weierstrass semigroups of Kummer extensions with one place at infinity, that is, algebraic curves defined by the affine equation

$$\mathcal{X}: \quad Y^m = f(X) = \prod_{i=1}^{r}(X-\alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \text{and} \quad 1 \leq \lambda_i < m, \tag{4.1}$$

where $r \geq 2$ and $m \geq 2$ are integers such that $\operatorname{Char}(\mathbb{F}_q) \nmid m$, $\alpha_1, \ldots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $(m, \lambda_0) = 1$.

Abdón, Borges, and Quoos [1] provided an arithmetical criterion to determine if a positive integer is an element of the gap set of $H(Q)$, where $Q \in \mathcal{P}_{K(\mathcal{X})}$ lies over a totally ramified place in the extension $K(\mathcal{X})/K(x)$. As a consequence, they explicitly described the semigroup $H(Q)$ when $f(X)$ is a separable polynomial, that is, when $\lambda_1 = \lambda_2 = \cdots = \lambda_r = 1$. This description was generalized by Castellanos, Masuda, and Quoos in [12], where they study the curve $\mathcal{X}$ given in (4.1) for the case $\lambda_1 = \lambda_2 = \cdots = \lambda_r$.

The Weierstrass semigroup $H(Q_\infty)$ at the only place at infinity $Q_\infty \in \mathcal{P}_{K(\mathcal{X})}$ of $\mathcal{X}$ was explicitly described in the following particular cases:

i) For $\lambda_1 = \lambda_2 = \cdots = \lambda_r$, see [12, Theorem 3.2].

ii) For any λ_1 and $\lambda_2 = \lambda_3 = \cdots = \lambda_r = 1$, see [58, Remark 2.8].

This chapter aims to explicitly describe the Weierstrass semigroup $H(Q_\infty)$ in the general case, that is, we determine the Weierstrass semigroup at the only place at infinity Q_∞ of the curve $\mathcal{X}$ given in (4.1). Moreover, we provide a system of generators for the semigroup $H(Q_\infty)$, and as a consequence, we provide an explicit description of the gap set $G(Q_\infty)$ and generalize the closed formula for the Geil-Matsumoto bound given by Bras-Amorós and Vico-Oton in Theorem 1.2.14. Furthermore, we study the Frobenius number and the multiplicity of the semigroup $H(Q_\infty)$ establishing a relationship between them, and provide sufficient conditions for the semigroup $H(Q_\infty)$ to be symmetric. Finally, we characterize certain $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$.

4.1 The semigroup $H(Q_\infty)$

Consider the algebraic curve

$$\mathcal{X}: \quad Y^m = \prod_{i=1}^{r}(X-\alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \text{and} \quad 1 \leq \lambda_i < m,$$

where $m \geq 2$ and $r \geq 2$ are positive integers such that $\mathrm{Char}(\mathbb{F}_q) \nmid m$, $\alpha_1, \ldots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $(m, \lambda_0) = 1$. From Proposition 1.2.8 and the Riemann-Hurwitz formula, we obtain that the genus of the curve $\mathcal{X}$ is given by

$$g(\mathcal{X}) = \frac{(m-1)(r-1) + r - \sum_{i=1}^{r}(m, \lambda_i)}{2}. \tag{4.2}$$

In this section, as one of our main results, we provide an explicit description of the Weierstrass semigroup $H(Q_\infty)$ at the only place at infinity Q_∞ of $\mathcal{X}$. We start by recalling the property described in [29, p. 94], which states that for m and λ positive integers,

$$\sum_{i=1}^{\lambda-1}\left\lfloor \frac{im}{\lambda} \right\rfloor = \frac{(m-1)(\lambda-1) + (m,\lambda) - 1}{2}. \tag{4.3}$$

To prove the main result of this chapter, we need the following technical lemma.

Lemma 4.1.1. *Let $r, m, \lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_r$ be positive integers such that $\lambda_0 = \sum_{i=1}^{r} \lambda_i$ and $r < \lambda_0$. For $k \in \{r, \ldots, \lambda_0 - 1\}$, we define*

$$\eta_k := \max\left\{\rho_{s_1,\ldots,s_r} : \sum_{i=1}^{r} s_i = k,\ 1 \leq s_i \leq \lambda_i\right\}, \text{ where } \rho_{s_1,\ldots,s_r} := \min_{1\leq i\leq r}\left\lfloor \frac{s_i m}{\lambda_i}\right\rfloor.$$

Then the sequence $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0-1}$ is characterized by the following equality of multisets

$$\left\{\!\!\left\{\eta_k : r \leq k \leq \lambda_0 - 1\right\}\!\!\right\} = \left\{\!\!\left\{\left\lfloor \frac{s_i m}{\lambda_i}\right\rfloor : 1 \leq s_i < \lambda_i,\ 1 \leq i \leq r\right\}\!\!\right\}. \tag{4.4}$$

In particular, we have

$$\sum_{k=r}^{\lambda_0-1} \eta_k = \frac{(m-1)(\lambda_0 - r) - r + \sum_{i=1}^{r}(m,\lambda_i)}{2}.$$

Proof. First of all, note that, from the definition of η_k, we have that $\eta_k < m$ for each k. Furthermore, if $\eta_k = \rho_{u_1,\ldots,u_r} = \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor$ for some j, where $\sum_{i=1}^{r} u_i = k$ and $r \leq k \leq \lambda_0 - 2$, then $u_j < \lambda_j$ and

$$\eta_k = \rho_{u_1,\ldots,u_r} \leq \rho_{u_1,\ldots,u_j+1,\ldots,u_r} \leq \eta_{k+1}.$$

This proves that $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0-1} < m$ is a non-decreasing sequence. Let $S_1 := \{\!\{\eta_k : r \leq k \leq \lambda_0 - 1\}\!\}$ and $S_2 := \{\!\{\lfloor s_i m/\lambda_i \rfloor : 1 \leq s_i < \lambda_i,\ 1 \leq i \leq r\}\!\}$. Now we are going to prove that $S_1 = S_2$. From the definition of η_k, we have that $S_1^* \subseteq S_2^*$. Furthermore, since the multisets S_1 and S_2 have the same cardinality, to prove that $S_1 = S_2$ it is sufficient to show that $m_{S_1}(\eta_k) \leq m_{S_2}(\eta_k)$ for each k, that is, if $m_{S_1}(\eta_k) = n \geq 1$ then there exist distinct elements $j_1, j_2, \ldots, j_n \in \{1, \ldots, r\}$ and elements $s_{j_1}, s_{j_2}, \ldots, s_{j_n}$ with $1 \leq s_{j_i} \leq \lambda_{j_i} - 1$ such that

$$\eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor = \cdots = \left\lfloor \frac{s_{j_n} m}{\lambda_{j_n}} \right\rfloor.$$

If $n = 1$, there is nothing to prove, so we can assume that $n > 1$. Without loss of generality, suppose that

$$\eta_{k-1} < \eta_k = \eta_{k+1} = \cdots = \eta_{k+n-1}, \tag{4.5}$$

where $\eta_{k-1} := 0$ if $k = r$. From the inclusion $S_1^* \subseteq S_2^*$, there exist $j_1 \in \{1, \ldots, r\}$ and $s_{j_1} \in \{1, \ldots, \lambda_{j_1} - 1\}$ such that $\eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor$. Now, for each $i \in \{1, \ldots, r\}$ we define the set

$$\Gamma_i := \left\{ s \in \mathbb{N} : \eta_k \leq \left\lfloor \frac{sm}{\lambda_i} \right\rfloor \text{ and } 1 \leq s \leq \lambda_i \right\}.$$

Next, we prove that $\Gamma_i \neq \emptyset$ for each i. Since $s_{j_1} < \lambda_{j_1}$, for $i \neq j_1$ we have that

$$\left\lfloor \frac{s_{j_1} \lambda_i}{\lambda_{j_1}} \right\rfloor + 1 \leq \lambda_i \quad \text{and} \quad \eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \left(\frac{s_{j_1} \lambda_i}{\lambda_{j_1}} \right) \frac{m}{\lambda_i} \right\rfloor \leq \left\lfloor \left(\left\lfloor \frac{s_{j_1} \lambda_i}{\lambda_{j_1}} \right\rfloor + 1 \right) \frac{m}{\lambda_i} \right\rfloor,$$

which implies that $\left\lfloor \frac{s_{j_1} \lambda_i}{\lambda_{j_1}} \right\rfloor + 1 \in \Gamma_i$ for $i \neq j_1$ and $s_{j_1} \in \Gamma_{j_1}$. Let t_i be the smallest element of Γ_i. From definition of the set Γ_{j_1}, we have that $t_{j_1} \leq s_{j_1}$. If $t_{j_1} < s_{j_1}$ then

$$1 < \frac{m}{\lambda_{j_1}} \leq \frac{m}{\lambda_{j_1}} + \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor - \eta_k \leq \frac{m}{\lambda_{j_1}} + \left\lfloor \frac{(s_{j_1} - 1) m}{\lambda_{j_1}} \right\rfloor - \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor \leq \frac{s_{j_1} m}{\lambda_{j_1}} - \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor,$$

a contradiction, therefore $t_{j_1} = s_{j_1}$. Also, from definition of the sets Γ_i, we have that

$$\left\lfloor \frac{(t_i - 1) m}{\lambda_i} \right\rfloor < \eta_k = \rho_{t_1, \ldots, t_r} \text{ for } i = 1, \ldots, r.$$

Note that $k = \sum_{i=1}^r t_i$. In fact, let $k' := \sum_{i=1}^r t_i$. By definition of $\eta_{k'}$, we have that $\eta_k = \rho_{t_1, \ldots, t_r} \leq \eta_{k'}$, and from (4.5) we deduce that $k \leq k'$. On the other hand, suppose that $(u_1, \ldots, u_r)$ is an r-tuple such that $\eta_k = \rho_{u_1, \ldots, u_r}$, $\sum_{i=1}^r u_i = k$, and $1 \leq u_i \leq \lambda_i$. If there exists $j \in \{1, \ldots, r\}$ such that $u_j < t_j$, then

$$\eta_k = \rho_{u_1, \ldots, u_r} = \min_{1 \leq i \leq r} \left\lfloor \frac{u_i m}{\lambda_i} \right\rfloor \leq \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor \leq \left\lfloor \frac{(t_j - 1) m}{\lambda_j} \right\rfloor < \eta_k,$$

a contradiction. Therefore $t_i \leq u_i$ for each $i = 1, \ldots, r$, and this implies that $k' \leq k$. Thus, we conclude that $k = k' = \sum_{i=1}^r t_i$.

