Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica

Wanderson Tenorio

Generalized Weierstrass semigroups and codes

Semigrupos de Weierstrass generalizados e códigos

CAMPINAS
2017

Wanderson Tenorio

Generalized Weierstrass semigroups and codes

Semigrupos de Weierstrass generalizados e códigos

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Thesis presented to the Institute of Mathematics, Statistics and Scientific Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Doctor in Mathematics.

Orientador: Fernando Eduardo Torres Orihuela

Coorientador: Carlos Munuera Gómez

Este exemplar corresponde à versão final da tese defendida pelo aluno Wanderson Tenorio, e orientada pelo Prof. Dr. Fernando Eduardo Torres Orihuela.

Campinas
2017

Agência(s) de fomento e nº(s) de processo(s): CNPq, 159852/2014-5, 201584/2015-8; CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

T258g

Tenorio, Wanderson, 1989-
Generalized Weierstrass semigroups and codes / Wanderson Tenorio. – Campinas, SP : [s.n.], 2017.

Orientador: Fernando Eduardo Torres Orihuela.
Coorientador: Carlos Munuera Gómez.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Weierstrass, Semigrupos de. 2. Poincaré, Séries de. 3. Curvas Castle. 4. Códigos algébricos-geométricos. I. Torres Orihuela, Fernando Eduardo,1961-. II. Munuera Gómez, Carlos. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Semigrupos de Weierstrass generalizados e códigos
Palavras-chave em inglês:
Weierstrass semigroups
Poincaré series
Castle curves
Algebraic-geometric codes
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Fernando Eduardo Torres Orihuela [Orientador]
Julio José Moyano-Fernández
Cícero Fernandes de Carvalho
Herivelto Martins Borges Filho
Jose Gilvan de Oliveira
Data de defesa: 22-02-2017
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 22 de fevereiro de 2017 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). FERNANDO EDUARDO TORRES ORIHUELA

Prof(a). Dr(a). JULIO JOSÉ MOYANO-FERNÁNDEZ

Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO

Prof(a). Dr(a). HERIVELTO MARTINS BORGES FILHO

Prof(a). Dr(a). JOSE GILVAN DE OLIVEIRA

A Ata da defesa com as respectivas assinaturas dos membros
encontra-se no processo de vida acadêmica do aluno.

To my parents, my brother, and my girlfriend.

Acknowledgement

I would like to express my special appreciation and sincere gratitude to my advisor, Professor Fernando Eduardo Torres Orihuela, for all his support, comprehension, and encouragement that were essential to making this work possible.

I am also very thankful to my co-advisor Professor Carlos Munuera, for his support and attention during my visit to the University of Valladolid/Spain, and for many useful discussions and advice.

I would like to thank the committee members, Professor Julio José Moyano-Fernández, Professor Cícero Fernandes de Carvalho, Professor Herivelto Martins Borges Filho, and Professor Jose Gilvan de Oliveira, for their valuable comments and suggestions that helped me to improve the exposition of this work.

Many thanks to the Department of Algebra, Analysis, Geometry, and Topology of the University of Valladolid for the hospitality and support so that I could enjoy the nice academic environment of that university. In particular, special thanks to Professor Antonio Campillo for his generous availability for stimulating conversations.

I would like to thank all my friends during my stay at UNICAMP. Special thanks to Aydee, Eduardo, Felipe, Jhony, Juliana, Kamila, Stephanie, Thais, and Vladimir for their friendship and constant support in Campinas. Many thanks also to Steve, Paulo César, and Matheus for our interesting and pleasant meetings during the CAta Seminar.

I would like to thank my family to whom this thesis is dedicated: my parents Moisés and Fátima, my brother William, and my girlfriend Daniella. For their love, encouragement, and unconditional support along all this journey in Campinas.

Finally, I thank CAPES and CNPq for their important financial support during my doctoral studies.

Resumo

Semigrupos de Weierstrass generalizados associados a vários pontos de uma curva algébrica têm sido uma ferramenta importante no estudo de códigos algébricos-geométricos. Neste contexto este trabalho lida com a estrutura de semigrupos de Weierstrass generalizados em vários pontos. Apresentamos uma descrição destes objetos que nos permite obter propriedades a respeito da estrutura aritmética de divisores suportados nos pontos especificados e seus espaços de Riemann-Roch correspondentes. Esta caracterização nos possibilita mostrar que as séries de Poincaré associadas a semigrupos de Weierstrass generalizados carregam informação essencial para descrever inteiramente seus respectivos semigrupos. Tratamos também de códigos algébricos-geométricos construídos a partir de curvas satisfazendo condições relacionadas a estes semigrupos, as curvas do tipo Castle. Desenvolvemos este conceito para curvas multipontuadas e mostramos como os semigroupos de Weierstrass generalizados podem ser usados para estudar os parâmetros de códigos multipontuais sobre tais curvas. Além disso, apresentamos algumas aplicações das técnicas Castle para a construção de códigos quânticos e códigos com localidade.

Palavras-chave: semigrupos de Weierstrass generalizados, séries de Poincaré, curvas Castle, códigos algébricos-geométricos.

Abstract

Generalized Weierstrass semigroups associated to several points of an algebraic curve have been an important tool in the study of algebraic-geometric codes. In this setting, this work deals with the structure of generalized Weierstrass semigroups at several points. We present a description that enables us to derive properties concerned with the arithmetical structure of divisors supported on the specified points and their corresponding Riemann-Roch spaces. This characterization allows us to show that the Poincaré series associated to generalized Weierstrass semigroups carry essential information to describe entirely their respective semigroups. We also address algebraic-geometric codes arising from curves satisfying conditions related to these semigroups, the curves of Castle type. We develop this concept for multi-pointed curves and show how the generalized Weierstrass semigroups can be used to study the parameters of multipoint codes on such curves. In addition, we present some applications of Castle techniques to the construction of quantum codes and codes with locality.

Keywords: generalized Weierstrass semigroups, Poincaré series, Castle curves, algebraic-geometric codes.

Contents

Introduction

Since the appearance of the theory of Weierstrass points in the 19th century to Riemann surfaces and its generalization in the 1930s to curves defined over fields of any characteristic, its objects have contributed to the development of many areas, theoretical and applied. More recently, with the successful construction of linear error-correcting codes through algebraic-geometric tools by Goppa [Gop81], the Weierstrass semigroups at either one or several points have played a crucial role in the study of these combinatorial objects. These codes are obtained by evaluating functions of an algebraic curve $\mathcal{X}$ (defined over a finite field) at rational points of $\mathcal{X}$, the so-called *algebraic geometric code*. When these functions are allowed to have only a specific pole on $\mathcal{X}$, the code obtained is said a *one-point code*. Otherwise, it is called a *multipoint code*.

The notion of Weierstrass semigroups at several points appeared in [Arb+85] for pairs. They were introduced as subsemigroups of $\mathbb{N}_0^2$, a natural extension of Weierstrass semigroups at a point. Kim [Kim94] and Homma [Hom96] were the first to consider the arithmetical properties of these semigroups. They studied the cardinality of the complement of these objects in $\mathbb{N}_0^2$ and developed a method to construct them by the knowledge of the Weierstrass numerical semigroups at each point. Similar arithmetical questions were treated for more points; see [BK98].

Later, Matthews [Mat01] used the arithmetical structure of the Weierstrass semigroups at pairs given by the works [Hom96; Kim94] to study the two-point algebraic-geometric codes. The techniques employed allowed improving the Goppa bound for the minimum distance of such codes. Besides, they derived codes with better parameters than comparable one-point codes constructed on the same curve and conclude that there exist multipoint codes that can not be obtained as punctured one-point codes. The outcomes of this new approach became the multipoint codes a central object of investigation and lead to the development of the theory of Weierstrass semigroups at several points. Many works arose in this setting, we refer e.g. to [HK01; Mat04; CT05]. In particular, Matthews [Mat04] formulated a method to constructed Weierstrass semigroups, extending the construction of [Hom96; Kim94] to several points.

Another type of natural extension of the notion of Weierstrass numerical semigroups to several points is due to Delgado [Del90], who introduced the generalized Weierstrass semigroup at ℓ specified points as a subsemigroup of $\mathbb{Z}^\ell$ instead of $\mathbb{N}_0^\ell$. Interpreting the Weierstrass

numerical semigroups as a semigroup of orders of functions that are regular outside the ℓ points, he observed that his definition was more general than that given in [Arb+85]. Nevertheless, his focus was on the consequences of a similar concept of symmetry for numerical semigroups, and it was not connected applications until 2006 when Beelen and Tutaş [BT06] revisited the definition to introduce new objects in the approach and to study their properties. It was used again by Beelen [Bee07] to formulate a bound of the order type on the minimum distance of arbitrary algebraic geometric codes, which was later improved in the sequence of works [DK09], [DP10], and [DKP11] by Duursma, Kirov, and Park.

However, despite the recent utilization of generalized Weierstrass semigroups, no method related to their construction has been developed. Since this approach is more embracing than the classical one from [Arb+85] and has been used to applications, is natural to ask whether one can extend the known techniques to the general case.

In this work, we deal with the arithmetical structure of generalized Weierstrass semigroups and issues that arise from this concept. In this direction, we also aim to provide a tool to the study of classical and recent topics in coding theory as quantum codes and locally recoverable codes under the perspective of the algebraic-geometric codes. These subjects have been trends in coding theory mainly for their applications to new and sophisticated systems of communication, and have recently received much attention. With this purpose, our program is to use the techniques developed for the classical setting from the aforementioned works to furnish a characterization of the generalized Weierstrass semigroups and to thus explore related problems, as for instance the Poincaré series associated to these semigroups and their systematic usage in the analysis of algebraic-geometric codes. Regarding applications to codes, we use algebraic geometry techniques, specially those related to the Castle curves, to contribute to the construction of these new objects in coding theory.

We now give an outline of the content of this thesis:

Chapter 1 contains a short introduction to the preliminaries that will be used throughout this work. In Section 1.1 we recall some notions related to error-correcting codes. In Section 1.2 we present the background on algebraic curves, which we use in Section 1.3 to remember the definition of algebraic-geometric codes and their main properties. These themes are classical and can be found e.g. in [TVN07].

Chapter 2 presents a study of some aspects of generalized Weierstrass semigroups, which is a refinement of the classical notion of Weierstrass semigroups at several points. Section 2.1 is preparatory to what will be used in the chapter. There we set up notation and terminology, and discuss some properties of these objects. In Section 2.2 we develop a characterization of generalized Weierstrass semigroups based on least upper bounds of absolute maximals (Theorem 2.2.5), establishing a notion of generating sets for such semigroups. While these generators constitute an infinite set, we prove (Theorem 2.2.8) they can be finitely determined. Section

2.3 shows the consequences of the asserted properties from Section 2.2 to the Poincaré series associated to the Weierstrass semigroups. We conclude (Theorem 2.3.3) that the Poincaré series carry sufficient information to construct the whole semigroup, and furthermore can be finitely determined by their semigroup polynomials. Section 2.4 introduces a simple numerical equivalence for symmetric generalized Weierstrass semigroups and derives functional equations for their corresponding Poincaré series.

Chapter 3 gives the concept of multi-pointed curves of Castle type, which is a natural extension of the idea behind pointed curves that are Castle and weak Castle. Section 3.1 is introductory and reviews some features of Castle and weak Castle curves, as well as properties of one-point algebraic geometric codes constructed from them, the so-called Castle and weak Castle codes. In Section 3.2 we introduce the notion of multi-pointed curves of Castle type (Definition 3.2.1) and provide some examples of classical multi-pointed curves satisfying such conditions. Multipoint algebraic geometric codes on multi-pointed curves of Castle type conditions are considered in Section 3.3. There we use the properties (Proposition 3.2.5) to show that the parameters of such codes can be studied through the generalized Weierstrass semigroups

Chapter 4 addresses the use of weak Castle codes and their trace codes to produce quantum error-correcting codes from the CSS constructions. Section 4.1 summarizes the mathematical setting to quantum error-correction. We also recall the CSS constructions of quantum codes from nested classical codes and give some procedures to obtain quantum codes from an increasing sequence of linear codes. Since weak Castle codes have a natural sequence, in Section 4.2 we provide quantum codes from such sequences. We also give sufficient conditions to ensure the self-orthogonality of weak Castle codes (Proposition 4.2.5). In Section 4.3 we present computational examples of quantum codes obtained from curves by CSS constructions. We compare their parameters with codes from the literature. Once we have presented some weak Castle codes defined over large finite fields, Section 4.4 explores the trace and subfield subcode construction of such codes to produce quantum codes over smaller fields through CSS constructions. We show a sufficient condition to obtain the self-orthogonality of traces of Castle codes (Proposition 4.4.6). The results of this chapter have been presented at the Third IMAC and Singacom Day on Algebraic Applications to Information Theory, Castellón/Spain, May 2016, and published in [MTT16].

Chapter 5 provides some contributions to the construction of locally recoverable codes from algebraic curves. Section 5.1 is introductory. There we give the notion locality in coding theory and present the construction of locally recoverable codes based on Reed-Solomon codes whose local recovery procedure relies on polynomial interpolation. In Section 5.2 we review the construction of locally recoverable codes arising from algebraic curves, which is a natural extension of ideas of the Reed-Solomon-like construction given in Subsection 5.1.1, and give a refinement of this approach that produces improvements in the parameters of such codes (Theorem 5.2.5). We conclude the section by giving a family of locally recoverable codes derived

from curves with a simpler local recovery procedure than polynomial interpolation (Proposition 5.2.14). The contents of this chapter have been submitted for publication [MT16].

Chapter 1

Background

This chapter is dedicated to set up the terminology and notation, as well as to enunciate the basic results that will be used throughout the thesis. Our exposition on this background material follows [TVN07], [Mor91], and [Sti09].

A brief introduction to error-correcting codes is made in Section 1.1, where we specially remember some aspects concerned to the class of linear codes. Section 1.2 presents a short introduction to the theory of algebraic curves. We mostly focus to the arithmetical proprieties mainly on account of our interest in their applications to error-correcting codes in the positive characteristic case. The main results are the Riemann-Roch Theorem, the Residue formula, and the Riemann-Hurwitz genus formula, which are classical and can be found e.g. in [HKT08] and [Ser12]. The chapter ends with the Goppa construction of linear codes in Section 1.3, which is based on algebraic curves defined over finite fields. This relates the subjects from the preceding sections, yielding an arithmetic/algebraic-geometric viewpoint to the combinatorial objects from the first section. For further references concerning these topics, we refer the reader to [HKT08; Duu08; MO15; vv88; Ser12; HVP98].

As standard notation to be used throughout text, we will let $\mathbb{Z}$ denote the set of integers, $\mathbb{N}_0$ denote set of non-negative integers, $\mathbb{C}$ denote the field of complex numbers, and $\mathbb{F}_q$ denote the finite field with q elements, for q a power of a prime number.

1.1 Error-correcting codes

Let A be a finite set. For n a positive integer, the Hamming distance between two elements $\mathbf{x} = (x_1, ..., x_n)$ and $\mathbf{y} = (y_1, ..., y_n)$ in the set $A^n = \underbrace{A \times \cdots \times A}_{n \text{ times}}$ is defined by

$$d(\mathbf{x}, \mathbf{y}) := \#\{i \ : \ x_i \neq y_i\}.$$

Denote by q the cardinality of A. A *q-ary code C of length n over an alphabet A* is a non-empty subset of A^n. The cardinality $M := \#C$ and its log-cardinality $k := \log_q M$ are important

parameters of C. The *minimum distance* of C is

$$d = d(C) := \min\{d(\mathbf{x}, \mathbf{y}) \ : \ \mathbf{x}, \mathbf{y} \in C, \ \mathbf{x} \neq \mathbf{y}\}.$$

A code with these parameters is usually denoted by $[n, M, d]_q$, or $[n, k, d]_q$. Its elements are called *codewords* and its components are the *coordinates*, or *symbols*.

Since error-correcting codes are designed keeping in mind their effectiveness in applications, it is appropriated to enhance the alphabet A with some algebraic structure in order to obtain improved methods in the treatment of the codes. In this way, we have the notion of a linear code.

Let $\mathbb{F}_q$ be the finite field of cardinality q. A *q-ary linear code* C of length n is a linear subspace of $\mathbb{F}_q^n$. For a linear code C, its log-cardinality k agrees with the $\mathbb{F}_q$-dimension of the subspace C, called in this case the *dimension* of C. The minimum distance d of C coincides with

$$\min\{\mathrm{wt}(\mathbf{x}) \ : \ \mathbf{x} \in C, \ \mathbf{x} \neq 0\},$$

where $\mathrm{wt}(\mathbf{x}) := \#\{i \ : x_i \neq 0\}$ is said the *weight* of a vector $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{F}_q^n$. The set $\{i \ : x_i \neq 0\}$ is also called the *support* of $\mathbf{x}$, denoted by $\mathrm{supp}(\mathbf{x})$.

The relationship among the parameters of an $[n, k, d]_q$ linear code C can be expressed by the Singleton bound

$$d \leq n - k + 1; \tag{1.1.1}$$

see [TVN07, Prop. 1.1.41]. A linear code attaining this bound is called a *maximum distance separable*, or *MDS code*.

Denote by $\langle -, - \rangle$ the usual (Euclidean) inner product in $\mathbb{F}_q^n$, $\langle \mathbf{x}, \mathbf{y} \rangle = \sum x_i y_i$. Given a linear code C over $\mathbb{F}_q$, the *dual* of C is the orthogonal complement of C in $\mathbb{F}_q^n$

$$C^\perp := \{\mathbf{y} \in \mathbb{F}_q^n \ : \ \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}. \tag{1.1.2}$$

Observe that $C^\perp$ is indeed a linear code. As an immediate consequence of the definition, the dimension of $C^\perp$ is $n - k$, with k the dimension of C, and $(C^\perp)^\perp = C$. We say that C is *self-dual* if $C = C^\perp$, and *self-orthogonal* if $C \subseteq C^\perp$, that is if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ for all $\mathbf{x}, \mathbf{y} \in C$.

Denote by $*$ the coordinate-wise multiplication in $\mathbb{F}_q^n$, $\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$. Given an n-tuple $\mathbf{x}$ of nonzero elements in $\mathbb{F}_q$, the map $\mathbb{F}_q^n \to \mathbb{F}_q^n$, $\mathbf{y} \mapsto \mathbf{x} * \mathbf{y}$, is linear and bijective. Furthermore it is an isometry for the Hamming metric. For a linear code C over $\mathbb{F}_q$, we shall write $\mathbf{x} * C = \{\mathbf{x} * \mathbf{y} \ : \ \mathbf{y} \in C\}$. Two codes $C_1, C_2 \subseteq \mathbb{F}_q^n$ are called *formally equivalent* if there

exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_1 = \mathbf{x} * C_2$. Similarly, we say that C is *formally self-dual* if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $\mathbf{x} * C = C^\perp$, and *formally self-orthogonal* if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $\mathbf{x} * C \subseteq C^\perp$.

As a notation, given a vector $\mathbf{x} \in \mathbb{F}_q^n$ and an integer t, we let $\mathbf{x}^t = (x_1^t, \ldots, x_n^t)$ (when this makes sense). For $X \subseteq \mathbb{F}_q^n$, let $X^t := \{\mathbf{x}^t : \mathbf{x} \in X\}$.

Lemma 1.1.1. Let C be a linear code over $\mathbb{F}_q$ and $\mathbf{x} \in ({\mathbb{F}_q}^\times)^n$. Then $\mathbf{x} * C^\perp = (\mathbf{x}^{-1} * C)^\perp$.

Proof. Since both codes have equal dimension, it suffices to prove one inclusion. Let $\mathbf{v} \in \mathbf{x} * C^\perp$. There exists $\mathbf{a} \in C^\perp$ such that $\mathbf{v} = \mathbf{x} * \mathbf{a}$. Then $\mathbf{v} * \mathbf{x}^{-1} = \mathbf{a} \in C^\perp$, hence $0 = \langle (\mathbf{v} * \mathbf{x}^{-1}), \mathbf{c} \rangle = \langle \mathbf{v}, (\mathbf{x}^{-1} * \mathbf{c}) \rangle$ for all $\mathbf{c} \in C$, so $\mathbf{v} \in (\mathbf{x}^{-1} * C)^\perp$. □

Let us consider $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ the trace map (associated to the field extension $\mathbb{F}_{q^r}|\mathbb{F}_q$) given by $\mathrm{tr}(x) = x + x^q + \cdots + x^{q^{r-1}}$. Consider also its coordinate-wise extension $\mathrm{tr} : \mathbb{F}_{q^r}^n \to \mathbb{F}_q^n$ by $\mathrm{tr}(\mathbf{x}) = (\mathrm{tr}(x_1), \ldots, \mathrm{tr}(x_n))$. Both maps are $\mathbb{F}_q$-linear and surjective.

Definition 1.1.2. Let $C \subseteq \mathbb{F}_{q^r}^n$ be a code over $\mathbb{F}_{q^r}$. The *subfield subcode* of C over $\mathbb{F}_q$ is

$$C|\mathbb{F}_q := C \cap \mathbb{F}_q^n.$$

The *trace code* of C is

$$\mathrm{tr}(C) := \{\mathrm{tr}(\mathbf{x}) \ : \ \mathbf{x} \in C\}.$$

The above codes over $\mathbb{F}_q$ arising from a code over $\mathbb{F}_{q^r}$ are related by the following result.

Theorem 1.1.3 (Delsarte). For C a code over $\mathbb{F}_{q^r}$ holds

$$(C|\mathbb{F}_q)^\perp = \mathrm{tr}(C^\perp).$$

Proof. See [Sti09, Th. 9.1.2]. □

1.2 Algebraic curves

Let $\mathtt{k}$ be a perfect field. By a *projective algebraic curve* $\mathcal{X}$ defined over $\mathtt{k}$, we mean a one-dimensional projective variety defined over $\mathtt{k}$, that is to say, the ideal of $\mathcal{X}$ is generated by homogeneous polynomials with coefficients in $\mathtt{k}$. We say that $\mathcal{X}$ is geometrically irreducible if the ideal of $\mathcal{X}$ is prime ideal in the ring of polynomials with coefficients in $\bar{\mathtt{k}}$, an algebraic closure of $\mathtt{k}$. A point on $\mathcal{X}$ is called a *rational point* if there exists a representative for P with all homogeneous coordinates in $\mathtt{k}$.

