Polynesian Journal of Mathematics

Volume 2, Issue 1

On the non-special divisors in algebraic function fields defined over finite fields

Stéphane Ballet Mahdi Koutchoukali

Received 25 Oct 2024
Revised 22 Feb 2025
Accepted 3 Mar 2025
Published 7 Mar 2025
Communicated by Roger Oyono

DOI: 10.69763/polyjmath.2.1

Polynesian Journal of Mathematics
Volume 2, Issue 1 (Mar. 2025)

On the non-special divisors in algebraic function fields defined over finite fields

Stéphane Ballet Mahdi Koutchoukali

Aix–Marseille Université, CNRS, Institut de Mathématiques de Marseille, France

Abstract

In the theory of algebraic function fields and their applications to information theory, the Riemann–Roch theorem plays a fundamental role. But its use, delicate in general, is efficient and practical for applications especially in the case of non-special divisors. In this paper, we survey known results concerning non-special divisors in algebraic function fields defined over finite fields and enrich it with new results about the existence of such divisors in curves of defect k. Our presentation is self-contained with full proofs given for each result, either original proofs or shorter, alternative proofs.

Keywords: Finite field, function field, non-special divisor.

1 Introduction

1.1 General context

This article is mainly a survey highlighting the current state-of-the-art on the existence and the construction of non-special divisors in algebraic function fields defined over finite fields. The growing importance of this topic has attracted many mathematicians and computer scientists, who developed new ideas and obtained new results. Finite fields constitute an important area of mathematics. They arise in many applications, particularly in areas related to information theory, for example cryptography and error-correcting codes. Moreover, algebraic-geometric codes "à la Goppa" whose performance as error-correcting codes was proven by the results of Tsfasman–Vladuts–Zink in [29] also play an important role in cryptography and in algorithmic or computational algebraic geometry as demonstrated by the work carried out in recent years on secret sharing schemes (see for example [8], [4], [5] and [30]) or on the algebraic complexity of the multiplication in the finite fields (see the survey [2]). In all of these cases, the use of the Riemann–Roch theorem with non-special divisors of degree d in algebraic function fields of genus g over finite fields, in particular in the non-trivial case where $g - 1 \leqslant d \leqslant 2g - 2$, is crucial.

1.2 Organisation

In this paper, we give a survey of the known results concerning the non-special divisors in the algebraic function fields defined over finite fields, enriched with some unpublished recent results. In particular, we have chosen to be self-contained by giving the full proofs of each result that relates directly to the non-special divisors, the original proofs or shorter alternative proofs.

In Section 2, we present Notation and the well-known elementary results about non-special divisors in algebraic function fields defined over an arbitrary field. In Section 3, we focus on the results concerning the existence of non-special divisors of degree g and $g-1$. Finally, in section 3.6, new results are proposed on the existence of these divisors in curves of defect k.

2 Preliminaries

2.1 Notation.

Let $\mathbf{F}/\mathbb{F}_q$ be an algebraic function field of one variable defined over a finite field $\mathbb{F}_q$. We will always suppose that the full constant field of $\mathbf{F}/\mathbb{F}_q$ is $\mathbb{F}_q$ and denote by g the genus of $\mathbf{F}$. If D is a (rational) divisor, recall that the $\mathbb{F}_q$-Riemann–Roch vector space associated to D and denoted $\mathcal{L}(D)$ is the subspace of rational functions

$$\mathcal{L}(D) = \{x \in \mathbf{F} : (x) \geqslant -D\} \cup \{0\}. \tag{1}$$

By the Riemann–Roch theorem we know that the dimension of this vector space, denoted by $\dim(D)$, is related to the genus of $\mathbf{F}$ and to the degree $\deg(D)$ of D by

$$\dim(D) = \deg(D) - g + 1 + \dim(\kappa - D), \tag{2}$$

where κ denotes a canonical divisor of $\mathbf{F}/\mathbb{F}_q$. In this relation, the complementary term $i(D) = \dim(\kappa - D)$ is called the index of speciality and is not easy to compute in general. In particular, a divisor D is non-special when the index of speciality $i(D)$ is zero. Let us recall the usual notation (for the basic notions related to an algebraic function field see [25]). For any integer $k \geqslant 1$ we denote by $\mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$ the set of places of degree k, by $B_k(\mathbf{F}/\mathbb{F}_q)$ the cardinality of this set and by $\mathsf{P}(\mathbf{F}/\mathbb{F}_q) = \cup_k \mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$. The divisor group of $\mathbf{F}/\mathbb{F}_q$ is denoted by $\mathsf{D}(\mathbf{F}/\mathbb{F}_q)$. If a divisor $D \in \mathsf{D}(\mathbf{F}/\mathbb{F}_q)$ is such that

$$D = \sum_{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q)} n_P P,$$

the support of D is the following finite set

$$\operatorname{supp}(D) = \left\{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q) : n_P \neq 0\right\}$$

and its degree is

$$\deg(D) = \sum_{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q)} n_P \deg(P).$$

We denote by $\mathrm{D}_n(\mathbf{F}/\mathbb{F}_q)$ the set of divisors of degree n. We say that the divisor D is effective if for each $P \in \mathrm{supp}(D)$ we have $n_P \geqslant 0$ and we denote by $\mathrm{D}_n^+(\mathbf{F}/\mathbb{F}_q)$ the set of effective divisors of degree n and by $A_n = \#\mathrm{D}_n^+(\mathbf{F}/\mathbb{F}_q)$ the cardinal of the set $\mathrm{D}_n^+(\mathbf{F}/\mathbb{F}_q)$. In general, we will note $\#\mathcal{U}$ the cardinal of the set $\mathcal{U}$. The dimension of a divisor D, denoted by $\dim(D)$, is the dimension of the vector space $\mathcal{L}(D)$ defined by formula (1). Let $x \in \mathbf{F}/\mathbb{F}_q$, we denote by (x) the divisor associated to the rational function x, namely

$$(x) = \sum_{P \in \mathrm{P}(\mathbf{F}/\mathbb{F}_q)} v_P(x)P,$$

where v_P is the valuation at the place P. Such a divisor (x) is called a principal divisor, and the set of principal divisors is a subgroup of $\mathrm{D}_0(\mathbf{F}/\mathbb{F}_q)$ denoted by $\mathrm{Princ}(\mathbf{F}/\mathbb{F}_q)$. The factor group

$$\mathcal{C}(\mathbf{F}/\mathbb{F}_q) = \mathrm{D}(\mathbf{F}/\mathbb{F}_q)/\mathrm{Princ}(\mathbf{F}/\mathbb{F}_q)$$

is called the divisor class group. If D_1 and D_2 are in the same class, namely if the divisor $D_1 - D_2$ is principal, we will write $D_1 \sim D_2$. We will denote by $[D]$ the class of the divisor D.

If $D_1 \sim D_2$, the following holds

$$\deg(D_1) = \deg(D_2), \quad \dim(D_1) = \dim(D_2),$$

so that we can define the degree $\deg([D])$ and the dimension $\dim([D])$ of a class. Since the degree of a principal divisor is 0, we can define the subgroup $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)^0$ of classes of degree 0 divisors in $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)$. It is a finite group and we denote by h its order, called the *class number* of $\mathbf{F}/\mathbb{F}_q$. Moreover if

$$L(t) = \sum_{i=0}^{2g} a_i t^i = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha_i} t)$$

with $|\alpha_i| = \sqrt{q}$ is the numerator of the Zeta function of $\mathbf{F}/\mathbb{F}_q$, we have $h = L(1)$. Finally we will denote $h_{n,k}$ the number of classes of divisors of degree n and of dimension k.

In the sequel, we may simultaneously use the dual language of (smooth, absolutely irreducible, projective) curves by associating to $\mathbf{F}/\mathbb{F}_q$ a unique ($\mathbb{F}_q$-isomorphism class of) curve $\mathbf{C}(\mathbb{F}_q)$ defined over $\mathbb{F}_q$ of genus g and conversely to such a curve its function field $\mathbf{C}(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational points on $\mathbf{C}$, and $\mathbb{F}_q(\mathbf{C})$ is the field of rational functions on $\mathbf{C}$ over $\mathbb{F}_q$. Because, by F.K. Schmidt's theorem (cf. [25, Corollary V.1.11]) there always exists a rational divisor of degree one, the group $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)^0$ is isomorphic to the group of $\mathbb{F}_q$-rational points on the Jacobian of $\mathbf{C}$, denoted by $\mathrm{Jac}(\mathbf{C})$. In particular $h(\mathbf{F}/\mathbb{F}_q) = \#\mathrm{Jac}(\mathbf{C})(\mathbb{F}_q)$ is the cardinal of the set $\mathrm{Jac}(\mathbf{C})(\mathbb{F}_q)$.

2.2 Elementary results on non-special divisors.

Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g > 0$. First recall some results about non-special divisors (cf. [25]). If $\deg(D) < 0$, then $\dim(D) = 0$ and if $\deg(D) \geqslant 0$ then $\dim(D) \geqslant \deg(D) - g + 1$. When $0 \leqslant \deg(D) \leqslant 2g - 2$, the computation of $\dim(D)$ is difficult, but we have the following general results.

Proposition 2.1. 1. *$\mathbb{F}_q \subset \mathcal{L}(D)$ if and only if $D \geqslant 0$.*

2. *If $\deg(D) > 2g - 2$, then D is non-special.*

3. *The property of a divisor D being special or non-special depends only on the class of D up to equivalence.*

4. *Any canonical divisor κ is special, $\deg(\kappa) = 2g - 2$ and $\dim(\kappa) = g$.*

5. *Any divisor D with $\dim(D) > 0$ and $\deg(D) < g$ is special.*

6. *If D is non-special and $D' \geqslant D$ then D' is non-special.*

7. *For any divisor D with $0 \leqslant \deg(D) \leqslant 2g - 2$, $\dim(D) \leqslant 1 + \frac{1}{2}\deg(D)$ holds.*

For the rational function field $\mathbf{F} = \mathbb{F}_q(x)$ ($g = 0$), there is no non-zero regular differential, thus, all divisors of degree $d \geqslant 0$ are non-special. From now, we focus on the existence of non-special divisors of degree g or $g - 1$. Note that $g - 1$ is the least possible degree for a divisor D to be non-special. We have the following trivial observations.

Lemma 2.2. *Assume $g \geqslant 1$. Let $D \in \mathrm{D}(\mathbf{F}/\mathbb{F}_q)$ and set $d = \deg(D)$.*

1. *If $d = g$, D is a non-special divisor if and only if $\dim(D) = 1$. Assume that D is a non-special divisor of degree g; then, $D \sim D_0$, where D_0 is effective. If $D \geqslant 0$ and $d = g$, D is non-special divisor if and only if $\mathcal{L}(D) = \mathbb{F}_q$.*

2. *If $d = g - 1$, D is a non-special divisor if and only if $\dim(D) = 0$. A non-special divisor of degree $g - 1$, if any, is never effective.*

3. *If $g > 1$ and $A_{g-1} = 0$, then any divisor of degree $g - 1$ is non-special.*

A consequence of assertion 1 is the following.

Lemma 2.3. *Assume that D is an effective non-special divisor of degree $g \geqslant 1$. If there exists a degree one place P such that $P \notin \mathrm{supp}(D)$, then $D - P$ is a non-special divisor of degree $g - 1$.*

3 Existence of non-special divisors of degree g and $g - 1$

Unless otherwise specified, the results in this section come from [1] by S. Ballet and D. Le Brigand. They determine the necessary and sufficient conditions for the existence of non-special divisors of degree g and $g - 1$ in the general case and they apply them to the cases of $g = 1$ and $g = 2$.

3.1 General case

Here, we give some general results about non-special divisors of degree g and $g-1$.

Proposition 3.1. *Let* $\mathbf{F}/\mathbb{F}_q$ *be an algebraic function field of genus* $g \geqslant 1$.

1. *If* $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant g$, *there exists a non-special divisor* D *such that* $D \geqslant 0$, $\deg(D) = g$ *and* $\operatorname{supp}(D) \subset \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q)$.
2. *If* $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant g+1$, *there exists a non-special divisor such that* $\deg(D) = g-1$ *and* $\operatorname{supp}(D) \subset \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q)$.

Proof.

1. See [25, Proposition I.6.10].
2. Let $T \subset \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q)$ be such that $\#T = g$ and, using assertion 1, let $D \geqslant 0$ be a non-special divisor such that $\deg(D) = g$ and $\operatorname{supp}(D) \subset T$. Select $P \in \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q) \setminus \operatorname{supp}(D)$ and apply Lemma 2.3.

□

We denote by $\mathcal{E}_g$ and $\mathcal{E}_{g-1}$ the following properties:

$\mathcal{E}_g$: $\mathbf{F}/\mathbb{F}_q$ has an effective non-special divisor of degree g.

$\mathcal{E}_{g-1}$: $\mathbf{F}/\mathbb{F}_q$ has a non-special divisor of degree $g-1$.

If $\mathbf{F}/\mathbb{F}_q$ has enough rational places compared to the genus, then $\mathcal{E}_g$ and $\mathcal{E}_{g-1}$ are true.

Proposition 3.2. *Let* $\mathbf{F}/\mathbb{F}_q$ *be a function field of genus* g. *Denote by* h *the order of the divisor class group of* $\mathbf{F}/\mathbb{F}_q$.

1. *If* $A_g < h(q+1)$, *then* $\mathcal{E}_g$ *is true.*
2. *If* $A_{g-1} < h$, *then* $\mathcal{E}_{g-1}$ *is true.*
3. *Assume* $g \geqslant 2$. *If* $A_{g-2} < h$, *then* $\mathcal{E}_g$ *is true.*
4. *If* $g = 2$ *or* 3, $\mathcal{E}_g$ *is untrue if and only if* $A_{g-2} = h$.

