ON KUMMER EXTENSIONS WITH ONE PLACE AT INFINITY

ERIK A. R. MENDOZA

Abstract. Let K be the algebraic closure of $\mathbb{F}_q$. We provide an explicit description of the Weierstrass semigroup $H(Q_\infty)$ at the only place at infinity Q_∞ of the curve $\mathcal{X}$ defined by the Kummer extension with equation $y^m = f(x)$, where $f(x) \in K[x]$ is a polynomial satisfying $\gcd(m, \deg f) = 1$. As a consequence, we determine the Frobenius number and the multiplicity of $H(Q_\infty)$ in some cases, and we discuss sufficient conditions for the Weierstrass semigroup $H(Q_\infty)$ to be symmetric. Finally, we characterize certain maximal Castle curves of type $(\mathcal{X}, Q_\infty)$.

1. Introduction

Let K be the algebraic closure of the finite field $\mathbb{F}_q$ with q elements. Consider $\mathcal{X}$ a nonsingular, projective, absolutely irreducible algebraic curve over K with genus $g(\mathcal{X})$ and denote by $K(\mathcal{X})$ its function field. For a function $z \in K(\mathcal{X})$, we let $(z), (z)_\infty$ and $(z)_0$ stand for the principal, pole and zero divisor of the function z in $K(\mathcal{X})$ respectively.

Given a place Q in the set of places $\mathcal{P}_{K(\mathcal{X})}$ of the function field $K(\mathcal{X})$, the *Weierstrass semigroup* associated to the place Q is given by

$$H(Q) := \{s \in \mathbb{N}_0 : (z)_\infty = sQ \text{ for some } z \in K(\mathcal{X})\},$$

the complementary set $G(Q) := \mathbb{N} \setminus H(Q)$ is called the *gap set* at Q, and the Weierstrass Gap Theorem [15, Theorem 1.6.8] states that if $g(\mathcal{X}) > 0$, then there exist exactly $g(\mathcal{X})$ gaps at Q

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

The smallest nonzero element of $H(Q)$ is called the multiplicity of $H(Q)$ and is denoted by $m_{H(Q)}$, the largest element of $G(Q)$ is called the Frobenius number and is denoted by $F_{H(Q)}$, and we say that the Weierstrass semigroup $H(Q)$ is symmetric if $F_{H(Q)} = 2g(\mathcal{X}) - 1$.

The knowledge of the inner structure of the Weierstrass semigroup $H(Q)$ at one place in the function field $K(\mathcal{X})$ has various applications in the area of algebraic curves over finite fields. Among the most interesting ones we have the construction of algebraic geometry codes with good parameters, see [10]; the determination of the automorphism group of an algebraic curve, see [8]; to decide if a place is Weierstrass, see [1], and obtain upper bounds for the number of rational places (places of degree one) of a curve, such as the

Keywords: Kummer extensions, Weierstrass semigroup.

Mathematics Subject Classification (2010): 14H55, 11R58.

The research of Erik A. R. Mendoza was partially supported by FAPERJ/RJ-Brazil (Grant 201.650/2021).

Lewittes bound [7] which establishes that the number $\#\mathcal{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational places of a curve $\mathcal{X}$ defined over $\mathbb{F}_q$ is upper bounded by

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

where Q is an $\mathbb{F}_q$-rational place of $\mathcal{X}$. The best-known upper bound for the number of $\mathbb{F}_q$-rational places is the Hasse-Weil bound

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

and a curve is called $\mathbb{F}_q$-maximal if equality holds in the Hasse-Weil bound.

A pointed algebraic curve $(\mathcal{X}, Q)$ over $\mathbb{F}_q$, where Q is an $\mathbb{F}_q$-rational place of $\mathcal{X}$, is called a *Castle curve* if the semigroup $H(Q)$ is symmetric and equality holds in (1). Castle curves were introduced in [12] and have been studied due to their interesting properties related to the construction of algebraic geometry codes with good parameters and its duals, see [11, 12].

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 is a totally ramified place in a Kummer extension defined by the equation $y^m = f(x)$, $f(x) \in K[x]$. As a consequence, they explicitly described the semigroup $H(Q)$ when $f(x)$ is a separable polynomial. This description was generalized by Castellanos, Masuda, and Quoos [3], where they study the Kummer extension defined by $y^m = f(x)^\lambda$, where $\lambda \in \mathbb{N}$ and $f(x) \in K[x]$ is a separable polynomial satisfying $\gcd(m, \lambda \deg f) = 1$.