Now, we show that there exist distinct elements $j_2, \ldots, j_n \in \{1, \ldots, r\} \setminus \{j_1\}$ such that

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \cdots = \left\lfloor \frac{t_{j_n} m}{\lambda_{j_n}} \right\rfloor.$$

Suppose that $\eta_k < \left\lfloor \frac{t_j m}{\lambda_j} \right\rfloor$ for each $j \in \{1, \dots, r\} \setminus \{j_1\}$, then $\eta_k < \rho_{t_1,\dots,t_{j_1}+1,\dots,t_r} \leq \eta_{k+1}$ since $\sum_{i=1}^r t_i = k$. This is a contradiction to (4.5). Therefore there exists $j_2 \in \{1, \dots, r\} \setminus \{j_1\}$ satisfying

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{t_{j_2} m}{\lambda_{j_2}} \right\rfloor \quad \text{and} \quad t_{j_2} < \lambda_{j_2},$$

where the strict inequality $t_{j_2} < \lambda_{j_2}$ follows from the fact that $\eta_k < m$. If $\eta_k < \left\lfloor \frac{t_j m}{\lambda_j} \right\rfloor$ for each $j \in \{1, \dots, r\} \setminus \{j_1, j_2\}$, then $\eta_k < \rho_{t_1,\dots,t_{j_1}+1,\dots,t_{j_2}+1,\dots,t_r} \leq \eta_{k+2}$, again a contradiction to (4.5). Therefore there exists $j_3 \in \{1, \dots, r\} \setminus \{j_1, j_2\}$ such that

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{t_{j_2} m}{\lambda_{j_2}} \right\rfloor = \left\lfloor \frac{t_{j_3} m}{\lambda_{j_3}} \right\rfloor \quad \text{and} \quad t_{j_3} < \lambda_{j_3}.$$

By continuing this process, we obtain distinct elements $j_1, j_2, \dots, j_n$ such that

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \cdots = \left\lfloor \frac{t_{j_n} m}{\lambda_{j_n}} \right\rfloor \text{ and } t_{j_i} < \lambda_{j_i} \text{ for each } i = 1, \dots, n.$$

Finally, from (4.3), we conclude that

$$\begin{aligned} \sum_{k=r}^{\lambda_0 - 1} \eta_k = \sum_{i=1}^{r} \sum_{s=1}^{\lambda_i - 1} \left\lfloor \frac{sm}{\lambda_i} \right\rfloor &= \sum_{i=1}^{r} \frac{(m-1)(\lambda_i - 1) - 1 + (m, \lambda_i)}{2} \\ &= \frac{(m-1)(\lambda_0 - r) - r + \sum_{i=1}^r (m, \lambda_i)}{2}. \end{aligned}$$

□

Theorem 4.1.2. *Let $m \geq 2$ and $r \geq 2$ be integers such that $\mathrm{Char}(\mathbb{F}_q) \nmid m$. Let $\mathcal{X}$ be the algebraic curve defined by the affine equation*

$$\mathcal{X}: \quad Y^m = \prod_{i=1}^{r} (X - \alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \text{and } 1 \leq \lambda_i < m, \tag{4.6}$$

where $\alpha_1, \dots, \alpha_r$ are pairwise distinct elements of K. Define $\lambda_0 := \sum_{i=1}^r \lambda_i$, and suppose that $(m, \lambda_0) = 1$. Then the Weierstrass semigroup at the only place at infinity $Q_\infty \in \mathcal{P}_{K(\mathcal{X})}$ is given by the disjoint union

$$H(Q_\infty) = \langle m, \lambda_0 \rangle \uplus \biguplus_{k=r}^{\lambda_0 - 1} B_k,$$

where $B_k = \{mk - k'\lambda_0 : k' = 1, \dots, \eta_k\}$, and η_k are defined as in Lemma 4.1.1. In particular,

$$H(Q_\infty) = \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \dots, \lambda_0 - 1 \rangle. \tag{4.7}$$

Proof. Clearly the result holds if $r = \lambda_0$, therefore we can assume that $r < \lambda_0$. We start by computing some principal divisors in $K(\mathcal{X})$. Let $P_{\alpha_i} \in \mathcal{P}_{K(x)}$ be the place corresponding to $\alpha_i \in K$. For $k \in \{r, \ldots, \lambda_0 - 1\}$, let $s_1, \ldots, s_r$ be positive integers such that $1 \leq s_i \leq \lambda_i$ and $\sum_{i=1}^{r} s_i = k$. Then, from Propositions 1.2.6 and 1.2.8,

$$(x-\alpha_i)_{K(\mathcal{X})} = \frac{m}{(m,\lambda_i)} \sum_{\substack{Q|P_{\alpha_i}\\ Q\in\mathcal{P}_{K(\mathcal{X})}}} Q - mQ_\infty, \quad (y)_{K(\mathcal{X})} = \sum_{i=1}^{r} \frac{\lambda_i}{(m,\lambda_i)} \sum_{\substack{Q|P_{\alpha_i}\\ Q\in\mathcal{P}_{K(\mathcal{X})}}} Q - \lambda_0 Q_\infty,$$

and

$$\left(\frac{\prod_{i=1}^{r}(x-\alpha_i)^{s_i}}{y^{\rho_{s_1,\ldots,s_r}}}\right)_{K(\mathcal{X})} = \sum_{i=1}^{r} \frac{s_i m - \lambda_i \rho_{s_1,\ldots,s_r}}{(m,\lambda_i)} \sum_{\substack{Q|P_{\alpha_i}\\ Q\in\mathcal{P}_{K(\mathcal{X})}}} Q - (mk - \lambda_0 \rho_{s_1,\ldots,s_r})\, Q_\infty.$$

By the definition of η_k, we have that $0 < mk - \lambda_0\eta_k \in H(Q_\infty)$ for $r \leq k < \lambda_0$ and therefore

$$\langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k \subseteq H(Q_\infty). \tag{4.8}$$

Now, we prove that the union given in (4.8) is disjoint. For $k \in \{r, \ldots, \lambda_0 - 1\}$ and $k' \in \{1, \ldots, \eta_k\}$, an element of B_k can be written as

$$mk - k'\lambda_0 = m\lambda_0 - (\lambda_0 - k)m - k'\lambda_0.$$

Therefore, from Proposition 1.1.2, $B_k \cap \langle m, \lambda_0 \rangle = \emptyset$. On the other hand, we have that $B_{k_1} \cap B_{k_2} = \emptyset$ for $k_1 \neq k_2$. In fact, if $mk_1 - \lambda_0 k_1' = mk_2 - \lambda_0 k_2'$ for $r \leq k_1, k_2 < \lambda_0$, $1 \leq k_1' \leq \eta_{k_1}$, and $1 \leq k_2' \leq \eta_{k_2}$ then $m(k_1 - k_2) = \lambda_0(k_1' - k_2')$. Since $(m, \lambda_0) = 1$ and $2 - \lambda_0 \leq k_1 - k_2 \leq \lambda_0 - 2$, we conclude that $k_1 = k_2$.

Finally, we prove that equality holds in (4.8). Since

$$g(\mathcal{X}) = \frac{(m-1)(r-1) + r - \sum_{i=1}^{r}(m,\lambda_i)}{2} \quad \text{and} \quad g_{\langle m,\lambda_0\rangle} = \frac{(m-1)(\lambda_0-1)}{2},$$

from Lemma 4.1.1 we obtain that

$$\#\left(\dot{\bigcup_{k=r}^{\lambda_0-1}} B_k\right) = \sum_{k=r}^{\lambda_0-1} \eta_k = \frac{(m-1)(\lambda_0 - r) - r + \sum_{i=1}^{r}(m,\lambda_i)}{2} = \#\left(H(Q_\infty) \setminus \langle m, \lambda_0\rangle\right)$$

and the result follows. □

In general, we have that a minimal system of generators of a numerical semigroup H has cardinality at most the multiplicity of the semigroup, that is, $e_H \leq m_H$, see [55, Proposition 2.10]. Since $m \in H(Q_\infty)$, $e_{H(Q_\infty)} \leq m_{H(Q_\infty)} \leq m$. However, in general, it is difficult to obtain a minimal system of generators to $H(Q_\infty)$ from the system of generators given in (4.7).

For example, for the curve $Y^5 = X(X-1)^2$ defined over $\mathbb{F}_q$ with $5 \nmid q$, the system of generators for the semigroup $H(Q_\infty)$ provided by Theorem 4.1.2 is given by $H(Q_\infty) = \langle 3, 4, 5\rangle$ and therefore is a minimal system of generators. However, this does not happen in general. In fact, if $\eta_k = \eta_{k+1}$ for some k then we can remove the element $m(k+1) - \lambda_0\eta_{k+1}$ of the system of generators given in (4.7) since $m(k+1) - \lambda_0\eta_{k+1} = mk - \lambda_0\eta_k + m$. More generally, define $\lambda := \max_{1\leq i\leq r}\lambda_i$. If $\lambda = 1$ then $H(Q_\infty) = \langle m, \lambda_0\rangle$ and $e_{H(Q_\infty)} = 2$. If $\lambda > 1$, then for $i \in \{\lfloor m/\lambda\rfloor, \dots, m - \lceil m/\lambda\rceil\}$ define $k_i := 0$ if there is no $k \in \{r, \dots, \lambda_0 - 1\}$ such that $\eta_k = i$, and $k_i := \min\{k : r \leq k < \lambda_0, \eta_k = i\}$ otherwise. Thus, for each i such that $k_i \neq 0$ and k such that $\eta_k = i$, we can write $mk - \lambda_0\eta_k = mk_i - \lambda_0\eta_{k_i} + m(k - k_i)$. Therefore, by removing the element $mk - \lambda_0\eta_k$ from the system of generators given in (4.7) we obtain that

$$H(Q_\infty) = \left\langle m, \lambda_0, mk_i - \lambda_0\eta_{k_i} : i = \left\lfloor\frac{m}{\lambda}\right\rfloor, \dots, m - \left\lceil\frac{m}{\lambda}\right\rceil \text{ and } k_i \neq 0\right\rangle$$

and $e_{H(Q_\infty)} \leq m - \left\lceil\frac{m}{\lambda}\right\rceil - \left\lfloor\frac{m}{\lambda}\right\rfloor + 3 \leq m$.