Proof. Recall that, in any function field, there exists a degree 1 divisor (this is a result of F.K. Schmidt; see [25, Corollary V.1.11] for instance), so there exist divisors of any degree $\geqslant 1$. Let $d \geqslant 1$ and $D_0 \in \mathsf{D}_d^+(\mathbf{F}/\mathbb{F}_q)$, and consider the map

$$\psi_{d,D_0} : \begin{cases} \mathsf{D}_d^+(\mathbf{F}/\mathbb{F}_q) \longrightarrow \operatorname{Jac}(\mathbf{F}/\mathbb{F}_q) \\ \qquad\qquad D \longmapsto [D - D_0]. \end{cases}$$

1. First, it is well known that $1 \leqslant h \leqslant A_g$ is true for any function field. Indeed, let D be such that $\deg(D) = g$. By the Riemann–Roch, $\dim(D) \geqslant 1$; thus, there exists an effective divisor of degree g which is equivalent to D. So assume $D_0 \in \mathsf{D}_g^+(\mathbf{F}/\mathbb{F}_q)$ and consider the map ψ_{g,D_0}. For all $[R] \in \operatorname{Jac}(\mathbf{F}/\mathbb{F}_q)$, we have $\deg(R + D_0) = g$; thus, $\dim(R + D_0) \leqslant 1$ and there exists $u \in \mathbf{F}^*$ such that $D := R + D_0 + (u)$ is in

$\mathrm{D}_g^+(\mathbf{F}/\mathbb{F}_q)$ and $[R] = [D - D_0] = \psi_{g,D_0}(D)$. This proves that ψ_{g,D_0} is surjective and that $h \leqslant A_g$. Assume now that $\mathbf{F}/\mathbb{F}_q$ has no non-special divisor D of degree g. Then, $\dim(D) \geqslant 2$ for all degree g divisors; thus, for all $[R] \in \mathrm{Jac}(\mathbf{F}/\mathbb{F}_q)$, we have

$$\#\left\{D \in \mathrm{D}_g^+(\mathbf{F}/\mathbb{F}_q), [D - D_0] = [R]\right\} = \frac{q^{\dim(R+D_0)} - 1}{q-1} \geqslant \frac{q^2-1}{q-1} = q+1$$

and $A_g \geqslant h(q+1)$.

2. A divisor D of degree $g-1$ is non-special if and only if $\dim(D) = 0$. If $g = 1$, there exists a non-special divisor of degree $g - 1 = 0$ if and only if $h = B_1 > 1 = A_0$, since two distinct degree one places are not equivalent. Assume now that $g > 1$. Hence, it is sufficient to prove the existence of a divisor of degree $g - 1$ which is not equivalent to any effective divisor. If $A_{g-1} = 0$, the result is proved. Otherwise, let D_0 be an effective divisor of degree $g - 1 \geqslant 1$ and consider the map ψ_{g-1,D_0}. If $A_{g-1} < h$, this map is not surjective. Hence, there exists a zero-degree divisor R such that $[R]$ is not in the image of ψ_{g-1,D_0}. Consequently, $D = R + D_0$ is a divisor of degree $g - 1$ which is not equivalent to an effective divisor. Thus, D is non-special.

3. From the functional equation of the zeta function, it can be deduced (see [18, Lemma 3(i)]) that, for $g \geqslant 1$, one has

$$A_n = q^{n+1-g}A_{2g-2-n} + h\frac{q^{n+1-g}-1}{q-1} \qquad \text{for all} \qquad 0 \leqslant n \leqslant 2g-2.$$

For $g \geqslant 2$ and $n = g$ this gives

$$A_g = h + qA_{g-2}.$$

Thus, if $g \geqslant 2$,

$$A_g < (q+1)h \Longleftrightarrow A_{g-2} < h.$$

4. Assume that $g = 2$ or 3. Then if $\deg(D) = g$ and $\dim(D) \geqslant 2$, one has $\dim(D) = 2$ by assertion 7 of Proposition 2.1, since $\dim(D) \leqslant \frac{g}{2} + 1$. Thus, $\mathcal{E}_g$ is untrue if and only if $A_g = (q+1)h$, which is equivalent to $A_{g-2} = h$.

□

We quote the following consequence of assertion 2.

Corollary 3.3. *Let $\mathrm{F}/\mathbb{F}_q$ be an algebraic function field of genus $g \geqslant 2$ such that $A_{g-1} \geqslant 1$. Denote by h the order of the divisor class group of $\mathrm{F}/\mathbb{F}_q$. Then $\mathcal{E}_{g-1}$ is untrue if and only if there exist h elements of $\mathrm{D}_{g-1}^+(\mathbf{F}/\mathbb{F}_q)$ pairwise non-equivalent.*

Proof. Let r be the maximum number of pairwise non-equivalent elements of $\mathrm{D}_{g-1}^+(\mathbf{F}/\mathbb{F}_q)$ and let $D_1, \ldots, D_r$ be elements of $\mathrm{D}_{g-1}^+(\mathbf{F}/\mathbb{F}_q)$ pairwise non-equivalent. Then

$$\{[0] = [D_1 - D_1], [D_2 - D_1], \ldots, [D_r - D_1]\}$$

is a subset of $\mathrm{Jac}(\mathbf{F}/\mathbb{F}_q)$ of order r. If $r = h$, for any divisor D of degree $d = g - 1$, we have $[D - D_1] = [D_i - D_1]$ for some i, $1 \leqslant i \leqslant h$, and then $D \sim D_i$. Thus, $\dim(D) \geqslant 1$. If $r < h$, ψ_{g-1,D_1} is not surjective and the result follows. □

3.2 Existence of non-special divisors of degree g

Now, we particularly focus on the non-special divisors of degree g. First, we give useful properties and interesting information to study the existence of non-special divisors. For example, it is known that this existence is relied on the number of effective divisors of certain degrees A_n.

Lemma 3.4. *If $B_1 \geqslant m \geqslant 1$, then for all $n \geqslant 2$ one has*

$$A_n \geqslant mA_{n-1} - \frac{m(m-1)}{2}A_{n-2}. \tag{3}$$

Proof. See [18, Lemma 4]. □

Moreover, it is also related to the class number h of algebraic function fields.

Proposition 3.5. *Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g \geqslant 2$. We denote by h its divisor class number.*

- *Up to isomorphism, there are 4 function fields $\mathbf{F}/\mathbb{F}_q$, 2 of them being hyperelliptic, such that $h = 1$ and $g \geqslant 2$. They are obtained for $\mathbf{F} = \mathbb{F}_2(x, y)$ as in Table 1.*
- *Up to isomorphism, there are 15 functions fields $\mathbf{F}/\mathbb{F}_q$, 7 of them being hyperelliptic, such that $h = 2$ and $g \geqslant 2$.They are obtained for $\mathbf{F} = \mathbb{F}_2(x, y)$ as in Table 2.*

Proof. See [13] and [15] for the solutions of the ($h = 1$) problem and [12, Proposition 3.1 and Theorem 4.1] for the solutions of the ($h = 2$) problem. □

Proposition 3.6. *An algebraic function field $\mathbf{F}/\mathbb{F}_q$ of genus $g \geqslant 2$ has an effective non-special divisor of degree g in the following cases:*

(i) $q \geqslant 3$.

(ii) $q = 2$ *and* $g = 2$, *unless* $\mathbf{F} = \mathbb{F}_2(x, y)$ *with*

$$y^2 + y + (x^5 + x^3 + 1) = 0, \qquad \textit{and}$$
$$y^2 + y + (x^3 + x^2 + 1)/(x^3 + x + 1) = 0.$$

(iii) $q = 2$ *and* $g = 3$.

(iv) $q = 2$, $g \geqslant 4$ *and* $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 3$.

g	Equation	B_1	B_2	B_3
2	$y^2 + y + (x^5 + x^3 + 1) = 0$	1	2	
2	$y^2 + y + (x^3 + x^2 + 1)/(x^3 + x + 1) = 0$	0	3	
3	$y^4 + xy^3 + (x + 1)y + (x^4 + x^3 + 1) = 0$	0	0	1
3	$y^4 + xy^3 + (x + 1)y + (x^4 + x + 1) = 0$	0	1	1

Table 1: The four function fields for which $h = 1$ and $g \geqslant 2$.

q	g	Equation	B_1	B_2	B_3	B_4
3	2	$y^2 - 2(x^2 + 1)(x^4 + 2x^3 + x + 1) = 0$	1	5		
2	2	$y^2 + y + (x^3 + x + 1)/(x^2 + x + 1) = 0$	1	3		
		$y^2 + y + (x^4 + x + 1)/x = 0$	2	1		
2	3	$y^2 + y + (x^4 + x^3 + x^2 + x + 1)/(x^3 + x + 1) = 0$	1	2	1	
		$y^2 + y + (x^5 + x^2 + 1)/(x^2 + x + 1) = 0$	1	3	0	
		$y^2 + y + (x^6 + x + 1)/(x^2 + x + 1)^3 = 0$	0	4	2	
		$y^2 + y + (x^4 + x^3 + 1)/(x^4 + x + 1) = 0$	0	3	2	
		$y^4 + xy^3 + (x + 1)y + (x^4 + x^2 + 1) = 0$	0	2	2	
		$y^3 + (x^2 + x + 1)y + (x^4 + x^3 + 1) = 0$	1	0	3	
		$y^3 + y + (x^4 + x^3 + 1) = 0$	1	1	2	
2	4	$y^3 + (x^4 + x^3 + 1)y + (x^6 + x^3 + 1) = 0$	0	0	4	2
		$y^3 + (x^4 + x^2 + 1)y + (x^6 + x^5 + 1) = 0$	0	0	4	2
		$y^3 + (x^4 + x^3 + 1)y + (x^6 + x + 1) = 0$	0	1	3	3
		$y^6 + xy^5 + (x^2 + 1)y^4 + (x^3 + x^2)y^3$ $+(x^6 + x^5 + x^3 + x + 1) = 0$	0	1	1	3
		$y^6 + xy^5 + x^3y^3 + y^2 + (x^5 + x^2)y + (x^6 + x^2 + 1) = 0$	0	1	2	3

Table 2: The fifteen function fields for which $h = 2$ and $g \geqslant 2$.

Proof. We set $L(t) := L(\mathbf{F}/\mathbb{F}_q, t)$. For $g \geqslant 2$, it follows that (see [18, Lemma 3])

$$\sum_{n=0}^{g-2} A_n t^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n t^{2g-2-n} = \frac{L(t) - ht^g}{(1-t)(1-qt)}.$$

Substituting $t = q^{-1/2}$ into the last identity, we obtain

$$2\sum_{n=0}^{g-2} q^{-n/2} A_n + q^{-(g-1)/2} A_{g-1} = \frac{h - q^{g/2} L(q^{-1/2})}{\left(q^{1/2}-1\right)^2 q^{(g-1)/2}}$$

and, since $L(q^{-1/2}) = \prod_{i=1}^{g} \left|1 - \pi_i q^{-1/2}\right|^2 \geqslant 0$, we have

$$2\sum_{n=0}^{g-2} q^{(g-1-n)/2} A_n + A_{g-1} \leqslant \frac{h}{\left(q^{1/2}-1\right)^2}. \tag{4}$$

Now consider each case in turn:

(i) If $q \geqslant 3$. Using (4), $A_{g-2} \geqslant h$ implies

$$2q^{1/2} \leqslant \frac{1}{\left(q^{1/2}-1\right)^2},$$

which is absurd if $q \geqslant 3$. Thus, $A_{g-2} < h$ is always satisfied and so $\mathcal{E}_g$ is true.

(ii) If $q = 2$ and $g \geqslant 3$, (4) implies

$$4A_{g-3} + 2\sqrt{2}A_{g-2} + A_{g-1} \leqslant \frac{h}{\left(\sqrt{2}-1\right)^2} = \left(3 + 2\sqrt{2}\right) h. \tag{5}$$

Assume that $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant m = 3$; then, by (3) with $n = g-1$, we have $A_{g-1} + 3A_{g-3} \geqslant 3A_{g-2}$, and finally, using (5),

$$A_{g-3} + \left(3 + 2\sqrt{2}\right) A_{g-2} \leqslant \left(3 + 2\sqrt{2}\right) h.$$

Since $A_{g-3} \geqslant 1$, because if $g = 3$, $A_{g-3} = A_0 = 1$ and if $g > 3$, $A_{g-3} \geqslant B_1(\mathbf{F}/\mathbb{F}_q) \geqslant m = 3$, we deduce that, if $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 3$ and $g \geqslant 3$, then $A_{g-2} < h$ and so $\mathcal{E}_g$ is true.

(iii) If $q = 2$ and $g = 2$, using assertion (4) of Proposition 3.2. In fact, $\mathcal{E}_g$ is untrue if and only if $h = A_{g-2} = A_1 = B_1(\mathbf{F}/\mathbb{F}_q)$. Since $\mathcal{E}_g$ is true if $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 3$, we are left with $h = B_1(\mathbf{F}/\mathbb{F}_q) = 1$ or 2 and we deduce from Proposition 3.5 that there is no solution.

(iv) If $q = 2$ and $g = 2$, using assertion (4) of Proposition 3.2, $\mathcal{E}_g$ is untrue if and only if $h = A_{g-2} = A_0 = 1$. By Proposition 3.5 there are only two function fields $\mathbf{F}/\mathbb{F}_q$ of genus 2 such that $h = 1$. They are such that $q = 2$ and $\mathbf{F} = \mathbb{F}_2(x, y)$, with

- $y^2 + y + (x^5 + x^3 + 1) = 0$ and $B_1(\mathbf{F}/\mathbb{F}_q) = 1$, $B_2(\mathbf{F}/\mathbb{F}_q) = 2$.
- $y^2 + y + (x^3 + x^2 + 1)/(x^3 + x + 1) = 0$ and $B_1(\mathbf{F}/\mathbb{F}_q) = 0$, $B_2(\mathbf{F}/\mathbb{F}_q) = 3$.

Since $h = 1$, all divisors of a given degree $d > 0$ are equivalent. In particular, all the divisors of degree $g = 2$ are equivalent to any divisor of $\mathrm{D}_2^+(\mathbf{F}/\mathbb{F}_q)$, and therefore they are special.

□

The following lemma from H. Niederreiter and C. Xing in [18, Lemma 6] is another characterization of the existence of these divisors. This result is less precise than Proposition 3.6 and the proof is based on the same tools.

Lemma 3.7. *There exists an effective divisor D of $\mathbf{F}/\mathbb{F}_q$ with $\deg(D) = g$ and $\dim(D) = 1$ if either $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 2$ and $q \geqslant 3$, or $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 4$ and $q = 2$.*

Proof. The lemma is trivial for $g = 0$. If $g = 1$, let D be a rational place of $\mathbf{F}/\mathbb{F}_q$, then $\dim(D) = 1$. Now let $g \geqslant 2$. Suppose that $\dim(D) \geqslant 2$ for any positive divisor D with $\deg(D) = g$. If $g = 2$, then by [18, Lemma 3(i)] we have $A_2 = q + h$ and by [18, Lemma 5] we have $A_2 \geqslant (q+1)h$. Thus $h \leqslant 1$, which contradicts $h \geqslant A_1 \geqslant 2$.

So we may assume $g \geqslant 3$. Substituting $t = q^{-1/2}$ in the identity in [18, Lemma 3(ii)], we obtain

$$2\sum_{n=0}^{g-2} q^{-n/2}A_n + q^{-(g-1)/2}A_{g-1} = \frac{h - q^{g/2}L(q^{-1/2})}{\left(q^{1/2}-1\right)^2 q^{(g-1)/2}}.$$

Since

$$L(q^{-1/2}) = \prod_{j=1}^{g}\left|1 - \alpha_j q^{-1/2}\right|^2 \geqslant 0,$$

we infer that

$$2\sum_{n=0}^{g-2} q^{(g-1-n)/2}A_n + A_{g-1} \leqslant \frac{h}{\left(q^{1/2}-1\right)^2}. \tag{6}$$

Since [18, Lemma 3(i)] yields $A_g = h + qA_{g-2}$ and [18, Lemma 5] yields $A_g \geqslant (q+1)h$, we have $A_{g-2} \geqslant h$. From (6) we then get

$$2q^{1/2} \leqslant \frac{1}{\left(q^{1/2}-1\right)^2}.$$

This inequality is impossible if $q \geqslant 3$, hence it remains to prove the lemma for $q = 2$.