For a general Kummer extension with one place at infinity

$$\mathcal{X}: \quad y^m = \prod_{i=1}^{r} (x - \alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \text{and} \quad 1 \leq \lambda_i < m, \tag{2}$$

where $m \geq 2$ and $r \geq 2$ are integers such that $\gcd(m, q) = 1$, $\alpha_1, \dots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $\gcd(m, \lambda_0) = 1$, the Weierstrass semigroup $H(Q_\infty)$ at the only place at infinity Q_∞ of $\mathcal{X}$ was explicitly described in the following particular cases:

i) For $\lambda_1 = \lambda_2 = \cdots = \lambda_r$, see [3, Theorem 3.2].
ii) For any λ_1 and $\lambda_2 = \lambda_3 = \cdots = \lambda_r = 1$, see [16, Remark 2.8].

This article 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 of the curve $\mathcal{X}$ given in (2). Moreover, we provide a system of generators for the semigroup $H(Q_\infty)$ and, as a consequence, we obtain interesting results including the following theorems:

Theorem A (see Theorem 4.4)**.** *Let $F_{H(Q_\infty)}$ be the Frobenius number of the semigroup $H(Q_\infty)$. Then*

$$F_{H(Q_\infty)} = m(r-1) - \lambda_0 \textit{ and } H(Q_\infty) \textit{ is symmetric} \quad \Leftrightarrow \quad \lambda_j \mid m \textit{ for each } j = 1, \dots, r.$$

Theorem B (see Theorem 4.7)**.** *Suppose that* $\gcd(m, \lambda_j) = 1$ *for each* $j = 1, \dots, r$*. Then the following 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 one:

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

Theorem C (see Theorem 5.3). *Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_{q^2}$,* $\gcd(m, \lambda_j) = 1$ *for $j = 1, \ldots, r$ and $r < m$. Then*

$(\mathcal{X}, Q_\infty)$ *is $\mathbb{F}_{q^2}$-maximal Castle curve* $\Leftrightarrow$ $\mathcal{X}$ *is $\mathbb{F}_{q^2}$-maximal, $\lambda_1 = \cdots = \lambda_r$, and $m = q+1$.*

This paper is organized as follows. In Section 2 we introduce the preliminaries and notation that will be used throughout this paper. In Section 3 we present the main result of this paper which gives the explicit description of the semigroup $H(Q_\infty)$ (see Theorem 3.2). In Section 4 we provide an explicit description of the gap set $G(Q_\infty)$ (see Proposition 4.1), we study the Frobenius number and the multiplicity of the semigroup $H(Q_\infty)$ establishing a relationship between them (see Proposition 4.6), and provide sufficient conditions for the semigroup $H(Q_\infty)$ to be symmetric (see Theorems 4.4 and 4.7). In Section 5, we characterize certain $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$ (see Theorem 5.3).

2. Preliminaries and notation

Throughout this article, we 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 and b integers, 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. 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. 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.

2.1. Numerical semigroups.

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 $\mathbb{N}_0 \setminus H$ is finite. The elements of $G := \mathbb{N}_0 \setminus H$ 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. The numerical semigroup H is called symmetric if $F_H = 2g_H - 1$. Moreover, we say that the set $\{a_1, \ldots, a_d\} \subset H$ is a system of generators of the numerical semigroup H if

$$H = \langle a_1, \ldots, a_d\rangle := \{t_1a_1 + \cdots + t_da_d : t_1, \ldots, t_d \in \mathbb{N}_0\}.$$

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 is called the embedding dimension of H and will be denoted by e_H.

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. Moreover, several important results are associated with the Apéry set.

Proposition 2.1. *[14, 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 2.2. *[14, Proposition 4.10] Let H be a numerical semigroup and 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*

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

On the other hand, the following result characterizes the elements of a numerical semigroup generated by two elements and will be useful in this paper.