Example 4.1.3 (Plane model of the *GGS* curve)**.** *The GGS curve is the first generalization of the GK curve, which is the first example of a maximal curve not covered by the Hermitian curve, see [20]. The GGS curve is an $\mathbb{F}_{q^{2n}}$-maximal curve for $n \geq 3$ an odd integer, and it is described by the following plane model:*

$$Y^{q^n+1} = (X^q + X)h(X)^{q+1}, \qquad \textit{where } h(X) = \sum_{i=0}^{q}(-1)^{i+1}X^{i(q-1)}.$$

This curve only has one place at infinity Q_∞. In order to calculate the Weierstrass semigroup $H(Q_\infty)$, note that $h(X)$ is a separable polynomial of degree $q(q-1)$. Using our standard notation as in Theorem 4.1.2, we have that $m = q^n + 1$, $r = q^2$, $\lambda_0 = q^3$, $\lambda_1 = \cdots = \lambda_q = 1$, and $\lambda_{q+1} = \cdots = \lambda_{q^2} = q + 1$. From the characterization of the multiset $S = \{\!\{\eta_k : r \leq k \leq \lambda_0 - 1\}\!\}$ given in Lemma 4.1.1, we have that

$$S^* = \left\{\frac{(\beta+1)(q^n+1)}{q+1} : 0 \leq \beta \leq q-1\right\}.$$

Furthermore, since $\lambda_1 = \cdots = \lambda_q = 1$ and $\lambda_{q+1} = \cdots = \lambda_{q^2} = q+1$, we have $m_S(a) = q^2 - q$ for each $a \in S^*$. Thus, since $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0 - 1}$ is a non-decreasing sequence, we obtain that

$$\begin{array}{ccccccccc}
\eta_r & = & \eta_{r+1} & = & \dots & = & \eta_{r+q^2-q-1} & = & \frac{q^n+1}{q+1} \\
\eta_{r+q^2-q} & = & \eta_{r+q^2-q+1} & = & \dots & = & \eta_{r+2(q^2-q)-1} & = & \frac{2(q^n+1)}{q+1} \\
 & & & & \vdots & & & & \\
\eta_{r+\beta(q^2-q)} & = & \eta_{r+\beta(q^2-q)+1} & = & \dots & = & \eta_{r+(\beta+1)(q^2-q)-1} & = & \frac{(\beta+1)(q^n+1)}{q+1} \\
 & & & & \vdots & & & & \\
\eta_{r+(q-1)(q^2-q)} & = & \eta_{r+(q-1)(q^2-q)+1} & = & \dots & = & \eta_{r+q(q^2-q)-1} & = & \frac{q(q^n+1)}{q+1}.
\end{array}$$

Therefore,

$$\eta_{r+\beta(q^2-q)+i} = \frac{(\beta+1)(q^n+1)}{q+1} \quad \textit{for } 0 \leq \beta \leq q-1 \textit{ and } 0 \leq i \leq q^2 - q - 1.$$

Moreover, since

$$m(r+\beta(q^2-q))-\lambda_0\eta_{r+\beta(q^2-q)}=(q-\beta)\frac{q(q^n+1)}{q+1}\ \textit{for } 0\leq\beta\leq q-1,$$

it follows from Theorem 4.1.2 that

$$H(Q_\infty)=\left\langle q^n+1, q^3, \frac{q(q^n+1)}{q+1}\right\rangle.$$

As expected, this description of $H(Q_\infty)$ matches the result given in [31, Corollary 3.5].

Let $n\geq 3$ be an odd integer, m be a divisor of q^n+1, and d be a divisor of $q+1$ such that $(m, d(q-1))=1$. From Theorem 2.1.1, the curve $\mathcal{Y}_{d,1,m}$ given by the affine equation

$$\mathcal{Y}_{d,1,m}:\quad Y^m=X^d(X^d-1)\left(\frac{X^{d(q-1)}-1}{X^d-1}\right)^{q+1}$$

is a subcover of the BM curve and has only one place at infinity Q_∞. In the following result, using Theorem 4.1.2, we compute the Weierstrass semigroup $H(Q_\infty)$.

Proposition 4.1.4. *Let $n\geq 3$ be an odd integer, m be a divisor of q^n+1, and d be a divisor of $q+1$ such that $(m,d(q-1))=1$. Consider the curve*

$$\mathcal{Y}_{d,1,m}:\quad Y^m=X^d(X^d-1)\left(\frac{X^{d(q-1)}-1}{X^d-1}\right)^{q+1}.$$

Then the Weierstrass semigroup at the only place at infinity Q_∞ is given by

$$H(Q_\infty)=\left\langle m, \lambda_0, mk_\beta-\lambda_0\left\lfloor\frac{(\beta+1)m}{q+1}\right\rfloor : \beta=0,\dots,q-1\right\rangle,$$

where $\lambda_0=dq(q-1)$ and $k_\beta=d(q-1)(\beta+1)+1+\left\lfloor\frac{\beta d}{q+1}\right\rfloor-\beta d$.

Proof. Using our standard notation, we have that $r=d(q-1)+1$, $\lambda_0=dq(q-1)$, $\lambda_1=d$, $\lambda_2=\cdots=\lambda_{d+1}=1$ and $\lambda_{d+2}=\cdots=\lambda_{d(q-1)+1}=q+1$. From the characterization of $S=\{\!\{\eta_k : r\leq k\leq\lambda_0-1\}\!\}$ given in Lemma 4.1.1, we obtain that

$$S^*=\left\{\left\lfloor\frac{(\beta+1)m}{q+1}\right\rfloor : 0\leq\beta\leq q-1\right\}.$$

Now, define $\delta_\beta:=\left\lceil\frac{(\beta+1)d}{q+1}\right\rceil-\left\lfloor\frac{(\beta+1)d}{q+1}\right\rfloor$ for $1\leq\beta\leq q-1$. Since $\lambda_1=d$, $\lambda_2=\cdots=\lambda_{d+1}=1$, and $\lambda_{d+2}=\cdots=\lambda_{d(q-1)+1}=q+1$, we have

$$m_S\left(\left\lfloor\frac{(\beta+1)m}{q+1}\right\rfloor\right)=\begin{cases} d(q-2), & \text{if } \delta_\beta=1,\\ d(q-2)+1, & \text{if } \delta_\beta=0,\end{cases}$$

or, equivalently,

$$m_S\left(\left\lfloor\frac{(\beta+1)m}{q+1}\right\rfloor\right)=d(q-2)+1-\delta_\beta. \tag{4.9}$$

In order to calculate the semigroup $H(Q_\infty)$, let $k_{\beta,i} := r + \beta(d(q-2)+1) - \sum_{j=0}^{\beta-1}\delta_j + i$ for $0 \leq \beta \leq q-1$ and $0 \leq i \leq d(q-2) - \delta_\beta$. From (4.9) and since $\eta_r \leq \eta_{r-1} \leq \cdots \leq \eta_{\lambda_0-1}$ is a non-decreasing sequence, we obtain that

$$\begin{array}{ccccccccc}
\eta_r & = & \eta_{r+1} & = & \dots & = & \eta_{r+d(q-2)-\delta_0} & = & \left\lfloor \frac{m}{q+1} \right\rfloor \\
\eta_{r+d(q-2)+1-\delta_0} & = & \eta_{r+d(q-2)+2-\delta_0} & = & \dots & = & \eta_{r+2(d(q-2)+1)-1-\delta_0-\delta_1} & = & \left\lfloor \frac{2m}{q+1} \right\rfloor \\
 & & & & \vdots & & & & \\
\eta_{k_{\beta,0}} & = & \eta_{k_{\beta,1}} & = & \dots & = & \eta_{k_{\beta,d(q-2)-\delta_\beta}} & = & \left\lfloor \frac{(\beta+1)m}{q+1} \right\rfloor \\
 & & & & \vdots & & & & \\
\eta_{k_{q-1,0}} & = & \eta_{k_{q-1,1}} & = & \dots & = & \eta_{k_{q-1,d(q-2)-\delta_{q-1}}} & = & \left\lfloor \frac{qm}{q+1} \right\rfloor .
\end{array}$$

Therefore $\eta_{k_{\beta,i}} = \left\lfloor \frac{(\beta+1)m}{q+1} \right\rfloor$ for $0 \leq \beta \leq q-1$ and $0 \leq i \leq d(q-2) - \delta_\beta$. From Theorem 4.1.2, we conclude that

$$H(Q_\infty) = \left\langle m, \lambda_0, mk_{\beta,0} - \lambda_0 \left\lfloor \frac{(\beta+1)m}{q+1} \right\rfloor : \beta = 0, \dots, q-1 \right\rangle.$$

Now the proposition follows from the fact that $\beta - \sum_{j=0}^{\beta-1}\delta_j = \left\lfloor \frac{\beta d}{q+1} \right\rfloor$ for $0 \leq \beta \leq q-1$. □

Henceforth, to simplify the notation, we define

$$\eta_s := \begin{cases} 0, & \text{if } 0 \leq s < r, \\ m-1, & \text{if } \lambda_0 \leq s, \end{cases} \quad \text{and} \quad \epsilon_k := mk - \lambda_0(\eta_k + 1) \text{ for } k \in \mathbb{N}_0. \tag{4.10}$$

Therefore we obtain that

$$H(Q_\infty) = \langle \epsilon_k + \lambda_0 : k = 1, r, \dots, \lambda_0 \rangle. \tag{4.11}$$

We complete this section by generalizing Theorem 1.2.14 given by Bras-Amorós and Vico-Oton. For this purpose, suppose that the curve $\mathcal{X}$ given in (4.6) is defined over $\mathbb{F}_q$. From (4.11) and Theorem 1.2.13, the Geil-Matsumoto bound associated to the semigroup $H(Q_\infty)$, denoted by $GM_q(H(Q_\infty))$, is given by

$$GM_q(H(Q_\infty)) = \#\left(H(Q_\infty) \setminus \bigcup_{k=1,r,\dots,\lambda_0} ((\epsilon_k + \lambda_0)q + H(Q_\infty)) \right) + 1. \tag{4.12}$$

Proposition 4.1.5. *Let $\mathcal{X}$ be the curve given in Theorem 4.1.2. If $\mathcal{X}$ is defined over $\mathbb{F}_q$ then*

$$\#\mathcal{X}(\mathbb{F}_q) \leq 1 + \sum_{k=0}^{\lambda_0-1} \max\left\{0, \min_{\ell\in\{1,r,\dots,\lambda_0\}} \left\{ \eta_k - q\eta_\ell - \eta_{k_\ell} - m\left\lfloor \frac{k-q\ell}{\lambda_0} \right\rfloor \right\}\right\},$$

where $k_\ell := (k - q\ell) \mod \lambda_0$.

Proof. From (4.12), we obtain that

$$GM_q(H(Q_\infty)) = \#\left\{ s \in H(Q_\infty) : \begin{array}{c} s - (\epsilon_1 + \lambda_0)q \notin H(Q_\infty) \\ s - (\epsilon_r + \lambda_0)q \notin H(Q_\infty) \\ \vdots \\ s - (\epsilon_{\lambda_0} + \lambda_0)q \notin H(Q_\infty) \end{array} \right\} + 1.$$

Therefore, to obtain a closed formula for $GM_q(H(Q_\infty))$, we need to count the elements $s \in H(Q_\infty)$ such that $s - (\epsilon_k + \lambda_0)q \notin H(Q_\infty)$ for each $k = 1, r, \ldots, \lambda_0$. From Theorem 4.1.2, the semigroup $H(Q_\infty)$ is given by the disjoint union $H(Q_\infty) = \langle m, \lambda_0 \rangle \uplus B$, where $B := \uplus_{k=r}^{\lambda_0 - 1} B_k$ and $B_k = \{mk - k'\lambda_0 : k' = 1, \ldots, \eta_k\}$. Thus, it is necessary to analyze two cases, when $s \in \langle m, \lambda_0 \rangle$ and when $s \in B$.