If $q = 2$ and $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 4$, then from (6) we obtain

$$4A_{g-3} + 2\sqrt{2}A_{g-2} + A_{g-1} \leqslant \frac{h}{\left(\sqrt{2}-1\right)^2}. \tag{7}$$

Together with [18, Lemma 4] with $m = 3$ and $n = g - 1$ this yields

$$A_{g-3} + \left(3 + 2\sqrt{2}\right) A_{g-2} \leqslant \frac{h}{\left(\sqrt{2} - 1\right)^2}. \tag{8}$$

if we use [18, Lemma 4] with $m = 4$ and $n = g - 1$ in (7), then we get

$$-2A_{g-3} + \left(4 + 2\sqrt{2}\right) A_{g-2} \leqslant \frac{h}{\left(\sqrt{2} - 1\right)^2}. \tag{9}$$

By eliminating A_{g-3} from (8) and (9), we arrive at

$$\left(10 + 6\sqrt{2}\right) A_{g-2} \leqslant \frac{3h}{\left(\sqrt{2} - 1\right)^2},$$

and therefore

$$10 + 6\sqrt{2} \leqslant \frac{3}{\left(\sqrt{2} - 1\right)^2},$$

which is absurd. □

3.3 Existence of non-special divisors of degree $g - 1$

In this section, we are interested in the non-special divisors of degree $g - 1$. We begin with the particular case where $g = 1$.

If the genus of $F/\mathbb{F}_q$ is $g = 1$, any divisor of degree $d = g$ is non-special since $d \geqslant 2g - 1 = 1$ and there exists a non-special divisor of degree $g - 1 = 0$ if and only if the divisor class number h is > 1, i.e. $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant 2$. So there are exactly three function fields of genus one which have no non-special divisor of degree $g - 1$. They are the elliptic solutions to the divisor class number one problem (see [14] and [15]):

$$\begin{aligned} q &= 2, & y^2 + y + (x^3 + x + 1) &= 0, & \\ q &= 3, & y^2 - (x^3 + 2x + 2) &= 0, & \\ q &= 4, & y^2 + y + (x^3 + a) &= 0, & \text{where } \mathbb{F}_4 = \mathbb{F}_2(a). \end{aligned}$$

So, in the rest of this paper, except otherwise stated, we consider function fields of genus at least two.

Theorem 3.8. *Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g \geqslant 2$. Then $\mathcal{E}_{g-1}$ is true in the following cases:*

(i) $q \geqslant 4$.

(ii) $g = 2$, *unless* $\mathbf{F}/\mathbb{F}_q := \mathbb{F}_2(x, y)/\mathbb{F}_2$, *with*

$$\begin{aligned} y^2 + y + (x^5 + x^3 + 1) &= 0, \qquad \textit{or} \\ y^2 + y + (x^4 + x + 1)/x &= 0. \end{aligned}$$

Proof. Recall that, $A_{g-1} = 0$, the existence is clear.

(i) Assume $q \geqslant 4$. By (4), for $g \geqslant 2$ we have:

$$A_{g-1} < 2q^{(g-1)/2}A_0 + A_{g-1} \leqslant 2\sum_{n=0}^{g-2} q^{(g-1-n)/2}A_n + A_{g-1} \leqslant \frac{h}{\left(q^{1/2}-1\right)^2}.$$

Thus, if $q \geqslant 4$, we have $A_{g-1} < h$ and the result follows from Proposition 3.2.

(ii) Assume $g = 2$. If $A_{g-1} = B_1(\mathbf{F}/\mathbb{F}_q) < h$, the result follows from Proposition 3.2. This is the case when $B_1(\mathbf{F}/\mathbb{F}_q) = 0$ and then all divisors of degree $g-1$ are non-special. If $B_1(\mathbf{F}/\mathbb{F}_q) \geqslant g+1 = 3$, the result is true by Proposition 3.1. The remaining cases are $B_1(\mathbf{F}/\mathbb{F}_q) = 1$ or 2 with $h = B_1(\mathbf{F}/\mathbb{F}_q)$. By Proposition 3.5, there are two solutions:

(a) $B_1(\mathbf{F}/\mathbb{F}_q) = 1$ and $h = 1$. There is a unique function field satisfying these conditions. It is $\mathbf{F}/\mathbb{F}_q := \mathbb{F}_2(x,y)/\mathbb{F}_2$, with

$$y^2 + y + (x^5 + x^3 + 1) = 0.$$

Since $h = 1$, all divisors of degree $g-1 = 1$ are equivalent to the place of degree 1; thus, they are special.

(b) $B_1(\mathbf{F}/\mathbb{F}_q) = 2$ and $h = 2$. There is a unique function field satisfying these conditions. It is $\mathbf{F}/\mathbb{F}_q := \mathbb{F}_2(x,y)/\mathbb{F}_2$, with

$$y^2 + y + (x^4 + x + 1)/x = 0.$$

Since the two degree one places are non-equivalent, it follows from Corollary 3.3 that $\mathcal{E}_{g-1}$ is untrue.

□

In the following lemma, the value of A_{g-1} is given in terms of coefficients of the polynomial $L(\mathbf{F}/\mathbb{F}_q, t)$.

Lemma 3.9. *Let* $\mathbf{F}/\mathbb{F}_q$ *be a function field of genus* g *and let* $L(t) = \sum_{i=0}^{2g} a_i t_i$ *be the numerator of its Zeta function. Then*

$$A_{g-1} = \frac{1}{q-1}\left(h - \left(a_g + 2\sum_{i=0}^{g-1} a_i\right)\right).$$

Proof. It is a well-known result that

$$Z(t) = \sum_{m=0}^{+\infty} A_m t^m = \frac{\sum_{i=0}^{2g} a_i t^i}{(1-t)(1-qt)}.$$

We deduce that for all $m \geqslant 0$,

$$A_m = \sum_{i=0}^{m} \frac{q^{m-i+1} - 1}{q - 1} a_i.$$

In particular,

$$(q-1)A_{g-1} = \sum_{i=0}^{g-1} \left(q^{g-i} - 1\right) a_i.$$

Since $a_i = q^{i-g} a_{2g-i}$, for all $i = 0, \ldots, g$, we obtain

$$(q-1)A_{g-1} = q^g \sum_{i=0}^{g-1} q^{-i} a_i - \sum_{i=0}^{g-1} a_i = q^g \sum_{i=0}^{g-1} q^{-i} q^{i-g} a_{2g-i} - \sum_{i=0}^{g-1} a_i.$$

Hence,

$$(q-1)A_{g-1} = \sum_{i=0}^{g-1} \left(a_{2g-i} - a_i\right).$$

Furthermore, we know that $h = L(1) = \sum_{i=0}^{2g} a_i$, therefore,

$$A_{g-1} = \frac{1}{q-1} \left(h - \left(a_g + 2 \sum_{i=0}^{g-1} a_i \right) \right).$$

□

The preceding lemma, Corollary 3.3 and Assertion 2 of Proposition 3.2 yield:

Corollary 3.10. *Let* $\mathrm{F}/\mathbb{F}_q$ *be a function field of genus* g *and* $L(t) = \sum_{i=0}^{2g} a_i t^i$ *be the L-polynomial of* $\mathrm{F}/\mathbb{F}_2$*. Then*

- *For* $q \geqslant 3$, $a_g + 2\sum_{i=0}^{g-1} a_i \geqslant 0$ *if and only if* $\mathcal{E}_{g-1}$ *is true.*
- *For* $q = 2$, $a_g + 2\sum_{i=0}^{g-1} a_i > 0$ *if and only if* $\mathcal{E}_{g-1}$ *is true.*

Example 3.11. The Hermitian function field $\mathrm{F}/\mathbb{F}_{q^2}$ is such that $\mathrm{F} = \mathbb{F}_q(x, y)$ with $y^q + y - x^{q+1} = 0$. It is a maximal function field of genus $g = \frac{q(q-1)}{2}$ and it is the constant field extension of $\mathrm{G}/\mathbb{F}_q$, where $\mathrm{G} = \mathbb{F}_q(x, y)$, with $y^q + y - x^{q+1} = 0$. We can say that $\mathrm{G}/\mathbb{F}_q$ is a "constant field restriction" of $\mathrm{F}/\mathbb{F}_{q^2}$. All subfields of the Hermitian function field $\mathrm{F}/\mathbb{F}_{q^2}$ are maximal function fields.

Corollary 3.12. *If the algebraic function field* $\mathrm{G}/\mathbb{F}_q$ *is a constant field restriction of a maximal function field* $\mathrm{F}/\mathbb{F}_{q^2} = \mathrm{G}.\mathbb{F}_{q^2}/\mathbb{F}_{q^2}$*, then* $\mathrm{G}/\mathbb{F}_q$ *contains a non-special divisor of degree* $g - 1$.

3.4 Particular cases : ordinary curves over $\mathbb{F}_2$ and $\mathbb{F}_3$

The following results treat the particular case of ordinary curves in [3, Section 4].

Let C/k be a genus g (smooth projective absolutely irreducible) curve defind over a finite field $k = \mathbb{F}_{p^n}$. Classically, one defines the p-rank γ of this curve as the integer $0 \leqslant \gamma \leqslant g$ such that $\#\mathrm{Jac}(\mathrm{C})[p](\overline{k}) = p^\gamma$. In particular C is said to be ordinary if $\gamma = g$. There is another equivalent characterization in terms of the L-polynomial, namely $\gamma = \deg(L(t) \bmod p)$, see [16]. In particular, C is ordinary if and only if p does not divide a_g.

Proposition 3.13. *Let* C *be an ordinary curve of genus $g > 0$ over a finite field k of characteristic* 2. *There is always a non-special divisor of degree $g - 1$ on* C.

Proof. Let $f \in k(\mathrm{C})$ such that $df \neq 0$. Developing f in power series at any point of C, we see that df has only zeros and poles of even multiplicity. Hence there exists a rational divisor of degree $(2g-2)/2 = g-1$ such that $(df) = 2D_0$. It is easy to show that the class of this divisor does not depend on the choice of f and it is called the canonical theta characteristic divisor. In [26, Prop.3.1], it is shown that there is a bijection between $\mathcal{L}(D_0)$ and the space of exact regular differentials (i.e. the regular differentials ω such that $\omega = df$ for $f \in k(\mathrm{C})$). Now by [22, Prop.8], a regular differential ω is exact if and only if $C(\omega) = 0$ where C is the Cartier operator. Moreover by [22, Prop.10], Jac(C) is ordinary if and only if C is bijective. So the only exact regular differential is 0 and $\dim(D_0) = 0$. Hence D_0 is the divisor we were looking for. □

Note, that the previous proof gives a way to explicitly construct a degree $g - 1$ divisor of dimension zero. We will now generalize Proposition 3.13 (and Lemma 3.9) but without such an explicit construction.

Lemma 3.14. *Let* $\mathrm{F}/\mathbb{F}_q$ *be a function field of genus g and let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the numerator of its Zeta function. Then*

$$A_{g-k} = \frac{1}{q-1}\left[q^{-k+1}\left(h - \sum_{i=0}^{g+k-1} a_i\right) - \sum_{i=0}^{g-k} a_i\right].$$

Proof. The proof is similar to Lemma 3.9 (see [3, Lemma 3.6]). □

Proposition 3.15. *Let* C *be a curve of genus $g > 0$ defined over a finite field $\mathbb{F}_q$ of characteristic p and of p-rank γ. There is always a degree $\gamma - 1$ zero dimension divisor on* C.

Proof. Recall that if $h_{n,k}$ denotes the number of classes of divisors of degree n and of dimension k, for all $g \geqslant k > 0$, we get

$$h = \sum_{i=0}^{\infty} h_{g-k,i}$$

so

$$h_{g-k,0} = h - \sum_{i=1}^{\infty} h_{g-k,i}.$$

Now

$$A_{g-k} = \sum_{i=1}^{\infty} \frac{q^i - 1}{q-1} h_{g-k,i}$$

hence we can write

$$\sum_{i=1}^{\infty} h_{g-k,i} = \sum_{i=1}^{\infty} q^i h_{g-k,i} - (q-1)A_{g-k}.$$

Using the expression of A_{g-k} from Lemma 3.14 and

$$h = \sum_{i=0}^{g+k-1} a_i + \sum_{i=g+k}^{2g} a_i \equiv \sum_{i=0}^{\gamma} a_i \pmod p$$

we get, for $k = g - \gamma + 1$,

$$\begin{aligned} h_{g-k,0} &= h\left(1 + q^{-k+1}\right) - q^{-k+1} \sum_{i=0}^{g+k-1} a_i - \sum_{i=0}^{g-k} a_i - \sum_{i=1}^{\infty} q^i h_{g-k,i} \\ &= \sum_{i=0}^{2g} a_i + q^{-k+1} \sum_{i=g+k}^{2g} a_i - \sum_{i=0}^{g-k} a_i - \sum_{i=1}^{\infty} q^i h_{g-1,i} \\ &= \sum_{i=g-k+1}^{2g} a_i + q^{-k+1} \sum_{i=g+k}^{2g} a_i - \sum_{i=1}^{\infty} q^i h_{g-1,i} \\ &\equiv \sum_{i=g-k+1}^{\gamma} a_i \pmod p \\ &\equiv a_\gamma \not\equiv 0 \pmod p. \end{aligned}$$

Hence $h_{\gamma-1,0}$ is not zero and hence is positive. □

Remark 3.16. Note that this proposition is interesting only in the case where $q = 2$ and $\gamma = g - k$ with $k \leqslant 3$ or $q = 3$ and $\gamma = g$.

Corollary 3.17. *Let* C *be an ordinary curve of genus $g > 0$ over a finite field $\mathbb{F}_q$. There is always a non-special divisor of degree $g - 1$ on* C.

3.5 Particular case : Asymptotically exact towers

In this section we adapt the results in [3, Section 5.2] to prove the existence of non-special divisors of degree $g - 1$ in asymptotically exact towers.

First, let us recall the notion of asymptotically exact sequence of algebraic function fields introduced in [27].