Proposition 2.3. *[13, Lemma 1] Let $x \in \mathbb{Z}$ and let $n_1, n_2 \geq 2$ be positive integers such that $(n_1, n_2) = 1$. Then $x \notin \langle n_1, n_2 \rangle$ if and only if $x = n_1 n_2 - a n_1 - b n_2$ for some $a, b \in \mathbb{N}$.*

2.2. **Function Fields.** Let $\mathcal{X}$ be a nonsingular, projective, absolutely irreducible algebraic curve over K with genus $g(\mathcal{X})$ and $K(\mathcal{X})$ be the function field of $\mathcal{X}$. For each place $Q \in \mathcal{P}_{K(\mathcal{X})}$, the Weierstrass semigroup $H(Q)$ has the structure of a numerical semigroup. Moreover, it is a well-known fact that for all but finitely many places $Q \in \mathcal{P}_{K(\mathcal{X})}$, 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.

Several upper bounds for the number of rational places of algebraic curves are available in the literature. The Hasse-Weil bound states that for a curve $\mathcal{X}$ defined over $\mathbb{F}_q$,

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

The curve $\mathcal{X}$ is called $\mathbb{F}_q$-maximal if equality holds in the Hasse-Weil bound. Among other upper bounds for the number of rational places, we have the Lewittes bound [7].

Theorem 2.4 (Lewittes bound)**.** *Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$ and let Q be a rational place of $\mathcal{X}$. Then*

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

For more on numerical semigroups and function fields, we refer to the books [14] and [15] respectively.

3. The semigroup $H(Q_\infty)$

Consider the algebraic curve

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

where $m \ge 2$ and $r \ge 2$ are positive 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 $(m, \lambda_0) = 1$. By [15, Proposition 3.7.3], this curve has genus

$$g(\mathcal{X}) = \frac{(m-1)(r-1) + r - \sum_{i=1}^r (m, \lambda_i)}{2}. \tag{3}$$

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 [5, p. 94], which states that, for m and λ positive integers,

$$\sum_{i=1}^{\lambda-1} \left\lfloor \frac{im}{\lambda} \right\rfloor = \frac{(m-1)(\lambda-1) + (m,\lambda) - 1}{2}. \tag{4}$$

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

Lemma 3.1. *Let $r, m, \lambda_0, \lambda_1, \lambda_2, \dots, \lambda_r$ be positive integers such that $\lambda_0 = \sum_{i=1}^r \lambda_i$ and $r < \lambda_0$. For $k \in \{r, \dots, \lambda_0 - 1\}$, we define*

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

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

$$\left\{\!\!\left\{ \eta_k : r \le k \le \lambda_0 - 1 \right\}\!\!\right\} = \left\{\!\!\left\{ \left\lfloor \frac{s_i m}{\lambda_i} \right\rfloor : 1 \le s_i < \lambda_i,\ 1 \le i \le r \right\}\!\!\right\}. \tag{5}$$

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 $\eta_k = \rho_{u_1,\dots,u_r} = \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor$ for some j, where $\sum_{i=1}^r u_i = k$ and $r \le k \le \lambda_0 - 2$, then $u_j < \lambda_j$ and

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

This proves that $\eta_r \le \eta_{r+1} \le \cdots \le \eta_{\lambda_0-1} < m$ is a non-decreasing sequence. Let $S_1 := \{\!\{ \eta_k : r \le k \le \lambda_0 - 1 \}\!\}$ and $S_2 := \{\!\{ \lfloor s_i m/\lambda_i \rfloor : 1 \le s_i < \lambda_i, 1 \le i \le r \}\!\}$. 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 $m_{S_1}(\eta_k) \le m_{S_2}(\eta_k)$ 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

$$\eta_{k-1} < \eta_k = \eta_{k+1} = \cdots = \eta_{k+n-1}, \tag{6}$$

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 $\eta_k = \lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \rfloor$. 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 $\lfloor \frac{s_{j_1} \lambda_i}{\lambda_{j_1}} \rfloor + 1 \in \Gamma_i$ 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 (6), 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 $\eta_k < \lfloor \frac{t_j m}{\lambda_j} \rfloor$ for each $j \in \{1, \ldots, r\} \setminus \{j_1\}$, then $\eta_k < \rho_{t_1, \ldots, t_{j_1}+1, \ldots, t_r} \leq \eta_{k+1}$ since $\sum_{i=1}^r t_i = k$. This is a contradiction to (6). Therefore there exists $j_2 \in \{1, \ldots, r\} \setminus$

