Weierstrass semigroups of maximal function fields with applications to AG codes

Vicino, Lara

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Weierstrass semigroups of maximal function fields with applications to AG codes

Lara Vicino

Kongens Lyngby 2023

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Richard Petersens Plads, building 324,
2800 Kongens Lyngby, Denmark
Phone +45 4525 3031
compute@compute.dtu.dk
www.compute.dtu.dk

Summary (English)

In this thesis, we study Weierstrass semigroups at one or multiple places of certain maximal function fields, with a twofold purpose: extending the theoretical knowledge on these function fields and investigating applications to Algebraic Geometry codes (AG codes).

The first major contribution of the thesis consists in the determination of the Weierstrass semigroups at all the places of one of the known maximal function fields with the third largest genus. Consequently, we are also able to determine the full automorphism group of the function field. We find several different types of Weierstrass semigroups and a surprisingly rich set of Weierstrass places, which had never been observed before for any of the other maximal function fields for which the Weierstrass places are known.

A second major contribution presented in this dissertation is the computation of the Weierstrass semigroups at certain pairs of places of two different families of maximal function fields: the Beelen-Montanucci function fields and the Skabelund function field obtained as a cyclic extension of the Suzuki one. As a result, we are able to estimate the minimum distance of certain two-point AG codes from these function fields, obtaining improvements on comparable AG codes that had previously been studied in the literature.

As a final contribution, we present the study of upper and lower bounds for a constant that captures the asymptotic behaviour of the number of rational points of projective curves over a finite field, when the degree of the curve becomes large with respect to the field cardinality. The exact value of the constant remains unknown, but improvements to the previously known bounds are found.

Summary (Danish)

I denne afhandling studerer vi Weierstrass-semigrupper ved ét eller flere steder af visse maksimale funktionslegemer, med et todelt formål: dels at udvide den teoretiske viden om disse funktionslegemer og dels at undersøge anvendelser inden for Algebraisk Geometri-koder (AG koder).

Det første væsentlige bidrag består i bestemmelsen af Weierstrass-semigrupperne ved alle steder af ét af de kendte maksimale funktionslegemer med det tredjestørste genus. En konsekvens af dette er, at vi er i stand til at bestemme den fulde automorfigruppe for funktionslegemet. Vi finder mange forskellige typer af Weierstrass-semigrupper og en overraskende rig mængde af Weierstrass-steder, som aldrig før er blevet observeret for nogen af de andre maksimale funktionslegemer, hvor Weierstrass-stederne er kendte.

Et andet væsentligt bidrag er beregningen af Weierstrass-semigrupperne ved visse par af steder for to forskellige familier af maksimale funktionslegemer: Beelen-Montanucci funktionslegemerne og Skabelund funktionslegemet, der opnås ved en cyklisk udvidelse af Suzuki funktionslegemet. Som følge af dette er vi i stand til at estimere minimumsafstanden for visse to-punkt AG koder fra disse funktionslegemer, og vi opnår forbedringer i forhold til sammenlignelige AG koder, der tidligere er blevet studeret i litteraturen.

Til sidst præsenterer vi studiet af øvre og nedre grænser for en konstant, der beskriver hvordan antallet af rationelle punkter på projektive kurver over et endeligt legeme opfører sig asymptotisk, når graden af kurven bliver stor i forhold til legemets kardinalitet. Den præcise værdi af konstanten er stadig ukendt, men vi opnår forbedringer af de tidligere kendte grænser.

Preface

The work contained in this thesis was developed during my PhD studies under the supervision of Professor Peter Beelen and Associate Professor Maria Montanucci. The studies were conducted at the Technical University of Denmark, in the period from 15 October 2020 to 14 October 2023.

During this period, I co-authored five scientific papers: [11], [65], [6], [12] and [64]. The following list outlines the publication status of the aforementioned papers:

- [11] is published in the proceedings of the 18th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory,
- [65] and [12] are published in the international journal *Finite Fields and Their Applications*,
- [6] and [64] are available online and are currently submitted for publication in international journals.

This thesis includes, in a more extensive version, the contents of [11], [65], [12] and [64]. In particular, the results contained in [65], [12] and [64] have been rewritten in the language of function fields and, where specified, extended with further results.

The thesis comprises six chapters.

Chapter 1 provides an introduction to the central topics of the thesis and explains the motivations for their study.

Chapter 2 includes a presentation of the essential background theory and introduces the notations necessary for the discussion of the work presented in the rest of the manuscript. The results recalled in the chapter are widely known and therefore nearly all of them are presented without proofs. References to the pertinent literature are given at the beginning of each section and, for the possibly less famous results, are also specified alongside the statements.

Chapter 3, Chapter 4 and Chapter 5 contain, respectively, a detailed discussion of the results presented in [12], [64, 65] and [11].

Chapter 6 concludes the manuscript, summarizing the main contributions of this dissertation to the field of research and considering possible ideas for further investigation.

Unless otherwise specified, statements such as theorems, propositions, lemmas and corollaries that appear in this thesis, alongside their relative proofs and data and results arising from them, are, up to our knowledge, original. When already known results are included, it is explicitly indicated and references are given.

Lyngby, 14-October-2023

Lara Vicino

Acknowledgements

I would like to express my most sincere appreciation and heartfelt gratitude to my supervisors Peter Beelen and Maria Montanucci. Their exceptional mathematical knowledge and their thoughtful kindness have guided me with brilliant wisdom and unwavering support through every aspect and challenge of my PhD studies. I consider myself incredibly lucky for having been a PhD student under their supervision, and I am profoundly grateful for the trust they have placed in me over these years. They have consistently been, and will continue to be, an enduring source of inspiration for me, both in Mathematics and beyond.

I wish to extend my sincere thanks to Daniele Bartoli and the entire Finite Geometry group at the University of Perugia, where I completed my external research stay. They warmly welcomed me and provided me with new and exciting learning opportunities, for which I am genuinely grateful.

I am sincerely thankful to Matteo Bonini, who first introduced me to the study of curves over finite fields and AG codes. He guided me in writing my Master's thesis and provided constant support during my early steps into the world of academic research.

I would like to warmly thank all the fellow PhD students that I have met through these years in Building 303B. I have had the pleasure of spending countless lunch breaks, coffee breaks and "Friday bars" with them, and their company has been wonderfully lively in every occasion. I am grateful for the cheerful camaraderie and mutual support that we have shared through our PhD journeys.

I wish to express many special thanks to my brilliant and gentle colleague

Jonathan Tilling Niemann, with whom I have had the pleasure of sharing the office during the last months of my PhD. I am truly glad for the friendship we have developed through our numerous conversations, spanning from Mathematics to the Danish language, cycling, music, and a refreshing variety of other topics. I would also really like to thank him for thoroughly reviewing the Danish version of the summary of this thesis.

I am deeply grateful to Sarah Ellinor Engell, for our friendship that unfolded during shared chocolate breaks and evolved into a very special treasure to me. Her boundless energy and free-spirited attitude have gently led me out of many comfort zones and have been an unshakeable source of strength in navigating both the ordinary and the extraordinary adventures of everyday life. I am thankful for our spontaneous explorations of some of the coziest corners in Copenhagen and for all her relentless help and encouragement throughout my study of the Danish language, which has been a wonderful source of motivation and enjoyment.

I am wholeheartedly grateful to Leonardo Landi, who has been and will forever be like a brother to me, both in Mathematics and in life. I feel unbelievably lucky for having shared with him a part of my PhD life, working together and learning from his mathematical wit and experience. I am indebted for our animated discussions, always flavoured with his lively humour, which invariably spanned a variety of topics and have inspired me in innumerable ways. I am thankful beyond words for the caring friendship we have developed, which has been an unwavering source of happiness for me, both through the darkest and the brightest of times.

In the most heartfelt way, I wish to thank all the friends in the team of MIX Copenhagen LGBTQIA+ Film Festival 2023: Ajo, Ale, Amanda, Ana, Andrea, Claudia, Ebrar, Hugo, Mihaela, Sina and Soll. Working with them for bringing MIX 2023 to life has been one of the most extraordinary experiences of my life, and words fall short in expressing how grateful I am for the wealth of knowledge and inspiration I have gained from each of them. I am immensely happy and feel extremely privileged for being part of such a vibrant and diverse team, and I am utterly excited for the upcoming Festival.

I would like to extend my warmest thanks to Alice, Daphne and Francesca, who truly are like family to me. We have faced together the toughest of times, standing by each other under any circumstances and despite the geographical distance. We have also shared countless joyful moments, bearing witness to and celebrating our individual growth and achievements. Our enduring friendship, with its heartwarming essence of sisterhood, has been a cornerstone in my life throughout the years, providing me with a sense of home that I know will always last.

I genuinely wish to express my deepest thanks to my parents, Celestina and Pietro, for their constant and loving support, as well as for all the opportunities they have provided me throughout my life. I am immensely grateful for their steadfast presence during every moment of need and for their complete and persistent trust in me.

Contents

Chapter 1

Introduction

Several aspects of our everyday life revolve around instant communications and unrestrained access to information. In this setting, a pivotal role is played by digital telecommunications, that make worldwide prompt transmission of data possible. However, transmitting information through a communication channel poses various challenges, that need to be faced in order to ensure reliability in the communication process. Indeed, a channel is inherently *noisy*, which means that, during the transmission, messages will possibly be altered due to the intrinsic properties of the channel.

In 1948, C. Shannon published the groundbreaking paper *A Mathematical Theory of Communication* [78], which laid the foundations of the field of Information Theory. In this work, he formalized the concept of transmission of information through a noisy communication channel, showing theoretically that, regardless of the degree of noise contamination, it is always possible to reliably transmit data, up to a certain maximum rate.

Therefore, these results initiated also the field of Coding Theory, that deals with the development and study of methods to ensure the reliable transmission of data through unreliable channels. There are different branches of Coding Theory, each focusing on certain specific problems regarding digital data transmission. Among these, *channel coding* is the one dealing with error correction, that is, the study and implementation of tools which, by means of adding *redundancy* to

a message, guarantee that a receiver is able to recover the original information even if the message is altered by the noise in the channel.

The techniques for adding redundancy to a message in such a way that, up to a certain extent, the detection and correction of errors is possible, are called *error correcting codes*. The first error correcting code was invented by R. W. Hamming in 1950 [43], paving the way for the future development of Coding Theory. A first intuitive way of adding redundancy to a message is, for instance, to transmit it multiple consecutive times across the channel. Nonetheless, when dealing with consistent amounts of information to be transmitted, this method is highly inefficient, if not unfeasible at all.

For this reason, several more sophisticated methods for *encoding* (adding redundancy) and *decoding* (retrieving the original information) have been developed and studied through the years. Among these methods, many have their roots in theoretical results from the fields of Algebra and Algebraic Geometry, and their study is therefore often referred to as Algebraic Coding Theory. In fact, the nowadays most widely used error correcting codes are *Reed-Solomon codes*, that are a special class of the so-called *Algebraic Geometry codes* (*AG codes* for short). The name of this kind of codes is due to the fact that they are constructed from algebraic curves (or, more in general, from algebraic varieties) over finite fields, which are a classical object of study in Algebraic Geometry. In the case of curves, as it will be more precisely discussed in Chapter 2, the construction of AG codes can be equivalently described in the setting of algebraic function fields of one variable, which is the perspective that we adopt throughout this manuscript.

While Reed-Solomon codes have several excellent properties and provide efficient solutions in many present real-life applications, the new developments of the digital era yield several new settings in which their features, in the long run, will not be enough. For instance, distributed data storage systems will soon need more efficient codes to handle the ever growing amount of data that is produced and needs to be safely stored across the globe. In this setting, AG codes could provide new error correcting codes able to tackle the new challenges in storage and communication systems, see for instance [17].

AG codes were first introduced by V.D. Goppa between the 70's and the 80's (see [36–40]), with a construction coming from algebraic curves over finite fields. Soon afterwards, in 1982, a striking result on these codes was proved by M. Tsfasman, S. Vlăduţ and T. Zink in [86], as a consequence of their work on modular and Shimura curves. Indeed, they related their results to the existence of sequences of asymptotically good codes and showed that there are some AG codes that are better than random codes, if the cardinality q of the field is a square and $q \geq 49$.

This result, that a large part of the mathematical community had before believed to be untrue, sparked a vast interest in the study of AG codes and their properties. Since a fundamental role in the construction of AG codes is played by the function field of the underlying curve, this entailed that the study of certain classes of function fields, in particular those with many rational places with respect to their genus, started thriving beyond the borders of pure Algebraic Geometry.

For instance, the *Weierstrass semigroup* at one or multiple places of a function field is an algebraic object that carries a notable amount of information with respect to the AG codes constructed form the function field, see for instance [21], [24, 25] and [62] for the one-point case and [50–52], [67, 68], [15] and [5] for the two-point case. In fact, the knowledge of Weierstrass semigroups can be used to compute the *dimension* of such codes, which is the parameter giving a measure of how much redundancy is added to the messages, or to estimate their *minimun distance*, which is instead the parameter giving a measure of how many errors can be detected or corrected.

The results contained in this thesis mostly concern Weierstrass semigroups at one or multiple places of certain maximal function fields, with the aim to expand the knowledge on these function fields also with respect to the construction of AG codes with good parameters. More specifically, the manuscript is organized in the following way.

In Chapter 2, we introduce the essential background setting necessary for the discussion of the work presented in the rest of the dissertation. In Section 2.1 and Section 2.2, we collect some fundamental results on algebraic function fields of one variable and algebraic curves, while in Section 2.3 and in Section 2.4 we recall some basic concepts regarding numerical semigroups and a generalization of Weierstrass semigroups to the case of pairs of places. Finally, in Section 2.5, we introduce Algebraic Geometry codes and certain bounds for the minimum distance of some classes of such codes.

In Chapter 3, a first major result is presented, which consists in the determination of the Weierstrass semigroups at all the places of one of the known maximal function fields with the third largest genus, that we denote by $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. As a consequence, the full automorphism group of the function field is also computed. More precisely, in Section 3.1, we describe $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ and set the notations that are used throughout the rest of the discussion, while also computing the principal divisors and the power series expansions at certain places of some specific functions. In particular, we explicitly determine a canonical divisor that is crucial for the results in Section 3.5 and Section 3.6. Section 3.2 deals instead with the computation of two families of functions in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ that play a key role for determining the Weierstrass semigroups. In Section 3.3, Section 3.4, Section 3.5 and Section 3.6, we then explicitly compute the semigroups at all

the places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, pointing out some final remarks on the Weierstrass places in Section 3.7. Lastly, the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is determined in Section 3.8.

In Chapter 4, we present a second major result of this thesis, that is the determination of the Weierstrass semigroups at certain pairs of places of two different families of maximal function fields: the Beelen-Montanucci function fields and the Skabelund function field obtained as a cyclic extension of the Suzuki one. As a result, we are able to study two-point AG codes from these function fields. In Section 4.1, we study the case of two-point codes from the Beelen-Montanucci function fields $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, for all $n \geq 3$ odd, and we compare our results with those obtained in [5] from the Garcia-Güneri-Stichtenoth function fields $\mathbb{F}_{q^{2n}}(\mathcal{GGS}_n)$. On the other hand, in Section 4.2, we study the case of two-point codes from the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$.

In Chapter 5, the final contribution that we present is the study of upper and lower bounds for the constant $D(q)$ introduced by M. Homma in [49]. This constant captures the asymptotic behaviour of the number of rational points of projective curves over $\mathbb{F}_q$, when the degree d of the curve becomes large with respect to q. We first slightly improve Homma's upper bound on $D(q)$, in Section 5.1, by means of refining the argument provided in [49]. Afterwards, in Section 5.2, we explicitly construct a sequence of curves whose degrees are close to their number of rational points, in order to show that $D(q) \geq 1$. Finally, in Section 5.3, we prove the lower bound $D(q^2) \geq \frac{q^2-q}{q+1}$, using a particular tower of function fields over $\mathbb{F}_{q^2}$ that was constructed recursively by A. Garcia and H. Stichtenoth in [31]. Although Weierstrass semigroups are not the main focus of this final chapter, they still play a crucial role for the proof of the results in Section 5.3, which constitutes the main part of the chapter.

Chapter 2

Background

The purpose of this chapter is to summarize the essential background theory necessary for the results presented in the thesis, and to set the notations that are used throughout the manuscript. More specifically, Section 2.1 and Section 2.2 contain a collection of fundamental results on algebraic function fields of one variable and algebraic curves, while Section 2.3 and Section 2.4 include salient concepts regarding numerical semigroups and a generalization of Weierstrass semigroups to the case of pairs of places. Finally, Section 2.5 consists of a brief introduction to Algebraic Geometry codes and to some specific bounds for the minimum distance of certain classes of the aforementioned codes.

2.1 Algebraic function fields of one variable

Almost all the results contained in this section, including their proofs, can be found in [81, Chapters 1,3,4,5,7], to which we refer for a more detailed and thorough exposition. For the results not contained in [81], we specify the related references throughout the discussion.

Let K be a perfect field of characteristic $\mathrm{char}(K) = p \geq 0$ and let $\mathbb{K}$ denote a fixed algebraic closure of K.

Definition 2.1. *An* algebraic function field F of one variable *over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

Henceforth, let F be an algebraic function field of one variable over K. We assume that K is the *full constant field* of F, which means that $K = \{z \in F \mid z \text{ is algebraic over } K\}$ and, for brevity, we simply refer to F as a *function field*. The most basic example of a function field is the *rational function field* $F = K(x)$, for some $x \in F$ which is transcendental over K.

Definition 2.2. *A* discrete valuation *of F is a function $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties:*

(i) $v(x) = \infty \Longleftrightarrow x = 0$

(ii) $v(xy) = v(x) + v(y) \ \forall\ x, y \in F$

(iii) $v(x + y) \geq min\{v(x), v(y)\} \ \forall\ x, y \in F$

(iv) $v(a) = 0 \ \ \forall\ 0 \neq a \in K.$

For a discrete valuation v of F, the *Strict Triangle Inequality* holds, namely if $x, y \in F$ with $v(x) \neq v(y)$, then $v(x + y) = \min\{v(x), v(y)\}$.

A *valuation ring* of a function field F is a ring O_P such that $K \subsetneqq \mathrm{O}_P \subsetneqq F$ and for all $z \in F$ we have that either $z \in \mathrm{O}_P$ or $z^{-1} \in \mathrm{O}_P$. It can be shown that O_P is a local principal ideal domain whose unique maximal ideal P is called a *place* of the function field F. If $t \in F$ is a generator of P, then t is said to be a *local parameter* at P and each $0 \neq z \in F$ has a unique representation of the form $z = t^n u$, for some $n \in \mathbb{Z}$ and $u \in \mathrm{O}_P^*$, with O_P^* being the group of units of O_P. In particular, these properties show that O_P is in fact a *discrete valuation ring* (DVR). The discrete valuation of F associated with O_P is the map $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ such that $v_P(0) := \infty$ and $v_P(z) := n$, for $0 \neq z \in F$, $z = t^n u$, with t a local parameter at P and $u \in \mathrm{O}_P^*$.

More specifically, a local parameter t can be used in order to define an embedding of F in the field of formal Laurent series $F((T))$, where T is a variable. This means that every $z \in F$ can be written as

$$z = \sum_{i=v_P(z)}^{\infty} c_i t^i, \quad c_i \in K.$$

Note that a valuation ring O_P is uniquely determined by its maximal ideal P, as $\mathrm{O}_P = \{z \in F \mid z^{-1} \notin P\}$. More precisely, the following result shows that places, valuation rings and discrete valuations are essentially equivalent notions.

Theorem 2.3. *Let F be a function field over K.*

(i) For a place P of F, the function v_P defined above is a discrete valuation of F. Moreover we have

$$\begin{aligned} \mathrm{O}_P &= \{z \in F \mid v_P(z) \geq 0\} \\ \mathrm{O}_P^* &= \{z \in F \mid v_P(z) = 0\} \\ P &= \{z \in F \mid v_P(z) > 0\}. \end{aligned}$$

(ii) An element $x \in F$ is a local parameter at P if and only if $v_P(x) = 1$.

(iii) Conversely, suppose that v is a discrete valuation of F. Then the set $P := \{z \in F \mid v_P(z) > 0\}$ is a place of F and $\mathrm{O}_P = \{z \in F \mid v_P(z) \geq 0\}$ is the corresponding valuation ring.

Let P be a place of F and O_P its valuation ring, then O_P/P is a field and, for $x \in \mathrm{O}_P$, we define $x(P) \in \mathrm{O}_P/P$ to be the residue class of x modulo P. Since $K \subseteq \mathrm{O}_P$ and $K \cap P = \{0\}$, it holds that the residue class map $\mathrm{O}_P \longrightarrow \mathrm{O}_P/P$ induces a canonical embedding of K into O_P/P, so that we can always consider K as a subfield of $F_P := \mathrm{O}_P/P$ via this embedding. The *degree* of a place P is then defined as $\deg(P) := [F_P : K]$ and the places of degree one are called *K-rational* (or just *rational*).

Let now $\mathbb{P}_F := \{P \mid P \text{ is a place of } F\}$ be the set of places of F and let $z \in F$ and $P \in \mathbb{P}_F$. We say that P is a *zero* of z if $v_P(z) > 0$, while P is said to be a *pole* of z if $v_P(z) < 0$. If $v_P(z) = m > 0$, P is a zero of z of *order* (or *multiplicity*) m; if $v_P(z) = -m < 0$, P is a pole of z of *order* (or *multiplicity*) m.

The following results ensure that the degree of a place is always finite and that $\mathbb{P}_F$ is always non-empty.

Proposition 2.4. *If P is a place of F and $0 \neq x \in P$, then*

$$\deg(P) \leq [F : K(x)] < \infty.$$

Lemma 2.5. *In a function field F over K every element $0 \neq x \in F$ has only finitely many zeros and poles, and each $z \in F$ transcendental over K has at least one zero and one pole. As a consequence, $\mathbb{P}_F \neq \emptyset$.*

We recall now the concepts of divisors, canonical divisors and Riemann-Roch spaces. These notions are in fact needed in order to define the genus of the function field F and to state the Riemann-Roch Theorem.

Definition 2.6. *The* divisor group $\mathrm{Div}(F)$ *of F is defined as the (additively written) free abelian group which is generated by the places of F. The elements of* $\mathrm{Div}(F)$ *are called* divisors *of F and each is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

with $n_P \in \mathbb{Z}$, almost all $n_P = 0$. The support *of D is defined as*

$$\mathrm{supp}(D) := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ are added coefficient-wise

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P,$$

and the zero element of the divisor group $\mathrm{Div}(F)$ *is the divisor*

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \quad \text{all} \quad r_P = 0.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathrm{Div}(F)$ we define $v_Q(D) := n_Q$. A partial ordering on $\mathrm{Div}(F)$ *is defined by*

$$D_1 \leq D_2 : \quad \Longleftrightarrow \quad v_P(D_1) \leq v_P(D_2) \quad \forall\ P \in \mathbb{P}_F.$$

A divisor $D \geq 0$ is called effective*, and the* degree *of a divisor is defined as*

$$\deg(D) := \sum_{P \in \mathbb{P}_F} v_P(D) \deg(P).$$

Lemma 2.5 ensures that the following definition can be stated.

Definition 2.7. *Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (resp. poles) of x in $\mathbb{P}_F$. We define*

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \qquad \textit{the } \text{zero divisor } \textit{of } x$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P, \qquad \textit{the } \text{pole divisor } \textit{of } x$$

$$(x) := (x)_0 - (x)_\infty = \sum_{P \in \mathbb{P}_F} v_P(x) P, \quad \textit{the } \text{principal divisor } \textit{of } x.$$

A remarkable result is that all principal divisors have degree zero. More precisely, for any $x \in F \setminus K$ it holds that

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

The set of principal divisors $\mathrm{Princ}(F) := \{(x) \mid 0 \neq x \in F\}$ is a normal subgroup of $\mathrm{Div}(F)$, and the quotient group $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ is called the *divisor class group* of F. Two divisors $D, D' \in \mathrm{Div}(F)$ are said to be *equivalent*, $D \sim D'$, if their images in $\mathrm{Cl}(F)$ via the projection map are the same, i.e., if $D = D' + (x)$ for some $x \in F \setminus \{0\}$.

Definition 2.8. *Let $A \in \mathrm{Div}(F)$, the* Riemann-Roch space *associated to A is*

$$L(A) := \{x \in F \setminus \{0\} \mid (x) \geq -A\} \cup \{0\}.$$

The Riemann-Roch space $L(A)$ is a K-vector space and its dimension is denoted by $\ell(A)$. In particular, $\ell(A) = 0$ if $\deg(A) < 0$, see [81, Corollary 1.4.12]. It can be shown that there exists a constant $\gamma \in \mathbb{Z}$ such that, for all divisors $A \in \mathrm{Div}(F)$, it holds $\deg(A) - \ell(A) \leq \gamma$. As a result, the *genus* of a function field F can be defined in the following way.

Definition 2.9. *The* genus $g(F)$ *of F is defined by*

$$g(F) := \max\{\deg(A) - \ell(A) + 1 \mid A \in \mathrm{Div}(F)\} \geq 0.$$

Let now p be a prime number, $h \in \mathbb{Z}_{>0}$ and $q := p^h$. Denote by $\mathbb{F}_q$ the finite field with q elements and as $\overline{\mathbb{F}}_q$ a fixed algebraic closure of $\mathbb{F}_q$. Consider F a function field over $\mathbb{F}_q$ of genus g and denote by $N(F)$ the cardinality of the set $\{P \in \mathbb{P}_F \mid P \text{ is } \mathbb{F}_q\text{-rational}\}$. Then, the following renowned result by H. Hasse and A. Weil gives both an upper and a lower bound for the number $N(F)$.

Theorem 2.10 (Hasse-Weil)**.** *Let F be a function field over $\mathbb{F}_q$ of genus g. Then*

$$|N(F) - (q+1)| \leq 2g\sqrt{q}.$$

A function field F with genus $g > 0$ and attaining the Hasse-Weil upper bound is said to be $\mathbb{F}_q$*-maximal* or simply *maximal*, if the field of definition is clear.

Remark 2.11. *If F has genus zero, it trivially attains the Hasse-Weil upper bound. On the other hand, if the genus of F is positive, then a necessary condition for F to be maximal is that q is a square.*

Example 2.12 (The Hermitian function field)**.** *The* Hermitian *function field is defined over* $\mathbb{F}_{q^2}$ *as* $H := \mathbb{F}_{q^2}(u, v)$*, with* $u^{q+1} + v^{q+1} + 1 = 0$*. It can be shown that its genus is equal to* $\frac{q(q-1)}{2}$ *and that* H *is* $\mathbb{F}_{q^2}$*-maximal. In [74], H.-G. Rück and H. Stichtenoth showed that* H *is in fact the only* $\mathbb{F}_{q^2}$*-maximal function field of genus* $\frac{q(q-1)}{2}$*, up to* $\mathbb{F}_{q^2}$*-isomorphism.*

On the other hand, the asymptotic behaviour of the number of rational places of a function field over $\mathbb{F}_q$, when the genus g becomes large with respect to q, is described by Ihara's constant. For a given q, let $g \geq 0$ and define

$$N_q(g) := \max\{N(F) \mid F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g\}.$$

Then, *Ihara's constant* is the real number

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1, \tag{2.1}$$

where the inequality on the right-hand side is the celebrated bound by V. Drinfeld and S. Vlăduţ (see [20, Theorem 1]). If q is a square, it was proved by Y. Ihara in [56] and by M. Tsfasman, S. Vlăduţ and T. Zink in [86] that $A(q)$ attains the Drinfeld-Vlăduţ bound, that is, $A(q) = \sqrt{q} - 1$.

Let henceforth F be a function field over K of genus g.

Definition 2.13. *An* adele *of* F *is a mapping*

$$\alpha : \begin{cases} \mathbb{P}_F \longrightarrow F \\ P \longmapsto \alpha_P \end{cases}$$

such that $\alpha_P \in \mathrm{O}_P$ *for almost all* $P \in \mathbb{P}_F$*. The set*

$$\mathcal{A}_F := \{\alpha \mid \alpha \text{ is an adele of } F\}$$

is called the adele space *of* F *and it is a* K*-vector space.*

For a divisor $A \in \mathrm{Div}(F)$, we define the following K-subspace of $\mathcal{A}_F$:

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \text{ for all } P \in \mathbb{P}_F\}.$$

A *Weil differential* of F is a K-linear map $\omega : \mathcal{A}_F \longrightarrow K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in \mathrm{Div}(F)$. It can be shown that the set

$$\Omega_F := \{\omega \mid \omega \text{ is a Weil differential of } F\}$$

of Weil differentials of F is in fact a one-dimensional vector space over F.

For each Weil differential $\omega \neq 0$, consider the set

$$M(\omega) := \{A \in \mathrm{Div}(F) \mid \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

It can be proved that there is a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ for all $A \in M(\omega)$. Such a divisor is usually referred to as the divisor (ω) of the differential ω and it is called a *canonical divisor*. For $P \in \mathbb{P}_F$, the valuation of ω at P is hence defined as $v_P(\omega) := v_P((\omega))$ and P is said to be a zero (resp. pole) of ω if $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). Moreover, a Weil differential ω is called *regular at* P if $v_P(\omega) \geq 0$, and it is said to be *regular* (or *holomorphic*) if it is regular at all places $P \in \mathbb{P}_F$.

For a place $P \in \mathbb{P}_F$ and $x \in F$, define $\iota_P(x) \in \mathcal{A}_F$ to be the adele such that

$$\iota_P(x)(Q) = \begin{cases} x & \text{if} \quad Q = P \in \mathbb{P}_F, \\ 0 & \text{if} \quad Q \neq P \in \mathbb{P}_F. \end{cases}$$

The *local component* of a Weil differential $\omega \in \Omega_F$ at P is defined to be the K-linear mapping

$$\omega_P : \begin{cases} F \longrightarrow K \\ x \longmapsto \omega(\iota_P(x)). \end{cases}$$

An important property of canonical divisors of a function field F is that any two of them are equivalent, i.e., they form a whole class in the divisor class group $\mathrm{Cl}(F)$, which is called the *canonical class* of F. This shows in particular that any two canonical divisors have the same degree, which can be proven to be $2g - 2$ as a consequence of the following fundamental theorem.

Theorem 2.14 (Riemann-Roch Theorem)**.** *Let W be a canonical divisor of F. Then for each divisor $A \in \mathrm{Div}(F)$,*

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

A divisor $A \in \mathrm{Div}(F)$ is called *non-special* if

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

As a consequence of the Riemann-Roch Theorem, it directly follows that a divisor A with $\deg(A) \geq 2g - 1$ is non-special.

The Riemann-Roch Theorem is also crucial for investigating the properties of elements of F having exactly one pole, as it constitutes an essential tool for the proof of Weierstrass Gap Theorem.

Definition 2.15. *Let $P \in \mathbb{P}_F$ and $n \in \mathbb{Z}_{\geq 0}$. The integer n is called a* pole number *of P if there exists an element $x \in F$ such that $(x)_\infty = nP$. Otherwise, n is called a* gap number *of P.*

The set of pole numbers of a place P is denoted by $H(P)$ and it is called the *Weierstrass semigroup* at P, since it is a sub-semigroup of the additive semigroup $\mathbb{N}$ (in our notations, $0 \in \mathbb{N}$). Its elements are usually referred to as the *non-gaps* at P. The set $G(P) := \mathbb{N} \setminus H(P)$ is instead the set of gap numbers at P and its elements are called the *gaps* at P.

Theorem 2.16 (Weierstrass Gap Theorem)**.** *Let F be a function field of genus g and P a place of degree 1. Then, there are exactly g gap numbers $i_1 < \cdots < i_g$ of P and, in particular, $i_1 = 1$ and $i_g \leq 2g - 1$.*

Remark 2.17. *Let $K = \mathbb{K}$ and let F be a function field over K. It can be shown (see [82]) that almost all the places of F (that is, all but finitely many) have the same Weierstrass semigroup, that is hence referred to as the* generic *semigroup. On the other hand, the finitely many places of F having a Weierstrass semigroup that is different from the generic one are called the* Weierstrass places *of F.*

Let ω be a regular Weil differential of F. The following result relates the valuation of ω at a place $P \in \mathbb{P}_F$ to the gaps at P.

Proposition 2.18 ([76, Corollary 14.2.5])**.** *Let F be a function field over K of genus g. Let P be a place of F and ω be a regular differential of F. Then $v_P(\omega) + 1$ is a gap at P.*

Let now F' be a function field over K where $F' \supseteq F$ is an algebraic extension of F, that we denote by F'/F. Note that, since we assumed K to be perfect, the extension F'/F is separable. As above, let $\mathbb{P}_{F'}$ be the set of places of F' and let $P' \in \mathbb{P}_{F'}$. The place P' is said to *lie over* $P \in \mathbb{P}_F$ if $P \subseteq P'$. Similarly, we say that P' is an *extension* of P, or that P *lies under* P', and we write $P'|P$.

It can be shown that, for each place $P' \in \mathbb{P}_{F'}$, there is precisely one place $P \in \mathbb{P}_F$ such that $P'|P$, namely $P = P' \cap F$. Conversely, each place $P \in \mathbb{P}_F$ has at least one, but only finitely many extensions $P' \in \mathbb{P}_{F'}$. Moreover, for an extension $P'|P$ there is a canonical embedding of $F_P := \mathrm{O}_P/P$ as a subfield of $F'_{P'} := \mathrm{O}_{P'}/P'$, given by $x(P) \longmapsto x(P')$, for all $x \in \mathrm{O}_P$. Therefore, we can consider the field extension $F'_{P'}/F_P$ and define $f(P'|P) := [F'_{P'} : F_P]$, that is called the *relative degree* of P' over P. Furthermore, there exists a positive integer $e(P'|P)$, called the *ramification index* of P' over P, such that $v_{P'}(x) = e(P'|P) \cdot v_P(x)$ for all $x \in F$.

Theorem 2.19 (Kummer). *Consider $P \in \mathbb{P}_F$ and assume that $F' = F(y)$, with $y \in F'$ such that its minimal polynomial over F is $\varphi(T) \in \mathrm{O}_P[T]$. Denote by $\bar{\varphi}(T)$ the polynomial whose coefficients are the residue classes in F_P of the coefficients of $\varphi(T)$. Moreover, let*

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i} \in F_P[T]$$

be the decomposition of $\bar{\varphi}(T)$ into irreducible factors over F_P. Choose monic polynomials $\varphi_i(T) \in \mathrm{O}_P[T]$ such that

$$\bar{\varphi}_i(T) = \gamma_i(T) \quad \textit{and} \quad \deg\, \varphi_i(T) = \deg\, \gamma_i(T).$$

Then, for $1 \le i \le r$, there are places $P_i \in \mathbb{P}_{F'}$ such that

$$P_i|P, \quad \varphi_i(y) \in P_i, \quad f(P_i|P) \ge \deg\, \gamma_i(T) \quad \textit{and} \quad P_i \ne P_j \textit{ for } i \ne j.$$

Furthermore, if

$$\varepsilon_i = 1 \quad \forall\, i = 1, \ldots, r,$$

then there exists precisely one place $P_i \in \mathbb{P}_{F'}$ with $P_i|P$ and $\varphi_i(y) \in P_i$, for $1 \le i \le r$. The places $P_1, \ldots, P_r$ are exactly all the places of F' lying over P and

$$\varepsilon_i = e(P_i|P), \quad \deg\, \gamma_i(T) = f(P_i|P)$$

for all $i = 1, \ldots, r$.

Let F'' be another function field over K, such that F''/F' is an algebraic extension, and let $P'' \in \mathbb{P}_{F''}$ be a place of F'' lying over $P' \in \mathbb{P}_{F'}$. Then,

$$e(P''|P) = e(P''|P') \cdot e(P'|P) \quad \text{and} \quad f(P''|P) = f(P''|P') \cdot f(P'|P).$$

Moreover, for a place $P \in \mathbb{P}_F$ we define its *conorm* with respect to F'/F as the divisor of F' given by

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

The following result combines the just introduced definitions into a single fundamental equality.

Theorem 2.20 (Fundamental Equality). *Let F'/F be a finite extension, let $P \in \mathbb{P}_F$ and let $P'_1, \ldots, P'_m \in \mathbb{P}_{F'}$ be all the places of F' lying over P. Then*

$$[F' : F] = \sum_{i=1}^{m} e(P'_i|P) \cdot f(P'_i|P).$$

If F'/F is a finite extension of degree n, we say that $P \in \mathbb{P}_F$ *splits completely* in F'/F if there are exactly n distinct places $P' \in \mathbb{P}_{F'}$ lying over it. Note that, by the Fundamental Equality, this implies that $e(P'|P) = f(P'|P) = 1$ for all the extensions of P. Conversely, we say that P is *totally ramified* in F'/F if there is exactly one place $P' \in \mathbb{P}_{F'}$ such that $P'|P$ and $e(P'|P) = n$. Furthermore, P is said to be *ramified* in F'/F if there is at least one extension $P'|P$ such that $e(P'|P) > 1$, while we say that P is *unramified* in F'/F if $e(P'|P) = 1$ for all $P'|P$. The function field extension F'/F is said to be *ramified* (resp. *unramified*) if at least one place $P \in \mathbb{P}_F$ is ramified in F'/F (resp. if all $P \in \mathbb{P}_F$ are unramified in F'/F).

We recall now the Riemann-Hurwitz Genus Formula, that is a key result relating the genus g of F to the genus g' of F', for F'/F a finite separable extension of function fields. Let $P \in \mathbb{P}_F$ and let O'_P be the integral closure of O_P in F'. Denote by

$$\mathcal{C}_P := \{z \in F' \mid \mathrm{Tr}_{F'/F}(z \cdot \mathrm{O}'_P) \subseteq \mathrm{O}_P\}$$

the *complementary module* over O_P, where $\mathrm{Tr}_{F'/F}(\cdot)$ denotes the usual field trace. Then, there exists an element $t \in F'$ such that $\mathcal{C}_P = t \cdot \mathrm{O}'_P$ and $v_{P'}(t) \leq 0$ for all $P'|P$. Moreover, for almost all $P \in \mathbb{P}_F$ we have $\mathcal{C}_P = \mathrm{O}'_P$, so that the *different* divisor of the extension F'/F can be defined in the following way.

Definition 2.21. *Let $P \in \mathbb{P}_F$ and $\mathcal{C}_P = t \cdot \mathrm{O}'_P$ be the complementary module over O_P. Then, for $P'|P$ we define the* different exponent *of P' over P as*

$$d(P'|P) := -v_{P'}(t) \geq 0.$$

The different *of F'/F is defined to be the effective divisor*

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'.$$

Theorem 2.22 (Riemann-Hurwitz Genus Formula)**.** *Let F be a function field over K of genus g and F' be a function field over K of genus g' such that F'/F is a finite separable extension. Then*

$$2g' - 2 = [F' : F](2g - 2) + \deg \mathrm{Diff}(F'/F).$$

Theorem 2.23 (Dedekind's Different Theorem)**.** *Let F'/F be as before and $P \in \mathbb{P}_F$. For all $P' \in \mathbb{P}_{F'}$ with $P'|P$, it holds that $d(P'|P) \geq e(P'|P) - 1$. In particular, $d(P'|P) = e(P'|P) - 1$ if and only if $e(P'|P)$ is not divisible by the characteristic of K.*

If the characteristic of K is positive and divides $e(P'|P)$, Dedekind's Different Theorem does not provide an effective way for computing the different exponent.

However, if the extension F'/F is a Galois extension, there is another fundamental result providing an explicit formula for $d(P'|P)$, namely Hilbert's Different Formula. To the aim of stating this result, we start by discussing some generalities regarding the automorphisms of a function field F, and subsequently we recall the definition of Galois extension of function fields.

Let F be a function field defined over K and let $\mathbb{K}$ be a fixed algebraic closure of K. Furthermore, let $\Psi \supseteq F$ be a fixed algebraic closure of F and consider the compositum of F and $\mathbb{K}$ in Ψ, namely $\bar{F} := F\mathbb{K}$. The field $\bar{F}$ is a function field extending F and it is called a *constant field extension* of F. The group of $\mathbb{K}$-*automorphisms* of F, also referred to as the *full automorphism group* of F, is defined as

$$\mathrm{Aut}(F) := \{\sigma : \bar{F} \longrightarrow \bar{F} \mid \sigma \text{ is an isomorphism with } \sigma(z) = z \ \forall z \in \mathbb{K}\}.$$

In particular, if F is defined over $K \neq \mathbb{K}$, then we also define the group $\mathrm{Aut}_K(F)$ of K-*rational automorphisms* of F, that is, the subgroup of $\mathrm{Aut}(F)$ given by

$$\mathrm{Aut}_K(F) := \{\sigma \in \mathrm{Aut}(F) \mid \sigma(F) \subseteq F\}.$$

By [41, Theorem 3.10] it holds that, if F is a maximal function field defined over $\mathbb{F}_q$ of genus strictly larger than 1, then $\mathrm{Aut}_{\mathbb{F}_q}(F) = \mathrm{Aut}(F)$. Moreover, it is interesting to observe that places lying in the same orbit under the action of $\mathrm{Aut}(F)$ have the same Weierstrass semigroup. Indeed, as a more general case of [81, Lemma 3.5.2 (a)], it holds that

$$v_{\sigma(P)}(y) = v_P(\sigma^{-1}(y)), \tag{2.2}$$

for any $y \in F$, $P \in \mathbb{P}_F$ and $\sigma \in \mathrm{Aut}(F)$, which implies precisely that $H(P)$ and $H(\sigma(P))$ are equal (see Definition 2.15).

Let now $F' \supseteq F$ be another function field defined over K, such that F'/F is a finite separable extension of function fields. The automorphism group of the extension F'/F is defined as

$$\mathrm{Aut}(F'/F) := \{\sigma : F' \longrightarrow F' \mid \sigma \text{ is an isomorphism with } \sigma(z) = z \ \forall z \in F\},$$

and [81, Lemma 3.5.2] ensures that equation (2.2) holds in particular in the case $\sigma \in \mathrm{Aut}(F'/F)$. Moreover, it also guarantees that, for all $\sigma \in \mathrm{Aut}(F'/F)$ and for all $P' \in \mathbb{P}_{F'}$, if $P'|P \in \mathbb{P}_F$ then $\sigma(P')|P$ and

$$e(\sigma(P')|P) = e(P'|P), \quad f(\sigma(P')|P) = f(P'|P) \quad \text{and} \quad d(\sigma(P')|P) = d(P'|P).$$

The extension F'/F is said to be *Galois* if the automorphism group $\mathrm{Aut}(F'/F)$ has order equal to $[F' : F]$. If this condition is satisfied, $\mathrm{Aut}(F'/F)$ is called

the *Galois group* of F'/F and denoted by $\mathrm{Gal}(F'/F)$. An important observation concerning a Galois extension F'/F is that, if $P \in \mathbb{P}_F$, then $\mathrm{Gal}(F'/F)$ acts transitively on the set $\{P' \in \mathbb{P}_{F'} \mid P' \text{ lies over } P\}$ of extensions of P in F' (see [81, Theorem 3.7.1]).