Let $\mathtt{k}(\mathcal{X})$ be the field of $\mathtt{k}$-rational functions of $\mathcal{X}$, that is, quotient of homogeneous polynomials over $\mathtt{k}$ of same degree. This is a one-variable algebraic function field over $\mathtt{k}$, that is, a

finite extension of some rational function field over $\mathtt{k}$.

Let P be a point on $\mathcal{X}$. Let $\mathcal{O}_P$ be the set of $\mathtt{k}$-rational functions that are regular at P, which is in fact a local ring with maximal ideal denoted by $\mathfrak{m}_P$. Let $\mathtt{k}(P) = \mathcal{O}_P/\mathfrak{m}_P$ be the residue class field of P which is a finite extension of $\mathtt{k}$. A point P is called non-singular if $\dim(\mathfrak{m}_P/\mathfrak{m}_P^2) = 1$. Otherwise, P is called singular. Equivalently, P is non-singular if and only if $\mathcal{O}_P$ is a discrete valuation ring. In this case, an element t_P such that $\mathfrak{m}_P = t_P\mathcal{O}_P$ is called a local parameter of $\mathcal{X}$ at P, and we have associated to P a valuation on $\mathtt{k}(\mathcal{X})$, that is, a surjective function $v_P : \mathtt{k}(\mathcal{X})^\times \to \mathbb{Z}$ satisfying

(i) $v_P(fg) = v_P(f) + v_P(g)$;

(ii) $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$;

(iii) $v_P(c) = 0$ for $c \in \mathtt{k}^\times$.

Moreover, any rational function has a unique expansion into a Laurent series in a local parameter t_P at P. We thus have a field embedding $\mathtt{k}(\mathcal{X}) \hookrightarrow \mathtt{k}((t_P))$. A curve is called non-singular if every point on $\mathcal{X}$ is non-singular.

Let $\mathcal{X}$ be a non-singular, geometrically irreducible, projective curve defined over $\mathtt{k}$. A *divisor* D on $\mathcal{X}$ is a formal finite sum of points of $\mathcal{X}$, $D = \sum n_P P$, with n_P integers. The *support* of a divisor D is the set

$$\{P \in \mathcal{X} \ : \ n_P \neq 0\},$$

usually denoted by $\mathrm{Supp}(D)$. We denote the set of divisor on $\mathcal{X}$ by $\mathrm{Div}(\mathcal{X})$, which is an Abelian group with the natural addition of divisors. The degree $\deg(D)$ of a divisor $D = \sum n_P P \in \mathrm{Div}(\mathcal{X})$ is the integer $\sum n_P \deg(P)$. We say D is *effective*, $D \geq 0$, if $n_P \geq 0$ for each P on $\mathcal{X}$. This concept induces a partial order on $\mathrm{Div}(\mathcal{X})$ given by $D \geq E$ if $D - E$ is effective.

We associate to any $f \in \mathtt{k}(\mathcal{X})^\times$ a divisor by

$$\mathrm{div}(f) := \sum_{P \in \mathcal{X}} v_P(f) P,$$

called *principal divisor* of f. Since any f has finitely many zeroes and poles on $\mathcal{X}$, we thus have $\mathrm{Supp}(\mathrm{div}(f))$ is finite. Observe also that $\mathrm{div}(f)$ is a difference of two effective divisors

$$\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f),$$

where

$$\mathrm{div}_0(f) = \sum_{v_P(f)>0} v_P(f) P \qquad \text{and} \qquad \mathrm{div}_\infty(f) = \sum_{v_P(f)<0} v_P(f) P,$$

called respectively of *divisor of zeroes* and *divisor of poles* of f. It is easily seen that principal divisors on $\mathcal{X}$ form a subgroup of $\mathrm{Div}(\mathcal{X})$, denoted by $\mathrm{Princ}(\mathcal{X})$. Also, it enables us to say that two divisors $D, E \in \mathrm{Div}(\mathcal{X})$ are *linearly equivalent* and write $D \sim E$, if $D - E \in \mathrm{Princ}(\mathcal{X})$. The group $\mathrm{Div}(\mathcal{X})/\mathrm{Princ}(\mathcal{X})$ of divisor equivalence classes is called *divisor class group*. It is a finite group.

Theorem 1.2.1. The degree of a principal divisor is 0.

Given $D \in \mathrm{Div}(\mathcal{X})$, we can associate to it the set

$$\mathcal{L}(D) := \{f \in \mathtt{k}(\mathcal{X})^{\times} \ : \ \mathrm{div}(f) + D \geq 0\} \cup \{0\},$$

called the *Riemann-Roch space* of D. The set $\mathcal{L}(D)$ is a $\mathtt{k}$-vector space whose dimension we shall denote by $\ell(D)$.

Theorem 1.2.2. The dimension $\ell(D)$ of $\mathcal{L}(D)$ is finite for any $D \in \mathrm{Div}(\mathcal{X})$ and only depends on the linear equivalence class of D.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant k-morphism between projective curves. Hence we have a field embedding $f^* : \mathtt{k}(\mathcal{Y}) \hookrightarrow \mathtt{k}(\mathcal{X})$ and thus the finite field extension degree $[\mathtt{k}(\mathcal{X}) : f^*(\mathtt{k}(\mathcal{Y}))]$ is called *degree* of f, denoted by $\deg(f)$. In case that $\mathcal{X}$ and $\mathcal{Y}$ are non-singular curves, f is said a *covering* of curves. Let $f : \mathcal{X} \to \mathcal{Y}$ be a covering and $P \in \mathcal{X}$ any point. The *ramification index* e_P of f at P is the integer $v_P(f^*(t_{f(P)}))$, where $t_{f(P)}$ is a local parameter of $\mathcal{Y}$ at $f(P)$. Observe that e_P is well defined and $e_P \geq 1$, since $f^*(t_{f(P)})$ vanishes at P. It satisfies $t_{f(P)} = t_P^{e_P} u$, for $u \in \mathcal{O}_P$ and t_P a local parameter of $\mathcal{X}$ at P. We say $P \in \mathcal{Y}$ is a *ramification point* of f if $e_P \geq 2$. Otherwise, we say P is *unramified*.

Given a covering $f : \mathcal{X} \to \mathcal{Y}$ and a divisor $D = \sum n_Q Q$ on $\mathcal{Y}$, we define the *pullback* of D by the divisor on $\mathcal{X}$

$$f^*(D) := \sum_{Q \in Supp(D)} \sum_{P \in f^{-1}(Q)} n_Q e_P P.$$

We thus have a map $f^* : \mathrm{Div}(\mathcal{Y}) \to \mathrm{Div}(\mathcal{X})$.

Theorem 1.2.3. For any $D \in \mathrm{Div}(\mathcal{Y})$, we have $\deg(f^*(D)) = \deg(D)\deg(f)$.

A *derivation* on $\mathcal{X}$ is a $\mathtt{k}$-linear map $d : \mathtt{k}(\mathcal{X}) \to \mathtt{k}(\mathcal{X})$ satisfying $d(f_1 f_2) = f_1 df_2 + f_2 df_1$. Denote by $\mathrm{Der}(\mathcal{X})$ the set of derivations on $\mathcal{X}$.

Theorem 1.2.4. Let t be local parameter at a point P on $\mathcal{X}$. Then there exists a unique derivation $d_t : \mathtt{k}(\mathcal{X}) \to \mathtt{k}(\mathcal{X})$ such that $d_t t = 1$. Moreover $\mathrm{Der}(\mathcal{X})$ is a one-dimensional $\mathtt{k}(\mathcal{X})$-vector space and d_t is a basis for every local parameter t at P.

A *rational differential form* on $\mathcal{X}$ is a $\mathtt{k}(\mathcal{X})$-linear map from $\mathrm{Der}(\mathcal{X})$ to $\mathtt{k}(\mathcal{X})$.

Theorem 1.2.5. The set $\Omega(\mathcal{X})$ of rational differential forms of $\mathcal{X}$ is a one-dimensional $\mathtt{k}(\mathcal{X})$-vector space and dt is a basis for every local parameter.

For any point $P \in \mathcal{X}$, let t_P be a local parameter of $\mathcal{X}$ at P. Thus for any rational differential form ω there exists an unique rational function f_P such that $\omega = f_P dt_P$. We define the *divisor* of ω by

$$\mathrm{div}(\omega) := \sum v_P(\omega)P,$$

where $v_P(\omega) := v_P(f_P)$.

The divisor class of a rational differential form on $\mathcal{X}$ is called the *canonical class* of $\mathcal{X}$ and its divisors are called *canonical divisors* of $\mathcal{X}$. Notice that the canonical divisor class definition makes sense since the quotient of two rational differential forms is a rational function on $\mathcal{X}$.

Given D a divisor on $\mathcal{X}$, define the set of rational differential forms

$$\Omega(D) := \{\omega \in \Omega(\mathcal{X})\backslash\{0\} \ : \ \mathrm{div}(\omega) - D \geq 0\} \cup \{0\},$$

which is a $\mathtt{k}$-vector space whose dimension is denoted by $i(D)$, called *speciality index* of D.

Theorem 1.2.6 (of duality)**.** Let D be a divisor on $\mathcal{X}$ and K a canonical divisor on $\mathcal{X}$ given by a rational differential form ω. Then the map $\mathcal{L}(K - D) \to \Omega(D)$ given by $f \mapsto f\omega$ is an isomorphism of $\mathtt{k}$-vector spaces. In particular, $i(D) = \ell(K - D)$.

The integer $i(0) = \ell(K)$ for all canonical divisor K is called *genus* of $\mathcal{X}$, denoted by $g(\mathcal{X})$.

Theorem 1.2.7 (Riemann-Roch)**.** For any $D \in \mathrm{Div}(\mathcal{X})$, we have

$$\begin{aligned}\ell(D) &= \deg(D) + 1 - g(\mathcal{X}) + i(D) \\ &= \deg(D) + 1 - g(\mathcal{X}) + \ell(K - D),\end{aligned}$$

where K is a canonical divisor on $\mathcal{X}$.

Proposition 1.2.8. (i) $\deg(K) = 2g(\mathcal{X}) - 2$ for any canonical divisor K on $\mathcal{X}$;

(ii) $\ell(D) = \deg(D) + 1 - g(\mathcal{X})$ for any divisor D on $\mathcal{X}$ with $\deg(D) \geq 2g(\mathcal{X}) - 1$;

(iii) K is a canonical divisor on $\mathcal{X}$ if and only if $\deg(K) = 2g(\mathcal{X}) - 2$ and $\ell(K) \geq g(\mathcal{X})$.

Let P be a point on $\mathcal{X}$. We define the *residue* of a rational differential form ω at P by

$$\mathrm{res}_P(\omega) := \mathrm{Tr}_{\mathtt{k}(P)|\mathtt{k}}(a_{-1})$$

where a_{-1} is given by the expansion of f_P into the Laurent series $\sum a_i t_P^i$ and Tr is the trace map from residue class field $\mathtt{k}(P)$ to $\mathtt{k}$.

Proposition 1.2.9. (i) $\mathrm{res}_P(\omega)$ does not depend on the choice of a local parameter t_P;

(ii) res_P is a $\mathtt{k}$-linear functional on $\Omega(\mathcal{X})$;

(iii) $\mathrm{res}_P(df) = 0$ for all $f \in \mathtt{k}(\mathcal{X})^\times$;

(iv) $\mathrm{res}_P(df/f) = v_P(f)$ for all $f \in \mathtt{k}(\mathcal{X})^\times$.

Theorem 1.2.10. If ω is a rational differential form on a non-singular projective curve, then

$$\sum_{P \in \mathcal{X}} \mathrm{res}_P(\omega) = 0. \qquad \text{(Residue formula)}$$

Let $\varphi : \mathcal{X} \to \mathcal{Y}$ be a covering of curves and let $\omega = \sum_i f_i dg_i \in \Omega(\mathcal{Y})$. Define the *pullback* of ω by

$$\varphi^*(\omega) := \sum_i \varphi^*(f_i) d\varphi^*(g_i) \in \Omega(\mathcal{X}).$$

This notion does not depend on the choice of a representation of ω. We thus have a $\mathtt{k}$-linear map $\varphi^* : \Omega(\mathcal{Y}) \to \Omega(\mathcal{X})$.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a covering of projective curves. Suppose moreover f is separable, that is the field extension $\mathtt{k}(\mathcal{X})|f^*(\mathtt{k}(\mathcal{Y}))$ is separable. For $P \in \mathcal{X}$, let $Q = f(P)$, t_P and t_Q their respective local parameters on $\mathcal{X}$ and $\mathcal{Y}$. Consider the integer

$$b_P := v_P(f^*(dt_Q)/dt_P).$$

Observe that if P is a ramification point of f then $b_P \neq 0$. Define

$$B_f := \sum b_P P \in \mathrm{Div}(\mathcal{X})$$

the so-called *ramification divisor* of f. (recall the set of ramification points of a separable covering is finite)

Theorem 1.2.11. (Riemann-Hurwitz-Zeuthen formula) Let $f : \mathcal{X} \to \mathcal{Y}$ be a separable covering of curves of degree d. Then

$$2g(\mathcal{X}) - 2 = d(2g(\mathcal{Y}) - 2) + \deg(B_f).$$

1.3 Algebraic-geometric codes

Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible algebraic curve of genus g defined over $\mathbb{F}_q$. Take two rational divisors D and G on $\mathcal{X}$ with disjoint supports and such that

D is the sum of n rational distinct points, $D = P_1 + \cdots + P_n$. For $\mathcal{P} = \mathrm{Supp}(D)$, let us consider the linear evaluation map at $\mathcal{P}$

$$\begin{array}{rccc} \mathrm{ev}_{\mathcal{P}} & : & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ & & f & \mapsto & (f(P_1), ..., f(P_n)) \end{array}.$$

The *algebraic geometry code* (or AG code) defined by the triple $(\mathcal{X}, D, G)$ via the $\mathcal{L}$-construction is the image $\mathrm{ev}_{\mathcal{P}}(\mathcal{L}(G))$, denoted by $C_{\mathcal{L}}(\mathcal{X}, D, G)$, or simply $C_{\mathcal{L}}(D, G)$ when the curve $\mathcal{X}$ is clear in the context. Its dimension is $k = \ell(G) - \ell(G - D)$ and its minimum distance d satisfies the so-called *Goppa bound*

$$d \geq n - \deg(G). \tag{1.3.1}$$

Remark 1.3.1. Observe that $C_{\mathcal{L}}(D, G)$ reaches the Goppa bound if and only if there exists divisor D' on $\mathcal{X}$ such that $0 \leq D' \leq D$, $\deg(D') = \deg(G)$ and $\ell(G - D') \leq 0$; see [Sti09, Rmk. 2.2.5].

The so-called *improved Goppa bound* gives us

$$d \geq n - \deg(G) + \lambda_{a+1}, \tag{1.3.2}$$

where $a = \ell(G - D)$ is the *abundance* of $C_{\mathcal{L}}(D, G)$ and, for an integer $r \geq 1$, λ_r is the r-th *gonality* of $\mathcal{X}$ defined by

$$\lambda_r := \min\{\deg(A) \ : \ A \text{ is a rational divisor on } \mathcal{X} \text{ with } \ell(A) \geq r\}.$$

The sequence $(\lambda_r)_{r \geq 1}$ is called the *gonality sequence* of $\mathcal{X}$.

Let us consider the linear residue map at $\mathcal{P}$

$$\begin{array}{rccc} \mathrm{res}_{\mathcal{P}} & : & \Omega(G - D) & \longrightarrow & \mathbb{F}_q^n \\ & & \omega & \mapsto & (\mathrm{res}_{P_1}(\omega), ..., \mathrm{res}_{P_n}(\omega)). \end{array}$$

The *algebraic geometry code* defined by the triple $(\mathcal{X}, D, G)$ via the Ω-construction is the image $\mathrm{res}_{\mathcal{P}}(\Omega(G - D))$, denoted by $C_{\Omega}(\mathcal{X}, D, G)$, or simply $C_{\Omega}(D, G)$ for short. The dimension and minimum distance of $C_{\Omega}(D, G)$ satisfy respectively

$$k = i(G - D) - i(G) \qquad \text{and} \qquad d \geq \deg(G) - (2g - 2). \tag{1.3.3}$$

As consequence of residue formula, the constructions above are related by the following result.

Theorem 1.3.2. The codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ are dual of each other, that is

$$C_{\Omega}(D, G) = C_{\mathcal{L}}(D, G)^{\perp}.$$

Proof. Since by Riemann-Roch theorem $C_\Omega(D,G)$ and $C_\mathcal{L}(D,G)^\perp$ have the same dimension, it is equivalent to show that we have $\langle \mathbf{x},\mathbf{y}\rangle = 0$ for $\mathbf{x} = \mathrm{ev}_\mathcal{P}(f)$ with $f \in \mathcal{L}(G)$ and $\mathbf{y} = \mathrm{res}_\mathcal{P}(\omega)$ with $\omega \in \Omega(D-G)$. Notice that $\langle \mathbf{x},\mathbf{y}\rangle = \sum_{i=1}^n f(P_i)\,\mathrm{res}_{P_i}(\omega) = \sum_{i=1}^n \mathrm{res}_{P_i}(f\omega)$. As $\mathrm{div}(f) \geq -G$ and $\mathrm{div}(\omega) \geq G - D$, we get $\mathrm{div}(f\omega) \geq -D$. Hence the differential form does not have poles outside $\mathcal{P}$, and consequently it does not have non-zero residue outside $\mathcal{P}$. It follows from Residue formula that

$$\sum_{i=1}^n \mathrm{res}_{P_i}(f\omega) = \sum_{P\in\mathcal{X}} \mathrm{res}_{P_i}(f\omega) = 0.$$

□

The following result shows the equivalence between the $\mathcal{L}$ and Ω constructions.

Proposition 1.3.3. The codes $C_\Omega(D,G)$ and $C_\mathcal{L}(D,\mathrm{div}(\omega)-G+D)$ are formally equivalent. Precisely, for any $\omega \in \Omega(\mathcal{X})$ with $v_{P_i}(\omega) = -1$, the equality holds

$$C_\Omega(D,G) = \mathbf{x} * C_\mathcal{L}(D,\mathrm{div}(\omega)-G+D)$$

where $\mathbf{x} = (\mathrm{res}_{P_1}(\omega),\ldots,\mathrm{res}_{P_n}(\omega)) \in (\mathbb{F}_q^\times)^n$.

Proof. Notice that as $v_{P_i}(\omega) = -1$, we have D and $\mathrm{div}(\omega)-G+D$ with disjoint supports. By Theorem 1.2.6 (of duality) we have the isomorphism $\mathcal{L}(\mathrm{div}(\omega)-G+D) \to \Omega(G-D)$ given by $f \mapsto f\omega$. Since $\mathrm{res}_{P_i}(f\omega) = f(P_i)\,\mathrm{res}_{P_i}(\omega)$, we have the assertion by using Theorem 1.3.2. □

The previous result is refined as follows.

Proposition 1.3.4. There exists a differential form $\eta \in \Omega(\mathcal{X})$ such that $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1,\ldots,n$, and in particular

$$C_\Omega(D,G) = C_\mathcal{L}(D,\mathrm{div}(\eta)-G+D).$$

Proof. See [Sti09, Lem. 2.2.9, Prop. 2.2.10]. □

Proposition 1.3.5. (a) Suppose $G_1, G_2 \in \mathrm{Div}(\mathcal{X})$ with $G_1 \sim G_2$ and disjoint support from $\mathcal{P}$. Then $C_\mathcal{L}(D,G_1)$ and $C_\mathcal{L}(D,G_2)$ are formally equivalent. The same holds for $C_\Omega(D,G_1)$ and $C_\Omega(D,G_2)$.

(b) Conversely, if a code $C \subseteq \mathbb{F}_q^n$ is formally equivalent to $C_\mathcal{L}(D,G)$ (resp. $C_\Omega(D,G)$) then there exists $G' \in \mathrm{Div}(\mathcal{X})$ with $G' \sim G$ and disjoint support from $\mathcal{P}$ such that $C = C_\mathcal{L}(D,G')$ (resp. $C_\Omega(D,G')$).

Proof. See [Sti09, Prop. 2.2.14]. □

Chapter 2

Generalized Weierstrass semigroups and their Poincaré series

Weierstrass semigroups at a rational point on an algebraic curve is a classical matter in the theory of Weierstrass points. They are related to dimensions of Riemann-Roch spaces associated, and from this particular relation, we have their many applications. Theoretical questions concerning these objects are still an active line of investigation as e.g. understanding their role in the setting of numerical semigroups or when numerical semigroups arise from a pointed curve.

The notion of Weierstrass semigroups admits interpretations that allow us to extend this concept to several rational points of an algebraic curve in two different approaches so that we also have the dimensions of the corresponding Riemann-Roch spaces involved, the so-called *Weierstrass semigroups* and *generalized Weierstrass semigroups* at several points. These extensions constitute a recent topic of research that has received substantial attention and developed many techniques to understand their arithmetical structures, mainly because of their applications to coding theory.

On the other hand, the notion of Poincaré series arose as an arithmetic/combinatorial tool to describe in a series the properties related to homogeneous components of a graded algebraic object. In this setting, motivated by local structures associated to singularity curves, a definition of Poincaré series associated to generalized Weierstrass semigroups was introduced in [Moy11]. Since the generalized Weierstrass semigroups at several points have a natural multi-indexed filtration structure by finite dimensional vector spaces (the Riemann-Roch spaces associated), their corresponding Poincaré series can be considered to codify theses spaces.