$\{j_1\}$ 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 $j \in \{1, \ldots, r\} \setminus \{j_1, j_2\}$, then $\eta_k < \rho_{t_1,\ldots,t_{j_1}+1,\ldots,t_{j_2}+1,\ldots,t_r} \leq \eta_{k+2}$, again a contradiction to (6). Therefore there exists $j_3 \in \{1, \ldots, r\} \setminus \{j_1, j_2\}$ 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 $j_1, j_2, \ldots, j_n$ such that

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

Finally, from (4), 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 3.2. *Let $m \geq 2$ and $r \geq 2$ be integers such that $p \nmid m$. Let $\mathcal{X}$ be the algebraic curve defined by the affine equation*

$$\mathcal{X}: \quad y^m = \prod_{i=1}^{r} (x - \alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad \textit{and} \quad 1 \leq \lambda_i < m, \tag{7}$$

where $\alpha_1, \ldots, \alpha_r$ 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

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

where $B_k = \{mk - k'\lambda_0 : k' = 1, \ldots, \eta_k\}$ and η_k are defined as in Lemma 3.1. In particular,

$$H(Q_\infty) = \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \ldots, \lambda_0 - 1 \rangle. \tag{8}$$

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 $k \in \{r, \dots, \lambda_0 - 1\}$, let $s_1, \dots, s_r$ be positive integers such that $1 \le s_i \le \lambda_i$ and $\sum_{i=1}^{r} s_i = k$. Then

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

and

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

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

$$\langle m, \lambda_0\rangle \cup \bigcup_{k=r}^{\lambda_0-1} B_k \subseteq H(Q_\infty). \tag{9}$$

Now, we prove that the union given in (9) is disjoint. For $k \in \{r, \dots, \lambda_0 - 1\}$ and $k' \in \{1, \dots, \eta_k\}$, 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 2.3, $B_k \cap \langle m, \lambda_0\rangle = \emptyset$. On the other hand, we have that $B_{k_1} \cap B_{k_2} = \emptyset$ for $k_1 \ne k_2$. In fact, if $mk_1 - \lambda_0 k_1' = mk_2 - \lambda_0 k_2'$ for $r \le k_1, k_2 < \lambda_0$, $1 \le k_1' \le \eta_{k_1}$, and $1 \le k_2' \le \eta_{k_2}$, then $m(k_1 - k_2) = \lambda_0(k_1' - k_2')$. Since $(m, \lambda_0) = 1$ and $2 - \lambda_0 \le k_1 - k_2 \le \lambda_0 - 2$, we conclude that $k_1 = k_2$.

Finally, we prove that equality holds in (9). 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 3.1 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, $e_H \le m_H$, see [14, Proposition 2.10]. Since $m \in H(Q_\infty)$, $e_{H(Q_\infty)} \le m_{H(Q_\infty)} \le m$. However, in general, it is difficult to obtain a minimal system of generators to $H(Q_\infty)$ from the system of generators given in (8).

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 3.2 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 (8) 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 (8) 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 $e_{H(Q_\infty)} \leq m - \lceil \frac{m}{\lambda}\rceil - \lfloor \frac{m}{\lambda}\rfloor + 3 \leq m$.

Example 3.3 (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 [4]. 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:*

$$y^{q^n+1} = (x^q + x)h(x)^{q+1}, \text{ where } h(x) = \sum_{i=0}^{q}(-1)^{i+1}x^{i(q-1)}.$$

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 3.2, 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 3.1, 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,

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

Moreover, since

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

it follows from Theorem 3.2 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 [6, 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 $(m, d(q-1))=1$. In [9, Theorem 3.1], the authors study the $\mathbb{F}_{q^{2n}}$-maximal curve defined by the affine equation

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

This curve is a subcover of the second generalization of the GK curve given by Beelen and Montanucci [2] and has only one place at infinity Q_∞. In the following result, using Theorem 3.2, we compute the Weierstrass semigroup $H(Q_\infty)$.

Proposition 3.4. *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*

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

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 3.1, 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,

$$m_S\left(\left\lfloor\frac{(\beta+1)m}{q+1}\right\rfloor\right)=d(q-2)+1-\delta_\beta. \tag{10}$$

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 $0 \le \beta \le q-1$ and $0 \le i \le d(q-2) - \delta_\beta$. From (10) and since $\eta_r \le \eta_{r-1} \le \cdots \le \eta_{\lambda_0 - 1}$ 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 $0 \le \beta \le q-1$ and $0 \le i \le d(q-2) - \delta_\beta$. From Theorem 3.2, 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 $0 \le \beta \le q-1$. $\square$

4. 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 3.2, in this section we study the Frobenius number $F_{H(Q_\infty)}$, the multiplicity $m_{H(Q_\infty)}$, and the relationship between them.