Our strategy will be to use the result given in [11, Lemma 2.1], which states that, for an integer i,

$$i \notin \langle m, \lambda_0 \rangle \quad \Leftrightarrow \quad m(ic \mod \lambda_0) > i,$$

where c is the inverse of m modulo λ_0.

Case A: $s \in \langle m, \lambda_0 \rangle$. Then $s = am + b\lambda_0$, where a and b are non-negative integers such that $a \leq \lambda_0 - 1$. For $\ell \in \{1, r, \ldots, \lambda_0\}$ and $k \in \{r, \ldots, \lambda_0 - 1\}$ we have that

$$\begin{aligned} s - (\epsilon_\ell + \lambda_0)q \notin \langle m, \lambda_0 \rangle &\Leftrightarrow (a - \ell q)m + (b + q\eta_\ell)\lambda_0 \notin \langle m, \lambda_0 \rangle \\ &\Leftrightarrow m[((a - \ell q)m + (b + q\eta_\ell)\lambda_0)c \mod \lambda_0] > (a - \ell q)m \\ &\quad + (b + q\eta_\ell)\lambda_0 \\ &\Leftrightarrow m((a - \ell q) \mod \lambda_0) > (a - \ell q)m + (b + q\eta_\ell)\lambda_0 \\ &\Leftrightarrow m((a - \ell q) \mod \lambda_0 - (a - \ell q)) > (b + q\eta_\ell)\lambda_0 \\ &\Leftrightarrow m\left\lceil \frac{\ell q - a}{\lambda_0} \right\rceil - q\eta_\ell > b \end{aligned}$$

and

$$\begin{aligned} s - (\epsilon_\ell + \lambda_0)q \in B_k &\Leftrightarrow am + b\lambda_0 - (m\ell - \lambda_0\eta_\ell)q = mk - k'\lambda_0 \text{ for some } 1 \leq k' \leq \eta_k \\ &\Leftrightarrow m(q\ell + k - a) = \lambda_0(b + q\eta_\ell + k') \\ &\Leftrightarrow k = (a - \ell q) \mod \lambda_0 \quad \text{and} \quad k' = m\left\lceil \frac{\ell q - a}{\lambda_0} \right\rceil - b - q\eta_\ell. \end{aligned}$$

Therefore $s - (\epsilon_\ell + \lambda_0)q \notin H(Q_\infty)$ if and only if $b < m\left\lceil \frac{\ell q - a}{\lambda_0} \right\rceil - q\eta_\ell - \eta_{a_\ell}$.

Case B: $s \in B$. Then $s = ma - b\lambda_0$, where a and b are positive integers such that $r \leq a < \lambda_0$ and $1 \leq b \leq \eta_a$. For $\ell \in \{1, r, \ldots, \lambda_0\}$ and $k \in \{r, \ldots, \lambda_0 - 1\}$ we have that

$$\begin{aligned} s - (\epsilon_\ell + \lambda_0)q \notin \langle m, \lambda_0 \rangle &\Leftrightarrow (a - \ell q)m + (q\eta_\ell - b)\lambda_0 \notin \langle m, \lambda_0 \rangle \\ &\Leftrightarrow m[((a - \ell q)m + (q\eta_\ell - b)\lambda_0)c \mod \lambda_0] > (a - \ell q)m \\ &\quad + (q\eta_\ell - b)\lambda_0 \\ &\Leftrightarrow m((a - \ell q) \mod \lambda_0) > (a - \ell q)m + (q\eta_\ell - b)\lambda_0 \\ &\Leftrightarrow m((a - \ell q) \mod \lambda_0 - (a - \ell q)) > (q\eta_\ell - b)\lambda_0 \\ &\Leftrightarrow q\eta_\ell - m\left\lceil \frac{\ell q - a}{\lambda_0} \right\rceil < b \end{aligned}$$

and

$$\begin{aligned}
s-(\epsilon_\ell+\lambda_0)q\in B_k &\Leftrightarrow ma-b\lambda_0-(m\ell-\lambda_0\eta_\ell)q=mk-k'\lambda_0 \text{ for some } 1\le k'\le\eta_k\\
&\Leftrightarrow m(a-q\ell-k)=\lambda_0(b-q\eta_\ell-k')\\
&\Leftrightarrow k=(a-q\ell) \mod \lambda_0 \quad\text{and}\quad k'=b-q\eta_\ell+m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil.
\end{aligned}$$

Therefore $s-(\epsilon_\ell+\lambda_0)q\notin H(Q_\infty)$ if and only if $q\eta_\ell-m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil+\eta_{a_\ell}<b$. Consequently,

$$\begin{aligned}
GM_q(H(Q_\infty)) &= 1+\sum_{a=0}^{\lambda_0-1}\max\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}\\
&\quad+\sum_{a=r}^{\lambda_0-1}\max\left\{0,\eta_a-\max\left\{0,\max_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{q\eta_\ell+\eta_{a_\ell}-m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil\right\}\right\}\right\}\\
&=1+\sum_{a=0}^{\lambda_0-1}\max\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}\\
&\quad+\sum_{a=r}^{\lambda_0-1}\max\left\{0,\eta_a+\min\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}\right\}\\
&=1+\sum_{a=0}^{r-1}\max\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}\\
&\quad+\sum_{a=r}^{\lambda_0-1}\max\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{\eta_a+m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}\\
&=1+\sum_{a=0}^{\lambda_0-1}\max\left\{0,\min_{\ell\in\{1,r,\dots,\lambda_0\}}\left\{\eta_a+m\left\lceil\frac{\ell q-a}{\lambda_0}\right\rceil-q\eta_\ell-\eta_{a_\ell}\right\}\right\}.
\end{aligned}$$

□

In particular, for $\lambda_1=\lambda_2=\cdots=\lambda_r=1$ we obtain that $\lambda_0=r$, $H(Q_\infty)=\langle m,r\rangle$, and from Proposition 4.1.5 we have

$$\begin{aligned}
GM_q(\langle m,r\rangle) &= 1+\sum_{k=0}^{r-1}\max\left\{0,\min_{\ell\in\{1,r\}}\left\{-q\eta_\ell-m\left\lfloor\frac{k-q\ell}{r}\right\rfloor\right\}\right\}\\
&=1+\sum_{k=0}^{r-1}\max\left\{0,\min\left\{q,\left\lceil\frac{q-k}{r}\right\rceil m\right\}\right\}\\
&=1+\sum_{k=0}^{r-1}\min\left\{q,\left\lceil\frac{q-k}{r}\right\rceil m\right\}.
\end{aligned}$$

As expected, for this case the closed formula coincides with the one described in Theorem 1.2.14.

4.2 The Frobenius number $F_{H(Q_\infty)}$ and the multiplicity $m_{H(Q_\infty)}$

With the explicit description of the Weierstrass semigroup $H(Q_\infty)$ given in Theorem 4.1.2, in this section we study the Frobenius number $F_{H(Q_\infty)}$, the multiplicity $m_{H(Q_\infty)}$, and the relationship between them. We start by noticing that not all the elements $\epsilon_{r-1}, \dots, \epsilon_{\lambda_0-1}$ defined in (4.10) are necessarily positive, however the following result states that the largest of them is equal to the Frobenius number $F_{H(Q_\infty)}$. Moreover, we explicitly describe the gap set $G(Q_\infty)$.

Proposition 4.2.1. *Using the same notation as in Theorem 4.1.2, we have that*

$$F_{H(Q_\infty)} = \max\{\epsilon_{r-1}, \dots, \epsilon_{\lambda_0-1}\}$$

and

$$G(Q_\infty) = \left\{ma - b\lambda_0 : 1 \le a \le \lambda_0 - 1,\, \eta_a + 1 \le b \le \left\lfloor \frac{am}{\lambda_0} \right\rfloor\right\}.$$

Proof. From Theorem 4.1.2, we have that

$$G(Q_\infty) = \mathbb{N} \setminus \left(\langle m, \lambda_0 \rangle \mathbin{\dot\cup} \dot{\bigcup_{k=r}^{\lambda_0-1}} B_k \right) = (\mathbb{N} \setminus \langle m, \lambda_0 \rangle) \setminus \left(\dot{\bigcup_{k=r}^{\lambda_0-1}} B_k \right),$$

where $B_k = \{m\lambda_0 - (\lambda_0 - k)m - k'\lambda_0 : 1 \le k' \le \eta_k\}$. Moreover, from Proposition 1.1.2 we know that the elements of $\mathbb{N} \setminus \langle m, \lambda_0 \rangle$ are of the form $m\lambda_0 - am - b\lambda_0$, where a and b are positive integers. Therefore,

$$G(Q_\infty) = \{m\lambda_0 - am - b\lambda_0 : \text{the pair } (a, b) \text{ is in } \Delta\} \cap \mathbb{N},$$

where $\Delta = \{(a, b) \in \mathbb{N}^2 : \eta_{\lambda_0-a} + 1 \le b\}$, and

$$F_{H(Q_\infty)} = \max_{(a,b)\in\Delta} \{m\lambda_0 - am - b\lambda_0\}.$$

By the definition of the set Δ, $\max_{(a,b)\in\Delta}\{m\lambda_0 - am - b\lambda_0\}$ is attained at an element in Δ of the form $(k, \eta_{\lambda_0-k} + 1)$ for some $k \in \{1, \dots, \lambda_0 - r + 1\}$, see Figure 1. Thus, $F_{H(Q_\infty)} = \max\{\epsilon_{r-1}, \dots, \epsilon_{\lambda_0-1}\}$. Moreover,

$$\begin{aligned} G(Q_\infty) &= \{m\lambda_0 - am - b\lambda_0 : \text{the pair } (a, b) \text{ is in } \Delta\} \cap \mathbb{N} \\ &= \{m(\lambda_0 - a) - b\lambda_0 : 1 \le a \le \lambda_0 - 1,\, \eta_{\lambda_0-a} + 1 \le b\} \cap \mathbb{N} \\ &= \left\{ma - b\lambda_0 : 1 \le a \le \lambda_0 - 1,\, \eta_a + 1 \le b \le \left\lfloor \frac{am}{\lambda_0} \right\rfloor\right\}. \end{aligned}$$

□

Now, we provide sufficient conditions to determine whether the semigroup $H(Q_\infty)$ is symmetric. In particular, by [34, Proposition 50], we give sufficient conditions for Q_∞ to be a Weierstrass place. For this, we need a remark and a lemma.