In this chapter, we study Poincaré series associated to Weierstrass semigroups at several points as invariants of these semigroups. In particular, we show in Section 2.3 that these formal multivariate series carry enough information to recover entirely the semigroups. For this, we provide in Section 2.2 a description of generalized Weierstrass semigroups at several points in terms of least upper bounds of absolute maximal elements in the semigroups and prove that

these special elements in the semigroups belong to the support of the corresponding Poincaré series.

The description from Section 2.2 enables us to formulate moreover that generalized Weierstrass semigroups are determined finitely by certain absolute maximal elements, and therefore we obtain a method to construct these semigroups from finite elements. As a consequence, we establish a functional equation to the Poincaré series and prove that they are finitely determined by their semigroup polynomials, as shown in Section 2.3.

In Section 2.4 we present a general functional equation to Poincaré series associated to symmetric generalized Weierstrass semigroups.

2.1 Generalized Weierstrass semigroups at several points

Let $\mathcal{X}$ be a projective, non-singular, and geometrically irreducible algebraic curve of genus $g = g(\mathcal{X})$ defined over a perfect field $\mathtt{k}$ with its function field $\mathtt{k}(\mathcal{X})$. Given Q a point on $\mathcal{X}$, we call an integer α a *gap* at Q if $\ell(\alpha Q) = \ell((\alpha-1)Q)$. Otherwise, α is called a *non-gap* at Q. Denote by $H(Q)$ the set of non-gaps at Q.

Theorem 2.1.1 (Weierstrass Gap Theorem)**.** Suppose that Q is a $\mathtt{k}$-rational point on $\mathcal{X}$. Then $H(Q)$ is a subsemigroup of $\mathbb{N}_0$ with respect to the usual addition and its complement in $\mathbb{N}_0$ is finite with exactly g gaps at Q.

Proof. See [Sti09, Th. 1.6.8]. □

The set $H(Q)$ is referred as the *Weierstrass numerical semigroup* of $\mathcal{X}$ at Q. We can express it equivalently as

$$H(Q) = \{\alpha \in \mathbb{N}_0 \ : \ \exists\ f \in \mathtt{k}(\mathcal{X})^\times \text{ with } \operatorname{div}_\infty(f) = \alpha Q\} \tag{2.1.1a}$$
$$= \{-v_Q(f) \in \mathbb{N}_0 \ : \ f \in \mathcal{L}(\infty Q)\backslash\{0\}\}, \tag{2.1.1b}$$

where $\mathcal{L}(\infty Q)$ denotes the ring of rational functions of $\mathcal{X}$ having poles only at Q.

The characterizations above of $H(Q)$ enable us to extend the notion of Weierstrass semigroups to several points in two different ways. The first idea in this direction was introduced by Arbarello et al. in [Arb+85, p. 365] following the description (2.1.1a) and developed for many authors; see e.g. [Kim94; Hom96; Mat04; CT05]. A more general extension to several points based on (2.1.1b) appeared in the Delgado's work [Del90] and was explored recently by Beelen and Tutaş in [BT06]. Next we briefly describe these two approaches.

Assume $\mathcal{X}$ as before. Let $Q_1, \ldots, Q_\ell$ be $\ell \geq 2$ pairwise distinct $\mathtt{k}$-rational points of $\mathcal{X}$. The subsemigroup of $\mathbb{N}_0^m$

$$H(\mathbf{Q}) := \{(\alpha_1, \ldots, \alpha_\ell) \in \mathbb{N}_0^\ell \ : \ \exists\ f \in \mathtt{k}(\mathcal{X})^\times \text{ with } \operatorname{div}_\infty(f) = \sum_{i=1}^{\ell} \alpha_i Q_i\} \tag{2.1.2}$$

is called the (*classical*) *Weierstrass semigroup* at the ℓ-tuple $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$.

Remark 2.1.2. The complement $\mathbb{N}_0^\ell \backslash H(\mathbf{Q})$, whose elements are also called *gaps* at $\mathbf{Q}$, is likewise a finite set but now its cardinality depends on the choice of the ℓ-tuple $\mathbf{Q}$; see [Hom96].

As mentioned, many works appeared in this direction dealing with methods to determine Weierstrass semigroups and to estimate the number of gaps at several points. In particular, it has been mainly studied due to their applications to error-correcting codes; see e.g. [HK01; Mat01; Mat04; CT05].

Interpreted as in (2.1.1b), Weierstrass semigroups motivate a more embracing generalization to several points which allows us to consider semigroups in $\mathbb{Z}^\ell$ instead of in $\mathbb{N}_0^\ell$ as in (2.1.2). As we will see later, these semigroups codify not only effective divisors but all divisors on $\mathcal{X}$ supported on points of the ℓ-tuple $\mathbf{Q}$. With this purpose, let us denote by $R_{\mathbf{Q}}$ the ring of functions of $\mathcal{X}$ that are regular outside $\{Q_1, \ldots, Q_\ell\}$. Considering v_{Q_i} the valuation of $\mathtt{k}(\mathcal{X})$ associated to Q_i, for $f \in \mathtt{k}(\mathcal{X})^\times$, denote by $\rho_{\mathbf{Q}}(f)$ the ℓ-tuple $(-v_{Q_1}(f), \ldots, -v_{Q_\ell}(f))$. The set

$$\widehat{H}(\mathbf{Q}) := \{\rho_{\mathbf{Q}}(f) \in \mathbb{Z}^\ell \ : \ f \in R_{\mathbf{Q}} \backslash \{0\}\} \tag{2.1.3}$$

is called the *generalized Weierstrass semigroup* of $\mathcal{X}$ at $\mathbf{Q}$; see [Del90; BT06].

From the valuation properties, $\widehat{H}(\mathbf{Q})$ is a subsemigroup of $\mathbb{Z}^\ell$ with respect to the usual addition; moreover, it is shown in [BT06, Prop. 2] that the semigroups $H(\mathbf{Q})$ and $\widehat{H}(\mathbf{Q})$ are related by

$$H(\mathbf{Q}) = \widehat{H}(\mathbf{Q}) \cap \mathbb{N}_0^\ell.$$

From now on, we shall restrict ourselves to the study of generalized Weierstrass semigroups since they contain the classical one by the relation above. In what follows we characterize their elements in terms of dimensions of Riemann-Roch spaces associated. For this purpose, let us fix some helpful notation:

- For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell$, we set $D(\boldsymbol{\alpha}) := \sum_{i=1}^\ell \alpha_i Q_i$, $|\boldsymbol{\alpha}| := \sum_{i=1}^\ell \alpha_i$, $\mathcal{L}(\boldsymbol{\alpha}) := \mathcal{L}(D(\boldsymbol{\alpha}))$ the Riemann-Roch space associated to $D(\boldsymbol{\alpha})$ and $\ell(\boldsymbol{\alpha})$ its $\mathtt{k}$-dimension.
- Let $I := \{1, 2, \ldots, \ell\}$. For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell$, $J \subsetneq I$ and $i \in I$, we set

$$\overline{\nabla}_J(\boldsymbol{\alpha}) := \{(\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}^\ell \ : \ \beta_i = \alpha_i \ \forall \ i \in J \text{ and } \beta_j < \alpha_j \ \forall \ j \notin J\}$$

$$\overline{\nabla}_i(\boldsymbol{\alpha}) := \overline{\nabla}_{\{i\}}(\boldsymbol{\alpha})$$

$$\nabla_i^\ell(\boldsymbol{\alpha}) := \{(\beta_1, \ldots, \beta_\ell) \in \widehat{H}(\mathbf{Q}) \ : \ \beta_i = \alpha_i \text{ and } \beta_j \leq \alpha_j \ \forall \ j \neq i\}.$$

- For $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$ and a non-empty subset $J \subsetneq I$, let

$$\overline{\nabla}(\boldsymbol{\alpha}) := \bigcup_{i=1}^{\ell} \overline{\nabla}_i(\boldsymbol{\alpha}), \quad \nabla(\boldsymbol{\alpha}) := \overline{\nabla}(\boldsymbol{\alpha}) \cap \widehat{H}(\mathbf{Q}) \text{ and } \nabla_J(\boldsymbol{\alpha}) := \overline{\nabla}_J(\boldsymbol{\alpha}) \cap \widehat{H}(\mathbf{Q}).$$

- For any subset $J \subsetneq I$, denote by $\mathbf{1}_J$ the ℓ-tuple whose the j-th coordinate 1 if $j \in J$ and 0 otherwise; for instance, $\mathbf{1}_I = \mathbf{1}$ is the all 1 ℓ-tuple, $\mathbf{1}_\emptyset$ is the all zero ℓ-tuple, and $\mathbf{e}_i = \mathbf{1}_{\{i\}}$.

The next result was originally proved by Delgado [Del90, p. 629] in the case of algebraically closed fields. For the general case, it can be adapted by using ideas from Carvalho and Torres in [CT05, Lem. 2.2] as follows.

Proposition 2.1.3. Let $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$ and suppose that $\#\mathtt{k} \geq \ell$. Then

(1) $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$ if and only if $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{e}_i) + 1$ for all $i \in I$;

(2) $\nabla_i^\ell(\boldsymbol{\alpha}) = \emptyset$ if and only if $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{e}_i)$.

Proof. (1) If $\boldsymbol{\alpha} \in \widehat{H}_{\mathcal{X}}(\mathbf{Q})$, then there exists $f \in R_{\mathbf{Q}}$ such that $v_{Q_i}(f) = -\alpha_i$ for all $i \in I$, and consequently, $f \in \mathcal{L}(\boldsymbol{\alpha}) \backslash \mathcal{L}(\boldsymbol{\alpha} - \mathbf{e}_i)$ for every $i \in I$. Thus, $\ell(\boldsymbol{\alpha} - \mathbf{e}_i) = \ell(\boldsymbol{\alpha}) - 1$ for all $i \in I$. Conversely, from $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{e}_i) + 1$ for all $i \in I$, there exist $f_i \in \mathcal{L}(\boldsymbol{\alpha}) \backslash \mathcal{L}(\boldsymbol{\alpha} - \mathbf{e}_i)$ for every $i \in I$. Hence, $v_{Q_i}(f_i) = -\alpha_i$ and $v_{Q_j}(f_i) \geq -\alpha_j$ if $j \neq i$. Consider

$$f_i = a_{ij} t_{Q_j}^{v_{Q_j}(f_i)} + \cdots \in \mathtt{k}((t_{Q_j}))$$

the local expansion of f_i at Q_j in Laurent series in t_{Q_j}. We claim that there exists $(b_1, \ldots, b_\ell) \in \mathtt{k}^\ell$ such that $f = \sum_{i=1}^{\ell} b_i f_i \in R_{\mathbf{Q}}$ and $v_{Q_j}(f) = -\alpha_j$ for all $j \in I$. Indeed, taking $(b_1, \ldots, b_\ell) \in \mathtt{k}^\ell$ outside the union of ℓ hyperplanes, it guarantees that $v_{Q_j}(f) = -\alpha_j$ for every j. But as $\#\mathtt{k} \geq \ell$, this choice of $(b_1, \ldots, b_\ell) \in \mathtt{k}^\ell$ can always be done.
(2) Note that $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{e}_i) + 1$ if and only if there exists $f \in \mathcal{L}(\boldsymbol{\alpha}) \backslash \mathcal{L}(\boldsymbol{\alpha} - \mathbf{e}_i)$, which is equivalent to $\rho_{\mathbf{Q}}(f) \in \nabla_i^\ell(\boldsymbol{\alpha})$. □

With the description of elements of $\widehat{H}(\mathbf{Q})$ given above, we obtain the behaviour of Riemann-Roch spaces of each divisor on $\mathcal{X}$ supported on $Q_1, \ldots, Q_\ell$ through the knowledge of the generalized Weierstrass semigroup at $\mathbf{Q}$. As an immediate consequence, we obtain the following property concerning trivial elements in $\widehat{H}(\mathbf{Q})$.

Corollary 2.1.4. Let $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$ and assume that $\#\mathtt{k} \geq \ell$. If $|\boldsymbol{\alpha}| < 0$ then $\boldsymbol{\alpha} \notin \widehat{H}(\mathbf{Q})$. Furthermore, $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$ whenever $|\boldsymbol{\alpha}| \geq 2g$.

Proof. It follows from Theorem 2.1.3(a) and the Riemann-Roch theorem. □

Remark 2.1.5. As observed in [CT05, p. 214] in case of Weierstrass semigroups in (2.1.2), the assumption on the cardinality of $\mathtt{k}$ is indeed essential for this characterization.

2.2 Determining generalized Weierstrass semigroups

In this section we investigate how to determine generalized Weierstrass semigroups. As a conclusion, we present a description of them in terms of least upper bounds of special elements, an analogous approach to that introduced by Kim [Kim94] for pairs and generalized by Matthews [Mat04] in the case of classical Weierstrass semigroups at several points. Moreover, we show that it is possible to determine these generating elements from a finite number of them.

With this purpose, let us assume $\mathcal{X}$ a curve over $\mathtt{k}$ and $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$ an ℓ-tuple of $\mathtt{k}$-rational points of $\mathcal{X}$ under the same assumptions as in the last section. We also suppose that $\#\mathtt{k} \geq \ell \geq 2$.

2.2.1 Generating sets for $\widehat{H}(\mathbf{P})$

We start by recalling the notion of maximality from [Del90]. It translates arithmetical properties of Riemann-Roch spaces $\mathcal{L}(\boldsymbol{\alpha})$ into some subsets of $\mathbb{Z}^\ell$ related to $\boldsymbol{\alpha}$.

An element $\boldsymbol{\alpha}$ of $\widehat{H}(\mathbf{Q})$ is said *maximal* if $\nabla(\boldsymbol{\alpha}) = \emptyset$. If moreover $\nabla_J(\boldsymbol{\alpha}) = \emptyset$ for every non-empty subset $J \subsetneq I$, $\boldsymbol{\alpha}$ is called an *absolute maximal*. Denote respectively by $\mathcal{M}(\mathbf{Q})$ and $\Gamma(\mathbf{Q})$ the sets of maximal and absolute maximal elements of $\widehat{H}(\mathbf{Q})$.

Notice that when $\ell = 2$, every maximal element is absolute maximal.

Example 2.2.1. This example elucidates the maximal elements of a generalized Weierstrass semigroup of the Hermitian curve given by the affine equation $x^4 = y^3 + y$ over $\mathbb{F}_9$ at pair (Q, P), where Q is the point *at infinity* and $P = (0 : 0 : 1)$. In the Figure 2.1, the maximal elements are represented by the circles $\circ$, whereas the remaining elements of the semigroup are represented by the filled circles $\bullet$.

Denoting $\Lambda_0 := \{\boldsymbol{\alpha} \in \mathbb{Z}^\ell \ : \ |\boldsymbol{\alpha}| = 0\}$, we follow [BT06] to consider the next interesting functions.

Definition 2.2.2. For $i \in I$, we define for any $\boldsymbol{\alpha} \in \Lambda_0$

$$\sigma_i(\boldsymbol{\alpha}) := \min\{\lambda \in \mathbb{Z} \ : \ (\alpha_1, \ldots, \alpha_{i-1}, \lambda, \alpha_{i+1}, \ldots, \alpha_\ell) \in \widehat{H}(\mathbf{Q})\}.$$

When $\ell = 2$, these functions play an important role in the description of the generalized Weierstrass semigroup. Since elements in Λ_0 are of type $(j, -j)$ for $j \in \mathbb{Z}$, rewriting $\sigma_i : \mathbb{Z} \to \mathbb{Z}$, $i = 1, 2$ (see [BT06, Sec. 3] for details), it follows from [BT06, Prop. 14 (i)] that

$$\sigma_1(\sigma_2(j)) = j = \sigma_2(\sigma_1(j)) \quad \text{for} \quad j \in \mathbb{Z}.$$

This allows us to see that the sets

$$\{(j, \sigma_2(j)) \in \widehat{H}(\mathbf{Q}) \ : \ j \in \mathbb{Z}\} = \{(\sigma_1(j), j) \in \widehat{H}(\mathbf{Q}) \ : \ j \in \mathbb{Z}\} \tag{2.2.1}$$

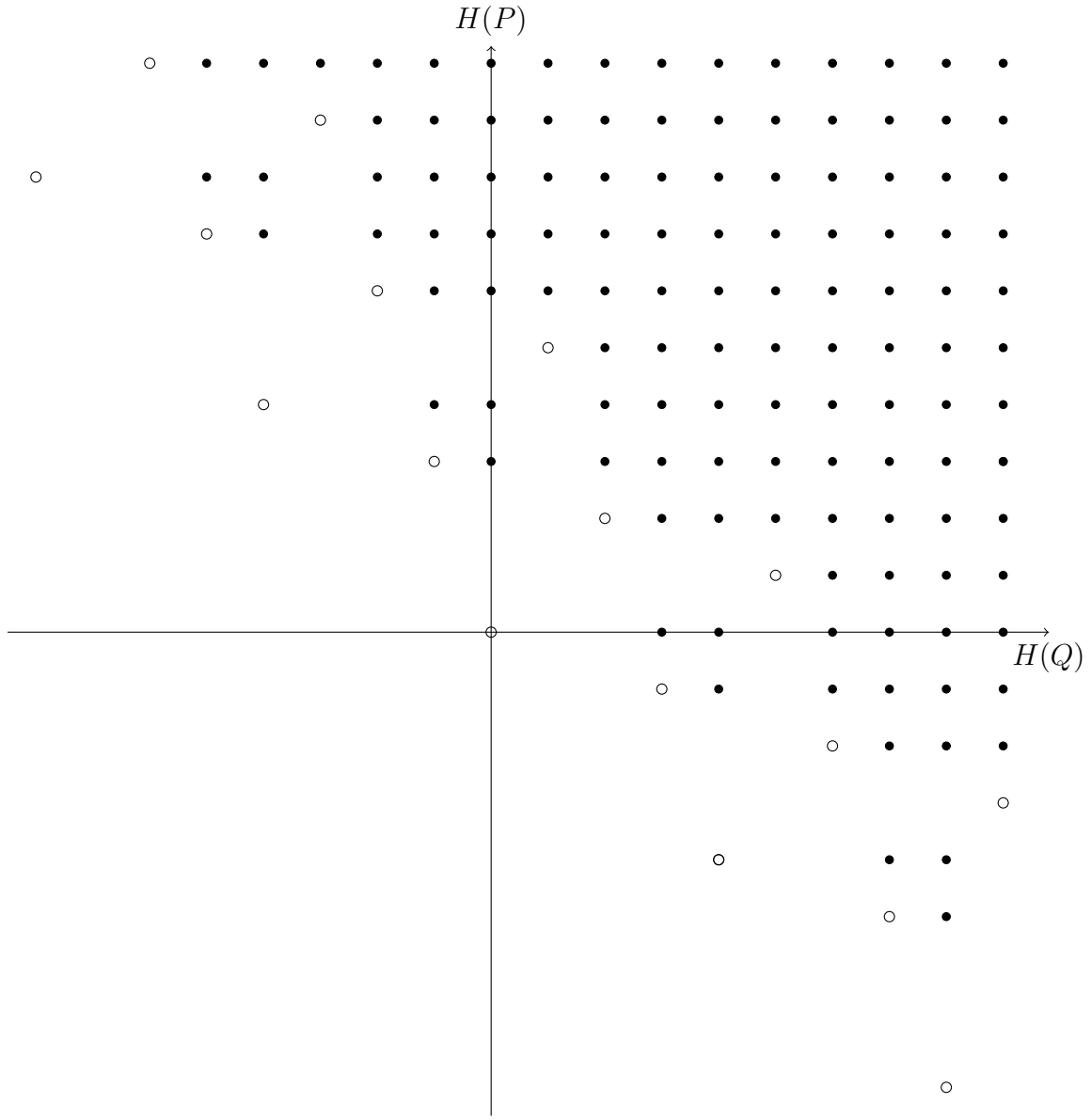

Figure 2.1: Maximal elements of $\widehat{H}(Q,P)$

coincide exactly with the set of maximal elements $\mathcal{M}(\mathbf{Q})$ of $\widehat{H}(\mathbf{Q})$. Furthermore, adapting ideas from [Kim94; Hom96], a straightforward verification shows that

$$\widehat{H}(\mathbf{Q}) = \{(\max\{\alpha_1,\beta_1\},\max\{\alpha_2,\beta_2\}) \in \mathbb{Z}^2 \ : \ \boldsymbol{\alpha},\boldsymbol{\beta} \in \mathcal{M}(\mathbf{Q})\}. \tag{2.2.2}$$

In the remaining of this subsection, we investigate the relationship between maximal elements and generating sets for generalized Weierstrass semigroups at several points, taking account the characterization from (2.2.2) in the case of pairs.

In our next proposition, we state equivalences concerning the absolute maximal property.

Proposition 2.2.3. Let $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$. Then the following statements are equivalent:

(i) $\boldsymbol{\alpha}$ is absolute maximal;

(ii) $\nabla_i^\ell(\boldsymbol{\alpha}) = \{\boldsymbol{\alpha}\}$ for all $i \in I$;

(iii) $\nabla_i^\ell(\boldsymbol{\alpha}) = \{\boldsymbol{\alpha}\}$ for some $i \in I$;

(iv) $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{1}) + 1$.

Proof. Let us first prove that (i) implies (ii). Since $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$, we get $\{\boldsymbol{\alpha}\} \subseteq \nabla_i^\ell(\boldsymbol{\alpha})$ for all $i \in I$. If $\boldsymbol{\beta} \in \nabla_j^\ell(\boldsymbol{\alpha})$ with $\boldsymbol{\beta} \neq \boldsymbol{\alpha}$ for some $j \in I$, then there exists a subset $J \subsetneq I$ containing j such that $\boldsymbol{\beta} \in \nabla_J(\boldsymbol{\alpha})$, contradicting the hypothesis.