Definition 3.18. *Consider a sequence $\mathcal{F}/\mathbb{F}_q = (\mathrm{F}_k/\mathbb{F}_q)_{k\geqslant 1}$ of algebraic function fields $\mathrm{F}_k/\mathbb{F}_q$ defined over $\mathbb{F}_q$ of genus g_k. We suppose that the sequence of genus g_k is an increasing sequence growing to infinity. The sequence $\mathcal{F}/\mathbb{F}_q$ is called* asymptotically exact *if, for all $m \geqslant 1$, the following limit exists:*

$$\beta_m(\mathcal{F}/\mathbb{F}_q) = \lim_{g_k\to\infty} \frac{B_m(\mathrm{F}_k/\mathbb{F}_q)}{g_k}$$

where $B_m(\mathrm{F}_k/\mathbb{F}_q)$ is the number of places of degree m on $\mathrm{F}_k/\mathbb{F}_q$.

Now, let us recall the following two results used by I. Shparlinski, M. Tsfasman and S. Vladut in [24]. These results follow easily from Corollary 2 and Theorem 6 of [27].

Lemma 3.19. *Let $\mathcal{F}/\mathbb{F}_q = (\mathrm{F}_k/\mathbb{F}_q)_{k\geqslant 1}$ be an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_q$ and h_k be the class number of $\mathrm{F}_k/\mathbb{F}_q$. Then*

$$\log_q h_k = g_k \left(1 + \sum_{m=1}^{\infty} \beta_m \cdot \log_q \frac{q^m}{q^m - 1}\right) + o(g_k)$$

Lemma 3.20. *Let A_{a_k} be the number of effective divisors of degree a_k on $\mathrm{F}_k/\mathbb{F}_q$. If*

$$a_k \geqslant g_k \left(\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m - 1}\right) + o(g_k)$$

then

$$\log_q A_{a_k} = a_k + g_k \cdot \sum_{m=1}^{\infty} \beta_m \cdot \log_q \frac{q^m}{q^m - 1} + o(g_k).$$

These asymptotic properties were established in [27] and [28] in order to estimate the class number h of algebraic function fields of genus g defined over $\mathbb{F}_q$ and also in order to estimate their number of classes of effective divisors of degree $m \leqslant g - 1$. Namely, I. Shparlinski, M. Tsfasman and S. Vladut used in [24] the inequality $2A_{g_k(1-\varepsilon)} < h_k$ where $0 < \varepsilon < \frac{1}{2}$ and k big enough, under the hypothesis of Lemma 3.19. In the same spirit, we give here a particular case of their result in the following proposition.

Proposition 3.21. *Let $\mathcal{F}/\mathbb{F}_q = (\mathrm{F}_k/\mathbb{F}_q)_{k\geqslant 1}$ be an asymptotically exact sequence of algebraic function field defined over $\mathbb{F}_q$. Then, there exists an integer k_0 such that for any integer $k \geqslant k_0$, we get:*

$$A_{g_k - 1} < h_k$$

and there is a non-special divisor of degree $g - 1$ in $\mathrm{F}_k/\mathbb{F}_q$.

Proof. The total number of linear equivalence classes of an arbitrary degree equals to the divisor class number h_k of $\mathrm{F}_k/\mathbb{F}_q$, which is given by Lemma 3.19. Moreover, for g_k sufficiently large, we have:

$$\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m - 1} \leqslant \frac{1}{\sqrt{q}+1} \sum_{m=1}^{\infty} \frac{m\beta_m}{q^{\frac{m}{2}} - 1} < \frac{1}{2}$$

since $q \geqslant 2$ and $\sum_{m=1}^{\infty} \frac{m\beta_m}{q^{\frac{m}{2}}-1} \leqslant 1$ by Corollary 1 of [27]. As $\frac{1}{g_k} < \frac{1}{2}$, one has

$$g_k\left(1 - \frac{1}{g_k}\right) \geqslant g_k\left(\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m - 1}\right) + o(g_k)$$

for k big enough. Therefore, we can apply Lemma 3.20 and compare $\log_q A_{g_k(1-1/g_k)}$ with $\log_q h_k$ given by Lemma 3.19. Hence, there exists an integer k_0 such that for $k \geqslant k_0$, $A_{g_k-1} < h_k$. We conclude by Proposition 3.2. □

3.6 Particular case : curves of defect k over $\mathbb{F}_2$ and $\mathbb{F}_3$

In this section, we will focus on curves over $\mathbb{F}_2$ and $\mathbb{F}_3$ of genus $g \geqslant 3$. The existence of non-special divisors of degree $g-1$ is assured for $q \geqslant 4$, moreover, the cases of curves of genus $g = 1, 2$ were studied in the introduction of section 3.3 and Theorem 3.8. The goal is to give some examples of function fields that contain these divisors.

For $r \geqslant 1$, consider the number

$$N_r := N(\mathbf{F}_r) = \#\left\{P \in \mathrm{P}(\mathbf{F}_r/\mathbb{F}_{q^r}) : \deg(P) = 1\right\}$$

where $\mathbf{F}_r = \mathbf{F}\mathbb{F}_{q^r}$ is the constant field extension of $\mathbf{F}/\mathbb{F}_q$ of degree r. Let us remind the equation from [25, Corollary 5.1.16]: for all $r \geqslant 1$, we have

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r = q^r + 1 - \sum_{i=1}^{g} 2q^{r/2} cos(\pi r \phi_i) \tag{10}$$

where $(\alpha_1, \ldots, \alpha_{2g}) = (q^{1/2}e^{i\pi\phi_1}, \ldots, q^{1/2}e^{i\pi\phi_g}, q^{1/2}e^{-i\pi\phi_1}, \ldots, q^{1/2}e^{-i\pi\phi_g})$ are the reciprocals of the roots of $L(t)$ with $\phi_i \in [0, 1]$. In particular, since $N_1 = N(\mathbf{F})$, we have

$$N(\mathbf{F}) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Proposition 3.22 ([25, Corollary 5.1.17]). *Let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the L-polynomial of $\mathbf{F}/\mathbb{F}_q$, and $S_r := N_r - (q^r + 1)$. Then we have:*

(a) $L'(t)/L(t) = \sum_{r=1}^{\infty} S_r t^{r-1}$.

(b) $a_0 = 1$ *and*

$$ia_i = S_i a_0 + S_{i-1}a_1 + \cdots + S_1 a_{i-1} \tag{11}$$

for $i = 1, \ldots, g$.

Given $N_1, \ldots, N_g$ and using $a_{2g-i} = q^{g-i}a_i$, we can determine $L(t)$ from (11).

Let $\mathbf{F}$ be an algebraic function field over $\mathbb{F}_2$ or $\mathbb{F}_3$ of genus g, and k its defect, i.e.,

$$|N_1(\mathbf{F}/\mathbb{F}_2) - (q + 1)| = g\left[2\sqrt{q}\right] - k$$

where $[x]$ denotes the largest integer $\leqslant x$. Let

$$L(t) = \sum_{i=0}^{2g} a_i t^i = \prod_{i=1}^{g} [(1 - \alpha_i t)(1 - \overline{\alpha_i} t)]$$

be the numerator of the Zeta function of $\mathbf{F}$. Recall that with the previous conditions, one has

$$\left|N_1(\mathbf{F}/\mathbb{F}_q) - (q+1)\right| = \left|-\sum_{i=1}^{2g} \alpha_i\right| = g\left[2\sqrt{q}\right] - k$$

and then

$$k = g\left[2\sqrt{q}\right] - \left|\sum_{i=1}^{2g} \alpha_i\right|. \tag{12}$$

We know that, if $N_1 \geqslant g + 1$, there exists a non-special divisor of degree $g - 1$. Moreover we know all the curves which contain this kind of divisors over $\mathbb{F}_2$ for $g = 1$ and 2. Since for defect-2 curves over $\mathbb{F}_2$ with $g \geqslant 3$ one has

$$|N_1 - 3| = 2g - 2 \quad \Longrightarrow \quad N_1 = 2g + 1 \quad \Longrightarrow \quad N_1 \geqslant g + 1,$$

the existence of these divisors is obvious and we do not need to use the coefficients a_n for this purpose. Nevertheless, for a defect $k \geqslant 3$ curves over $\mathbb{F}_2$ and $\mathbb{F}_3$ ($q = 2$ or 3, hence $\left[2\sqrt{q}\right] = q$), one has

$$|N_1 - (q+1)| = qg - k \quad \Longrightarrow \quad N_1 = -qg + k + q + 1 \text{ or } N_1 = qg - k + q + 1.$$

The goal of this section is to prove the existence of non-special divisor of degree $g - 1$ for curves that satisfy

$$0 \leqslant N_1 = -qg + k + q + 1 \leqslant g \quad \text{or} \quad 0 \leqslant N_1 = qg - k + q + 1 \leqslant g. \tag{13}$$

The following results generalize the cases (a) and (d) of [23, Theorem 2.5.1] by J.-P. Serre and will help us determine the sign of $a_g + 2\sum_{i=0}^{g-1} a_i$ (in order to apply 3.10).

Lemma 3.23. *Let α be a totally positive algebraic integer and $\mathrm{k}(\alpha) = Tr(\alpha) - d(\alpha)$ (recall that $Tr(\alpha)$ is the sum of the conjugates of α, it is totally positive if all its conjugates are real > 0, that $d(\alpha)$ is the degree of its minimal polynomial and $Tr(\alpha) \geqslant d(\alpha)$ (see [23, Remark 2.2.3])). One has:*

- *If $\mathrm{k}(\alpha) = 0$, then $\alpha = 1$.*
- *If $d(\alpha) = 1$, then $\alpha = \mathrm{k}(\alpha) + 1$.*
- *If $d(\alpha) = 2$, then $\alpha = \frac{\mathrm{k}(\alpha)+2\pm\sqrt{(\mathrm{k}(\alpha)+2)^2-4n}}{2}$ with $\frac{(\mathrm{k}(\alpha)+2)^2}{4} > n$.*

Proof.
- For the case $\mathrm{k}(\alpha) = 0$ see [23, Corollary 2.2.4].

- If $d(\alpha) = 1$, then the minimal polynomial of α is $x - Tr(\alpha)$ and $\alpha = Tr(\alpha)$, we conclude that $\mathrm{k}(\alpha) = Tr(\alpha) - 1 = \alpha - 1$.
- If $d(\alpha) = 2$, then the minimal polynomial of α is $x^2 - Tr(\alpha)x + n = x^2 - (\mathrm{k}(\alpha) + 2)x + n$ with real positive roots, namely $\frac{\mathrm{k}(\alpha)+2\pm\sqrt{(\mathrm{k}(\alpha)+2)^2-4n}}{2}$ only if $\frac{(\mathrm{k}(\alpha)+2)^2}{4} > n$. □

Theorem 3.24. *For a curve over $\mathbb{F}_q$ such that $\left|N_1(\mathrm{F}/\mathbb{F}_q) - (q+1)\right| = g\left[2\sqrt{q}\right] - k$ with $g \geqslant 2$, one has*

(a) For $3 \leqslant k \leqslant 2 \cdot \left[2\sqrt{q}\right]$, if there exists $i \in \{1, \ldots, g\}$ such that $\alpha_i + \overline{\alpha_i} = \left[2\sqrt{q}\right] - k$, then we can reorganize the tuple $(\alpha_1 + \overline{\alpha_1}, \ldots, \alpha_g + \overline{\alpha_g})$ to get

$$(\alpha_1 + \overline{\alpha_1}, \ldots, \alpha_g + \overline{\alpha_g}) = \pm\left(\left[2\sqrt{q}\right], \ldots, \left[2\sqrt{q}\right], \left[2\sqrt{q}\right] - k\right)$$

(b) If there exist $i, j \in \{1, \ldots, g\}$ such that $\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}$ and $\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}$ are conjugate with $d\left(\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}\right) = 2$ and

$$\alpha_i + \overline{\alpha_i} + \alpha_j + \overline{\alpha_j} = 2\left[2\sqrt{q}\right] - k$$

then we can reorganize the tuple $(\alpha_1 + \overline{\alpha_1}, \ldots, \alpha_i + \overline{\alpha_i}, \ldots, \alpha_g + \overline{\alpha_g})$ to get

$$\begin{aligned}&(\alpha_1 + \overline{\alpha_1}, \ldots, \alpha_g + \overline{\alpha_g})\\ &= \pm\left(\left[2\sqrt{q}\right], \ldots, \left[2\sqrt{q}\right], \left[2\sqrt{q}\right] + 1 - \frac{k+2+\Delta}{2}, \left[2\sqrt{q}\right] + 1 - \frac{k+2-\Delta}{2}\right)\end{aligned}$$

with $\Delta = \sqrt{(k+2)^2 - 4n}$ and $\frac{(k+2)^2}{4} > n$.

This holds for $-2\left(2\sqrt{q} - \left[2\sqrt{q}\right]\right) \leqslant k \pm \Delta \leqslant 4\sqrt{q} + 2\left[2\sqrt{q}\right]$.

Proof. It is enough to prove the proposition in the case $N_1(\mathrm{F}/\mathbb{F}_q) - (q+1) = g\left[2\sqrt{q}\right] - k$ which means $k = g\left[2\sqrt{q}\right] - \sum_{i=1}^{2g} \alpha_i$ by (12).