Let F'/F be a Galois extension with Galois group $G := \mathrm{Gal}(F'/F)$ and consider $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ such that $P'|P$. For every $i \in \mathbb{Z}_{\geq -1}$, the *i-th ramification group* of $P'|P$ is defined as

$$G_i(P'|P) := \{\sigma \in G \mid v_{P'}(\sigma(z) - z) \geq i + 1 \ \forall z \in \mathrm{O}_{P'}\}.$$

For all $i \in \mathbb{Z}_{\geq -1}$, the i-th ramification group $G_i := G_i(P'|P)$ is a subgroup of G and, in particular,

$$G_{-1} \supseteq G_0 \supseteq \cdots G_i \supseteq G_{i+1} \supseteq \cdots \quad \text{with } G_m = \{id\} \text{ for } m \text{ sufficiently large,}$$

where id denotes the identity element of G. Furthermore, it holds that

$$|G_{-1}| = e(P'|P) \cdot f(P'|P) \quad \text{and} \quad |G_0| = e(P'|P),$$

and, if the characteristic of F is $p > 0$, then G_1 is a normal subgroup of G_0 and $|G_1| = p^\ell$, for some $\ell \in \mathbb{Z}_{\geq 0}$, while the quotient group G_0/G_1 is cyclic and has order relatively prime to p. Moreover, for all $i \in \mathbb{Z}_{\geq 1}$, the group G_{i+1} is a normal subgroup of G_i and the quotient G_i/G_{i+1} is an elementary abelian group of exponent p.

We are now ready to state the following crucial result, that relates the different exponent $d(P'|P)$ and the ramification groups $G_i(P'|P)$.

Theorem 2.24 (Hilbert's Different Formula)**.** *Let F'/F be a Galois extension of function fields, $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ such that $P'|P$. Then*

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

Since eventually, for i large enough, $G_i(P'|P) = \{id\}$, note that the above sum is in fact finite.

We conclude this section by recalling the definitions of two specific kinds of Galois extensions, namely Kummer and Artin-Schreier extensions.

Proposition 2.25 (Kummer extensions)**.** *Let F be an algebraic function field over K, with K containing a primitive n-th root of unity ($n > 1$ and relatively prime to* $\mathrm{char}(K)$*). Assume that $u \in F$ is an element such that*

$$u \neq w^d \quad \textit{for all } w \in F \textit{ and } d \mid n, d > 1.$$

Let $F' = F(y)$, with $y^n = u$. Then F'/F is said to be a Kummer extension *of F. It is a cyclic Galois extension of degree n and the minimal polynomial of y over F is $T^n - u$. Moreover, for $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ such that $P'|P$, define $r_P := \gcd(n, v_P(u)) > 0$. Then*

$$e(P'|P) = \frac{n}{r_P} \quad \text{and} \quad d(P'|P) = \frac{n}{r_P} - 1.$$

The following corollary is a special case of Proposition 2.25, which we highlight as it is often particularly convenient for showing that certain extensions are Kummer extensions.

Corollary 2.26 ([81, Corollary 3.7.4])**.** *Let F be an algebraic function field over K and $F' = F(y)$, with $y^n = u \in F$ and $n \not\equiv 0 \pmod{\mathrm{char}(K)}$. Further, assume that K contains a primitive n-th root of unity and that there exists a place $Q \in \mathbb{P}_F$ such that $\gcd(v_Q(u), n) = 1$. Then K is the full constant field of F', the extension F'/F is cyclic of degree n and*

$$g(F') = 1 + n(g(F) - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P)\deg(P),$$

where r_P is as defined in Proposition 2.25.

Proposition 2.27 (Artin-Schreier extensions)**.** *Let F be an algebraic function field over K, with $\mathrm{char}(K) = p > 0$. Assume that $u \in F$ is an element such that*

$$u \neq w^p - w \quad \text{for all } w \in F.$$

Let $F' = F(y)$, with $y^p - y = u$. Then F'/F is said to be an Artin-Schreier extension *of F. It is a cyclic Galois extension of degree p and, for $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ such that $P'|P$, the following hold. Let m_P be the integer*

$$m_P := \begin{cases} m & \text{if } \exists\, z \in F \text{ with } v_P(u - (z^p - z)) = -m < 0, \quad m \not\equiv 0 \pmod{p} \\ -1 & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

Then, P is unramified if and only if $m_P = -1$, while it is totally ramified if and only if $m_P > 0$. In the latter case, if P' is the unique place of F' lying over P, then $d(P'|P) = (p-1)(m_P + 1)$.

2.2 Algebraic curves over a finite field

For the results collected in this section and their proofs, our main references are [29] and [46, Chapters 1,3,4,8].

As in the previous section, let K be a perfect field of characteristic $\mathrm{char}(K) = p \geq 0$ and let $\mathbb{K}$ denote a fixed algebraic closure of K. Let K^* (resp. $\mathbb{K}^*$) be the multiplicative group of invertible elements of K (resp. $\mathbb{K}$).

For a positive integer n, we define the n-th dimensional affine space over $\mathbb{K}$ as the set of n-tuples of elements of $\mathbb{K}$, namely

$$\mathbb{A}^n := \{(a_0, \ldots, a_{n-1}) \mid a_i \in \mathbb{K}\ \forall i = 0, \ldots, n-1\}.$$

The n-th dimensional projective space $\mathbb{P}^n$ over $\mathbb{K}$ is the set of $(n+1)$-tuples $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}$ with at least one nonzero coordinate, modulo the equivalence relation

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \quad \Longleftrightarrow \quad \exists \lambda \in \mathbb{K}^* \text{ such that } a_i = \lambda b_i\ \forall i = 0, \ldots, n.$$

The equivalence class of a tuple $(a_0, \ldots, a_n)$ is denoted by $[a_0 : \cdots : a_n] := \{(\lambda a_0, \ldots, \lambda a_n) \mid \lambda \in \mathbb{K}^*\}$ and it is called a *point* of $\mathbb{P}^n$ with *homogeneous coordinates* $a_0, \ldots, a_n$.

A *homogeneous polynomial* in $\mathbb{K}[x_0, \ldots, x_n]$ is either a constant polynomial or a polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ of positive degree d such that $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in \mathbb{K}$. An ideal $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ is said to be a *homogeneous ideal* if it is generated by homogeneous polynomials. To a homogeneous ideal $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ we associate the subset of $\mathbb{P}^n$

$$V(I) := \{P \text{ point of } \mathbb{P}^n \mid f(P) = 0,\ \forall \text{ homogeneous } f \in I\} \subseteq \mathbb{P}^n,$$

which is called a *projective algebraic set*. This definition allows to endow $\mathbb{P}^n$ with the Zariski topology, in which the closed sets are precisely projective algebraic sets.

Let $V \subseteq \mathbb{P}^n$ be a projective algebraic set. In the following discussion, we indicate as $V(\mathbb{K})$ the collection of points of V, and as $V(K)$ the subset of $V(\mathbb{K})$ containing the points with homogeneous coordinates that can all be chosen to be elements of K. The points in $V(K)$ are said to be *K-rational*, or simply *rational*, if the field of definition is clear. The *homogeneous ideal of* V is defined as

$$I(V) := \{f \in \mathbb{K}[x_0, \ldots, x_n] \mid f \text{ is homogeneous}, \forall P \in V(\mathbb{K})\ f(P) = 0\}.$$

A projective algebraic set V is said to be *irreducible* over $\mathbb{K}$ (or *absolutely irreducible*) if it cannot be written as $V = V_1 \cup V_2$, with $V_1, V_2 \subseteq \mathbb{P}^n$ algebraic sets both different from V. An absolutely irreducible projective algebraic set is said to be a *projective variety*, and it can be shown that V is a projective variety if and only if $I(V)$ is a prime ideal of $\mathbb{K}[x_0, \ldots, x_n]$.

For a projective variety $V \subseteq \mathbb{P}^n$, we define the *homogeneous coordinate ring* of V to be

$$\mathbb{K}[V] := \mathbb{K}[x_0, \ldots, x_n]/I(V),$$

while the *field of rational functions* of V is defined to be the following subfield of the field of fractions of $\mathbb{K}[V]$:

$$\mathbb{K}(V) := \left\{ \frac{f + I(V)}{h + I(V)} \;\middle|\; f, h \text{ homogeneous}, \deg(f) = \deg(h),\ h \notin I(V) \right\}. \tag{2.3}$$

The field $\mathbb{K}(V)$ is also simply referred to as the *function field* of V and the *dimension* of the variety V is defined as the transcendence degree of the field extension $\mathbb{K}(V)/\mathbb{K}$.

A *projective algebraic curve* $\mathcal{X} \subseteq \mathbb{P}^n$ is a projective variety of dimension 1. The curve $\mathcal{X}$ is said to be *defined over* K if its homogeneous ideal $I(\mathcal{X})$ can be generated by homogeneous polynomials with coefficients in K. If that is the case, $I(\mathcal{X})$ is also a prime ideal of $K[x_0, \ldots, x_n]$ and we can define the *K-rational function field* of $\mathcal{X}$, denoted by $K(\mathcal{X})$, in a similar way as in equation (2.3). Namely, we consider the following subfield of the field of fractions of $K[x_0, \ldots, x_n]/I(\mathcal{X})$:

$$K(\mathcal{X}) := \left\{ \frac{f + I(\mathcal{X})}{h + I(\mathcal{X})} \;\middle|\; f, h \text{ homogeneous}, \deg(f) = \deg(h),\ h \notin I(\mathcal{X}) \right\}.$$

Note that, in particular, $K(\mathcal{X})$ is a subfield of $\mathbb{K}(\mathcal{X})$.

Definition 2.28. *Let $P \in \mathcal{X}(\mathbb{K})$. Then, a rational function $\alpha \in K(\mathcal{X})$ is* regular *at P if there exist $f, h \in K[x_0, \ldots, x_n]$ homogeneous of the same degree such that $\alpha = \frac{f+I(\mathcal{X})}{h+I(\mathcal{X})}$, with $h(P) \neq 0$.*

Let now $\mathcal{X} \subseteq \mathbb{P}^n$ and $\mathcal{Y} \subseteq \mathbb{P}^m$ be two curves, a *rational map*

$$\varphi = [\alpha_0 : \cdots : \alpha_m] : \mathcal{X} \longrightarrow \mathcal{Y}$$

is an element $\varphi \in \mathbb{P}^m(K(\mathcal{X}))$. The map φ is said to be *regular* at a point P of $\mathcal{X}$ if there exists $\lambda \in K(\mathcal{X})$ such that $\lambda\alpha_i$ is regular at P for all $i = 0, \ldots, m$ and there exists $j \in \{0, \ldots, m\}$ such that $(\lambda\alpha_j)(P) \neq 0$. If this is the case, then $\varphi(P)$ is the point of $\mathcal{Y}$ defined as

$$\varphi(P) := [(\lambda\alpha_0)(P) : \cdots : (\lambda\alpha_m)(P)].$$

A rational map $\varphi : \mathcal{X} \longrightarrow \mathcal{Y}$ is said to be *dominant* if the image of φ in $\mathcal{Y}$ is dense in $\mathcal{Y}$, with respect to the Zariski topology. If a rational map $\varphi : \mathcal{X} \longrightarrow \mathcal{Y}$ is regular at every point P of $\mathcal{X}$, then φ is called a *morphism*.

Let now $\mathcal{Z} \subseteq \mathbb{P}^k$ be another curve and let $\varphi = [\alpha_0 : \cdots : \alpha_m] : \mathcal{X} \longrightarrow \mathcal{Y}$ and $\psi = [\beta_0 : \cdots : \beta_k] : \mathcal{Y} \longrightarrow \mathcal{Z}$ be rational maps. If $f_i, h_i \in \mathbb{K}[x_0, \ldots, x_m]$ are such that $\beta_i = \frac{f_i + I(\mathcal{Y})}{h_i + I(\mathcal{Y})}$ and $h_i(\alpha_0, \ldots, \alpha_m) \neq 0$ for all $i = 0, \ldots, k$, we define the composition of the rational maps φ and ψ as

$$\psi \circ \varphi := [\gamma_0 : \cdots : \gamma_k],$$

with $\gamma_i := \frac{f_i(\alpha_0, \ldots, \alpha_m)}{h_i(\alpha_0, \ldots, \alpha_m)}$. If instead there exists an index j such that $h_j(\alpha_0, \ldots, \alpha_m) = 0$, then $\psi \circ \varphi$ is not defined.

A rational map $\varphi : \mathcal{X} \longrightarrow \mathcal{Y}$ is said to be *birational* (and $\mathcal{X}, \mathcal{Y}$ are said to be *birationally equivalent*) if there exists a rational map $\varphi^{-1} := \psi : \mathcal{Y} \longrightarrow \mathcal{X}$ such that $\psi \circ \varphi = \mathrm{id}_{\mathcal{X}}$ and $\varphi \circ \psi = \mathrm{id}_{\mathcal{Y}}$, where $\mathrm{id}_{\mathcal{X}}$ (resp. $\mathrm{id}_{\mathcal{Y}}$) is the identity map on $\mathcal{X}$ (resp. $\mathcal{Y}$). If both φ and φ^{-1} are morphisms, φ is called an *isomorphism*. It can be shown that being birationally equivalent is in fact an equivalence relation on the class of projective curves.

It can be proved that a rational map between curves is dominant if and only if it is non-constant. In this setting, we can define the *pull-back* of a non-constant rational map $\varphi : \mathcal{X} \longrightarrow \mathcal{Y}$, which gives a correspondence between the function fields $\mathbb{K}(\mathcal{X})$ and $\mathbb{K}(\mathcal{Y})$ (and in particular between $K(\mathcal{X})$ and $K(\mathcal{Y})$, if $\mathcal{X}$ and $\mathcal{Y}$ are both defined over K).

Theorem 2.29. *Let $\varphi = [\alpha_0 : \cdots : \alpha_m] : \mathcal{X} \longrightarrow \mathcal{Y}$ be a non-constant rational map. Then the map*

$$\varphi^* : \begin{cases} \mathbb{K}(\mathcal{Y}) & \longrightarrow & \mathbb{K}(\mathcal{X}) \\ \frac{f + I(\mathcal{Y})}{h + I(\mathcal{Y})} & \longmapsto & \frac{f(\alpha_0, \ldots, \alpha_m) + I(\mathcal{X})}{h(\alpha_0, \ldots, \alpha_m) + I(\mathcal{X})} \end{cases}$$

is called the pull-back *of φ and it is a non-trivial field homomorphism such that $\varphi^*(c) = c$ for all $c \in \mathbb{K}$ (i.e., φ^* is a $\mathbb{K}$-homomorphism). In particular, φ is birational if and only if φ^* is an isomorphism, which means that the curves $\mathcal{X}$ and $\mathcal{Y}$ are birationally equivalent if and only if their function fields are $\mathbb{K}$-isomorphic.*

From the results just discussed and from those contained in the previous section, it follows that the algebraic function fields of one variable over a field $\mathbb{K}$ are precisely the function fields of curves defined over $\mathbb{K}$.

On one hand, it is immediate to see that $\mathbb{K}(\mathcal{X}) = \mathbb{K}(\bar{x}_1, \ldots, \bar{x}_n)$, where $\bar{x}_i := \frac{x_i + I(\mathcal{X})}{x_0 + I(\mathcal{X})}$, for $i = 1, \ldots, n$. Moreover, by [87, Chapter 2, Theorem 30] and by the Primitive Element Theorem, it can also be seen that there exist $j \in \{1, \ldots, n\}$ and $y \in \mathbb{K}(\bar{x}_1, \ldots, \bar{x}_n)$ such that $\mathbb{K}(\bar{x}_1, \ldots, \bar{x}_n) = \mathbb{K}(\bar{x}_j, y)$, which is a function field of one variable over $\mathbb{K}$ (see Definition 2.1). Note that, in the light of Theorem 2.29,

this means in particular that any projective curve $\mathcal{X}$ is birationally equivalent to a projective plane curve.

On the other hand, if F is a function field of one variable over $\mathbb{K}$, then it is a finite extension of $\mathbb{K}(x)$, for some x transcendental over $\mathbb{K}$, so that by the Primitive Element Theorem it can be described as $F = \mathbb{K}(x, y)$, for some $y \in F$. Hence, by what just observed above, this means precisely that F can be seen as the function field of a projective plane curve $\mathcal{X}$.

By virtue of this correspondence, we define the genus of a curve $\mathcal{X}$ to be the genus of its function field $\mathbb{K}(\mathcal{X})$.

Definition 2.30. *Let $P \in \mathcal{X}(\mathbb{K})$. The* local ring *of $\mathcal{X}$ at P is*

$$\mathbb{K}[\mathcal{X}]_P := \{\alpha \in \mathbb{K}(\mathcal{X}) \mid \alpha \text{ is regular at } P\}.$$

It can be shown that, for any point P, the ring $\mathbb{K}[\mathcal{X}]_P$ is a Noetherian local integral domain, whose maximal ideal is

$$M_P := \{\alpha \in \mathbb{K}[\mathcal{X}]_P \mid \alpha(P) = 0\}.$$

Definition 2.31. *A point $P \in \mathcal{X}(\mathbb{K})$ is said to be* nonsingular *if the local ring $\mathbb{K}[\mathcal{X}]_P$ is a DVR of $\mathbb{K}(\mathcal{X})$. Conversely, if $\mathbb{K}[\mathcal{X}]_P$ is not a DVR, the point P is said to be* singular*. The curve $\mathcal{X}$ is said to be* nonsingular *if every point P in $\mathcal{X}(\mathbb{K})$ is nonsingular.*

Note that, if $\mathcal{X}$ is defined over K, the above discussion and definitions actually hold for K, also in the case that $K \neq \mathbb{K}$, so that algebraic function fields of one variable over K are precisely the function fields of curves defined over K, and Definitions 2.30 and 2.31 can be stated as well in this setting.

There is a precise relation between points of a curve $\mathcal{X}$ defined over $\mathbb{K}$ and DVRs of the function field $\mathbb{K}(\mathcal{X})$, which is summarized in the following result (see [46, Theorem 4.32]).

Theorem 2.32. *Let O_M be a DVR of $\mathbb{K}(\mathcal{X})$ with maximal ideal M. Then there exists a unique point P of $\mathcal{X}$ such that*

$$\mathbb{K}[\mathcal{X}]_P \subseteq \mathrm{O}_M, \quad \mathbb{K}[\mathcal{X}]_P \cap M = M_P.$$

The point P is called the center *of the DVR O_M. Moreover, if P is a nonsingular point of $\mathcal{X}$, then $\mathbb{K}[\mathcal{X}]_P$ is the only DVR of $\mathbb{K}(\mathcal{X})$ centered at P.*

Equivalently, if P is the center of a DVR O_M, we also say that it is the center of the place M, or that M is centered at P.

Remark 2.33. *Theorem 2.32 implies that each nonsingular point P of $\mathcal{X}$ corresponds to exactly one place of $\mathbb{K}(\mathcal{X})$, namely P corresponds to the maximal ideal M_P of the local ring at P, and vice-versa. On the other hand, if P is a singular point of $\mathcal{X}$, then the local ring $\mathbb{K}[\mathcal{X}]_P$ is not a DVR and there might be multiple places of $\mathbb{K}(\mathcal{X})$ centered at P. Moreover note that, for Theorem 2.32 to be valid, it is essential that the field $\mathbb{K}$ is algebraically closed. In fact, if $\mathcal{X}$ is defined over $K \neq \mathbb{K}$, then the K-rational nonsingular points of $\mathcal{X}$ are still in one-to-one correspondence with the K-rational places of $K(\mathcal{X})$, but for the non-K-rational points the correspondence fails, also in the case in which they are nonsingular. For more details, see for instance [81, Appendix B.10] and [46, Chapters 4,5,8].*

Remark 2.33 suggests that the study of curves with singular points might pose more challenges than the study of nonsingular curves. However, the following result shows that, even when we are interested in studying curves with singular points, we can ultimately consider the case of nonsingular curves.

Theorem 2.34. *Every projective curve $\mathcal{X}$ is birationally equivalent to a nonsingular projective curve $\tilde{\mathcal{X}}$ (possibly in a higher dimensional projective space), called the* desingularization *of $\mathcal{X}$.*

Hence, when dealing with a curve $\mathcal{X}$ having singular points, we can always consider instead the desingularization $\tilde{\mathcal{X}}$ and study its properties by focusing on the function field $\mathbb{K}(\tilde{\mathcal{X}})$ of $\tilde{\mathcal{X}}$, since this is isomorphic to $\mathbb{K}(\mathcal{X})$ by Theorem 2.29. In particular, if $\mathcal{X}$ is defined over $K \neq \mathbb{K}$, then also the K-rational function fields $K(\tilde{\mathcal{X}})$ and $K(\mathcal{X})$ are isomorphic.

2.3 Numerical semigroups

The following section comprises some introductory results on numerical semigroups, which are part of the essential background knowledge required for the study of Weierstrass semigroups. An extensive and accurate exposition of these notions is contained in [73, Chapter 1]. In our notations, we always assume that $0 \in \mathbb{N}$.

A *numerical semigroup* $S \subseteq \mathbb{N}$ is a sub-semigroup of the additive semigroup $\mathbb{N}$. Any subset of elements of S that generate the whole semigroup is called a *generating set* of S, while the set $G := \mathbb{N} \setminus S$ is called the set of *gaps* of the semigroup. The *genus* of S is defined as $g(S) := |G| < \infty$. These notions are particularly important in Chapter 3, where we study Weierstrass semigroups at

all the places of a certain maximal function field. Indeed, as noted in Section 2.1, the Weierstrass semigroup $H(P)$ at a place P is a numerical semigroup and its genus $g(H(P))$ is precisely equal to the genus of the function field.

The *multiplicity* of a semigroup S is defined as

$$m_S := \min\{s \in S \mid s > 0\}$$

and the *conductor* of S is

$$c_S := 1 + \max G(S),$$

i.e., it is the smallest nonnegative integer c_S such that $\mathbb{Z}_{\geq c_S}$ is contained in the semigroup. Moreover, S is said to be *symmetric* if

$$\forall\, n \in \mathbb{N}, \text{ either } n \in S \text{ or } (\max G(S) - n) \in S.$$

It is a well-known result that S is symmetric if and only if $\max G(S) = 2g(S) - 1$, see [73, Corollary 4.5, 1)].

An important object associated to a semigroup S is the *Apéry set* of S. This is defined as the set

$$A(S) := \{s \in S \mid s - m_S \notin S\}. \tag{2.4}$$

The Apéry set consists of m_S elements, that form a complete set of (minimal) representatives for the congruence classes of $\mathbb{Z}$ modulo m_S. The knowledge of the Apéry set of a semigroup S provides a way of computing the genus of the semigroup, since it can be shown that

$$g(S) = \sum_{a \in A(S)} \left\lfloor \frac{a}{m_S} \right\rfloor. \tag{2.5}$$

However, the computation of the Apéry set is, in general, a difficult task, therefore it is convenient to also consider different methods for the computation of the genus. We here recall the particular case of telescopic semigroups (see [47, Section 5.4]), for which there is a closed formula for the computation of the genus that does not involve the Apéry set.

Let $(a_1, \ldots, a_k)$ be a sequence of positive integers with greatest common divisor equal to 1. Define

$$d_i := \gcd(a_1, \ldots, a_i) \qquad \text{and} \qquad A_i := \left\{ \frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i} \right\},$$

for $i = 1, \ldots, k$. Let $d_0 := 0$ and H_i be the semigroup generated by A_i. If $a_i/d_i \in H_{i-1}$ for all $i = 2, \ldots, k$, then the sequence $(a_1, \ldots, a_k)$ is called *telescopic*.

A numerical semigroup is called *telescopic* if it is generated by a telescopic sequence and, from [47, Proposition 5.35], it holds that the genus of a telescopic semigroup S generated by a telescopic sequence $(a_1, \ldots, a_k)$ is equal to

$$g(S) = \frac{1}{2}\left(1 + \sum_{i=1}^{k}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right). \tag{2.6}$$

2.4 Two-point Weierstrass semigroups

In Section 2.1, we recalled the definition and some basic results on Weierstrass semigroups. The aim of this section is to focus on the background notions regarding a generalization of Weierstrass semigroups introduced in [13] by P. Beelen and N. Tutaş. The proofs and a more detailed presentation of the results that we collect here can be found in the cited paper.

Let F be a function field over $\mathbb{F}_q$ and let Q, P be two distinct $\mathbb{F}_q$-rational places of F. Denote by $\mathcal{R}(Q, P)$ the ring of functions in F that are regular except possibly at Q and P, namely

$$\mathcal{R}(Q, P) := \{f \in F \mid v_R(f) \geq 0 \; \forall R \neq Q, P\}. \tag{2.7}$$

Definition 2.35 ([13, Definition 1])**.** *The* two-point Weierstrass semigroup $H(Q, P)$ *can be defined as the set*

$$H(Q, P) := \{(i, j) \in \mathbb{Z}^2 \mid \exists f \in \mathcal{R}(Q, P) \setminus \{0\}, v_Q(f) = -i, v_P(f) = -j\}.$$

The period π *of* $H(Q, P)$ *is defined to be*

$$\pi := \min\{k \in \mathbb{N} \setminus \{0\} \mid k(Q - P) \textit{ is a principal divisor}\}. \tag{2.8}$$

Note that $H(Q, P)$ is in fact a sub-semigroup of the additive semigroup $\{(i, j) \in \mathbb{Z}^2 \mid i + j \geq 0\}$, since the Riemann-Roch space $L(iQ + jP) = \{0\}$ if $i + j < 0$, see [5, Remark 7].

Moreover, let $\tau_{Q,P}$ be the function

$$\begin{aligned} \tau_{Q,P} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ i &\longmapsto \min\{j \mid (i, j) \in H(Q, P)\}. \end{aligned} \tag{2.9}$$

This function was introduced in [13] and is a generalization of a function previously introduced in [60], describing a bijection between the sets of gaps $G(P)$ and $G(Q)$. As a consequence of the Riemann-Roch Theorem, it holds that $\tau_{Q,P}(i) + i \leq 2g(F)$

for all $i \in \mathbb{Z}$, see [5, Remark 7]. The function $\tau_{Q,P}$ has many peculiar properties and we summarize in the following proposition those that will be useful for us in Chapter 4.

Proposition 2.36 ([13, Propositions 14,17])**.** *Let π be the period of the two-point Weierstrass semigroup $H(Q,P)$ and g be the genus of F. Then:*

1. *$\tau_{Q,P}$ is bijective, with inverse map $\tau_{Q,P}^{-1} = \tau_{P,Q}$;*
2. *$-i \leq \tau_{Q,P}(i) \leq 2g - i$ for all $i \in \mathbb{Z}$;*
3. *$\tau_{Q,P}(i+\pi) = \tau_{Q,P}(i) - \pi$ for all $i \in \mathbb{Z}$;*
4. *$\sum_{i=c}^{\pi+c-1}(i + \tau_{Q,P}(i)) = \pi g$ for all $c \in \mathbb{Z}$.*

Furthermore, as explicitly proved in [65, Corollary 2.10], $\tau_{Q,P}$ allows the determination of $H(Q,P)$ as

$$H(Q,P) = \{(i,j) \in \mathbb{Z}^2 \mid \tau_{Q,P}(i) \leq j, \tau_{Q,P}^{-1}(j) \leq i\},$$

therefore its knowledge is essentially equivalent to the knowledge of the two-point semigroup.

For computational purposes that will be clear in Chapter 4, it is convenient to provide a method to describe the map $\tau_{Q,P}^{-1} = \tau_{P,Q}$. The following proposition shows how $\tau_{Q,P}^{-1}(j)$ can be computed efficiently for all $j \in \mathbb{Z}$.

Proposition 2.37 ([65, Proposition 2.7])**.** *Let π be the period of the two-point Weierstrass semigroup $H(Q,P)$. Let $j \in \mathbb{Z}$ and $i := \tau_{Q,P}^{-1}(j)$. Then $i = i' - j + \tau_{Q,P}(i')$, where i' is the unique integer in $\{0,\ldots,\pi-1\}$ such that $\tau_{Q,P}(i') \equiv j \pmod{\pi}$.*

Proof. From Proposition 2.36, we have that $\tau_{Q,P}(a+\pi) = \tau_{Q,P}(a) - \pi$ for all $a \in \mathbb{Z}$ and that $\tau_{Q,P}$ is bijective; thus, $\{\tau_{Q,P}(a) \mid 0 \leq a < \pi\}$ is a complete set of representatives of congruence classes modulo π. In particular, there exists a unique $i' \in \{0,\ldots,\pi-1\}$ such that $\tau_{Q,P}(i') \equiv j \pmod{\pi}$. Write $\tau_{Q,P}(i) = j = \tau_{Q,P}(i') + (j - \tau_{Q,P}(i'))$. Then

$$\tau_{Q,P}(i') = \tau_{Q,P}(i) - (j - \tau_{Q,P}(i')) = \tau_{Q,P}(i + (j - \tau_{Q,P}(i'))), \tag{2.10}$$

where the last equality follows from Proposition 2.36 3., as $j - \tau_{Q,P}(i')$ is a multiple of π. Applying $\tau_{Q,P}^{-1}$ to the left and the right side of equation (2.10), we hence obtain that $i' = i + j - \tau_{Q,P}(i')$ and the proposition follows. $\square$

2.5 Algebraic Geometry codes

In this section, we deal with the pivotal definitions and results concerning Algebraic Geometry (AG) codes and certain bounds for the minimum distance of the duals of some specific classes of such codes. For a deeper and extensive exposition of the results discussed here, we refer to [8], [47, Chapter 4] and [81, Chapter 2].

Let p be a prime, h a positive integer and $\mathbb{F}_q$ be the finite field with $q = p^h$ elements.

A *linear* $[n, k, d]$ *code* C over the alphabet $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$, seen as a vector space over $\mathbb{F}_q$. The positive integer n is called the *length* of C and the integer k is the dimension of C as a vector space over $\mathbb{F}_q$ and it is called the *dimension* of the code. For $C \neq \{0\}$, d is the *minimum distance* of C and it is defined as follows:

$$d := \min\{\delta(a, b) \mid a, b \in C \text{ and } a \neq b\},$$

where $\delta(a, b) := |\{i \mid a_i \neq b_i\}|$ is the *Hamming distance* on $\mathbb{F}_q^n$. If $C = \{0\}$, we set $d := 0$. Moreover, given a code $C \subseteq \mathbb{F}_q^n$, its *dual code* is defined as

$$C^\perp := \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \quad \forall\, c \in C\},$$

where $\langle u, c\rangle$ denotes the canonical inner product on $\mathbb{F}_q^n$. If C is an $[n, k, d]$ code, the integers n, k, d are referred to as the *parameters* of C. A fundamental relation among the parameters of an $[n, k, d]$ code is given by the renowned *Singleton bound*, that is,

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

The codes attaining this bound are called *Maximum Distance Separable codes*, or simply *MDS codes*.

Let now F be a function field of genus g over $\mathbb{F}_q$, let $P_1, \ldots, P_n$ be pairwise distinct rational places of F and define the divisor $D := P_1 + \cdots + P_n \in \mathrm{Div}(F)$. Moreover, let $G \in \mathrm{Div}(F)$ be another $\mathbb{F}_q$-rational divisor such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$.

Definition 2.38. *Let ev_D be the evaluation map defined as follows:*

$$\begin{aligned} ev_D : \quad & L(G) \longrightarrow \mathbb{F}_q^n \\ & f \longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

The Algebraic Geometry code *(or simply* AG code*) $C_L(D, G)$ associated with the divisors D and G is defined as*

$$C_L(D, G) := \{ev_D(f) \mid f \in L(G)\}.$$

It can be shown that $C_L(D,G)$ is an $[n,k,d]$ code with parameters

$$k = \ell(G) - \ell(G-D) \quad \text{and} \quad d \geq n - \deg(G).$$

The bound $d \geq n - \deg(G)$ is called the *Goppa bound*. In particular, if $2g-2 < \deg(G) < n$, then $k = \deg(G) - g + 1$ and $n - \deg(G) > 0$. Moreover, we have that

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

which gives an intuition of why, for constructing AG codes with good parameters, we are in general interested in considering maximal function fields.

With notations as above, given $P_1, \ldots, P_n$ distinct rational places of F, it can be proved that there exists a Weil differential η of F such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for all $i = 1, \ldots, n$, see [81, Lemma 2.2.9]. Given such a differential and an $[n,k,d]$ AG code $C_L(D,G)$, by [81, Proposition 2.2.10] we have that the AG code $C_L(D,H)$, with $H := D - G + (\eta)$, is equal to the code $C_L(D,G)^\perp$, that is hence an $[n, n-k, d']$ AG code. The Goppa bound for its minimum distance reads as $d' \geq n - \deg(H) = \deg(G) - 2g + 2$.

An AG code $C_L(D,G)$ is called *one-point* if the support of the divisor G consists of one place of F, while $C_L(D,G)$ is called *two-point* if the support of G consists precisely of two distinct places, namely if $G = aQ + bP$, with $Q, P \in \mathbb{P}_F$, $Q \neq P$. It is worth mentioning that, in the literature, it is common to refer also to duals of one-point (resp. two-point) codes simply as one-point (resp. two-point) codes, although this terminology is slightly abusive. Indeed, even though the dual $C_L(D,G)^\perp$ of a one-point (resp. two-point) code is itself an AG code $C_L(D,H)$, the support of the divisor H might in general not consist of only one place (resp. two distinct places).

Duals of one-point and two-point AG codes have been extensively studied in the literature. This is due to the fact that it is possible to obtain bounds for the minimum distance of these codes that are more refined than the Goppa bound. In fact, although always providing an interesting bound on the minimun distance when $\deg(G) < n$, in several cases the Goppa bound turns out to be not sharp. An interesting bound worth mentioning, from this point of view, is the *Feng-Rao bound* for the minimum distance of duals of one-point codes. This bound has its roots in the work appeared in [24] and [21], and was introduced by G.-L. Feng and T.R.N. Rao in [25] (see also [62]).

Definition 2.39. *Let F be a function field of genus g and let $P, P_1, \ldots, P_n \in \mathbb{P}_F$ be rational places. Furthermore, let $H(P) = \{h_1 := 0 < h_2 < \ldots\}$ be the Weierstrass semigroup at P and, for any $\ell \in \mathbb{N}$, let*

$$\nu_\ell := |\{(i,j) \in \mathbb{N}^2 \ \mid \ h_i + h_j = h_{\ell+1}\}|.$$

For $D := P_1 + \cdots + P_n \in \mathrm{Div}(F)$ *and* $C_\ell := C_L(D, h_\ell P)^\perp$*, the* Feng-Rao designed minimum distance *of* C_ℓ *is defined as*

$$d_{ORD}(C_\ell) := \min\{\nu_m \mid m \geq \ell\}.$$

Since it holds that

$$d \geq d_{ORD}(C_\ell) \geq h_\ell - 2g + 2,$$

the integer $d_{ORD}(C_\ell)$ is also called the *Feng-Rao bound* or the *order bound*.

In Chapter 4, we use a generalization of the Feng-Rao bound that was introduced by P. Beelen in [8]. This generalization, known as the *generalized order bound*, applies to the duals of AG codes such that the support of the divisor G is constituted by multiple distinct places and it gives improvements on the Goppa bound for the minimum distance of such codes. In order to recall the definition of the generalized order bound, we first introduce some preliminary notions.

Definition 2.40 ([8, Definition 1])**.** *Let* G *be a divisor of a function field* F *and let* $R \in \mathbb{P}_F$ *be a rational place. The set of* G-non-gaps at R *is defined as*

$$H(R; G) := \left\{ -v_R(f) \;\middle|\; f \in \bigcup_{i=-\deg(G)}^{\infty} L(G + iR) \setminus \{0\} \right\}.$$

It follows immediately that $H(R; G + R) = H(R; G)$ and that $H(R; 0)$ is the Weierstrass semigroup $H(R)$ at R. Moreover, define

$$N(R; G) := \{(i, j) \in H(R; 0) \times H(R; G) \mid i + j = v_R(G) + 1\},$$
$$\nu(R; G) := \#N(R; G).$$

Definition 2.41 ([8, Definition 6])**.** *Let* $D := P_1 + \cdots + P_n$ *be a divisor that is a sum of* n *distinct rational places of the function field* F *and* G *be another rational divisor of* F*. Further, suppose that* $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$*. For any infinite sequence* $S = R_1, R_2, \ldots$ *of rational places in* $\mathbb{P}_F \setminus \mathrm{supp}(D)$*, define*

$$d_S(G) := \min\{\nu(R_{i+1}; G + R_1 + \cdots + R_i)\},$$

where the minimum is taken over all $i \geq 0$ *such that* $L(G + R_1 + \cdots + R_i) \neq L(G + R_1 + \cdots + R_{i+1})$*. Moreover, define*

$$d(G) := \max\, d_S(G),$$

where the maximum is taken over all infinite sequences S *of rational places in* $\mathbb{P}_F \setminus \mathrm{supp}(D)$*.*

Remark 2.42. *Note that, in Definition 2.41, the assumption that the places $R_1, R_2, \ldots$ constituting a sequence S are rational is not essential, as one can always extend the constant field of definition of F.*

Proposition 2.43 ([8, Theorem 7])**.** *Let $C_L(D, G)$ be an AG code with D and G as in Definition 2.41. Then, the minimum distance d' of the dual code $C_L(D, G)^\perp$ satisfies the inequality $d' \geq d(G)$.*

This shows that the integer $d(G)$ is in fact a lower bound for the minimum distance d' of $C_L(D, G)^\perp$. It is called the *generalized order bound*, since it can be seen as a generalization of the Feng-Rao bound for duals of one-point AG codes (see Definition 2.39). Furthermore, in [8, Proposition 10] it is shown that the generalized order bound $d(G)$ is always at least as good as the Goppa bound, that is, $d(G) \geq \deg(G) - 2g + 2$, where g is the genus of the function field F. More precisely, the following lemma shows that $d(G)$ coincides with the Goppa bound, if G has degree larger than or equal to $4g - 1$, and it cannot be worse than the Goppa bound if $\deg(G) < 4g - 1$.

Lemma 2.44 ([65, Lemma 2.3])**.** *Let D and G as in Definition 2.41. Let $g := g(\mathcal{X})$. Then $d(G) \geq \deg(G) - 2g + 2$. If $\deg(G) \geq 4g - 1$, the equality $d(G) = \deg(G) - 2g + 2$ holds.*

Proof. The inequality $d(G) \geq \deg(G) - 2g + 2$ follows directly from [8, Proposition 10]. Assume $\deg(G) \geq 4g - 1$. Fix a sequence $S = R_1, R_2, \ldots$ of places in $\mathbb{P}_F \setminus \operatorname{supp}(D)$. As in particular $\deg(G) \geq 2g - 1$, the Riemann-Roch Theorem implies that $L(G + R_1 + \cdots + R_i) \neq L(G + R_1 + \cdots + R_{i+1})$ for all $i \geq 0$. Moreover, it follows from [8, Remark 5] that $\nu(R_{i+1}; 0, G + R_1 + \cdots + R_i) = \deg(G + R_1 + \cdots + R_i) - 2g + 2$ for all $i \geq 0$. As a consequence,

$$d_S(G) = \nu(R_1; 0, G) = \deg(G) - 2g + 2.$$

Since $d_S(G)$ does not depend on the chosen sequence S, the conclusion follows. □

Remark 2.45 ([65, Remark 2.4])**.** *Though the generalized order bound $d(G)$ can be obtained theoretically by considering all possible sequences of places that do not occur in the support of D, this is not feasible in practice unless we restrict the set of possible sequences to a finite set. A first step into this direction is to observe that the computation of $d(G)$ using Definition 2.41 is only needed when $\deg(G) < 4g - 1$ (see Lemma 2.44) and that, in this case, only the first $4g - 1 - \deg(G)$ entries from every sequence S are relevant to define $d(G)$. However, some additional condition must be imposed: for example, at the cost of obtaining a possibly worse bound, one restricts the choice of the places that can occur in a sequence S to a finite set of places $\mathcal{P}$, chosen beforehand. For*

practical convenience, the set $\mathcal{P}$ can be chosen as the set of rational places of F that are not in the support of D.

For simplicity, in Chapter 4, we will apply the restriction suggested in Remark 2.45, when needed for practical purposes. With slight abuse of notation, we will continue to denote the bound with $d(G)$ and we will refer to it simply as the *order bound*. Note that this choice does not affect the statements of Proposition 2.43 and Lemma 2.44.

It is interesting to observe that, to study two-point AG codes $C_L(D, aQ+bP)^\perp$ by making use of the order bound, the knowledge of the function $\tau_{Q,P}$ is particularly important, as it provides a simple way for determining the dimension of $L(aQ + bP)$, $a, b \in \mathbb{N}$, and for explicitly computing the set of G-non-gaps at Q and the set of G-non-gaps at P. This was proved in [5], in the two following results.

Theorem 2.46 ([5, Theorem 9])**.** *Let $G = aQ+bP$ with $a, b \in \mathbb{N}$. The Riemann-Roch space $L(G)$ has dimension $|\{i \leq a \mid \tau_{Q,P}(i) \leq b\}|$.*

Corollary 2.47 ([5, Corollary 10])**.** *Let $G = aQ + bP$ with $a, b \in \mathbb{N}$. Then $H(Q; G) = \{i \in \mathbb{Z} \mid \tau_{Q,P}(i) \leq b\}$ and $H(P; G) = \{i \in \mathbb{Z} \mid \tau^{-1}_{Q,P}(i) \leq a\}$.*

Chapter 3

On a maximal function field with the third largest genus

This chapter comprises the study of the Weierstrass semigroup at every place and the description of the full automorphism group of a maximal function field having the third largest possible genus. The results included in the chapter are contained in [12] and were jointly developed by P. Beelen, M. Montanucci and the author of this thesis. In Section 3.3 and Section 3.4, the work contained in [12] is expanded with new results not included in the original paper.

A celebrated result due to Y. Ihara [56] is that the genus of an $\mathbb{F}_{q^2}$-maximal function field is always less than or equal to the value

$$g_1 := \frac{q(q-1)}{2},$$

which is precisely the genus of the Hermitian function field, see Example 2.12. Subsequently, H.-G. Rück and H. Stichtenoth showed in [74] that the Hermitian function field is the only maximal function field of genus g_1, up to $\mathbb{F}_{q^2}$-isomorphism.