Since (ii) immediately implies (iii), let us assume (iii). To prove (iv) it is sufficient to show that $\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) = \ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c \cup \{i\}})$ for every subset $J \subsetneq I$ containing i, which is equivalent to $\nabla_i^\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) = \emptyset$ by Proposition 2.1.3 (2). But, since

$$\nabla_i^\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) \subseteq \nabla_i^\ell(\boldsymbol{\alpha}) = \{\boldsymbol{\alpha}\},$$

the only possibility is $\nabla_i^\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) = \emptyset$ because $\boldsymbol{\alpha} \notin \nabla_i^\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c})$.

To deduce (i) from (iv), notice that $\ell(\boldsymbol{\alpha} - \mathbf{e}_i) = \ell(\boldsymbol{\alpha} - \mathbf{1})$ for every $i \in I$. If $\nabla_J(\boldsymbol{\alpha}) \neq \emptyset$ for some non-empty $J \subsetneq I$, since $\nabla_J(\boldsymbol{\alpha}) \subseteq \nabla_j^\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c})$ for any $j \in J$, by Proposition 2.1.3 (2) we get

$$\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) = \ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c} - \mathbf{e}_j) + 1.$$

Since $J \subsetneq I$, it follows that $\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) \leq \ell(\boldsymbol{\alpha} - \mathbf{e}_j)$ for $j \in I \backslash J$. As $\ell(\boldsymbol{\alpha} - \mathbf{1}_{J^c} - \mathbf{e}_i) \geq \ell(\boldsymbol{\alpha} - \mathbf{1})$ because $J \neq \emptyset$, we have

$$\ell(\boldsymbol{\alpha} - \mathbf{e}_j) \geq \ell(\boldsymbol{\alpha} - \mathbf{1}) + 1,$$

which gives us a contradiction. □

Remark 2.2.4. The main consequence of the result above is that it allows us to regard absolute maximal elements $\boldsymbol{\alpha}$ as minimal elements in the sets

$$\{\boldsymbol{\beta} \in \widehat{H}(\mathbf{Q}) \ : \ \beta_i = \alpha_i\} \text{ for } i = 1, \ldots, \ell,$$

with respect to the standard Bruhat (partial) order on $\mathbb{Z}^\ell$ given by

$$(\alpha_1, \ldots, \alpha_\ell) \leq (\beta_1, \ldots, \beta_\ell) \Leftrightarrow \alpha_i \leq \beta_i \text{ for all } i = 1, \ldots, \ell.$$

This interpretation coincides exactly with the notion used by Matthews in [Mat04] to formulate the concept of generating sets for $H(\mathbf{Q})$ and extends the approach of [Kim94; Hom96] for pairs.

Given $\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^s \in \mathbb{Z}^\ell$, define their least upper bound by

$$\operatorname{lub}(\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^s) := (\max\{\beta_1^1, \ldots, \beta_1^s\}, \ldots, \max\{\beta_\ell^1, \ldots, \beta_\ell^s\}) \in \mathbb{Z}^\ell.$$

We next formulate a characterization of generalized Weierstrass semigroups through least upper bounds of their absolute maximal elements. This description is analogous to that afforded by Matthews in [Mat04] for classical Weierstrass semigroups at several points.

Theorem 2.2.5. The generalized Weierstrass semigroup of $\mathcal{X}$ at the ℓ-tuple $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$ can be written as

$$\widehat{H}(\mathbf{Q}) = \{\operatorname{lub}(\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^\ell) \ : \ \boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^\ell \in \Gamma(\mathbf{Q})\}.$$

Proof. We begin by observing that for $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \in \Gamma(\mathbf{Q}) \subseteq \widehat{H}(\mathbf{Q})$, we obtain $\operatorname{lub}(\boldsymbol{\beta}^1, \boldsymbol{\beta}^2) \in \widehat{H}(\mathbf{Q})$ since it is always possible to find $(b_1, b_2) \in \mathtt{k}^2$ outside the union of at most ℓ one-dimensional linear spaces thanks to $\#\mathtt{k} \geq \ell$, in order to obtain $h := b_1 f_1 + b_2 f_2 \in R_{\mathbf{Q}}$ with $\rho_{\mathbf{Q}}(h) = \operatorname{lub}(\boldsymbol{\beta}_1, \boldsymbol{\beta}_2)$, where $f_1, f_2 \in R_{\mathbf{Q}}$ are such that $\boldsymbol{\beta}_1 = \rho_{\mathbf{Q}}(f_1)$ and $\boldsymbol{\beta}_2 = \rho_{\mathbf{Q}}(f_2)$. This argument may be extended to show that $\operatorname{lub}(\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^\ell) \in \widehat{H}(\mathbf{Q})$ for $\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^\ell \in \Gamma(\mathbf{Q})$ and thus we have the inclusion $\supseteq$. On the other hand, suppose that $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q}) \backslash \Gamma(\mathbf{Q})$. By Proposition 2.2.3, it follows that $\nabla_i^\ell(\boldsymbol{\alpha}) \supsetneq \{\boldsymbol{\alpha}\}$ for all i, and thus there exists $\boldsymbol{\beta}^i \in \nabla_i^\ell(\boldsymbol{\alpha})$ with $\boldsymbol{\beta}^i \neq \boldsymbol{\alpha}$ minimal with respect to $\leq$. Therefore, $\boldsymbol{\alpha}$ can be written as $\boldsymbol{\alpha} = \operatorname{lub}(\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^\ell)$, which concludes the proof. □

As a consequence, the generalized Weierstrass semigroups are entirely determined by their absolute maximal elements. In what follows we present the outcomes of this property which seem at first glance to justify why this characterization is appropriated to the study of these objects. To be precise, we analyze the relationship between the Riemann-Roch spaces of divisors associated and absolute maximal elements of generalized Weierstrass semigroups.

Given $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$, let

$$\Gamma(\boldsymbol{\alpha}) := \{\boldsymbol{\beta} \in \Gamma(\mathbf{Q}) \ : \ \boldsymbol{\beta} \leq \boldsymbol{\alpha}\}. \tag{2.2.3}$$

For $i \in I$, define on $\Gamma(\boldsymbol{\alpha})$ the relation

$$\boldsymbol{\beta} \equiv_i \boldsymbol{\beta}' \text{ if and only if } \ \beta_i = \beta_i'. \tag{2.2.4}$$

Notice that $\equiv_i$ is an equivalence relation on $\Gamma(\boldsymbol{\alpha})$. Denote by $\Gamma(\boldsymbol{\alpha})/\equiv_i$ the set of equivalence classes $[\boldsymbol{\beta}]_i$ for $\boldsymbol{\beta} \in \Gamma(\boldsymbol{\alpha})$. In our next theorem, we formulate a characterization of dimensions $\ell(\boldsymbol{\alpha})$ in terms of absolute maximal elements.

Theorem 2.2.6. Let $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$. Then

$$\ell(\boldsymbol{\alpha}) = \#(\Gamma(\boldsymbol{\alpha})/\equiv_i).$$

In particular, $\#(\Gamma(\boldsymbol{\alpha})/\equiv_i)$ does not depend on i.

Proof. Observe first that the conditions imposed on $\boldsymbol{\beta} \in \Gamma(\mathbf{Q})$ by $\boldsymbol{\beta} \leq \boldsymbol{\alpha}$ and $|\boldsymbol{\beta}| \geq 0$ imply that $\Gamma(\boldsymbol{\alpha})$ is finite. Note also that the dimension $\ell(\boldsymbol{\alpha})$ is the number of proper inclusions in the filtration

$$\mathcal{L}(\boldsymbol{\alpha}) \supseteq \mathcal{L}(\boldsymbol{\alpha} - \mathbf{e}_i) \supseteq \mathcal{L}(\boldsymbol{\alpha} - 2\mathbf{e}_i) \supseteq \cdots \supseteq \mathcal{L}(\boldsymbol{\alpha} - j\mathbf{e}_i) \supseteq \cdots \supseteq \{0\}.$$

From Proposition 2.1.3(2), $\ell(\boldsymbol{\alpha} - j\mathbf{e}_i) \neq \ell(\boldsymbol{\alpha} - (j-1)\mathbf{e}_i)$ if and only if $\nabla_i^{\ell}(\boldsymbol{\alpha} - j\mathbf{e}_i) \neq \emptyset$. It is equivalent to the existence of an absolute maximal $\boldsymbol{\beta} \in \widehat{H}(\mathbf{Q})$ with $\beta_i = \alpha_i - j$ and $\boldsymbol{\beta} \leq \boldsymbol{\alpha} - j\mathbf{e}_i \leq \boldsymbol{\alpha}$, which, according to Remark 2.2.4, is a minimal element with respect to $\leq$ in the set $\{\boldsymbol{\gamma} \in \widehat{H}(\mathbf{Q}) \ : \ \gamma_i = \alpha_i - j\}$. □

Write $\Gamma(\boldsymbol{\alpha})/\equiv_i \ = \{[\boldsymbol{\beta}^1]_i, \ldots, [\boldsymbol{\beta}^{\ell(\boldsymbol{\alpha})}]_i\}$ for a choice of representative classes, and denote, by convenient abuse of notation, $\rho_{\mathbf{Q}}^{-1}(\Gamma(\boldsymbol{\alpha})/\equiv_i) \ = \{f_1, \ldots, f_{\ell(\boldsymbol{\alpha})}\}$, where $f_j \in \rho_{\mathbf{Q}}^{-1}(\boldsymbol{\beta}^j)$ for $j = 1, \ldots, \ell(\boldsymbol{\alpha})$. Refining the connection established above, we next describe how the absolute maximal elements of $\widehat{H}(\mathbf{Q})$ carry intrinsic information on $R_{\mathbf{Q}}$ as a $\mathtt{k}$-vector space.

Corollary 2.2.7. Let $\boldsymbol{\alpha} \in \mathbb{Z}^{\ell}$. The set $\rho_{\mathbf{Q}}^{-1}(\Gamma(\boldsymbol{\alpha})/\equiv_i)$ is a basis for the Riemann-Roch space $\mathcal{L}(\boldsymbol{\alpha})$. In particular, the ring of functions of $\mathcal{X}$ that are regular outside $Q_1, \ldots, Q_{\ell}$ is spanned by $\rho_{\mathbf{Q}}^{-1}(\Gamma(\mathbf{Q}))$ as an infinite-dimensional $\mathtt{k}$-vector space.

Proof. We first observe that $\rho_{\mathbf{Q}}^{-1}(\Gamma(\boldsymbol{\alpha})) \subseteq \mathcal{L}(\boldsymbol{\alpha})$, and so it remains to prove that $\rho_{\mathbf{Q}}^{-1}(\Gamma(\boldsymbol{\alpha})/\equiv_i)$ is a linearly independent subset of $\mathcal{L}(\boldsymbol{\alpha})$. Indeed, assuming $\ell(\boldsymbol{\alpha}) > 1$, if $\sum_{j=1}^{\ell(\boldsymbol{\alpha})} b_j f_j = 0$ for $b_j \in \mathtt{k}$ not all zero, then $\min\{v_{Q_i}(f_1), \ldots, v_{Q_i}(f_{\ell(\boldsymbol{\alpha})})\}$ is attained at least two times, which gives a contradiction by the definition of $\equiv_i$ in (2.2.4). Therefore, $\rho_{\mathbf{Q}}^{-1}(\Gamma(\boldsymbol{\alpha})/\equiv_i)$ is a basis of $\mathcal{L}(\boldsymbol{\alpha})$. The latter assertion follows by noticing that $R_{\mathbf{Q}} = \bigcup_{\boldsymbol{\alpha} \in \mathbb{Z}^{\ell}} \mathcal{L}(\boldsymbol{\alpha})$. □

2.2.2 Determining generating sets of $\widehat{H}(\mathbf{P})$

Although generalized Weierstrass semigroups have the description as in the Theorem 2.2.5, computing all absolute maximal elements is not an easy task since the set formed by them is infinite. In this way, we would like to know whether the set $\Gamma(\mathbf{Q})$ of absolute maximal elements can be finitely determined. For this purpose, assume that $\mathtt{k}$ is a finite field. Let us start this discussion with the case $\ell = 2$. Here the characterization of elements of $\mathcal{M}(\mathbf{Q})$ as in (2.2.1) is essential since by [BT06, Prop. 14 (vii)], the function σ_2 in Definition 2.2.2 has the periodical property

$$\sigma_2(j + a) = \sigma_2(j) - a \quad \text{for } j \in \mathbb{Z}, \tag{2.2.5}$$

where a is the smallest positive integer t such that $(t, -t) \in \widehat{H}(\mathbf{Q})$. Hence, it is possible to determine $\mathcal{M}(\mathbf{Q})$ from the knowledge of the finite set

$$\{(j, \sigma_2(j)) \ : \ 0 \leq j < a\}. \tag{2.2.6}$$

For the general case we can consider a similar approach: for $i = 1, \ldots, \ell - 1$, let a_i be the smallest positive integer t such that $t(Q_i - Q_{i+1})$ is a principal divisor on $\mathcal{X}$, and denote by $\boldsymbol{\eta}^i \in \mathbb{Z}^\ell$ the ℓ-tuple whose j-th coordinate is

$$\eta^i_j = \begin{cases} a_i & , \text{ if } j = i \\ -a_i & , \text{ if } j = i+1 \\ 0 & , \text{ otherwise.} \end{cases} \tag{2.2.7}$$

Notice that such a_i's are guaranteed by the finiteness of the divisor class group. Consider the region

$$\mathcal{C} := \{\boldsymbol{\alpha} \in \mathbb{Z}^\ell \ : \ 0 \leq \alpha_i < a_i \text{ for } i = 1, \ldots, \ell - 1\}.$$

As noticed in [BT06, Sec. 2], the functions $f \in R^\times_{\mathbf{Q}}$ are such that the support of $\operatorname{div}(f)$ is a subset of $\{Q_1, \ldots, Q_\ell\}$ and their image under $\rho_{\mathbf{Q}}$ form a lattice in Λ_0. Denote by $\Theta(\mathbf{Q})$ its sublattice generated by the elements $\boldsymbol{\eta}^1, \ldots, \boldsymbol{\eta}^{\ell-1}$.

Similarly to the properties (2.2.5) and (2.2.6) satisfied by pairs, we can establish the following general statement on maximal elements in generalized Weierstrass semigroups.

Theorem 2.2.8. The maximal elements of $\widehat{H}(\mathbf{Q})$ are finitely determined by maximal elements in $\mathcal{C}$ modulo the lattice $\Theta(\mathbf{Q})$. Namely,

$$\mathcal{M}(\mathbf{Q}) = (\mathcal{M}(\mathbf{Q}) \cap \mathcal{C}) + \Theta(\mathbf{Q}).$$

Furthermore, this property also holds for absolute maximal elements of $\widehat{H}(\mathbf{Q})$, that is,

$$\Gamma(\mathbf{Q}) = (\Gamma(\mathbf{Q}) \cap \mathcal{C}) + \Theta(\mathbf{Q}).$$

Proof. Notice first that if $\boldsymbol{\alpha} \in \mathcal{M}(\mathbf{Q}) \cap \mathcal{C}$ and $\boldsymbol{\eta} \in \Theta(\mathbf{Q})$, then $\boldsymbol{\alpha} + \boldsymbol{\eta} \in \mathcal{M}(\mathbf{Q})$ since otherwise $\boldsymbol{\gamma} \in \nabla(\boldsymbol{\alpha} + \boldsymbol{\eta})$ implies $\boldsymbol{\gamma} - \boldsymbol{\eta} \in \nabla(\boldsymbol{\alpha})$, contradicting the maximality of $\boldsymbol{\alpha}$. On the other hand, given $\boldsymbol{\alpha} \in \mathcal{M}(\mathbf{Q})$, there exists $\boldsymbol{\eta} \in \Theta(\mathbf{Q})$ such that $\boldsymbol{\alpha} - \boldsymbol{\eta} \in \mathcal{C}$. We claim that $\boldsymbol{\alpha} - \boldsymbol{\eta} \in \mathcal{M}(\mathbf{Q})$. Indeed, $\boldsymbol{\alpha} - \boldsymbol{\eta}$ belongs to $\widehat{H}(\mathbf{Q})$ by the semigroup property. If $\boldsymbol{\gamma} \in \nabla(\boldsymbol{\alpha} - \boldsymbol{\eta})$, then $\boldsymbol{\gamma} + \boldsymbol{\eta} \in \nabla(\boldsymbol{\alpha})$, contrary to $\boldsymbol{\alpha}$ being maximal.

Now, suppose that $\boldsymbol{\alpha} \in \Gamma(\mathbf{Q})$. Since $\boldsymbol{\alpha}$ is maximal, there exists $\boldsymbol{\eta} \in \Theta(\mathbf{Q})$ such that $\boldsymbol{\alpha} - \boldsymbol{\eta} \in \mathcal{M}(\mathbf{Q}) \cap \mathcal{C}$. It remains to show that $\boldsymbol{\alpha} - \boldsymbol{\eta} \in \Gamma(\mathbf{Q})$. On the contrary, from Proposition 2.2.3, we would have $\boldsymbol{\gamma} \in \nabla^\ell_i(\boldsymbol{\alpha} - \boldsymbol{\eta})$ for some $i \in I$, with $\boldsymbol{\gamma} \neq \boldsymbol{\alpha} - \boldsymbol{\eta}$, which means that $\boldsymbol{\gamma} + \boldsymbol{\eta} \in \nabla^\ell_i(\boldsymbol{\alpha})$, contradicting the absolute maximality of $\boldsymbol{\alpha}$, because $\boldsymbol{\gamma} + \boldsymbol{\eta} \neq \boldsymbol{\alpha}$. On the other hand, given $\boldsymbol{\alpha} \in \Gamma(\mathbf{Q}) \cap \mathcal{C}$, it follows from Proposition 2.2.3 that $\boldsymbol{\alpha} + \boldsymbol{\eta}^j$ is absolute maximal for $j = 1, \ldots, \ell - 1$. As each element $\boldsymbol{\eta}$ in $\Theta(\mathbf{Q})$ is an integral linear combination of $\boldsymbol{\eta}^1, \ldots, \boldsymbol{\eta}^{\ell-1}$, we have $\boldsymbol{\alpha} + \boldsymbol{\eta} \in \Gamma(\mathbf{Q})$. □

It turns out that generalized Weierstrass semigroups can be determined by the absolute

maximal elements in $\mathcal{C}$ and $\boldsymbol{\eta}^1, \ldots, \boldsymbol{\eta}^{\ell-1}$. In the next example, we present a conjecture supported by numerical evidences about these finite elements in the case of several collinear points on the Hermitian curve.

Example 2.2.9. Let q be a prime power. Let $\mathcal{H}_q$ denote the Hermitian curve over $\mathbb{F}_{q^2}$ given by the affine equation

$$x^{q+1} = y^q + y.$$

Let us consider the q elements $b \in \mathbb{F}_{q^2}$ such that $b^q + b = 0$, say $b_1, \ldots, b_q$. For $j = 1, \ldots, q$, let Q_j denote the point $(0 : b_j : 1)$, and let Q denote the point at infinite of $\mathcal{H}$. We have the following principal divisors on $\mathcal{H}$:

$$\operatorname{div}(x) = Q_1 + \cdots + Q_q - qQ$$

and if $y_j := y - b_j$ for $j = 1, \ldots, q$, then

$$\operatorname{div}(y_j) = (q+1)(Q_j - Q).$$

Now let $\mathbf{Q}_\ell$ be the $(\ell+1)$-tuple $(Q, Q_1, \ldots, Q_\ell)$ of rational points on $\mathcal{H}$, for $\ell = 1, \ldots, q$. This example is about the absolute maximal elements of $\widehat{H}(\mathbf{Q}_\ell)$ for $\ell = 1, \ldots, q$ in the region $\mathcal{C}$ that will allow us to generate the generalized Weierstrass semigroups at $\mathbf{Q}_\ell$ as in Theorem 2.2.5. First we notice that $a_j = q + 1$ for $j = 1, \ldots, \ell$, and thus

$$\boldsymbol{\eta}^j = (0, \ldots, 0, \underbrace{q+1}_{j\text{-th entry}}, -(q+1), 0, \ldots, 0) \in \mathbb{Z}^{\ell+1};$$

cf. (2.2.7). Denote $\boldsymbol{\alpha}^{i,\ell} := (i, \ldots, i, q(q-i-(\ell-1)) - \ell) \in \mathbb{Z}^{\ell+1}$ for $i = 1, \ldots, q$, and let

$$\mathcal{A}_\ell = \{\boldsymbol{\alpha}^{i,\ell} \ : \ i = 1, \ldots, q\} \cup \{\mathbf{0}\} \subseteq \mathbb{Z}^{\ell+1},$$

where $\mathbf{0} = (0, \ldots, 0)$. Notice that $\mathcal{A}_\ell \subseteq \widehat{H}(\mathbf{Q}_\ell) \cap \mathcal{C}$, since an elementary computation shows that the rational function $\frac{x^{q+1-i}}{y_1 \cdots y_{\ell-1} \cdot y_\ell^{q-\ell-i+1}}$ of $\mathcal{H}$ is regular outside $\{Q, Q_1, \ldots, Q_\ell\}$ and gives

$$\rho_{\mathbf{Q}_\ell}\left(\frac{x^{q+1-i}}{y_1 \cdots y_{\ell-1} \cdot y_\ell^{q-\ell-i+1}}\right) = \boldsymbol{\alpha}^{i,\ell}.$$

Based on computations for several values of q, our conjecture is that $\mathcal{A}_\ell = \Gamma(\mathbf{Q}_\ell) \cap \mathcal{C}$. We believe that, according to Theorem 2.2.8, the $q+\ell+1$ elements in $\mathcal{A}_\ell \cup \{\boldsymbol{\eta}^1, \ldots, \boldsymbol{\eta}^\ell\}$ will ensure the entire characterization of $\widehat{H}(\mathbf{Q}_\ell)$.