Let $\kappa : \mathbb{Z}[X] \to \mathbb{Z}$ be the map defined by

$$\kappa\left(b_0X^n - b_1X^{n-1} + \ldots + b_n\right) = b_1 - n$$

and $P \in \mathbb{Z}[X]$ be the polynomial

$$P(X) = X^g - a_1X^{g-1} + \ldots + a_g = \prod_{i=1}^{g}\left(X - \left[2\sqrt{q}\right] - 1 + \alpha_i + \overline{\alpha_i}\right);$$

its roots are real and positive since $\left[2\sqrt{q}\right] + 1 \geqslant \alpha_i + \overline{\alpha_i} = 2\sqrt{q} \cdot cos(\pi\phi_i)$ with $\pi\phi_i$ the argument of α_i. Then we have

$$\kappa(P(X)) = \sum_{i=1}^{g}\left(\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}\right) - g = g\left[2\sqrt{q}\right] + g - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i}) - g = k.$$

Now, let $P(X) = \prod_{\lambda=1}^{r} Q_\lambda(X) = \prod_{\lambda=1}^{r}\left(X^{\deg(Q_\lambda)} - a_{1,\lambda}X^{\deg(Q_\lambda)-1} + \ldots\right)$ be the decomposition of P as a product of irreducible polynomials. We have

$$a_1 = \sum_{\lambda=1}^{r} a_{1,\lambda} \qquad \text{and} \qquad a_1 - g = \sum_{\lambda=1}^{r} a_{1,\lambda} - \sum_{\lambda=1}^{r} \deg(Q_\lambda);$$

thus

$$\kappa(P(X)) = \sum_{\lambda=1}^{r} \kappa\left(Q_\lambda(X)\right) = k. \tag{14}$$

(a) Let $i \in \{1, \ldots, g\}$ be such that $\alpha_i + \overline{\alpha_i} = \left[2\sqrt{q}\right] - k$, then $\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i} \in \mathbb{Z}$ which means that there exists $\lambda' \in \{1, \ldots, r\}$ such that $Q_{\lambda'}(X) = X - \left[2\sqrt{q}\right] - 1 + \alpha_i + \overline{\alpha_i}$. Thus $d\left(\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}\right) = 1$ and $\mathrm{Tr}\left(\left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}\right) = \left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}$. By (14), we have

$$\begin{aligned}
\kappa(P(X)) &= \sum_{\lambda=1}^{r} \kappa\left(Q_\lambda(X)\right) \\
&= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + \kappa\left(Q_{\lambda'(X)}\right) \\
&= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + \left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i} - 1 \\
&= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + \left[2\sqrt{q}\right] - \left[2\sqrt{q}\right] + k \\
&= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + k = k.
\end{aligned}$$

Notice that if $\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}$ is a root of Q_λ where $\lambda \neq \lambda'$ then, with the notation of Lemma 3.23, one has

$$\begin{aligned}
\kappa\left(Q_\lambda(X)\right) &= \mathrm{Tr}\left(\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}\right) - d\left(\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}\right) \\
&= \mathrm{k}\left(\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}\right) \geqslant 0
\end{aligned}$$

We conclude that $\kappa\left(Q_\lambda(X)\right) = \mathrm{k}\left(\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}\right) = 0$ for $\lambda \neq \lambda'$. By Lemma 3.23, one has $\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j} = 1$ thus $\left[2\sqrt{q}\right] = \alpha_j + \overline{\alpha_j}$ for $j \neq i$ and, by assumption, $\alpha_i + \overline{\alpha_i} = \left[2\sqrt{q}\right] - k$. Finally, the argument θ_i with $2\sqrt{q} \cdot cos(\theta_i) = \alpha_i + \overline{\alpha_i} = \left[2\sqrt{q}\right] - k$ exists if $0 \leqslant k \leqslant 2 \cdot \left[2\sqrt{q}\right]$. We are interested, here, by $3 \leqslant k \leqslant 2 \cdot [2\sqrt{q}]$ since the cases 0, 1 and 2 were studied in [23, Theorem 2.5.1].

(b) Let $\beta_i = \left[2\sqrt{q}\right] + 1 - \alpha_i - \overline{\alpha_i}$ and $\beta_j = \left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}$.
There exists $\lambda' \in \{1, \dots, r\}$ such that

$$\begin{aligned} Q_{\lambda'}(X) &= X^2 - a_{1,\lambda'}X + a_{2,\lambda'} \qquad \text{with} \\ a_{1,\lambda'} &= \operatorname{Tr}(\beta_i) = \operatorname{Tr}(\beta_j) = 2\left[2\sqrt{q}\right] + 2 - \alpha_i - \overline{\alpha_i} - \alpha_j - \overline{\alpha_j} \end{aligned}$$

By (14), one has

$$\begin{aligned} \kappa(P(X)) &= \sum_{\lambda=1}^{r} \kappa(Q_\lambda(X)) \\ &= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + \kappa\left(Q_{\lambda'(X)}\right) \\ &= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + 2\left[2\sqrt{q}\right] + 2 - \alpha_i - \overline{\alpha_i} - \alpha_j - \overline{\alpha_j} - 2 \\ &= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + 2\left[2\sqrt{q}\right] - 2\left[2\sqrt{q}\right] + k \\ &= \sum_{\substack{\lambda=1 \\ \lambda\neq\lambda'}}^{r} \kappa\left(Q_\lambda(X)\right) + k = k. \end{aligned}$$

As in (a), we conclude that $\kappa\left(Q_\lambda(X)\right) = \mathrm{k}\left(\left[2\sqrt{q}\right] + 1 - \alpha_j - \overline{\alpha_j}\right) = 0$ for $\lambda \neq \lambda'$ and since $d(\beta_i) = d(\beta_j) = 2$, by Lemma 3.23 one has

$$\beta_i = \frac{\mathrm{k}(\beta_i) + 2 - \sqrt{(\mathrm{k}(\beta_i) + 2)^2 - 4n}}{2} = \frac{k + 2 + \sqrt{(k+2)^2 - 4n}}{2}$$

and

$$\beta_j = \frac{\mathrm{k}(\beta_j) + 2 - \sqrt{(\mathrm{k}(\beta_j) + 2)^2 - 4n}}{2} = \frac{k + 2 - \sqrt{(k+2)^2 - 4n}}{2}$$

thus $\alpha_i + \overline{\alpha_i} = \left[2\sqrt{q}\right] + 1 - \frac{k+2+\Delta}{2}$ and $\alpha_j + \overline{\alpha_j} = \left[2\sqrt{q}\right] + 1 - \frac{k+2-\Delta}{2}$.
Finally, the arguments θ_i, θ_j with $2\sqrt{q}\cdot cos(\theta_i) = \alpha_i + \overline{\alpha_i}$ and $2\sqrt{q}\cdot cos(\theta_j) = \alpha_j + \overline{\alpha_j}$ exist if

$$-1 \leqslant \frac{[2\sqrt{q}] + 1 - \frac{k+2\pm\Delta}{2}}{2\sqrt{2}} \leqslant 1$$

which means

$$-2(2\sqrt{q} - [2\sqrt{q}]) \leqslant k \pm \Delta \leqslant 4\sqrt{q} + 2[2\sqrt{q}].$$

□

q	g	k	$\mathcal{E}_{g-1}$
2	3	3	True
2	3	4	True
3	3	5	True
3	3	6	True

Table 3: Whether specific function fields admit a non-special divisor of degree $g - 1$.

Remark 3.25. The conditions of Theorem 3.24 are too constraining but they describe possibly infinitely many curves if we refer to [23, Theorem 2.4.1].

Theorem 3.26. *Let $\left\{\alpha_1 + \overline{\alpha_1}, \ldots, \alpha_g + \overline{\alpha_g}\right\}$ be a set of algebraic integers. Suppose that the polynomial $\prod_{i=1}^{g} (X - \alpha_i - \overline{\alpha_i})$ can be factored as $P_1 \cdot P_2$ such that P_1 and P_2 are monic, non constant polynomials in $\mathbb{Z}[X]$ and their resultant is equal to 1 or -1. Then the $(\alpha_i)_{1 \leqslant i \leqslant g}$ can not come from a curve.*

Now, we have enough information to calculate the sum $a_g + 2\sum_{i=0}^{g-1} a_i$ using (10) and Proposition 3.22, in order to apply Corollary 3.10. Therefore, under the conditions of (13), case (a) of Theorem 3.24, and Theorem 3.26, we can build Table 3.

Furthermore, under the conditions of (13), case (b) of Theorem 3.24, and Theorem 3.26, we can build Table 4.

In the table provided, we present the signs of the sum $a_g + 2\sum_{i=0}^{g-1} a_i$ for curves with defect $k > 2$. These results were obtained through direct computation, without a formal proof. However, it is worth noting that these signs can be theoretically established using the same method developed in [11] for curves with defect 2. That method relies on an explicit form of the coefficients of the L-polynomial, which provides a rigorous framework for extending these results to higher defect values, should one wish to pursue a theoretical proof.

4 Construction of non-special divisors of degree g and $g - 1$

In this section, we focus on constructing non-special divisors of degrees g and $g - 1$ in different contexts. We divide the section into three examples to show how the methods can be applied. The first example looks at Kummer extensions and Hermitian curves, where we use their specific algebraic properties to build the divisors. The second example works with an asymptotically good tower, showing how the construction benefits from the tower's properties. Finally, the third example deals with a case where the curve has a large number of points, which makes the construction easier.

q	g	k	n	$\mathcal{E}_{g-1}$
2	3	3	1	False
2	3	3	2	True
2	3	3	4	True
2	3	3	6	False
2	3	4	1	True
2	3	4	2	False
2	3	4	3	False
2	3	4	5	True
2	3	4	7	True
2	3	4	8	True
2	3	4	9	True
2	3	5	8	True
2	4	5	8	True
2	3	5	9	True
2	4	5	9	True
2	3	5	10	True
2	4	5	10	True
2	3	5	11	True
2	4	5	11	True
2	3	5	12	True
2	4	5	12	True
2	3	6	13	True
2	4	6	13	True
2	3	6	14	True
2	4	6	14	True
2	3	6	15	True
2	4	6	15	True
2	3	6	16	True
2	4	6	16	True
2	3	7	19	True
2	4	7	19	True
2	5	7	19	True
2	3	7	20	True
2	5	8	25	True
2	4	7	20	True
2	5	7	20	True
2	3	8	25	True
2	4	8	25	True
3	3	5	4	True
3	3	5	6	True
3	3	5	8	True
3	3	5	9	False
3	3	5	10	False
3	3	5	11	False
3	3	5	12	False
3	3	6	4	False
3	3	6	5	False
3	3	6	7	True
3	3	6	9	True
3	3	6	10	True
3	3	6	11	True
3	3	6	12	True
3	3	6	13	True
3	3	6	14	True
3	3	6	15	True
3	3	6	16	True
3	3	7	12	False
3	3	7	13	False
3	3	7	14	False
3	3	7	15	False
3	3	7	16	True
3	3	7	17	True
3	3	7	18	True
3	3	7	19	True
3	3	7	20	True
3	3	8	19	True
3	4	8	23	True
3	4	8	19	True
3	3	8	20	False
3	4	8	20	False
3	3	8	21	True
3	4	8	21	True
3	3	8	22	True
3	4	8	22	True
3	3	8	23	True
3	3	8	24	True
3	4	8	24	True
3	3	8	25	True
3	4	8	25	True
3	3	9	27	True
3	4	9	27	True
3	3	9	28	False
3	4	9	28	False
3	3	9	29	True
3	4	9	29	True
3	3	9	30	True
3	4	9	30	True
3	3	10	34	True
3	4	10	34	True
3	3	10	35	True
3	4	10	35	True
3	3	10	36	True
3	4	10	36	True
3	3	11	42	True
3	4	11	42	True
3	5	11	42	True
3	3	12	49	True
3	4	12	49	True
3	5	12	49	True

Table 4: Whether specific function fields admit a non-special divisor of degree $g - 1$ where g is the genus, k the defect and n the integer defined in Lemma 3.23.

4.1 Example on Kummer extension and hermitian curves

This subsection presents the work of E. Camps Moreno, H. H. Lopez and G. L. Matthews in [17] which is based on the Weierstrass semigroup to find the explicit form of non-special divisors of degree g and $g-1$ on Kummer extensions and Hermitian curves.

For a curve C defined by $f(y) = g(x)$ over a finite field $\mathbb{F}_q$, we denote P_{ab} a point on C corresponding to $x = a$ and $y = b$. If C has a unique point at infinity, we denote it by P_∞.

We say that a divisor A is supported by a point $P \in \mathrm{C}$ if and only if $v_P(A) \neq 0$.

Consider m distinct rational points $P_1, \dots, P_m$ on a curve $\mathbf{C}$. The Weierstrass semigroup associated with the m-tuple of points is defined as the set of all tuples $\alpha \in \mathbb{N}^m$ for which there exists a function $f \in \mathrm{C}(\mathbb{F}_q)$ such that the pole divisor of f satisfies

$$(f)_\infty = \sum_{i=1}^{m} \alpha_i P_i.$$

We denote this semigroup by

$$H(P_1, \dots, P_m) := \left\{ \alpha \in \mathbb{N}^m : \exists f \in \mathrm{C}(\mathbb{F}_q) \text{ with } (f)_\infty = \sum_{i=1}^{m} \alpha_i P_i \right\}.$$

An equivalent characterization of $\alpha \in H(P_1, \dots, P_m)$ is that

$$\dim\left(\sum_{i=1}^{m} \alpha_i P_i\right) = \dim\left(\sum_{i=1}^{m} \alpha_i P_i - P_j\right) + 1$$

for all j such that $1 \leqslant j \leqslant m$. The complement of $H(P_1, \dots, P_m)$ in $\mathbb{N}^m$ is called the set of Weierstrass gaps and denoted by

$$G(P_1, \dots, P_m) := \mathbb{N}^m \setminus H(P_1, \dots, P_m).$$

A key quantity associated with the semigroup $H(P)$ for a single point $P \in \mathrm{C}(\mathbb{F}_q)$ is its multiplicity

$$\gamma(H(P)) := \min\{a : a \in H(P) \setminus \{0\}\}.$$

To study the structure of $H(P_1, \dots, P_m)$, we introduce a partial order on $\mathbb{N}^m$. For tuples $(n_1, \dots, n_m)$ and $(p_1, \dots, p_m)$, we define

$$(n_1, \dots, n_m) \preceq (p_1, \dots, p_m) \quad \iff \quad n_i \leqslant p_i \text{ for all } i, 1 \leqslant i \leqslant m.$$

The semigroup for each individual point P_i is denoted by $\Gamma^+(P_i) := H(P_i)$. For $l \geqslant 2$, we extend this to multiple points as

$$\Gamma^+(P_1, \dots, P_m) := \left\{ v \in \mathbb{Z}^{+l} : \begin{array}{l} v \text{ is minimal in } \{w \in H(P_{i_1}, \dots, P_{i_l}) : v_i = w_i\} \\ \text{for some } i, 1 \leqslant i \leqslant l \end{array} \right\}.$$

Given a subset $I \subseteq \{1, \ldots, m\}$ of cardinality l, the natural inclusion $\iota_I : \mathbb{N}^l \to \mathbb{N}^m$ maps to coordinates indexed by I. The minimal generating set of $H(P_1, \ldots, P_m)$ is then

$$\Gamma(P_1, \ldots, P_m) := \bigcup_{l=1}^{m} \bigcup_{\substack{I=\{i_1,\ldots,i_l\} \\ i_1<\cdots<i_l}} \iota_I \left(\Gamma^+(P_{i_1}, \ldots, P_{i_l})\right).$$

Finally, the semigroup $H(P_1, \ldots, P_m)$ can be reconstructed entirely from its minimal generating set $\Gamma(P_1, \ldots, P_m)$. When $1 \leqslant m < \#\mathbb{F}_q$, we have

$$H(P_1, \ldots, P_m) = \{\mathrm{lub}\{v_1, \ldots, v_m\} : v_1, \ldots, v_m \in \Gamma(P_1, \ldots, P_m)\} \tag{15}$$

where the least upper bound is defined as

$$\mathrm{lub}\left\{v^{(1)}, \ldots, v^{(t)}\right\} := \left(\max\left\{v_1^{(1)}, \ldots, v_1^{(t)}\right\}, \ldots, \max\left\{v_n^{(1)}, \ldots, v_n^{(t)}\right\}\right).$$

Proposition 4.1 is the most important result of this subsection, as it provides a fundamental criterion for proving the non-speciality of divisors. This proposition will be repeatedly used throughout to demonstrate the non-speciality of various constructed divisors.