These results raised the interest in the study of the spectrum of genera of maximal function fields, i.e., the set of possible values that the genus of an $\mathbb{F}_{q^2}$-maximal function field can attain, and in the characterization of maximal function fields

with genera equal to the largest values in the spectrum. In [27], R. Fuhrmann and F. Torres determined the second largest genus to be

$$g_2 := \left\lfloor \frac{(q-1)^2}{4} \right\rfloor,$$

and in [26] R. Fuhrmann, A. Garcia and F. Torres characterized, for q odd, the function fields having this genus. More precisely, they showed that a maximal function field has genus g_2 if and only if it is $\mathbb{F}_{q^2}$-isomorphic to the $\mathbb{F}_{q^2}$-rational function field of the curve defined by the affine equation

$$\mathcal{X}_2 : x^q + x = y^{\frac{q+1}{2}}.$$

For q even, a weaker although similar result was instead obtained in [1] by M. Abdón and F. Torres, who proved the characterization under the extra condition that the function field had a particular Weierstrass place. They showed that, if the extra condition is satisfied, then a function field has genus g_2 if and only if it is $\mathbb{F}_{q^2}$-isomorphic to $\mathbb{F}_{q^2}(\mathcal{Y}_2)$, where $\mathcal{Y}_2$ is the curve defined over $\mathbb{F}_{q^2}$ by the affine equation

$$\mathcal{Y}_2 : x^{\frac{q}{2}} + \ldots + x^2 + x = y^{q+1}.$$

The value of the third largest genus was instead computed by G. Korchmáros and F. Torres in [63], where it was proved to be

$$g_3 := \left\lfloor \frac{q^2-q+4}{6} \right\rfloor,$$

and examples of maximal function fields whose genus attains the value g_3 had already been provided in [32] and [16, Theorem 2.1]. More specifically, the $\mathbb{F}_{q^2}$-rational function fields of the plane curves defined over $\mathbb{F}_{q^2}$ by the following affine equations are maximal and have genus precisely g_3:

$$\begin{aligned}
&\mathcal{X}_3 : x^{\frac{q+1}{3}} + x^{\frac{2(q+1)}{3}} + y^{q+1} = 0, \quad \text{if} \quad q \equiv 2 \pmod 3 \\
&\mathcal{Y}_3 : y^q - yx^{\frac{2(q-1)}{3}} + x^{\frac{q-1}{3}} = 0, \quad \text{if} \quad q \equiv 1 \pmod 3 \\
&\mathcal{Z}_3 : y^q + y + \left(\sum_{i=1}^{t} x^{\frac{q}{p^i}} \right)^2 = 0, \quad \text{if} \quad q = 3^t.
\end{aligned} \tag{3.1}$$

Note that all these examples are Galois subfields of degree 3 of the Hermitian function field, and it is still an open problem to determine whether they are the only $\mathbb{F}_{q^2}$-maximal function fields of genus g_3, up to isomorphism.

In this chapter, we are interested in the study of the $\mathbb{F}_{q^2}$-rational function field of the curve $\mathcal{X}_3$. However, in order to have a more concise discussion, we do not

investigate directly $\mathbb{F}_{q^2}(\mathcal{X}_3)$, but we focus instead on the study of its constant field extension with the algebraic closure of $\mathbb{F}_{q^2}$, that is, the field $\mathbb{F}_{q^2}(\mathcal{X}_3)\overline{\mathbb{F}}_{q^2}$. Note that this is precisely the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ of the curve $\mathcal{X}_3$, see (2.3).

In particular, we determine the Weierstrass semigroup at every place of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ and give a complete description of the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. Note that, by [81, Theorem 3.6.3], it holds that the genus of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is equal to the genus g_3 of $\mathbb{F}_{q^2}(\mathcal{X}_3)$.

The chapter is organized as follows: in Section 3.1, we describe the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, setting the notations that are used throughout the rest of the discussion. We explicitly compute the principal divisors and the power series expansions at certain places of some specific functions, that will come in handy later. Moreover, we determine a particular canonical divisor that will be important for the results in Section 3.5 and Section 3.6. In Section 3.2, we compute two families of functions in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ that play a key role for the computation of the Weierstrass semigroups. Sections 3.3, 3.4, 3.5 and 3.6 are devoted to the explicit computation of the Weierstrass semigroups at all the places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, while Section 3.7 collects some conclusive remarks on the Weierstrass places. Finally, in Section 3.8, we determine the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

3.1 The function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$

We start by investigating some properties of the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. For more convenient notations, we set $m := \frac{q+1}{3}$, so that the affine equation of $\mathcal{X}_3$ in (3.1) reads

$$\mathcal{X}_3 : y^{q+1} + x^{2m} + x^m = 0 \tag{3.2}$$

and $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ can be described as $\overline{\mathbb{F}}_{q^2}(x, y)$, with $y^{q+1} + x^{2m} + x^m = 0$.

Moreover, let $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ be the function field of the *Hermitian curve* $\mathcal{H}$, that is, the curve defined over $\mathbb{F}_{q^2}$ by the affine equation

$$\mathcal{H} : u^{q+1} + v^{q+1} + 1 = 0. \tag{3.3}$$

The function field $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ can be described as $\overline{\mathbb{F}}_{q^2}(u, v)$, with $u^{q+1} + v^{q+1} + 1 = 0$. Note that the Hermitian function field H described in Example 2.12 is in fact the $\mathbb{F}_{q^2}$-rational function field of $\mathcal{H}$. We define the rational map

$$\varphi : \begin{cases} \mathcal{H} & \longrightarrow & \mathcal{X}_3 \\ (u, v) & \longmapsto & (u^3, uv), \end{cases}$$

and note that the pull-back map of φ,

$$\varphi^* : \overline{\mathbb{F}}_{q^2}(\mathcal{X}_3) \longrightarrow \overline{\mathbb{F}}_{q^2}(\mathcal{H}),$$

defines a Galois extension $\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ of degree 3, with $x := u^3$ and $y := uv$. In particular, the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ of the extension is generated by the automorphism

$$\tau : (u, v) \longmapsto (\zeta_3 u, \zeta_3^2 v), \tag{3.4}$$

where ζ_3 is a primitive cube root of unity in $\overline{\mathbb{F}}_{q^2}$.

Remark 3.1. *The extension $\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is unramified: indeed, by the Riemann-Hurwitz Genus Formula, it holds that*

$$\begin{aligned}
\deg \mathrm{Diff}(\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) &= 2g(\overline{\mathbb{F}}_{q^2}(\mathcal{H})) - 2 - 3(2g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) - 2) \\
&= 2\left(\frac{q(q-1)}{2}\right) - 2 - 3\left(\frac{2(q^2-q+4)}{6} - 2\right) \\
&= q^2 - q - 2 - (q^2 - q - 2) \\
&= 0,
\end{aligned}$$

which implies that $\mathrm{Diff}(\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = 0$. *The extension $\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is hence unramified. As a consequence of this fact, if Q is a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ lying over the place P of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, then for any $f \in \overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ it holds that $v_Q(f) = v_P(f)$.*

Furthermore, as the field $\overline{\mathbb{F}}_{q^2}$ is algebraically closed, the relative degrees of all the places in the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ are equal to 1.

Let $a \in \overline{\mathbb{F}}_{q^2}^*$ be such that $a^m + 1 \neq 0$ and consider the place P_a that is the zero of the function $x - a$ in $\overline{\mathbb{F}}_{q^2}(x)$. The polynomial $\rho(T) := T^{q+1} + x^{2m} + x^m$ is the minimal polynomial of y over $\overline{\mathbb{F}}_{q^2}(x)$ and is an element of $\mathrm{O}_{P_a}[T]$. In particular, let $\rho_i(T) := T - b\xi^i \in \mathrm{O}_{P_a}[T]$, for $i = 0, \ldots, q$, where ξ is a primitive $(q+1)$-th root of unity in $\overline{\mathbb{F}}_{q^2}$ and $b \in \overline{\mathbb{F}}_{q^2}^*$ is such that $b^{q+1} = -a^{2m} - a^m$. Moreover, let

$$\bar{\rho}(T) := T^{q+1} + a^{2m} + a^m \in \overline{\mathbb{F}}_{q^2}[T]$$

be the polynomial whose coefficients are the residue classes in O_{P_a}/P_a of the coefficients of $\rho(T)$. Then, the decomposition of $\bar{\rho}(T)$ into irreducible factors over $\overline{\mathbb{F}}_{q^2}$ is

$$\bar{\rho}(T) = \prod_{i=0}^{q}(T - b\xi^i) = \prod_{i=0}^{q} \bar{\rho}_i(T). \tag{3.5}$$

Since $\rho_i(T) = \bar{\rho}_i(T) \in \overline{\mathbb{F}}_{q^2}[T]$ for each $i = 0, \ldots, q$, by Theorem 2.19 there exists a unique place $P_{(a,b\xi^i)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ such that $P_{(a,b\xi^i)}|P_a$ and $\rho_i(y) \in P_{(a,b\xi^i)}$. Moreover, it holds that

$$e(P_{(a,b\xi^i)}|P_a) = 1$$

for all $i = 0, \ldots, q$. This means that, for all $i = 0, \ldots, q$, the functions $x - a$ and $y - b\xi^i$ in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ have only one common zero, namely the place $P_{(a,b\xi^i)}$.

Let now, instead, $a \in \overline{\mathbb{F}}_{q^2}^*$ be such that $a^m + 1 = 0$. Note that all such a are in fact in $\mathbb{F}_{q^2}^*$, as $m = \frac{q+1}{3}$. Since $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$ is a Kummer extension of degree $q+1$ (see Corollary 2.26), by Proposition 2.25 we immediately have that there exists a unique place $P_{(a,0)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ such that

$$P_{(a,0)}|P_a, \quad e(P_{(a,0)}|P_a) = q+1 \quad \text{and} \quad y \in P_{(a,0)}.$$

This place is the only common zero of the functions $x - a$ and y in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$.

By virtue of these considerations, for $a \in \overline{\mathbb{F}}_{q^2}^*$ and $b \in \overline{\mathbb{F}}_{q^2}$ such that $b^{q+1} = -a^{2m} - a^m$, we will henceforth denote by $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ the place that is the common zero of the functions $x - a$ and $y - b$ in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. In a similar way, still as a consequence of Theorem 2.19, we will also denote by $Q_{(A,B)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{H})}$ the place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ that is the common zero of the functions $u - A$ and $v - B$ in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, for $A, B \in \overline{\mathbb{F}}_{q^2}$.

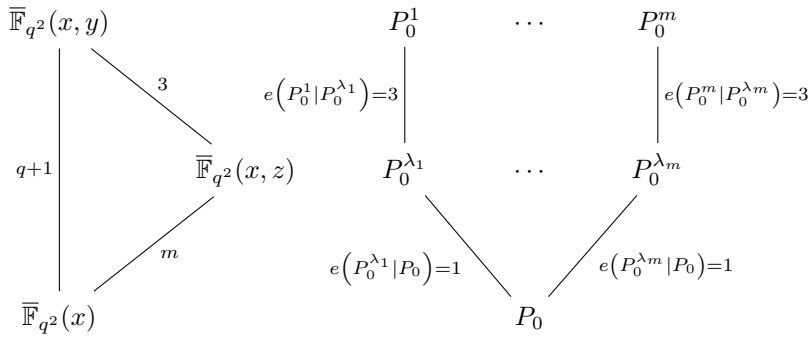
Let now $z := \frac{y^3}{x}$, so that $z^m = -(x^m + 1)$ and the function field extension $\overline{\mathbb{F}}_{q^2}(z,x)/\overline{\mathbb{F}}_{q^2}(x)$ is a Kummer extension of degree m (see Proposition 2.25 and Corollary 2.26). Denote by P_0 the zero of x in $\overline{\mathbb{F}}_{q^2}(x)$ and by $\rho(T) := T^m + x^m + 1$ the minimal polynomial of z over $\overline{\mathbb{F}}_{q^2}(x)$. With notations as before, we have

$$\bar{\rho}(T) := T^m + 1 = \prod_{i=1}^{m}(T - \lambda_i) \in \mathrm{O}_{P_0}/P_0[T], \tag{3.6}$$

with $\lambda_i \in \overline{\mathbb{F}}_{q^2}^*$, $\lambda_i^m = -1$ for all $i = 1, \ldots, m$. Note that the λ_i are all distinct and, since $2m$ divides $q^2 - 1$, they are all elements of $\mathbb{F}_{q^2}^*$. By Theorem 2.19, equation (3.6) implies that there are precisely m places $\{P_0^{\lambda_i}\}_{i=1}^m$ of $\overline{\mathbb{F}}_{q^2}(z,x)$ lying over P_0, each such that $e(P_0^{\lambda_i}|P_0) = 1$. Observing that $\overline{\mathbb{F}}_{q^2}(z,x) = \overline{\mathbb{F}}_{q^2}(y^3,x)$, it is then immediate to see that the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(z,x)$ is Kummer of degree 3 and the places $P_0^{\lambda_i}$ are totally ramified in this extension. Hence, it follows that there are precisely m places $P_0^1, \ldots, P_0^m \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ lying over P_0 in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$, with

$$e(P_0^i|P_0) = 3$$

for all $i = 1, \ldots, m$.



Let now P_∞ denote the pole of x in $\overline{\mathbb{F}}_{q^2}(x)$. With completely similar arguments, setting $w := \frac{x^2}{y^3}$ and considering the extension $\overline{\mathbb{F}}_{q^2}(w,x)/\overline{\mathbb{F}}_{q^2}(x)$, with $w^m = -\frac{1}{1+\frac{1}{x^m}}$, it also follows that there are exactly m places $P_\infty^1, \ldots, P_\infty^m \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ lying over P_∞ in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$, with

$$e(P_\infty^i|P_\infty) = 3$$

for all $i = 1, \ldots, m$.

For reasons that will be clear from the subsequent discussion, we now set the following notations:

$$\begin{aligned}
\mathfrak{R} &:= \{P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \mid a, b \in \mathbb{F}_{q^2}^* \text{ and } a^m + 1 \neq 0\} \\
\mathcal{O}_0 &:= \{P_0^1, \ldots, P_0^m\} \\
\mathcal{O}_\infty &:= \{P_\infty^1, \ldots, P_\infty^m\} \\
\mathcal{O}_m &:= \{P_{(a,0)} \mid a \in \mathbb{F}_{q^2}^*,\ a^m + 1 = 0\}
\end{aligned}$$

and

$$\mathcal{O} := \mathcal{O}_0 \cup \mathcal{O}_\infty \cup \mathcal{O}_m. \tag{3.7}$$

Remark 3.2. *Consider the $\mathbb{F}_{q^2}$-rational function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$ of the curve $\mathcal{X}_3$. Similarly to what we observed for the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$, the extension $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ is also a Kummer extension of degree $q+1$. Moreover, the preceding discussion concerning the extensions $\overline{\mathbb{F}}_{q^2}(z,x)/\overline{\mathbb{F}}_{q^2}(x)$ and $\overline{\mathbb{F}}_{q^2}(w,x)/\overline{\mathbb{F}}_{q^2}(x)$ holds also for the extensions $\mathbb{F}_{q^2}(z,x)/\mathbb{F}_{q^2}(x)$ and $\mathbb{F}_{q^2}(w,x)/\mathbb{F}_{q^2}(x)$. This is the case since, as already noted, the elements λ_i in equation* (3.6) *are in fact elements of $\mathbb{F}_{q^2}^*$.*

Therefore, denoting with $\bar{P}_0$ and $\bar{P}_\infty$ the zero and the pole of x in $\mathbb{F}_{q^2}(x)$, respectively, we have that there are exactly m places $\bar{P}_0^1, \ldots, \bar{P}_0^m \in \mathbb{P}_{\mathbb{F}_{q^2}(\mathcal{X}_3)}$ lying over

$\bar{P}_0$ and m places $\bar{P}^1_\infty, \ldots, \bar{P}^m_\infty \in \mathbb{P}_{\mathbb{F}_{q^2}(\mathcal{X}_3)}$ lying over $\bar{P}_\infty$, with

$$e(\bar{P}^i_0|\bar{P}_0) = e(\bar{P}^i_\infty|\bar{P}_\infty) = 3 \quad \textit{and} \quad f(\bar{P}^i_0|\bar{P}_0) = f(\bar{P}^i_\infty|\bar{P}_\infty) = 1$$

for all $i = 1, \ldots, m$.

Moreover, again by arguments similar to those discussed above, for all $a \in \mathbb{F}^*_{q^2}$ and $b \in \mathbb{F}_{q^2}$ such that $b^{q+1} = -a^{2m} - a^m$, it holds that the functions $x - a$ and $y - b$ in $\mathbb{F}_{q^2}(\mathcal{X}_3)$ have precisely one common zero $\bar{P}_{(a,b)}$. This place is $\mathbb{F}_{q^2}$-rational and lies over the zero $\bar{P}_a$ of x in $\mathbb{F}_{q^2}(x)$, with $f(\bar{P}_{(a,b)}|\bar{P}_a) = 1$. If $a^m + 1 \neq 0$, then $e(\bar{P}_{(a,b)}|\bar{P}_a) = 1$, while if $a^m + 1 = 0$, then $e(\bar{P}_{(a,0)}|\bar{P}_a) = q + 1$. Theorem 2.19 implies also that these places are precisely all the remaining $\mathbb{F}_{q^2}$-rational places of $\mathbb{F}_{q^2}(\mathcal{X}_3)$. Furthermore, it follows that, in the constant field extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(\mathcal{X}_3)$, the place $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$ is the only place lying over $\bar{P}_{(a,b)} \in \mathbb{P}_{\mathbb{F}_{q^2}(\mathcal{X}_3)}$, for all $a \in \mathbb{F}^*_{q^2}$ and $b \in \mathbb{F}_{q^2}$ with $b^{q+1} = -a^{2m} - a^m$.

Remark 3.3. *In the constant field extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(\mathcal{X}_3)$, we have*

$$\deg \operatorname{Con}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(\mathcal{X}_3)}(P) = \deg(P)$$

for all places $P \in \mathbb{P}_{\mathbb{F}_{q^2}(\mathcal{X}_3)}$, see [81, Theorem 3.6.3]. Therefore, each rational place of $\mathbb{F}_{q^2}(\mathcal{X}_3)$ lies under exactly one place of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ and Remark 3.2 implies that

- *$P^i_0|\bar{P}^i_0$, for all $i = 1, \ldots, m$,*
- *$P^i_\infty|\bar{P}^i_\infty$, for all $i = 1, \ldots, m$,*
- *$P_{(a,b)}|\bar{P}_{(a,b)}$, for each $a \in \mathbb{F}^*_{q^2}$ and $b \in \mathbb{F}_{q^2}$ with $b^{q+1} = -a^{2m} - a^m$.*

This means that there is a one-to-one correspondence between the $\mathbb{F}_{q^2}$-rational places of $\mathbb{F}_{q^2}(\mathcal{X}_3)$ and the places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ in $\mathcal{O} \cup \mathfrak{R}$.

$$
\begin{tikzcd}
\mathcal{O} \cup \mathfrak{R} \arrow[d, dash, "1:1"] & \overline{\mathbb{F}}_{q^2}(x,y) \arrow[dr, dash, "3"] \arrow[dd, dash] & & \\
 & & \overline{\mathbb{F}}_{q^2}(x,z) \arrow[dr, dash, "m"] \arrow[dd, dash] & \\
\{\mathbb{F}_{q^2}\text{-rational places}\} & \mathbb{F}_{q^2}(x,y) \arrow[dr, dash, "3"] & & \overline{\mathbb{F}}_{q^2}(x) \arrow[dd, dash] \\
 & & \mathbb{F}_{q^2}(x,z) \arrow[dr, dash, "m"] & \\
 & & & \mathbb{F}_{q^2}(x)
\end{tikzcd}
$$

Since, as already observed, the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$ is a Kummer extension of degree $q+1$, the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x))$ is cyclic and generated by the automorphism $y \longmapsto \delta y$, where δ is a primitive $(q+1)$-th root of unity in $\overline{\mathbb{F}}_{q^2}$. The sets $\mathcal{O}_0$ and $\mathcal{O}_\infty$ are distinct orbits of the action of $\mathrm{Gal}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x))$ on the places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, while all the places in $\mathcal{O}_m$ are fixed by $\mathrm{Gal}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x))$. However, the notation introduced in equation (3.7) is convenient since, in Corollary 3.7, we will show that the set $\mathcal{O}$ is contained in an orbit of the automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ and, in Section 3.8, we will in fact show that $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$, in its action on $\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$.

We now determine the divisors of several elementary functions in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. We denote as D_∞ the divisor

$$D_\infty := \sum_{j=1}^{m} P_\infty^j.$$

For a place $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}$, we define the function

$$x_a := \frac{x-a}{a},$$

which, as we will see later, turns out to be a local parameter for $P_{(a,b)}$. Furthermore, let $t_{P(a,b)}$ be the function

$$t_{P_{(a,b)}} := ma^{m-1}(2a^m+1)(x-a) + b^q(y-b) \tag{3.8}$$

in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, and let $Q_{(A,B)}$ be a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ lying over $P_{(a,b)}$. Note that $t_{P_{(a,b)}}$ is the function associated to the tangent line at the affine point with (x,y)-coordinates (a,b) of the plane curve defined by equation (3.2).

With $\mathcal{O}$ defined as in equation (3.7), for $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ we define

$$\alpha(P_{(a,b)}) := \frac{a^m}{1+a^m} = \frac{A^{q+1}}{1+A^{q+1}}. \tag{3.9}$$

As $1-\alpha(P_{(a,b)}) = \frac{1}{1+a^m}$, in particular $1-\alpha(P_{(a,b)}) \neq 0$ and we can define the following nonzero function in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, which will be useful later:

$$\begin{aligned} f_0 :&= \frac{3(1-\alpha(P_{(a,b)}))}{A^{q+1}} t_{P_{(a,b)}} \\ &= (1-\alpha(P_{(a,b)}))\left(\frac{\left(2A^{q+1}+1\right)}{A^3}(x-a) + \frac{3B^q}{A}(y-b)\right), \end{aligned} \tag{3.10}$$

where $A^3 = a$ and $AB = b$. Given a place $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ and $Q_{(A,B)}$ a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ lying over $P_{(a,b)}$, the following proposition describes the local power series expansion of the functions x_a and f_0 at $Q_{(A,B)}$, with respect to the local parameter $T := \frac{u-A}{A}$. In this proposition, as well as in the remainder of the chapter, whenever we write $f = g + O(T^n)$, for f and g nonzero elements of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, we mean that $v_{P_{(a,b)}}(f-g) \geq n$.

Proposition 3.4. *Let $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ and $Q_{(A,B)}$ a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ lying over $P_{(a,b)}$. Consider the functions x_a, f_0 and $T := (u-A)/A$, which is a local parameter at $Q_{(A,B)}$. Then, the local power series expansions of x_a and f_0 at $Q_{(A,B)}$ with respect to T are*

$$\begin{aligned} x_a &= 3T + 3T^2 + T^3, \\ f_0 &= 3T^2 + (\alpha(P_{(a,b)}) + 1)T^3 + O(T^q), \end{aligned} \tag{3.11}$$

where $\alpha(P_{(a,b)})$ is as defined in equation (3.9).

Proof. For convenience, we will simply write α instead of $\alpha(P_{(a,b)})$ in this proof. We start by computing the local power series expansions of the functions $x-a$ and $y-b$ with respect to the local parameter $T := (u-A)/A$ at $Q_{(A,B)}$. We have:

$$\begin{aligned} x_a = \frac{x-a}{a} = \frac{x-A^3}{A^3} = \frac{u^3-A^3}{A^3} &= \frac{(u-A)^3 + 3A(u-A)^2 + 3A^2(u-A)}{A^3} \\ &= 3T + 3T^2 + T^3 \end{aligned}$$

and

$$\begin{aligned} y-b = uv - AB &= (u-A)(v-B) + B(u-A) + A(v-B) - AB + AB \\ &= A(v-B)(T+1) + ABT. \end{aligned} \tag{3.12}$$

Moreover, from $v^{q+1}+u^{q+1}+1=0$, we obtain

$$(u-A)^{q+1}-A^{q+1}+A^q u+Au^q+(v-B)^{q+1}-B^{q+1}+B^q v+Bv^q+1=0$$

or equivalently

$$A^{q+1}T^{q+1}+(v-B)^{q+1}+A^{q+1}T^q+B(v-B)^q+A^{q+1}T+B^q(v-B)=0$$

which gives $v-B=-\frac{A^{q+1}}{B^q}T+O(T^q)$. Combining this with equation (3.12), we obtain

$$\begin{aligned} y-b &= A(v-B)(T+1)+ABT=-A\frac{A^{q+1}}{B^q}T(T+1)+ABT+O(T^q)\\ &= A\left(B-\frac{A^{q+1}}{B^q}\right)T-\frac{A^{q+2}}{B^q}T^2+O(T^q). \end{aligned}$$

We can now compute also the local power series expansion of the function f_0 at $Q_{(A,B)}$ with respect to the local parameter T. Using equation (3.10) and the previously computed expansions of x_a and $y-b$, we find

$$\begin{aligned} f_0 &= (1-\alpha)(3\left(A^{q+1}+1\right)T^2+\left(2A^{q+1}+1\right)T^3)+O(T^q)\\ &= 3T^2+(\alpha+1)T^3+O(T^q), \end{aligned}$$

where in the final equality we used that $\alpha=A^{q+1}/(1+A^{q+1})$. □

Proposition 3.5. *In the above notations, the principal divisors of the functions $x_a, x, y, y-b$ and f_0 in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ are:*

$$(x_a)=\begin{cases} P_{(a,b)}+\sum_{\xi^{q+1}=1,\ \xi\neq 1}P_{(a,\xi b)}-3D_\infty & \text{if} \quad a^m\neq -1,\\ (q+1)P_{(a,0)}-3D_\infty & \text{if} \quad a^m=-1, \end{cases} \tag{3.13}$$

and

$$\begin{aligned} (x) &= 3\sum_{i=j}^{m}P_0^j-3D_\infty,\\ (y) &= \sum_{j=1}^{m}P_0^j+\sum_{a^m+1=0}P_{(a,0)}-2D_\infty,\\ (y-b) &= P_{(a,b)}+E_b-2D_\infty, \end{aligned} \tag{3.14}$$

where $E_b\in \mathrm{Div}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is an effective divisor of degree $2m-1$. Moreover, if $P_{(a,b)}\in\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}\setminus\mathcal{O}$ and $\alpha(P_{(a,b)})\neq -1$, then $P_{(a,b)}\notin \mathrm{supp}(E_b)$. Furthermore, for $P_{(a,b)}\in\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)}\setminus\mathcal{O}$, let f_0 be the function defined in equation (3.10). Then

$$(f_0)=2P_{(a,b)}+E_0-3D_\infty, \tag{3.15}$$

where $E_0\in\mathrm{Div}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is an effective divisor such that $P_{(a,b)}\notin\mathrm{supp}(E_0)$.

Proof. To find the divisors of x_a and x, recall that $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$ is a Kummer extension of degree $q+1$. Then, it is sufficient to note that the zeros of x^m+1 are totally ramified in this extension, while the zero and the pole of x have ramification index equal to three, see the discussion before Remark 3.2. No further ramification occurs, as $y^{q+1} = -x^m(x^m+1)$. This equation also gives the divisor of y. It is not clear that the divisor of $y-b$ is of the form as stated in the proposition, but it might happen that $P_{(a,b)} \in \operatorname{supp}(E_b)$. In this case, the polynomial $f(x) := x^{2m} + x^m + b^{q+1}$ would have a as a multiple root. Since $3f'(x) = x^{m-1}(2x^m+1)$ and $P_{(a,b)} \notin \mathcal{O}$, this can only happen if $2a^m+1=0$. Using that $\alpha(P_{(a,b)})+1 = (2a^m+1)/(a^m+1)$, the result on the divisor of $y-b$ follows.

Finally, from equation (3.11), we know that $v_{P_{(a,b)}}(f_0) = 2$ and, as f_0 is a linear combination of x_a and $y-b$, by the triangle inequality we also know that $v_{P_\infty^j}(f_0) = -3$ and that f_0 has no poles outside the P_∞^j, $1 \le j \le m$. Hence, equation (3.15) follows. □

Lemma 3.6. *The automorphism group* $\operatorname{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ *contains a subgroup* G *of order* $2(q+1)^2$*, which is isomorphic to a semidirect product of an abelian group* A *of order* $(q+1)^2/3$ *and a symmetric group of order* 6*. More precisely,*

$$A := \{\theta_{\gamma,\delta}(x,y) = (\gamma x, \delta y) \mid \gamma^m = \delta^{q+1} = 1\},$$

while the symmetric group of order 6 *is generated by the involution* θ_2 *and the order* 3 *automorphism* θ_3 *given by*

$$\theta_2(x,y) = \left(\frac{1}{x}, \frac{y}{x}\right) \quad \text{and} \quad \theta_3(x,y) = \left(\frac{y^3}{x^2}, \frac{y}{x}\right).$$

Proof. By direct computation, it can be checked that $\langle A, \theta_2, \theta_3\rangle$ is an automorphism group of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, that is, all the maps presented in the lemma preserve the equation $y^{q+1}+x^m+x^{2m}=0$. The group T generated by θ_2 and θ_3 is isomorphic to the symmetric group of order 6 as $\theta_2\theta_3\theta_2 = \theta_3^2$, again by direct computation. Both θ_2 and θ_3 normalize A, since computations show that $\theta_2\theta_{\gamma,\delta}\theta_2 = \theta_{\gamma^{-1},\delta\gamma^{-1}}$ and $\theta_3\theta_{\gamma,\delta}\theta_3^{-1} = \theta_{\gamma\delta^{-3},\gamma\delta^{-2}}$, hence T normalizes A. Since T and A have trivial intersection, we hence obtain that $\langle A, T\rangle = A \rtimes T$. □

Corollary 3.7. *Let* $\mathcal{O}$ *be the set defined in equation* (3.7)*. Then* $|\mathcal{O}| = q+1$ *and* $\mathcal{O}$ *is an orbit of the automorphism group* G *defined in Lemma 3.6, in its natural action on the places of* $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$*.*

Proof. We observe that the Galois group of the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$, that is the cyclic group generated by $(x,y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes each place in the set $\mathcal{O}_m$, while it acts transitively on the sets

$\mathcal{O}_0$ and $\mathcal{O}_\infty$. The group A, as defined in Lemma 3.6, acts transitively on the set $\mathcal{O}_m$, since it maps x to γx, where $\gamma^m = 1$. The automorphism θ_2 maps x to $1/x$ and hence, from equation (3.14), merges the two Galois orbits $\mathcal{O}_0$ and $\mathcal{O}_\infty$ under the action of G. Instead, the automorphism θ_3 acts as a cycle of order 3 on $\mathcal{O}_0$, $\mathcal{O}_\infty$ and $\mathcal{O}_m$. This can be seen from equation (3.14) and the fact that θ_3 maps x to y^3/x^2. As a result, all the three considered sets are merged into one orbit under the action of G. □

Remark 3.8. *Let Φ be the $\mathbb{F}_{q^2}$-Frobenius map and $\bar{a} \in \mathbb{F}_{q^2}$ be such that $\bar{a}^m = -1$. Then, from the Fundamental Equation [46, Page xix (ii)] it follows in particular that, for any $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$, there exist functions $f_{P_{(a,b)},i} \in \overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ and $\phi_{P_{(a,b)}} \in \overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ such that*

$$(f_{P_{(a,b)},i}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - (q+1)P_\infty^i, \tag{3.16}$$

for all $i = 1, \ldots, m$, and

$$(\phi_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - (q+1)P_{(\bar{a},0)}.$$

Hence, we can consider the following function in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, that will be useful later:

$$F_{P_{(a,b)}} := \phi_{P_{(a,b)}} \cdot x_{\bar{a}}. \tag{3.17}$$

By Proposition 3.5, the principal divisor of $F_{P_{(a,b)}}$ is

$$(F_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - 3\sum_{j=1}^{m} P_\infty^j.$$

We conclude the section computing a particular canonical divisor in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, that will be important for the study of the Weierstrass semigroups. Indeed, we will use it in order to construct certain regular differentials that will allow the determination of the set of gaps at each place $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ (see Proposition 2.18).

Lemma 3.9. *The divisor $(q-2)D_\infty$ is canonical. More precisely,*

$$\left(\frac{ydx}{x(x^m+1)}\right) = (q-2)D_\infty.$$

Proof. The result follows directly from the fact that $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\overline{\mathbb{F}}_{q^2}(x)$ is a Kummer extension of degree $q+1$, see the discussion before Remark 3.2 and the proof of Proposition 3.5. Hence, we have

$$(dx) = 2\sum_{j=1}^{m} P_0^j + q\sum_{a^m+1=0} P_{(a,0)} - 4D_\infty$$

and the claim follows from direct computations, by using Proposition 3.5. □

Corollary 3.10. *Let P be a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ not in $\mathcal{O}_\infty$. Then, for any $h \in L((q-2)D_\infty)$, the integer $v_P(h)+1$ is a gap of the Weierstrass semigroup at P.*

Proof. From Proposition 2.18 and Lemma 3.9, it is enough to consider the regular differential

$$w := \frac{hydx}{x(x^m+1)}.$$

Since $v_P(w) = v_P(h)$, the corollary follows. □

3.2 Two families of functions in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$

The aim of this section is to prove Theorem 3.19 and Theorem 3.20, that introduce two families of functions in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ with prescribed vanishing orders at certain places. These functions will be crucial for the computation of the Weierstrass semigroups at all the places not contained in $\mathcal{O}$.

We start by giving the following definition, introducing some functions that will be practical to use in the proofs of Theorem 3.19 and Theorem 3.20.

Definition 3.11. *Let $i \in \mathbb{Z}$. Furthermore, let $\mathbb{F}$ be a field of characteristic different from three and assume that it contains a primitive cube root of unity, which we will denote by ζ_3. Then we define the following rational functions in $\mathbb{F}(s)$:*

$$\mathcal{P}_i(s) := \frac{(s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}}{3(\zeta_3-\zeta_3^2)s(s-1)}$$

and

$$\mathcal{Q}_i(s) := \frac{\left(\frac{1-\zeta_3}{3}\right)(s+\zeta_3)^{3i-1} + \left(\frac{1-\zeta_3^2}{3}\right)(s+\zeta_3^2)^{3i-1}}{s-1}.$$

Note that it is not strictly necessary to assume that the field $\mathbb{F}$ contains a primitive cube root of unity. If it does not, the above definition makes sense over the larger field $\mathbb{F}(\zeta_3)$, but actually Galois theory can be used to show that $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ are in $\mathbb{F}(s)$.

Example 3.12. *Assume $\mathbb{F} = \mathbb{Q}$. Then $\mathcal{P}_0(s) = 0$, $\mathcal{P}_1(s) = 1$, $\mathcal{P}_2(s) = 2s^3-3s^2-3s+2$ and $\mathcal{P}_3(s) = 3s^6-9s^5-9s^4+33s^3-9s^2-9s+3$. Moreover, $\mathcal{Q}_1(s) = s+1$, $\mathcal{Q}_2(s) = s^4+s^3-9s^2+s+1$, $\mathcal{Q}_3(s) = s^7+s^6-27s^5+29s^4+29s^3-27s^2+s+1$, and $\mathcal{Q}_0(s) = (s^2-s+1)^{-1}$.*

In fact, as illustrated in this example, for positive values of i the rational functions $\mathcal{P}_i(s)$ and $\mathcal{Q}_j(s)$ are polynomials in s. We investigate this further in the following lemma.

Lemma 3.13. *Let $i \in \mathbb{Z}_{>0}$. Then $\mathcal{P}_i(s)$ is a nonzero polynomial of degree at most $3i-3$, while $\mathcal{Q}_i(s)$ is a nonzero polynomial of degree $3i-2$.*

Proof. It is easy to see that, for any $i \in \mathbb{Z}_{>0}$, the polynomial $\tilde{\mathcal{P}}_i(s) := (s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}$ has at most degree $3i-1$. It is not the zero polynomial, since if s is substituted by $-\zeta_3$, one obtains

$$\tilde{\mathcal{P}}_i(-\zeta_3) = 0^{3i} - (-\zeta_3+\zeta_3^2)^{3i} = (-1+\zeta_3)^{3i}, \tag{3.18}$$

which is not zero, as $\zeta_3 \neq 1$. Here we used that the field $\mathbb{F}$ does not have characteristic three. It is easy to see that $\tilde{\mathcal{P}}_i(0) = 0$, while

$$\tilde{\mathcal{P}}_i(1) = (1+\zeta_3)^{3i} - (1+\zeta_3^2)^{3i} = (-\zeta_3^2)^{3i} - (-\zeta_3)^{3i} = (-1)^i - (-1)^i = 0.$$

We may conclude that $\mathcal{P}_i(s)$ is a polynomial of degree at most $3i-3$. Similarly, the polynomial $\tilde{\mathcal{Q}}_i(s) := \frac{1-\zeta_3}{3}(s+\zeta_3)^{3i-1} + \frac{1-\zeta_3^2}{3}(s+\zeta_3^2)^{3i-1}$ is a polynomial of degree $3i-1$ having 1 as a root. Hence $\mathcal{Q}_i(s)$ is a polynomial of degree $3i-2$. $\square$

It can also be seen that the coefficient of s^{3i-3} of the polynomial $\mathcal{P}_i(s)$ equals $3i(\zeta_3-\zeta_3^2)$. Hence, if the characteristic of the field $\mathbb{F}$, which already is assumed to be distinct from three, is zero or does not divide i, then the degree of $\mathcal{P}_i(s)$ is exactly $3i-3$. Since we will work over $\overline{\mathbb{F}}_{q^2}$, where $q \equiv 2 \pmod 3$, it may well happen that $\deg(\mathcal{P})_i(s) < 3i-3$.

The following lemma gives a relation, that will come in handy later, between the rational functions just introduced.

Lemma 3.14. *Let $i, j, \ell \in \mathbb{Z}$. Then*

$$\mathcal{P}_i(s)\mathcal{P}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{P}_{\ell+i}(s) = (s^2-s+1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{P}_\ell(s) \tag{3.19}$$

and

$$\mathcal{P}_i(s)\mathcal{Q}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{Q}_{\ell+i}(s) = (s^2-s+1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{Q}_\ell(s). \tag{3.20}$$

Proof. For convenience, we will simply write $\mathcal{P}_i$ and $\mathcal{Q}_j$ instead of $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ in this proof. We only prove the second identity, since the first one can be proved in a very similar way, with simpler looking intermediate expressions.

First of all, using Definition 3.11 and writing $S_1 = s + \zeta_3$, $S_2 = s + \zeta_3^2$, one obtains by direct computation

$$3(\zeta_3 - \zeta_3^2)s(s-1)^2\mathcal{P}_i\mathcal{Q}_{\ell+j} =$$
$$\frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3i}S_2^{3j+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3i}S_1^{3j+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}$$

and

$$3(\zeta_3 - \zeta_3^2)s(s-1)^2\mathcal{P}_j\mathcal{Q}_{\ell+i} =$$
$$\frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3j}S_2^{3i+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3j}S_1^{3i+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}.$$

Hence

$$3(\zeta_3 - \zeta_3^2)s(s-1)^2(\mathcal{P}_i\mathcal{Q}_{\ell+j} - \mathcal{P}_j\mathcal{Q}_{\ell+i}) =$$
$$(S_1S_2)^{3j}\left(\frac{1-\zeta_3}{3}(S_1^{3\ell+3i-3j-1} - S_2^{3i-3j}S_1^{3\ell-1}) + \frac{1-\zeta_3^2}{3}(S_1^{3i-3j}S_2^{3\ell-1} - S_2^{3\ell+3i-3j-1})\right)$$
$$= (S_1S_2)^{3j}(S_1^{3(i-j)} - S_2^{3(i-j)})\left(\frac{1-\zeta_3}{3}S_1^{3\ell-1} + \frac{1-\zeta_3^2}{3}S_2^{3\ell-1}\right)$$
$$= 3(\zeta_3 - \zeta_3^2)s(s-1)^2(s^2-s+1)^{3j}\mathcal{P}_{i-j}\mathcal{Q}_\ell.$$

For the last equality, note that $S_1S_2 = s^2 - s + 1$. □

Remark 3.15. *For any $i \in \mathbb{Z}_{>0}$, the polynomials $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ have no common roots. Indeed, this is clear for $i = 1$, since $\mathcal{P}_1(s) = 1$. If $i \geq 2$, Lemma 3.14 applied with $\ell = 0$ and $j = i - 1$ implies that*

$$\mathcal{P}_i(s)\mathcal{Q}_{i-1}(s) - \mathcal{P}_{i-1}(s)\mathcal{Q}_i(s) = (s^2 - s + 1)^{3i-4},$$

where we used that $\mathcal{Q}_0(s) = (s^2 - s + 1)^{-1}$. Hence, the only possible common roots of $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ could be $-\zeta_3$ or $-\zeta_3^2$, the roots of $s^2 - s + 1$. However, equation (3.18) implies that $\mathcal{P}_i(-\zeta_3) \neq 0$ and similarly one sees that $\mathcal{P}_i(-\zeta_3^2) \neq 0$.

Remark 3.16. *Let $\mathbb{F} = \overline{\mathbb{F}}_{q^2}$ be the algebraic closure of $\mathbb{F}_{q^2}$. Then, for any $\alpha \in \mathbb{F} \setminus \{0, 1, -\zeta_3, -\zeta_3^2\}$, there exists $i > 0$ such that $\mathcal{P}_{i+1}(\alpha) = 0$. Indeed, for such α one has $\mathcal{P}_{i+1}(\alpha) = 0$ if and only if $((\alpha + \zeta_3)/(\alpha + \zeta_3^2))^{3i+3} = 1$. Since any nonzero element of $\mathbb{F}$ has a finite multiplicative order, the existence of i follows. Moreover, since $\mathcal{P}_1(s) = 1$, we see that $i > 0$.*

This remark motivates the following definition.

Definition 3.17. *Let $\alpha \in \overline{\mathbb{F}}_{q^2} \setminus \{0, 1, -\zeta_3, -\zeta_3^2\}$. Then we define the $\mathcal{P}$-*order *of α as the smallest positive integer i such that $\mathcal{P}_{i+1}(\alpha) = 0$.*

Later, we will apply the notion of a $\mathcal{P}$-order in case $\alpha = \alpha(P_{(a,b)})$. The following lemma is a first source of information in this setting.

Lemma 3.18. *Let i be a positive integer. The number of $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ such that $\alpha(P_{(a,b)})$ has $\mathcal{P}$-order i is equal to $(q+1)^2\varphi(i+1)$ if $\gcd(i+1,p) = 1$ and 0 otherwise. Here, $\varphi(\cdot)$ denotes Euler's totient function. Moreover, for $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$, it holds that $a, b \in \mathbb{F}_{q^2}$ if and only if $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$ or the $\mathcal{P}$-order i of $\alpha(P_{(a,b)})$ satisfies that $i+1$ divides m.*

Proof. If $\alpha := \alpha(P_{(a,b)})$ has $\mathcal{P}$-order i for some positive integer i, then $\alpha \notin \{0, 1, -\zeta_3, -\zeta_3^2\}$ and $P_{(a,b)} \notin \mathcal{O}$. As observed in Remark 3.16, we have $\mathcal{P}_{i+1}(\alpha) = 0$ if and only if $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3i+3} = 1$. If the characteristic p divides $i+1$, we see that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3(i+1)/p} = 1$, implying that $\mathcal{P}_j(\alpha) = 0$ for some j strictly smaller than $i+1$. By definition of $\mathcal{P}$-order, this is impossible. If $\gcd(p, i+1) = 1$, the α that have $\mathcal{P}$-order i are precisely those satisfying that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^3$ is a primitive $(i+1)$-th root of unity. Hence, there are $3\varphi(i+1)$ many α with $\mathcal{P}$-order i. Since $\alpha = a^m/(1+a^m)$ and $\alpha \notin \{0,1\}$, for each such α there are m distinct possibilities for a. Since $P_{(a,b)} \notin \mathcal{O}$, for each such a there are $q+1$ distinct possibilities for b. This proves the first part of the lemma.