We close this section by exploring the consequences of Theorem 2.2.8 to Riemann-Roch spaces associated to divisors supported on subsets of $\{Q_1, \ldots, Q_\ell\}$. To this end, let us define

for $\boldsymbol{\alpha}, \boldsymbol{\alpha}' \in \mathbb{Z}^\ell$ the relation

$$\boldsymbol{\alpha} \equiv \boldsymbol{\alpha}' \text{ if and only if } \boldsymbol{\alpha} - \boldsymbol{\alpha}' \in \Theta(\mathbf{Q}). \tag{2.2.8}$$

Observe that the foregoing relation is an equivalence relation in $\mathbb{Z}^\ell$, because $\Theta(\mathbf{Q})$ is a lattice in Λ_0. Writing $[\boldsymbol{\alpha}]$ the equivalence class of $\boldsymbol{\alpha}$ for $\equiv$, we can state the following property of dimensions in these equivalence classes.

Corollary 2.2.10. Let $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$. Then $\ell(\boldsymbol{\alpha}') = \ell(\boldsymbol{\alpha})$ for any $\boldsymbol{\alpha}' \in [\boldsymbol{\alpha}]$.

Proof. Note that $\boldsymbol{\beta} \in \Gamma(\mathbf{Q})$ if and only if $\boldsymbol{\beta} + \boldsymbol{\eta} \in \Gamma(\mathbf{Q})$ for any $\boldsymbol{\eta} \in \Theta(\mathbf{Q})$. Hence $\boldsymbol{\beta} \in \Gamma(\boldsymbol{\alpha})$ is equivalent to $\boldsymbol{\beta} + \boldsymbol{\eta} \in \Gamma(\boldsymbol{\alpha} + \boldsymbol{\eta})$ for $\boldsymbol{\eta} \in \Theta(\mathbf{Q})$, and thus $\Gamma(\boldsymbol{\alpha} + \boldsymbol{\eta}) = \boldsymbol{\eta} + \Gamma(\boldsymbol{\alpha})$. Therefore

$$\#(\Gamma(\boldsymbol{\alpha} + \boldsymbol{\eta})/\equiv_i) = \#((\boldsymbol{\eta} + \Gamma(\boldsymbol{\alpha}))/\equiv_i) = \#(\Gamma(\boldsymbol{\alpha})/\equiv_i),$$

which completes the proof by invoking Theorem 2.2.6. □

Since $\Gamma(\mathbf{Q}) \cap \mathcal{C}$ is finite, let $\boldsymbol{\beta}^1, \ldots, \boldsymbol{\beta}^c$ be its elements. For $i = 1, \ldots, c$, let $f_i \in R_{\mathbf{Q}}$ be a function such that $\rho_{\mathbf{Q}}(f_i) = \boldsymbol{\beta}^i$. Analogously, for $i = 1, \ldots, \ell - 1$, let $g_i \in R_{\mathbf{Q}}$ be a function such that $\rho_{\mathbf{Q}}(g_i) = \boldsymbol{\eta}^i$. We can thus state the following concerning such functions.

Corollary 2.2.11. The ring $R_{\mathbf{Q}}$ of functions of $\mathcal{X}$ that are regular outside $Q_1, \ldots, Q_\ell$ is spanned as $\mathtt{k}$-vector space by the set of functions

$$\{f_i \cdot g_1^{i_1} \cdots g_{\ell-1}^{i_{\ell-1}} \ : \ 0 \leq i \leq c \text{ and } i_j \in \mathbb{Z} \text{ for } j = 1, \ldots, \ell - 1\}.$$

Proof. According to Corollary 2.2.7, we have $\rho_{\mathbf{Q}}^{-1}(\Gamma(\mathbf{Q}))$ is a generating set for $R_{\mathbf{Q}}$ as a $\mathtt{k}$-vector space. From Theorem 2.2.8 we have $\Gamma(\mathbf{Q}) = (\Gamma(\mathbf{Q}) \cap \mathcal{C}) + \Theta(\mathbf{Q})$, which concludes the proof. □

2.3 Poincaré series of generalized Weierstrass semigroups

Throughout this section we consider $\mathcal{X}$ an algebraic curve over $\mathtt{k}$ together with an ℓ-tuple $\mathbf{Q}$ of $\mathtt{k}$-rational points on $\mathcal{X}$ where $\#\mathtt{k} \geq \ell \geq 1$, under same conditions as in Section 2.2. Since the ring $R_{\mathbf{Q}}$ of regular functions of $\mathcal{X}$ outside $\{Q_1, \ldots, Q_\ell\}$ can be written as

$$R_{\mathbf{Q}} = \bigcup_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} \mathcal{L}(\boldsymbol{\alpha}),$$

and $\mathcal{L}(\boldsymbol{\alpha}) \subseteq \mathcal{L}(\boldsymbol{\beta})$ whenever $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ for $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Z}^\ell$, we have a multi-index filtration of $R_{\mathbf{Q}}$ by Riemann-Roch spaces $\mathcal{L}(\boldsymbol{\alpha})$ which are $\mathtt{k}$-vector spaces of finite dimension $\ell(\boldsymbol{\alpha})$. Associated with the filtration $(\mathcal{L}(\boldsymbol{\alpha}))_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell}$, we can define

$$L(\mathbf{t}) := \sum_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} d(\boldsymbol{\alpha}) \cdot \mathbf{t}^{\boldsymbol{\alpha}} \in \mathbb{Z}[[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]], \tag{2.3.1}$$

where $\mathbf{t}^{\boldsymbol{\alpha}}$, for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell$, stands for the monomial $t_1^{\alpha_1} \cdots t_\ell^{\alpha_\ell}$, and

$$d(\boldsymbol{\alpha}) = \dim_{\mathtt{k}}(\mathcal{L}(\boldsymbol{\alpha})/\mathcal{L}(\boldsymbol{\alpha} - \mathbf{1})) \leq \ell.$$

Remark 2.3.1. By $\mathbb{Z}[[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]]$ we mean the set of $\mathbb{Z}$-valued formal series (or formal distributions) in multi-variables $t_1, \ldots, t_\ell$, which are formal expressions $\sum_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} s(\boldsymbol{\alpha}) \mathbf{t}^{\boldsymbol{\alpha}}$ for $s(\boldsymbol{\alpha}) \in \mathbb{Z}$. When $s(\boldsymbol{\alpha}) = 0$ for all but finitely many $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$, we refer to $\sum_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} s(\boldsymbol{\alpha}) \mathbf{t}^{\boldsymbol{\alpha}}$ as a Laurent polynomial, and denote their set by $\mathbb{Z}[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]$. Given a formal series $S(\mathbf{t})$, its support is the set $\{\boldsymbol{\alpha} \in \mathbb{Z}^\ell \ : \ s(\boldsymbol{\alpha}) \neq 0\}$. The set $\mathbb{Z}[[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]]$ has a polynomial-like $\mathbb{Z}$-module structure in the sense that addition and scalar multiplication are performed as for polynomials. However, $\mathbb{Z}[[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]]$ is no longer a ring, since the natural multiplication relation

$$\left(\sum_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} s(\boldsymbol{\alpha}) \mathbf{t}^{\boldsymbol{\alpha}} \right) \left(\sum_{\boldsymbol{\alpha}' \in \mathbb{Z}^\ell} s'(\boldsymbol{\alpha}') \mathbf{t}^{\boldsymbol{\alpha}'} \right) = \sum_{\boldsymbol{\alpha} \in \mathbb{Z}^\ell} \left(\sum_{\boldsymbol{\alpha}' \in \mathbb{Z}^\ell} s(\boldsymbol{\alpha}') s(\boldsymbol{\alpha} - \boldsymbol{\alpha}') \right) \mathbf{t}^{\boldsymbol{\alpha}}$$

does not make sense in general. But this rule gives us on $\mathbb{Z}[[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]]$ a module structure over the ring of Laurent polynomials $\mathbb{Z}[t_1^{\pm 1}, \ldots, t_\ell^{\pm 1}]$. This module usually contains many torsion elements.

Observe that when $\ell = 1$, $L(\mathbf{t})$ is just a formal power series. It codifies the elements of Weierstrass numerical semigroup $\widehat{H}(Q_1) = H(Q_1)$, since $\alpha \in \widehat{H}(Q_1)$ if and only if $d(\alpha) = 1$. We thus have

$$L(t) = \sum_{\alpha \in \widehat{H}(Q_1)} t^\alpha. \tag{2.3.2}$$

Nevertheless, it does not remain true for several points, that is, there are elements outside $\widehat{H}(\mathbf{Q})$ appearing in the support of $L(\mathbf{t})$; cf. the so-called gaps in [CT05]. It thus motivates a more convenient definition of formal series related to $\widehat{H}(\mathbf{Q})$.

Definition 2.3.2. The *Poincaré series associated to* $\widehat{H}(\mathbf{Q})$ is defined to be the multivariate formal series $P(\mathbf{t})$ satisfying

$$(1 - t_1 \cdots t_\ell) \cdot P(\mathbf{t}) = \prod_{i=1}^{\ell} (1 - t_i) \cdot L(\mathbf{t}). \tag{2.3.3}$$

As we shall see in Subsection 2.3.1, we can explicitly exhibit a such formal series satisfying the functional equation (2.3.3) (cf. Proposition 2.3.4), and therefore this notion is well-defined.

In [Moy11, Sec. 3.2], Moyano-Fernández specializes the two point case $\mathbf{Q} = (Q_1, Q_2)$ and obtains that the related Poincaré series (2.3.3) is expressed simply as

$$P(\mathbf{t}) = \sum_{\boldsymbol{\alpha} \in \mathcal{M}(\mathbf{Q})} \mathbf{t}^{\boldsymbol{\alpha}}, \tag{2.3.4}$$

where $\mathcal{M}(\mathbf{Q})$ is the set of maximal elements of $\widehat{H}(\mathbf{Q})$. As we have seen in (2.2.2), the maximal elements determine entirely the generalized Weierstrass semigroups at pair. Therefore, the Poincaré series (2.3.4) carries enough information on the semigroup $\widehat{H}(\mathbf{Q})$ at a pair of points.

With this in mind, this section is devoted to study the behavior of Poincaré series under the aforementioned property whenever $\ell = 2$. In particular, we shall be interested in proving the main result of this section.

Theorem 2.3.3. The Poincaré series associated to a generalized Weierstrass semigroup at several points of $\mathcal{X}$ determines completely the whole semigroup. Furthermore, it is finitely determined even having an infinity support.

2.3.1 Poincaré series as an invariant of $\widehat{H}(\mathbf{Q})$

In order to make a precise description of Poincaré series $P(\mathbf{t})$ associated to generalized Weierstrass semigroups, we consider some auxiliary formal series that shall enable us to explore some computational aspects of $P(\mathbf{t})$. Let

$$Q(\mathbf{t}) := \prod_{i=1}^{\ell}(1 - t_i) \cdot L(\mathbf{t}).$$

Writing $Q(\mathbf{t}) = \sum_{\boldsymbol{\alpha}\in\mathbb{Z}^\ell} q(\boldsymbol{\alpha}) \cdot \mathbf{t}^{\boldsymbol{\alpha}}$, its coefficients $q(\boldsymbol{\alpha})$ are given exactly by

$$q(\boldsymbol{\alpha}) = \sum_{J\in\mathcal{P}(I)} (-1)^{\#J} d(\boldsymbol{\alpha} - \mathbf{1}_J), \tag{2.3.5}$$

where $\mathcal{P}(I)$ denotes the power set of I.

For each $i \in I$, let us also consider

$$P_i(\mathbf{t}) := \sum_{\boldsymbol{\alpha}\in\mathbb{Z}^\ell} p_i(\boldsymbol{\alpha}) \cdot \mathbf{t}^{\boldsymbol{\alpha}}$$

the formal series whose coefficients $p_i(\boldsymbol{\alpha})$ are

$$p_i(\boldsymbol{\alpha}) = (-1)^{\ell-1} \sum_{J\in\mathcal{P}(I\setminus\{i\})} (-1)^{\#J} d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e}_i), \tag{2.3.6}$$

for $d_i(\boldsymbol{\alpha})$ representing the $\mathtt{k}$-dimension of $\mathcal{L}(\boldsymbol{\alpha})/\mathcal{L}(\boldsymbol{\alpha} - \mathbf{e}_i)$. The following result connects $Q(\mathbf{t})$ and each $P_i(\mathbf{t})$. It is the analogue of that established in [DGN08, Prop. 8] to our context, and their proofs run very closely with minor adjustments that for completeness we shall indicate below.

Proposition 2.3.4. Let $\boldsymbol{\alpha} \in \mathbb{Z}^\ell$ and $i \in I$. Then $q(\boldsymbol{\alpha}) = p_i(\boldsymbol{\alpha}) - p_i(\boldsymbol{\alpha} - \mathbf{1})$. In particular,

$$Q(\mathbf{t}) = (1 - t_1 \cdots t_\ell) \cdot P_i(\mathbf{t}),$$

which means that $P_i(\mathbf{t})$ does not depend on i and coincides with the Poincaré series $P(\mathbf{t})$.

Proof. We first notice that for any reordering $\{i_1, \ldots, i_{\ell-1}\}$ of $I\backslash\{i\}$ and any $\boldsymbol{\beta} \in \mathbb{Z}^\ell$ we can write

$$d(\boldsymbol{\beta}) = d_{i_1}(\boldsymbol{\beta}) + d_{i_2}(\boldsymbol{\beta} - \mathbf{e_{i_1}}) + \cdots + d_{i_{\ell-1}}(\boldsymbol{\beta} - \mathbf{e_{i_1}} - \cdots - \mathbf{e_{i_{\ell-2}}}) + d_i(\boldsymbol{\beta} - \mathbf{1} + \mathbf{e_i})$$

and

$$d(\boldsymbol{\beta} + \mathbf{e_i}) = d_i(\boldsymbol{\beta} + \mathbf{e_i}) + d_{i_1}(\boldsymbol{\beta}) + d_{i_2}(\boldsymbol{\beta} - \mathbf{e_{i_1}}) + \cdots + d_{i_{\ell-1}}(\boldsymbol{\beta} - \mathbf{e_{i_1}} - \cdots - \mathbf{e_{i_{\ell-2}}}),$$

from which we deduce

$$d(\boldsymbol{\beta}) - d(\boldsymbol{\beta} + \mathbf{e_i}) = d_i(\boldsymbol{\beta} - \mathbf{1} + \mathbf{e_i}) - d_i(\boldsymbol{\beta} + \mathbf{e_i}). \tag{2.3.7}$$

By (2.3.6), we have

$$p_i(\boldsymbol{\alpha}) - p_i(\boldsymbol{\alpha} - \mathbf{1}) = (-1)^{\ell-1} \sum_{J \in \mathcal{P}(I\backslash\{i\})} (-1)^{\#J} \left(d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e_i}) - d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J - \mathbf{1} + \mathbf{e_i})\right)$$

and, by taking $\boldsymbol{\beta} = \boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J$ in (2.3.7), we obtain

$$p_i(\boldsymbol{\alpha}) - p_i(\boldsymbol{\alpha} - \mathbf{1}) = (-1)^{\ell} \sum_{J \in \mathcal{P}(I\backslash\{i\})} (-1)^{\#J} \left(d(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J) - d(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e_i})\right),$$

which equals to

$$(-1)^{\ell} \sum_{J \in \mathcal{P}(I\backslash\{i\})} (-1)^{\#J} \left(d(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) - d(\boldsymbol{\alpha} - \mathbf{1}_{J^c\backslash\{i\}})\right),$$

since $\mathbf{1} - \mathbf{1}_J = \mathbf{1}_{J^c}$. As for any $J \in \mathcal{P}(I\backslash\{i\})$ we have

$$d(\boldsymbol{\alpha} - \mathbf{1}_{J^c}) - d(\boldsymbol{\alpha} - \mathbf{1}_{J^c\backslash\{i\}}) = (-1)^{\ell} \left(d(\boldsymbol{\alpha} - \mathbf{1}_J) - d(\boldsymbol{\alpha} - \mathbf{1}_J - \mathbf{e}_i)\right),$$

we thus obtain

$$p_i(\boldsymbol{\alpha}) - p_i(\boldsymbol{\alpha} - \mathbf{1}) = \sum_{J \in \mathcal{P}(I\backslash\{i\})} (-1)^{\#J} \left(d(\boldsymbol{\alpha} - \mathbf{1}_J) - d(\boldsymbol{\alpha} - \mathbf{1}_J - \mathbf{e_i})\right),$$

which completes the proof by noticing that $\mathcal{P}(I) = \mathcal{P}(I\backslash\{i\}) \cup \{J \cup \{i\} \ : \ J \in \mathcal{P}(I\backslash\{i\})\}$ in the expression (2.3.5). □

We have thus obtained an expression to coefficients of $P(\mathbf{t})$ in terms of (2.3.6). In the proposition to be proved, we use that expression to state a characterization of likely elements in the support of $P(\mathbf{t})$, extending somewhat the formula (2.3.4) to several points. This result is the version of [Moy15, Prop. 3.8] for Poincaré series associated to generalized Weierstrass semigroups, and for the sake of clarity, we shall point its proof out.

Proposition 2.3.5. Let $P(\mathbf{t}) = \sum_{\boldsymbol{\alpha}\in\mathbb{Z}^\ell} p(\boldsymbol{\alpha})\mathbf{t}^{\boldsymbol{\alpha}}$ be the corresponding Poincaré series of $\widehat{H}(\mathbf{Q})$. One has the following statements:

(a) if $\boldsymbol{\alpha} \notin \widehat{H}(\mathbf{Q})$ then $p(\boldsymbol{\alpha}) = 0$;

(b) if $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})\backslash\mathcal{M}(\mathbf{Q})$ then $p(\boldsymbol{\alpha}) = 0$;

(c) if $\boldsymbol{\alpha} \in \Gamma(\mathbf{Q})$ then $p(\boldsymbol{\alpha}) = 1$.

Proof. From Proposition 2.1.3 (2) we have $d_i(\boldsymbol{\beta}) = 0$ if and only if $\nabla_i^\ell(\boldsymbol{\beta}) = \emptyset$, and thus for any $i, j \in I$ with $i \neq j$ and $\boldsymbol{\beta} \in \mathbb{Z}^\ell$, we get

$$d_i(\boldsymbol{\beta} + \mathbf{e_i} + \mathbf{e_j}) \geq d_i(\boldsymbol{\beta} + \mathbf{e_i}),$$

because $\nabla_i^\ell(\boldsymbol{\beta} + \mathbf{e_i} + \mathbf{e_j}) \supseteq \nabla_i^\ell(\boldsymbol{\beta} + \mathbf{e_i})$. Hence, for any $i \in I$ and any reordering $\{i_1, \ldots, i_{\ell-1}\}$ of $I\backslash\{i\}$, we have

$$0 \leq d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e_i}) \leq d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e_i} + \mathbf{e_{i_1}}) \leq \cdots \leq d_i(\boldsymbol{\alpha}) \leq 1. \tag{2.3.8}$$

To prove (a), we observe that from Proposition 2.1.3, we have $d_i(\boldsymbol{\alpha}) = 0$ for some $i \in I$. Consequently, by (2.3.8), each summand $d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e}_i)$ of the coefficients $p_i(\boldsymbol{\alpha})$ in (2.3.6) is zero and therefore $p_i(\boldsymbol{\alpha}) = 0$, which gives (a) from Proposition 2.3.4. Now, assuming $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})\backslash\mathcal{M}(\mathbf{Q})$, then $\nabla_i(\boldsymbol{\alpha}) \neq \emptyset$ for some $i \in I$, which implies $d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e_i}) = 1$, since $\nabla_i(\boldsymbol{\alpha}) = \nabla_i^\ell(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e_i})$ and by Proposition 2.1.3 (2). Therefore, all other following terms in the inequalities (2.3.8) are 1 and thus

$$p_i(\boldsymbol{\alpha}) = (-1)^{\ell-1}\sum_{j=0}^{\ell-1}(-1)^j \sum_{\substack{J\in\mathcal{P}(I\backslash\{i\}) \\ \#J=j}} d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e}_i) \tag{2.3.9a}$$

$$= (-1)^{\ell-1}\sum_{j=0}^{\ell-1}(-1)^j \binom{\ell-1}{j}, \tag{2.3.9b}$$

which yields $p_i(\boldsymbol{\alpha}) = 0$, since the sum in (2.3.9b) is 0. For $\boldsymbol{\alpha} \in \Gamma(\mathbf{Q})$, it follows from Proposition 2.1.3 that $d_i(\boldsymbol{\alpha}) = 1$ since $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$, and $d_i(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{1}_J + \mathbf{e}_i) = 0$ for all $J \subsetneq I\backslash\{i\}$ because $d(\boldsymbol{\alpha}) = 1$ by Proposition 2.2.3. The proof concludes by observing that from (2.3.9a) we obtain $p_i(\boldsymbol{\alpha}) = (-1)^{\ell-1}(-1)^{\ell-1} = 1$ □

Therefore, from the items (a) and (b) in Proposition 2.3.5, we can rewrite the Poincaré series $P(\mathbf{t})$ associated to $\widehat{H}(\mathbf{Q})$ as

$$P(\mathbf{t}) = \sum_{\boldsymbol{\alpha}\in\mathcal{M}(\mathbf{Q})} p(\boldsymbol{\alpha})\mathbf{t}^{\boldsymbol{\alpha}}, \tag{2.3.10}$$

with possibly zero coefficients $p(\boldsymbol{\alpha})$. Notice that in this form, $P(\mathbf{t})$ agrees exactly with that afforded by (2.3.4) for the two point case. Furthermore, by item (c), the absolute maximal elements of $\widehat{H}(\mathbf{Q})$ appear in the support of $P(\mathbf{t})$.