Remark 4.2.2. *Due to the characterization of the sequence $\eta_r \le \eta_{r+1} \le \dots \le \eta_{\lambda_0-1}$ given in Lemma 4.1.1, we can see that, for $s \in \mathbb{N}_0$, $\eta_s + \eta_{r+\lambda_0-1-s} = m$ or $\eta_s + \eta_{r+\lambda_0-1-s} = m - 1$.*

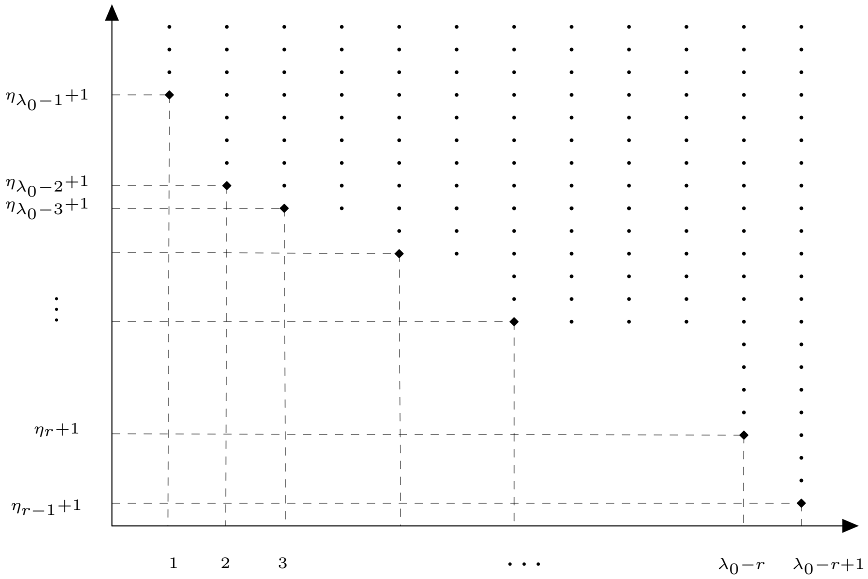

Figure 1 – Description of the set Δ

In fact, if $0 \leq s \leq r-1$ *or* $\lambda_0 \leq s$ *the assertion is clear. Let* $k \in \{r, \dots, \lambda_0 - 1\}$ *and* $n \in \mathbb{N}$ *be such that*

$$\eta_{k-1} < \eta_k = \eta_{k+1} = \cdots = \eta_{k+n-1} < \eta_{k+n}.$$

From Lemma 4.1.1, there exist exactly n *distinct elements* $j_1, \dots, j_n \in \{1, \dots, r\}$ *and positive integers* $s_{j_1}, \dots, s_{j_n}$ *such that* $1 \leq s_{j_i} < \lambda_{j_i}$ *and*

$$\eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{s_{j_2} m}{\lambda_{j_2}} \right\rfloor = \cdots = \left\lfloor \frac{s_{j_n} m}{\lambda_{j_n}} \right\rfloor.$$

Without loss of generality, we can assume that

$$\left\lceil \frac{s_{j_1} m}{\lambda_{j_1}} \right\rceil \leq \left\lceil \frac{s_{j_2} m}{\lambda_{j_2}} \right\rceil \leq \cdots \leq \left\lceil \frac{s_{j_n} m}{\lambda_{j_n}} \right\rceil$$

and therefore

$$\left\lfloor \frac{(\lambda_{j_n} - s_{j_n}) m}{\lambda_{j_n}} \right\rfloor \leq \left\lfloor \frac{(\lambda_{j_{n-1}} - s_{j_{n-1}}) m}{\lambda_{j_{n-1}}} \right\rfloor \leq \cdots \leq \left\lfloor \frac{(\lambda_{j_1} - s_{j_1}) m}{\lambda_{j_1}} \right\rfloor.$$

This leads to

$$\eta_{r+\lambda_0-1-(k+i)} = \left\lfloor \frac{(\lambda_{j_{i+1}} - s_{j_{i+1}}) m}{\lambda_{j_{i+1}}} \right\rfloor \text{ for } i = 0, \dots, n-1$$

and, consequently,

$$\eta_{k+i} + \eta_{r+\lambda_0-1-(k+i)} = \left\lfloor \frac{s_{j_{i+1}} m}{\lambda_{j_{i+1}}} \right\rfloor + \left\lfloor \frac{(\lambda_{j_{i+1}} - s_{j_{i+1}}) m}{\lambda_{j_{i+1}}} \right\rfloor = m - \left(\left\lceil \frac{s_{j_{i+1}} m}{\lambda_{j_{i+1}}} \right\rceil - \left\lfloor \frac{s_{j_{i+1}} m}{\lambda_{j_{i+1}}} \right\rfloor \right)$$

for $i = 0, \dots, n-1$*. In particular, if* $(m, \lambda_j) = 1$ *for each* j*, we obtain that* $\eta_s + \eta_{r+\lambda_0-1-s} = m - 1$ *for* $s \in \mathbb{N}_0$*, and if* λ_j *divides* m *for each* j*, we obtain that* $\eta_s + \eta_{r+\lambda_0-1-s} = m$ *for* $s = r, \dots, \lambda_0 - 1$*.*

Lemma 4.2.3. *For $k \in \mathbb{N}_0$, the following statements hold:*

i) If $\eta_k + \eta_{r+\lambda_0-1-k} = m$ then $\epsilon_k + \epsilon_{r+\lambda_0-1-k} = \epsilon_{r-1} - \lambda_0$ and $\epsilon_{r-1} > \epsilon_k$.

ii) If $\eta_k + \eta_{r+\lambda_0-1-k} = m - 1$ then $\epsilon_k + \epsilon_{r+\lambda_0-1-k} = \epsilon_{r-1}$, and $\epsilon_{r-1} > \epsilon_k$ if and only if $0 < \epsilon_{r+\lambda_0-1-k}$.

iii) $\epsilon_k < 0$ if and only if $\eta_k = \left\lfloor \frac{km}{\lambda_0} \right\rfloor$.

Proof. *i*) It is enough to note that

$$\begin{aligned}\epsilon_{r+\lambda_0-1-k} &= m(r+\lambda_0-1-k) - \lambda_0(\eta_{r+\lambda_0-1-k}+1)\\ &= m(r+\lambda_0-1-k) - \lambda_0\,(m-\eta_k+1)\\ &= m(r-1) - \lambda_0 - mk + \lambda_0\eta_k\\ &= \epsilon_{r-1} - \epsilon_k - \lambda_0.\end{aligned}$$

Therefore, $\epsilon_{r-1} - \epsilon_k = \epsilon_{r+\lambda_0-1-k} + \lambda_0 > 0$.

ii) Similar to item *i*).

iii) Since $mk = \lambda_0\eta_k + (mk - \lambda_0\eta_k)$ and $0 \leq mk - \lambda_0\eta_k$, we conclude that $\eta_k = \lfloor km/\lambda_0 \rfloor$ if and only if $mk - \lambda_0\eta_k < \lambda_0$. □

Theorem 4.2.4. *With the same notation as in Theorem 4.1.2, the following statements are equivalent:*

i) $F_{H(Q_\infty)} = \epsilon_{r-1}$ and $H(Q_\infty)$ is symmetric.

ii) λ_j divides m for each $j = 1, \ldots, r$.

Proof. Suppose that $H(Q_\infty)$ is symmetric and $F_{H(Q_\infty)} = \epsilon_{r-1}$. From (4.2) we obtain that

$$F_{H(Q_\infty)} = m(r-1) - \lambda_0 = m(r-1) - \sum_{j=1}^{r}(m, \lambda_j).$$

This implies that λ_j divides m for each $j = 1, \ldots, r$.

Conversely, assume that λ_j divides m for each $j = 1, \ldots, r$. From Remark 4.2.2 we have that $\eta_k + \eta_{r+\lambda_0-1-k} = m$ for $k = r, \ldots, \lambda_0 - 1$, and from item *i*) of Lemma 4.2.3, $\epsilon_{r-1} > \epsilon_k$ for $k = r, \ldots, \lambda_0 - 1$. Therefore, from Proposition 4.2.1, $F_{H(Q_\infty)} = \max\{\epsilon_{r-1}, \ldots, \epsilon_{\lambda_0-1}\} = \epsilon_{r-1}$ and

$$2g(\mathcal{X}) - 1 = m(r-1) - \sum_{i=j}^{r}(m, \lambda_j) = m(r-1) - \lambda_0 = \epsilon_{r-1} = F_{H(Q_\infty)}.$$

□

Example 4.2.5. *From Example 4.1.3, we know that the Weierstrass semigroup at the only place at infinity of the GGS curve is given by $H(Q_\infty) = \langle q^n+1, q^3, q(q^n+1)/(q+1)\rangle$. Therefore, we can determine if $H(Q_\infty)$ is symmetric and we can calculate the Frobenius number $F_{H(Q_\infty)}$. However, due to Theorem 4.2.4, it is possible to know this without computing the semigroup $H(Q_\infty)$ explicitly. In fact, since $q+1$ divides q^n+1, $H(Q_\infty)$ is symmetric and*

$$F_{H(Q_\infty)} = (q^n+1)(q^2-1) - q^3 = q^{n+2} - q^n - q^3 + q^2 - 1.$$

Next, we improve Proposition 4.2.1 to compute the Frobenius number $F_{H(Q_\infty)}$ and establish a relationship between $F_{H(Q_\infty)}$ and the multiplicity $m_{H(Q_\infty)}$.

Proposition 4.2.6. *Using the same notation as in Theorem 4.1.2, the following statements hold:*

i) $F_{H(Q_\infty)} = \epsilon_{r-1}$ *if and only if* $\eta_s < \lfloor sm/\lambda_0 \rfloor$ *for each* $s \in \{r, \dots, \lambda_0 - 1\}$ *such that* $\eta_s + \eta_{r+\lambda_0-1-s} = m-1$.

ii) $F_{H(Q_\infty)} = \max_{r-1\le k<\lambda_0} \left\{\epsilon_k : \eta_k = \left\lfloor \frac{(k+1-r)m}{\lambda_0} \right\rfloor\right\}$.

iii) If $(m, \lambda_j) = 1$ *for each* $j = 1, \dots, r$ *then* $m_{H(Q_\infty)} = \min\{m, m(r-1) - F_{H(Q_\infty)}\}$.

iv) If λ_j *divides* m *for each* $j = 1, \dots, r$ *then* $m_{H(Q_\infty)} = \min\{m, \lambda_0, \epsilon_{r-1} - \max_{r\le k<\lambda_0} \epsilon_k\}$.