Now suppose that $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ is such that $a, b \in \mathbb{F}_{q^2}$ and $\alpha^2 - \alpha + 1 \neq 0$. First of all, we claim that in this case $\alpha \in \mathbb{F}_q$. Indeed, since $a, b \in \mathbb{F}_{q^2}$, we obtain that $a^{3m} = a^{q+1} \in \mathbb{F}_q$ and $a^{2m} + a^m = -b^{q+1} \in \mathbb{F}_q$. But then $a^m = (a^{3m}+a^{2m}+a^m)/(a^{2m}+a^m+1) \in \mathbb{F}_q$. Here we used that $a^{2m}+a^m+1 \neq 0$, which follows from the assumption that $\alpha^2 - \alpha + 1 \neq 0$. Now $a^m \in \mathbb{F}_q$, which implies that $\alpha = a^m/(1+a^m) \in \mathbb{F}_q$. In particular $\alpha^q = \alpha$. This in turn implies that

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^q = \frac{\alpha^q+\zeta_3^q}{\alpha^q+\zeta_3^{2q}} = \frac{\alpha+\zeta_3^2}{\alpha+\zeta_3},$$

which is exactly the inverse of $\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}$. Hence $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3m} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$, which shows that $i+1$ divides m.

Conversely, if $\alpha^2 - \alpha + 1 = 0$, then a satisfies $a^{2m} + a^m + 1 = 0$, which implies that $b^{q+1} = 1$ and hence $a, b \in \mathbb{F}_{q^2}$. If $\alpha^2 - \alpha + 1 \neq 0$ and $i+1$ divides m, then $3(i+1)$ divides $q+1$ and $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3(i+1)} = 1$. Hence $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$, which after clearing denominators amounts to the equation $(\alpha+\zeta_3)^{q+1} - (\alpha+\zeta_3^2)^{q+1} = 0$. This is a polynomial in α of degree q and we have already seen that this equation is satisfied for all $\alpha \in \mathbb{F}_q$. We may therefore conclude that $\alpha \in \mathbb{F}_q$. From this, it follows that $a^m \in \mathbb{F}_q$, which implies that $b^{q+1} = -a^{2m} - a^m \in \mathbb{F}_q$. Hence, also in this case we conclude that both $a, b \in \mathbb{F}_{q^2}$. $\square$

Next, we use the polynomials $\mathcal{P}_j(s)$ and $\mathcal{Q}_j(s)$ to investigate the existence of functions that will be useful later when determining gaps at the places $P_{(a,b)} \in \overline{\mathbb{F}}_{q^2}(\mathcal{X}_3) \setminus \mathcal{O}$.

Theorem 3.19. *Let $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ and suppose that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 \neq 0$. Furthermore, let i be the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. If $i \leq m-2$, then there exists a function $f_i \in L((3i+3)D_\infty)$ such that $v_{P_{(a,b)}}(f_i) = 3i+3$. Moreover, for each $j \in \mathbb{Z}$ with $0 \leq j \leq \min\{i-1, m-2\}$, there exists a function $f_j \in L((3j+3)D_\infty)$ with $v_{P_{(a,b)}}(f_j) = 3j+2$.*

Proof. Throughout the proof we simplify the notation by writing α instead of $\alpha(P_{(a,b)})$. In a similar vein, we will write $\mathcal{P}_j$ and $\mathcal{Q}_j$, rather than $\mathcal{P}_j(\alpha)$ and $\mathcal{Q}_j(\alpha)$.

Let $Q_{(A,B)}$ be a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ lying over $P_{(a,b)}$ and let $T := (u-A)/A$, which is a local parameter at $Q_{(A,B)}$. For each j such that $0 \leq j \leq i$, we claim that there exists a function $f_j \in L((3j+3)D_\infty)$ such that the local power series expansion of f_j at $Q_{(A,B)}$ with respect to the local parameter T is

$$f_j = 3\mathcal{P}_{j+1}T^{3j+2} + \mathcal{Q}_{j+1}T^{3j+3} + O(T^q). \tag{3.21}$$

Note that, by definition of the $\mathcal{P}$-order, this will imply that

$$f_i = \mathcal{Q}_{i+1}T^{3i+3} + O(T^q). \tag{3.22}$$

This is sufficient to prove the theorem since, as observed in Remark 3.1, $v_{Q_{(A,B)}}(f_j) = v_{P_{(a,b)}}(f_j)$ and $3j+3 < q$ for all j under consideration.

First of all, note that, for $j=0$, we can take f_0 to be exactly the function defined in equation (3.10) and whose local power series expansion with respect to T was computed in equation (3.11). To show the result for $j=1$, we define

$$f_1 := -9x_a^2 + 27f_0 - 3(\alpha-5)x_a f_0 + (\alpha^2 - \alpha - 5)f_0^2.$$

Elementary calculations show that the local power series expansion of f_1 at $Q_{(A,B)}$ with respect to T is precisely

$$f_1 = 3\mathcal{P}_2T^5 + \mathcal{Q}_2T^6 + O(T^q).$$

For $j=2$, we instead define

$$f_2 := (\alpha+1)^{-3}\left(-27\mathcal{P}_2 f_1 + 3\mathcal{P}_2^2 f_0^2 x_a - 3\mathcal{P}_2(\alpha^4+\alpha^3-4\alpha^2-4\alpha+3)f_0^3\right) + (7\alpha^2-16\alpha+7)f_1 f_0.$$

A somewhat lengthy, but elementary, calculation shows that the local power series expansion of f_2 equals

$$f_2 = 3\mathcal{P}_3 T^8 + \mathcal{Q}_3 T^9 + O(T^q).$$

For $3 \leq j \leq i$, we assume now that f_{j-1} and f_{j-2} have the form claimed in equation (3.21) and we construct inductively the remaining functions f_j in the following way, defining:

$$f_j := -\frac{\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0}{(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2}}.$$

The idea of choosing the functions $f_{j-2}f_1$ and $f_{j-1}f_0$ is that the vanishing order at $Q_{(A,B)}$ is $3j+1$ for both. Hence, a suitable linear combination of them will vanish with order at least $3j+2$. Moreover, as $f_{j-2}f_1$ and $f_{j-1}f_0$ lie in $L((3j+3)D_\infty)$, a linear combination of them does as well. Therefore, we only need to show that

$$\begin{aligned}\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = \\ = -(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2} \left(3\mathcal{P}_{j+1} T^{3j+2} + \mathcal{Q}_{j+1} T^{3j+3} + O(T^q)\right).\end{aligned}$$

The local power series expansion of $\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0$ with respect to T can be obtained from the expansions of the functions $f_{j-2}f_1$ and $f_{j-1}f_0$, which are:

$$\begin{aligned}f_{j-2}f_1 &= \left(3\mathcal{P}_{j-1} T^{3j-4} + \mathcal{Q}_{j-1} T^{3j-3} + O(T^q)\right)\left(3\mathcal{P}_2 T^5 + \mathcal{Q}_2 T^6 + O(T^q)\right) \\ &= 9\mathcal{P}_2 \mathcal{P}_{j-1} T^{3j+1} + (3\mathcal{P}_{j-1}\mathcal{Q}_2 + 3\mathcal{P}_2 \mathcal{Q}_{j-1}) T^{3j+2} + \mathcal{Q}_2 \mathcal{Q}_{j-1} T^{3j+3} + O(T^q), \\ f_{j-1}f_0 &= \left(3\mathcal{P}_j T^{3j-1} + \mathcal{Q}_j T^{3j} + O(T^q)\right)\left(3T^2 + \mathcal{Q}_1 T^3 + O(T^q)\right) \\ &= 9\mathcal{P}_j T^{3j+1} + (3\mathcal{P}_j \mathcal{Q}_1 + 3\mathcal{Q}_j) T^{3j+2} + \mathcal{Q}_1 \mathcal{Q}_j T^{3j+3} + O(T^q).\end{aligned}$$

Hence, we have

$$\begin{aligned}\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = \\ = 3(\mathcal{P}_{j-1}\mathcal{P}_j \mathcal{Q}_2 + \mathcal{P}_2 \mathcal{P}_j \mathcal{Q}_{j-1} - \mathcal{P}_2 \mathcal{P}_{j-1} \mathcal{P}_j \mathcal{Q}_1 - \mathcal{P}_2 \mathcal{P}_{j-1} \mathcal{Q}_j) T^{3j+2} + \\ + \left(\mathcal{P}_j \mathcal{Q}_{j-1} \mathcal{Q}_2 - \mathcal{P}_{j-1} \mathcal{P}_2 \mathcal{Q}_j \mathcal{Q}_1\right) T^{3j+3} + O(T^q).\end{aligned}$$

We are therefore left to prove the two following identities:

$$\begin{aligned}3(\mathcal{P}_{j-1}\mathcal{P}_j \mathcal{Q}_2 + \mathcal{P}_2 \mathcal{P}_j \mathcal{Q}_{j-1} - \mathcal{P}_2 \mathcal{P}_{j-1} \mathcal{P}_j \mathcal{Q}_1 - \mathcal{P}_2 \mathcal{P}_{j-1} \mathcal{Q}_j) = \\ = -3(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2} \mathcal{P}_{j+1}\end{aligned} \tag{3.23}$$

and

$$\mathcal{P}_j \mathcal{Q}_{j-1} \mathcal{Q}_2 - \mathcal{P}_{j-1} \mathcal{P}_2 \mathcal{Q}_j \mathcal{Q}_1 = -(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2} \mathcal{Q}_{j+1}. \tag{3.24}$$

This can be conveniently done by using Lemma 3.14. Indeed, consider first equation (3.23) and use identity (3.20) as

$$\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j = \mathcal{P}_{j-2}\mathcal{Q}_0 \cdot (s^2 - s + 1)^6,$$

i.e., with indices $(j, 2, 0)$ (listed in order as in the statement of Lemma 3.14). Then, we obtain

$$\begin{aligned} \mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j &= \mathcal{P}_{j-1}(\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j) \\ &= \mathcal{P}_{j-1} \cdot (\alpha^2 - \alpha + 1)^5\mathcal{P}_{j-2}. \end{aligned} \tag{3.25}$$

By using again equation (3.20), this time with indices $(j-1, 1, 0)$, we can also rewrite

$$\begin{aligned} \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 &= \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{P}_1 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 \\ &= -\mathcal{P}_2\mathcal{P}_j(\mathcal{P}_{j-1}\mathcal{Q}_1 - \mathcal{P}_1\mathcal{Q}_{j-1}) \\ &= -\mathcal{P}_2\mathcal{P}_j \cdot (\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2}. \end{aligned} \tag{3.26}$$

Then, by equations (3.25) and (3.26), we have that equation (3.23) is equivalent to

$$\mathcal{P}_{j-1} \cdot (\alpha^2 - \alpha + 1)^5\mathcal{P}_{j-2} - \mathcal{P}_2\mathcal{P}_j \cdot (\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2} = -(\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2}\mathcal{P}_{j+1}.$$

Dividing out the factor $(\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2}$ both in the right hand side and the left hand side of this equality and rearranging the terms, we obtain

$$\mathcal{P}_{j-1} \cdot (\alpha^2 - \alpha + 1)^3 = \mathcal{P}_2\mathcal{P}_j - \mathcal{P}_{j+1},$$

which holds by Lemma 3.14, as it is precisely identity (3.19) with indices $(j, 1, 1)$.

In order to prove equation (3.24), we can argue in a similar way. Indeed, we have:

$$\begin{aligned} \mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2 - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 &= (\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j + \mathcal{P}_2\mathcal{Q}_j)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 \\ &= \left(\mathcal{P}_{j-2} \cdot (\alpha^2 - \alpha + 1)^5 + \mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1, \end{aligned}$$

where the last equality follows from equation (3.20) with indices $(j, 2, 0)$. Moreover,

$$\begin{aligned} &\left(\mathcal{P}_{j-2} \cdot (\alpha^2 - \alpha + 1)^5 + \mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 = \\ &\quad = \mathcal{P}_{j-2} \cdot (\alpha^2 - \alpha + 1)^5\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{Q}_j\left(\mathcal{P}_{j-1}\mathcal{Q}_1 - \mathcal{P}_1\mathcal{Q}_{j-1}\right) \\ &\quad\quad = \mathcal{P}_{j-2} \cdot (\alpha^2 - \alpha + 1)^5\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2} \cdot (\alpha^2 - \alpha + 1)^2, \end{aligned}$$

where the last equality follows from equation (3.20) with indices $(j-1,1,0)$. Finally, using again equation (3.20) with indices $(2,1,j-1)$, we have

$$\begin{aligned}\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2 &= \\ &= -\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\left(\mathcal{P}_2\mathcal{Q}_j-\mathcal{Q}_{j-1}\cdot(\alpha^2-\alpha+1)^3\mathcal{P}_1\right) \\ &= -\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\mathcal{Q}_{j+1},\end{aligned}$$

which proves equation (3.24).

From this, equation (3.21) follows directly, while equation (3.22) follows observing that $\mathcal{P}_{i+1}=0$ by hypothesis and $\mathcal{Q}_{i+1}\neq 0$ by Remark 3.15. As we have already observed that, by construction, $f_j\in L((3j+3)D_\infty)$ for all j in $0\le j\le i$, the proof of the theorem is then completed. □

Note that the proof of Theorem 3.19 does not work if $\alpha^2-\alpha+1=0$. However, another approach, different but very similar, can be used, as it will become clear in the proof of the following result. Recall that, if $\alpha^2-\alpha+1=0$, then α is not a root of any $\mathcal{P}_i$, for all $i\in\mathbb{Z}_{>0}$.

Theorem 3.20. *Suppose that $P_{(a,b)}$ is a place of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ such that $\alpha(P_{(a,b)})^2-\alpha(P_{(a,b)})+1=0$. Then, for every positive integer i such that $i\le m-2$, there exists a function $g_i\in L((3i+3)D_\infty)$ with $v_{P_{(a,b)}}(g_i)=3i+2$.*

Proof. As before, in this proof we write α instead of $\alpha(P_{(a,b)})$ and $\mathcal{P}_j$, $\mathcal{Q}_j$ instead of $\mathcal{P}_j(\alpha)$, $\mathcal{Q}_j(\alpha)$. For each $i\in\mathbb{Z}_{\ge 0}$, we claim that there exists a function $g_i\in L((3i+3)D_\infty)$ such that the local power series expansion of g_i at $Q_{(A,B)}$ with respect to the local parameter $T:=(u-A)/A$ is:

$$g_i=3T^{3i+2}+(\alpha+1)T^{3i+3}+O(T^q). \tag{3.27}$$

Denoting by f_0 and f_1, the functions constructed in the previous theorem, we see that $g_0=f_0$, while $g_1=(2\alpha-1)f_1/9$, since

$$(2\alpha-1)3\mathcal{P}_2\equiv 27 \pmod{\alpha^2-\alpha+1}$$

and

$$(2\alpha-1)\mathcal{Q}_2\equiv 9\alpha+9 \pmod{\alpha^2-\alpha+1}.$$

For $i\ge 2$, we assume now that g_{i-1} and g_{i-2} have the form claimed in equation (3.27) and we construct inductively the remaining functions g_i by taking a suitable linear combination of

$$g_{i-1},\quad g_{i-2}\cdot g_0\cdot x_a,\quad g_{i-2}\cdot g_0^2 \quad\text{and}\quad g_{i-1}\cdot g_0.$$

The point of choosing these four functions is that their vanishing orders at $Q_{(A,B)}$ are $3i-1$, $3i-1$, $3i$ and $3i+1$ respectively. Therefore a suitable linear combination of them will vanish with order at least $3i+2$. Moreover, since the four functions all lie in $L((3i+3)D_\infty)$, any linear combination of them does as well.

More in detail, if we set

$$g_i := (6\alpha-3)g_{i-1} - \frac{2\alpha-1}{3}g_{i-2}g_0x_a + \frac{3\alpha-2}{3}g_{i-2}g_0^2 - (\alpha-2)g_{i-1}g_0,$$

then a direct computation shows that equation (3.27) is satisfied. □

With Theorem 3.19 and Theorem 3.20 established, we now have all the necessary tools for the computation of the Weierstrass semigroup at every place of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. We will assume that q is at least five, so that $m \geq 2$. If $q = 2$, the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is in fact elliptic, so all Weierstrass semigroups are just $\{0\} \cup \mathbb{Z}_{\geq 2}$ in that case. We start with the determination of the semigroup at the places in the set $\mathcal{O}$ and then continue to all the other places, starting from those in $\mathfrak{R}$.

Remark 3.21. *Note that the Fundamental Equation [46, Page xix (ii)] and [46, Proposition 10.9] have as a direct consequence that both q and $q+1$ are non-gaps at all the places in $\mathcal{O} \cup \mathfrak{R}$. However, in Theorem 3.22 and in Lemma 3.24, we prove this fact again, as we show this with some easy explicit computations.*

3.3 The Weierstrass semigroup at $P \in \mathcal{O}$

Theorem 3.22. *Let $P \in \mathcal{O}$. Then $H(P) = \langle q-2, q, q+1 \rangle$.*

Proof. We will prove that

$$H(P_{(a,0)}) = \langle q-2, q, q+1 \rangle$$

for $P_{(a,0)} \in \mathcal{O}_m$ and hence the result will follow as, by Corollary 3.7, $\mathcal{O}$ is contained in an orbit of $\mathrm{Aut}(\mathcal{X}_3)$ and all the places in the same orbit have the same Weierstrass semigroup.

We start by showing that the semigroup $H := \langle q-2, q, q+1 \rangle$, that is to say, the semigroup generated by $q-2, q$ and $q+1$, is contained in $H(P_{(a,0)})$. Proposition 3.5 implies that the functions

$$\frac{1}{x-a}, \quad \frac{y}{x-a}, \quad \text{and} \quad \frac{y^3}{x(x-a)}$$

in $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ only have a pole at $P_{(a,0)}$ and of order $q+1$, q, and $q-2$ respectively. This shows that $q-2, q, q+1 \in H(P_{(a,0)})$, proving that $H \subseteq H(P_{(a,0)})$.

Hence, to conclude the proof of the theorem it is sufficient to show that the genus of the semigroup H is equal to $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. To do so, note that semigroup H is telescopic, since the sequence $(a_1, a_2, a_3) := (q-2, q+1, q)$ is a telescopic sequence. Then, defining $d_0 = 0$, $d_1 = q-2$, $d_2 = \gcd(q-2, q+1) = 3$, and $d_3 = \gcd(q-2, q, q+1) = 1$, the genus of H is given by (see equation (2.6))

$$g(H) = \frac{1}{2}\left(1 + \sum_{i=1}^{3}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right) = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)).$$

□

Remark 3.23. *Using equation* (2.5)*, we can compute the Apéry set $A(H)$ of the semigroup*

$$H := \langle q-2, q, q+1 \rangle$$

determined in Theorem 3.22.

Note first that the multiplicity of H is $q-2$. We claim that the following set

$$\begin{aligned} A := \{&0, q, q+1\} \\ &\cup \{iq + (i-2), iq + (i-1), i(q+1) \mid i = 2, \dots, m-2\} \\ &\cup \{(m-1)q + (m-3), (m-1)q + (m-2)\} \\ &\cup \{mq + (m-2)\} \end{aligned}$$

is the Apéry set of the semigroup H. To prove this result, we first show that A contains exactly $q-2$ elements, that are representatives of pairwise distinct congruence classes modulo $q-2$, so that $\sum_{a\in A(H)} \left\lfloor \frac{a}{q-2} \right\rfloor \leq \sum_{a\in A} \left\lfloor \frac{a}{q-2} \right\rfloor$. Then, since by equation (2.5) *we have that $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = \sum_{a\in A(H)} \left\lfloor \frac{a}{q-2} \right\rfloor$, we conclude the proof showing that $\sum_{a\in A} \left\lfloor \frac{a}{q-2} \right\rfloor = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.*

Observe that

- $0, q, q+1$ *are representatives for the classes of* $0, 2, 3$*, respectively;*
- $iq + (i-1) \equiv 3i - 1 \pmod{q-2}$*, and hence the elements $iq + (i-1)$, for $i = 2, \dots, m-2$, form a set of representatives for the congruence classes of $5, 8, \dots 3m-7$;*
- *similarly, as $i(q+1) \equiv 3i \pmod{q-2}$, the elements $i(q+1)$, for $i = 2, \dots, m-2$, are a set of representatives for the congruence classes of $4, 7, \dots 3m-8$.*

- *Moreover, as* $iq + (i-2) \equiv 3i - 2 \pmod{q-2}$*, the elements* $iq + (i-2)$*, for* $i = 2, \ldots, m-2$*, are a set of representatives for the congruence classes of* $6, 9 \ldots, 3m-6$*.*

- *Finally,* $(m-1)q + (m-3) \equiv 3m-5 \pmod{q-2}$ *and* $(m-1)q + (m-2) \equiv 3m-4 \pmod{q-2}$*, while* $mq + (m-2) \equiv 1 \pmod{q-2}$*.*

Therefore, the set A *contains exactly* $3(m-3)+6 = q-2$ *distinct elements, each of which is a representative for a congruence class modulo* $q-2$*.*

Now, note that

$$\left\lfloor \frac{q}{q-2} \right\rfloor = \left\lfloor \frac{q+1}{q-2} \right\rfloor = 1$$

and that, for every $i = 2, \ldots, m-2$*,*

$$\left\lfloor \frac{iq + (i-2)}{q-2} \right\rfloor = \left\lfloor \frac{iq + (i-1)}{q-2} \right\rfloor = \left\lfloor \frac{i(q+1)}{q-2} \right\rfloor = i.$$

Moreover, we have

$$\left\lfloor \frac{(m-1)q + (m-3)}{q-2} \right\rfloor = \left\lfloor \frac{(m-1)q + (m-2)}{q-2} \right\rfloor = m-1$$

and

$$\left\lfloor \frac{mq + (m-2)}{q-2} \right\rfloor = m+1.$$

Therefore, we obtain

$$\begin{aligned}
\sum_{a \in A} \left\lfloor \frac{a}{q-2} \right\rfloor &= 2 + 3 \sum_{i=2}^{m-2} i + 2(m-1) + m + 1 \\
&= 3m + 1 + 3 \sum_{i=1}^{m-3} (i+1) \\
&= \frac{q^2 - q + 4}{6} = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)).
\end{aligned}$$

3.4 Weierstrass semigroups at $P_{(a,b)} \in \mathfrak{R}$

Lemma 3.24. *Let* $P_{(a,b)} \in \mathfrak{R}$*. Then* $q+1$ *and* q *are contained in* $H(P_{(a,b)})$*.*

Proof. The fact that $q+1 \in H(P_{(a,b)})$ is simply a consequence of equation (3.16). To prove that $q \in H(P_{(a,b)})$, let $P_{(\bar{a},0)} \in \mathcal{O}_m$ and consider the function

$$\mathfrak{f} := \frac{(x-a) f_{P_{(\bar{a},0)},1}}{f_{P_{(a,b)},1}(x-\bar{a})},$$

where the functions $f_{P_{(a,b)},1}$ and $f_{P_{(\bar{a},0)},1}$ are defined as in equation (3.16). Then, from equations (3.16), (3.13), (3.14), one has

$$\begin{aligned}(\mathfrak{f}) &= P_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi\neq 1} P_{(a,\xi b)} - 3\sum_{j=1}^{m} P_\infty^j + (q+1)P_{(\bar{a},0)} - (q+1)P_\infty^1 + \\ &\quad - (q+1)P_{(a,b)} + (q+1)P_\infty^1 - (q+1)P_{(\bar{a},0)} + 3\sum_{i=1}^{m} P_\infty^i \\ &= -\,qP_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi\neq 1} P_{(a,\xi b)},\end{aligned}$$

implying that $q \in H(P_{(a,b)})$. □

Theorem 3.25. *Let $P_{(a,b)} \in \mathfrak{R}$ be a place such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$. Then*

$$H(P_{(a,b)}) = \langle q, q+1, (q-1)+i(q-2) \mid i = 0,\dots,m-2\rangle.$$

Proof. We start by showing that the semigroup $H := \langle q, q+1, (q-1)+i(q-2) \mid i = 0,\dots,m-2\rangle$ is contained in $H(P_{(a,b)})$. To this aim, we show that $q, q+1, (q-1)+i(q-2)$, for all $i = 0,\dots,m-2$, are pole numbers of $P_{(a,b)}$. By Lemma 3.24, we already know that $q, q+1 \in H(P_{(a,b)})$, so we are left to show that $(q-1)+i(q-2)$ is a pole number for every $i = 0,\dots,m-2$. We prove this considering the following family of functions. For all i such that $0 \le i \le m-2$, let $P_{(\bar{a},0)} \in \mathcal{O}_m$ and define the function

$$G_i := \frac{g_i \cdot f_{P_{(\bar{a},0)},1}^{i+1}}{f_{P_{(a,b)},1}^{i+1} \cdot (x-\bar{a})^{i+1}},$$

where the functions g_i are those constructed in Theorem 3.20. Then, using equations (3.16), (3.13), (3.14) and Theorem 3.20, the divisor of the function G_i

is seen to be

$$\begin{aligned}(G_i) = \quad & (3i+2)P_{(a,b)} + E_i - (3i+3)\sum_{j=1}^{m} P_\infty^j \\ & + (i+1)(q+1)P_{(\bar{a},0)} - (i+1)(q+1)P_\infty^1 \\ & - (i+1)(q+1)P_{(a,b)} + (i+1)(q+1)P_\infty^1 \\ & - (i+1)(q+1)P_{(\bar{a},0)} + (3i+3)\sum_{j=1}^{m} P_\infty^j \\ = \quad & E_i - ((q-1)+i(q-2))P_{(a,b)},\end{aligned}$$

where $E_i \in \mathrm{Div}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_i)$. Therefore, $(q-1)+i(q-2) \in H(P_{(a,b)})$ for all $i = 1, \ldots, m-2$.

To complete the proof, we need to show that the genus of the semigroup H is less than or equal to $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. Indeed, the inequality $g(H) \geq g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is already clear, since we just showed that $H \subseteq H(P_{(a,b)})$. Of course we know that $0 \in H$, but we claim that, for $j = 1, \ldots, m-1$, all integers in $\{j(q-2)+1, \ldots, j(q+1)\}$ are in H as well. This is clear for $j = 1$, since $q-1, q, q+1 \in H$. If this is true for some $j < m-1$, then adding $q-1$ and $q+1$ to all integers in $\{j(q-2)+1, \ldots, j(q+1)\}$ shows that the consecutive integers in $\{(j+1)(q-2)+2, \ldots, (j+1)(q+1)\}$ are all in H. Since $(j+1)(q-2)+1 = (q-1)+j(q-2) \in H$, we conclude that all integers in $\{(j+1)(q-2)+1, \ldots, (j+1)(q+1)\}$ are in H, which proves the claim. Now note that $\{(m-1)(q-2)+1, \ldots, (m-1)(q+1)\}$ consists of $q-2$ consecutive integers, all in H. Adding integral multiples of $q-1$ and q to this set, we obtain that all integers greater than or equal to $(m-1)(q-2)+1+q-1 = (m-1)(q+1)+2$ are in H. This means that the following inequality holds for the genus of H:

$$g(H) \leq (q-2) + (q-5) + \cdots + 3 + 1,$$

where the final $+1$ counts the potential gap $(m-1)(q+1)+1$. Hence

$$g(H) \leq 1 + 3\sum_{k=1}^{m-1} k = 1 + 3m(m-1)/2 = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)),$$

which is what we needed to show. □

Remark 3.26. *As in Remark 3.23, we compute the Apéry set $A(H)$ of the semigroup*

$$H := \langle q, q+1, (q-1)+i(q-2) \mid i = 0, \ldots, m-2 \rangle$$

determined in Theorem 3.25.

We first note that the multiplicity of H is $q-1$ and we claim that the following set

$$\begin{aligned} A := \{&0, q, q+1\} \\ &\cup \{(q-1)+(i-1)(q-2), iq+(i-1), i(q+1) \ \mid i = 2, \dots, m-1\} \\ &\cup \{m(q-1)+2m-1\} \end{aligned}$$

is the Apéry set of H. Similarly to the discussion in Remark 3.23, we first show that A contains precisely $q-1$ elements, that are representatives of pairwise distinct congruence classes modulo $q-1$, so that $\sum_{a\in A(H)} \left\lfloor \frac{a}{q-1} \right\rfloor \leq \sum_{a\in A} \left\lfloor \frac{a}{q-1} \right\rfloor$. Then, since $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = \sum_{a\in A(H)} \left\lfloor \frac{a}{q-1} \right\rfloor$, we conclude the proof showing that $\sum_{a\in A} \left\lfloor \frac{a}{q-1} \right\rfloor = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

Observe that

- *$0, q, q+1$ are representatives for the classes of $0, 1, 2$, respectively;*
- *$iq+(i-1) \equiv 2i-1 \pmod{q-1}$, and hence the elements $iq+(i-1)$, for $i = 2, \dots, m-1$, form a set of representatives for the congruence classes of $3, 5, \dots 2m-3$;*
- *similarly, as $i(q+1) \equiv 2i \pmod{q-1}$, the elements $i(q+1)$, for $i = 2, \dots, m-1$, are a set of representatives for the congruence classes of $4, 6, \dots 2m-2$.*
- *Moreover, as $(q-1)+(i-1)(q-2) \equiv q-1-(i-1) \pmod{q-1}$, the elements $(q-1)+(i-1)(q-2)$, for $i = 2, \dots, m-1$, are a set of representatives for the congruence classes of $2m, \dots, q-3, q-2$. Finally, $m(q-1)+2m-1$ is a representative for the class of $2m-1$.*

Therefore, the set A contains exactly $3(m-2)+4 = q-1$ distinct elements, each of which is a representative for a congruence class modulo $q-1$.

Finally, note that

$$\left\lfloor \frac{(q-1)+(q-2)}{q-1} \right\rfloor = \left\lfloor \frac{q}{q-1} \right\rfloor = \left\lfloor \frac{q+1}{q-1} \right\rfloor = 1$$

and that, for every $i = 2, \dots, m-2$

$$\left\lfloor \frac{(q-1)+i(q-2)}{q-1} \right\rfloor = \left\lfloor \frac{iq+(i-1)}{q-1} \right\rfloor = \left\lfloor \frac{i(q+1)}{q-1} \right\rfloor = i.$$

Moreover, we have

$$\left\lfloor \frac{(m-1)q+(m-2)}{q-1} \right\rfloor = \left\lfloor \frac{(m-1)(q+1)}{q-1} \right\rfloor = m-1$$

and

$$\left\lfloor \frac{m(q-1)+2m-1}{q-1} \right\rfloor = m.$$

Therefore, we obtain

$$\begin{aligned}\sum_{a\in A} \left\lfloor \frac{a}{q-1} \right\rfloor &= 3 + 3\sum_{i=2}^{m-2} i + 2(m-1) + m \\ &= 3\sum_{i=1}^{m-1} i + 1 \\ &= \frac{q^2-q+4}{6} = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)).\end{aligned}$$

Theorem 3.27. *Let $P_{(a,b)} \in \mathfrak{R}$ be a place such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 \neq 0$. Furthermore, let i be the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. If $i \leq m-2$, then*

$$H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j = 0, \ldots, i-1 \rangle.$$

If $i = m-1$, then

$$H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2) \mid j = 0, \ldots, m-2 \rangle.$$

Proof. We first assume that $i \leq m-2$.We proceed similarly as in the proof of Theorem 3.25, showing that the semigroup $H := \langle q-1, q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j = 1, \ldots, i-1 \rangle$ is contained in $H(P_{(a,b)})$ and has at most $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ gaps. For all j such that $j = 1, \ldots, i-1$, let $P_{(\bar{a},0)} \in \mathcal{O}_m$ and define the function

$$F_j := \frac{f_j \cdot f_{P_{(\bar{a},0)},1}^{j+1}}{f_{P_{(a,b)},1}^{j+1} \cdot (x-\bar{a})^{j+1}},$$

where the f_j are the functions constructed in Theorem 3.19. Using equations (3.16), (3.13), (3.14) and Theorem 3.20, the divisor of the function F_j can be seen to be

$$\begin{aligned}(F_j) = \quad & (3j+2)P_{(a,b)} + E_j - (3j+3)D_\infty \\ & + (j+1)(q+1)P_{(\bar{a},0)} - (j+1)(q+1)P_\infty^1 \\ & - (j+1)(q+1)P_{(a,b)} + (j+1)(q+1)P_\infty^1 \\ & - (j+1)(q+1)P_{(\bar{a},0)} + (3j+3)D_\infty \\ = \quad & E_j - ((q-1)+j(q-2))P_{(a,b)},\end{aligned}$$

where $E_j \in \mathrm{Div}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_j)$. Therefore, $(q-1)+j(q-2) \in H(P)$ for all $j = 1, \ldots, i-1$. Similarly,

$$\begin{aligned}(F_i) = \quad & (3i+3)P_{(a,b)} + E_i - (3i+3)D_\infty \\ & + (i+1)(q+1)P_{(\bar{a},0)} - (i+1)(q+1)P^1_\infty \\ & - (i+1)(q+1)P_{(a,b)} + (i+1)(q+1)P^1_\infty \\ & - (i+1)(q+1)P_{(\bar{a},0)} + (3i+3)D_\infty \\ = \quad & E_i - ((q-1)+i(q-2)-1)P_{(a,b)},\end{aligned}$$

where $E_i \in \mathrm{Div}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_i)$. We have hence shown that $H \subseteq H(P_{(a,b)})$.

What remains to be shown is that the genus of the semigroup H does not exceed $g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. We know that $0 \in H$ and, just as in the proof of Theorem 3.25, we conclude that all integers in the set $\{j(q-2)+1, \ldots, j(q+1)\}$ are in H, for any $j = 1, \ldots, i$. Furthermore, we have already shown that $(i+1)(q-2) \in H$ and adding $q-1$, q, and $q+1$ to the integers in $\{i(q-2)+1, \ldots, i(q+1)\}$ yields that $\{(i+1)(q-2)+2, \ldots, (i+1)(q+1)\} \subseteq H$.

Since $P_{(a,b)} \in \mathfrak{R}$, Lemma 3.18 implies that $i+1$ divides m. We claim that, for $k = 0, \ldots, m/(i+1)-1$ and all $j = 1, \ldots, i$, the sets $\{(k(i+1)+j)(q-2)+1, \ldots, (k(i+1)+j)(q+1)\}$ are contained in H as well as the integer $((k+1)(i+1))(q-2)$ and the set $\{(k+1)(i+1)(q-2)+2, \ldots, (k+1)(i+1)(q+1)\}$. We have so far shown this for $k = 0$. If the claim is true for some $k-1 < m/(i+1)-1$, adding $(i+1)(q-2)$ and the integers in $\{(i+1)(q-2)+2, \ldots, (i+1)(q+1)\}$ immediately shows that the claim is true for k as well, proving the initial claim. For $k = m/(i+1)-1$, we obtain that $\{m(q-2)+2, \ldots, m(q+1)\}$, which contains q consecutive integers, is a subset of H. This shows that all integers greater than or equal to $m(q-2)+2 = (m-1)(q+1)+2$ are in H. Estimating the number of gaps is now done very similarly as in the proof of Theorem 3.25. The number of gaps of the semigroup there is in fact exactly the same as those of the semigroup H constructed here: in the proof of Theorem 3.25, for all $k = 1, \ldots, m/(i+1)-1$, the integer $k(i+1)(q-2)$ was a gap, while $k(i+1)(q-2)+1$ was not. Now we have instead that $k(i+1)(q-2)$ is in H and $k(i+1)(q-2)+1$ is not, hence $g(H) \leq g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ holds again.

We are left to prove the theorem if $i = m-1$. Using exactly the same approach as above, we can show that $H := \langle q-1, q, q+1, (q-1)+j(q-2) \mid j = 1, \ldots, m-2 \rangle$ is contained in $H(P_{(a,b)})$. Now note that H is exactly the same semigroup as the one occurring in Theorem 3.25, hence $g(H) \leq g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ holds in this case as well. □

Remark 3.28. *Similarly to what done in Remark 3.23 and Remark 3.26, we here compute the Apéry set of the semigroup H determined in Theorem 3.27 for*

the cases $i \leq m-2$. The case $i = m-1$ is indeed the same as the semigroup determined in Theorem 3.25.

As in Remark 3.26, note firstly that the multiplicity of H is $q-1$. We define the following sets:

$$\begin{aligned}
A_1 &:= \{0, q, q+1, m(q-1)+2m-1\},\\
A_2 &:= \{jq+(j-1), j(q+1) \ \mid \ j = 2, \dots, m-1\},\\
A_3 &:= \{(q-1)+j(q-2) \ \mid \ 1 \leq j \leq m-2 \ \wedge \ j+1 \not\equiv 0, 1 \pmod{i+1}\},\\
A_4 &:= \left\{(q-1)+j(q-2)-1 \ \mid \ j = ki+(k-1) \wedge k = 1, \dots, \left\lfloor \frac{m-2}{i+1} \right\rfloor \right\}\\
&\quad \cup \left\{(q-1)+j(q-2)-1+q \ \mid \ j = ki+(k-1) \wedge k = 1, \dots, \left\lfloor \frac{m-2}{i+1} \right\rfloor \right\}.
\end{aligned}$$

Note that the set A_4 can also be rewritten as

$$A_4 = \left\{k(i+1)(q-2),\ k(i+1)(q-2)+q \ \mid k = 1, \dots, \left\lfloor \frac{m-2}{i+1} \right\rfloor \right\};$$

furthermore, if $i = 1$, the set A_3 is empty.

We claim that the set

$$\tilde{A} := A_1 \cup A_2 \cup A_3 \cup A_4$$

is the Apéry set $A(H)$ of the semigroup H. We start by showing that the elements of $\tilde{A}$ are all distinct and constitute a complete set of representatives for the congruence classes modulo $q-1$. Similarly to what done in the proof of Remark 3.26, we observe that

- *$0, q, q+1$ are representatives for the classes of $0, 1, 2$, respectively;*
- *$jq+(j-1) \equiv 2j-1 \pmod{q-1}$, and hence the elements $jq+(j-1)$, for $j = 2, \dots, m-1$, form a set of representatives for the congruence classes of $3, 5, \dots 2m-3$;*
- *similarly, as $j(q+1) \equiv 2j \pmod{q-1}$, the elements $j(q+1)$, for $j = 2, \dots, m-1$, are a set of representatives for the congruence classes of $4, 6, \dots 2m-2$;*
- *$m(q-1)+2m-1$ is a representative for the class of $2m-1$.*
- *Finally, the elements of $A_3 \cup A_4$ are a set of representatives for the congruence classes of $2m, \dots, q-3, q-2$. Indeed, if $(q-1)+j(q-2) \in A_3$,*

then $(q-1)+j(q-2) \equiv q-1-j \pmod{q-1}$. *On the other hand, for the elements of* A_4 *we have that, for all* $j = ki+(k-1)$, *with* $k = 1, \ldots, \left\lfloor \frac{m-2}{i+1} \right\rfloor$,

$$(q-1)+j(q-2)-1 \equiv q-1-(j+1) \pmod{q-1}$$

and

$$(q-1)+j(q-2)-1+q \equiv q-1-j \pmod{q-1}.$$

This shows that, for each $j = 1, \ldots, m-2$, *there is exactly one element of* $\tilde{A}$ *that is congruent to* $q-1-j$ *modulo* $q-1$.

Therfore, we conclude that $\tilde{A}$ *contains a representative for each congruence class modulo* $q-1$ *and* $|\tilde{A}| = 4+2(m-2)+(m-2) = q-1$.

Finally, we observe that

$$\left\lfloor \frac{q}{q-1} \right\rfloor = \left\lfloor \frac{q+1}{q-1} \right\rfloor = 1,$$

$$\left\lfloor \frac{m(q-1)+2m-1}{q-1} \right\rfloor = m,$$

and, for every $j = 2, \ldots, m-1$,

$$\left\lfloor \frac{jq+(j-1)}{q-1} \right\rfloor = \left\lfloor \frac{j(q+1)}{q-1} \right\rfloor = j.$$

Moreover, for the elements of A_3, *we have that*

$$\left\lfloor \frac{(q-1)+j(q-2)}{q-1} \right\rfloor = j,$$

while, for the elements of A_4, *we have*

$$\left\lfloor \frac{(q-1)+j(q-2)-1}{q-1} \right\rfloor = j$$

and

$$\left\lfloor \frac{(q-1)+j(q-2)-1+q}{q-1} \right\rfloor = j+1.$$

Therefore, we obtain

$$\begin{aligned}
\sum_{a \in A} \left\lfloor \frac{a}{q-1} \right\rfloor &= 2+m+2\sum_{j=2}^{m-1} j + \sum_{j=1}^{m-2} j \\
&= 2\sum_{j=1}^{m-1} j + \sum_{j=1}^{m-2} j + m \\
&= \frac{q^2-q+4}{6} = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)),
\end{aligned}$$

which concludes the proof.

In the following two sections, we compute the Weierstrass semigroups at all the remaining places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, namely at all the places $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$. We start by computing the semigroup for the generic case, i.e., for the non-Weierstrass places of the curve and, lastly, we determine the semigroups for the remaining Weierstrass places.

3.5 The generic case

Theorem 3.29. *Let $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ be such that $\mathcal{P}_j(\alpha(P_{(a,b)})) \neq 0$ for all $j = 2, \dots, m-1$. Then*

$$G(P_{(a,b)}) = \{jq + k \mid j = 0, \dots, m-2,\ k = 1, \dots, q-3j-2\} \cup \{(m-1)q+1\},$$

that is,

$$H(P_{(a,b)}) = \{0, (j+1)(q-3)+2+k, (m-1)q+2, \dots \mid j = 0, \dots, m-2,\ k = 0, \dots, 3j+1\}.$$

Proof. Let $G := \{jq+k \mid j = 0, \dots, m-2,\ k = 1, \dots, q-3j-2\} \cup \{(m-1)q+1\}$ be the putative set of gaps. Direct computations show that

$$|G| = 1 + \sum_{j=0}^{m-2} (q - (3j+2)) = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)).$$

We need to prove that, for every $g \in G$, there exists a function $h_g \in L((q-2)D_\infty)$ such that $v_{P_{(a,b)}}(h_g) = g - 1$, see Proposition 2.18.

Let $g = jq + k \in G$. We distinguish the following cases.