2.3.2 Poincaré series and its semigroup polynomial

In the previous subsection, we exploited the computational assertion given in Proposition 2.3.4 for coefficients of $P(\mathbf{t})$ so that we could study the support of $P(\mathbf{t})$ in Proposition 2.3.5 and consequently derive the expression (2.3.10) for $P(\mathbf{t})$ in terms of maximal elements of $\widehat{H}(\mathbf{Q})$. However, as observed in Section 2.2, there are infinitely many absolute maximal elements in $\widehat{H}(\mathbf{Q})$, and so the support of $P(\mathbf{t})$ is also infinity. In the following we investigate the outcomes produced by Theorem 2.2.8 in the Poincaré series $P(\mathbf{t})$. With this in mind, let us first take a look at the one and two point cases.

For example, when $\ell = 2$, combining (2.3.4), (2.2.1), and (2.2.5), the Poincaré series can be seen as

$$P(\mathbf{t}) = \sum_{j\in\mathbb{Z}} \mathbf{t}^{(j,\sigma_2(j))} = \left(\sum_{i\in\mathbb{Z}} \mathbf{t}^{i(a,-a)}\right) \cdot \left(\sum_{j=0}^{a-1} \mathbf{t}^{(j,\sigma_2(j))}\right), \tag{2.3.11}$$

where the second factor in the right-hand side is a Laurent polynomial. The relation (2.3.11) actually seems to generalize the functional equation satisfied when $\ell = 1$

$$P(t) = \frac{P^*(t)}{(1-t)} = \left(\sum_{i\in\mathbb{N}_0} t^i\right) \cdot P^*(t), \tag{2.3.12}$$

where $P^*(t)$ is the univariate polynomial

$$t^c + (1-t) \sum_{\substack{\alpha\in H(Q_1)\\ \alpha<c}} t^\alpha$$

for c the conductor of $\widehat{H}(Q_1) = H(Q_1)$, as remarked by Moyano-Fernández in [Moy11, Prop. 2].

We next show that a general formula like (2.3.12) and (2.3.11) also holds in the case of several points as stated in the following theorem.

Theorem 2.3.6. Let $P^*(\mathbf{t})$ be the multivariate Laurent polynomial

$$P^*(\mathbf{t}) := \sum_{\boldsymbol{\alpha}\in\mathcal{M}(\mathbf{Q})\cap\mathcal{C}} p(\boldsymbol{\alpha})\mathbf{t}^{\boldsymbol{\alpha}}.$$

Then the Poincaré series $P(\mathbf{t})$ associated to $\widehat{H}(\mathbf{Q})$ satisfies

$$P(\mathbf{t}) = \left(\sum_{\boldsymbol{\eta}\in\Theta(\mathbf{Q})} \mathbf{t}^{\boldsymbol{\eta}}\right)\cdot P^*(\mathbf{t}). \tag{2.3.13}$$

Proof. Having established $P(\mathbf{t})$ as in (2.3.10), it follows from Theorem 2.2.8 that the proof is completed by showing that $p(\boldsymbol{\alpha}) = p(\boldsymbol{\alpha}+\boldsymbol{\eta})$ for any $\boldsymbol{\alpha}\in\mathcal{M}(\mathbf{Q})\cap\mathcal{C}$ and $\boldsymbol{\eta}\in\Theta(\mathbf{Q})$. Since the coefficiente $p(\boldsymbol{\alpha})$ is as in (2.3.6) for any $i\in I$, it is enough to prove that $d_i(\boldsymbol{\alpha}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i) = d_i(\boldsymbol{\alpha}+\boldsymbol{\eta}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i)$ for any $J\in\mathcal{P}(I\backslash\{i\})$, which is equivalent to show that $\nabla_i\ell(\boldsymbol{\alpha}) = \emptyset$ if and only if $\nabla_i^\ell(\boldsymbol{\alpha}+\boldsymbol{\eta}) = \emptyset$. But that holds true since $\boldsymbol{\eta}, -\boldsymbol{\eta}\in\widehat{H}(\mathbf{Q})$. □

The Laurent polynomial $P^*(\mathbf{t})$ satisfying the functional equation (2.3.13) is called the *semigroup polynomial* associated to $\widehat{H}(\mathbf{Q})$.

We now conclude the present section by proving our Theorem 2.3.3 which summarizes the main properties of Poincaré series associated to Weierstrass semigroups developed along this section.

Proof of Theorem 2.3.3. According to Theorem 2.2.5, the absolute maximal elements in $\widehat{H}(\mathbf{Q})$ determine entirely the semigroup via least upper bounds. Since Proposition 2.3.5 (c) asserts the coefficients of absolute maximal elements in Poincaré series are non-zero, thus the Poincaré series carries sufficient information to determine all the semigroup. Additionally, the Proposition 2.3.6 states that the semigroup polynomial $P^*(\mathbf{t})$ determines finitely the Poincaré series $P(\mathbf{t})$ through the functional equation (2.3.13). This proves the theorem. □

2.4 Symmetry and functional equations

In this section we explore functional equations to Poincaré series of generalized Weierstrass semigroups satisfying a special condition of symmetry. With this aim, we let $\mathcal{X}$ be a curve of genus g defined over $\mathtt{k}$ and $\mathbf{Q} = (Q_1,\ldots,Q_\ell)$ an ℓ-tuple of $\mathtt{k}$-rational points of $\mathcal{X}$ under the same conditions as in Section 2.2. Unless otherwise mentioned, we even assume that $\#\mathtt{k}\geq\ell\geq 2$.

We next introduce a concept of symmetry of generalized Weierstrass semigroups.

Definition 2.4.1. We say that $\widehat{H}(\mathbf{Q})$ is *symmetric* if there exists an element $\boldsymbol{\gamma}\notin\widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\gamma}| = 2g-1$, where g is the genus of $\mathcal{X}$.

Remark 2.4.2. (1) Observe that this notion of symmetry accords and extends precisely that in the case $\ell = 1$, which says that a Weierstrass semigroup $\widehat{H}(Q) = H(Q)$ is symmetric if $2g-1 \notin \widehat{H}(Q)$, where g is genus of the curve. However, Definition 2.4.1 does not make sense to general subsemigroups of $\mathbb{Z}^\ell$ that are not generalized Weierstrass semigroups.

(2) Notice also that since $|\boldsymbol{\gamma}| = 2g-1$, we get by Proposition 1.2.8(ii) that $\ell(\boldsymbol{\gamma}) = g$. As $\boldsymbol{\gamma} \notin \widehat{H}(\mathbf{Q})$, it follows from Proposition 2.1.3 (1) that $\ell(\boldsymbol{\gamma} - \mathbf{e}_i) = \ell(\boldsymbol{\gamma})$ for some $i \in I$. Since $|\boldsymbol{\gamma} - \mathbf{e}_i| = 2g-2$ and $\ell(\boldsymbol{\gamma} - \mathbf{e}_i) = g$, we obtain by Proposition 1.2.8(iii) that $D(\boldsymbol{\gamma} - \mathbf{e}_i)$ is a canonical divisor on $\mathcal{X}$. Therefore, the symmetry property of $\widehat{H}(\mathbf{Q})$ implies the existence of a canonical divisor supported on a subset of $\{Q_1, \ldots, Q_\ell\}$. This is actually an equivalence among other properties satisfied by symmetric generalized Weierstrass semigroups, as we will see in Proposition 2.4.4.

The next lemma generalizes the result stated in [Del90, p. 629] to non-algebraically closed fields. Although their proof follow similar lines, it is necessary some adaptations that we present below.

Lemma 2.4.3. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell$. Then $\nabla(\boldsymbol{\alpha}) = \emptyset$ if and only if there exists a canonical divisor K on $\mathcal{X}$ with $v_{Q_i}(K) = \alpha_i - 1$ for $i = 1, \ldots, \ell$, and $K \geq D(\boldsymbol{\alpha} - \mathbf{1})$.

Proof. Observe that from Proposition 2.1.3 (2) and by Riemann-Roch theorem, we have the following equivalences

$$\begin{aligned}
\nabla(\boldsymbol{\alpha}) = \emptyset &\iff \nabla_j^\ell(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e}_j) = \emptyset \text{ for all } j \in I \\
&\iff \ell(\boldsymbol{\alpha} - \mathbf{1} + \mathbf{e}_j) = \ell(\boldsymbol{\alpha} - \mathbf{1}) \text{ for all } j \in I \\
&\iff \ell(K' - \boldsymbol{\alpha} + \mathbf{1} - \mathbf{e}_j) + 1 = \ell(K' - \boldsymbol{\alpha} + \mathbf{1}) \text{ for all } j \in I \\
&\iff \exists\, f_j \in \mathcal{L}(K' - \boldsymbol{\alpha} + \mathbf{1}) \backslash \mathcal{L}(K' - \boldsymbol{\alpha} + \mathbf{1} - \mathbf{e}_j) \text{ for all } j \in I,
\end{aligned}$$

where K' is a canonical divisor on $\mathcal{X}$. Therefore, $\nabla(\boldsymbol{\alpha}) = \emptyset$ is equivalent to the existence of $f_j \in \mathtt{k}(\mathcal{X})^\times$ for $j = 1, \ldots, \ell$, satisfying

$$v_{Q_j}(f_j) = \alpha_j - v_{Q_j}(K') - 1 \quad \text{and} \quad v_{Q_i}(f_j) \geq \alpha_i - v_{Q_i}(K') - 1 \text{ if } i \neq j.$$

By the assumption $\#\mathtt{k} \geq \ell$, we can proceed exactly as in the proof of Proposition 2.1.3 to choose an appropriate element $(b_1, \ldots, b_\ell) \in \mathtt{k}^\ell$ in order to get $f = \sum_{j=1}^\ell b_j f_j \in R_{\mathbf{Q}}$ with $v_{Q_i}(f) = \alpha_i - v_{Q_i}(K') - 1$ for all $i \in I$, since for any $Q \neq Q_i$ on $\mathcal{X}$ we obtain $v_Q(f) \geq \min_{j=1}^\ell \{v_Q(f_j)\} \geq -v_Q(K')$. Consequently, the canonical divisor $K = \operatorname{div}(f) + K'$ satisfies $v_{Q_i}(K) = \alpha_i - 1$ and $K - D(\boldsymbol{\alpha} - \mathbf{1}) \geq 0$, which is the desired conclusion. □

We present below an additional equivalence to the statements established by Delgado in [Del90, p. 630] and revisited by Moyano-Fernández in [Moy11, Th. 3] with further details.

Proposition 2.4.4. The following conditions are equivalent:

(1) $\widehat{H}(\mathbf{Q})$ is symmetric;

(2) There exists a canonical divisor K on $\mathcal{X}$ such that $\mathrm{Supp}(K) \subseteq \{Q_1, \ldots, Q_\ell\}$;

(3) There exists $\boldsymbol{\sigma} \in \widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\sigma}| = 2g - 2 + \ell$ satisfying the property:

$$\text{If } \boldsymbol{\beta} \in \mathbb{Z}^\ell, \text{ then } \boldsymbol{\beta} \in \widehat{H}(\mathbf{Q}) \text{ if and only if } \nabla(\boldsymbol{\sigma} - \boldsymbol{\beta}) = \emptyset.$$

Proof. (1) $\Rightarrow$ (2) It is exactly that stated in Remark 2.4.2(2).
(2) $\Rightarrow$ (3) Let K be a canonical divisor on $\mathcal{X}$ such that $K = D(\boldsymbol{\delta})$ for $\boldsymbol{\delta} \in \mathbb{Z}^\ell$ with $|\boldsymbol{\delta}| = 2g - 2$. Taking $\boldsymbol{\sigma} = \boldsymbol{\delta} + \mathbf{1}$, we have $\boldsymbol{\sigma} \in \widehat{H}(\mathbf{Q})$ because $|\boldsymbol{\sigma}| = 2g - 2 + \ell$ with $\ell \geq 2$. If $\boldsymbol{\beta} \in \widehat{H}(\mathbf{Q})$, then $\nabla(\boldsymbol{\sigma} - \boldsymbol{\beta}) = \emptyset$ since otherwise, one would have $\nabla(\boldsymbol{\sigma}) \neq \emptyset$. Conversely, for any $\boldsymbol{\beta} \in \mathbb{Z}^\ell$, assume $\nabla(\boldsymbol{\sigma} - \boldsymbol{\beta}) = \emptyset$. Then, by the Lemma 2.4.3, there exists a canonical divisor K' on $\mathcal{X}$ such that $v_{Q_i}(K') = \sigma_i - \beta_i - 1$ for all $i \in I$ and $K' \geq D(\boldsymbol{\sigma} - \boldsymbol{\beta} - \mathbf{1})$. Thus, there exists $f \in \mathtt{k}(\mathcal{X})^\times$ such that $K' = K + \mathrm{div}(f)$. We claim that $f \in R_{\mathbf{Q}}$, because as $v_Q(f) = v_Q(K') - v_Q(K) = v_Q(K')$ and $K' \geq D(\boldsymbol{\sigma} - \boldsymbol{\beta} - \mathbf{1})$, then $v_Q(f) \geq 0$ if $Q \neq Q_i$ and $-v_{Q_i}(f) = (\sigma_i - 1) - (\sigma_i - \beta_i - 1) = \beta_i$ for every $i \in I$. Therefore, $\boldsymbol{\beta} \in \widehat{H}(\mathbf{Q})$.
(3) $\Rightarrow$ (1) Note that $\boldsymbol{\sigma} - \mathbf{1} + \mathbf{e}_i \notin \widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\sigma} - \mathbf{1} + \mathbf{e}_i| = 2g - 1$ for all $i \in I$, since otherwise $\boldsymbol{\sigma} - \mathbf{1} + \mathbf{e}_i \in \nabla_i(\boldsymbol{\sigma})$, which does not happen because $\boldsymbol{\sigma} \in \mathcal{M}(\mathbf{Q})$. □

Remark 2.4.5. (1) From the proof above, if an element $\boldsymbol{\sigma} \in \widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\sigma}| = 2g - 2 + \ell$, then $D(\boldsymbol{\sigma} - \mathbf{1})$ is a canonical divisor on $\mathcal{X}$. Hence, there exists a canonical divisor K on $\mathcal{X}$ whose support is exactly $\{Q_1, \ldots, Q_\ell\}$ if and only if there exists an element $\boldsymbol{\sigma} \in \widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\sigma}| = 2g - 2 + \ell$ and $\sigma_i \neq 1$ for $i = 1, \ldots, \ell$.

(2) Notice that, if $\widehat{H}(\mathbf{Q})$ is symmetric, then for each $\boldsymbol{\alpha} \in \mathcal{M}(\mathbf{Q})$ there exists an unique $\boldsymbol{\beta} \in \mathcal{M}(\mathbf{Q})$ such that $\boldsymbol{\alpha} + \boldsymbol{\beta} = \boldsymbol{\sigma}$. Indeed, taking $\boldsymbol{\beta} = \boldsymbol{\sigma} - \boldsymbol{\alpha}$, we have $\boldsymbol{\beta} \in \widehat{H}(\mathbf{Q})$ since $\nabla(\boldsymbol{\sigma} - \boldsymbol{\beta}) = \nabla(\boldsymbol{\alpha}) = \emptyset$. Furthermore, $\nabla(\boldsymbol{\beta}) = \emptyset$ because $\boldsymbol{\alpha} \in \widehat{H}(\mathbf{Q})$. Therefore, $\boldsymbol{\beta} = \boldsymbol{\sigma} - \boldsymbol{\alpha} \in \mathcal{M}(\mathbf{Q})$. As a consequence, we obtain that $\boldsymbol{\sigma} \in \mathcal{M}(\mathbf{Q})$ since $\mathbf{0} \in \mathcal{M}(\mathbf{Q})$.

The following technical lemma provides a relation that will be used in Theorem 2.4.7 to derive a functional equation for Poincaré series associated to symmetric Weierstrass semigroups. It is a version of [CDK94, Th. 3.6] adapted to our setting.

Lemma 2.4.6. Let $\boldsymbol{\alpha} \in \mathbb{Z}^m$ and $i \in I$. If $\widehat{H}(\mathbf{Q})$ is symmetric then

$$d_i(\boldsymbol{\alpha}) + d_i(\boldsymbol{\sigma} - \boldsymbol{\alpha} - \mathbf{1} + \mathbf{e}_i) = 1,$$

where $\boldsymbol{\sigma}$ is a maximal element of $\widehat{H}(\mathbf{Q})$ as in Proposition 2.4.4 (3).

Proof. From Remark 2.4.5 (1), we have $D(\boldsymbol{\sigma} - \mathbf{1})$ is a canonical divisor on $\mathcal{X}$. Hence, from Riemann-Roch theorem we obtain

$$\ell(\boldsymbol{\alpha}) = |\boldsymbol{\alpha}| + 1 - g + \ell(\boldsymbol{\sigma} - \boldsymbol{\alpha} - \mathbf{1}) \tag{2.4.1}$$

and

$$\ell(\boldsymbol{\alpha}-\mathbf{e}_i)=|\boldsymbol{\alpha}|-g+\ell(\boldsymbol{\sigma}-\boldsymbol{\alpha}-\mathbf{1}+\mathbf{e}_i), \tag{2.4.2}$$

which completes the proof by subtracting (2.4.2) from (2.4.1). □

In [Moy11, Prop. 6], the Poincaré series associated to symmetric generalized Weierstrass semigroups at two points are shown to satisfy the functional equation

$$P(\mathbf{t})=\mathbf{t}^{\boldsymbol{\sigma}}P(\mathbf{t}^{-1}), \tag{2.4.3}$$

where $\boldsymbol{\sigma}$ is as in Proposition 2.4.4 (3). We can now formulate a generalization of the functional equations (2.4.3) to multivariable Poincaré series of generalized Weierstrass semigroups at several points.

Theorem 2.4.7. If $\widehat{H}(\mathbf{Q})$ is symmetric then its corresponding Poincaré series satisfies

$$P(\mathbf{t})=(-1)^{\ell}\mathbf{t}^{\boldsymbol{\sigma}}P(\mathbf{t}^{\mathbf{-1}}),$$

where $\boldsymbol{\sigma}$ is a maximal element of $\widehat{H}(\mathbf{Q})$ as in Proposition 2.4.4 (3).

Proof. Let $\boldsymbol{\alpha}\in\mathbb{Z}^{\ell}$. Notice that $d_i(\boldsymbol{\alpha}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i)=d_i(\boldsymbol{\alpha}-\mathbf{1}_{J^c})$ for every $J\in\mathcal{P}(I\backslash\{i\})$. Since $(-1)^{\#J^c}=(-1)^{\ell-1}(-1)^{\#J}$, we can write

$$p(\boldsymbol{\alpha})=p_i(\boldsymbol{\alpha})=(-1)^{\ell-1}\sum_{J\in\mathcal{P}(I\backslash\{i\})}(-1)^{\#J}d_i(\boldsymbol{\alpha}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i)=\sum_{J\in\mathcal{P}(I\backslash\{i\})}(-1)^{\#J}d_i(\boldsymbol{\alpha}-\mathbf{1}_J)$$

and

$$(-1)^{\ell-1}p(\boldsymbol{\sigma}-\boldsymbol{\alpha})=(-1)^{\ell-1}p_i(\boldsymbol{\sigma}-\boldsymbol{\alpha})=\sum_{J\in\mathcal{P}(I\backslash\{i\})}(-1)^{\#J}d_i(\boldsymbol{\sigma}-\boldsymbol{\alpha}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i).$$

We thus obtain the following relation by Lemma 2.4.6

$$\begin{aligned}p(\boldsymbol{\alpha})+(-1)^{\ell-1}p(\boldsymbol{\sigma}-\boldsymbol{\alpha})&=\sum_{J\in\mathcal{P}(I\backslash\{i\})}(-1)^{\#J}[d_i(\boldsymbol{\alpha}-\mathbf{1}_J)+d_i(\boldsymbol{\sigma}-\boldsymbol{\alpha}-\mathbf{1}+\mathbf{1}_J+\mathbf{e}_i)]\\&=\quad 0.\end{aligned} \tag{2.4.4}$$

Hence, using the expression (2.3.10) for $P(\mathbf{t})$ and $p(\boldsymbol{\alpha})=(-1)^{\ell}p(\boldsymbol{\sigma}-\boldsymbol{\alpha})$ by (2.4.4), it follows from Remark 2.4.5 (2) that

$$\begin{aligned}P(\mathbf{t})&=\sum_{\boldsymbol{\alpha}\in\mathcal{M}(\mathbf{Q})}p(\boldsymbol{\alpha})\mathbf{t}^{\boldsymbol{\alpha}}\\&=(-1)^{\ell}\sum_{\boldsymbol{\alpha}\in\mathcal{M}(\mathbf{Q})}p(\boldsymbol{\sigma}-\boldsymbol{\alpha})\mathbf{t}^{\boldsymbol{\alpha}}\\&=(-1)^{\ell}\sum_{\boldsymbol{\beta}\in\mathcal{M}(\mathbf{Q})}p(\boldsymbol{\beta})\mathbf{t}^{\boldsymbol{\sigma}-\boldsymbol{\beta}}\\&=(-1)^{\ell}\mathbf{t}^{\boldsymbol{\sigma}}\sum_{\boldsymbol{\beta}\in\mathcal{M}(\mathbf{Q})}p(\boldsymbol{\beta})\mathbf{t}^{-\boldsymbol{\beta}}\\&=(-1)^{\ell}\mathbf{t}^{\boldsymbol{\sigma}}P(\mathbf{t}^{-1}).\end{aligned}$$

□

In particular, we can also derive an functional equation for $Q(\mathbf{t})$ as follows.

Corollary 2.4.8. If $\widehat{H}(\mathbf{Q})$ is symmetric, the following functional equation holds true

$$Q(\mathbf{t}) = (-1)^{\ell-1}\mathbf{t}^{\boldsymbol{\sigma}}Q(\mathbf{t}^{-\mathbf{1}}),$$

where $\boldsymbol{\sigma}$ is a maximal element of $\widehat{H}(\mathbf{Q})$ as in Proposition 2.4.4 (3).