Henceforth, to simplify the notation, we define

$$\eta_s := \begin{cases} 0, & \text{if } 0 \le s < r, \\ m-1, & \text{if } \lambda_0 \le s, \end{cases} \quad \text{and} \quad \epsilon_k := mk - \lambda_0(\eta_k + 1) \text{ for } k \in \mathbb{N}_0. \tag{11}$$

Thus, from Theorem 3.2, we obtain that

$$H(Q_\infty) = \langle \epsilon_k + \lambda_0 : k = 1, r, \dots, \lambda_0 \rangle . \tag{12}$$

We start by noticing that not all the elements $\epsilon_{r-1}, \dots, \epsilon_{\lambda_0 - 1}$ defined in (11) 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 4.1. *Using the same notation as in Theorem 3.2, 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 3.2, we have that

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

where $B_k = \{m\lambda_0 - (\lambda_0 - k)m - k'\lambda_0 : k' = 1, \dots, \eta_k\}$. Moreover, from Proposition 2.3, 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,

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

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

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

□

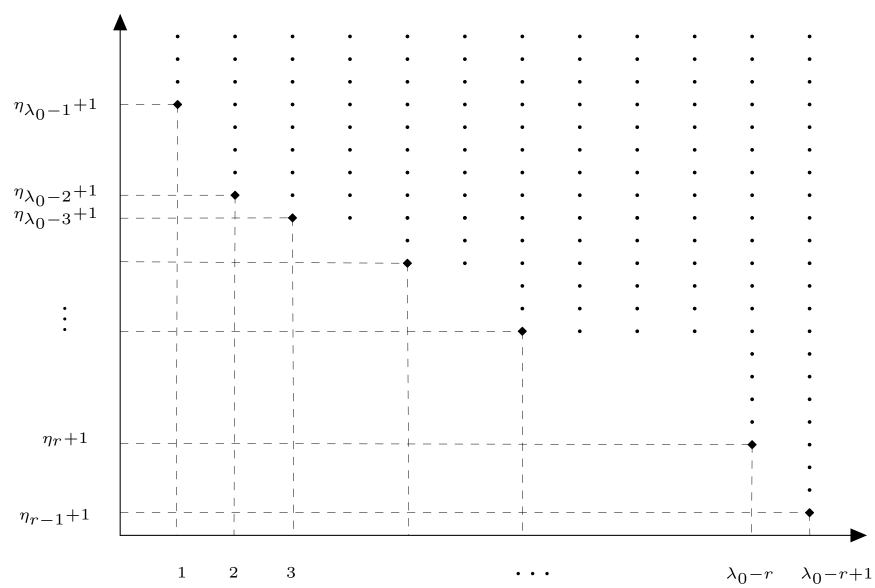

Figure 1. Description of the set Δ

Now, we provide sufficient conditions to determine whether the semigroup $H(Q_\infty)$ is symmetric. For this, we need a remark and a lemma.

Remark 4.2. *Due to the characterization of the sequence $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0-1}$ given in Lemma 3.1, we can see that, for $s \in \mathbb{N}_0$, $\eta_s + \eta_{r+\lambda_0-1-s} = m$ or $\eta_s + \eta_{r+\lambda_0-1-s} = m-1$. In fact, if $0 \leq s \leq r-1$ or $\lambda_0 \leq s$ the assertion is clear. Let $k \in \{r, \ldots, \lambda_0 - 1\}$ 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 3.1, there exist exactly n distinct elements $j_1, \ldots, j_n \in \{1, \ldots, r\}$ and positive integers $s_{j_1}, \ldots, s_{j_n}$ 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

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

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 $i = 0, \ldots, n-1$. 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 $s = r, \ldots, \lambda_0 - 1$.