Proposition 4.1. *Let $A = \sum_{i=1}^m \alpha_i P_i$ be an effective divisor of degree g. If $\gamma \nleqslant \alpha$ for all $\gamma \in \Gamma(P_1, \ldots, P_m)$, then A is non-special.*

Proof. Let $A = \sum_{i=1}^m \alpha_i P_i \in \mathrm{D}(\mathrm{F}/\mathbb{F}_q)$ be an effective divisor such that $\sum_{i=1}^m \alpha_i = g$. Assume that A is special. This means that $\dim(A) > \deg(A) + 1 - g = 1$, which implies $\dim(A) \geqslant 2$. By definition of special divisors, there exists $w \in H(P_1, \ldots, P_m)$ satisfying $w \leqslant \alpha$.

From (15), the Weierstrass semigroup $H(P_1, \ldots, P_m)$ is generated by the elements of $\Gamma(P_1, \ldots, P_m)$. Hence, w can be expressed as the least upper bound of some $v_1, \ldots, v_m \in \Gamma(P_1, \ldots, P_m)$. Specifically, there exist $v_1, \ldots, v_m \in \Gamma(P_1, \ldots, P_m)$ such that:

$$v_1 \leqslant lub\{v_1, \ldots, v_m\} = w \leqslant \alpha.$$

The contrapositive of this reasoning shows that if no such $w \leqslant \alpha$ exists in $H(P_1, \ldots, P_m)$, then A cannot be special. This completes the proof. □

The following proposition provides the properties of the first example of function fields, which will serve as the foundation for constructing the desired divisors.

Proposition 4.2. *Let $\mathrm{F}/\mathbb{F}_q(y)$ be the Kummer extension defined by*

$$x^m = \prod_{i=1}^{r} (y - \alpha_i)$$

and let P_i the place associated with $y - \alpha_i$. Then

$$\Gamma^+(P_1) = \mathbb{N} \setminus \left\{mk + j : 1 \leqslant j \leqslant m - 1 - \left\lfloor \frac{m}{r} \right\rfloor, 0 \leqslant k \leqslant r - 2 - \left\lfloor \frac{rj}{m} \right\rfloor\right\}$$

and, for $2 \leqslant l \leqslant r - \left\lfloor \frac{r}{m} \right\rfloor$ *, the semigroup* $\Gamma^+(P_1, \ldots, P_l)$ *is given by*

$$\left\{(ms_1 + j, \ldots, ms_l + j) : 1 \leqslant j \leqslant m - 1 \left\lfloor \frac{m}{r} \right\rfloor, s_i \geqslant 0, \sum_{i=1}^{l} s_i = r - l - \left\lfloor \frac{rj}{m} \right\rfloor \right\}.$$

Proof. See [7, Theorem 3.2] and [10, Theorem 10]. □

The following lemma will ensure that the divisor defined in 4.4 has degree g.

Lemma 4.3. *Let* $r, m \in \mathbb{Z}^+$ *be relatively prime.*

1. *Let* $1 \leqslant j \leqslant m - 1$ *and set* $t = r \bmod m$*. Then*

$$\left\lfloor \frac{r(j+1)}{m} \right\rfloor - \left\lfloor \frac{rj}{m} \right\rfloor = \begin{cases} \left\lfloor \frac{r}{m} \right\rfloor + 1 & \textit{if } j = \left\lfloor \frac{km}{t} \right\rfloor \textit{ with } 1 \leqslant k \leqslant t - 1, \\ \left\lfloor \frac{r}{m} \right\rfloor & \textit{otherwise.} \end{cases}$$

2. *If* $t < m$*, then*

$$\sum_{k=1}^{t-1} \left\lfloor \frac{km}{t} \right\rfloor = \frac{(m-1)(t-1)}{2}.$$

Proof. See [17, Lemma 7]. □

Theorem 4.4. *Let* $F/\mathbb{F}_q(y)$ *by the Kummer extension defined by*

$$x^m = \prod_{i=1}^{r} (y - \alpha_i)$$

where $\alpha_i \in \mathbb{F}_q$ *and* $(r, m) = 1$*. For* $1 \leqslant j \leqslant m - 1 - \left\lfloor \frac{m}{r} \right\rfloor$*, define the following values:*

- $l_j = r - \left\lfloor \frac{rj}{m} \right\rfloor$.
- $s_j = l_j - l_{j+1}$ *if* $j < m - 1 - \left\lfloor \frac{m}{r} \right\rfloor$ *and* $s_{m-1-\left\lfloor \frac{m}{r} \right\rfloor} = l_{m-1-\left\lfloor \frac{m}{r} \right\rfloor} - 1 = \max\left\{1, \left\lfloor \frac{m}{r} \right\rfloor\right\}$.

Then A *is an effective non-special divisor of degree* g *with support contained in the set* $\left\{P_{0b} : \prod_{i=1}^{r}(b - \alpha_i) = 0\right\}$ *if and only if*

$$A = \sum_{j=1}^{m-1-\left\lfloor \frac{m}{r} \right\rfloor} j \sum_{i=1}^{s_j} P_{0b_{j_i}}.$$

In particular, if $r < m$*,*

$$A = \sum_{j=1}^{r-1} \left\lfloor \frac{jm}{r} \right\rfloor P_{0b_j}.$$

Proof. The argument combines explicit calculations of $\deg(A)$, where Lemma 4.3 is used to show that $\deg(A) = g$, and properties of the Weierstrass semigroup (via Proposition 4.1), which ensure that A is non-special. For the remainder of the proof, we start with an effective non-special divisor B of degree $g-1$ and demonstrate that its structure must satisfy the required form. Specifically, we prove that B can be decomposed as $B = \sum_{j=1}^{\gamma} jD_j$ (with $\gamma = m - 1 - \lfloor \frac{m}{r} \rfloor$), where each D_j is either zero or the sum of distinct rational places of degree 1, ensuring disjoint supports across j. This will guarantee that B aligns with the desired construction, even in the case where $r < m$.

We start by observing that

$$A = \sum_{j=1}^{m-1-\lfloor \frac{m}{r} \rfloor} jD_j = \sum_{j=1}^{m-1-\lfloor \frac{m}{r} \rfloor} j \sum_{i=1}^{s_j} P_{0b_{j_i}},$$

where each D_j is defined as

$$D_j = \begin{cases} \sum_{i=1}^{s_j} P_{0b_{j_i}} & \text{if } s_j > 0, \\ 0 & \text{if } s_j = 0, \end{cases}$$

for $1 \leqslant j \leqslant m - 1 - \lfloor \frac{m}{r} \rfloor$. Our goal is to show that A has degree g. Let $t = r \bmod m$. Then

$$\begin{aligned} \deg(A) &= \sum_{i=1}^{m-1-\lfloor \frac{m}{r} \rfloor} js_j \\ &= \sum_{i=1}^{m-1} j \left\lfloor \frac{r}{m} \right\rfloor + \sum_{k=1}^{t-1} \left\lfloor \frac{km}{t} \right\rfloor && \text{(Lemma 4.3, part (1))} \\ &= \frac{(m-1)m}{2} \left\lfloor \frac{r}{m} \right\rfloor + \frac{(m-1)(t-1)}{2} && \text{(Lemma 4.3, part (2))} \\ &= \frac{(m-1)}{2} \left(m \left\lfloor \frac{r}{m} \right\rfloor + t - 1 \right) \\ &= \frac{(m-1)(r-1)}{2} \\ &= g \end{aligned}$$

Next, we prove that A is non-special using Proposition 4.1. Let $v \in \mathbb{N}^{l_1 - 1}$ such that:

$$A = \sum_{i=1}^{l_1 - 1} v_i P_i.$$

Since $v_i \leqslant m - 1 - \lfloor \frac{m}{r} \rfloor$ for all i, Proposition 4.2 implies that $v_i < w$ for any $w \in \Gamma^+(P_i)$. Therefore

$$\iota_{\{i\}}(w) \nleqslant v$$

for any $w \in \Gamma^+(P_i)$.

Now, consider $w \in \Gamma^+\left(P_{i_j} \mid j \in I \subset \{1, \ldots, l_1 - 1\}\right)$. If $w_i > m - \left\lfloor \frac{m}{r} \right\rfloor$ for some i, then $w \nleqslant v$. Otherwise, assume $w = (k, \ldots, k)$ for some $1 \leqslant k \leqslant m - 1 - \left\lfloor \frac{m}{r} \right\rfloor$. Proposition 4.2 shows that $\# I = l_k$, and the number of entries of v greater than or equal to k is:

$$\sum_{i=k}^{m-1-\left\lfloor \frac{m}{r} \right\rfloor} s_i = l_k - 1.$$

Thus, for any I of cardinality l_k, we have $\iota_I(w) \nleqslant v$. Consequently, $w \nleqslant v$ for all $w \in \Gamma(\operatorname{supp}(A))$, which confirms that A is non-special.

Next, let $\gamma = m - 1 - \left\lfloor \frac{m}{r} \right\rfloor$, and consider B, an effective non-special divisor of degree g, supported on $\operatorname{supp}((x))$. Suppose there exists P such that $v_P(B) \geqslant \gamma + 1$. In this case, $\iota(\gamma + 1) \leqslant B$, which contradicts the non-special nature of B.

We express B as

$$B = \sum_{j=1}^{\gamma} j D_j,$$

where each D_j is either zero or the sum of distinct rational places of degree 1, and the supports satisfy

$$\operatorname{supp}(D_j) \cap \operatorname{supp}(D_h) = \varnothing, \qquad \text{for } j \neq h.$$

Note that this decomposition ensures that each D_j is disjointly supported, maintaining the structure required for B, thus

$$\# \operatorname{supp}(B) \leqslant l_1 - 1 < r = \# \operatorname{supp}((x)_0).$$

For D_γ we have

$$\deg(D_\gamma) \leqslant l_\gamma - 1 = s_\gamma.$$

Similarly, for $1 \leqslant h \leqslant \gamma$, it holds that

$$\sum_{j=h}^{\gamma} \deg(D_j) \leqslant \deg(D_h) + \sum_{j=h+1}^{\gamma} \deg(D'_j) \leqslant l_h - 1.$$

Now, define $D'_h \geqslant D_h$ such that

$$\operatorname{supp}(D_h) \subseteq \operatorname{supp}((x)_0) \setminus \operatorname{supp}\left(B + \sum_{j=h+1}^{\gamma} D'_j\right)$$

and ensure that

$$\sum_{j=h}^{\gamma} D'_h = \sum_{j=h}^{\gamma} \# \operatorname{supp}(D'_j) = l_h - 1.$$

From this construction, it follows that

$$\deg(D'_h) = s_h.$$

Consequently, we have

$$g = \deg(B) \leqslant \sum_{j=1}^{\gamma} j \cdot \deg(D'_j) = \sum_{j=1}^{\gamma} js_j = g.$$

This equality implies that $D'_h = D_h$ for all $1 \leqslant h \leqslant \gamma$, confirming that B has the desired structure.

Finally, in the case where $r < m$, Lemma 4.3 states that $s_j = 1$ if $j = \left\lfloor \frac{km}{r} \right\rfloor$, and $s_j = 0$ otherwise. Hence, $D_j = P_k$ or 0. □

Corollary 4.5. *On the norm-trace curve given by $y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{\frac{q^r-1}{q-1}}$ over $\mathbb{F}_{q^r}$, any effective non-special divisor of degree g supported by points P_{0b} is of the form*

$$A = \sum_{i=1, q\nmid i}^{\frac{q^r-1}{q-1}-2} iP_{0b_i}.$$

Proof. Let $u = \frac{q^r-1}{q-1}$. Suppose that

$$\left\lfloor \frac{(r-1)u}{q^{r-1}} \right\rfloor = u - 2.$$

Our goal is to show that $\left\lfloor \frac{jm}{r} \right\rfloor$ cannot be divisible by q. To justify this, observe that

$$u - 2 - \#\big\{i \in \{1, \ldots, u-2\} : q \mid i\big\} = u - 2 - \frac{u-1}{q} + 1 = \frac{u-1}{q}(q-1) = q^{r-1} - 1.$$

This equality follows from the fact that $u = \frac{q^r-1}{q-1}$ is a multiple of q. The term $\#\{i : q \mid i\} = \frac{u-1}{q}$ counts the multiples of q in $\{1, \ldots, u-2\}$. Subtracting this count from $u-2$ and adding 1 adjusts the range correctly, leaving $\frac{u-1}{q}(q-1)$, which simplifies to $q^{r-1} - 1$.

Consequently, the divisor A is given by

$$A = \sum_{j=1}^{q^{r-1}-1} \left\lfloor \frac{ju}{q^{r-1}} \right\rfloor P_j.$$

This expression ensures that A is non-special and has degree g. Furthermore, by Theorem 4.4, any other divisor with these characteristics must take this specific form.

Next, we show that $\left\lfloor \frac{ju}{q^{r-1}} \right\rfloor$ is not divisible by q for any $1 \leqslant j \leqslant q^{r-1} - 1$. Suppose, for contradiction, that

$$\left\lfloor \frac{ju}{q^{r-1}} \right\rfloor = qk,$$

for some $1 \leqslant k \leqslant \frac{u-1}{q} - 1$. Then, the equality

$$ju = q^r k + z = u(q-1)k + k + z$$

implies that $u \mid (k+z)$. However, note that

$$k+z < \frac{u-2}{q} + q^{r-1} = \frac{uq-1}{q} < u.$$

Since $k+z$ is strictly less than u, it cannot be a multiple of u, contradicting the assumption that $u \mid (k+z)$.

Therefore, no such k can exist, and we conclude that $\left\lfloor \frac{ju}{q^{r-1}} \right\rfloor$ is not divisible by q for any j. This completes the proof. □

The following corollary provides the explicit form of the desired divisors in the case of the second example of function fields discussed in this subsection.

Corollary 4.6. *On the Hermitian curve $y^q + y - x^{q+1} = 0$ over $\mathbb{F}_{q^2}$, any effective non-special divisor of degree g with support contained in $\{P_{0b_i} : 1 \leqslant i \leqslant q\}$ is of the form*

$$A = \sum_{i=1}^{q-1} iP_{0b_i}.$$

We now construct non-special divisors of degree $g-1$ by building on the non-special divisors of degree g established earlier. Using Lemma 2.3 and Theorem 4.4, we have the following explicit construction.