Proof. *i)* It follows from Lemma 4.2.3 and the fact that $\eta_s \le \lfloor sm/\lambda_0 \rfloor$ for all $s \in \mathbb{N}_0$.

ii) It is enough to note that, from Lemma 4.2.3, we can rewrite the Frobenius number $F_{H(Q_\infty)}$ as

$$\begin{aligned}
F_{H(Q_\infty)} &= \max_{r\le k<\lambda_0} \{\epsilon_{r-1}, \epsilon_k : \epsilon_{r+\lambda_0-1-k} < 0,\ \eta_k + \eta_{r+\lambda_0-1-k} = m-1\} \\
&= \max_{r\le k<\lambda_0} \left\{\epsilon_{r-1}, \epsilon_k : \eta_{r+\lambda_0-1-k} = \left\lfloor \frac{(r+\lambda_0-1-k)m}{\lambda_0} \right\rfloor, \eta_k + \eta_{r+\lambda_0-1-k} = m-1\right\} \\
&= \max_{r\le k<\lambda_0} \left\{\epsilon_{r-1}, \epsilon_k : \eta_k = \left\lfloor \frac{(k+1-r)m}{\lambda_0} \right\rfloor\right\} \\
&= \max_{r-1\le k<\lambda_0} \left\{\epsilon_k : \eta_k = \left\lfloor \frac{(k+1-r)m}{\lambda_0} \right\rfloor\right\}.
\end{aligned}$$

iii) From (4.11) and Lemma 4.2.3, we obtain that

$$\begin{aligned}
m_{H(Q_\infty)} &= \min\left\{m, \lambda_0, \lambda_0 + \min_{r\le k<\lambda_0} \epsilon_k\right\} \\
&= \min\left\{m, \lambda_0, \lambda_0 + \min_{r\le k<\lambda_0} \{\epsilon_{r-1} - \epsilon_{r+\lambda_0-1-k}\}\right\} \\
&= \min\left\{m, \lambda_0, \lambda_0 + \epsilon_{r-1} - \max_{r\le k<\lambda_0} \epsilon_{r+\lambda_0-1-k}\right\} \\
&= \min\left\{m, \lambda_0, \lambda_0 + \epsilon_{r-1} - \max_{r\le k<\lambda_0} \epsilon_k\right\} \\
&= \min\left\{m, m(r-1) - F_{H(Q_\infty)}\right\}.
\end{aligned}$$

iv) Similar to the proof of item *iii*). □

Next, we observe that for the curve $\mathcal{X}$ defined in (4.6), the elements of the set $\{\epsilon_k + \lambda_0 : k = 0, \dots, \lambda_0 - 1\} \subseteq H(Q_\infty)$ form a complete set of representatives for the congruence classes of $\mathbb{Z}$ modulo λ_0 and

$$\sum_{k=0}^{\lambda_0-1} \left\lfloor \frac{\epsilon_k + \lambda_0}{\lambda_0} \right\rfloor = g(\mathcal{X}).$$

Therefore, from Proposition 1.1.4, the Apéry set of λ_0 in the Weierstrass semigroup $H(Q_\infty)$ is given by

$$\operatorname{Ap}(H(Q_\infty), \lambda_0) = \{\epsilon_k + \lambda_0 : k = 0, \dots, \lambda_0 - 1\}.$$

We use this description of the Apéry set $\operatorname{Ap}(H(Q_\infty), \lambda_0)$ to characterize the symmetric Weierstrass semigroups $H(Q_\infty)$ when $(m, \lambda_j) = 1$ for each $j = 1, \dots, r$.

Theorem 4.2.7. *Suppose that $(m, \lambda_j) = 1$ for $j = 1, \dots, r$. Then the followings statements are equivalent:*

i) $H(Q_\infty) = \langle m, r \rangle$.

ii) $\lambda_1 = \lambda_2 = \cdots = \lambda_r$.

If in addition $r < m$ then all these statements are equivalent to the following:

iii) $H(Q_\infty)$ *is symmetric.*

Proof. Clearly the result holds if $r = \lambda_0$. Suppose that $r < \lambda_0$.

i) $\Rightarrow$ *ii*) : We start by proving that r divides λ_0. In fact, since $\lambda_0, mr - \lambda_0 \in H(Q_\infty) = \langle m, r \rangle$, there exist $\alpha, \alpha', \tau, \tau' \in \mathbb{N}_0$, where $\tau, \tau' \leq m - 1$ and $\tau \neq 0$, such that $\lambda_0 = \alpha m + \tau r$ and $mr - \lambda_0 = \alpha' m + \tau' r$. Therefore $m(r - \alpha - \alpha') = r(\tau + \tau')$. Since $H(Q_\infty) = \langle m, r \rangle$, $(m, r) = 1$ and therefore m divides $\tau + \tau'$, where $1 \leq \tau + \tau' \leq 2m - 2$. This implies that $\tau + \tau' = m$ and $\alpha = -\alpha'$. It follows that $\alpha = \alpha' = 0$ and $\lambda_0 = \tau r$.

Now, let $\lambda := \max_{1 \leq i \leq r} \lambda_i$ and note that $\tau r = \lambda_0 = \sum_{i=1}^{r} \lambda_i \leq \lambda r$, therefore $\tau \leq \lambda$. In the following, we prove that $\tau = \lambda$, which implies that $\lambda_1 = \lambda_2 = \cdots = \lambda_r$.

For $\beta \in \{1, \dots, \tau - 1\}$ and $i \in \{0, \dots, r - 1\}$ we have that

$$\epsilon_{\beta r + i} + \lambda_0 = mr - (r - i)m - (\tau \eta_{r\beta + i} - m\beta) r \in H(Q_\infty) = \langle m, r \rangle.$$

Therefore, from Proposition 1.1.2, it follows that

$$\eta_{r\beta+i} \leq \left\lfloor \frac{\beta m}{\tau} \right\rfloor \text{ for } 1 \leq \beta \leq \tau - 1 \text{ and } 0 \leq i \leq r - 1. \tag{4.13}$$

For $\beta = 1$ in (4.13) we obtain that

$$\left\lfloor \frac{m}{\lambda} \right\rfloor = \eta_r \leq \eta_{r+i} \leq \left\lfloor \frac{m}{\tau} \right\rfloor \text{ for } 0 \leq i \leq r-1,$$

and for $\beta = \tau - 1$ and $i = r-1$ in (4.13),

$$m - \left\lceil \frac{m}{\lambda} \right\rceil = \left\lfloor \frac{(\lambda-1)m}{\lambda} \right\rfloor = \eta_{\lambda_0 - 1} = \eta_{r(\tau-1)+r-1} \leq \left\lfloor \frac{(\tau-1)m}{\tau} \right\rfloor = m - \left\lceil \frac{m}{\tau} \right\rceil.$$

Since $(m, \lambda) = (m, \tau) = 1$, then $\left\lfloor \frac{m}{\lambda} \right\rfloor = \left\lfloor \frac{m}{\tau} \right\rfloor$ and therefore $\eta_{r+i} = \left\lfloor \frac{m}{\lambda} \right\rfloor$ for $0 \leq i \leq r-1$. Thus, from the characterization of the sequence $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0-1}$ given in (4.4), we have that

$$\eta_r = \left\lfloor \frac{m}{\lambda_1} \right\rfloor = \left\lfloor \frac{m}{\lambda_2} \right\rfloor = \cdots = \left\lfloor \frac{m}{\lambda_r} \right\rfloor = \eta_{2r-1}$$

and therefore $\eta_{2r} = \left\lfloor \frac{2m}{\lambda} \right\rfloor$. Moreover, from Remark 4.2.2, $\eta_{\lambda_0-1-i} = m - 1 - \eta_{r+i} = \left\lfloor \frac{(\lambda-1)m}{\lambda} \right\rfloor$ for $0 \leq i \leq r-1$ and hence $\eta_{\lambda_0-r-1} = \left\lfloor \frac{(\lambda-2)m}{\lambda} \right\rfloor$.

For $\beta = 2$ in (4.13) we have that

$$\left\lfloor \frac{2m}{\lambda} \right\rfloor = \eta_{2r} \leq \eta_{2r+i} \leq \left\lfloor \frac{2m}{\tau} \right\rfloor \text{ for } 0 \leq i \leq r-1,$$

and for $\beta = \tau - 2$ and $i = r-1$ in (4.13),

$$m - \left\lceil \frac{2m}{\lambda} \right\rceil = \left\lfloor \frac{(\lambda-2)m}{\lambda} \right\rfloor = \eta_{\lambda_0-r-1} = \eta_{r(\tau-2)+r-1} \leq \left\lfloor \frac{(\tau-2)m}{\tau} \right\rfloor = m - \left\lceil \frac{2m}{\tau} \right\rceil.$$

Similarly to the previous case, we deduce that $\left\lfloor \frac{2m}{\lambda} \right\rfloor = \left\lfloor \frac{2m}{\tau} \right\rfloor$, $\eta_{2r+i} = \left\lfloor \frac{2m}{\lambda} \right\rfloor$ and $\eta_{\lambda_0-r-1-i} = \left\lfloor \frac{(\lambda-2)m}{\lambda} \right\rfloor$ for $0 \leq i \leq r-1$. This implies that $\eta_{3r} = \left\lfloor \frac{3m}{\lambda} \right\rfloor$ and $\eta_{\lambda_0-2r-1} = \left\lfloor \frac{(\lambda-3)m}{\lambda} \right\rfloor$.

By continuing this process, we obtain that

$$\eta_{r\beta+i} = \left\lfloor \frac{\beta m}{\lambda} \right\rfloor \text{ for } 1 \leq \beta \leq \tau - 1 \text{ and } 0 \leq i \leq r-1.$$

In particular, for $\beta = \tau - 1$ and $i = r-1$ we have that

$$\left\lfloor \frac{(\tau-1)m}{\lambda} \right\rfloor = \eta_{r(\tau-1)+r-1} = \eta_{r\tau-1} = \eta_{\lambda_0-1} = \left\lfloor \frac{(\lambda-1)m}{\lambda} \right\rfloor.$$

This implies that $\tau = \lambda$.

ii) $\Rightarrow$ *i)* : Suppose that $\lambda_1 = \lambda_2 = \cdots = \lambda_r$. Then $\lambda_0 = r\lambda_r$ and $\eta_{\beta r+i} = \left\lfloor \frac{\beta m}{\lambda_r} \right\rfloor$ for $1 \leq \beta \leq \lambda_r - 1$ and $0 \leq i \leq r-1$. On the other hand, from Theorem 4.1.2,

$$\begin{aligned} H(Q_\infty) &= \left\langle m, r\lambda_r, r\left(\beta m - \lambda_r \left\lfloor \frac{\beta m}{\lambda_r} \right\rfloor\right) : \beta = 1, \ldots, \lambda_r - 1 \right\rangle \\ &= \left\langle m, r\lambda_r, r\lambda_r \left\{ \frac{\beta m}{\lambda_r} \right\} : \beta = 1, \ldots, \lambda_r - 1 \right\rangle. \end{aligned}$$

Since $(m, \lambda_r) = 1$, there exists $\beta' \in \{1, \ldots, \lambda_r - 1\}$ such that $\left\{\frac{\beta' m}{\lambda_r}\right\} = \frac{1}{\lambda_r}$ and therefore $H(Q_\infty) = \langle m, r\rangle$.