Lemma 4.3. *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 4.4. *With the same notation as in Theorem 3.2,*

$$F_{H(Q_\infty)} = \epsilon_{r-1} \text{ and } H(Q_\infty) \text{ is symmetric} \quad \Leftrightarrow \quad \lambda_j \mid m \text{ for each } j = 1, \ldots, r.$$

Proof. Suppose that $H(Q_\infty)$ is symmetric and $F_{H(Q_\infty)} = \epsilon_{r-1}$. From (3) 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 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 4.3, $\epsilon_{r-1} > \epsilon_k$ for $k = r, \ldots, \lambda_0 - 1$. Therefore, from Proposition 4.1, $F_{H(Q_\infty)} = \max\{\epsilon_{r-1}, \ldots, \epsilon_{\lambda_0-1}\} = \epsilon_{r-1}$ 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 4.5. *From Example 3.3, 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 4.4, 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 4.1 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 4.6. *Using the same notation as in Theorem 3.2, 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* $s \in \{r, \ldots, \lambda_0 - 1\}$ *such that* $\eta_s + \eta_{r+\lambda_0-1-s} = m - 1$.

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

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

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

Proof. *i*) It follows from Lemma 4.3 and the fact that $\eta_s \leq \lfloor sm/\lambda_0 \rfloor$ for all $s \in \mathbb{N}_0$.

ii) It is enough to note that, from Lemma 4.3, 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 (12) and Lemma 4.3, 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 (7), 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 2.1, the Apéry set of λ_0 in the Weierstrass semigroup $H(Q_\infty)$ is given by

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

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

Theorem 4.7. *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 $\beta \in \{1, \ldots, \tau - 1\}$ and $i \in \{0, \ldots, r - 1\}$ 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 2.3, it follows that

$$\eta_{r\beta+i} \leq \left\lfloor \frac{\beta m}{\tau} \right\rfloor \text{ for } 1 \leq \beta \leq \tau - 1 \text{ and } 0 \leq i \leq r - 1. \tag{13}$$

For $\beta = 1$ in (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 (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 $\lfloor \frac{m}{\lambda} \rfloor = \lfloor \frac{m}{\tau} \rfloor$ and therefore $\eta_{r+i} = \lfloor \frac{m}{\lambda} \rfloor$ 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 (5), 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 $\eta_{2r} = \lfloor \frac{2m}{\lambda} \rfloor$. Moreover, from Remark 4.2, $\eta_{\lambda_0-1-i} = m - 1 - \eta_{r+i} = \lfloor \frac{(\lambda-1)m}{\lambda} \rfloor$ for $0 \leq i \leq r - 1$ and hence $\eta_{\lambda_0-r-1} = \lfloor \frac{(\lambda-2)m}{\lambda} \rfloor$.

For $\beta = 2$ in (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 (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 $\lfloor \frac{2m}{\lambda} \rfloor = \lfloor \frac{2m}{\tau} \rfloor$, $\eta_{2r+i} = \lfloor \frac{2m}{\lambda} \rfloor$ and $\eta_{\lambda_0-r-1-i} = \lfloor \frac{(\lambda-2)m}{\lambda} \rfloor$ for $0 \leq i \leq r - 1$. This implies that $\eta_{3r} = \lfloor \frac{3m}{\lambda} \rfloor$ and $\eta_{\lambda_0-2r-1} = \lfloor \frac{(\lambda-3)m}{\lambda} \rfloor$.

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 $1\le\beta\le\lambda_r-1$ and $0\le i\le r-1$. On the other hand, from Theorem 3.2,

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

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

$$(\epsilon_k+\lambda_0)\equiv 0 \mod m \quad \text{if and only if} \quad 0\le k\le r-1. \tag{14}$$

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

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

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 2.2, we have that

$$\epsilon_{\sigma(i)}+\epsilon_{\sigma(\lambda_0-1-i)}=m(r-1)-\lambda_0-r \quad \text{for } i=0,\ldots,\lambda_0-1. \tag{15}$$

On the other hand, from Proposition 4.3, we know that

$$\epsilon_{\sigma(i)}+\epsilon_{r+\lambda_0-1-\sigma(i)}=m(r-1)-\lambda_0 \quad \text{for } i=0,\ldots,\lambda_0-1. \tag{16}$$

Let $\lambda>0$ and $0\le r'<r$ 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 (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 λ_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 (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 (15) and (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 $i_3 \in \{0, \ldots, \lambda_0 - 1\}$ 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 $i_1, \ldots, i_\lambda$ 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 $H(Q_\infty) = \langle m, r \rangle$. □