1. If $\lfloor \frac{k}{3} \rfloor \neq 0$, then we define:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 0 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot t_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

2. If $\lfloor \frac{k}{3} \rfloor = 0$, we define instead:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} & \text{if } k = 1, \\ \\ F^j_{P_{(a,b)}} \cdot (y-b) & \text{if } k = 2. \end{cases}$$

Here, the function $f_{\lfloor \frac{k}{3} \rfloor - 1}$ is one of the functions f_i constructed in Theorem 3.19 and the function $F_{P_{(a,b)}}$ is as defined in equation (3.17).

Note that, as $j = 0, \ldots, m-2$, for $k = 3, \ldots, q-3j-2$ it holds that

$$0 \leq \left\lfloor \frac{k}{3} \right\rfloor - 1 \leq \left\lfloor \frac{q-3j-2}{3} \right\rfloor - 1 = \frac{q-2}{3} - j - 1 = m - 2 - j \leq m - 2,$$

hence the function h_g is well defined, for any $i = 0, \ldots, m-2$ and $k = 1, \ldots, q-3j-2$. Indeed, defining the function h_g in this way, for any $g = jq + k \in G$, we have what follows.

Case 1: $\lfloor \frac{k}{3} \rfloor \neq 0$.

If $k \equiv 0 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 \right) + 2 = jq + k - 1$$

and

$$\begin{aligned} (h_g)_\infty &\leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1 \right) \right) D_\infty = (3j+k) D_\infty \\ &\leq (3j + q - 3j - 2) D_\infty = (q-2) D_\infty. \end{aligned}$$

If $k \equiv 1 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 \right) + 2 + 1 = jq + (k-1) - 3 + 3 = jq + k - 1$$

and

$$\begin{aligned} (h_g)_\infty &\leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1 \right) + 2 \right) D_\infty = (3j + k + 1) D_\infty \\ &\leq (3j + q - 3j - 4 + 1) D_\infty = (q-3) D_\infty, \end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 1 \pmod 3$, then $k \leq (q - 3j - 2) - 2 = q - 3j - 4$.

If $k \equiv 2 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1\right) + 2 + 2 = jq + (k-2) - 3 + 4 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1\right) + 3\right) D_\infty = (3j + k + 1)D_\infty \\ &\leq (3j + q - 3j - 3 + 1)D_\infty = (q-2)D_\infty,\end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 2 \pmod 3$, then $k \leq (q - 3j - 2) - 1 = q - 3j - 3$.

Case 2: $\left\lfloor \frac{k}{3} \right\rfloor = 0$.

If $k = 1$, then

$$v_{P_{(a,b)}}(h_g) = jq$$

and

$$(h_g)_\infty \leq (3j)D_\infty \leq ((q+1) - 6)D_\infty = (q-5)D_\infty.$$

If $k = 2$, then

$$v_{P_{(a,b)}}(h_g) = jq + 1$$

and

$$(h_g)_\infty \leq (3j + 2)D_\infty \leq ((q+1) - 6 + 2)D_\infty = (q-3)D_\infty.$$

□

Since the Weierstrass semigroup at all but a finite number of places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is as described in Theorem 3.29 (see Remark 2.17), we call

$$H_{gen} := \{0, (j+1)(q-3)+2+k, (m-1)q+2, \ldots \mid j = 0, \ldots, m-2,\ k = 0, \ldots, 3j+1\}$$

the *generic* Weierstrass semigroup of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ and

$$G_{gen} := \{jq + k \mid j = 0, \ldots, m-2,\ k = 1, \ldots, q - 3j - 2\} \cup \{(m-1)q + 1\}$$

the *generic* set of gaps of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$.

3.6 Weierstrass semigroups at the remaining Weierstrass places

Theorem 3.30. *Let $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ and let i be the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. Suppose that $i \leq m-2$. Then*

$$\begin{aligned} G(P_{(a,b)}) = \Big(G_{gen} \setminus \Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\}\Big) \\ \cup \Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\}, \end{aligned} \tag{3.28}$$

that is,

$$\begin{aligned} H(P_{(a,b)}) = \Big(H_{gen} \setminus \Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\}\Big) \\ \cup \Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\}. \end{aligned}$$

Proof. Let G as in equation (3.28) be the putative set of gaps. Since the cardinality of the set

$$\Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\}$$

is the same as the cardinality of the set

$$\Big\{(m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \Big\},$$

it follows immediately that $|G(P_{(a,b)})| = |G_{gen}| = g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. Hence, as in the proof of Theorem 3.29, we are now left to show that, for each $g \in G$, there exists a function h_g such that $h_g \in L((q-2)D_\infty)$ and $v_{P_{(a,b)}}(h_g) = g-1$.

For any $g = jq + k$, let $\mathfrak{c} := \left\lfloor \frac{k}{3(i+1)} \right\rfloor$. We can then write

$$\left\lfloor \frac{k}{3} \right\rfloor = \mathfrak{c}(i+1) + h,$$

where h is an integer such that $0 \leq h \leq i$, and

$$k = \left\lfloor \frac{k}{3} \right\rfloor \cdot 3 + r = 3\mathfrak{c}(i+1) + 3h + r,$$

where r is an integer such that $0 \leq r \leq 2$. First note that, with this choice of $\mathfrak{c}$, $0 \leq \left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) \leq i-1$ for all k such that $\left\lfloor \frac{k}{3} \right\rfloor \neq \mathfrak{c}(i+1)$. Indeed,

$$\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) \leq i-1 \quad \Longleftrightarrow \quad \left\lfloor \frac{k}{3} \right\rfloor - \mathfrak{c} \leq i + \mathfrak{c}i,$$

hence, as $\lfloor \frac{k}{3} \rfloor = \mathfrak{c}(i+1)+h$, with h an integer such that $0 \le h \le i$, we obtain

$$\left\lfloor \frac{k}{3} \right\rfloor - \mathfrak{c} \le i + \mathfrak{c}i \quad \Longleftrightarrow \quad \mathfrak{c}(i+1)+h-\mathfrak{c} \le i+\mathfrak{c}i \quad \Longleftrightarrow \quad h \le i,$$

which is satisfied.

We now distinguish the following cases.

1. If $\lfloor \frac{k}{3} \rfloor \neq \mathfrak{c}(i+1)$, then we define:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 0 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_{\lfloor \frac{k}{3} \rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot t_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

2. If $\lfloor \frac{k}{3} \rfloor = \mathfrak{c}(i+1)$, we define instead:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot (y-b) \cdot t_{P_{(a,b)}} \cdot f_{i-1} \cdot f_i^{\mathfrak{c}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \le m-2-i, \\ F^j_{P_{(a,b)}} \cdot f_{\frac{k}{3}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \ge m-1-i, \\ F^j_{P_{(a,b)}} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

Indeed, for $g = jq + k \in G$, we have the following situation.

Case 1: $\lfloor \frac{k}{3} \rfloor \neq \mathfrak{c}(i+1)$.

If $k \equiv 0 \pmod 3$, then

$$\begin{aligned} v_{P_{(a,b)}}(h_g) &= jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) \\ &= jq + k - 3 + 2 = jq + k - 1 \end{aligned}$$

and

$$\begin{aligned} (h_g)_\infty &\le (3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)+1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k)D_\infty \\ &\le (3j+q-3j-2)D_\infty = (q-2)D_\infty, \end{aligned}$$

where the last inequality above follows from the fact that $k \leq q - 3j - 2$.

If $k \equiv 1 \pmod 3$, then

$$\begin{aligned} v_{P_{(a,b)}}(h_g) &= jq + 1 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) \\ &= jq + (k-1) - 3 + 3 = jq + k - 1 \end{aligned}$$

and

$$\begin{aligned} (h_g)_\infty &\leq (3j + 2 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) + 1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j + k + 1)D_\infty \\ &\leq (3j + q - 3j - 3)D_\infty = (q-3)D_\infty, \end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 1 \pmod 3$, then $k \leq (q - 3j - 2) - 2 = q - 3j - 4$.

If $k \equiv 2 \pmod 3$, then

$$\begin{aligned} v_{P_{(a,b)}}(h_g) &= jq + 2 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) \\ &= jq + (k-2) - 3 + 4 = jq + k - 1 \end{aligned}$$

and

$$\begin{aligned} (h_g)_\infty &\leq (3j + 3 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) + 1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j + k + 1)D_\infty \\ &\leq (3j + q - 3j - 2)D_\infty = (q-2)D_\infty, \end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 2 \pmod 3$, then $k \leq (q - 3j - 2) - 1 = q - 3j - 3$.

Case 2: $\left\lfloor \frac{k}{3} \right\rfloor = \mathfrak{c}(i+1)$.

If $k \equiv 0 \pmod 3$ and $j \leq m - 2 - i$, then

$$v_{P_{(a,b)}}(h_g) = jq+1+2+3(i-1)+2+3(\mathfrak{c}-1)(i+1) = jq+3\mathfrak{c}(i+1)-1 = jq+k-1$$

and

$$\begin{aligned} (h_g)_\infty &\leq (3j + 2 + 3 + 3i + 3(\mathfrak{c}-1)(i+1))D_\infty \\ &= (3j + k + 2)D_\infty \\ &\leq (3j + q - 3j - 5 + 2)D_\infty = (q-3)D_\infty, \end{aligned}$$

since in this case $k \leq q-3j-3 \equiv 2 \pmod 3$ and hence, as $k \equiv 0 \pmod 3$, then $k \leq (q-3j-3)-2 = q-3j-5$.

If $k \equiv 0 \pmod 3$ and $j \geq m-1-i$, note that, as $3j \geq q-3i-2$, then $k \leq q-3j-2 \leq q-(q-3i-2)-2 = 3i$ and $\frac{k}{3}-1 \leq i-1$. Hence, we have that

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\frac{k}{3}-1\right) + 2 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j + 3\left(\frac{k}{3}\right)\right) D_\infty \\ &= (3j+k)D_\infty \\ &\leq (3j+q-3j-2)D_\infty = (q-2)D_\infty,\end{aligned}$$

since $k \leq q-3j-2$ in this case.

If $k \equiv 1 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 3\mathfrak{c}(i+1) = jq + k - 1,$$

as $3\left\lfloor \frac{k}{3} \right\rfloor = 3\mathfrak{c}(i+1) = k-1$. Moreover,

$$\begin{aligned}(h_g)_\infty &\leq (3j + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k-1)D_\infty \\ &\leq (3j+q-3j-2-1)D_\infty = (q-3)D_\infty,\end{aligned}$$

since $k \leq q-3j-2$.

If $k \equiv 2 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 1 + 3\mathfrak{c}(i+1) = jq + (k-2) + 1 = jq + k - 1,$$

as $3\left\lfloor \frac{k}{3} \right\rfloor = 3\mathfrak{c}(i+1) = k-2$. Moreover,

$$\begin{aligned}(h_g)_\infty &\leq (3j + 2 + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k)D_\infty \\ &\leq (3j+q-3j-2)D_\infty = (q-2)D_\infty,\end{aligned}$$

since $k \leq q-3j-2$. $\square$

3.7 Final remarks on the Weierstrass places

In this section, we collect a few further facts on the Weierstrass places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$.

From the previous discussion, we have a complete determination of all types of Weierstrass semigroups that occur at the different places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. Here, we start by computing, for places $P \in \mathcal{O}$ or $P_{(a,b)} \in \mathfrak{R}$, how many of them attain a given type of semigroup. To avoid trivial cases, we assume $q \geq 5$.

Remark 3.31. *Henceforth, for simplicity, given a place $P_{(a,b)}$ we will often, with slight abuse of notation, refer to the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$ just as the $\mathcal{P}$-order of $P_{(a,b)}$.*

Theorem 3.32. *The number of distinct Weierstrass semigroups among the places in $\mathcal{O} \cup \mathfrak{R}$ is exactly the same as the number of divisors of m. The semigroups that occur and the places for which they occur are:*

- $H(P) = \langle q-2, q, q+1 \rangle$ *for* $q+1$ *many* $P \in \mathcal{O}$.
- $H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j = 0, \ldots, i-1 \rangle$, *where* $1 \leq i \leq m-2$ *and* $i+1$ *divides* m, *for the* $(q+1)^2\varphi(i+1)$ *many* $P_{(a,b)} \in \mathfrak{R}$ *for which* $\alpha(P_{(a,b)})$ *has* $\mathcal{P}$*-order* i.
- $H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2) \mid j = 0, \ldots, m-2 \rangle$ *for the* $(q+1)^2\varphi(m)$ *many* $P_{(a,b)} \in \mathfrak{R}$ *for which* $\alpha(P_{(a,b)})$ *has* $\mathcal{P}$*-order* $m-1$ *as well as for the* $2m(q+1)$ *many* $P_{(a,b)} \in \mathfrak{R}$ *for which* $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$.

Proof. First of all, Theorems 3.22, 3.25 and 3.27 combined describe all possible Weierstrass semigroups that occur among the places in $\mathcal{O} \cup \mathfrak{R}$. Moreover, Lemma 3.18 implies that the only possible $\mathcal{P}$-orders i for such places correspond to divisors $i+1 \geq 2$ of m. Therefore, the total number of possible Weierstrass semigroups is exactly the number of divisors of m, where the divisor 1 counts the semigroup $\langle q-2, q, q+1 \rangle$.

As for the number of places in $\mathcal{O} \cup \mathfrak{R}$ attaining a particular type of semigroup: we know that $|\mathcal{O}| = q+1$, while Lemma 3.18 implies how many places $P_{(a,b)} \in \mathfrak{R}$ have $\mathcal{P}$-order equal to a given i. The only number of places left to determine is those $P_{(a,b)} \in \mathfrak{R}$ such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$. Using that $\alpha(P_{(a,b)}) = a^m/(1+a^m)$, we see that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$ if and only if $a^{2m} + a^m + 1 = 0$ and $b^{q+1} = -1$. Hence, for exactly $2m(q+1)$ many $P_{(a,b)} \in \mathfrak{R}$ one has $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$. □

Remark 3.33. *It can also be observed that the indicated generators in Theorem 3.32 are in all cases a minimal set of generators. Moreover, by Remark 3.3,*

the cardinality of the set $\mathcal{O} \cup \mathfrak{R}$ is equal to the number of $\mathbb{F}_{q^2}$-rational places of the function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$, that is $q^2 + 1 + 2qg(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = \frac{(q+1)(q^2+q+3)}{3}$, by Theorem 2.10. Then, as a sanity check, note that indeed,

$$q + 1 + \sum_{i=1;i+1|m}^{m-1} (q+1)^2\varphi(i+1) + 2m(q+1) = q^2 + 1 + 2qg(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)),$$

using the equation $\sum_{d|m} \varphi(d) = m$ where the sum is over all divisors of m.

Furthermore, the multiplicity and the conductor of the semigroups are easy to determine, since they can be directly deduced from the knowledge of the Apéry sets, which we have already computed in Remark 3.23, Remark 3.26 and Remark 3.28. In particular, we have already shown that the multiplicity of the semigroups is $q-1$, unless $P \in \mathcal{O}$, in which case it is $q-2$. Moreover, from the definition of Apéry set $A(S)$ (see equation (2.4)) of a semigroup S, it is also immediate to realize that the conductor c of S is simply $c = 1 + \max A(S) - m_S$, where m_S is the multiplicity of S. Therefore, by Remark 3.23, Remark 3.26 and Remark 3.28, we obtain that, for all $P \in \mathcal{O} \cup \mathfrak{R}$, the conductor of $H(P)$ is $2g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

However, note that, in our case, we could have also computed the conductor directly, without knowing the Apéry set, in the following way. Recall that $(q-2)D_\infty$ is a canonical divisor by Lemma 3.9, hence $3D_\infty \sim (q+1)P_{(a,0)}$ by equation (3.13). Moreover, for any $P \in \mathcal{O} \cup \mathfrak{R}$, by the Fundamental Equation we have that $(q+1)P \sim (q+1)P_{(a,0)}$ and hence that $(q-2)mP$ is a canonical divisor. As a consequence, $(q-2)m + 1 = 2g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) - 1$ is a gap and hence $H(P)$ is symmetric. This implies exactly that, for all $P \in \mathcal{O} \cup \mathfrak{R}$, the conductor of $H(P)$ is $2g(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

Proposition 3.34. *Only for $q \in \{2, 5, 8\}$ all the Weierstrass places of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ are precisely those in $\mathcal{O} \cup \mathfrak{R}$.*

Proof. Lemma 3.18 and Theorem 3.30 imply that a Weierstrass place in $\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ exists precisely if there exists i such that $1 \leq i \leq m-2$, $\gcd(i+1, p) = 1$ and $i+1$ does not divide m. Since m has at most $m/3+1$ divisors (not counting m itself) and there are at most $\lfloor m/p \rfloor$ multiples of p between 1 and m, we see that, if $m - 2 > 1 + m/3 + m/p$, then there exists a Weierstrass place in $\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$. Since $p \geq 2$, and $m - 2 > 1 + m/3 + m/2$ if and only if $q > 53$, this already shows that there exists a Weierstrass place not in $\mathcal{O} \cup \mathfrak{R}$ for all $q > 53$. On the other hand, it is immediate to check that at least one i satisfying the conditions exists for $q \in \{11, 17, 23, 29, 32, 41, 47, 53\}$, while no such i exists for $i \in \{2, 5, 8\}$. $\square$

Remark 3.35. *At this point, we are able to determine the number of distinct possible Weierstrass semigroups $H(P)$ as P varies. Indeed, the possible $\mathcal{P}$-orders less than or equal to $m-1$ are simply the number of i between 1 and $m-1$, such that $\gcd(p, i+1) = 1$. Counting the semigroup for $P \in \mathcal{O}$ as well, this gives $m - \lfloor m/p \rfloor$ possible semigroups different from the generic one. The generic semigroup corresponds to those places P of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ whose $\mathcal{P}$-order is at least m. Hence, there are precisely $m - \lfloor m/p \rfloor + 1$ possible semigroups.*

Remark 3.36. *For the places in $\mathcal{O} \cup \mathfrak{R}$, we determined the multiplicity and conductor of the corresponding Weierstrass semigroup. Using Theorem 3.29, we see that, in the generic case, the smallest positive non-gap in $H(P)$ is $q-1$, while the largest gap is $(m-1)q+1$. Hence, in the generic case, the multiplicity is $q-1$ and the conductor $(m-1)q+2$. On the other hand, in the case that $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ has $\mathcal{P}$-order $i \leq m-2$, Theorem 3.30 implies that the largest gap is still $(m-1)q+1$ and therefore that the conductor is $(m-1)q+2$.*

Concerning the places $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ with $\mathcal{P}$-order $i \leq m-2$, the situation for the multiplicity is instead more complicated and we discuss it in the following theorem.

Theorem 3.37. *Let $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$. Then the multiplicity of the semigroup $H(P_{(a,b)})$ is $q-2$ or $q-1$. Moreover, the following are equivalent:*

1. *The multiplicity of $H(P_{(a,b)})$ is $q-2$.*
2. *The $\mathcal{P}$-order i of $\alpha(P_{(a,b)})$ is such that $i+1$ divides $m-1$.*
3. *$\mathcal{P}_{m-1}(\alpha(P_{(a,b)})) = 0$.*
4. *The $\mathbb{F}_{q^2}$-Frobenius of the affine point (a,b), that is $\Phi(a,b) := (a^{q^2}, b^{q^2})$, lies on the tangent line at (a,b) of the plane curve defined by the equation $y^{q+1} + x^{2m} + x^m = 0$.*

Proof. Comparing the gap set in the generic case and the case described in Theorem 3.30, we see that the only difference is that the value of certain gaps is increased by one. Since, in the generic case, $1, \ldots, q-2$ are gaps and $q-1$ is not a gap, this means that the multiplicity of $H(P_{(a,b)})$ for any $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus (\mathcal{O} \cup \mathfrak{R})$ can be either $q-2$ or $q-1$, which proves the first part of the theorem. We now proceed to show the equivalence of the four listed items. For convenience, we write $P = P_{(a,b)}$ and $\alpha = \alpha(P_{(a,b)})$.

(1) $\Rightarrow$ (2) : Assume that $q-2 \in H(P)$ and let i be the $\mathcal{P}$-order of α. Then, according to Theorem 3.30, $q-2$ can be written in the form $(m-2-i-\ell(i+$

$1))q + (\ell+1)(3i+3)$ for some ℓ between 0 and $\lfloor (m-2-i)/(i+1) \rfloor$. Then necessarily $m-2-i-\ell(i+1) = 0$, which is only possible if $\ell = (m-2-i)/(i+1)$ is an integer. Hence $i+1$ divides $m-1$.

(2) $\Rightarrow$ (3) : From the definition of the polynomial $\mathcal{P}_{i+1}(s)$, we see that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{i+1} = 1$. If $i+1$ divides $m-1$, this implies that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{m-1} = 1$, which in turn implies that $\mathcal{P}_{m-1}(\alpha) = 0$.

(3) $\Rightarrow$ (4) : The tangent line ℓ_P of the plane curve $y^{q+1}+x^{2m}+x^m = 0$ at (a,b) is given by the equation $a^{m-1}(2a^m+1)(x-a)+3b^q(y-b) = 0$. Hence $\Phi(a,b)$ lies on ℓ_P if and only if $a^m(2a^m+1)(a^{q^2-1}-1)+3b^{q+1}(b^{q^2-1}-1) = 0$. Using that $b^{q+1} = -a^{2m}-a^m$, we can express all quantities in this equation in terms of a^m and obtain the equivalent equation $a^m((a^m)^{q-1}-1)^2(2(a^m)^q+(a^m)^{q-1}+a^m+2) = 0$. Since $P \notin (\mathcal{O} \cup \mathfrak{R})$, we know in particular that $a^m \notin \mathbb{F}_q$ and hence we conclude that

$$(a^{q^2}, b^{q^2}) \in \ell_P \Longleftrightarrow 2(a^m)^q + (a^m)^{q-1} + a^m + 2 = 0.$$

Using that $a^m = \alpha/(1-\alpha)$, we conclude that

$$(a^{q^2}, b^{q^2}) \in \ell_P \Longleftrightarrow \alpha^{q-1} + (\alpha-1)^{q-1} + 1 = 0. \tag{3.29}$$

Now let us investigate our assumption: $\mathcal{P}_{m-1}(\alpha) = 0$. This implies

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q-2} = 1 \text{ and hence } \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{2},$$

which in turn gives

$$0 = (\alpha+\zeta_3)^q(\alpha+\zeta_3^2)^2-(\alpha+\zeta_3^2)^q(\alpha+\zeta_3)^2 = (\alpha^q+\zeta_3^2)(\alpha+\zeta_3^2)^2-(\alpha^q+\zeta_3)(\alpha+\zeta_3)^2.$$

Multiplying everything out and dividing by $\zeta_3^2-\zeta_3$, we find that

$$0 = 2\alpha^{q+1} - \alpha^q + \alpha^2 - 2\alpha = \alpha(\alpha-1)(\alpha^{q-1} + (\alpha-1)^{q-1} + 1).$$

In light of equation (3.29), we hence obtain that $\Phi(a,b) \in \ell_P$.

(4) $\Rightarrow$ (1) : If $\Phi(a,b) \in \ell_P$, then the function t_P/F_P, see equations (3.8) and (3.17), has a pole of order $q-2$ at $P_{(a,b)}$ and no other poles. Since we have already seen that $H(P)$ has multiplicity $q-1$ or $q-2$, the conclusion is that the multiplicity is $q-2$. □

Remark 3.38. *Let us denote by W_q the total number of Weierstrass places. We have seen that*

$$\begin{aligned} W_q &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2 \left(\sum_{i=0}^{m-1} \varphi(i+1) - \sum_{i=0}^{(m-1)/p-1} \varphi(p\cdot(i+1)) \right) \\ &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2 \left(\sum_{i=1}^{m} \varphi(i) - \sum_{i=1}^{(m-1)/p} \varphi(p\cdot i) \right). \end{aligned}$$

Here the notation $\sum_{i=0}^{\xi}$ *for* $\xi \in \mathbb{R}_{\geq 0}$ *is shorthand for* $\sum_{i=0}^{\lfloor \xi \rfloor}$.

Using iteratively that

$$\sum_{i=1}^{(m-1)/p} \varphi(p \cdot i) = (p-1) \sum_{i=1}^{(m-1)/p} \varphi(i) + \sum_{i=1}^{(m-1)/p^2} \varphi(p \cdot i),$$

we obtain that

$$\sum_{i=1}^{(m-1)/p} \varphi(p \cdot i) = \sum_{e=1}^{\lfloor \log_p(m-1) \rfloor} (p-1) \sum_{i=1}^{(m-1)/p^e} \varphi(i).$$

It is well known, see for example [44, Theorem 330], that $\sum_{i=1}^{N} \varphi(i) = \frac{3}{\pi^2} N^2 + O(N \log(N))$ *asymptotically as* $N \to \infty$.

Hence, we have that

$$\begin{aligned}
\sum_{i=1}^{(m-1)/p} \varphi(p \cdot i) &= \sum_{e=1}^{\lfloor \log_p(m-1) \rfloor} \frac{3(p-1)(m-1)^2}{\pi^2 p^{2e}} + O\left(\sum_{e=1}^{\lfloor \log_p(m-1) \rfloor} \frac{m-1}{p^e} \log_p\left(\frac{m-1}{p^e}\right)\right) \\
&= \frac{3(p-1)(m-1)^2}{\pi^2} \frac{1 - p^2/p^{2\lfloor \log_p(m-1) \rfloor}}{p^2-1} \\
&\qquad + O\left(\int_0^{\log_p(m-1)} \frac{m-1}{p^e} \log_p\left(\frac{m-1}{p^e}\right) de \right) \\
&= \frac{3(m-1)^2}{\pi^2(p+1)} - \frac{3p^2}{\pi^2(p+1)} \left(\frac{m-1}{p^{\lfloor \log_p(m-1) \rfloor}} \right)^2 + O(q \log(q)) \\
&= \frac{3(m-1)^2}{\pi^2(p+1)} + O(q \log(q)).
\end{aligned}$$

Going back to the number of Weierstrass places, we see that

$$\begin{aligned}
W_q &= (q+1)^2 \left(\sum_{i=1}^{m-1} \varphi(i) - \sum_{i=1}^{(m-1)/p} \varphi(p \cdot i) \right) + O(q^2) && (3.30) \\
&= (q+1)^2 \left(\frac{3(m-1)^2}{\pi^2} - \frac{3(m-1)^2}{\pi^2(p+1)} \right) + O(q^3 \log(q)) && (3.31) \\
&= \frac{3(m-1)^2(q+1)^2}{\pi^2} \frac{p}{p+1} + O(q^3 \log(q)) && (3.32) \\
&= \frac{q^4}{3\pi^2} \frac{p}{p+1} + O(q^3 \log(q)). && (3.33)
\end{aligned}$$

Recall now that the number of places in $\mathcal{O} \cup \mathfrak{R}$ *is the same as the number of* $\mathbb{F}_{q^2}$*-rational places of the function field* $\mathbb{F}_{q^2}(\mathcal{X}_3)$ *(see Remark 3.3), which is* $O(q^3)$.

Therefore, equation (3.30) *shows that, for large q, the number of Weierstrass places not in $\mathcal{O}\cup\mathfrak{R}$, vastly outnumbers the number of Weierstrass places contained in such set. In the setting of the function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$, this means that the number of non-rational Weierstrass places is significantly larger than the number of rational places, when q is large.*

3.8 The full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$

Knowing the Weierstrass semigroup at all the places in the set $\mathcal{O}\cup\mathfrak{R}$ allows us, in particular, to determine the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$. Therefore, we devote this section to this aim. As before, $q \equiv 2 \pmod 3$ and we denote by p the characteristic of $\mathbb{F}_{q^2}$. As discussed in Section 3.1, the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ can be seen as a subfield of the Hermitian function field $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, and the extension $\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is an unramified Galois extension of degree 3 (see Remark 3.1 and the preceding discussion). The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_{q^2}(\mathcal{H})/\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is generated by the automorphism τ, defined in equation (3.4), which is a useful observation when constructing automorphisms of the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$.

Indeed, a way to find automorphisms of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is to consider the normalizer $N(\langle\tau\rangle)$ of $\langle\tau\rangle$ in $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{H})) \cong \mathrm{PGU}(3,q)$. Doing so, the group $N(\langle\tau\rangle)/\langle\tau\rangle$ is theoretically guaranteed to be a subgroup of the full automorphism group of the fixed field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ of $\langle\tau\rangle$. The group $N(\langle\tau\rangle)$ in $\mathrm{PGU}(3,q)$ is a well-known maximal subgroup stabilizing a self-polar triangle, see [46, Theorem A.10]. It has order $6(q+1)^2/\gcd(3,q+1) = 2(q+1)^2$ and is isomorphic to the semidirect product of an abelian group of order $(q+1)^2/3$ containing τ and a symmetric group of order 6. This explains the structure of the automorphism group described in Lemma 3.6.

Remark 3.39. *Note that, in our notations from Chapter 2,* $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = \mathrm{Aut}(\mathbb{F}_{q^2}(\mathcal{X}_3))$ *and, since the curve $\mathcal{X}_3$ is defined over $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^2}(\mathcal{X}_3)$ is maximal and of genus at least 2, by [41, Theorem 3.10] it holds that* $\mathrm{Aut}(\mathbb{F}_{q^2}(\mathcal{X}_3)) = \mathrm{Aut}_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}(\mathcal{X}_3))$.

We now begin our study of the group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

Lemma 3.40. *Let $\mathcal{O}$ be the set defined in equation* (3.7)*. Then $\mathcal{O}$ is an orbit of* $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

Proof. Consider the constant field extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(\mathcal{X}_3)$. As noted in Remark 3.39, we have that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = \mathrm{Aut}(\mathbb{F}_{q^2}(\mathcal{X}_3)) = \mathrm{Aut}_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}(\mathcal{X}_3))$

and, by [41, Proposition 3.8, Theorem 3.10], it follows that $\mathrm{Aut}(\mathbb{F}_{q^2}(\mathcal{X}_3))$ acts on the set of $\mathbb{F}_{q^2}$-rational places of $\mathbb{F}_{q^2}(\mathcal{X}_3)$. This means that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ acts on the set $\mathcal{O} \cup \mathfrak{R}$, see Remark 3.2 and Remark 3.3. Let $H(P_{(a,b)})$ and $H(P)$ be the Weierstrass semigroups at a place $P_{(a,b)} \in \mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$ and $P \in \mathcal{O}$, respectively. Since the semigroups $H(P_{(a,b)})$ and $H(P)$ are not the same (see Theorem 3.22, Theorem 3.25 and Theorem 3.27), the automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ acts separately on $\mathcal{O}$ and $\mathbb{P}_{\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)} \setminus \mathcal{O}$. Moreover, since, from Corollary 3.7, the set $\mathcal{O}$ is an orbit of $G \subseteq \mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$, we deduce that $\mathcal{O}$ is also an orbit of the entire $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. □

We now use that $\mathcal{O}$ is an orbit in order to start investigating the p-Sylow subgroups of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$.

Lemma 3.41. *Let $q \geq 11$. Let S_p denote a Sylow subgroup of* $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. *Then $|S_p| < q$.*

Proof. Since S_p acts on $\mathcal{O}$ by Lemma 3.40, we see that S_p has at least one fixed place $P \in \mathcal{O}$. Since $\mathbb{F}_{q^2}(\mathcal{X}_3)$ is maximal, it is a well-known result that it has p-rank zero. This can be seen for instance by [80, Satz 1], as the p-rank and the Hasse-Witt invariant are equivalent notions (see the discussion after [46, Definition 6.97]). Then, by [46, Lemma 11.129], it follows that every nontrivial element of S_p has exactly one fixed place and, more specifically, by [46, Remark 11.128], that all the nontrivial elements of S_p have the same fixed place. This implies that S_p acts with long orbits on $\mathcal{O} \setminus \{P\}$, which in turn implies that $|S_p| \leq q$.

Suppose now that $|S_p| = q$. Observe first that, since $\mathcal{O}$ is an orbit under the action of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$, then, in particular, the stabilizers of the places in $\mathcal{O}$ are all conjugated with respect to this action. Since, by the arguments above, the stabilizer of the place $P \in \mathcal{O}$ contains S_p, this hence implies that the stabilizer of any place $Q \in \mathcal{O} \setminus \{P\}$ contains a Sylow p-subgroup as well, that acts transitively on $\mathcal{O} \setminus \{Q\}$ (as we are assuming that the cardinality of a p-Sylow is q). This implies that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ acts 2-transitively on $\mathcal{O}$, and the stabilizer of two places is cyclic in this action, since it is of order relatively prime to p (see [46, Theorem 11.49]). Hence, from [59, Theorem 1.1], we have that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ has a regular normal subgroup N, unless:

- $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is isomorphic to either $\mathrm{PSL}(2,q)$, $\mathrm{PGL}(2,q)$, or
- $q = \bar{q}^3$ and $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is isomorphic to $\mathrm{PSU}(3,\bar{q})$ or $\mathrm{PGU}(3,\bar{q})$, or
- $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is isomorphic to the Suzuki group $Sz(\bar{q})$, where $q = \bar{q}^2$.

The first two possibilities can be excluded, since in that case $|\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))|$ would not be divisible by $2(q+1)^2$. Furthermore, if $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ was isomorphic to the Suzuki group $Sz(\bar{q})$, then the characteristic would be two and $q = \bar{q}^2$ would be an even power of two. However, this is impossible, since $q \equiv 2 \pmod 3$. This means that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ has a regular normal subgroup N. Then, from [14, Theorem 1.7.6], we see that $|\mathcal{O}| = q+1 = \ell^h$ for some $h \in \mathbb{Z}_{>0}$ and some prime number ℓ. If q is odd, this cannot happen as $q+1$ is divisible by 6. If q is even, we would have $|\mathcal{O}| = q+1 = 2^n+1 = \ell^h$. If $h = 1$, this would mean that ℓ is a Fermat prime, which is only possible if n is a power of two. However, since n is odd, this would imply $n = 1$. This is impossible, since $q \geq 11$. If $h > 1$, then from Catalan's Conjecture (Mihailescu's Theorem [69]), we see that the only possibility is that $\ell = 3$ and $n = 3$. This is again not possible, since we assumed that $q \geq 11$. Hence, we conclude that the only possibility is $|S_p| < q$. □

We now prove a lemma that will allow us to identify certain automorphisms of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$.

Lemma 3.42. *Let $\alpha \in \mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ and suppose that $\alpha(x)$ is a cube, when seen as an element of the function field $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$. Then α can be lifted to an automorphism $\bar{\alpha}$ of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$.*

Proof. Since α is an automorphism of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, we know that

$$\alpha(y)^{q+1} + \alpha(x)^{(q+1)/3} + \alpha(x)^{2(q+1)/3} = 0.$$

Let $\alpha(x) = w^3$, where $w = w(u,v) \in \overline{\mathbb{F}}_{q^2}(\mathcal{H})$, and define $\bar{\alpha}(u) = w$ and $\bar{\alpha}(v) = \frac{\alpha(y)}{\bar{\alpha}(u)}$. Then

$$\begin{aligned}\bar{\alpha}(u)^{q+1} + \bar{\alpha}(v)^{q+1} + 1 &= w^{q+1} + \frac{\alpha(y)^{q+1}}{w^{q+1}} + 1 \\ &= \frac{\alpha(x)^{2(q+1)/3} + \alpha(y)^{q+1} + \alpha(x)^{(q+1)/3}}{w^{q+1}} \\ &= 0.\end{aligned}$$

This means that $\bar{\alpha}$ preserves the defining equation of the Hermitian function field and defines an automorphism of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$. □

Note that, since all automorphisms of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ are defined over $\mathbb{F}_{q^2}$, the automorphism $\bar{\alpha}$ will also be defined over $\mathbb{F}_{q^2}$. Therefore, if $\alpha(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, it was necessarily already a cube in $\mathbb{F}_{q^2}(\mathcal{H})$, see [41, Proposition 3.8, Theorem 3.10].

3.8.1 Case q odd

We start by observing that the case $q = 5$ is already settled. Indeed, if $q = 5$, the plane curve defined by the (affine) equation $X^5 + X = Y^3$ is birationally equivalent to $\mathcal{X}_3$. The corresponding isomorphism of function fields is described as $x = wX + (wX)^{-1}, y = Y/X$, where $w^2 = 2$. This curve is known to have an automorphism group that is isomorphic to a semidirect product of a cyclic group of order 3 with $\mathrm{PGL}(2, 5)$, see [46, Theorem 12.11]. In particular, $|\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))| = 360$ if $q = 5$, which is five times the cardinality of the group of automorphisms G described in Lemma 3.6.

Henceforth, in this subsection, we assume that $q \geq 11$ and that q is odd. Under these assumptions, we wish to use the information that $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ to show that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ actually coincides with the group of automorphisms G determined in Lemma 3.6. To see why this holds, let us first prove, under the aforementioned hypotheses on q, that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is tame, that is, it does not contain any element of order p.

Lemma 3.43. *Let $q \geq 11$ and q odd. Then $|\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))|$ is not divisible by the characteristic p of the field $\mathbb{F}_{q^2}$.*

Proof. Suppose by contradiction that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ admits a Sylow p-subgroup S_p of order p^i for some $i \geq 1$. As we have seen in the proof of Lemma 3.41, we may assume that S_p fixes a place $P_{(a,0)} \in \mathcal{O}_m \subseteq \mathcal{O}$ and that it acts with long orbits on $\mathcal{O} \setminus \{P_{(a,0)}\}$. Furthermore, by Lemma 3.41, we may also assume that $|S_p| < q$.

Recall that the automorphism $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes the set $\mathcal{O}_m$ point-wise, while it acts transitively on the sets $\mathcal{O}_0$ and $\mathcal{O}_\infty$. From this, it follows that σ normalizes S_p (see [46, Theorem 11.49]) and preserves the orbit of S_p containing $\mathcal{O}_m$. We have thus two possibilities for any fixed $P_{(\bar{a},0)} \in \mathcal{O}_m$: either the orbit of S_p containing $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$, or it contains entirely either $\mathcal{O}_0$ or $\mathcal{O}_\infty$. In the second case, we would get that $|S_p| \geq (q+1)/3+1$ and hence $|S_p| = q$, which is not possible. Therefore, we can deduce that, for any place $P_{(\bar{a},0)} \in \mathcal{O}_m$, the S_p-orbit of $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$. Since S_p acts on $\mathcal{O} = \mathcal{O}_m \cup \mathcal{O}_0 \cup \mathcal{O}_\infty$, S_p must then act with long orbits on $\mathcal{O}_0 \cup \mathcal{O}_\infty$, which is a set of cardinality $2(q+1)/3$. We hence obtain the desired contradiction, as $2(q+1)/3$ is not divisible by p. □

Theorem 3.44. *Let $q \geq 11$, q odd. Then $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = G$, where G is the group of automorphisms described in Lemma 3.6.*

Proof. Suppose by contradiction that $|\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))| > |G|$. Let $G_{P_{(a,0)}}$ be

the stabilizer in G of a place $P_{(a,0)} \in \mathcal{O}_m \subseteq \mathcal{O}$. Since, by the orbit-stabilizer theorem, $|G| = |\mathcal{O}||G_{P_{(a,0)}}|$ and, by Lemma 3.40, $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$, the stabilizer $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))_{P_{(a,0)}}$ of $P_{(a,0)}$ in $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ contains some extra automorphism $\gamma \notin G_{P_{(a,0)}}$. Let C_{q+1} be the cyclic group generated by $\sigma : (x, y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity. Then, since $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))_{P_{(a,0)}}$ is cyclic (as follows by [46, Theorem 11.49], from the fact that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is of order relatively prime to p), γ commutes with C_{q+1} and hence it acts on the places that C_{q+1} fixes (and, in general, on its orbits). This means that γ acts on the sets $\mathcal{O}_m$ and $\mathcal{O}_0 \cup \mathcal{O}_\infty$, because the set $\mathcal{O}_m$ is exactly the set of all the places fixed by C_{q+1}. Since $\mathcal{O}_0$ and $\mathcal{O}_\infty$ are orbits of C_{q+1} of the same length, then either γ fixes both $\mathcal{O}_0$ and $\mathcal{O}_\infty$, or it interchanges them.

If γ fixes both $\mathcal{O}_0$ and $\mathcal{O}_\infty$, then it fixes the divisor of x from equation (3.14). This means that $\gamma(x) = \lambda x$, for some constant $\lambda \in \overline{\mathbb{F}}_{q^2}^*$. Hence, $\gamma(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, as $x = u^3$ and λ is a constant. Suppose instead that γ interchanges $\mathcal{O}_0$ and $\mathcal{O}_\infty$. Then, γ maps the divisor of x to the divisor of $1/x$, meaning that there exists a constant λ such that $\gamma(x) = \lambda/x$. Hence, in all cases $\alpha(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$.

From Lemma 3.42, γ can hence be lifted to an automorphism $\bar{\gamma}$ of $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ acting on the set of $3(q+1)$ places lying over those in $\mathcal{O}$. These places are the zeros of three functions, in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, that geometrically correspond to three lines intersecting each other in three points outside the Hermitian curve $\mathcal{H}$, that is, a self-polar triangle. Since this shows that γ is induced by $N(\langle\sigma\rangle)$, we hence have that $\gamma \in G$, which gives a contradiction.

□

3.8.2 Case q even

We now turn our attention to the case where q is even, that is to say when $q = 2^n$, n odd. If $q = 2$, the function field $\overline{\mathbb{F}}_4(\mathcal{X}_3)$ is isomorphic to the Hermitian function field $\overline{\mathbb{F}}_4(\mathcal{H})$ and therefore has $\mathrm{PGU}(3, 2)$ as automorphism group, which contains 216 elements. Note that here only automorphisms defined over $\mathbb{F}_{q^2}$ were considered, hence, in this case, there are twelve times more automorphisms than described in Lemma 3.6. If $q = 8$, the automorphism group of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is also known, as in this case $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ is isomorphic to the Giulietti-Korchmáros maximal function field, see [33]. This function field can for example be regarded as the function field of the plane curve with affine equation $Y^9 = (X^2+X)(X^2+X+1)^3$. An explicit isomorphism on the level of function fields is then given by $X = \zeta_3 + (x^5 + x^4 + x^3)/y^9$ and $Y = (x^5 + x^4 + x^3)/y^8$.

Hence, for $q = 8$, the automorphism group of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is a semidirect product of a cyclic group of order 3 and $\mathrm{PGU}(3,2)$, resulting in 648 automorphisms, four times more than those contained in the group from Lemma 3.6.

For the remainder of this subsection, we will assume that $q = 2^n$, $n \geq 5$ odd. We will show that, in this case, the automorphism group of $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ coincides with the group G from Lemma 3.6. To this aim, a similar argument as in the previous subsection will be provided. Of course, in this case, we cannot prove that $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ is tame, as G itself is nontame. We will in fact first prove that, if a Sylow 2-subgroup of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ has order larger than 2, then its cardinality must be $q/2$.