Now, suppose that $r < m$.

$i) \Rightarrow iii)$: It is clear.

$iii) \Rightarrow i)$: We are going to prove that $(m, r) = 1$. We start by noting two important facts. First, note that

$$(\epsilon_k + \lambda_0) \equiv 0 \mod m \quad \text{if and only if} \quad 0 \leq k \leq r - 1. \tag{4.14}$$

Second, since $r < m$ and $(m, \lambda_j) = 1$ for each j, then $H(Q_\infty)$ is symmetric if and only if $m_{H(Q_\infty)} = r$. In fact, for this case we have that $g(\mathcal{X}) = (m-1)(r-1)/2$. Furthermore, from item $iii)$ of Proposition 4.2.6, $m_{H(Q_\infty)} = \min\{m, m(r-1) - F_{H(Q_\infty)}\}$. If $H(Q_\infty)$ is symmetric, then $F_{H(Q_\infty)} = 2g(\mathcal{X}) - 1 = m(r-1) - r$ and

$$m_{H(Q_\infty)} = \min\{m, m(r-1) - F_{H(Q_\infty)}\} = \min\{m, r\} = r.$$

Conversely, if $m_{H(Q_\infty)} = r$ then $m(r-1) - F_{H(Q_\infty)} = r$ and therefore $F_{H(Q_\infty)} = 2g(\mathcal{X}) - 1$. This implies that $H(Q_\infty)$ is symmetric.

Let σ be the permutation of the set $\{0, \ldots, \lambda_0 - 1\}$ such that

$$\text{Ap}(H(Q_\infty), \lambda_0) = \{0 = \epsilon_{\sigma(0)} + \lambda_0 < \epsilon_{\sigma(1)} + \lambda_0 < \cdots < \epsilon_{\sigma(\lambda_0 - 1)} + \lambda_0\}.$$

Since $(m, \lambda_j) = 1$ for $j = 1, \ldots, r$ and $H(Q_\infty)$ is symmetric, then $F_{H(Q_\infty)} = \epsilon_{\sigma(\lambda_0 - 1)} = m(r-1) - r$. Thus, from Proposition 1.1.5, we have that

$$\epsilon_{\sigma(i)} + \epsilon_{\sigma(\lambda_0 - 1 - i)} = m(r-1) - \lambda_0 - r \quad \text{for } i = 0, \ldots, \lambda_0 - 1. \tag{4.15}$$

On the other hand, from Proposition 4.2.3, we know that

$$\epsilon_{\sigma(i)} + \epsilon_{r + \lambda_0 - 1 - \sigma(i)} = m(r-1) - \lambda_0 \quad \text{for } i = 0, \ldots, \lambda_0 - 1. \tag{4.16}$$

Let $\lambda > 0$ and $0 \leq r' < r$ be integers such that $\lambda_0 = \lambda r + r'$, and $i_1 \in \{0, \ldots, \lambda_0 - 1\}$ be such that $\sigma(\lambda_0 - 1 - i_1) = r - 1$. Then, from (4.15),

$$\epsilon_{\sigma(i_1)} = m(r-1) - \lambda_0 - r - \epsilon_{\sigma(\lambda_0 - 1 - i_1)} = m(r-1) - \lambda_0 - r - \epsilon_{r-1} = -r.$$

If $(\epsilon_{\sigma(i_1)} + \lambda_0) \equiv 0 \mod m$, then m divides $\lambda_0 - r$ and therefore $\lambda_0 = ms + r$ for some integer s. Since $(m, \lambda_0) = 1$, we conclude that $1 = (m, \lambda_0) = (m, ms + r) = (m, r)$. Otherwise, from (4.14), $\sigma(i_1) \geq r$ and therefore there exists $i_2 \in \{0, \ldots, \lambda_0 - 1\}$ such that $\sigma(\lambda_0 - 1 - i_2) = r + \lambda_0 - 1 - \sigma(i_1)$. From (4.15) and (4.16), we have that

$$\epsilon_{\sigma(i_2)} = m(r-1) - \lambda_0 - r - \epsilon_{\sigma(\lambda_0 - 1 - i_2)} = m(r-1) - \lambda_0 - r - \epsilon_{r + \lambda_0 - 1 - \sigma(i_1)} = \epsilon_{\sigma(i_1)} - r = -2r.$$

If $(\epsilon_{\sigma(i_2)} + \lambda_0) \equiv 0 \mod m$, then m divides $\lambda_0 - 2r$ and therefore $(m, r) = 1$. Otherwise, $\sigma(i_2) \geq r$ and therefore there exists $i_3 \in \{0, \dots, \lambda_0 - 1\}$ such that $\sigma(\lambda_0 - 1 - i_3) = r + \lambda_0 - 1 - \sigma(i_2)$ and

$$\epsilon_{\sigma(i_3)} = m(r-1) - \lambda_0 - r - \epsilon_{\sigma(\lambda_0 - 1 - i_3)} = m(r-1) - \lambda_0 - r - \epsilon_{r + \lambda_0 - 1 - \sigma(i_2)} = \epsilon_{\sigma(i_2)} - r = -3r.$$

By continuing this process, we have that $(m, r) = 1$ or we obtain a sequence $i_1, \dots, i_\lambda$ such that

$$\sigma(i_j) \geq r \quad \text{and} \quad \epsilon_{\sigma(i_j)} = -jr \quad \text{for } 1 \leq j \leq \lambda.$$

If the latter happens then $0 < \epsilon_{\sigma(i_\lambda)} + \lambda_0 = \lambda_0 - \lambda r = r' < r$, a contradiction because $m_{H(Q_\infty)} = r$. Therefore, $(m, r) = 1$. Finally, since $\langle m, r \rangle \subseteq H(Q_\infty)$ and $g(\mathcal{X}) = (m-1)(r-1)/2$, we conclude that $H(Q_\infty) = \langle m, r \rangle$. □

4.3 Maximal Castle curves

In this section, as an application of the results obtained in this chapter, we characterize certain classes of $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$, where $\mathcal{X}$ is the curve defined by the equation $Y^m = f(X)$, $f(X) \in \mathbb{F}_{q^2}[X]$ and $(m, \deg f) = 1$, and Q_∞ is the only place at infinity of the curve $\mathcal{X}$. Some examples of $\mathbb{F}_{q^2}$-maximal Castle curves of this type are presented below:

- The Hermitian curve
$$Y^{q+1} = X^q + X.$$
- The curve over $\mathbb{F}_{q^2}$ defined by the affine equation
$$Y^{q+1} = a^{-1}(X^{q/p} + X^{q/p^2} + \cdots + X^p + X),$$
where $p = \mathrm{Char}(\mathbb{F}_q)$ and $a \in \mathbb{F}_{q^2}$ is such that $a^q + a = 0$ and $a \neq 0$.

Note that, in all cases, the places corresponding to the roots of the polynomial $f(X)$ are totally ramified in the extension $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}(x)$, the multiplicities of the roots of $f(X)$ are equals, and $m = q + 1$. We will show that, under certain conditions, all $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$ have these characteristics.

Lemma 4.3.1. *Let $\mathcal{X}$ be the algebraic curve given in Theorem 4.1.2, and let Q_∞ be its only place at infinity. Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_{q^2}$, $(m, \lambda_i) = 1$ for $i = 1, \dots, r$, $(\mathcal{X}, Q_\infty)$ is a Castle curve, and $r < m$. Then*

$$\mathcal{X} \text{ is } \mathbb{F}_{q^2}\text{-maximal if and only if } m = q + 1.$$

Proof. From the assumptions, we obtain that $g(\mathcal{X}) = (m-1)(r-1)/2$. Since $(\mathcal{X}, Q_\infty)$ is a Castle curve, $H(Q_\infty)$ is symmetric and therefore $F_{H(Q_\infty)} = 2g(\mathcal{X}) - 1 = mr - m - r$. Moreover, from item *iii)* of Proposition 4.2.6, $m_{H(Q_\infty)} = \min\{m, r\} = r$. Therefore, $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal if and only if

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 r + 1 = q^2 + 1 + q(m-1)(r-1).$$

Thus, the result follows. □

Lemma 4.3.2. *Let $\mathcal{X}$ be the algebraic curve given in Theorem 4.1.2, and let Q_∞ be its only place at infinity. Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_{q^2}$, $m = q+1$, $r < q+1$, $(q+1, \lambda_i) = 1$ for $i = 1, \ldots, r$, and $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal. The following statements are equivalent:*

i) $H(Q_\infty)$ *is symmetric.*

ii) $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1$.

iii) $\lambda_1 = \cdots = \lambda_r$.

Proof. Note that from the hypotheses we have that $g(\mathcal{X}) = q(r-1)/2$ and therefore $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2g(\mathcal{X})q = q^2 r + 1$.

i) $\Leftrightarrow$ *ii)* : It is enough to note that

$$\begin{aligned} H(Q_\infty) \text{ is symmetric } &\Leftrightarrow F_{H(Q_\infty)} = qr - q - 1 \\ &\Leftrightarrow m_{H(Q_\infty)} = r && \text{(from Proposition 4.2.6)} \\ &\Leftrightarrow \#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1. \end{aligned}$$

i) $\Leftrightarrow$ *iii)* : This follows directly from Theorem 4.2.7. □

We summarize these results in the following theorem.

Theorem 4.3.3. *Let $\mathcal{X}$ be the algebraic curve defined in Theorem 4.1.2, and let Q_∞ be its only place at infinity. Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_{q^2}$, $(m, \lambda_i) = 1$ for $i = 1, \ldots, r$, and $r < m$. Then the following statements are equivalent:*

i) $(\mathcal{X}, Q_\infty)$ *is a* $\mathbb{F}_{q^2}$*-maximal Castle curve.*

ii) $(\mathcal{X}, Q_\infty)$ *is a Castle curve and* $m = q+1$.

iii) $\mathcal{X}$ *is* $\mathbb{F}_{q^2}$*-maximal,* $H(Q_\infty)$ *is symmetric, and* $m = q+1$.

iv) $\mathcal{X}$ *is* $\mathbb{F}_{q^2}$*-maximal,* $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1$*, and* $m = q+1$.

v) $\mathcal{X}$ *is* $\mathbb{F}_{q^2}$*-maximal,* $\lambda_1 = \cdots = \lambda_r$*, and* $m = q+1$.