5. Maximal Castle curves

In this section, as an application of the results obtained, we characterize certain classes of $\mathbb{F}_{q^2}$-maximal Castle curves of type $(\mathcal{X}, Q_\infty)$ (that is, $\mathbb{F}_{q^2}$-maximal curves $\mathcal{X}$ such that $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1$ and $H(Q_\infty)$ is symmetric), 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 equal 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 5.1. *Let $\mathcal{X}$ be the algebraic curve given in Theorem 3.2 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 $i = 1, \ldots, r$, $(\mathcal{X}, Q_\infty)$ 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 *iii*) of Proposition 4.6, $m_{H(Q_\infty)} = \min\{m, r\} = r$. 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 5.2. *Let $\mathcal{X}$ be the algebraic curve given in Theorem 3.2 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) ⇔ *ii*) : It is enough to note that

$$\begin{aligned} H(Q_\infty) \text{ is symmetric } &\Leftrightarrow F_{H(Q_\infty)} = qr - q - 1 \\ &\Leftrightarrow m_{H(Q_\infty)} = r && \text{(from Proposition 4.6)} \\ &\Leftrightarrow \#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1. \end{aligned}$$

i) ⇔ *iii*) : This follows directly from Theorem 4.7. □

We summarize these results in the following theorem.

Theorem 5.3. *Let $\mathcal{X}$ be the algebraic curve defined in Theorem 3.2 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 4.4. Therefore, by assuming that $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal, we conclude that

$$(\mathcal{X}, Q_\infty) \text{ is } \mathbb{F}_{q^2}\text{-maximal Castle curve if and only if } \#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 m_{H(Q_\infty)} + 1.$$

6. Acknowledgment

I would like to thank Professors Luciane Quoos and Rohit Gupta, as well as the anonymous referees for their valuable comments and suggestions that improved the presentation of this paper.

References

[1] M. Abdón, H. Borges, and L. Quoos. Weierstrass points on Kummer extensions. *Adv. Geom.*, 19(3):323–333, 2019.

[2] P. Beelen and M. Montanucci. A new family of maximal curves. *J. Lond. Math. Soc. (2)*, 98(3):573–592, 2018.

[3] A. S. Castellanos, A. M. Masuda, and L. Quoos. One- and two-point codes over Kummer extensions. *IEEE Trans. Inform. Theory*, 62(9):4867–4872, 2016.

[4] A. Garcia, C. Güneri, and H. Stichtenoth. A generalization of the Giulietti-Korchmáros maximal curve. *Adv. Geom.*, 10(3):427–434, 2010.

[5] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[6] C. Güneri, M. Özdemir, and H. Stichtenoth. The automorphism group of the generalized Giulietti-Korchmáros function field. *Adv. Geom.*, 13(2):369–380, 2013.

[7] J. Lewittes. Places of degree one in function fields over finite fields. *J. Pure Appl. Algebra*, 69(2):177–183, 1990.

[8] L. Ma, C. Xing, and S. L. Yeo. On automorphism groups of cyclotomic function fields over finite fields. *J. Number Theory*, 169:406–419, 2016.

[9] E. A. R. Mendoza and L. Quoos. Explicit equations for maximal curves as subcovers of the BM curve. *Finite Fields Appl.*, 77:Paper No. 101945, 22, 2022.

[10] M. Montanucci and V. Pallozzi Lavorante. AG codes from the second generalization of the GK maximal curve. *Discrete Math.*, 343(5):111810, 17, 2020.

[11] C. Munuera, A. Sepúlveda, and F. Torres. Algebraic geometry codes from castle curves. In Á. Barbero, editor, *Coding Theory and Applications*, pages 117–127, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[12] C. Munuera, A. Sepúlveda, and F. Torres. Castle curves and codes. *Adv. Math. Commun.*, 3(4):399–408, 2009.

[13] J. C. Rosales. Fundamental gaps of numerical semigroups generated by two elements. *Linear Algebra Appl.*, 405:200–208, 2005.

[14] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[15] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[16] S. Tafazolian and F. Torres. On the curve $Y^n = X^\ell(X^m+1)$ over finite fields. *Adv. Geom.*, 19(2):263–268, 2019.

Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, CEP 21941-909, Rio de Janeiro, Brazil

Email address: erik@im.ufrj.br