Lemma 3.45. *Let $n \geq 5$ and $q = 2^n$. Let also S_2 denote a Sylow 2-subgroup of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. Then, either $|S_2| = 2$ or $|S_2| = q/2$. In the latter case, a 2-Sylow S_2 fixing a place $P_{(a,0)} \in \mathcal{O}_m$ acts on $\mathcal{O}$ with the following 3 orbits:*

- $\{P_{(a,0)}\}$,
- $\mathcal{O}_1^{S_2} := \mathcal{O}_0 \cup \{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$,
- $\mathcal{O}_2^{S_2} := \mathcal{O}_\infty \cup \{P_{(\gamma_1,0)}, \ldots, P_{(\gamma_{(q-2)/6},0)}\}$,

where $\{P_{(a,0)}\}$, $\{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$ and $\{P_{(\gamma_1,0)}, \ldots, P_{(\gamma_{(q-2)/6},0)}\}$ is a suitably chosen partition of $\mathcal{O}_m$.

Proof. Let S_2 be of order 2^i for some $i \geq 1$. Just as in the proof of Lemma 3.43, we may assume that S_2 fixes a place $P_{(a,0)} \in \mathcal{O}_m \subseteq \mathcal{O}$ and that it acts with long orbits on $\mathcal{O} \setminus \{P_{(a,0)}\}$. Furthermore, by Lemma 3.41, we may also assume that $|S_2| < q$.

Recall that the automorphism $\sigma : (x, y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes $P_{(a,0)}$ and hence normalizes S_2, from [46, Theorem 11.49]. Moreover, σ fixes the set $\mathcal{O}_m$ element-wise, while it acts transitively on $\mathcal{O}_0$ and $\mathcal{O}_\infty$. This means that, for any $P_{(\bar{a},0)} \in \mathcal{O}_m$, σ preserves the orbit of S_2 containing $P_{(\bar{a},0)}$. We have thus two possibilities for a fixed place $P_{(\bar{a},0)}$: either the orbit of S_2 containing $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$, or it contains entirely either $\mathcal{O}_0$ or $\mathcal{O}_\infty$.

If the second case never occurs, then S_2 acts semiregularly (i.e., all the orbits of the action are long orbits) on $\mathcal{O}_0 \cup \mathcal{O}_\infty$, which is a set of cardinality $2(q+1)/3$. This implies that $|S_2| = 2$. If, instead, the second case occurs for some $P_{(\bar{a},0)}$, then we get that $|S_2| \geq (q+1)/3 + 1 > q/4$ and hence $|S_2| = q/2$. Note that, in

this case, the only possible configuration of orbits of S_2 acting on the q places in $\mathcal{O} \setminus \{P_{(a,0)}\}$ is that S_2 has exactly 2 orbits of length $q/2$: one $\mathcal{O}_1^{S_2}$ containing $\mathcal{O}_0$ and $(q-2)/6$ places in $\mathcal{O}_m$, and another one $\mathcal{O}_2^{S_2}$ containing $\mathcal{O}_\infty$ and the remaining $(q-2)/6$ places in $\mathcal{O}_m$. □

We now exclude the second case in Lemma 3.45.

Lemma 3.46. *The case $|S_2| = q/2$ cannot occur.*

Proof. Suppose by contradiction $|S_2| = q/2$. With notations as in Lemma 3.45, we can assume that S_2 acts on $\mathcal{O}$ with three orbits $\{P_{(a,0)}\}$, $\mathcal{O}_1^{S_2}$ and $\mathcal{O}_2^{S_2}$. The cyclic group C_{q+1}, generated by $\sigma : (x, y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes any place in $\mathcal{O}_m$, in particular $P_{(a,0)}$, and hence normalizes S_2. In particular, the group generated by σ and the elements of S_2 has $|S_2|(q+1)$ many elements. Since the stabilizer of two places is tame and cyclic (see [46, Theorem 11.49]), we conclude that C_{q+1} is the stabilizer of two places, the place $P_{(a,0)}$ and any other place in $\mathcal{O}_m$.

Using the notations from Lemma 3.45, choose $\gamma \in S_2$ to be such that $\gamma(P_{(\beta_1,0)}) = P_{(\beta_2,0)}$, with $P_{(\beta_1,0)}, P_{(\beta_2,0)} \in \mathcal{O}_1^{S_2}$ distinct places. Such a γ exists, since $P_{(\beta_1,0)}$ and $P_{(\beta_2,0)}$ are in the same orbit under the action of S_2. Then, $\gamma^{-1} \cdot \sigma \cdot \gamma$ fixes $P_{(a,0)}$ and

$$\gamma^{-1} \cdot \sigma \cdot \gamma(P_{(\beta_1,0)}) = \gamma^{-1} \cdot \sigma(P_{(\beta_2,0)}) = \gamma^{-1}(P_{(\beta_2,0)}) = P_{(\beta_1,0)}.$$

Hence, $\gamma^{-1} \cdot \sigma \cdot \gamma$ is an element of order $q+1$ fixing both $P_{(a,0)}$ and $P_{(\beta_1,0)}$. This implies that $\gamma^{-1} \cdot \sigma \cdot \gamma \in C_{q+1}$ and, more specifically, that $\gamma^{-1} \cdot \sigma \cdot \gamma = \sigma^k$, where $(k, q+1) = 1$. Moreover, since C_{q+1} normalizes S_2, there exists $\tilde{\gamma} \in S_2$ such that $\sigma \cdot \gamma = \tilde{\gamma} \cdot \sigma$. Therefore,

$$\mathrm{id} = \gamma^{-1} \cdot \sigma \cdot \gamma \cdot \sigma^{-k} = \gamma^{-1}\tilde{\gamma} \cdot \sigma^{1-k}.$$

Since $S_2 \cap C_{q+1} = \{\mathrm{id}\}$, this implies that $k = 1$ and hence that γ and σ commute.

Now let ι be a suitable power of γ such that ι has order two. Then, for any $P_{(\beta_j,0)} \in \mathcal{O}_1^{S_2}$, we have that $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2}$, since S_2 acts on $\mathcal{O}_1^{S_2}$. On the other hand, using that σ and ι commute and that σ fixes all the places in $\mathcal{O}_m$, we have that $\sigma \cdot \iota(P_{(\beta_j,0)}) = \iota \cdot \sigma(P_{(\beta_j,0)}) = \iota(P_{(\beta_j,0)})$. Hence, $\iota(P_{(\beta_j,0)})$ is a place fixed by σ, which implies that $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_m$. We conclude that $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2} \cap \mathcal{O}_m = \{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$. In other words, this means that ι acts on the set $\{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$. Since $(q-2)/6 = (q/2-1)/3$ is an odd number, this implies that, apart from $P_{(a,0)}$, ι fixes at least one more place. However, since the characteristic is two and $\mathbb{F}_{q^2}(\mathcal{X}_3)$ is maximal and hence has 2-rank zero, this is impossible according to [46, Lemma 11.129]. □

We are now ready to compute $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ when q is even.

Theorem 3.47. *Let $q = 2^n$, $n \geq 5$ odd. Then* $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)) = G$.

Proof. Combining Lemma 3.45 and Lemma 3.46, we conclude that $|S_2| = 2$. Suppose now, by contradiction, that $|\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))| > |G|$. Let $G_{P_{(a,0)}}$ be the stabilizer in G of $P_{(a,0)} \in \mathcal{O}_m \subseteq \mathcal{O}$. Since, by the orbit-stabilizer theorem, $|G| = |\mathcal{O}||G_{P_{(a,0)}}|$ and, by Lemma 3.40, $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$, the stabilizer $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))_{P_{(a,0)}}$ of $P_{(a,0)}$ in $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ contains some extra automorphism $\gamma \notin G_{P_{(a,0)}}$. Also, since $|S_2| = 2$ and $|G| = 2(q+1)^2$, γ can be assumed to be of odd order.

Let C_{q+1} be the cyclic group generated by $\sigma : (x, y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity. Then, since the tame part of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))_{P_{(a,0)}}$ is cyclic (see [46, Theorem 11.49]), γ commutes with C_{q+1} and hence it acts on the places that are fixed by C_{q+1} (and, in general, on its orbits). At this point, the remainder of the proof is then exactly the same as the proof of Theorem 3.44. $\square$

Chapter 4

Two-point Weierstrass semigroups and AG codes

This chapter is devoted to the study of two-point AG codes from two different families of maximal function fields. Since a fundamental tool for the investigation of such codes are certain two-point Weierstrass semigroups, a consistent part of the chapter is dedicated to a thorough study of these algebraic objects. The results included in Section 4.1 are contained in [65] and were jointly developed by L. Landi and the author of this thesis. Those contained in Section 4.2 were instead presented in [64] and were obtained by L. Landi, M. Timpanella and the author of this thesis in a joint collaboration.

Starting from the description of the Weierstrass semigroup at a place discussed in Section 2.1 (see Definition 2.15), it appears natural to investigate the more general case in which multiple places are considered. With this regard, a generalization of Weierstrass semigroups to the case of more than one place first appeared in [3, p. 365]. Given a function field F, the Weierstrass semigroup at an n-tuple of rational places $P_1, \ldots, P_n \in \mathbb{P}_F$ was defined as

$$\tilde{H}(P_1, \ldots, P_n) := \{(k_1, \ldots, k_n) \in \mathbb{N}^n \mid \exists\, f \in F \text{ with } (f)_\infty = k_1 P_1 + \cdots + k_n P_n\}.$$

Since its definition, this generalization of the Weierstrass semigroup has been extensively studied in the literature. Some of its arithmetical and geometrical properties have been studied in [19], [4] and [57], and for small values of n some

specific cases have been explicitly investigated in [60], [48], [61] (case $n = 2$) and in [58] (case $n = 4$).

In the case $n = 2$, the connections with two-point AG codes have also been studied, for instance in [50], [67], [68], [51], [52] and [15]. The knowledge of $\tilde{H}(Q, P)$ is indeed crucial for the study of two-point codes, since it can be used for obtaining good bounds for their minimum distance, as done in [67, Theorem 2.1] and [50, Theorem 3.3]. With respect to this application, a tool that turned out to be particularly important is a bijective function between the set of gaps at a place Q and the set of gaps at another place P, that was introduced by S.J. Kim in [60]. The function introduced in this paper is

$$\begin{aligned} \sigma : \ G(Q) &\longrightarrow G(P) \\ i \quad &\longmapsto \min\{j \mid (i,j) \in \tilde{H}(Q,P)\} \end{aligned} \tag{4.1}$$

and it is closely connected to the determination of the semigroup $\tilde{H}(Q, P)$, as pointed out in [50].

In this spirit, P. Beelen and N. Tutaş introduced in [13] a different generalization of Weierstrass semigroups. In the above notations, they defined

$$H(P_1, \ldots, P_n) := \{(k_1, \ldots, k_n) \in \mathbb{Z}^n \mid \exists\, f \in \mathcal{R}(P_1, \ldots, P_n) \backslash \{0\}, v_{P_i}(f) = -k_i \ \forall\, i\},$$

where $\mathcal{R}(P_1, \ldots, P_n) := \{f \in F \mid v_R(f) \geq 0 \ \forall R \neq P_1, \ldots, P_n\}$. This definition has the advantage of allowing, in a natural way, the generalization of the function σ to a bijective function from $\mathbb{Z}$ to $\mathbb{Z}$. Indeed, as discussed in Section 2.4, one can define the function

$$\begin{aligned} \tau_{Q,P} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ i \ &\longmapsto \min\{j \mid (i,j) \in H(Q,P)\}, \end{aligned}$$

which by [13, Proposition 14] is bijective and has many further remarkable properties, as observed in Proposition 2.36.

Moreover, this generalization also turned out to be interesting for the study of two-point AG codes. Indeed, in [8] P. Beelen introduced a generalization of the Feng-Rao bound (see the *generalized order bound* defined in Definition 2.41 and Proposition 2.43) that gives good estimates for the minimum distance of AG codes with the support of the divisor G consisting of multiple places. In the case of two-point codes, the knowledge of the function $\tau_{Q,P}$ plays a fundamental role in the computation of this bound and allows to determine effectively the dimension of the codes, see Theorem 2.46 and Corollary 2.47. This has been pointed out in [5], where this second generalization of Weierstrass semigroups and the generalized order bound were used in order to study two-point AG codes

from the Garcia-Güneri-Stichtenoth function fields [30]. Such codes have been found to have excellent parameters.

In this chapter, we use the approach introduced in [5] in order to study two-point AG codes from two different families of maximal function fields, the Beelen-Montanucci function fields [10] and the Skabelund function field [79] obtained as a cyclic extension of the Suzuki function field. In Section 2.4 and Section 2.5, we have already thoroughly discussed the definitions and the essential results from [13] and [8] that we need.

The chapter is divided into two sections. In Section 4.1, we investigate two-point AG codes from the Beelen-Montanucci function fields $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, for all $n \geq 3$ odd, comparing our results with those obtained in [5] from the Garcia-Güneri-Stichtenoth function fields $\mathbb{F}_{q^{2n}}(\mathcal{GGS}_n)$. In Section 4.2, we study instead two-point codes from the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$. We observe that, for all the two-point codes considered from such function field, the minimum distance is always at least that of a one-point code of the same length and dimension.

4.1 The case of the Beelen-Montanucci function fields

Let q be a prime power, $n \geq 3$ be an odd integer and $m := (q^n + 1)/(q + 1)$. We start by recalling some context on the Beelen-Montanucci function fields.

In [33], M. Giulietti and G. Korchmáros constructed a maximal function field that, for $q > 2$, is not a subfield of the Hermitian one. This function field is the $\mathbb{F}_{q^6}$-rational function field of the curve

$$\mathcal{GK} : \begin{cases} y^{q+1} = x^q + x, \\ z^{q^2-q+1} = y\frac{x^{q^2}-x}{x^q+x}. \end{cases}$$

A first generalization of $\mathbb{F}_{q^6}(\mathcal{GK})$ to an infinite family of $\mathbb{F}_{q^{2n}}$-maximal function fields, for $n \geq 3$ an odd integer, was given by A. Garcia, C. Güneri and H. Stichtenoth in [30], where they constructed such a family as the $\mathbb{F}_{q^{2n}}$-rational function fields of the so-called $\mathcal{GGS}_n$ curves. These curves are defined over $\mathbb{F}_{q^{2n}}$ by the affine equations

$$\mathcal{GGS}_n : \begin{cases} y^{q+1} = x^q + x, \\ z^m = y\frac{x^{q^2}-x}{x^q+x}, \end{cases}$$

and in [30] it was shown that, for $n = 3$, the function field $\mathbb{F}_{q^{2n}}(\mathcal{GGS}_n)$ is precisely $\mathbb{F}_{q^6}(\mathcal{GK})$.

Another generalization of $\mathbb{F}_{q^6}(\mathcal{GK})$ was subsequently introduced by P. Beelen and M. Montanucci in [10]. For $n \geq 3$ odd, the Beelen-Montanucci function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is the $\mathbb{F}_{q^{2n}}$-rational function field of the curve

$$\mathcal{BM}_n : \begin{cases} y^{q+1} = x^{q+1} - 1, \\ z^m = y\frac{x^{q^2}-x}{x^{q+1}-1}. \end{cases} \tag{4.2}$$

The function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is maximal and for $n = 3$ it is isomorphic to $\mathbb{F}_{q^{2n}}(\mathcal{GGS}_n)$ and, equivalently, to $\mathbb{F}_{q^6}(\mathcal{GK})$. Furthermore, in [10] it is also proved that $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is isomorphic to $\mathbb{F}_{q^{2n}}(\mathcal{GGS}_n)$ if and only if $n = 3$.

For $n \geq 3$ an odd integer, consider the $\mathbb{F}_{q^{2n}}$-model of the Hermitian curve (see equation (3.3)) given by

$$\tilde{\mathcal{H}} : y^{q+1} = x^{q+1} - 1,$$

whose $\mathbb{F}_{q^{2n}}$-rational function field we denote by $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$. We collect some generalities on $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ and on the extension $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)/\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.

Let $s := \frac{y}{x}$, so that $s^{q+1} = 1 - \frac{1}{x^{q+1}}$ and the function field $\mathbb{F}_{q^{2n}}(s, x) = \mathbb{F}_{q^{2n}}(x, y) = \mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$. Denote by $\overline{P}$ the pole of x in $\mathbb{F}_{q^{2n}}(x)$ and with $\rho(T) := T^{q+1} + \frac{1}{x^{q+1}} - 1$ the minimal polynomial of s over $\mathbb{F}_{q^{2n}}(x)$. Then

$$\bar{\rho}(T) := T^{q+1} - 1 \in \mathbb{F}_{q^{2n}}[T]$$

is the polynomial whose coefficients are the residue classes in $\mathrm{O}_{\overline{P}}/\overline{P}$ of the coefficients of $\rho(T)$, and its decomposition into irreducible factors over $\mathrm{O}_{\overline{P}}/\overline{P}$ is

$$\bar{\rho}(T) = \prod_{i=1}^{q+1}(T - \xi^i),$$

where ξ is a primitive $(q+1)$-th root of unity in $\mathbb{F}_{q^{2n}}$. Hence, by Theorem 2.19, we have that for each $i = 1, \ldots, q+1$ there exists a unique place $P_{(\infty,\xi^i)} \in \mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ such that $P_{(\infty,\xi^i)}|\overline{P}$ and $s - \xi^i \in P_{(\infty,\xi^i)}$. Moreover, it holds that

$$e(P_{(\infty,\xi^i)}|\overline{P}) = 1$$

for all $i = 1, \ldots, q+1$. This means that, for all $i = 1, \ldots, q+1$, the functions $1/x$ and $s - \xi^i$ in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ have only one common zero, namely the place $P_{(\infty,\xi^i)}$. For more convenient notations:

- if q is even, we set $\overline{P}_i := P_{(\infty,\xi^{i-1})}$, for $i = 1, \ldots, q+1$,

- if q is odd, we set instead $\overline{P}_i := P_{(\infty,\xi^{\frac{q+1}{2}+(i-1)})}$, for $i = 1, \dots, q+1$.

We make this choice so that, in both cases, the place $\overline{P}_1$ denotes precisely the only common zero of the functions $1/x$ and $x+y$ in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.

Note that the places $\overline{P}_1, \dots, \overline{P}_{q+1}$ are exactly the poles of x in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$. Moreover, it is not difficult to see that these places are totally ramified in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)/\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$, as the extension is Kummer of degree m. We denote by P_i the place of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ lying over $\overline{P}_i$, for every $i = 1, \dots, q+1$, and set

$$O_1 := \{P_1, \dots, P_{q+1}\}.$$

Consider now $a \in \mathbb{F}^*_{q^{2n}}$ and let $\overline{Q}_a$ be the place that is the zero of the function $x - a$ in $\mathbb{F}_{q^{2n}}(x)$. Since $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})/\mathbb{F}_{q^{2n}}(x)$ is a Kummer extension of degree $q+1$ (see Corollary 2.26), by Proposition 2.25 we directly have that

- if $a^{q+1} - 1 = 0$, then there exists a unique place $\overline{Q}_{(a,0)}$ of $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ such that
$$\overline{Q}_{(a,0)} | \overline{Q}_a, \quad e(\overline{Q}_{(a,0)} | \overline{Q}_a) = q+1 \quad \text{and} \quad y \in \overline{Q}_{(a,0)}.$$
This place is the only common zero of the functions $x - a$ and y in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.
- If instead $a^{q+1} - 1 \neq 0$, then $\overline{Q}_a$ splits completely in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})/\mathbb{F}_{q^{2n}}(x)$, that is, for each $i = 1, \dots, q+1$, there exists a place $\overline{Q}_{(a,b\xi^i)}$ of $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ such that
$$\overline{Q}_{(a,b\xi^i)} | \overline{Q}_a, \quad e(\overline{Q}_{(a,b\xi^i)} | \overline{Q}_a) = 1 \quad \text{and} \quad y - b\xi^i \in \overline{Q}_{(a,b\xi^i)},$$
where $b \in \mathbb{F}^*_{q^{2n}}$ satisfies $b^{q+1} = a^{q+1} - 1$ and $\xi \in \mathbb{F}_{q^{2n}}$ is a primitive $q+1$-th root of unity.

All the places $\overline{Q}_{(a,0)}$ and $\overline{Q}_{(a,b\xi^i)}$ are totally ramified in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)/\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$, since the extension is Kummer of degree m. We denote by

$$O_2 := \{Q_1, \dots, Q_{q^3-q}\} \subseteq \mathbb{P}_{\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)}$$

the set of extensions of these places in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$. For convenience of notations, as it will be clear in the subsequent discussion, for all $a \in \mathbb{F}^*_{q^{2n}}$ with $a^{q+1} - 1 = 0$ we set $Q_a \in O_2$ to denote the place lying over $\overline{Q}_{(a,0)}$.

Remark 4.1. *Observe that, with this choice of notations, P_1 denotes the common zero of the functions $1/x$ and $x+y$ in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, while Q_1 denotes the common zero of the functions $x-1$ and y in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$.*

We now recall, in the following proposition, some of the main properties of the function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, which will be useful throughout the section.

Proposition 4.2. *Let q be a prime power, $n \geq 3$ an odd integer and $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ the corresponding Beelen-Montanucci function field. Moreover, with notations as above, consider the function field $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.*

1. *The function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is maximal and has genus*

$$g(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)) = \frac{1}{2}(q-1)(q^{n+1}+q^n-q^2)$$

   and

$$N_n := q^{2n+2} - q^{n+3} + q^{n+2} + 1$$

   $\mathbb{F}_{q^{2n}}$-rational places.

2. *The full automorphism group $\mathrm{Aut}(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$ is isomorphic to $\mathrm{SL}(2,q) \rtimes C_{q^n+1}$, where C_{q^n+1} is the cyclic group with q^n+1 elements, and the sets O_1 and O_2 are separate orbits in its action on the places of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$.*

Remark 4.3. *From a geometrical point of view, for every $i = 1, \ldots, q+1$, the place P_i in O_1 is centered at the point at infinity of $\mathcal{BM}_n$ that can be parametrized in homogeneous $[x : y : z : w]$-coordinates as $[1 : a_i : 0 : 0]$, with $a_i^{q+1} = 1$, $a_1 = -1$. On the other hand, for every $a \in \mathbb{F}_{q^{2n}}^*$ with $a^{q+1} - 1 = 0$, the place Q_a in O_2 is centered at the affine point of $\mathcal{BM}_n$ with homogeneous $[x : y : z : w]$-coordinates $[a : 0 : 0 : 1]$.*

Let now $M := (m-1)/(q^2-q)$. From [70, Theorem 1.1], the Weierstrass semigroup $H(P)$ at any place $P \in O_1$ is

$$H(P) = \langle q^n+1, mq + k(q^2-q) \mid k = 0, \ldots, M \rangle \tag{4.3}$$

and the Weierstrass semigroup $H(Q)$ at any place $Q \in O_2$ is

$$H(Q) = \langle q^n+1-m, q^n+1-k \mid k = 0, \ldots, M \rangle. \tag{4.4}$$

Since the Weierstrass semigroup at any place is invariant under the action of the automorphism group $\mathrm{Aut}(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$ on that place (see for example [81, Lemma 3.5.2]), places in the same orbit have the same Weierstrass semigroup. With notations as above, in the following discussion we will choose the places P_1 and Q_1 as representatives of the orbits O_1 and O_2, respectively.

Remark 4.4. *For any $i = 1, \ldots, q+1$, the stabilizer $\mathcal{S}_i$ of a place $\overline{P}_i \in \mathbb{P}_{\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})}$, under the action of $\mathrm{PGU}(3,q)$, contains a subgroup of cardinality*

$q(q-1)(q+1)$ that is isomorphic to the group $SL(2,q)$. As shown in [16, Lemma 3.1], this subgroup acts sharply transitively on the set of the remaining q^3-q places of $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ lying under the places in O_2, and it is lifted completely in $\mathrm{Aut}(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$, i.e., each of its elements can be extended in precisely m distinct ways to an automorphism of $\mathrm{Aut}(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$ (see Theorem 2.5 and the results in Section 4 of [10]). Therefore, the stabilizer of a place $P_i \in \mathbb{P}_{\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)}$ contains a subgroup isomorphic to $SL(2,q)$ and acting transitively on O_2. This implies that, for any choice of $P_i, P_j \in O_1$ and $Q_h, Q_k \in O_2$, there exists $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$ such that $\sigma(P_i) = P_j$ and $\sigma(Q_h) = Q_k$.

We now recall some functions in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ and their principal divisors, that will be useful in the discussion. Let

$$\alpha := \frac{x-1}{x+y} \quad \text{and} \quad \theta_k := \frac{z^k}{x+y}$$

for $k = 0, \ldots, M$. From [70, Lemmas 3.1, 3.3]:

$$(x+y) = mqP_1 - m\sum_{i=2}^{q+1} P_i, \tag{4.5}$$

$$(\alpha) = (q^n+1)(Q_1 - P_1), \tag{4.6}$$

$$(\theta_k) = k\sum_{i=1}^{q^3-q} Q_i + (m - k(q^2-q))\sum_{i=2}^{q+1} P_i - (mq + k(q^2-q))P_1. \tag{4.7}$$

Lemma 4.5. *Let $\tilde{\theta}_0 := \theta_0 - 1$. The principal divisor of $\tilde{\theta}_0$ in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is $(\tilde{\theta}_0) = mQ_1 + E - mqP_1$, where E is an effective divisor whose support does not contain Q_1 and P_1.*

Proof. Define $t := x+y-1$, so that $\tilde{\theta}_0 = -t/(x+y)$ and $\tilde{\theta}_0$ has principal divisor $(\tilde{\theta}_0) = (t) - (x+y)$. With the notations defined before Proposition 4.2, let $\overline{P}_1, \ldots, \overline{P}_{q+1}$ be the $q+1$ distinct poles of x in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ and, for $i = 1, \ldots, q+1$, let P_i be the unique place of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ lying over $\overline{P}_i$.

Since we already know the divisor of $x+y$ in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ (see equation (4.5)), in order to compute the divisor of $\tilde{\theta}_0$ we only need to determine the divisor of t in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$. We do this by determining the divisor of t in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ and then lifting it to $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$.

We start by noting that the pole divisor of t is the same as the pole divisor of $x+y$ in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$, which by equation (4.5) and the discussion above we already know to be $\sum_{i=2}^{q+1} \overline{P}_i$. Since the degree of this divisor is q, we deduce that t has at most q distinct zeros in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.

Furthermore, for $b \in \mathbb{F}_{q^{2n}}$, consider the function $x-(1-b)$ in $\mathbb{F}_{q^{2n}}(x)$ and let $\overline{Q}_{1-b}$ be the zero of this function in $\mathbb{F}_{q^{2n}}(x)$. We start by observing that the common zeros of $x-(1-b)$ and $y-b$ in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ are also zeros of t, since $x-(1-b)+y-b = x+y-1$. Therefore, in order to compute the principal divisor of t, we start by determining the common zeros of the functions $x-(1-b)$ and $y-b$.

Note that, since $b^{q+1}-(1-b)^{q+1}+1=0$ if and only if $b^q+b=0$, it is only meaningful to study the common zeros of the functions $x-(1-b)$ and $y-b$ for $b \in \mathbb{F}_{q^{2n}}$ such that $b^q+b=0$ (every such b is in fact an element of $\mathbb{F}_{q^2}$), as otherwise such functions would have no zeros in common in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.

If $b=0$, observe that $x-(1-b)=x-1$ and $y-b=y$ and hence, with notations as in the discussion before Remark 4.1, $\overline{Q}_{1-b}=\overline{Q}_1$ and $\overline{Q}_{(1,0)}$ is the only common zero of $x-1$ and y in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$.

On the other hand, if $b \neq 0$, we let $\rho(T) := T^{q+1}-x^{q+1}+1$ be the minimal polynomial of y over $\mathbb{F}_{q^{2n}}(x)$ and

$$\bar{\rho}(T) := T^{q+1}-(1-b)^{q+1}+1 = T^{q+1}-b^{q+1} \in \mathbb{F}_{q^{2n}}[T]$$

be the polynomial whose coefficients are the residue classes in $\mathrm{O}_{\overline{Q}_{1-b}}/\overline{Q}_{1-b}$ of the coefficients of $\rho(T)$. The decomposition of $\bar{\rho}(T)$ into irreducible factors over $\mathbb{F}_{q^{2n}}$ is

$$\bar{\rho}(T) = \prod_{i=0}^{q}(T-b\xi^i),$$

where ξ is a primitive $(q+1)$-th root of unity in $\mathbb{F}_{q^{2n}}$. Therefore, by Theorem 2.19, we have that there exists exactly one place $\overline{Q}_{(1-b,b\xi^i)} \in \mathbb{P}_{\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})}$ such that

$$\overline{Q}_{(1-b,b\xi^i)}|\overline{Q}_{1-b}, \quad y-b\xi^i \in \overline{Q}_{(1-b,b\xi^i)} \quad \text{and} \quad e(\overline{Q}_{(1-b,b\xi^i)}|\overline{Q}_{1-b})=1,$$

for each $i=0,\dots,q$.

Since $y-b\xi^i = y-b$ for $i=0$, we hence conclude that, for each $b \in \mathbb{F}_{q^2}$ satisfying $b^q+b=0$, the functions $x-(1-b)$ and $y-b$ have exactly one zero in common in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$, namely the place $\overline{Q}_{(1-b,b)}$. From what observed above, this implies that the q distinct places $\overline{Q}_{(1-b,b)}$, for $b \in \mathbb{F}_{q^2}$, $b^q+b=0$, are zeros of the function t in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$. Since we already noted that the pole divisor of t in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ is $\sum_{i=2}^{q+1}\overline{P}_i$, this means that the places $\overline{Q}_{(1-b,b)}$ are in fact all the zeros of t in $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ and therefore

$$(t)_{\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})} = \sum_{\substack{b\in\mathbb{F}_{q^2}\\ b^q+b=0}} \overline{Q}_{(1-b,b)} - \sum_{i=2}^{q+1}\overline{P}_i.$$

We also already observed, in the discussion preceding Proposition 4.2, that the places $\overline{Q}_{(1-b,b)}$ of $\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$ are totally ramified in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)/\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$. For $b \neq 0$, we denote by $Q_{i_b} \in O_2$ the unique extension of $\overline{Q}_{(1-b,b)}$ in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)/\mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})$, where i_b is an index in $\{2, \ldots, q^3 - q\}$, and we denote by Q_1 the unique extension of $\overline{Q}_{(1,0)}$ (see discussion before Remark 4.1). Since $[\mathbb{F}_{q^{2n}}(\mathcal{BM}_n) : \mathbb{F}_{q^{2n}}(\tilde{\mathcal{H}})] = m$, we hence obtain that the principal divisor of t in $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ is

$$(t) = mQ_1 + m \sum_{\substack{b \in \mathbb{F}_{q^2}^* \\ b^q + b = 0}} Q_{i_b} - m \sum_{i=2}^{q+1} P_i. \tag{4.8}$$

Therefore, since $(\tilde{\theta}_0) = (t) - (x + y)$, by equation (4.8) and equation (4.5) we have that

$$\begin{aligned}(\tilde{\theta}_0) &= mQ_1 + m \sum_{\substack{b \in \mathbb{F}_{q^2}^* \\ b^q + b = 0}} Q_{i_b} - m \sum_{i=2}^{q+1} P_i - mqP_1 + m \sum_{i=2}^{q+1} P_i \\ &= mQ_1 + m \sum_{\substack{b \in \mathbb{F}_{q^2}^* \\ b^q + b = 0}} Q_{i_b} - mqP_1,\end{aligned}$$

which gives the desired result. □

4.1.1 The two-point Weierstrass semigroup $H(Q_1, P_1)$

Our aim is now to study the duals of two-point AG codes from the function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, for all $n \geq 3$ odd.

More specifically, with the notations introduced in the previous section, we are interested in the codes $C_L(D, G)^\perp$, where $G := aQ_1 + bP_1$, for $a, b \in \mathbb{Z}$ such that $a + b \geq 0$, and D is the sum of all the $\mathbb{F}_{q^{2n}}$-rational places of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ different from Q_1 and P_1. The two-point Weierstrass semigroup $H(Q_1, P_1)$ plays a fundamental role in the investigation of such codes. Indeed, as pointed out in Section 2.4, the knowledge of $H(Q_1, P_1)$ is equivalent to that of the function τ_{Q_1,P_1} (see equation (2.9)), which is a crucial tool for computing the dimension of the codes $C_L(D, G)^\perp$ and the order bound for their minimum distance, see Definition 2.41, Theorem 2.46 and Corollary 2.47. Therefore, the aim of this subsection is to explicitly compute the function τ_{Q_1,P_1}.

We start by giving an explicit description of the ring of functions that are regular outside Q_1 and P_1 (see equation (2.7)), and by computing the period of $H(Q_1, P_1)$, see (2.8).

Proposition 4.6. $\mathcal{R}(Q_1, P_1) = \mathbb{F}_{q^{2n}}[\alpha, \alpha^{-1}, \tilde{\theta}_0, \theta_1, \theta_2, \ldots, \theta_M]$.

Proof. From (4.6), (4.7) and Lemma 4.5 it is clear that the $\mathbb{F}_{q^{2n}}$-rational functions $\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M$ are regular outside P_1; furthermore, from (4.3) it follows that

$$H(P_1) = \langle -v_{P_1}(\alpha), -v_{P_1}(\tilde{\theta}_0), -v_{P_1}(\theta_1), \ldots, -v_{P_1}(\theta_M)\rangle.$$

We first prove that the ring $\mathcal{R}(P_1) := \bigcup_{i\geq 0} L(iP_1)$ of $\mathbb{F}_{q^{2n}}$-rational functions that are regular outside P_1 is

$$\mathcal{R}(P_1) = \mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]. \tag{4.9}$$

It is clear that $\mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M] \subseteq \bigcup_{i\geq 0} L(iP_1)$. In fact, for each function h of the ring $\mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$, being h a combination of $\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M$, there exists a positive integer $\hat{\gamma}$ such that $h \in L(\hat{\gamma}P_1)$.
Conversely, if $h \in \bigcup_{i\geq 0} L(iP_1)$, then in particular $h \in L(i_h P_1)$ for some $i_h \geq 0$. We prove that h belongs to $\mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$ by induction on i_h. If $i_h = 0$, then trivially h belongs to $L(0) = \mathbb{F}_{q^{2n}} \subseteq \mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$. We proceed now to the induction step. Assume that the claim holds for all integers i_h less than or equal to $\tilde{n}$ and consider $i_h = \tilde{n} + 1$. If $\tilde{n} + 1$ is not an element of $H(P_1)$, then $h \in L(kP_1)$ for some $k \leq \tilde{n}$, and the thesis follows by induction. If instead $\tilde{n} + 1$ belongs to $H(P_1)$, then $\tilde{n} + 1$ can be written as a combination of $-v_{P_1}(\alpha), -v_{P_1}(\tilde{\theta}_0), -v_{P_1}(\theta_1), \ldots, -v_{P_1}(\theta_M)$, namely

$$\tilde{n} + 1 = a_1(-v_{P_1}(\alpha)) + \cdots + a_{M+2}(-v_{P_1}(\theta_M))$$

for some $a_i \in \mathbb{N}$, $1 \leq i \leq M + 2$. Then note that the pole divisor $(h)_\infty$ of h is

$$(h)_\infty = (\alpha^{a_1} \cdot \tilde{\theta}_0^{\,a_2} \cdot \theta_1^{a_3} \cdots \theta_M^{a_{M+2}})_\infty$$

and hence there exists $\lambda \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $h' := h - \lambda\alpha^{a_1} \cdot \tilde{\theta}_0^{\,a_2} \cdots \theta_1^{a_3} \cdots \theta_M^{a_{M+2}}$ is an element of $\bigcup_{i\geq 0} L(iP_1)$ with $v_{P_1}(h') > -(\tilde{n} + 1)$. By the induction hypothesis, $h' \in \mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$ and hence

$$h = h' + \lambda\alpha^{a_1} \cdot \tilde{\theta}_0^{\,a_2} \cdots \theta_1^{a_3} \cdots \theta_M^{a_{M+2}} \in \mathbb{F}_{q^{2n}}[\alpha, \tilde{\theta}_0, \theta_1, \ldots, \theta_M].$$

The statement of the proposition now follows. Indeed, it is clear from (4.6) and (4.9) that any function in $\mathbb{F}_{q^{2n}}[\alpha, \alpha^{-1}, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$ is regular outside Q_1 and P_1; conversely, for any $f \in \mathcal{R}(Q_1, P_1)$ there exists a suitable integer $k \geq 0$ such that $f\alpha^k$ belongs to $\mathcal{R}(P_1)$. This shows that f belongs to $\mathbb{F}_{q^{2n}}[\alpha, \alpha^{-1}, \tilde{\theta}_0, \theta_1, \ldots, \theta_M]$. □

Lemma 4.7. *The period π of the Weierstrass semigroup $H(Q_1, P_1)$ is $\pi = q^n + 1$.*

Proof. Assume by contradiction that $k(Q_1 - P_1)$ is a principal divisor for some $k \in \{1, \dots, q^n\}$. Let $f \in \mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ such that $(f) = k(Q_1 - P_1)$. In particular, k is a non-gap of the Weierstrass semigroup $H(Q_1)$, as $v_{Q_1}(f^{-1}) = -k$ and Q_1 is the only pole of f^{-1}. The smallest nonzero element of $H(Q_1)$ is $q^n + 1 - m$ (see (4.4)), hence $q^n + 1 - m \leq k \leq q^n$ and we can write $k = q^n + 1 - m + j$ for some $j \in \{0, \dots, m-1\}$. Since

$$(\alpha^{-1} f) = (q^n + 1 - k)(P_1 - Q_1) = (m - j)(P_1 - Q_1),$$

then $m - j$ must be a non-gap of the Weierstrass semigroup $H(Q_1)$; this is not possible, as $0 < m - j < qm = q^n + 1 - m$. □

Given Proposition 4.6 and Lemma 4.7, we are now able to prove the following theorem, which provides the explicit expression of the function τ_{Q_1,P_1}, see (2.9). As pointed out before, the knowledge of such function is sufficient to determine the two-point Weierstrass semigroup $H(Q_1, P_1)$, see Section 2.4.

Theorem 4.8. *Let $i \in \mathbb{Z}$ and write $i = -k(q^n + 1) - \ell m - \beta$ for a unique triple $(k, \ell, \beta) \in \mathbb{Z}^3$ such that $0 \leq \beta < m$, $0 \leq \ell < q + 1$. Let $\gamma := \lceil \beta / M \rceil$. Then*

$$\tau_{Q_1,P_1}(i) = k(q^n + 1) + (\gamma + \ell)mq + \beta(q^2 - q).$$

Proof. Define the map $\tilde{\tau} : \mathbb{Z} \to \mathbb{Z}$ such that $\tilde{\tau}(i) = k(q^n+1)+(\gamma+\ell)mq+\beta(q^2-q)$ for all $i \in \mathbb{Z}$ and k, ℓ, β, γ as in the assumptions. We will prove that $\tilde{\tau}(i) = \tau_{Q_1,P_1}(i)$ for all $i \in \mathbb{Z}$. In the following, we fix $i \in \mathbb{Z}$, so that k, ℓ, β, γ are fixed too. Choose M nonnegative integers $i_1, \dots, i_M$ such that

$$\sum_{j=1}^{M} i_j j = \beta \quad \text{and} \quad \sum_{j=1}^{M} i_j = \gamma.$$

Such choice of $i_1, \dots, i_M$ always exists: letting $\beta' := \beta \mod M$, if $\beta' \neq 0$ one can choose $i_M = \gamma - 1$, $i_{\beta'} = 1$ and $i_j = 0$ for $j \neq M, \beta'$. If $\beta' = 0$, one can instead choose $i_M = \gamma$ and $i_j = 0$ for $j \neq M$.
Consider now the function

$$f := \alpha^k \tilde{\theta_0}^{\ell} \prod_{j=1}^{M} \theta_j^{i_j}.$$

From (4.6), (4.7) and Lemma 4.5, the principal divisor of f is

$$\begin{aligned}(f) =& k(q^n+1)(Q_1-P_1)+\ell(mQ_1+E-mqP_1)+\\ &\sum_{j=1}^{M} i_j\left(j\sum_{i=1}^{q^3-q}Q_i+(m-j(q^2-q))\sum_{i=2}^{q+1}P_i-(mq+j(q^2-q))P_1\right)\\ =&\left(k(q^n+1)+\ell m+\sum_{j=1}^{M}i_jj\right)Q_1+E'-\\ &\left(k(q^n+1)+\left(\sum_{j=1}^{M}i_j+\ell\right)mq+\sum_{j=1}^{M}i_jj(q^2-q)\right)P_1\\ =&-iQ_1+E'-\tilde{\tau}(i)P_1.\end{aligned}$$

where E and E' are effective divisors whose supports do not contain Q_1 and P_1. The above computation shows that $(i,\tilde{\tau}(i))$ belongs to $H(Q_1,P_1)$ and thus $\tilde{\tau}(i)\geq\tau_{Q_1,P_1}(i)$ by definition of τ_{Q_1,P_1}.

Finally, we can use Lemma 2.36 *4)* to show that the equality $\tilde{\tau}(i)=\tau_{Q_1,P_1}(i)$ holds. Indeed, we have just proved that $\tilde{\tau}(i)\geq\tau_{Q_1,P_1}(i)$ for all $i\in\mathbb{Z}$ and therefore

$$\sum_{i=c}^{\pi+c-1}(i+\tilde{\tau}(i))\geq\sum_{i=c}^{\pi+c-1}(i+\tau_{Q,P}(i))=\pi g(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)) \tag{4.10}$$

for all $c\in\mathbb{Z}$. To conclude, it is enough to check that the left side of equation (4.16) is equal to $\pi g(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$. We can choose $c=-\pi+1$ without loss of generality, so that

$$\sum_{i=-\pi+1}^{0}(i+\tilde{\tau}(i))=\sum_{\beta=0}^{m-1}\sum_{\ell=0}^{q}(-m\ell-\beta+(\gamma+\ell)mq+\beta(q^2-q)). \tag{4.11}$$

Writing $\gamma=\frac{1}{M}(\beta+(M-\beta)\bmod M)$, the quantity on the right side of equation (4.11) yields

$$\begin{aligned}&-\frac{m^2q(q+1)}{2}-\frac{m(m-1)(q+1)}{2}+\frac{m^2(m-1)q(q+1)}{2M}+\\ &\frac{mq^2(q^2-1)(M-1)}{2}+\frac{m^2q^2(q+1)}{2}+\frac{m(m-1)q(q^2-1)}{2}.\end{aligned}$$

It can be checked with a direct computation that the above quantity is equal to $\frac{1}{2}(q^n+1)(q-1)(q^{n+1}+q^n-q^2)=\pi g(\mathbb{F}_{q^{2n}}(\mathcal{BM}_n))$. □

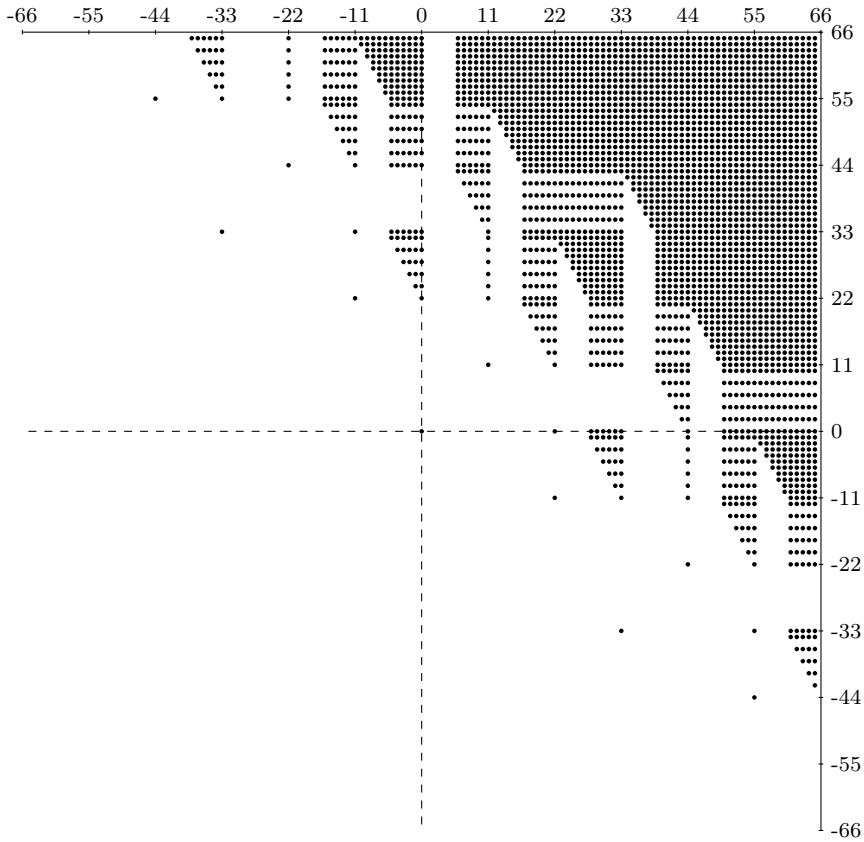


Figure 4.1: The two-point Weierstrass semigroup $H(Q_1, P_1)$ for $q = 2$ and $n = 5$, of period $\pi = 33$. Only the pairs $(i, j) \in H(Q_1, P_1)$ with $-2\pi < i, j < 2\pi$ are represented.