Theorem 4.7. *Let $\mathrm{F}/\mathbb{F}_q(y)$ by the Kummer extension defined by*

$$x^m = \prod_{i=1}^{r}(y-\alpha_i)$$

where $\alpha_i \in \mathbb{F}_q$ and $(r,m) = 1$. Then

$$A = \sum_{j=1}^{m-1-\lfloor \frac{m}{r} \rfloor} j \sum_{i=1}^{s_j} P_{0b_{j_i}} - P.$$

is a non-special divisor of degree $g-1$ for all $P \in \{P_{ab} : a \neq 0 \text{ or } b \neq b_{j_i}\} \cup \{P_\infty\}$. In particular there exist non-special divisors of degree $g-1$ supported on $\operatorname{supp}((x)_0) \cup \{P_{ab}\}$ *for any $a \neq 0$.*

Proof. Note that $A + P_{ab}$ is non-special of degree g by Theorem 4.4 and, by Lemma 2.3, we have A is non-special too. Given

$$\#\operatorname{supp}(A) = r - \left\lfloor \frac{r}{m} \right\rfloor - 1 \leqslant r-1,$$

we can take $P \in \operatorname{supp}(x) \setminus \operatorname{supp}(A) = \varnothing$. □

To conclude this section, [6, Lemma 4.1] explicitly describes the form of the non-special divisors of degree g and $g-1$ for the case of a curve $\mathrm{F}/\mathbb{F}_{q^2}$ defined by

$$y^{q+1} = x^2 + x. \tag{16}$$

Lemma 4.8. *Let q be odd, and let $\mathbf{F}/\mathbb{F}_{q^2}$ be the function field defined by* (16). *Let $P \in \left\{P_{ab} \in \mathrm{P}(\mathbf{F}/\mathbb{F}_{q^2}) \mid 2a+1 \neq 0\right\}$ be a rational place of $\mathbf{F}$. Then, gP is a non-special divisor of degree g. In particular, $gP - P'$ is a non-special divisor of degree $g-1$ for all rational places $P' \in \mathrm{P}(\mathbf{F}/\mathbb{F}_{q^2})$ distinct from P.*

Proof. The hyperelliptic involution of the curve defined by $y^{q+1} = x^2 + x$ is given by $\varphi(x, y) = (-x-1, y)$. Consequently, the fixed points of φ are the pairs $(a, b) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ such that $2a + 1 = 0$. Consider a rational place $P \in \left\{P_{ab} \in \mathrm{P}(\mathbf{F}/\mathbb{F}_{q^2}) \mid 2a+1 \neq 0\right\}$.

It is known that if P is a rational place of a hyperelliptic function field not fixed by the hyperelliptic involution, then the Weierstrass semigroup at P satisfies $H(P) = \{0, g+1, g+2, \ldots\}$, see [21, Satz 8]. As a result, we have $\mathcal{L}(gP) = \{0\}$, which implies that gP is a non-special divisor of degree g.

Moreover, for any rational place $P' \in \mathrm{P}(\mathbf{F}/\mathbb{F}_{q^2}) \setminus \{P\}$, the divisor $gP - P'$ is also non-special, as established in [1, Lemma 3]. □

4.2 Example on an asymptotically good tower

A tower $F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$ of algebraic function fields over a finite field $\mathbb{F}_q$ is said to be asymptotically good if

$$\lim_{m\to\infty} \frac{B_1(F_m/\mathbb{F}_q)}{g(F_m/\mathbb{F}_q)} > 0.$$

In this subsection, we focus on constructing non-special divisors of degree $g(F_m)$ using an example of an asymptotically good tower studied in [9] by A. Garcia and H. Stichtenoth. Since this setting is more complex, we introduce several definitions to explain the structures and properties clearly. Even though there are many definitions, they are important to understand the key aspects of function field towers and to prepare for the results that follow.

We will consider the tower $\mathcal{F} = (F_m)_{m\geqslant 1}$ of function fields $\mathbb{F}_m/K$ where $K = \mathbb{F}_{q^2}$ given by

$$F_m = K(x_1, \ldots, x_m) \quad \text{with} \quad x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1} \quad \text{for} \quad i = 1, \ldots, m-1.$$

The following proposition outlines key properties of the tower, such as its genus and ramification structure.

Proposition 4.9. *(i) For all $m \geqslant 2$, the extension F_m/F_{m-1} is Galois of degree q.*

(ii) The pole of x_1 in F_1 is totally ramified in F_m/T_1, i.e.,

$$(x_1)_\infty^{F_m} = q^{m-1} P_\infty^{(m)}$$

with a place $P_\infty^{(m)} \in \mathrm{P}_1(F_m)$ of degree one.

(iii) The genus is

$$g(F_m) = \begin{cases} (q^{m/2}-1)^2 & \text{if } m \equiv 0 \bmod 2, \\ (q^{(m+1)/2}-1)(q^{(m-1)/2}-1) & \text{if } m \equiv 1 \bmod 2. \end{cases}$$

Proof. For (i) and (ii), see [9, Lemma 3.3]. For (iii), see [9, Remark 3.8]. □

We now define $(c_m)_{m \geqslant 1}$, a key sequence that connects the degree of divisors with the structure of the function fields in the tower. It will play an important role in the final construction.

Definition 4.10. *For $m \geqslant 1$, let*

$$c_m = \begin{cases} q^m - q^{m/2} & \text{if } m \equiv 0 \bmod 2, \\ q^m - q^{(m+1)/2} & \text{if } m \equiv 1 \bmod 2. \end{cases}$$

Definition 4.11. *For $1 \leqslant j \leqslant m$, define*

$$\pi_j = \prod_{i=1}^{j} \left(x_i^{q-1} + 1 \right), \qquad \text{and}$$

$$\mathrm{L}_j^{(m)} = \left\{ P \in \mathrm{P}(F_m) : P \text{ is a zero of } x_i^{q-1} + 1 \text{ for some } i \in \{1, \ldots, j\} \right\}.$$

This lemma describes the principal divisors of $(\pi_j)_{1 \leqslant j \leqslant m}$, which are fundamental to understanding the supports and degrees of the divisors we construct.

Lemma 4.12. *(i) Let $1 \leqslant j \leqslant m$. Then the principal divisor of π_j is given by*

$$(\pi_j)^{F_m} = C_j^{(m)} - \left(q^m - q^{m-j}\right) P_\infty^{(m)},$$

where $C_j^{(m)} \geqslant 0$ is a divisor of F_m with

$$\operatorname{supp}\left(C_j^{(m)}\right) = \mathrm{L}_j^{(m)}.$$

(ii) Let $1 \leqslant j \leqslant m-1$ and $0 \leqslant e \leqslant q-1$. Then the principal divisor of $\pi_j x_{j+1}^e$ in F_m is given by

$$\left(\pi_j x_{j+1}^e\right)^{F_m} = D_{j,e}^{(m)} - \left(q^m - q^{m-j} + e q^{m-j-1}\right) P_\infty^{(m)},$$

where $D_{j,e}^{(m)} \geqslant 0$ is a divisor of F_m with

$$\mathrm{L}_j^{(m)} \subseteq \operatorname{supp}\left(D_{j,e}^{(m)}\right).$$

Proof. See [19, Lemma 3.4]. □

The following definition introduces $\left(A_j^{(m)}\right)_{m\geqslant 1}$, a divisor structured using the set $\mathrm{L}_j^{(m)}$ introduced in Definition 4.11. These divisors play a direct role in the construction of non-special divisors in the tower.

Definition 4.13. *For $1 \leqslant j \leqslant m$, let*

$$A_j^{(m)} = \sum_{P\in \mathrm{L}_j^{(m)}} P.$$

Remark 4.14. From Lemma 4.12 we have: $\pi_j \in \mathcal{L}\left(\left(q^m - q^{m-j}\right) P_\infty^{(m)} - A_j^{(m)}\right)$.

The following results, Proposition 4.15 and Lemma 4.16, provide the necessary properties for the construction. These results establish both the required dimension and degree.

Proposition 4.15. *For $1 \leqslant j \leqslant m$, one has*

$$\mathcal{L}\left(\left(q^m - q^{m-j}\right) P_\infty^{(m)} - A_j^{(m)}\right) = \langle \pi_j \rangle;$$

i.e., the space $\mathcal{L}((q^m - q^{m-j})P_\infty^{(m)} - A_j^{(m)})$ is one-dimensional.

Proof. See [19, Proposition 3.6]. □

Lemma 4.16 ([19, Lemma 3.7]). *Let $1 \leqslant j \leqslant m/2$. Then*

$$\deg(A_j^{(m)}) = q^j - 1.$$

Proof. Let $\mathcal{A}_i^{(m)} = \left\{P \in \mathrm{P}(F_m) : P \text{ is a zero of } x_i^{q-1} + 1\right\}$. It follows from [9, Lemma 3.6] that, for $1 \leqslant i \leqslant m/2$,

$$\deg\left(\sum_{P\in\mathcal{A}_i^{(m)}} P\right) = (q-1)q^{i-1}.$$

Since

$$A_j^{(m)} = \sum_{i=1}^{j} \sum_{P\in\mathcal{A}_i^{(m)}} P,$$

we obtain

$$\deg\left(A_j^{(m)}\right) = \sum_{i=1}^{j}(q-1)q^{i-1} = q^j - 1.$$

□

Definition 4.17. *We define a divisor $A^{(m)}$ of F_m as follows. Let $A^{(1)} = 0$ and, for $m \geqslant 2$,*

$$A^{(m)} = A_j^{(m)} \qquad \text{with} \qquad j = \begin{cases} \frac{m}{2} & \text{if } m \equiv 0 \bmod 2, \\ \frac{m-1}{2} & \text{if } m \equiv 1 \bmod 2. \end{cases}$$

The following lemma combines all earlier results to establish the main properties.

Lemma 4.18 ([19, Lemma 3.9]). *We have:*

1. $\deg(A^{(m)}) = c_m - g(F_m)$;
2. $\dim(c_m P_\infty^{(m)} - A^{(m)}) = 1$;

i.e., $c_m P_\infty^{(m)} - A^{(m)}$ *is non-special of degree* $g(F_m)$.

Proof. For $m = 1$, all assertions are immediate since $c_1 = g(F_1) = 0$ and $A^{(1)} = 0$. Now, let $m \geqslant 2$.

- If $m \equiv 0 \bmod 2$, we have

  $$c_m = q^m - q^{m/2} \qquad \text{and} \qquad g_m = (q^{m/2} - 1)^2.$$

  Hence

  $$c_m - g_m = q^{m/2} - 1 = (A^{(m)})$$

  by Lemma 4.16. On the other hand, using Proposition 4.15, we obtain

  $$\mathcal{L}(c_m P_\infty^{(m)} - A^{(m)}) = \mathcal{L}((q^m - q^{m/2})P_\infty^{(m)} - A_{m/2}^{(m)}) = \langle \pi_{m/2} \rangle.$$

- If $m \equiv 1 \bmod 2$, the proof follows from a similar argument.

□

4.3 Example of construction with a sufficiently large number of points

The results presented in this subsection (by H. Randriam in [20]), while seemingly technical and detailed, serve as essential tools for our main objective: the construction of non-special divisors of degree $g - 1$. The lemmas and definitions presented below create a step-by-step framework leading to the final construction. Each result is carefully built upon the previous one, establishing bounds and properties for divisors under various conditions.

The next lemma provides initial constraints on the size of a set $\mathcal{S}$, given certain conditions on divisors A and B. These bounds are fundamental for analyzing ordinarity and exceptionality in later results.

Lemma 4.19. *Let* C *be a curve of genus* g *defined over* $\mathbb{F}_q$, *and* $\mathcal{S} \subset \mathrm{C}(\mathbb{F}_q)$.

1. *Let* A *be an* $\mathbb{F}_q$*-rational divisor on* C *such that*

   $$i(A) = \dim(A) - (\deg(A) + 1 - g) \geqslant 1.$$

   Suppose that for all $P \in \mathcal{S}$ *we have* $\dim(A + P) > \dim(A)$. *Then*

   $$\#\mathcal{S} \leqslant g - \dim(A). \tag{17}$$

   (If $\deg(A) = -1$, *then, we also have* $\#\mathcal{S} \leqslant 1$.*)*

2. *Let B a $\mathbb{F}_q$-rational divisor on* C *such that* $\dim(B) \geqslant 1$. *Suppose that for all* $P \in \mathcal{S}$ *we have* $\dim(B - P) > \dim(B) - 1$. *Then*
$$\#\mathcal{S} \leqslant \deg(B) + 1 - \dim(B). \tag{18}$$
(If $\deg(B) = 2g - 1$, *we also have* $\#\mathcal{S} \leqslant 1$.*)*

Proof. See [20, Lemma 1]. □

The main result of this section is based on the following Lemma which extends the results of Lemma 4.19 to more complex cases, such as when multiple points are added or removed from a divisor.

For all $q > 1$ and all integer $n \geqslant 2$, define
$$\begin{aligned} G_q(n) &= \sum_{k=1}^{n-2} \frac{(q^{n-k} - 1)(q^{n-k-1} - 1)}{(q^n - 1)(q^{n-1} - 1)} \\ &= \frac{1}{q^2 - 1} - \frac{1 - \frac{(q-1)n}{q^n} - 1}{(q-1)(q^{n-1} - 1)}. \end{aligned}$$

Lemma 4.20. *Let* C *be a curve of genus g defined over* $\mathbb{F}_q$ *and* $\mathcal{S} \subset \mathrm{C}(\mathbb{F}_q)$.

1. *Let A be an $\mathbb{F}_q$-rational divisor on* C *such that* $\deg(A) \geqslant -2$ *and*
$$i(A) = \dim(A) - (\deg(A) + 1 - g) \geqslant 2.$$
Suppose that for all $P \in \mathcal{S}$ *we have* $\dim(A + 2P) > \dim(A)$. *Then*
$$\#\mathcal{S} \leqslant 3g + 3 + \deg(A) - 3\dim(A) \tag{19}$$
and
$$\#\mathcal{S} \leqslant \left(1 + \frac{q^{i(A)-2} - 1}{q^{i(A)} - 1}\right)^{-1} \left(6g - 6 - 2\deg(A) - 2G_q(i(A)) \cdot \#\mathrm{C}(\mathbb{F}_q)\right). \tag{20}$$
More generally, for all integers w such that $2 \leqslant w \leqslant i(A)$,
$$\begin{aligned} \#\mathcal{S} \leqslant (i(A) - w) + &\left(1 + \frac{q^{w-2} - 1}{q^w - 1}\right)^{-1} \\ &\left(6g - 6 - 2\deg(A) - 4(i(A) - w) - 2G_q(w) \cdot \#\mathrm{C}(\mathbb{F}_q)\right). \end{aligned} \tag{21}$$

2. *Let B an $\mathbb{F}_q$-rational divisor on* C *such as* $\deg(B) \leqslant 2g$ *and* $\dim(B) \geqslant 2$. *Suppose that for all* $P \in \mathcal{S}$ *we have* $\dim(B - 2P) > \dim(B) - 2$. *Then*
$$\#\mathcal{S} \leqslant 2\deg(B) + 2g + 4 - 3\dim(B) \tag{22}$$
and
$$\#\mathcal{S} \leqslant \left(1 + \frac{q^{\dim(B)-2} - 1}{q^{\dim(B)} - 1}\right)^{-1} \left(2\deg(B) + 2g - 2 - 2G_q(\dim(B)) \cdot \#\mathrm{C}(\mathbb{F}_q)\right). \tag{23}$$

More generally, for all integers w *such that* $2 \leqslant w \leqslant \dim(B)$*,*

$$\#\mathcal{S} \leqslant (l(B) - w) + \left(1 + \frac{q^{w-2} - 1}{q^w - 1}\right)^{-1} \left(2\deg(B) + 2g - 2 - 4(\dim(B) - w) - 2G_q(w) \cdot \#\mathrm{C}(\mathbb{F}_q)\right). \quad (24)$$

Proof. See [20, Lemma 2]. □

To simplify the application of these results, we define, over $\mathbb{Z}$, the functions $f_{1,\mathrm{C}}$ and $f_{2,\mathrm{C}}$, which summarize the bounds established in Lemmas 4.19 and 4.20:

$$f_{1,\mathrm{C}}(a) = \begin{cases} 1 & \text{if } a = -1, \\ g & \text{if } 0 \leqslant a \leqslant g - 2, , \\ 0 & \text{otherwise.} \end{cases} \qquad \text{and}$$

$$f_{2,\mathrm{C}}(a) = \begin{cases} g & \text{if } a = g-2, \\ \min_{2 \leqslant w \leqslant g-1-a} \left\lfloor (g - 1 - a - w) + \left(1 + \frac{q^{w-2}-1}{q^w-1}\right)^{-1} (2g - 2 + 2a + 4w - 2G_q(w)\#\mathrm{C}(\mathbb{F}_q)) \right\rfloor & \text{if } -2 \leqslant a \leqslant g-3, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 4.21. *Let* C *be a curve of genus* $g \geqslant 1$ *defined over* $\mathbb{F}_q$*. A divisor* D *on* C *is called* ordinary *if*

$$\dim(D) = max(0, \deg(D) + 1 - g).$$

Otherwise, D *is called* exceptional.