Proof. Let $\boldsymbol{\alpha} \in \mathbb{Z}^{\ell}$. From the Proposition 2.3.4 and the relation (2.4.4), we get

$$\begin{aligned} q(\boldsymbol{\alpha}) &= p(\boldsymbol{\alpha}) - p(\boldsymbol{\alpha} - \mathbf{1}) \\ &= (-1)^{\ell}(p(\boldsymbol{\sigma} - \boldsymbol{\alpha}) - p(\boldsymbol{\sigma} - \boldsymbol{\alpha} + \mathbf{1})) \\ &= (-1)^{\ell-1}(p(\boldsymbol{\sigma} - \boldsymbol{\alpha} + \mathbf{1}) - p(\boldsymbol{\sigma} - \boldsymbol{\alpha})) \\ &= (-1)^{\ell-1}q(\boldsymbol{\sigma} - \boldsymbol{\alpha} + \mathbf{1}), \end{aligned}$$

which proves the assertion. □

Chapter 3

Castle conditions on multipointed curves

Remember from Section 1.3 that an algebraic-geometric code is constructed on a curve $\mathcal{X}$ over a finite field by considering two rational divisors on $\mathcal{X}$ of disjoint support, D and G. When the latter is a multiple of a single point $Q \in \mathcal{X}(\mathbb{F}_q)$ outside the support of D, the code is called a *one-point code*. Otherwise, if $\#\mathrm{Supp}(G) \geq 2$, it is called a *multipoint code*.

One-point codes are the most studied codes among the whole family of AG codes and are in general well studied; see e.g. [HVP98; Duu08; MO15]. The main techniques in the study of the parameters of $C_{\mathcal{L}}(\mathcal{X}, D, mQ)$ (or $C_{\Omega}(\mathcal{X}, D, mQ)$) rely on the Weierstrass semigroup of $\mathcal{X}$ at Q. This numerical semigroup codifies the dimension behaviour of any one-point codes with $G = mQ$, and is also used to bound the minimum weight of codewords in one-point codes, which led to the formulation of order bounds on the minimum distance of one-point codes [Gei+11].

In particular, when the curve has some arithmetical properties, the study of parameters become simpler. This is the case of Castle and weak Castle curves [MST09; OM13], which encapsulates good properties on two simple arithmetical conditions. These curves have the good properties of the main important curves used to construct one-point codes. It allows us to give a theoretical treatment of the main one-point codes, unifying the theory behind them.

Matthews observed in [Mat01] that there exist multipoint codes with better parameters than any comparable one-point code. The strategy employed was selecting special divisors G with the aid of Weierstrass semigroups at several points. This led to improvements on the Goppa bound and consequently derived multipoint codes which can not be obtained as a punctured one-point code. These considerations led to the rise of many works on multipoint codes, specially on methods devoted to estimating their true minimum distances; see [DKP11] and the references therein.

In this chapter, we deal with multipoint codes constructed on curves satisfying certain conditions which extend naturally the arithmetic and geometric assumptions satisfied by Castle

and weak-Castle curves to multi-pointed curves. The main objective is to provide a systematic approach based on generalized Weierstrass semigroups at several points to treat multipoint AG codes. For this reason, we will make use of some terminology and results developed in Chapter 2.

3.1 Castle curves and one-point codes

We start this section by recalling the notion of Castle and weak Castle curves and their main features introduced in [MST09]. In particular, we shall focus our attention on describing the one-point codes arising from these curves, which contains many of the most known examples of one-point codes.

Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible algebraic curve of genus g defined over $\mathbb{F}_q$, and let Q be a rational point on $\mathcal{X}$. Recall that the Weierstrass semigroup of $\mathcal{X}$ at Q

$$H(Q) = \{\alpha \in \mathbb{N}_0 \ : \ \exists \ f \in \mathbb{F}_q(\mathcal{X})^\times \text{ with } \operatorname{div}_\infty(f) = \alpha Q\},$$

where $\mathbb{F}_q(\mathcal{X})$ is the function field of $\mathcal{X}$, is said symmetric if $2g-1 \notin H(Q)$. The Lewittes bound [OM13] yields an upper bound on the number of rational points of the pointed curve $(\mathcal{X}, Q)$

$$\#\mathcal{X}(\mathbb{F}_q) \leq q\rho(Q) + 1, \tag{3.1.1}$$

where $\rho(Q)$ is the first non-zero element of $H(Q)$, the *multiplicity* of $H(Q)$.

A pointed curve $(\mathcal{X}, Q)$ is called *Castle* if

(C1) The Weierstrass semigroup $H(Q)$ is symmetric; and

(C2) $\#\mathcal{X}(\mathbb{F}_q) = q\rho(Q) + 1$, that is, the number of rational points of $\mathcal{X}$ attains the Lewittes bound.

Many notable curves over finite fields satisfy the conditions above, for example Hermitian curves, Suzuki curves, Ree curves, and Norm-Trace curves, among others; see [MST09]. These examples are among the most studied curves for applications to one-point algebraic-geometric codes.

The concept of Castle curves can be generalized in the following way. A pointed curve $(\mathcal{X}, Q)$ over $\mathbb{F}_q$ satisfying (C1) and

(C2′) There exist a morphism $f : \mathcal{X} \to \mathbb{P}^1$ with $\operatorname{div}_\infty(f) = dQ$ and a set $U = \{\alpha_1, \ldots, \alpha_h\} \subseteq \mathbb{F}_q$ such that for all $i = 1, \ldots, h$, we have

$$f^{-1}(\alpha_i) \subseteq \mathcal{X}(\mathbb{F}_q) \ \text{ and } \ \#f^{-1}(\alpha_i) = d.$$

is called *weak Castle*.

Every Castle curve is in fact weak Castle; indeed, it is enough to observe that $f \in \mathbb{F}_q(\mathcal{X})^\times$ with $\mathrm{div}_\infty(f) = \rho(Q)Q$ and $U = \mathbb{F}_q$ satisfy the condition (C2'). Conversely, under the assumption of (C2'), we obtain $d \in H(Q)$. Furthermore, since f is unramified over each α_i, writing $f^{-1}(\alpha_i) = \{P_1^i, \ldots, P_d^i\}$, we have

$$\mathrm{div}(f - \alpha_i) = \sum_{j=1}^{d} P_j^i - dQ.$$

Let

$$D = D_{U,f} = \sum_{i=1}^{h} \sum_{j=1}^{d} P_j^i.$$

If $(\mathcal{X}, Q)$ is weak Castle and D is the sum of all rational points different from Q, it is said to be *complete*. The one-point codes $C_\mathcal{L}(D, mQ)$ of length $n = dh$ are called *weak Castle codes*, or simply *Castle codes* if $(\mathcal{X}, Q)$ satisfies (C2).

Castle and weak Castle curves have several nice properties that can be translated to codes arising from them. Next we see some these results obtained in [MST09].

Proposition 3.1.1. Let $(\mathcal{X}, Q)$ be a weak Castle curve of genus g over $\mathbb{F}_q$. The following hold.

(1) The divisors D and nQ are linearly equivalent. Then for $m < n$, $C_\mathcal{L}(D, mQ)$ reaches the Goppa bound if and only if $C_\mathcal{L}(D, (n-m)Q)$ does. For $m \geq n$, $C_\mathcal{L}(D, mQ)$ is an abundant code of abundance $\ell((m-n)Q)$.

(2) The divisor $(2g-2)Q$ is a canonical divisor on $\mathcal{X}$. Consequently, $(n+2g-2)Q - D$ is also a canonical divisor and there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that

$$C_\mathcal{L}(D, mQ)^\perp = \mathbf{x} * C_\mathcal{L}(D, m^\perp Q),$$

where $m^\perp = n + 2g - 2 - m$.

The vector $\mathbf{x}$ of item (2) does not depend on m and can be computed as in Proposition 1.3.3. It is also interesting to note that when $(\mathcal{X}, Q)$ is weak Castle, the set

$$M = \{m \in \mathbb{N}_0 \ : \ C_\mathcal{L}(D, mQ) \neq C_\mathcal{L}(D, (m-1)Q)\} = \{m_1 = 0, m_2, \ldots, m_n\},$$

called the *dimension set* of $(\mathcal{X}, Q)$, can easily computed as $M = H(Q) \setminus (n + H(Q))$. This set can be used to obtain good estimates on the minimum distance of codes $C_\mathcal{L}(D, m_iQ)$ by applying the order bound [Gei+11]. For further information on the order bound for Castle codes see [OM13].

3.2 Castle conditions for multi-pointed curves

In this section, we extend the ideas in Section 3.1 to multi-pointed curves and show some examples of curves satisfying this notion. The aim is to provide an useful framework for multi-pointed curves to deal with multipoint codes; we also show some examples to illustrate the theory.

Let $\mathcal{X}$ be a curve of genus g defined over $\mathbb{F}_q$. Let $Q_1, ..., Q_\ell \in \mathcal{X}(\mathbb{F}_q)$ be $\ell \geq 2$ pairwise distinct $\mathbb{F}_q$-rational points, and set $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$. Remember from Section 2.4 that the generalized Weierstrass semigroup $\widehat{H}(\mathbf{Q})$ is called symmetric if there exists $\boldsymbol{\gamma} \notin \widehat{H}(\mathbf{Q})$ with $|\boldsymbol{\gamma}| = 2g-1$. Recall also that for $\boldsymbol{\alpha} \in \mathbb{Z}^m$ we have $D(\boldsymbol{\alpha}) = \sum_{i=1}^{\ell} \alpha_i Q_i$.

Definition 3.2.1. Let $\ell \geq 2$. We say that an ℓ-pointed curve $(\mathcal{X}, \mathbf{Q})$ is of *Castle type* if it satisfies the following:

(i) The generalized Weierstrass semigroup $\widehat{H}(\mathbf{Q})$ is symmetric; and

(ii) There exist a morphism $\phi : \mathcal{X} \longrightarrow \mathbb{P}^1$ with $\mathrm{div}_\infty(\phi) = D(\boldsymbol{\alpha})$ and $\gamma_1, \ldots, \gamma_h \in \mathbb{F}_q$ satisfying $\#\phi^{-1}(\gamma_i) = |\boldsymbol{\alpha}|$ and $\phi^{-1}(\gamma_i) \subseteq \mathcal{X}(\mathbb{F}_q)$ for $i = 1, \ldots, h$.

Remark 3.2.2.

1. Observe that this definition is a natural extension of the notion of weak Castle curves to several points.

2. The condition (i) ensures, by Proposition 2.4.4, the existence of a canonical divisor on $\mathcal{X}$ whose support contained in $\{Q_1, \ldots, Q_\ell\}$. We can also see that if a generalized Weierstrass semigroup at ℓ-tuple of rational points is symmetric, then any other generalized Weierstrass semigroup at m'-tuple, $\ell' > \ell$, containing the ℓ previous points is symmetric.

3. The condition (ii) says that $\boldsymbol{\alpha} \in H(\mathbf{Q})$ and that $\mathcal{X}$ cover $\mathbb{P}^1$ via ϕ in a such way that h elements $\gamma \in \mathbb{F}_q$ are completely split and whose fibres $\phi^{-1}(\gamma)$ are rational points. We can thus deduce that
$$\#\mathcal{X}(\mathbb{F}_q) \geq h|\boldsymbol{\alpha}| + \ell. \tag{3.2.1}$$

Next, we present some examples of multi-pointed curves of Castle type.

Example 3.2.3. Let $\mathcal{K}$ be the Klein quartic over $\mathbb{F}_8$ defined by the projective equation

$$X^3Y + Y^3Z + XZ^3 = 0.$$

It is a genus 3 curve with 24 rational points. Let us consider the rational points $P := (0:0:1)$, $Q := (0:1:0)$ and $R := (1:0:0)$ of $\mathcal{K}$. The Klein quartic if of Castle type at the pair (Q, R). Considering the rational functions $x = X/Z$ and $y = Y/Z$, we have

$$\mathrm{div}(x) = 3P - (2Q + R)$$

and

$$\mathrm{div}(y) = P + 2R - 3Q.$$

Hence, for $i, j \in \mathbb{Z}$, we obtain

$$\mathrm{div}(x^i y^j) = (3i + j)P + (-2i - 3j)Q + (-i + 2j)R,$$

and it is possible to determine the generalized Weierstrass semigroup of the Klein quartic at the pair (Q, R) as in Figure 3.1.

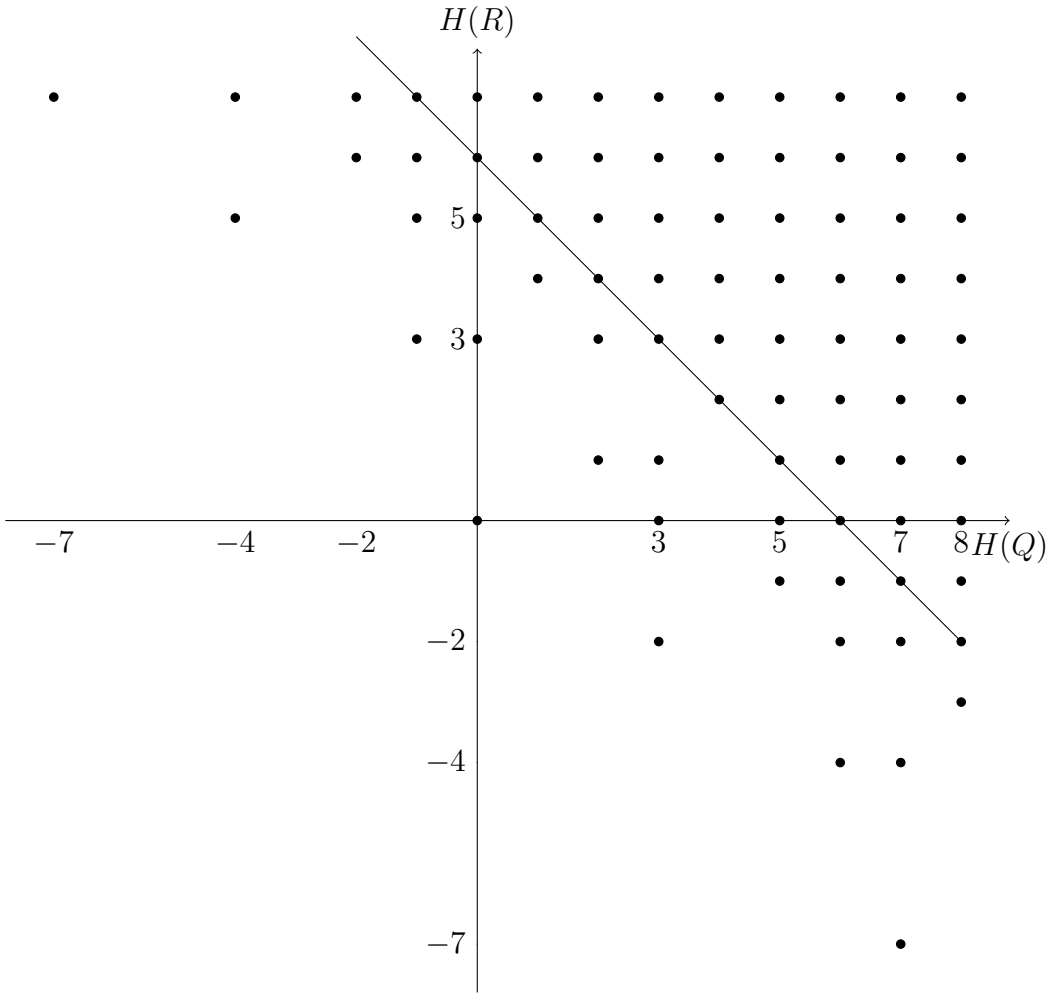

Figure 3.1: Generalized Weierstrass semigroup of $\mathcal{K}$ at (Q, R).

Notice that although the numerical Weierstrass semigroups $H(Q) = H(R) =< 3, 5, 7 >$ are not symmetric, $\widehat{H}(Q, R)$ is symmetric because neither $(3, 2)$ nor $(4, 1)$ belongs to $\widehat{H}(Q, R)$. The morphism $\phi = (y^7 + 1)/y^5x^2$ has pole divisor $10Q + 12R$, and each element in $\mathcal{K}(\mathbb{F}_8)\backslash\{Q, R\}$ is a zero for ϕ. Therefore $\mathcal{K}$ is of Castle type for the pair (Q, R) with ϕ, $h = 1$, and $\alpha_1 = 0 \in \mathbb{F}_q$. On the other hand, considering the morphism $\phi = x$, we have $\mathrm{div}_\infty(\phi) = 2Q + R$ and any $\alpha \in \mathbb{F}_q^\times$ is totally split. Hence, each of 21 point of $\mathcal{K}(\mathbb{F}_8)\backslash\{P, Q, R\}$ belongs to fibre $\phi^{-1}(\mathbb{F}_q^\times)$.

By Remark 3.2.2, $\mathcal{K}$ is also Castle for the triple (P, Q, R). Observe that in both case, the equality in Equation (3.2.1) is attained.

For our coding purposes, we are particularly interested in morphisms ϕ as in Definition 3.2.1(ii) whose number $h|\boldsymbol{\alpha}|$ of rational points in $\bigcup_{i=1}^{h} \phi^{-1}(\gamma_i)$ equals $\#\mathcal{X}(\mathbb{F}_q) - \ell$ in Equation (3.2.1). However, it is not always possible to obtain a suited morphism ϕ with this property, as we will see in next example.

Example 3.2.4. Let q be an odd prime power. Let $\mathcal{X}$ be the hyperelliptic curve defined over $\mathbb{F}_q$ given by affine equation

$$y^2 = x^q - x + 1.$$

Note that $\mathcal{X}$ is a Castle curve with $2q + 1$ rational points. Nevertheless, for Q the point at infinity of $\mathcal{X}$ and $P = (0 : 1 : 1)$, there is no morphism ϕ with pole divisor supported on $\{Q, P\}$ such that the equality in (3.2.1) holds. It can be reinterpreted that the divisor $D = \sum_{P \in \mathcal{X}(\mathbb{F}_q) \setminus \{Q_1, Q_2\}} P$ of degree $2q - 1$ is not linearly equivalent to any divisor supported on $\{Q_1, Q_2\}$.

The following result generalizes a property of the weak Castle pointed curves which will enable us to consider AG codes via the generalized Weierstrass semigroups.

Proposition 3.2.5. With the notation as above, let $(\mathcal{X}, \mathbf{Q})$ be a multi-pointed curve over $\mathbb{F}_q$ satisfying the Castle condition with $\phi : \mathcal{X} \longrightarrow \mathbb{P}^1$ the morphism associated to $\boldsymbol{\alpha} \in H(\mathbf{Q})$. Consider the divisor $D := \sum_{i=1}^{h} \sum_{P \in \phi^{-1}(\gamma_i)} P$. Then

(1) For each $\gamma_i \in \mathbb{F}_q$ such that $\#(\phi^{-1}(\gamma_i) \cap \mathcal{X}(\mathbb{F}_q)) = |\boldsymbol{\alpha}|$, we have

$$\operatorname{div}(\phi - \gamma_i) = D_{\gamma_i} - D(\boldsymbol{\alpha}),$$

where $D_{\gamma_i} = \sum_{P \in \phi^{-1}(\gamma_i)} P \leq D$;

(2) $D \sim hD(\boldsymbol{\alpha})$.

Proof. Since ϕ is unramified over each $\gamma_i \in \mathbb{F}_q$, and $\operatorname{div}_\infty(\phi) = D(\boldsymbol{\alpha})$, we have

$$\operatorname{div}(\phi - \gamma_i) = \sum_{P \in \phi^{-1}(\gamma_i)} P - D(\boldsymbol{\alpha}) = D_{\gamma_i} - D(\boldsymbol{\alpha}).$$

Hence the divisor of the function $z = \prod_{i=1}^{h} (\phi - \gamma_i)$ is

$$\operatorname{div}(z) = \sum_{i=1}^{h} D_{\gamma_i} - hD(\boldsymbol{\alpha}),$$

and therefore $D \sim hD(\boldsymbol{\alpha})$. □

Example 3.2.6. Let q be a prime power. Let $\mathcal{H}_q$ be the Hermitian curve over $\mathbb{F}_{q^2}$ as in Example 2.2.9. Let Q be the point at infinity on $\mathcal{H}_q$, and let Q_i denote the common zero of x and $y - b_i$, where $b_i \in \mathbb{F}_{q^2}$ satisfy $b_i^q + b_i = 0$ for $i = 1, \ldots, q$. Let $\mathbf{Q}_j = (Q, Q_1, \ldots, Q_j)$ be $(j+1)$-tuple of points on $\mathcal{H}_q$. As

$$\operatorname{div}(x^q - x) = D' - q^3 Q$$

and

$$\operatorname{div}(y - b_i) = (q+1)(Q_i - Q),$$

for $j = 1, \ldots, q$, we obtain

$$\operatorname{div}\left(\frac{x^q - x}{y(y-b_1)\cdots(y-b_j)}\right) = D_i - qQ_1 - \cdots - qQ_j - (q^3 - j(q+1))Q$$

The divisor D as in Proposition 3.2.5 will be used in next section to construct multipoint AG codes, and its degree will be related to the length of such codes. This is the reason that we search for curves of Castle type with maximum value as possible in the right-hand side in Equation (3.2.1). From this problem, we have the following question: given an ℓ-pointed curve $(\mathcal{X}, \mathbf{Q})$ with $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$ such that $\widehat{H}(\mathbf{Q})$ is symmetric, what are the $\boldsymbol{\alpha} \in H(\mathbf{Q})$ such that $(\mathcal{X}, \mathbf{Q})$ is of Castle type with $h|\boldsymbol{\alpha}|+\ell$ as big as possible? In this case, is it possible to characterize such elements $\boldsymbol{\alpha} \in H(\mathbf{Q})$?

3.3 Multipoint Castle codes

This section is devoted to study multipoint AG codes constructed on curves of Castle type. In particular, we interpret the parameters of these multipoint codes in terms of the theory of generalized Weierstrass semigroups at several points developed in Chapter 2.