4.1.2 Computation of the order bound and results

We are now ready to compute the order bound, under the restrictions of Remark 2.45, for dual codes of two-point AG codes from the function field $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, for all $n \geq 3$ odd. As pointed out in the previous subsection, we study the two-point codes $C_L(D, G)^\perp$ with $G := aQ_1 + bP_1$ and the divisor D that is the sum of all the $\mathbb{F}_{q^{2n}}$-rational places of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ different from Q_1 and P_1. The degree of D is therefore $\deg(D) = N_n - 2$, where $N_n := q^{2n+2} - q^{n+3} + q^{n+2} + 1$ is the number of $\mathbb{F}_{q^{2n}}$-rational places of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$. The two-point AG code $C_L(D, G)$ and its dual $C_L(D, G)^\perp$ are hence linear subspaces of $\mathbb{F}_{q^{2n}}^{N_n - 2}$.

Remark 4.9. *As a consequence of the observations in Remark 4.4, our study of*

the two-point codes $C_L(D,G)^\perp$ comprises in fact all the codes with $G := aQ_h + bP_k$ and D the sum of all the rational places of $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$ different from Q_h and P_k, for any $Q_h \in O_2$ and any $P_k \in O_1$.

Let $\delta := a+b$ be the degree of the divisor G and observe that, if $\delta \geq N_n + 2g - 3$, then the code $C_L(D,G)^\perp$ is the zero code; this follows from the fact that, if $\delta \geq N_n + 2g - 3$, the divisors G and $G - D$ are non-special, as their degrees exceed $2g-2$ and, from the Riemann-Roch theorem, $\dim(C_L(D,G)) = \dim(L(G)) - \dim(L(G-D)) = N_n - 2$.

Define $\Delta := 4g - 1$. As pointed out in Section 2.5, it is sufficient to determine the order bound for the code $C_L(D,G)^\perp$ in the case $\delta < \Delta$ only, since the order bound coincides with the Goppa bound if the degree of G is larger than or equal to Δ (see Lemma 2.44). The condition $\delta < \Delta$, which also implies $\deg(G) < \deg(D)$, makes the determination of the dimension of $C_L(D,G)^\perp$ a particularly easy task; indeed,

$$\dim(C_L(D,G)^\perp) = N_n - 2 - \dim(L(G)).$$

The dimension of $L(G)$ can be conveniently computed applying Theorem 2.46 with the map τ_{Q_1,P_1} defined in Theorem 4.8.

The algorithm we propose for computing the order bound for $C_L(D,G)^\perp$ is inspired by [5, Algorithm 1] and takes into account the observations above. Similarly to [5], we recursively obtain a bound for the minimum distance of the code $C_L(D,G)^\perp$ by successive iterations on the degree δ of G, starting from $\delta = \Delta - 1$ and decreasing δ by 1 at each round of the procedure, until $\delta = 0$. Observe that it is easy to check if

$$\dim(L(aQ_1 + bP_1)) \neq \dim(L((a+1)Q_1 + bP_1)), \tag{4.12}$$

since, from Theorem 2.46, equation (4.12) holds if and only if $\tau_{Q_1,P_1}(a+1) \leq b$. Similarly, the inequality $\dim(L(aQ_1 + bP_1)) \neq \dim(L(aQ_1 + (b+1)P_1))$ holds if and only if $\tau^{-1}_{Q_1,P_1}(b+1) \leq a$. Note that $\tau^{-1}_{Q_1,P_1}(b+1)$ can be computed using Proposition 2.37.

Furthermore, Corollary 2.47 ensures that the knowledge of the function τ_{Q_1,P_1} and its inverse provides also a straightforward way for computing the integers $\nu(Q_1; 0, \tilde{a}Q_1 + \tilde{b}P_1)$ and $\nu(P_1; 0, \tilde{a}Q_1 + \tilde{b}P_1)$, for any $\tilde{a}, \tilde{b} \in \mathbb{Z}_{\geq 0}$, $\tilde{a} + \tilde{b} = \delta$.

Algorithm 4.10. *Input: a prime power q and an odd integer $n \geq 3$.*
Output: a table T whose rows consist of three cells: the first cell contains an integer k representing the dimension of a code $C_L(D, aQ_1 + bP_1)^\perp$; the second cell contains a pair of integers (a,b) such that $d(aQ_1 + bP_1) \geq d(a'Q_1 + b'P_1)$ for all codes $C_L(D, a'Q_1 + b'P_1)^\perp$ of dimension k; the third cell contains $d(aQ_1 + bP_1)$.

1. *Initialize an empty table T.*

2. *Define $g := \frac{1}{2}(q-1)(q^{n+1}+q^n-q^2)$ and $\Delta := 4g-1$.*

3. *Construct an upper-left triangular matrix A of size $(\Delta+1)\times(\Delta+1)$ and set $A[a,\Delta-a] = \Delta-2g+2$ for $a = 0,\dots,\Delta$.*

4. *Define $\delta := \Delta - 1$.*

5. *For $a = 0,\dots,\delta$, define $b := \delta - a$ and*

$$d_{Q_1} := \begin{cases} \min\{\nu(Q_1;0,aQ_1+bP_1), A[a+1,b]\} & \text{if } \tau_{Q_1,P_1}(a+1) \le b, \\ A[a+1,b] & \text{otherwise}, \end{cases}$$

$$d_{P_1} := \begin{cases} \min\{\nu(P_1;0,aQ_1+bP_1), A[a,b+1]\} & \text{if } \tau^{-1}_{Q_1,P_1}(b+1) \le a, \\ A[a,b+1] & \text{otherwise}, \end{cases}$$

$$d := \max\{d_{Q_1}, d_{P_1}\}.$$

6. *Compute $k := \dim(C_L(D, aQ_1+bP_1)^{\perp})$.*

7. *Check if a row with value k in the first cell exists in the table T.*

   (a) *If such row does not exist, add a new row to T with k in the first cell, (a,b) in the second cell, d in the third cell.*

   (b) *If such row exists and d is strictly larger than the value in the third cell, update the row by overwriting the pair in the second cell with (a,b) and the value in the third cell with d.*

   (c) *If such row exists and d is not larger than the value in the third cell, do nothing.*

8. *Redefine $\delta := \delta - 1$ and repeat the procedure from step 5 until $\delta = 0$.*

The table T in output of Algorithm 4.10 stores the information on possible improvements on the minimum distance of codes $C_L(D,G)^{\perp}$ over the Goppa bound. Note for example that the improvements obtained for $q=2, n=3$ and $q=3, n=3$ are identical to the ones obtained in [5] (the case $q=2, n=3$ is summarized in Table 4.1, compare with [5, Table 1]); on one hand this should not surprise, since $\mathbb{F}_{q^6}(\mathcal{BM}_3)$ and $\mathbb{F}_{q^6}(\mathcal{GGS}_3)$ are isomorphic, but on the other hand it is interesting to see that the definition of order bound that we use, which is slightly weaker than the one given in [5], does not affect the estimate for the minimum distance in these particular cases.

k	(a,b)	d	k	(a,b)	d	k	(a,b)	d
195	(0, 37)	20	205	(1, 26)	11	215	(1, 16)	4
196	(1, 35)	19	206	(1, 25)	10	216	(7, 8)	4
197	(1, 34)	18	207	(1, 24)	9	217	(1, 14)	3
198	(1, 33)	17	208	(1, 23)	9	218	(1, 13)	3
199	(1, 32)	16	209	(1, 22)	8	219	(1, 11)	3
200	(1, 31)	15	210	(0, 22)	6	220	(4, 7)	2
201	(0, 31)	14	211	(0, 21)	6	221	(2, 7)	2
202	(1, 29)	13	212	(0, 20)	6	222	(2, 5)	2
203	(4, 25)	13	213	(0, 19)	6			
204	(0, 28)	12	214	(1, 17)	5			

Table 4.1: Table T obtained from Algorithm 4.10 with $q = 2$, $n = 3$ and code length $N_3 - 2 = 223$.

We also compared our results obtained using Algorithm 4.10 with the results obtained using [5, Algorithm 1] for $q = 2$ and $n = 5$. In this case, the two function fields $\mathbb{F}_{2^{10}}(\mathcal{BM}_5)$ and $\mathbb{F}_{2^{10}}(\mathcal{GGS}_5)$ are not isomorphic. Table 4.2 summarizes the cases where our results improve those from [5].

k	(a,b)	d	d_2	k	(a,b)	d	d_2
3875	(5, 132)	52	51	3920	(5, 87)	17	16
3876	(5, 131)	51	50	3926	(15, 71)	14	12
3878	(5, 129)	49	48	3927	(15, 70)	14	12
3880	(5, 127)	47	46	3928	(15, 69)	13	11
3904	(0, 108)	28	27	3929	(15, 68)	13	11
3909	(5, 98)	23	22	3930	(14, 68)	12	11
3917	(5, 90)	19	18	3934	(1, 77)	8	7

Table 4.2: For $q = 2$, $n = 5$, Table 4.2 reports the largest estimate for the minimum distance d of a code $C_L(D, aQ_1 + bP_1)^\perp$ of length $N_5 - 2 = 3967$ and dimension k and compares d with d_2, the largest estimate obtained in [5] for codes of same length and dimension. Only the cases where $d > d_2$ are reported.

4.2 The case of the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$

After having studied the case of the Beelen-Montanucci function fields, we continue our investigation focusing on one of the maximal function fields introduced by D. Skabelund in [79]. We start by setting the following notations, that will

be used throughout the section: let $s \in \mathbb{N}$, $s \geq 1$, and let $q_0 := 2^s$, $q := 2q_0^2$ and $m := q - 2q_0 + 1$.

The Suzuki function field $\mathbb{F}_q(\mathcal{S}_q)$ is the $\mathbb{F}_q$-rational function field of the curve defined by the affine equation

$$\mathcal{S}_q : y^q + y = x^{q_0}(x^q + x).$$

Its genus is equal to $q_0(q-1)$ and the set O of its rational places has cardinality q^2+1. Furthermore, the full automorphism group of $\mathbb{F}_q(\mathcal{S}_q)$ is the Suzuki group of cardinality $(q^2+1)q^2(q-1)$ and acts doubly transitively on the set O.

We consider now the constant field extension $\mathbb{F}_{q^4}(\mathcal{S}_q) := \mathbb{F}_q(\mathcal{S}_q)\mathbb{F}_{q^4}$ and note that, for each place in O, there is exactly one place of $\mathbb{F}_{q^4}(\mathcal{S}_q)$ lying over it, with relative degree equal to 4. Throughout this section, we denote by $\mathcal{O}$ the set of such places. It is not difficult to compute the total number of rational places of $\mathbb{F}_{q^4}(\mathcal{S}_q)$, which shows that such function field is in fact maximal.

The Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ is a Kummer extension of $\mathbb{F}_{q^4}(\mathcal{S}_q)$, namely it is the $\mathbb{F}_{q^4}$-rational function field of the curve given by the equations

$$\tilde{\mathcal{S}}_q : \begin{cases} y^q + y = x^{q_0}(x^q + x), \\ z^m = x^q + x. \end{cases} \tag{4.13}$$

It can be seen that all the places in $\mathcal{O}$ are totally ramified in the extension $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)/\mathbb{F}_{q^4}(\mathcal{S}_q)$. Henceforth, we set the notation

$$\tilde{\mathcal{O}} := \{Q \in \mathbb{P}_{\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)} \mid Q|\overline{Q},\ \overline{Q} \in \mathcal{O}\}$$

for the set of extensions of these places.

In the following proposition, we recall some of the main properties of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$. Further details can be found in [34] and [79].

Proposition 4.11 ([34, Section 3], [79, Section 3])**.** *Let $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ be the Skabelund function field as defined by equation* (4.13)*.*

- *The function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ is maximal, with genus*

$$g(\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)) = \frac{1}{2}q(q-1)^2$$

and $q^5 - q^4 + q^3 + 1$ $\mathbb{F}_{q^4}$-rational places.

- *The full automorphism group* $\mathrm{Aut}(\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q))$ *acts on the set of rational places of* $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ *with two short orbits; one is non-tame of size* q^2+1*, consisting of exactly the places in* $\tilde{\mathcal{O}}$*, the other is tame of size* $q^5-q^4+q^3-q^2$*, consisting of all the remaining* $\mathbb{F}_{q^4}$*-rational places.*

We denote by P_∞ the unique place of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ lying over the pole of x in the extension $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)/\mathbb{F}_{q^4}(\mathcal{S}_q)$, which belongs to the orbit $\tilde{\mathcal{O}}$. Moreover, we denote by $P_{(a,b,c)} \in \mathbb{P}_{\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)}$ the place that is the only common zero of the functions $x-a$, $y-b$ and $z-c$ in $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$, for $a,b,c \in \mathbb{F}_{q^4}$. Henceforth, for less cumbersome notations, we simply denote by P the place $P_{(0,0,0)} \in \tilde{\mathcal{O}} \setminus \{P_\infty\}$.

Remark 4.12. *From a geometrical point of view, the place* $P_{(a,b,c)} \in \mathbb{P}_{\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)}$ *is centered at the affine point of* $\tilde{\mathcal{S}}_q$ *that can be parametrized in homogeneous* $[x:y:z:w]$*-coordinates as* $[a:b:c:1]$*. On the other hand, the place* P_∞ *is centered at the only point at infinity of* $\tilde{\mathcal{S}}_q$*.*

In the following proposition, we recall the principal divisors of the coordinate functions and of the two functions

$$t := x^{2q_0+1} + y^{2q_0} \quad \text{and} \quad \beta := xy^{2q_0} + t^{2q_0}$$

in $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$.

Proposition 4.13 ([9, Section 2])**.** *The principal divisors in* $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ *of the functions* x,y,z,t,β *are:*

$$\begin{aligned}
(x) &= mP + E_x - (q^2-2qq_0+q)P_\infty,\\
(y) &= m(q_0+1)P + E_y - (q^2-qq_0+q_0)P_\infty,\\
(z) &= \sum_{\substack{a^q+a\,=\,0,\\ b^q+b\,=\,0}} P_{(a,b,0)} - q^2P_\infty,\\
(t) &= m(2q_0+1)P + E_t - (q^2-q+2q_0)P_\infty,\\
(\beta) &= (q^2+1)(P-P_\infty),
\end{aligned} \tag{4.14}$$

where E_x, E_y, E_t *are effective divisors whose support does not contain* P *and* P_∞*.*

4.2.1 The two-point Weierstrass semigroup $H(P,P_\infty)$

As in Section 4.1, we are again interested in using the order bound (see Definition 2.41) for estimating the minimum distance of the AG codes $C_L(D,G)^\perp$

with

$$D := \sum_{R \in \mathfrak{R} \setminus \{P, P_\infty\}} R \quad \text{and} \quad G := aP + bP_\infty, \tag{4.15}$$

where $\mathfrak{R}$ denotes the set of all $\mathbb{F}_{q^4}$-rational places of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ and $a, b \in \mathbb{Z}_{>0}$. Therefore, as discussed in Section 4.1.1, our first goal is to explicitly determine the function τ_{P,P_∞}, whose knowledge is equivalent to that of the two-point Weierstrass semigroup $H(P, P_\infty)$.

Since the places P_∞ and P lie in the same orbit under the action of the full automorphism group of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ (see Proposition 4.11), it holds that $H(P) = H(P_\infty)$. Moreover, the Weierstrass semigroup at every place of the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ is known, see [9]. We recall the structure of $H(P_\infty)$ in the following proposition.

Proposition 4.14 ([9, Theorem 3.2])**.** *The Weierstrass semigroup of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ at P_∞ is*

$$H(P_\infty) = \langle q^2 - 2qq_0 + q, q^2 - qq_0 + q_0, q^2 - q + 2q_0, q^2, q^2 + 1 \rangle.$$

To the aim of determining the function τ_{P,P_∞}, we now compute the ring $\mathcal{R}(P, P_\infty)$ of regular functions outside P and P_∞, see equation (2.7).

Proposition 4.15. *The ring of all $\mathbb{F}_{q^4}$-rational functions that are regular outside P and P_∞ is*

$$\mathcal{R}(P, P_\infty) = \mathbb{F}_{q^4}[x, y, z, t, \beta, \beta^{-1}].$$

Proof. It is clear from (4.14) that any function in $\mathbb{F}_{q^4}[x, y, z, t, \beta, \beta^{-1}]$ is regular outside P and P_∞. Conversely, from (4.14) and Proposition 4.14 it follows that the ring $\mathcal{R}(P_\infty)$ consisting of all $\mathbb{F}_{q^4}$-rational functions that are regular outside P_∞ is

$$\mathcal{R}(P_\infty) = \mathbb{F}_{q^4}[x, y, z, t, \beta].$$

Hence, for any $f \in \mathcal{R}(P, P_\infty)$ there exists a suitable integer $k \geq 0$ such that $f\beta^k$ belongs to $\mathcal{R}(P_\infty)$. This shows that f belongs to $\mathbb{F}_{q^4}[x, y, z, t, \beta, \beta^{-1}]$. □

Lemma 4.16. *The period of the Weierstrass semigroup $H(P, P_\infty)$ is $q^2 + 1$.*

Proof. Assume by contradiction that there exists a function f defined on $\tilde{\mathcal{S}}_q$ having principal divisor $(f) = k(P - P_\infty)$, for some $k \in \{1, \ldots, q^2\}$. Then k must be a non-gap of the Weierstrass semigroup $H(P_\infty)$. The smallest nonzero element of $H(P_\infty)$ is $q^2 - 2qq_0 + q$ (see Proposition 4.14), hence $q^2 - 2qq_0 + q \leq k \leq q^2$

and we can write $k = q^2 - 2qq_0 + q + j$ for some $j \in \{0, \dots, 2qq_0 - q\}$. The function βf^{-1} has principal divisor

$$(\beta f^{-1}) = (q^2 + 1 - k)(P - P_\infty) = (2qq_0 - q + 1 - j)(P - P_\infty),$$

hence $2qq_0 - q + 1 - j$ must be a non-gap of the Weierstrass semigroup $H(P_\infty)$. This is not possible, as $0 < 2qq_0 - q + 1 - j < 2qq_0 - q + 1 < q^2 - 2qq_0 + q$. $\square$

In the following discussion, we denote the period of $H(P, P_\infty)$ by $\rho := q^2 + 1$.

Lemma 4.17. *Let $i \in \mathbb{Z}$, $k := \left\lfloor \frac{i-1}{\rho} \right\rfloor$ and $r := i - k\rho - 1$. Then, i can be written uniquely as*

$$i = (k+1)\rho - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t),$$

with $a_t, a_x, a_y, a_z \in \mathbb{Z}$ such that $0 \le a_z \le m-1$ and

$$\begin{cases} 0 \le a_x \le q_0, a_y = 0, a_t = q_0 & \text{if } r < m(q_0+1), \\ 0 \le a_x \le q_0 - a_y, 0 \le a_y \le 1, 0 \le a_t \le q_0 - 1 & \text{otherwise.} \end{cases}$$

Proof. Observe that $k\rho + 1 \le i \le (k+1)\rho$ and $0 \le r \le \rho - 1$. Assume first $r < m(q_0+1)$ and note that the condition

$$0 \le \rho - 1 - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t) < m(q_0+1)$$

holds for any choices of a_t, a_x, a_y, a_z as in the assumptions. Moreover, suppose that r can be expressed as

$$r = \rho - 1 - (a_z + ma_x + (2q_0+1)mq_0) = \rho - 1 - (a'_z + ma'_x + (2q_0+1)mq_0),$$

with $0 \le a_z, a'_z \le m-1$, $0 \le a_x, a'_x \le q_0$. Considering the above equation modulo m, it directly follows that $a_z = a'_z$ and $a_x = a'_x$. Hence, there are precisely $m(q_0+1)$ distinct integers in the interval $[0, m(q_0+1)-1]$, one for each possible choice of a_t, a_x, a_y, a_z, that can be written as $\rho - 1 - (a_z + ma_x + (2q_0+1)mq_0)$. The first case of the statement follows.

A similar argument can be repeated for the case $m(q_0+1) \le r \le \rho - 1$; the condition

$$m(q_0+1) \le \rho - 1 - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t) \le \rho - 1$$

holds for any choices of a_t, a_x, a_y, a_z as in the assumptions. Further, assume that r can be expressed as:

$$\begin{aligned} r &= \rho - 1 - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t) \\ &= \rho - 1 - (a'_z + ma'_x + (q_0+1)ma'_y + (2q_0+1)ma'_t) \end{aligned}$$

with $0 \le a_z, a'_z \le m-1$, $0 \le a_x \le q_0 - a_y, 0 \le a'_x \le q_0 - a'_y, 0 \le a_y, a'_y \le 1, 0 \le a_t, a'_t \le q_0 - 1$. Considering the above equation first modulo m, then modulo $2q_0+1$, and finally modulo q_0+1, we conclude that $a_z = a'_z$, $a_x = a'_x$, $a_y = a'_y$, $a_t = a'_t$. There are $m(q+q_0)$ possible choices of a_t, a_x, a_y, a_z, as well as distinct integers in the interval $[m(q_0+1), \rho-1]$; we conclude that any integer in the interval $[m(q_0+1), \rho-1]$ can be expressed uniquely as $\rho - 1 - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t)$ and the second case of the statement follows. □

Theorem 4.18. *Let $i \in \mathbb{Z}$, $k := \left\lfloor \frac{i-1}{\rho} \right\rfloor$ and write*

$$i = (k+1)\rho - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t),$$

for a unique quadruple $(a_t, a_x, a_y, a_z) \in \mathbb{Z}^4$ such that $0 \le a_z \le m-1$, $0 \le a_y \le 1$, $0 \le a_x \le q_0 - a_y$ and $0 \le a_t \le q_0$. Then

$$\tau_{P,P_\infty}(i) = (a_z q^2 + a_t(q^2 - q + 2q_0) + a_y(q^2 - qq_0 + q_0) + a_x(q^2 - 2qq_0 + q)) - (k+1)\rho.$$

Proof. To prove the theorem, we define the map $\tilde{\tau} : \mathbb{Z} \to \mathbb{Z}$ such that

$$\tilde{\tau}(i) = (a_z q^2 + a_t(q^2 - q + 2q_0) + a_y(q^2 - qq_0 + q_0) + a_x(q^2 - 2qq_0 + q)) - (k+1)\rho$$

for all $i \in \mathbb{Z}$ and k, a_t, a_x, a_y, a_z as in the assumptions, and we show that $\tilde{\tau}(i) = \tau_{P,P_\infty}(i)$ for all $i \in \mathbb{Z}$.

We start by showing that $\tilde{\tau}(i) \ge \tau_{P,P_\infty}(i)$ for all $i \in \mathbb{Z}$. To this aim, let $i \in \mathbb{Z}$, $k := \left\lfloor \frac{i-1}{\rho} \right\rfloor$ as above and write i as

$$i = (k+1)\rho - (a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t),$$

for the suitable quadruple $(a_t, a_x, a_y, a_z) \in \mathbb{Z}^4$. Consider the function

$$f := \beta^{-(k+1)} t^{a_t} z^{a_z} y^{a_y} x^{a_x}.$$

Then, by Proposition 4.13, it follows that the principal divisor of f is

$$\begin{aligned}
(f) = &-(k+1)(q^2+1)(P - P_\infty) + a_z \left(\sum_{\substack{a^q + a = 0, \\ b^q + b = 0}} P_{(a,b,0)} - q^2 P_\infty \right) \\
&+ a_t \left(m(2q_0+1)P + E_z - (q^2 - q + 2q_0)P_\infty \right) \\
&+ a_y \left(m(q_0+1)P + E_y - (q^2 - qq_0 + q_0)P_\infty \right) \\
&+ a_x \left(mP + E_x - (q^2 - 2qq_0 + q)P_\infty \right) \\
= &- iP + E - \tilde{\tau}(i)P_\infty,
\end{aligned}$$

where E is an effective divisor whose support does not contain P and P_∞. The above computation shows that $(i, \tilde{\tau}(i))$ lies in $H(P, P_\infty)$ and thus $\tilde{\tau}(i) \geq \tau_{P,P_\infty}(i)$ by definition of τ_{P,P_∞}.

For showing that the equality $\tilde{\tau}(i) = \tau_{P,P_\infty}(i)$ holds for all $i \in \mathbb{Z}$, we can now use Proposition 2.36 *4)*. Indeed, we have just proved that $\tilde{\tau}(i) \geq \tau_{P,P_\infty}(i)$ for all $i \in \mathbb{Z}$ and therefore

$$\sum_{i=c}^{\pi+c-1} (i + \tilde{\tau}(i)) \geq \sum_{i=c}^{\pi+c-1} (i + \tau_{P,P_\infty}(i)) = \pi g(\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)) \tag{4.16}$$

for all $c \in \mathbb{Z}$. To conclude, it is enough to check that the left side of equation (4.16) is equal to $\pi g(\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q))$. We can choose $c = 0$ without loss of generality, hence we obtain

$$\begin{aligned}
&\sum_{i=0}^{\pi-1}(i + \tilde{\tau}(i)) = \\
&= -\sum_{a_z=0}^{m-1}\sum_{a_t=0}^{q_0-1}\sum_{a_y=0}^{1}\sum_{a_x=0}^{q_0-a_y}((a_z + ma_x + (q_0+1)ma_y + (2q_0+1)ma_t)+ \\
&- (a_z q^2 + a_t(q^2 - q + 2q_0) + a_y(q^2 - qq_0 + q_0) + a_x(q^2 - 2qq_0 + q)))+ \\
&- \sum_{a_z=0}^{m-1}\sum_{a_x=0}^{q_0}((a_z + ma_x + (2q_0+1)mq_0) - (a_z q^2 + q_0(q^2 - q + 2q_0) + a_x(q^2 - 2qq_0 + q))) \\
&= -(1-q^2)\left((q_0+1)q_0\frac{(m-1)m}{2} + q_0^2\frac{(m-1)m}{2} + (q_0+1)\frac{(m-1)m}{2}\right) + \\
&- (m - (q^2 - 2qq_0 + q))\left(\frac{q_0(q_0+1)}{2}q_0 m + \frac{(q_0-1)q_0}{2}q_0 m + \frac{q_0(q_0+1)}{2}m\right) + \\
&- ((2q_0+1)m - (q^2 - q + 2q_0))\left(\frac{(q_0-1)q_0}{2}(q_0+1)m + \frac{(q_0-1)q_0}{2}q_0 m + q_0(q_0+1)m\right) + \\
&- ((q_0+1)m - (q^2 - qq_0 + q_0))(q_0^2 m) = 16q_0^{10} - 16q_0^8 + 8q_0^6 - 4q_0^4 + q_0^2 = \pi g(\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)).
\end{aligned}$$

□

4.2.2 Results and comparisons

In this section, we present the results obtained for the AG codes $C_L(D, G)^\perp$ from $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$ with

$$D := \sum_{R \in \mathfrak{R} \setminus \{P, P_\infty\}} R \quad \text{and} \quad G := aP + bP_\infty,$$

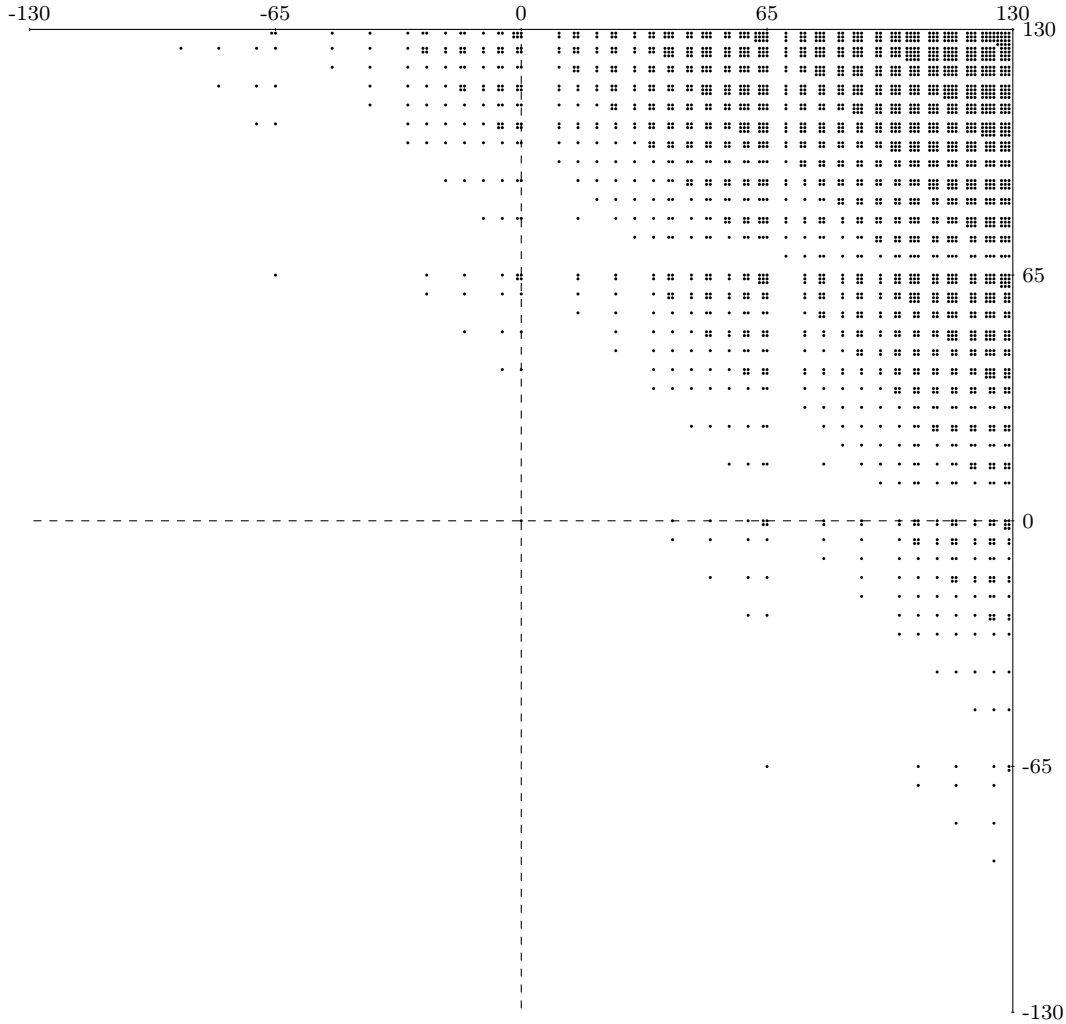


Figure 4.2: The two-point Weierstrass semigroup $H(P, P_\infty)$ for $s = 1$, of period $\pi = 65$. Only the pairs $(i, j) \in H(P, P_\infty)$ with $-2\pi < i, j < 2\pi$ are represented.

where $\mathfrak{R}$ denotes the set of all $\mathbb{F}_{q^4}$-rational places of $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$, $a, b \in \mathbb{Z}_{>0}$ and the parameter s is set to be $s = 1$ (see equation (4.15)). With this choice, we have $q_0 = 2$ and $q = 8$, so that the Skabelund function field $\mathbb{F}_{8^4}(\tilde{\mathcal{S}}_8)$ is maximal over $\mathbb{F}_{8^4}$ and has exactly 29185 $\mathbb{F}_{8^4}$-rational places. Hence, the associated two-point AG codes have length $N := |\mathfrak{R}| - 2 = 29183$.

The order bound for the minimum distance of these codes is computed with the same algorithm as Algorithm 4.10, which is inspired by [5, Algorithm 1]. Therefore, we refer to Section 4.1.2 for a thorough description of the algorithm and the technical details. Indeed, the assumptions that we made in Remark 2.45 for computational purposes hold for both cases. In particular, this means that we only consider codes with $a + b \leq 4g(\mathbb{F}_{8^4}(\tilde{\mathcal{S}}_8)) - 1$.

The results obtained show that in several cases the order bound significantly improves the Goppa bound. Moreover, we observed that, for all the two-point codes considered, the minimum distance is always at least that of the best comparable one-point code of the same dimension (see Table 4.3 for the details). In Table 4.3, we denote by d the order bound for the minimum distance of the two-point code $C_L(D, aP+bP_\infty)^\perp$ and with d_1 the order bound for the minimum distance of the best one-point code $C_L(D, b'P_\infty)^\perp$ with the same dimension k. The table contains all the results, for $s = 1$ and code length $N = 29183$, for which the difference between the estimates d and d_1 is larger than or equal to 10. The four rows in bold of Table 4.3 mark the codes for which $d - d_1 = 20$, which is the largest value obtained for such difference.

Remark 4.19. *Defining the curve $\tilde{\mathcal{S}}_q$ over $\mathbb{F}_q$, one could consider its $\mathbb{F}_q$-rational function field $\mathbb{F}_q(\tilde{\mathcal{S}}_q)$ and study two-point AG codes from it. In this setting, both the support of D and G would consist of $\mathbb{F}_q$-rational places, and one could in principle compute the order bound for these codes and compare them with the two-point codes arising from the Suzuki function field $\mathbb{F}_q(\mathcal{S}_q)$, that were studied in [68]. However, since the genus of $\mathbb{F}_q(\tilde{\mathcal{S}}_q)$ is considerably larger than the number of its $\mathbb{F}_q$-rational places, the order bound does not give a good estimate for the minimum distance in this case.*

Table 4.3: For $s = 1$, the table contains the best possible estimates for the minimum distance d and d_1, obtained with the order bound, for a two-point code $C_L(D, aP + bP_\infty)^\perp$ and a one-point code $C_L(D, b'P_\infty)^\perp$ of a certain dimension k and length $N = 29183$, respectively.

k	(a, b)	d	d_1	b'	k	(a, b)	d	d_1	b'
28860	(1, 517)	138	128	518	28933	(1, 444)	70	60	445
28861	(1, 516)	138	128	517	28934	(1, 443)	70	60	444
28864	(1, 513)	134	124	514	28935	(1, 442)	70	60	443
28865	(1, 512)	134	124	513	28936	(1, 441)	70	60	442
28866	(1, 511)	134	124	512	28938	(1, 439)	65	50	440
28868	(1, 509)	130	120	510	28939	(1, 438)	65	50	439
28869	(1, 508)	130	120	509	28940	(1, 437)	65	50	438
28870	(1, 507)	130	120	508	28941	(1, 436)	65	50	437

Continued on next page

Table 4.3 – continued from previous page

k	(a,b)	d	d_1	b'	k	(a,b)	d	d_1	b'
28871	(1, 506)	130	120	507	28942	(1, 435)	65	50	436
28874	(1, 503)	124	114	504	28943	(1, 434)	65	50	435
28875	(1, 502)	124	114	503	28944	(1, 433)	65	50	434
28876	(1, 501)	124	114	502	28945	(1, 432)	65	50	433
28878	(1, 499)	120	110	500	28946	(1, 431)	65	50	432
28879	(1, 498)	120	110	499	**28948**	**(6, 424)**	**60**	**40**	**430**
28880	(1, 497)	120	110	498	**28949**	**(6, 423)**	**60**	**40**	**429**
28881	(1, 496)	120	110	497	**28950**	**(6, 422)**	**60**	**40**	**428**
28884	(1, 493)	114	104	494	**28951**	**(6, 421)**	**60**	**40**	**427**
28885	(1, 492)	114	104	493	28952	(1, 425)	55	40	426
28886	(1, 491)	114	104	492	28953	(1, 424)	55	40	425
28888	(1, 489)	110	100	490	28954	(1, 423)	55	40	424
28889	(1, 488)	110	100	489	28955	(1, 422)	55	40	423
28890	(1, 487)	110	100	488	28956	(1, 421)	55	40	422
28891	(1, 486)	110	100	487	28957	(1, 420)	50	40	421
28898	(1, 479)	100	90	480	28958	(1, 419)	50	40	420
28899	(1, 478)	100	90	479	28959	(1, 418)	50	40	419
28900	(1, 477)	100	90	478	28960	(1, 417)	50	40	418
28901	(1, 476)	100	90	477	28961	(1, 416)	50	40	417
28908	(1, 469)	90	80	470	28978	(11, 389)	40	30	400
28909	(1, 468)	90	80	469	28979	(11, 388)	40	30	399
28910	(1, 467)	90	80	468	28980	(11, 387)	40	30	398
28911	(1, 466)	90	80	467	28981	(11, 386)	40	30	397
28923	(1, 454)	79	65	455	28997	(56, 324)	30	20	380
28924	(1, 453)	79	64	454	28998	(56, 323)	30	20	379
28925	(1, 452)	79	64	453	28999	(56, 322)	30	20	378
28926	(1, 451)	79	64	452	29000	(56, 321)	30	20	377
28927	(1, 450)	75	64	451	29001	(56, 320)	30	20	376
28928	(1, 449)	75	60	450	29002	(56, 319)	30	20	375
28929	(1, 448)	75	60	449	29003	(56, 318)	30	20	374
28930	(1, 447)	75	60	448	29004	(56, 317)	30	20	373
28931	(1, 446)	75	60	447	29005	(56, 316)	30	20	372
28932	(1, 445)	70	60	446					

Chapter 5

On the asymptotic behaviour of rational points of curves over $\mathbb{F}_q$

In order to investigate the subject of study of this final chapter, we need to adopt a more geometrical language. This entails that we start by fixing the following notations, that will be used throughout the discussion.

Let $\mathcal{X} \subseteq \mathbb{P}^n$ be a projective curve of genus g and degree d defined over $\mathbb{F}_q$. Here, by *genus* of the curve we mean the genus of its function field, while by *degree* of the curve we mean the maximum number of intersections (counted with multiplicity) of the curve with a hyperplane of $\mathbb{P}^n$ not containing any of its components. We say that a curve defined over $\mathbb{F}_q$ is *irreducible* (*over* $\mathbb{F}_q$) if it consists of only one component defined and irreducible over $\mathbb{F}_q$, while we call it *absolutely irreducible* if it is irreducible over $\overline{\mathbb{F}}_q$. Furthermore, the curve is said to be *nondegenerate* if it is not contained in any hyperplane of $\mathbb{P}^n$. Being consistent with Definition 2.31, we say that the curve $\mathcal{X}$ is nonsingular if all of its points (i.e., all the points in $\mathcal{X}(\overline{\mathbb{F}}_q)$) are nonsingular. Moreover, we say that an absolutely irreducible curve $\mathcal{X} \subseteq \mathbb{P}^n$ is a *complete intersection* if its homogeneous ideal is generated by precisely $n-1$ homogeneous polynomials, see Section 2.2 and [45, p.136]. Note that, with a slight abuse of terminology, in the following discussion we will use the term *curve* also when not dealing with

a variety, in the sense of Section 2.2, which means that we will also consider projective algebraic sets that are not absolutely irreducible.

In this chapter, we investigate lower and upper bounds for a constant introduced by M. Homma in [49], which measures the asymptotic behaviour of the number of rational points of projective curves over $\mathbb{F}_q$, when the degree becomes large. The results included in the chapter are contained in [11] and were jointly developed by P. Beelen, M. Montanucci and the author of this thesis.

In Chapter 2, we recalled the definition of Ihara's constant $A(q)$ (see (2.1)), which describes the asymptotic behaviour of the number of rational places of a function field F over $\mathbb{F}_q$, when the genus g becomes large with respect to q. As already observed in Section 2.1, the Drinfeld-Vlăduţ bound (see [20]) ensures that, for any q, Ihara's constant $A(q)$ satisfies the inequality

$$A(q) \leq \sqrt{q} - 1.$$

Furthermore, if q is a square, Y. Ihara in [56] and M. Tsfasman, S. Vlăduţ and T. Zink in [86] proved that $A(q)$ attains this bound, that is, $A(q) = \sqrt{q} - 1$.

Lower bounds for $A(q)$ have also been widely investigated in the literature, especially using the concept of (infinite) *towers* of function fields. A tower $\mathcal{F}$ of function fields over $\mathbb{F}_q$ is an infinite sequence

$$\mathcal{F} = (F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots \subsetneq F_n \subsetneq \ldots)$$

of function fields defined over $\mathbb{F}_q$, such that

- the genera $g(F_i) \to \infty$ for $i \to \infty$,
- for every i, $\mathbb{F}_q$ is the full constant field of F_i and the extension F_{i+1}/F_i is finite and separable.