Lemma 4.22 provides an upper bound on the size of $\mathcal{S}$, ensuring that this set is sufficiently small to satisfy the conditions required in Proposition 4.23. This connection is crucial for constructing divisors incrementally while maintaining their ordinarity.

Lemma 4.22. *Let* A *be a divisor on* C*,* $\mathcal{S} \subset \mathrm{C}(\mathbb{F}_q)$ *a set of rational points and* $s \in \{1, 2\}$*. Assume that* A *is ordinary, and* $A + sP$ *is exceptional for all* $P \in \mathcal{S}$*. Then*

$$\#S \leqslant f_{s,\mathrm{C}}(\deg(A)). \quad (25)$$

Proof. Let $a = \deg(A)$. We analyze the cases based on the value of s.

(i) Case $s = 1$:

(a) If $a \leqslant -2$ or $a \geqslant 2g - 2$, then $A + P$ is ordinary. This implies that $\mathcal{S}$ is empty, and we have $f_{1,\mathrm{C}}(a) = 0$.

(b) If $g - 1 \leqslant a \leqslant 2g - 3$, the ordinarity of A means $\dim(A) = a + 1 - g$. By Riemann–Roch, $A + P$ remains ordinary, leading to the same conclusion as the previous case.

(c) If $-1 \leqslant a \leqslant g-2$, the ordinarity of A implies $\dim(A) = 0$. For $A + P$ to be exceptional, $\dim(A + P) \geqslant 1$ must hold. This is addressed using Lemma 4.19-1.

(ii) Case $s = 2$:

(a) If $a \leqslant -3$ or $a \geqslant 2g - 1$, then $A + 2P$ is ordinary, implying that $\mathcal{S}$ is empty.

(b) If $g - 1 \leqslant a \leqslant 2g - 2$, the ordinarity of A ensures $\dim(A) = a + 1 - g$. Using Riemann–Roch, $A + 2P$ is also ordinary, leading to the same conclusion as above.

(c) If $a = g - 2$, the ordinarity of A implies $\dim(A) = 0$. For $A + 2P$ to be exceptional, $\dim(A + 2P) \geqslant 1$ must hold. By Lemma 4.19-1, we conclude that $\#S \leqslant g = f_{2,\mathrm{C}}(a)$.

(d) If $-2 \leqslant a \leqslant g - 3$, the ordinarity of A gives $\dim(A) = 0$, while the exceptionality of $A + 2P$ requires $\dim(A + 2P) \geqslant 1$. This is addressed using Lemma 4.20-1.

□

Proposition 4.23. *Let* C *be a curve of genus g defined over $\mathbb{F}_q$, $r \geqslant 1$ an integer, $s_1, \ldots, s_r \in \{1, 2\}$, $\mathbb{F}_q$-rational divisors $T_1, \ldots, T_r$ on* C*, and $d \in \mathbb{Z}$ an integer. The degree of T_i is denoted $t_i = \deg(T_i)$. Let D_0 be an $\mathbb{F}_q$-rational divisor on* C *of degree* $\deg(D_0) = d_0 \leqslant d$*, such that $s_i D_0 - T_i$ is ordinary. Finally, let $\mathcal{S} \subset \mathrm{C}(\mathbb{F}_q)$ be a set of points satisfying*

$$\#\mathcal{S} > \max_{d_0 \leqslant d' < d} \sum_{i=1}^{r} f_{s_i,\mathrm{C}}\left(s_i d' - t_i\right). \tag{26}$$

Then, there exists an $\mathbb{F}_q$-rational divisor D on C *of degree* $\deg(D) = d$*, such that $s_i D - T_i$ is ordinary. Furthermore, D can be chosen such that $D - D_0$ is effective and supported by points in $\mathcal{S}$. .*

Proof. We construct D incrementally. Let d' satisfy $d_0 \leqslant d' < d$. Suppose a divisor D' of degree d' has already been constructed such that $s_i D' - T_i$ is ordinary and $D' - D_0$ is effective and supported in $\mathcal{S}$.

By applying Lemma 4.22 with $s = s_i$ and $A = s_i D' - T_i$, we know that there are at most $f_{s_i,\mathrm{C}}(s_i d' - t_i)$ points $P \in \mathcal{S}$ such that $s_i(D' + P) - T_i$ becomes exceptional.

Using inequality (26), which ensures that $\#\mathcal{S}$ is sufficiently large, we can always find a point $P \in \mathcal{S}$ where $s_i(D' + P) - T_i$ remains ordinary. This guarantees that adding P to D' preserves the ordinarity condition for $s_i D' - T_i$. Furthermore, by construction, $(D' + P) - D_0$ remains effective and supported entirely within $\mathcal{S}$.

Finally, by repeating this process for each $d' < d$, we can incrementally construct D of degree d with the desired properties. The result follows by induction on d'. □

Lemma 4.24. *With the previous notations, $f_{s,\mathrm{C}}(a)$ is an increasing function when $a \leqslant g - 1 - s$, their maximum value on $\mathbb{Z}$ is $f_{s,\mathrm{C}}(g - 1 - s) = s^2 g$.*

Proof. See [20, Lemma 8]. □

Using the refined bounds from Lemma 4.24, Proposition 4.25 establishes the existence of divisors of any degree d with specific ordinarity properties, assuming the curve has a sufficiently large number of points.

Proposition 4.25. *Let* C *be a curve of genus* g *defined over* $\mathbb{F}_q$, $r \geqslant 1$ *an integer,* $s_1, \ldots, s_r \in \{1, 2\}$, $\mathbb{F}_q$*-rational divisors* $T_1, \ldots, T_r$ *on* C. *Assume that*

$$\#\mathrm{C}(\mathbb{F}_q) > \sum_{i=1}^{r} (s_i)^2 g.$$

Then, for all integer d, *there exists an* $\mathbb{F}_q$*-rational divisor* D *on* C *of degree* $\deg(D) = d$ *and supported in* $\mathrm{C}(\mathbb{F}_q)$, *such that* $s_iD - T_i$ *is ordinary.*

Proof. We apply Proposition 4.23 with $\mathcal{S} = \mathrm{C}(\mathbb{F}_q)$, and Lemma 4.24. □

Corollary 4.26 represents the main result of this subsection.

Corollary 4.26. *Let* C *be a curve of genus* g *defined over* $\mathbb{F}_q$, Q *and* G *two* $\mathbb{F}_q$*-rational divisors. We denote by* $k = \deg(Q)$ *and* $n = \deg(G)$ *their degrees. Assume that*

$$\#\mathrm{C}(\mathbb{F}_q) > 5g \qquad \text{and} \qquad n \geqslant 2k + g - 1.$$

Then, there exists an $\mathbb{F}_q$*-rational divisor* D *on* C *supported in* $\mathrm{C}(\mathbb{F}_q)$, *such that* $D - Q$ *is non-special of degree* $g - 1$ *and* $\dim(2D - G) = 0$.

In particular, if $n = 2k + g - 1$, *then* $D - Q$ *and* $2D - G$ *are non-special of degree* $g - 1$.

Proof. We apply Proposition 4.25 with $r = 2$, $s_1 = 1$, $T_1 = Q$, $s_2 = 2$, $T_2 = G$ and $d = k + g - 1$. □

Remark 4.27. Notice that the divisor D in the previous corollary can be built as seen in the proof of Proposition 4.23. Below is the summary of the steps with the conditions of Corollary 4.26:

1. Let Q and G be two $\mathbb{F}_q$-rational divisors with $\deg(Q) = k$ and $\deg(G) = 2k + g - 1$.
2. Let D_0 be a divisor such that $\deg(D_0) = d_0 \leqslant k + g - 1$ and $D_0 - Q$, $2D_0 - G$ are ordinary.
3. Build a divisor D' of degree d', $d_0 \leqslant d' < k + g - 1$ such that $D' - Q$, $2D' - G$ are ordinary and $D' - D_0$ effective.
4. We can find $P \in \mathrm{C}(\mathbb{F}_q)$ such that $D' + P - Q$, $2(D' + P) - G$ are ordinary.
5. We reapply step 4 until we obtain the desired divisor D with the desired degree $k + g - 1$.

Acknowledgements

The authors would like to thank the referees very much for their many valuable comments, which led to a significant improvement in the article.

References

[1] S. Ballet and D. Le Brigand. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. *Journal of Number Theory*, 116:293–310, 2006.

[2] S. Ballet, J. Chaumine, J. Pieltant, M. Rambaud, H. Randriambololona, and R. Rolland. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. *Russian Mathematical Surveys*, 1(76):29–89, 2021.

[3] S. Ballet, C. Ritzenthaler, and R. Rolland. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. *Acta Arithmetica*, 143(4):377–392, 2009.

[4] I. Cascudo, R. Cramer, and C. Xing. Bounds on the threshold gap in secret sharing and its applications. *IEEE Transactions on Information Theory*, 59(9):5600–5612, 2013.

[5] I. Cascudo, R. Cramer, and C. Xing. Torsion limits and Riemann-Roch systems for function fields and applications. *IEEE Transactions on Information Theory*, 60(7):3871–3888, 2014.

[6] A. S. Castellanos, A. V. Marques, and L. Quoos. Linear complementary dual codes and linear complementary pairs of AG codes in function fields. `https://www.arxiv.org/abs/2407.05845`, 2024.

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

[8] H. Chen and R. Cramer. Algebraic geometric secret sharing schemes and secure multiparty computations over small fields. In *Advances in Cryptology — CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 516–531. Springer, 2006.

[9] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[10] C. Hu and S. Yang. Weierstrass semigroups from Kummer extensions. *Finite Fields and Their Applications*, 45:264–284, 2017.

[11] M. Koutchoukali. On the coefficients of the zeta-function's L-polynomial for algebraic function fields over finite constant fields. *Contemporary Mathematics*, 2023. Accepted for publication.

[12] D. LeBrigand. Classification of algebraic function fields with divisor class number two. *Finite Fields and Their Applications*, 2:153–172, 1996.

[13] J. Leitzel, M. Madan, and C. Queen. Algebraic function fields with small class number. *Journal of Number Theory*, 7:11–27, 1975.

[14] R.E. MacRae. On unique factorization in certain rings of algebraic functions. *Journal of Algebra*, 17(2):243–261, 1971.

[15] M. Madan and C. Queen. Algebraic function fields of class number one. *Acta Arithmetica*, 20:423–432, 1972.

[16] Y. Manin. The Hasse–Witt matrix of an algebraic curve. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 25:153–172, 1961.

[17] G. L. Matthews, E. C. Moreno, and H. H. López. Explicit non-special divisors of small degree, algebraic geometric hulls, and LCD codes from Kummer extensions. *SIAM Journal on Applied Algebra and Geometry*, 2(8):394–413, 2024.

[18] H. Niederreiter and C. Xing. Low-discrepancy sequences and global function fields with many rational places. *Finite Fields and Their Applications*, 2:241–273, 1996.

[19] R. Pellikaan, H. Stichtenoth, and F. Torres. Weierstrass semigroups in an asymptotically good tower of function fields. *Finite Fields and Their Applications*, 4(4):381–392, 1998.

[20] H. Randriam. Divisors of the form $2D-G$ without sections and bilinear complexity of multiplication in finite fields. `https://www.arxiv.org/abs/1103.4335`, 2011.

[21] F. K. Schmidt. Zur arithmetischen Theorie der algebraischen Funktionen. II. Allgemeine Theorie der Weierstraßpunkte. *Mathematische Zeitschrift*, 1(45):243–261, 1939.

[22] J.-P. Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium Internacional de Topologia Algebraica*, pages 24–53. Universídad Nacional Autónoma de México, 1958.

[23] J.-P. Serre. *Rational points on curves over finite fields.* Documents Mathématiques 18. Société Mathématique de France, 2020.

[24] I. Shparlinski, M. Tsfasman, and S. Vladut. Curves with many points and multiplication in finite fields. In H. Stichtenoth and M. A. Tsfasman, editors, *Coding Theory and Algebraic Geometry — AGCT-3*, volume 1518, pages 145–169. Springer, 1992.

[25] H. Stichtenoth. *Algebraic Function Fields and Codes.* Number 314 in Lectures Notes in Mathematics. Springer, 1993.

[26] K.-O. Stör and J. Voloch. A formula for the Cartier operator on plane algebraic curves. *Journal für die reine und angewandte Mathematik*, 377:49–64, 1987.

[27] M. Tsfasman. Some remarks on the asymptotic number of points. In H. Stichtenoth and M. A. Tsfasman, editors, *Coding Theory and Algebraic Geometry — AGCT-3*, volume 1518 of *Lecture Notes in Mathematics*, pages 178–192. Springer, 1992.

[28] M. Tsfasman and S. Vladut. Asymptotic properties of zeta-functions. *Journal of Mathematical Sciences*, 84(5):1445–1467, 1997.

[29] M. A. Tsfasman, S. G. Vladut, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[30] S. Tutdere and O. Uzunkol. Construction of arithmetic secret sharing schemes by using torsion limits. *Hacettepe Journal of Mathematics and Statistics*, 49(2):638–647, 2020.