Finally, we note that for the case when λ_i divides m for each $i = 1, \ldots, r$, the Weierstrass semigroup $H(Q_\infty)$ is symmetric, see Theorem 4.2.4. Therefore, by assuming that $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal, we conclude that

$$(\mathcal{X}, Q_\infty) \text{ is } \mathbb{F}_{q^2}\text{-maximal Castle curve if and only if } \#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1.$$

Bibliography

[1] Miriam Abdón, Herivelto Borges, and Luciane Quoos. Weierstrass points on Kummer extensions. *Adv. Geom.*, 19(3):323–333, 2019.

[2] Miriam Abdón and Luciane Quoos. On the genera of subfields of the Hermitian function field. *Finite Fields Appl.*, 10(3):271–284, 2004.

[3] Miriam Abdón and Fernando Torres. On maximal curves in characteristic two. *Manuscripta Math.*, 99(1):39–53, 1999.

[4] Nurdagül Anbar, Alp Bassa, and Peter Beelen. A complete characterization of Galois subfields of the generalized Giulietti-Korchmáros function field. *Finite Fields Appl.*, 48:318–330, 2017.

[5] Daniele Bartoli and Giacomo Micheli. Algebraic constructions of complete m-arcs, 2020. Preprint, arXiv: 2007.00911.

[6] Daniele Bartoli, Maria Montanucci, and Giovanni Zini. Weierstrass semigroups at every point of the Suzuki curve. *Acta Arith.*, 197(1):1–20, 2021.

[7] Peter Beelen and Maria Montanucci. A new family of maximal curves. *J. Lond. Math. Soc. (2)*, 98(3):573–592, 2018.

[8] Peter Beelen and Maria Montanucci. On subfields of the second generalization of the GK maximal function field. *Finite Fields Appl.*, 64:101669, 24, 2020.

[9] Herivelto Borges, Beatriz Motta, and Fernando Torres. Complete arcs arising from a generalization of the Hermitian curve. *Acta Arith.*, 164(2):101–118, 2014.

[10] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[11] Maria Bras-Amorós and Albert Vico-Oton. On the Geil-Matsumoto bound and the length of AG codes. *Des. Codes Cryptogr.*, 70(1-2):117–125, 2014.

[12] Alonso S. Castellanos, Ariane M. Masuda, and Luciane Quoos. One- and two-point codes over Kummer extensions. *IEEE Trans. Inform. Theory*, 62(9):4867–4872, 2016.

[13] Alonso S. Castellanos and Guilherme Chaud Tizziotti. Two-point AG codes on the GK maximal curves. *IEEE Trans. Inform. Theory*, 62(2):681–686, 2016.

[14] Luciano da F. Costa. An introduction to multisets, 2021. Preprint, arXiv:2110.12902.

[15] Robert S. Coulter. The number of rational points of a class of Artin-Schreier curves. *Finite Fields Appl.*, 8(4):397–413, 2002.

[16] Yusuf Danisman and Mehmet Ozdemir. On the genus spectrum of maximal curves over finite fields. *J. Discrete Math. Sci. Cryptogr.*, 18(5):513–529, 2015.

[17] Stefania Fanali and Massimo Giulietti. Quotient curves of the GK curve. *Adv. Geom.*, 12(2):239–268, 2012.

[18] William Fulton. *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[19] Arnaldo Garcia and Alvaro Garzon. On Kummer covers with many rational points over finite fields. *J. Pure Appl. Algebra*, 185(1-3):177–192, 2003.

[20] Arnaldo Garcia, Cem Güneri, and Henning Stichtenoth. A generalization of the Giulietti-Korchmáros maximal curve. *Adv. Geom.*, 10(3):427–434, 2010.

[21] Arnaldo Garcia and Luciane Quoos. A construction of curves over finite fields. *Acta Arith.*, 98(2):181–195, 2001.

[22] Arnaldo Garcia, Henning Stichtenoth, and Chao-Ping Xing. On subfields of the Hermitian function field. *Compositio Math.*, 120(2):137–170, 2000.

[23] Olav Geil and Ryutaroh Matsumoto. Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups. *J. Pure Appl. Algebra*, 213(6):1152–1156, 2009.

[24] Massimo Giulietti and Gábor Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.*, 343(1):229–245, 2009.

[25] Massimo Giulietti, Gábor Korchmáros, and Fernando Torres. Quotient curves of the Suzuki curve. *Acta Arith.*, 122(3):245–274, 2006.

[26] Massimo Giulietti, Fernanda Pambianco, Fernando Torres, and Emanuela Ughi. On complete arcs arising from plane curves. *Des. Codes Cryptogr.*, 25(3):237–246, 2002.

[27] Massimo Giulietti, Luciane Quoos, and Giovanni Zini. Maximal curves from subcovers of the GK-curve. *J. Pure Appl. Algebra*, 220(10):3372–3383, 2016.

[28] Valery D. Goppa. Codes that are associated with divisors. *Problemy Peredači Informacii*, 13(1):33–39, 1977.

[29] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[30] Cem Güneri, Mehmet Özdemir, and Henning Stichtenoth. The automorphism group of the generalized Giulietti-Korchmáros function field. *Adv. Geom.*, 13(2):369–380, 2013.

[31] Cem Güneri, Mehmet Özdemir, and Henning Stichtenoth. The automorphism group of the generalized Giulietti-Korchmáros function field. *Adv. Geom.*, 13(2):369–380, 2013.

[32] Rohit Gupta, Erik A. R. Mendoza, and Luciane Quoos. Reciprocal polynomials and curves with many points over a finite field, 2021. Preprint, arXiv:2110.10620.

[33] Everett W. Howe. Curves of medium genus with many points. *Finite Fields Appl.*, 47:145–160, 2017.

[34] Sotiris Karanikolopoulos and Aristides Kontogeorgis. Automorphisms of curves and weierstrass semigroups, 2010. Preprint, arXiv:1005.2871.

[35] Motoko Qiu Kawakita. Kummer curves and their fibre products with many rational points. *Appl. Algebra Engrg. Comm. Comput.*, 14(1):55–64, 2003.

[36] Motoko Qiu Kawakita. Certain sextics with many rational points. *Adv. Math. Commun.*, 11(2):289–292, 2017.

[37] Steven L. Kleiman. Algebraic cycles and the Weil conjectures. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 359–386. North-Holland, Amsterdam, 1968.

[38] Joseph Lewittes. Places of degree one in function fields over finite fields. *J. Pure Appl. Algebra*, 69(2):177–183, 1990.

[39] Liming Ma, Chaoping Xing, and Sze Ling Yeo. On automorphism groups of cyclotomic function fields over finite fields. *J. Number Theory*, 169:406–419, 2016.

[40] Hiren Maharaj, Gretchen L. Matthews, and Gottlieb Pirsic. Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences. *J. Pure Appl. Algebra*, 195(3):261–280, 2005.

[41] Gretchen L. Matthews, Dane Skabelund, and Michael Wills. Triples of rational points on the Hermitian curve and their Weierstrass semigroups. *J. Pure Appl. Algebra*, 225(8):106623, 22, 2021.

[42] Erik A. R. Mendoza. On Kummer extensions with one place at infinity, 2022. Preprint, arXiv: 2208.09729.

[43] Erik A. R. Mendoza and Luciane Quoos. Explicit equations for maximal curves as subcovers of the BM curve. *Finite Fields Appl.*, 77:Paper No. 101945, 22, 2022.

[44] Marko Moisio. On the number of rational points on some families of Fermat curves over finite fields. *Finite Fields Appl.*, 13(3):546–562, 2007.

[45] Maria Montanucci and Vincenzo Pallozzi Lavorante. AG codes from the second generalization of the GK maximal curve. *Discrete Math.*, 343(5):111810, 17, 2020.

[46] Carlos Munuera, Alonso Sepúlveda, and Fernando Torres. Algebraic geometry codes from castle curves. In Ángela Barbero, editor, *Coding Theory and Applications*, pages 117–127, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[47] Carlos Munuera, Alonso Sepúlveda, and Fernando Torres. Castle curves and codes. *Adv. Math. Commun.*, 3(4):399–408, 2009.

[48] Francesco Noseda, Gilvan Oliveira, and Luciane Quoos. Bases for Riemann-Roch spaces of one-point divisors on an optimal tower of function fields. *IEEE Trans. Inform. Theory*, 58(5):2589–2598, 2012.

[49] Daniela Oliveira and Fabio E. Brochero Martínez. Artin-schreier curves given by $\mathbb{F}_q$-linearized polynomials, 2020. Preprint, arXiv:2012.01534.

[50] Ferruh Özbudak and Burcu Gülmez Temür. Finite number of fibre products of Kummer covers and curves with many points over finite fields. *Des. Codes Cryptogr.*, 70(3):385–404, 2014.

[51] Ferruh Özbudak, Burcu Gülmez Temür, and Oğuz Yayla. Further results on fibre products of Kummer covers and curves with many points over finite fields. *Adv. Math. Commun.*, 10(1):151–162, 2016.

[52] Antonio Rojas-León. On the number of rational points on curves over finite fields with many automorphisms. *Finite Fields Appl.*, 19:1–15, 2013.

[53] Karl Rökaeus. New curves with many points over small finite fields. *Finite Fields Appl.*, 21:58–66, 2013.

[54] José C. Rosales. Fundamental gaps of numerical semigroups generated by two elements. *Linear Algebra Appl.*, 405:200–208, 2005.

[55] José C. Rosales and Pedro A. García-Sánchez. *Numerical semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[56] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[57] Saeed Tafazolian, Arnoldo Teherán-Herrera, and Fernando Torres. Further examples of maximal curves which cannot be covered by the Hermitian curve. *J. Pure Appl. Algebra*, 220(3):1122–1132, 2016.

[58] Saeed Tafazolian and Fernando Torres. On the curve $Y^n = X^\ell(X^m + 1)$ over finite fields. *Adv. Geom.*, 19(2):263–268, 2019.

[59] Gerard van der Geer. Hunting for curves with many points. In *Coding and cryptology*, volume 5557 of *Lecture Notes in Comput. Sci.*, pages 82–96. Springer, Berlin, 2009.

[60] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler. Tables of curves with many points. 2009.

[61] Gerard van der Geer and Marcel van der Vlugt. How to construct curves over finite fields with many points. In *Arithmetic geometry (Cortona, 1994)*, Sympos. Math., XXXVII, pages 169–189. Cambridge Univ. Press, Cambridge, 1997.

[62] Gerard van der Geer and Marcel van der Vlugt. Kummer covers with many points. *Finite Fields Appl.*, 6(4):327–341, 2000.

[63] Chaoping Xing and Sze Ling Yeo. Algebraic curves with many points over the binary field. *J. Algebra*, 311(2):775–780, 2007.

[64] Shudi Yang and Chuangqiang Hu. Weierstrass semigroups from Kummer extensions. *Finite Fields Appl.*, 45:264–284, 2017.