As a consequence of the Riemann-Hurwitz Genus Formula (see Theorem 2.22), A. Garcia and H. Stichtenoth showed in [31, Corollary 2.2] that, for any tower $\mathcal{F}$, the sequence $\left\{\frac{N(F_i)}{g(F_i)}\right\}_{i\geq 0}$, where $N(F_i)$ denotes the number of rational places of F_i, is convergent. Hence, we have the well-defined notion of *limit* $\lambda(\mathcal{F})$ of a tower $\mathcal{F}$, that is,

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

By equation (2.1) and the definition of $\lambda(\mathcal{F})$, it immediately follows that

$$0 \leq \lambda(\mathcal{F}) \leq A(q),$$

and a tower $\mathcal{F}$ over $\mathbb{F}_q$ is said *asymptotically bad* if $\lambda(\mathcal{F}) = 0$, *asymptotically good* if $\lambda(\mathcal{F}) > 0$ or *asymptotically optimal* if $\lambda(\mathcal{F}) = A(q)$. This motivates why studying the limits of towers of function fields and constructing asymptotically good towers are interesting problems, also to the aim of finding nontrivial lower bounds for Ihara's constant $A(q)$. It was in fact using class field towers that J.-P. Serre proved, in [77], the inequality

$$A(q) > c \log_2(q),$$

for any q and for some constant $c > 0$ independent of q, which implies in particular that $A(q) > 0$ for all q. In [71, Theorem 5.2.9], H. Niederreiter and C. Xing showed that the constant c can be taken to be $c = \frac{1}{96}$. Later on, constructing certain recursive towers of function fields with many rational places, A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth proved in [7] that

$$A(q) \geq \frac{2}{\frac{1}{p^m-1} + \frac{1}{p^{m+1}-1}}$$

if $q = p^{2m+1}$, with $m > 0$, providing the currently best known lower bound for $A(q)$ in such cases. However, the exact value of $A(q)$ is unknown when q is not a square.

Observe that, in the light of Section 2.2 and with the terminology just introduced above, Ihara's constant can equivalently be seen as describing the asymptotic behaviour of rational points of projective, nonsingular, absolutely irreducible curves defined over $\mathbb{F}_q$. On the other hand, by considering projective irreducible curves over $\mathbb{F}_q$, with the only requirements of being nondegenerate and of positive degree, one can investigate a different asymptotic property, namely the asymptotic behaviour of the number of rational points of such curves when the degree (instead of the genus) becomes large with respect to q. This property was first considered by M. Homma in [49], which originated from previous work developed by himself and S.J. Kim in the series of papers [53–55].

In these papers, the authors showed that, if $\mathcal{X}$ is a (possibly absolutely reducible) plane curve without $\mathbb{F}_q$-linear components, then

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q + 1, \tag{5.1}$$

except for curves isomorphic over $\mathbb{F}_4$ to the curve defined by

$$\mathcal{K} : (X+Y+Z)^4 + (XY+YZ+ZX)^2 + XYZ(X+Y+Z) = 0,$$

which satisfies $|\mathcal{K}(\mathbb{F}_4)| = 14$. The bound (5.1) was originally conjectured by P. Sziklai in [83], where explicit examples of some curves achieving it had also been provided. The natural question on whether the bound (5.1) was valid for curves

in higher dimensional projective spaces $\mathbb{P}^n$, for $n \geq 3$, was then analyzed by M. Homma in [49], where it was shown that equation (5.1) is in fact also true when $n \geq 3$ and $\mathcal{X}$ has no $\mathbb{F}_q$-linear components, unless $d = q = 4$ and $\mathcal{X}$ is $\mathbb{F}_q$-isomorphic to the plane curve $\mathcal{K}$.

In the same paper [49], an analogue of Ihara's constant $A(q)$ was introduced, by replacing the genus g with the degree d. More precisely, the following definitions were given. For a fixed prime power q and a fixed positive integer d, let

$$M_q(d) := \max\{|\mathcal{X}(\mathbb{F}_q)| \mid \mathcal{X} \subseteq \mathbb{P}^n,\ n \geq 3,\ \text{irreducible curve of degree } d \text{ over } \mathbb{F}_q\},$$

i.e., $M_q(d)$ is the maximum number of $\mathbb{F}_q$-rational points that an irreducible curve of a fixed degree d, in a projective space of some dimension, can have. Note that here the dimension of the projective space is not fixed and therefore allowed to be arbitrarily large. An analogue of $A(q)$ is then defined as

$$D(q) := \limsup_{d \to \infty} \frac{M_q(d)}{d}, \tag{5.2}$$

which measures the asymptotic behavior of the number of rational points of projective curves over $\mathbb{F}_q$ when d becomes large. Throughout the chapter, we refer to $D(q)$ as *Homma's constant.*

In [49], it was already observed that, since the bound (5.1) is valid for curves in any projective space $\mathbb{P}^n$, $n \geq 2$, with the only exception mentioned above, one may conclude that $D(q) \leq q$. Moreover, in the same paper, the lower bound $D(q) \geq A(q)/2$ was also derived.

In the work contained in this chapter, we find new upper and lower bounds for the value of $D(q)$, by a refinement of Homma's methods and by using towers of algebraic function fields. The exact value of $D(q)$ remains unknown for all q.

Our main results are summarized in the following theorem.

Theorem 5.1. *Let $q = p^e$ be a prime power and let $D(q)$ be Homma's constant as defined in* (5.2)*. Then*

1. $D(q) \leq q - 1$,
2. $D(q) \geq 1$ *provided that* $q > 2$,
3. $D(q^2) \geq \frac{q}{q+1} A(q^2) = \frac{q^2-q}{q+1}$.

Note that the lower bound $D(q) \geq 1$ is interesting for small values of q only, since otherwise Homma's lower bound $D(q) \geq A(q)/2$ is better. The values $q \leq 31$

for which the lower bound $D(q) \geq 1$ is currently the best known are listed in Remark 5.5.

The chapter is organized as follows. In Section 5.1, we start by slightly improving Homma's upper bound on $D(q)$, refining the argument provided in [49] and thus proving Item 1 of Theorem 5.1. Subsequently, in Section 5.2, we prove Item 2 of Theorem 5.1. The technique that we use consists in explicitly constructing a sequence of curves whose degrees are close to their number of rational points. Finally, in Section 5.3, we prove Item 3 of Theorem 5.1, by making use of a particular tower of function fields over $\mathbb{F}_{q^2}$ that was constructed recursively by A. Garcia and H. Stichtenoth in [31].

5.1 An upper bound for $D(q)$: the proof of Item 1 of Theorem 5.1

The upper bound $D(q) \leq q$ obtained by M. Homma in [49, Proposition 5.4] was deduced from the bound (5.1), but in the same paper the following theorem was given.

Theorem 5.2 ([49, Theorem 3.2])**.** *Let $\mathcal{X} \subseteq \mathbb{P}^n$ be a nondegenerate irreducible curve of degree d defined over $\mathbb{F}_q$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leq \frac{(q-1)(q^{n+1}-1)}{q(q^n-1)-n(q-1)}d. \tag{5.3}$$

Using this result, we can already prove Item 1 in Theorem 5.1. Indeed, for a fixed value of q, considering equation (5.3) and dividing both sides by d gives

$$\frac{|\mathcal{X}(\mathbb{F}_q)|}{d} \leq \frac{(q-1)(q^{n+1}-1)}{q(q^n-1)-n(q-1)} = \frac{(q-1)\dfrac{(q^{n+1}-1)}{q^{n+1}}}{\dfrac{q(q^n-1)}{q^{n+1}} - \dfrac{n(q-1)}{q^{n+1}}}. \tag{5.4}$$

This observation can be used to improve the upper bound for $D(q)$. Note that by taking the $\limsup_{d\to\infty} M_q(d)/d$ as in (5.2), we are by definition of $D(q)$ considering curves of increasing degree. However, the dimension of the projective spaces containing the curves will also be increasing as d increases. Indeed, if for a family of curves $(\mathcal{X}_i)_{i\geq 0}$, with degrees d_i tending to infinity as i tends to infinity, there exists an $n \in \mathbb{N}$ such that, for all i, $\mathcal{X}_i \subseteq \mathbb{P}^n$, then $|\mathcal{X}_i(\mathbb{F}_q)| \leq |\mathbb{P}^n(\mathbb{F}_q)| = (q^{n+1}-1)/(q-1)$ for all i, implying that $|\mathcal{X}_i(\mathbb{F}_q)|/d_i$ tends to zero as i tends to infinity.

Now let $(\mathcal{X}_i)_{i\geq 0}$ be a family of curves with degrees d_i tending to infinity such that $\limsup_{i\to\infty} |\mathcal{X}_i(\mathbb{F}_q)|/d_i > 0$, and assume, for each i, that $\mathcal{X}_i$ is a nondegenerate curve contained in $\mathbb{P}^{n_i}$. We have seen that n_i tends to infinity as i tends to infinity, therefore, from equation (5.4), we obtain:

$$D(q) \leq \lim_{i\to\infty} \frac{(q-1)\dfrac{(q^{n_i+1}-1)}{q^{n_i+1}}}{\dfrac{q(q^{n_i}-1)}{q^{n_i+1}} - \dfrac{n_i(q-1)}{q^{n_i+1}}} = q-1.$$

This proves Item 1 of Theorem 5.1.

5.2 A lower bound for $D(q)$: the proof of Item 2 of Theorem 5.1

For a prime power $q = p^e$ strictly larger than two, consider the tower of function fields $\mathcal{T} = (T_m)_{m\geq 1}$ over $\mathbb{F}_q$ defined recursively by

$$T_1 = \mathbb{F}_q(x_1) \qquad \text{and} \qquad T_{i+1} = T_i(x_{i+1}) \qquad \text{with} \qquad x_{i+1}^{q-1} = -1 + (x_i+1)^{q-1}.$$

The tower $\mathcal{T}$ is similar to an asymptotically good tower considered in [81, Proposition 7.3.3], but the variation we consider is actually not asymptotically good.

A first observation is that the zero of x_1 in T_1 is totally ramified in the tower and therefore the equation $x_{i+1}^{q-1} = -1 + (x_i+1)^{q-1}$ is absolutely irreducible, when viewed as a polynomial in $T_i[x_{i+1}]$, for all integers $i \geq 1$. Indeed, for all $\beta \in \mathbb{F}_q^*$, let $P_{\beta-1}^{(1)}$ be the zero of the function $x_1 - (\beta-1)$ in $\mathbb{F}_q(x_1)$, and let $P_\infty^{(1)}$ be the pole of x_1 in $\mathbb{F}_q(x_1)$. Note that, with this choice of notations, we have that the zero of x_1 in $\mathbb{F}_q(x_1)$ is denoted by $P_0^{(1)} = P_{\beta-1}^{(1)}$, with $\beta = 1$. Let now $u_1 := (x_1+1)^{q-1} - 1$, then we have that

$$u_1 := (x_1+1)^{q-1} - 1 = \prod_{\beta\,\in\,\mathbb{F}_q^*} (x_1 + 1 - \beta) = \prod_{\beta\,\in\,\mathbb{F}_q^*} (x_1 - (\beta-1)),$$

and hence we immediately deduce that the principal divisor of the function u_1 in $\mathbb{F}_q(x_1)$ is

$$(u_1)_{\mathbb{F}_q(x_1)} = \sum_{\beta\,\in\,\mathbb{F}_q^*} P_{\beta-1}^{(1)} - (q-1)P_\infty^{(1)}.$$

Therefore, by Corollary 2.26, we directly obtain that the function field extension $\mathbb{F}_q(x_1, x_2)/\mathbb{F}_q(x_1) = T_2/T_1$ is Kummer of degree $q-1$. This follows for instance observing that $v_{P_0^{(1)}}(u_1) = 1$, hence $P_0^{(1)}$ is a place of $\mathbb{F}_q(x_1)$ such that $\gcd(v_{P_0^{(1)}}(u_1), q-1) = 1$. Then, by Proposition 2.25, it follows in particular that $P_0^{(1)}$ is totally ramified in $\mathbb{F}_q(x_1, x_2)/\mathbb{F}_q(x_1)$ and that the polynomial $x_2^{q-1} + 1 - (x_1+1)^{q-1}$, that defines the extension, is irreducible over $\mathbb{F}_q$. Also, denoting with $P_0^{(2)}$ the unique extension of $P_0^{(1)}$ in T_2/T_1, we have that $v_{P_0^{(2)}}(x_2) = 1$. Furthermore, since the above arguments hold as well if we consider the constant field extensions $\overline{\mathbb{F}}_q(x_1)$, $\overline{\mathbb{F}}_q(x_1, x_2)$, and the extension $\overline{\mathbb{F}}_q(x_1, x_2)/\overline{\mathbb{F}}_q(x_1)$, we also note that the polynomial $x_2^{q-1} + 1 - (x_1+1)^{q-1}$ is in fact absolutely irreducible. Let now $u_i := (x_i+1)^{q-1} - 1 \in T_i$ and consider the extension T_{i+1}/T_i, for any $i \geq 2$. Repeating the reasoning just discussed, mutatis mutandis, we can then iteratively show, for all $i \geq 2$, that there is exactly one place $P_0^{(i)}$ that is a zero of x_i in T_i, lies over $P_0^{(i-1)}$ and is totally ramified in T_{i+1}/T_i, with $P_0^{(i+1)}|P_0^{(i)}$ being its unique extension. Moreover, it holds that $v_{P_0^{(i)}}(x_i) = 1$ and that the equation $x_{i+1}^{q-1} = -1 + (x_i+1)^{q-1}$ is absolutely irreducible, when viewed as a polynomial in $T_i[x_{i+1}]$, for all $i \geq 2$.

The fact that the polynomial $x_{i+1}^{q-1} + 1 - (x_i+1)^{q-1} \in T_i[x_{i+1}]$ is absolutely irreducible, for all $i \geq 1$, implies in particular that the ideal $I_\ell := \langle x_2^{q-1} + 1 - (x_1+1)^{q-1}, \ldots, x_\ell^{q-1} + 1 - (x_{\ell-1}+1)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell]$ is a prime ideal. Since we wish to deal with projective curves, the following proposition, concerning the homogenization of the ideal I_ℓ, is essential.

Proposition 5.3. *Let $\ell > 1$ be an integer and define $I'_\ell := \langle x_2^{q-1} + z^{q-1} - (x_1+z)^{q-1}, \ldots, x_\ell^{q-1} + z^{q-1} - (x_{\ell-1}+z)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell, z]$. Then I'_ℓ is a homogeneous prime ideal and the homogenization of the prime ideal $I_\ell := \langle x_2^{q-1} + 1 - (x_1+1)^{q-1}, \ldots, x_\ell^{q-1} + 1 - (x_{\ell-1}+1)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell]$.*

Proof. For convenience, let us write $g_i := x_{i+1}^{q-1} + 1 - (x_i+1)^{q-1}$ and $g'_i := x_{i+1}^{q-1} + z^{q-1} - (x_i+z)^{q-1}$. We have already seen that the ideal I_ℓ is a prime ideal. Now let $>_{\text{deglex}}$ denote the degree-lexicographic ordering with $x_\ell >_{\text{deglex}} \ldots >_{\text{deglex}} x_1$ as a monomial ordering in $\mathbb{F}_q[x_1, \ldots, x_\ell]$. Since under this monomial ordering the leading terms of the g_i are coprime, the set $\{g_1, \ldots, g_{\ell-1}\}$ is a Gröbner basis of I_ℓ. Then, from [18, §8.4, Theorem 4], it follows that $\{g'_1, \ldots, g'_{\ell-1}\}$ is a Gröbner basis for the homogenization of I_ℓ, with respect to the monomial ordering $x_\ell >_{\text{deglex}} \ldots >_{\text{deglex}} x_1 > z$ in $\mathbb{F}_q[x_1, \ldots, x_\ell, z]$. Hence, I'_ℓ is a homogeneous prime ideal that is precisely the homogenization of the prime ideal I_ℓ. $\square$

With Proposition 5.3 in place, consider, for $\ell \in \mathbb{Z}_{\geq 2}$, the projective algebraic set

$\mathcal{X}_\ell \subseteq \mathbb{P}^\ell$ defined over $\mathbb{F}_q$ by the homogeneous equations

$$x_{i+1}^{q-1} = -z^{q-1} + (x_i + z)^{q-1} \quad \text{for } i = 1, \dots, \ell - 1. \tag{5.5}$$

By Proposition 5.3 and the preceding discussion, we have that $\mathcal{X}_\ell$ is actually an absolutely irreducible projective curve, that is in particular a complete intersection. Hence, it holds that $\deg(\mathcal{X}_\ell) = \deg(g_1') \cdots \deg(g_{\ell-1}') = (q-1)^{\ell-1}$ (see [23, Theorem III-71]).

Our goal is now to estimate the number of $\mathbb{F}_q$-rational points of $\mathcal{X}_\ell$. To this aim, we consider the number of projective points $[x_1 : x_2 : \cdots : x_\ell : 0]$ satisfying equation (5.5). Substituting $z = 0$ in equation (5.5), we obtain that

$$x_{i+1}^{q-1} = x_i^{q-1} \quad \text{for } i = 1, \dots, \ell - 1,$$

and, choosing $x_1 = 1$, we see that any solution is defined over $\mathbb{F}_q$ and that there are exactly $(q-1)^{\ell-1}$ points at infinity on $\mathcal{X}_\ell$. In particular, $|\mathcal{X}_\ell(\mathbb{F}_q)| \geq (q-1)^{\ell-1}$. Therefore, we deduce that

$$D(q) \geq \limsup_{\ell \to \infty} \frac{|\mathcal{X}_\ell(\mathbb{F}_q)|}{\deg(\mathcal{X}_\ell)} \geq \frac{(q-1)^{\ell-1}}{(q-1)^{\ell-1}} = 1,$$

which completes the proof of Item 2 of Theorem 5.1.

5.3 A lower bound for $D(q^2)$: the proof of Item 3 of Theorem 5.1

In order to prove Item 3 of Theorem 5.1, we use the following tower of function fields over $\mathbb{F}_{q^2}$, that was constructed recursively by A. Garcia and H. Stichtenoth in [31]:

$$F_1 = \mathbb{F}_{q^2}(x_1) \qquad \text{and} \qquad F_{i+1} = F_i(x_{i+1}) \qquad \text{with} \qquad x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}.$$

This tower is optimal in the sense that, if $N(F_i)$ denotes the number of rational places and $g(F_i)$ the genus of F_i, then $\lim_{m\to\infty} N(F_m)/g(F_m) = q - 1 = A(q^2)$, see [31, Theorem 3.1].

Indeed, by [31, Lemma 3.9], any zero of the function $x_1 - \alpha$ in F_1, for $\alpha \in \mathbb{F}_{q^2} \setminus \{\alpha \mid \alpha^q + \alpha = 0\}$, splits completely in the extension F_m/F_1, implying that $N(F_m) \geq (q-1)q^m$. Moreover, in [31, Remark 3.8] it is shown that the genus $g(F_m)$ of F_m, for any $m \geq 1$, is

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

For computing the genus $g(F_m)$, it is proven that the pole P_∞ of $x_1 \in F_1$ is totally ramified in all extensions F_m/F_1, $m \geq 2$, see [31, Lemma 3.3] and also [72, Proposition 1.1]. We denote here by $P_\infty^{(m)}$ the unique extension of P_∞ in F_m, for all $m \geq 2$. Moreover, note that $P_\infty^{(m)}$ is a rational place, since P_∞ is totally ramified in F_m/F_1.

Even though it is in general a difficult challenge to compute the Weierstrass semigroups at places in a tower, R. Pellikaan, H. Stichtenoth and F. Torres in [72] computed the Weierstrass semigroup $H(P_\infty^{(m)})$ at $P_\infty^{(m)}$ for all $m \geq 1$. More precisely, they proved that, for any $m \geq 2$, the semigroup at $P_\infty^{(m)}$ has a particularly interesting property, namely it can be computed from the one at $P_\infty^{(m-1)}$ by means of a recursive procedure. Indeed, from [72, Theorem 3.1] it follows that

$$H(P_\infty^{(m)}) = \begin{cases} \mathbb{Z}_{\geq 0} & \text{if} \quad m = 1 \\ qH(P_\infty^{(m-1)}) \cup \mathbb{Z}_{\geq c_m} & \text{if} \quad m > 1 \end{cases} \tag{5.6}$$

where $c_m := q^m - q^{\lceil \frac{m}{2} \rceil}$ is the conductor of $H(P_\infty^{(m)})$.

Let $\{\gamma_1, \ldots, \gamma_\ell\}$ be a set of generators of $H(P_\infty^{(m)})$, so that

$$H(P_\infty^{(m)}) = \langle \gamma_1, \ldots, \gamma_\ell \rangle,$$

and $0 < \gamma_1 < \cdots < \gamma_\ell$. Note that equation (5.6) implies that $\gamma_1 = q^{m-1}$, being the smallest positive element of $H(P_\infty^{(m)})$. This then implies that $H(P_\infty^{(m)}) \cap \mathbb{Z}_{<c_m+q^{m-1}}$ is a generating set and that therefore we may assume

$$\gamma_\ell \leq c_m + q^{m-1} - 1. \tag{5.7}$$

By definition of the Weierstrass semigroup $H(P_\infty^{(m)})$, there exist functions $f_1, \ldots, f_\ell \in F_m$ such that

$$(f_i)_\infty = \gamma_i P_\infty^{(m)}, \ i = 1, \ldots, \ell.$$

In [75], the functions $f_1, \ldots, f_\ell$ are used to define a birational morphism between a nonsingular projective curve $\mathcal{X}$ and a curve $\mathcal{X}'$, with only one point at infinity. Intuitively, the idea is to use such functions in order to define a map φ_m from the set of places of F_m to an algebraic curve $\mathcal{X}_m \subseteq \mathbb{P}^\ell$. This map is easiest to describe when first extending the constant field of F_m to the algebraic closure $\overline{\mathbb{F}}_{q^2}$ of $\mathbb{F}_{q^2}$, as all the places of $\bar{F}_m := F_m\overline{\mathbb{F}}_{q^2}$ are rational. We denote by $\bar{P}_\infty^{(m)}$ the only place of $\bar{F}_m$ lying over $P_\infty^{(m)}$ in the constant field extension $\bar{F}_m/F_m$, see [81, Theorem 3.6.3]. Moreover, with notations as in Section 2.1, we let here $f_i(Q) \in \mathrm{O}_Q/Q$ denote the residue class of the function f_i modulo the place Q.

Since $\mathrm{O}_Q/Q \cong \overline{\mathbb{F}}_{q^2}$, with slight abuse of notation we can then regard $f_i(Q)$ as an element of $\overline{\mathbb{F}}_{q^2}$.

In this setting, we define the map φ_m in the following way:

$$\varphi_m : \mathbb{P}(\bar{F}_m) \longrightarrow \mathbb{P}^\ell,$$

with

$$\begin{array}{rcll} \varphi_m(Q) & := & [1 : f_1(Q) : \cdots : f_\ell(Q)], & \text{if } Q \neq \bar{P}_\infty^{(m)}, \\ \varphi_m(Q) & := & [0 : \cdots : 0 : 1], & \text{otherwise.} \end{array}$$

By [35, Theorem 4.2.2], it holds that the image of φ_m is a projective curve $\mathcal{X}_m$ defined over $\mathbb{F}_{q^2}$, since the functions $f_1, \ldots, f_\ell \in F_m = \mathbb{F}_{q^2}(x_1, \ldots, x_m)$. Therefore, we henceforth consider the curve $\mathcal{X}_m$ as a curve defined over $\mathbb{F}_{q^2}$. Moreover, [75, Theorem 15] ensures that the $\mathbb{F}_{q^2}$-rational function field of $\mathcal{X}_m$ is exactly F_m, that apart from possibly $\varphi_m(\bar{P}_\infty^{(m)})$ the curve has no singular points and that $\bar{P}_\infty^{(m)}$ is the only place of F_m centered at the point $\varphi_m(\bar{P}_\infty^{(m)})$. In other words, this means that φ_m induces a bijection between $\mathbb{P}_{\bar{F}_m} \setminus \{\bar{P}_\infty^{(m)}\}$ and $\mathcal{X}_m(\overline{\mathbb{F}}_{q^2}) \setminus \{\varphi_m(\bar{P}_\infty^{(m)})\}$.

Remark 5.4. *The curve $\mathcal{X}_m$ is a nondegenerate curve in $\mathbb{P}^\ell$. Indeed, if this was not the case, then there would exist a combination $a_1 + a_2 f_1 + \cdots + a_{\ell+1} f_\ell$, for some $a_i \in \overline{\mathbb{F}}_{q^2}$ not all equal to zero, such that $a_1 + a_2 f_1 + \cdots + a_{\ell+1} f_\ell \equiv 0$, which is impossible by the linear independence of $\{1, f_1, \ldots, f_\ell\}$ over $\overline{\mathbb{F}}_{q^2}$ given by [81, Proposition 3.6.1].*

We now wish to investigate the degree and number of $\mathbb{F}_{q^2}$-rational points of the curve $\mathcal{X}_m$. The number of rational points is easy to bound, since the $\mathbb{F}_{q^2}$-rational places of F_m are in bijection with the points on $\mathcal{X}_m$ defined over $\mathbb{F}_{q^2}$. Indeed, the place $P_\infty^{(m)}$ corresponds to the projective point $[0 : \cdots : 0 : 1]$, while the remaining $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_m$ are nonsingular and hence each corresponds to a unique rational place of F_m (see Remark 2.33). This shows that

$$|\mathcal{X}_m(\mathbb{F}_{q^2})| = N(F_m) \geq (q-1)q^m, \tag{5.8}$$

where the inequality $N(F_m) \geq (q-1)q^m$ was already mentioned before, as a consequence of [31, Lemma 3.9].

At this point, we only need to derive some information on the degree $\deg(\mathcal{X}_m)$ of the curve $\mathcal{X}_m$. To this aim, we claim that the following chain of inequalities hold:

$$\deg(\mathcal{X}_m) \leq \gamma_\ell \leq c_m + q^{m-1} - 1. \tag{5.9}$$

In order to prove it, we start by observing that the last inequality is simply equation (5.7), therefore it is already settled. Furthermore, let $L(\gamma_\ell \bar{P}_\infty^{(m)})$ denote

the Riemann-Roch space of the divisor $\gamma_\ell \bar{P}_\infty^{(m)}$, and let $X_0, \ldots, X_\ell$ be a choice of coordinate functions in $\mathbb{P}^\ell$. We note that the points of intersection of the curve $\mathcal{X}_m$ and a hyperplane of equation $a_0X_0 + \cdots + a_\ell X_\ell = 0$ in $\mathbb{P}^\ell$ correspond, by the definition of φ_m, to the places that are zeros of the function $a_0 + \sum_{i=1}^{\ell} a_i f_i \in L(\gamma_\ell \bar{P}_\infty^{(m)})$. Then, since the pole divisor of $a_0 + \sum_{i=1}^{\ell} a_i f_i$ has degree at most γ_ℓ, the same is true for its zero divisor, and hence the number of intersection points is at most γ_ℓ.

Combining equation (5.8) and equation (5.9), and recalling that $A(q^2) = q - 1$, we hence obtain

$$D(q^2) \geq \limsup_{m\to\infty} \frac{|\mathcal{X}_m(\mathbb{F}_{q^2})|}{\deg(\mathcal{X}_m)} \geq \limsup_{m\to\infty} \frac{(q-1)q^m}{c_m + q^{m-1} - 1} = \frac{q^2 - q}{q+1},$$

and Item 3 of Theorem 5.1 follows.

Remark 5.5. *Item* 3 *of Theorem 5.1 improves Homma's lower bound* $D(q^2) \geq A(q^2)/2$ *for any value of* q. *The bound* $D(q) \geq 1$ *is instead interesting for small values of* $q > 2$, *since then Homma's lower bound* $D(q) \geq A(q)/2$ *is weaker. The following table provides, for those small values of* q, *the best known lower bound for* $A(q)/2$. *For all other values of* q, *except possibly when* q *is a prime,* $A(q) \geq 2$.

q	$A(q)/2 \geq$	reference
3	0.2464	[22]
4	0.5	[56, 86]
5	0.3636	[2, 85]
7	0.4615	[42]
8	0.75	[88]
11	0.5714	[42]
13	0.6	[66]
17	0.8	[66]
19	0.8	[42]
23	0.9230	[42]
29	0.9523	[42]
31	0.9523	[42]

Chapter 6

Conclusion

In this thesis, we investigated various aspects concerning maximal function fields over finite fields, with a particular focus on Weierstrass semigroups and their applications to Algebraic Geometry codes. In this concluding chapter, we summarize the main results that we obtained and reflect on some ideas for possible future research.

In Chapter 3, we computed the Weierstrass semigroups at all the places of the maximal function field $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$, which has the peculiarity of having the third possible largest genus in the spectrum of genera of maximal function fields. As a consequence of our results on the Weierstrass semigroups, we were also able to determine the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$. Our results show, quite surprisingly, that $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)$ has several different types of Weierstrass semigroups and that the set of its Weierstrass places is considerably richer than the set $\mathcal{O} \cup \mathfrak{R}$, which corresponds to the set of $\mathbb{F}_{q^2}$-rational places of $\mathbb{F}_{q^2}(\mathcal{X}_3)$, in the constant field extension $\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(\mathcal{X}_3)$. This behaviour had never been observed before, in any of the other maximal function fields for which the Weierstrass places are known. On the other hand, the determination of $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ shows that the function field does not seem to be particularly special with respect to its automorphisms, in the sense that, except for $q = 2, 5, 8$, the full automorphism group $\mathrm{Aut}(\overline{\mathbb{F}}_{q^2}(\mathcal{X}_3))$ consists precisely of the automorphisms inherited from the Hermitian function field. An interesting problem to be addressed in future research could for instance be the study of the Weierstrass

semigroups at the places of the two other known maximal function fields with the third largest genus, namely $\overline{\mathbb{F}}_{q^2}(\mathcal{Y}_3)$ and $\overline{\mathbb{F}}_{q^2}(\mathcal{Z}_3)$, with notations as in Chapter 3. Indeed, the full understanding of Weierstrass semigroups, Weierstrass places and automorphisms of these function fields might constitute an important step towards the characterization of maximal function fields with the third genus. Techniques involving the knowledge of these objects have in fact already been used for obtaining characterization results regarding other function fields, see for instance [26], [1], [28] and [84].

In Chapter 4, we determined the two-point Weierstrass semigroups at certain pairs of places of the Beelen-Montanucci function fields $\mathbb{F}_{q^{2n}}(\mathcal{BM}_n)$, for all $n \geq 3$ odd, and of the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$. In both cases, we used the results obtained on the semigroups in order to study two-point AG codes from the considered function fields. In the case of the Beelen-Montanucci function fields, it is interesting to note that we find in several cases AG codes with better parameters with respect to the comparable ones studied in [5] and constructed from the Garcia-Güneri-Stichtenoth function fields. In the case of the Skabelund function field $\mathbb{F}_{q^4}(\tilde{\mathcal{S}}_q)$, it is instead of interest to observe that, for all the two-point codes considered, the minimum distance is always at least that of the best comparable one-point code of the same dimension. However, in our discussion, we used a weaker version of the generalized order bound introduced in [8]. Therefore, it would be interesting to use sharper versions of the order bound (or possibly other bounds) in order to estimate the distance of the considered two-point codes.

Finally, in Chapter 5, we determined lower and upper bounds for the constant $D(q)$ introduced by M. Homma in [49]. We used different techniques for the proofs, including some based on the knowledge of the Weierstrass semigroups at certain places of a specific tower of function fields. Items 1 and 3 of Theorem 5.1 always improve the bounds for $D(q)$ previously obtained in [49], while Item 2 gives improvements only for values of $q \leq 31$, as pointed out in Remark 5.5. The newly computed bounds contribute to advance the understanding of the asymptotic behavior of the number of rational points of projective curves over $\mathbb{F}_q$, when the degree d of the curve becomes large with respect to q. On the other hand, we do not know whether the bounds stated in Item 1 and 3 of Theorem 5.1 are sharp, and the exact value of $D(q)$ remains unknown for all q. Therefore, further investigations on $D(q)$ and its relation with Ihara's constant $A(q)$ could be interesting, in order to understand more thoroughly the asymptotic behaviour of rational points of projective curves over $\mathbb{F}_q$.

Bibliography

[1] M. Abdón and F. Torres, *On maximal curves in characteristic two*, Manuscripta Mathematica, 99 (1999), pp. 39–53.

[2] B. Angles and C. Maire, *A note on tamely ramified towers of global function fields*, Finite Fields and Their Applications, 8 (2002), pp. 207–215.

[3] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves, Vol. 1*, vol. 267 of Grundlehren der mathematischen Wissenschaften, Springer-Verlag, New York, 1985.

[4] E. Ballico and S. J. Kim, *Weierstrass multiple loci of n-pointed algebraic curves*, Journal of Algebra, 199 (1998), pp. 455–471.

[5] E. Barelli, P. Beelen, M. Datta, V. Neiger, and J. S. H. Rosenkilde, *Two-point codes for the generalized GK curve*, IEEE Transactions on Information Theory, 64 (2018), pp. 6268–6276.

[6] D. Bartoli, G. Marino, A. Neri, and L. Vicino, *Exceptional scattered sequences*, arXiv preprint arXiv:2211.11477, (2022).

[7] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Moscow Mathematical Journal, 15 (2015), pp. 1–29.

[8] P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields and Their Applications, 13 (2007), pp. 665–680.

[9] P. Beelen, L. Landi, and M. Montanucci, *Weierstrass semigroups on the Skabelund maximal curve*, Finite Fields and Their Applications, 72 (2021), p. 101811.

[10] P. Beelen and M. Montanucci, *A new family of maximal curves*, Journal of the London Mathematical Society, 98 (2018), pp. 573–592.

[11] P. Beelen, M. Montanucci, and L. Vicino, *On the constant D(q) defined by Homma*, Arithmetic, Geometry, Cryptography, and Coding Theory 2021, 779 (2022), p. 33.

[12] ——, *Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus*, Finite Fields and Their Applications, 92 (2023), p. 102300.

[13] P. Beelen and N. Tutaş, *A generalization of the Weierstrass semigroup*, Journal of Pure and Applied Algebra, 207 (2006), pp. 243–260.

[14] N. L. Biggs, A. T. White, et al., *Permutation groups and combinatorial structures*, vol. 33, Cambridge University Press, 1979.

[15] A. S. Castellanos and G. C. Tizziotti, *Two-point AG codes on the GK maximal curves*, IEEE Transactions on Information Theory, 62 (2016), pp. 681–686.

[16] A. Cossidente, G. Korchmáros, and F. Torres, *Curves of large genus covered by the Hermitian curve*, Communications in Algebra, 28 (2000), pp. 4707–4728.

[17] A. Couvreur and H. Randriambololona, *Algebraic Geometry codes and some applications*, arXiv preprint arXiv:2009.01281, (2020).

[18] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer New York, NY, 1 ed., 1992.

[19] F. Delgado, *The symmetry of the Weierstrass generalized semigroups and affine embeddings*, Proceedings of the American Mathematical Society, 108 (1990), pp. 627–631.

[20] V. G. Drinfeld and S. G. Vlăduţ, *Number of points of an algebraic curve*, Functional Analysis and its Applications, 17 (1983), pp. 53–54.

[21] I. M. Duursma, *Majority coset decoding*, IEEE Transactions on Information Theory, 39 (1993), pp. 1067–1070.

[22] I. M. Duursma and K.-H. Mak, *On lower bounds for the Ihara constants A(2) and A(3)*, Compositio Mathematica, 149 (2013), pp. 1108–1128.

[23] D. Eisenbud and J. Harris, *The geometry of schemes*, vol. 197 of Graduate Texts in Mathematics, Springer, New York, NY, 1 ed., 2000.

[24] G.-L. Feng and T. R. N. Rao, *Decoding Algebraic-Geometric Codes up to the designed minimum distance*, IEEE Transactions on Information Theory, 39 (1993), pp. 37–45.

[25] ——, *A simple approach for construction of algebraic-geometric codes from affine plane curves*, IEEE Transactions on Information Theory, 40 (1994), pp. 1003–1012.

[26] R. Fuhrmann, A. Garcia, and F. Torres, *On maximal curves*, Journal of Number Theory, 67, pp. 29–51.

[27] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Mathematica, 89 (1996), pp. 103–106.

[28] ——, *On Weierstrass points and optimal curves*, Rendiconti del Circolo Matematico di Palermo Suppl., 51 (1998), pp. 25–46.

[29] W. Fulton, *Algebraic curves*, An Introduction to Algebraic Geometry, 54 (2008).

[30] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Advances in Geometry, 10 (2010), pp. 427–434.

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

[32] A. Garcia, H. Stichtenoth, and C. Xing, *On subfields of the Hermitian function field*, Compositio Mathematica, 120 (2000), pp. 137–170.

[33] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Mathematische Annalen, 343 (2009), pp. 229–245.

[34] M. Giulietti, M. Montanucci, L. Quoos, and G. Zini, *On some Galois covers of the Suzuki and Ree curves*, Journal of Number Theory, 189 (2018), pp. 220–254.

[35] D. M. Goldschmidt, *Algebraic functions and projective curves*, vol. 215 of Graduate Texts in Mathematics, Springer New York, NY, 1 ed., 2003.

[36] V. D. Goppa, *A new class of linear correcting codes*, Problemy Peredachi Informatsii, 6 (1970), pp. 24–30.

[37] ——, *A rational representation of codes and (L,g)-codes*, Problemy Peredachi Informatsii, 7 (1971), pp. 41–49.

[38] ——, *Codes associated with divisors*, Problemy Peredachi Informatsii, 13 (1977), pp. 33–39.

[39] ——, *Codes on algebraic curves*, Doklady Akademii Nauk SSSR, 259 (1981), pp. 1289–1290.

[40] ——, *Algebraico-geometric codes*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 46 (1982), pp. 762–781.

[41] B. Gunby, A. Smith, and A. Yuan, *Irreducible canonical representations in positive characteristic*, Research in Number Theory, 1 (2015), pp. 1–25.

[42] L. L. Hall-Seelig, *New lower bounds for the Ihara function A(q) for small primes*, Journal of Number Theory, 133 (2013), pp. 3319–3324.

[43] R. W. Hamming, *Error detecting and error correcting codes*, The Bell System Technical Journal, 29 (1950), pp. 147–160.

[44] G. H. Hardy, E. M. Wright, et al., *An introduction to the theory of numbers*, Oxford University Press, 1960.

[45] J. Harris, *Algebraic Geometry: a First Course*, vol. 133 of Graduate Texts in Mathematics, Springer, New York, NY, 1 ed., 1992.

[46] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, 2008.

[47] T. Høholdt, J. H. Van Lint, and R. Pellikaan, *Algebraic geometry codes*, Handbook of Coding Theory, 1 (1998), pp. 871–961.

[48] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Archiv der Mathematik, 67 (1996), pp. 337–348.

[49] ——, *A bound on the number of points of a curve in a projective space over a finite field*, Theory and applications of finite fields, 597 (2012), pp. 103–110.

[50] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, Journal of Pure and Applied Algebra, 162 (2001), pp. 273–290.

[51] ——, *Toward the determination of the minimum distance of two-point codes on a Hermitian curve*, Designs, Codes and Cryptography, 37 (2005), pp. 111–132.

[52] ——, *The complete determination of the minimum distance of two-point codes on a Hermitian curve*, Designs, Codes and Cryptography, 40 (2006), pp. 5–24.

[53] ——, *Around Sziklai's conjecture on the number of points of a plane curve over a finite field*, Finite Fields and Their Applications, 15 (2009), pp. 468–474.

[54] ——, *Sziklai's conjecture on the number of points of a plane curve over a finite field III*, Finite Fields and Their Applications, 16 (2010), pp. 315–319.

[55] ——, *Sziklai's conjecture on the number of points of a plane curve over a finite field II*, Finite Fields: Theory and Applications, Contemporary Mathematics, 518 (2010), pp. 225–234.

[56] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, Journal of the Faculty of Science, the University of Tokyo, Section 1A, 28 (1982), pp. 721–724.

[57] N. Ishii, *A certain graph obtained from a set of several points on a Riemann surface*, Tsukuba Journal of Mathematics, 23 (1999), pp. 55–89.

[58] ——, *Weierstrass gap sets for quadruples of points on compact Riemann surfaces*, Journal of Algebra, 250 (2002), pp. 44–66.

[59] W. M. Kantor, M. E. O'Nan, and G. M. Seitz, *2-transitive groups in which the stabilizer of two points is cyclic*, Journal of Algebra, 21 (1972), pp. 17–50.

[60] S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Archiv Der Mathematik, 62 (1994), pp. 73–82.

[61] S. J. Kim and J. Komeda, *The Weierstrass semigroup of a pair of Galois Weierstrass points with prime degree on a curve*, Bulletin of the Brazilian Mathematical Society, 36 (2005), pp. 127–142.

[62] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Transactions on Information Theory, 41 (1995), pp. 1720–1732.

[63] G. Korchmáros and F. Torres, *On the genus of a maximal curve*, Mathematische Annalen, 323 (2002), pp. 589–608.

[64] L. Landi, M. Timpanella, and L. Vicino, *Two-point AG codes from one of the Skabelund maximal curves*, arXiv preprint arXiv:2306.15327, (2023).

[65] L. Landi and L. Vicino, *Two-point AG codes from the Beelen-Montanucci maximal curve*, Finite Fields and Their Applications, 80 (2022), p. 102009.

[66] W.-C. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, Journal of Number Theory, 96 (2002), pp. 232–256.

[67] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography, 22 (2001), pp. 107–121.

[68] ——, *Codes from the Suzuki function field*, IEEE Transactions on Information Theory, 50 (2004), pp. 3298–3302.

[69] P. Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, Journal für die reine und angewandte Mathematik, 572 (2004), pp. 167–195.

[70] M. Montanucci and V. P. Lavorante, *AG codes from the second generalization of the GK maximal curve*, Discrete Mathematics, 343 (2020), p. 111810.

[71] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, vol. 285 of London Mathematical Society Lecture Note Series, Cambridge University Press, 2001.

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

[73] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, vol. 20 of Developments in Mathematics, Springer, New York, 1 ed., 2009.

[74] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields.*, Journal für die reine und angewandte Mathematik, 457 (1994), pp. 185–188.

[75] K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases*, IEEE Transactions on Information Theory, 41 (1995), pp. 1733–1751.

[76] G. D. V. Salvador, *Topics in the theory of algebraic function fields*, Birkhäuser, Boston, 2006.

[77] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, Comptes Rendus de l'Académie des Sciences - Series I - Mathematics, 296 (1983), pp. 397–402.

[78] C. E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, 27 (1948), pp. 379–423.

[79] D. C. Skabelund, *New maximal curves as ray class fields over Deligne-Lusztig curves*, Proceedings of the American Mathematical Society, 146 (2017), pp. 525–540.

[80] H. Stichtenoth, *Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers*, Archiv der Mathematik, 33 (1979), pp. 357–360.

[81] ——, *Algebraic function fields and codes*, vol. 254 of Graduate Texts in Mathematics, Springer, Berlin, 2 ed., 2009.

[82] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proceedings of the London Mathematical Society, 3 (1986), pp. 1–19.

[83] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields and Their Applications, 14 (2008), pp. 41–43.

[84] S. Tafazolian and F. Torres, *On the Ree curve*, Journal of Pure and Applied Algebra, 223 (2019), pp. 3831–3842.

[85] A. Temkine, *Hilbert class field towers of function fields over finite fields and lower bounds for A(q)*, Journal of Number Theory, 87 (2001), pp. 189–210.

[86] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, *Modular-curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Mathematische Nachrichten, 109 (1982), pp. 21–28.

[87] O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1, Van Nostrand, 1959.

[88] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in International Conference on Fundamentals of Computation Theory, Springer, 1985, pp. 503–511.