Let $\mathcal{X}$ be a curve of genus g defined over $\mathbb{F}_q$, and let $\mathbf{Q} = (Q_1, ..., Q_\ell)$ be an ℓ-tuple of pairwise distinct rational points such that the pair $(\mathcal{X}, \mathbf{Q})$ if of Castle type. Hence there exists $\boldsymbol{\alpha} \in H(\mathbf{Q})$ satisfying (ii) in Definition 3.2.1. Let D be the associated divisor according to Proposition 3.2.5.

For $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}^\ell$ with $0 \leq |\boldsymbol{\beta}| \leq h|\boldsymbol{\alpha}|+2g-2$, let $D(\boldsymbol{\beta}) = \sum_{i=1}^{\ell} \beta_i Q_i$. Consider hereafter the algebraic-geometric codes

$$C(\boldsymbol{\beta}) := C_{\mathcal{L}}(\mathcal{X}, D, D(\boldsymbol{\beta}))$$

of length $n := h|\boldsymbol{\alpha}|$, called *multipoint Castle codes*.

3.3.1 Duality

One characteristic of one-point Castle codes is that their dual are formally equivalent to another one-point Castle code. This property can be also extended to the family of multipoint Castle codes.

Proposition 3.3.1. The dual code $C(\boldsymbol{\beta})^{\perp}$ of $C(\boldsymbol{\beta})$ is formally equivalent to $C(\boldsymbol{\beta}')$ for some $\boldsymbol{\beta}' \in \mathbb{Z}^{\ell}$ with $|\boldsymbol{\beta}'| \geq 0$.

Proof. We first notice that from Theorem 1.3.2 and Proposition 1.3.3, the dual code $C(\boldsymbol{\beta})^{\perp}$ is formally equivalent to $C_{\mathcal{L}}(D, D + \operatorname{div}(\omega) - D(\boldsymbol{\beta}))$, where ω is a differential form with simple poles at $P \in \phi^{-1}(\gamma_i)$ for $i = 1, \ldots, h$. Let us consider the rational function $z = \prod_{i=1}^{h}(\phi - \alpha_i)$. Since z has simple zeros at $P \in \phi^{-1}(\gamma_i)$ for $i = 1, \ldots, h$, the differential form $\omega = dz/z$ has simple poles at $P \in \phi^{-1}(\gamma_i)$ for $i = 1, \ldots, h$. From Proposition 2.4.4 we obtain

$$D + \operatorname{div}(\omega) - D(\boldsymbol{\beta}) = D + \operatorname{div}(dz) - \operatorname{div}(z) - D(\boldsymbol{\beta}) = \operatorname{div}(dz) + hD(\boldsymbol{\alpha}) - D(\boldsymbol{\beta}).$$

Since $\widehat{H}(\mathbf{P})$ is symmetric, there exists a canonical divisor K supported on a subset of $\{Q_1, ..., Q_{\ell}\}$ by Proposition 2.4.4, and thus there exists $\boldsymbol{\sigma} \in \mathbb{Z}^{\ell}$ with $|\boldsymbol{\sigma}| = 2g - 2$ such that $K = D(\boldsymbol{\sigma})$. As $\operatorname{div}(dz) \sim D(\boldsymbol{\sigma})$, we have

$$D + \operatorname{div}(\eta) - D(\boldsymbol{\beta}) \sim D(\boldsymbol{\beta}'),$$

where $\boldsymbol{\beta}' = \boldsymbol{\sigma} + h\boldsymbol{\alpha} - \boldsymbol{\beta}$ with $|\boldsymbol{\beta}'| \geq 0$. The assertion thus follows by Proposition 1.3.5(a). □

3.3.2 Dimension

We next discuss a systematic method to compute the dimension of multipoint Castle codes through generalized Weierstrass semigroups. Let $k_{\boldsymbol{\beta}}$ denote the dimension of the code $C(\boldsymbol{\beta})$. From Proposition 3.2.5, we have $D \sim hD(\boldsymbol{\alpha}) = D(h\boldsymbol{\alpha})$, and since $k_{\boldsymbol{\beta}} = \ell(\boldsymbol{\beta}) - \ell(D(\boldsymbol{\beta}) - D)$ by (1.3.1), we can deduce

$$k_{\boldsymbol{\beta}} = \ell(\boldsymbol{\beta}) - \ell(\boldsymbol{\beta} - h\boldsymbol{\alpha}).$$

It means that the dimensions $k_{\boldsymbol{\beta}}$ are given in terms of divisors supported on a subset of $\{Q_1, \ldots, Q_{\ell}\}$, and we can thus use generalized Weierstrass semigroups to compute them by using Theorem 2.2.6 which states that for any $\boldsymbol{\alpha} \in \mathbb{Z}^{\ell}$ and $i \in \{1, \ldots, \ell\}$ we have

$$\ell(\boldsymbol{\alpha}) = \#(\Gamma(\boldsymbol{\alpha})/\equiv_i),$$

where $\Gamma(\boldsymbol{\alpha})$ and $\equiv_i$ are respectively as in (2.2.3) and (2.2.4). Furthermore, since dimensions are invariant for elements $\boldsymbol{\alpha} \in \mathbb{Z}^{\ell}$ modulo $\Theta(\mathbf{Q})$ by Corollary 2.2.10, this computation can be reduced to $\ell(\boldsymbol{\alpha}')$ for $\boldsymbol{\alpha}' \in \mathcal{C}$ in the equivalence class $[\boldsymbol{\alpha}]$ for the relation $\equiv$ defined in (2.2.8). Therefore, once the absolute maximal elements in the generalized Weierstrass semigroup of $\mathcal{X}$

at $\mathbf{Q} = (Q_1, \ldots, Q_\ell)$ are known, the dimensions $k_{\boldsymbol{\beta}}$ of the codes $C(\boldsymbol{\beta})$ can be computed via Theorem 2.2.6 to calculate $\ell(\boldsymbol{\beta})$ and $\ell(\boldsymbol{\beta} - h\boldsymbol{\alpha})$ separately.

3.3.3 Minimum distance

In the following we present some methods based on generalized Weierstrass semigroups to estimate the minimum distance of multipoint Castle codes. Let $d_{\boldsymbol{\beta}}$ denote the minimum distance of $C_{\boldsymbol{\beta}}$. Recall from Section 1.3 that for each integer $r \geq 1$, the *gonality sequence of* $\mathcal{X}$ is given by

$$\lambda_r = \min\{\deg(A) \ : \ A \in \mathrm{Div}_{\mathbb{F}_q}(\mathcal{X}) \text{ with } \ell(A) \geq r\}.$$

Hence, according to the improved Goppa bound (1.3.2), we get

$$d_{\boldsymbol{\beta}} \geq n - |\boldsymbol{\beta}| + \lambda_{a+1},$$

where a is the abundance of $C_{\boldsymbol{\beta}}$, i.e. $a = \ell(\boldsymbol{\beta} - h\boldsymbol{\alpha})$. We can state the following about minimum distances $d_{\boldsymbol{\beta}}$ of $C(\boldsymbol{\beta})$.

Proposition 3.3.2. (1) If $\boldsymbol{\beta} = t\boldsymbol{\alpha}$, for $t = 1, \ldots, h-1$, then $d_{\boldsymbol{\beta}} = n - |\boldsymbol{\beta}|$, that is, $C(\boldsymbol{\beta})$ reaches the Goppa bound.

(2) For $\boldsymbol{\beta} \leq (n, \ldots, n)$, the code $C(\boldsymbol{\beta})$ reaches the Goppa bound if and only if $C_{h\boldsymbol{\alpha}-\boldsymbol{\beta}}$ does.

(3) If $(h-1)\boldsymbol{\alpha} \leq \boldsymbol{\beta} \leq h\boldsymbol{\alpha}$ then $\lambda_2 \leq d_{\boldsymbol{\beta}} \leq |\boldsymbol{\alpha}|$.

Proof. From Remark 1.3.1 the code $C_{\boldsymbol{\beta}}$ reaches the Goppa bound if and only if there exists a divisor D' such that $0 \leq D' \leq D$ and $D' \sim D(\boldsymbol{\beta})$. Hence, (1) follows taking $D' = \sum_{i=1}^{t} \sum_{P \in \phi^{-1}(\gamma_i)} P$, since $D' \sim tD(\boldsymbol{\alpha}) = D(t\boldsymbol{\alpha})$. For (2), let D' be the divisor such that $D' \sim D(\boldsymbol{\beta})$. Thus, $D'' = D - D' \sim D(h\boldsymbol{\alpha} - \boldsymbol{\beta})$ because $D \sim D(h\boldsymbol{\alpha})$ by Proposition 3.2.5. As $d_{(h-1)\boldsymbol{\alpha}} \geq d_{\boldsymbol{\beta}} \geq d_{h\boldsymbol{\alpha}}$, item (3) follows by noticing that from (1) that $d_{(h-1)\boldsymbol{\alpha}} = |\boldsymbol{\alpha}|$ and $d_{h\boldsymbol{\alpha}} \geq \gamma_2$ from the improved Goppa bound. □

We now give a way to compute lower bounds on the minimum distance of multipoint Castle codes via generalized Weierstrass semigroups. We next describe a bound on the minimum distance of order type developed by Duursma and Park in [DP10] for arbitrary algebraic-geometric codes $C_{\mathcal{L}}(\mathcal{X}, D, G)$.

Remark 3.3.3. Duursma and Park observed in [DP10, Sec. 3] that if $\mathbf{x} \in C_{\mathcal{L}}(D, G) \backslash C_{\mathcal{L}}(D, G - Q)$ for Q a rational point on $\mathcal{X}$ outside $\mathrm{Supp}(D')$, then the divisor $A = \sum_{P \in \mathrm{supp}(\mathbf{x})} P$ satisfies

$$\ell(A) \neq \ell(A - Q) \text{ and } \ell(A - D + G) \neq \ell(A - D + G - Q). \tag{3.3.1}$$

They furthermore show in [DP10, Th. 5.3] that if there exists a sequence of divisors $A_1 \leq \cdots \leq A_w$ satisfying for $i = 1, \ldots, w$ that $A_{i+1} \geq A_i + Q$ for $i = 1, \ldots, w$ and

$$\ell(A_i) \neq \ell(A_i - Q) \text{ and } \ell(A_i - D + G) = \ell(A_i - D + G - Q),$$

then $\deg(A) \geq w$ for any divisor A with support disjoint of $A_w - A_1$ and satisfying (3.3.1).

From Remark 3.3.3, a such sequence gives us a lower bound on the minimum weight of codewords in the coset $C_{\mathcal{L}}(D, G)\backslash C_{\mathcal{L}}(D, G - Q)$ and consequently a lower bound on the minimum distance of $C_{\mathcal{L}}(D, G)$ by applying such technique to each coset in a sequence of nested AG codes containing $C_{\mathcal{L}}(D, G)$. However, it is not obvious how to choose a sequence of divisors (A_i) that gives the better result. This sequence is in general taken in a family of divisors, e.g. divisors supported on specific points. Next we interpret the Duursma and Park order bound to multipoint Castle codes in terms of the generalized Weierstrass semigroups tools to produce sequences of divisors supported in subsets of $\{Q_1, \ldots, Q_\ell\}$. According to Proposition 2.1.3 (2) and Proposition 3.2.5 (2), the Duursma and Park coset bound is interpreted in the setting of multipoint Castle codes as follows.

Proposition 3.3.4. Let $i \in \{1, \ldots, \ell\}$. Let $\boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_w \in \mathbb{Z}^\ell$ be a sequence such that $\boldsymbol{\gamma}_j \geq \boldsymbol{\gamma}_{j-1} + \mathbf{e}_i$ for $j = 2, \ldots, w$ and its elements satisfy for $j = 1, \ldots, w$:

(i) There exists an absolute maximal element of $\widehat{H}(\mathbf{Q})$ in $\nabla_i^\ell(\boldsymbol{\gamma}_j)$;

(ii) There does not exist absolute maximal element of $\widehat{H}(\mathbf{Q})$ in $\nabla_i^\ell(\boldsymbol{\gamma}_j + \boldsymbol{\beta} - h\boldsymbol{\alpha})$.

Then

$$\min \mathrm{wt}(C(\boldsymbol{\beta})\backslash C(\boldsymbol{\beta} - \mathbf{e}_i)) \geq w.$$

Next we give an example that illustrates the application of the previous result.

Example 3.3.5. Let $\mathcal{K}$ be the Klein curve as in Example 3.2.3 together with its rational points Q and R. As we have seen, $(\mathcal{K}, (Q, R))$ is of Castle type. Let us consider $C(10, 8)$ the multipoint Castle code defined on $(\mathcal{K}, (Q, R))$ with length 22 and dimension 17 over $\mathbb{F}_8$. Since by Example 3.2.3 we have $\boldsymbol{\alpha} = (10, 12)$ and $h = 1$, a sequence satisfying the conditions in Proposition 3.3.4 is

$$(0, 0) \leq (2, 1) \leq (3, 1) \leq (5, 1). \qquad \text{(cf. Figure 3.1)}$$

which provides $\min \mathrm{wt}(C(10, 8)\backslash C(9, 8)) \geq 4$. Notice that $(6, 1)$ does not satisfy (ii) in Proposition 3.3.4 because $\nabla_1^2(6, -3) \neq \emptyset$. However, we can take another sequence

$$(0, 0) \leq (2, 1) \leq (3, 1) \leq (4, 2) \leq (5, 2). \qquad \text{(cf. Figure 3.1)}$$

It gives an improvement $\min \mathrm{wt}(C(10, 8)\backslash C(9, 8)) \geq 5$. For further details on efficient computations of sequences of pairs see [DK09, Sec. 5].

Therefore for $(i_j)_{j\geq 1}$ a sequence of elements in $\{1,\ldots,\ell\}$, denoting $\boldsymbol{\beta}_0 = \boldsymbol{\beta}$ and $\boldsymbol{\beta}_{j+1} = \boldsymbol{\beta}_j - \mathbf{e}_{i_{j+1}}$ for $j \geq 1$, we obtain by the Proposition 3.3.3 a bound on the minimum distance of each coset in the sequence of nested multipoint Castle codes

$$C(\boldsymbol{\beta}) \supseteq C(\boldsymbol{\beta}_1) \supseteq C(\boldsymbol{\beta}_2) \supseteq \cdots$$

we get a lower bound on $d_{\boldsymbol{\beta}}$, that is,

$$d_{\boldsymbol{\beta}} \geq \min_{j\geq 0}\{\min \mathrm{wt}(C(\boldsymbol{\beta}_j)\backslash C(\boldsymbol{\beta}_j - \mathbf{e}_{i_{j+1}}))\}.$$

Chapter 4

Quantum codes from Castle curves

The aspects of the quantum model become the error correction crucial for achieving all its computational potential [Got02]. In this way, the quantum error-correcting codes have played an essential role in the protection against computational noises, and recently much research has been done to find good such codes. Calderbank and Shor [CS96], and Steane [Ste96] showed that quantum codes can be derived from classical linear error-correcting codes verifying certain self-orthogonality properties [AK01], including Euclidean and Hermitian self-orthogonality. This method, known as *CSS construction*, has received a lot of interest and allowed finding many powerful quantum codes.

Among all the classical codes used to produce quantum stabilizer codes, algebraic-geometric (AG) codes have received considerable attention [Che01; GH15; Jin14; JX12; KM08; KW08; SK06; Sha08]. Conditions for Euclidean self-orthogonality of AG codes are well known [Sti88] and allow us to translate the combinatorial nature of this problem into geometrical terms concerning the arithmetic of the involved curves. Furthermore, Hermitian self-orthogonality can be easily ensured in a similar manner.

Among all curves used to get AG codes, we can highlight the family of Castle and weak Castle curves [MST09], that combine the good properties of having a reasonable simple handling and producing codes with excellent parameters. In fact, most of the one-point AG codes studied in the literature belong to the family of Castle codes. Besides these codes have, in a natural way, self-orthogonality properties which are very close to those required for obtaining quantum stabilizer codes. It follows from the foregoing that many of the AG codes used to derive quantum codes are particular cases of weak Castle codes. In this chapter, we systematize these constructions, including them in the overall framework of Castle codes. To this end, we show the common theory that underlies all of them and we include many examples, some of which refer to curves and codes already treated in the literature.

Section 4.1 contains a brief introduction to the mathematical modeling of a quantum system and an overview of the constructions of quantum codes from classical codes. Section 4.2 is devoted to Algebraic Geometry codes, and mainly to Castle codes. These provide sequences of

self-orthogonal and formally self-orthogonal codes that can be used to produce quantum codes. We give sufficient conditions for self-duality and study in detail some particular families of curves and codes. In Section 4.3 we show some parameters of quantum codes we have obtained from the curves presented in the previous section. Rather than obtaining codes with new or excellent parameters, we are interested in showing the common theory on which all of them are based. Finally, in Section 4.4 we consider trace codes of AG codes defined over extensions of $\mathbb{F}_q$ and the quantum codes derived from them. Trace codes are closely related to subfield subcodes, from which have recently been obtained quantum codes with excellent parameters [GH15; GHR15].

4.1 Preliminaries on quantum codes

To understand the mathematical model of a quantum system, we begin with a analogy with the binary classical case. Remember that the classical representation of a basic unit of information is the bit, which assumes values in $\mathbb{F}_2$. In the quantum case, the set of a basic unit of quantum information is represented mathematically by $\mathbb{C}^2$ with the standard inner product, and whose the orthonormal canonical basis $\binom{1}{0}$ and $\binom{0}{1}$ is represented, following the Dirac notation, respectively by $|0\rangle$ and $|1\rangle$. Its elements, the so-called *quantum bits*, are described by

$$\alpha|0\rangle + \beta|1\rangle, \text{ where } \alpha, \beta \in \mathbb{C} \text{ with } |\alpha|^2+|\beta|^2= 1.$$

Notice that, contrary to the classical case, the quantum bit can assume a continuum of states.

Quantum bits can also be combined to represent a general quantum state of length n, similar to the classical use of combining n bits to obtain the space $\mathbb{F}_2^n$. The analogue of $\mathbb{F}_2^n$ corresponds to the tensor product $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$, the n-quantum binary system. Hence, a general quantum state of length n is a complex linear combination of the orthogonal basis

$$|\mathbf{a}\rangle := |a_1\rangle \otimes \cdots \otimes |a_n\rangle, \text{ where } \mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n.$$

Since in classical coding theory is often to consider codes over $\mathbb{F}_q$ as alphabet, for q any prime power, we next expose the generalization of aforementioned model to a non-binary quantum system. In this case, the *n-quantum q-ary system* is the space

$$(\mathbb{C}^q)^{\otimes n} = \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n \text{ times}} \cong \mathbb{C}^{q^n}.$$

To set some analogue terminology to the binary case, we fix a basis of $\mathbb{C}^q$ represented symbolically by $\{|a\rangle \ ; \ a \in \mathbb{F}_q\}$. A *quantum digit* is an element in $\mathbb{C}^q$ of form $\sum_{a\in\mathbb{F}_q} \alpha_a|a\rangle$, for $\alpha_a \in \mathbb{C}$.

In this way, the elements

$$|\mathbf{a}\rangle := |a_1\rangle \otimes \ldots \otimes |a_n\rangle, \text{ for } \mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n,$$

form an orthogonal basis for $(\mathbb{C}^q)^{\otimes n}$ with respect to the standard Hermitian inner product.

A q-ary *quantum error-correcting code* of *length* n and *dimension* $K \geq 1$ is a K-dimensional complex subspace Q of the quantum system $(\mathbb{C}^q)^{\otimes n}$.

Based on the quantum postulates, any transformation in a quantum system is linear and preserves inner product. Hence, it must occur as an unitary operator. In particular, the errors occurring in $(\mathbb{C}^q)^{\otimes n}$ act on the quantum states by unitary operators. We next describe a basis of linear transformations of $(\mathbb{C}^q)^{\otimes n}$ given by special unitary operators and the correctable errors for a quantum code. Given $a, b \in \mathbb{F}_q$, consider the unitary operators acting on a quantum digit $|u\rangle$ by

$$T_a|u\rangle = |u + a\rangle \text{ and } R_b|u\rangle = \xi^{\mathrm{tr}(bu)}|u\rangle,$$

where ξ is a p-th root of unity and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ the trace map. The space spanned by $\{T_a R_b \ ; \ a, b \in \mathbb{F}_q\}$ is the set of all handleable errors on a quantum digit.

As the set $\{|\mathbf{a}\rangle \ ; \ \mathbf{a} \in \mathbb{F}_q^n\}$ is a basis of $(\mathbb{C}^q)^{\otimes n}$, we can provide the special unitary operator in $(\mathbb{C}^q)^{\otimes n}$ through tensor products. Precisely, for $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, consider

$$T_{\mathbf{a}} = T_{a_1} \otimes \cdots \otimes T_{a_n} \text{ and } R_{\mathbf{b}} = R_{b_1} \otimes \cdots \otimes R_{b_n}.$$

Writing $E_{\mathbf{a},\mathbf{b}}$ for $T_{\mathbf{a}} R_{\mathbf{b}} = T_{a_1} R_{b_1} \otimes \cdots \otimes T_{a_n} R_{b_n}$, the operators $E_{\mathbf{a},\mathbf{b}}$, for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, form a base of the linear space of linear transformations of $(\mathbb{C}^q)^{\otimes n}$, called the *error basis*. Therefore, it is enough to be able to correct the errors $E_{\mathbf{a},\mathbf{b}}$. The *error group* of $(\mathbb{C}^q)^{\otimes n}$ is the set

$$G_n = \{\xi^i E_{\mathbf{a},\mathbf{b}} \ : \ \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \ , \ 0 \leq i \leq p-1\},$$

and the weight of an error $\xi^i E_{\mathbf{a},\mathbf{b}}$ in G_n is defined as

$$\mathrm{wt}(\xi^i E_{\mathbf{a},\mathbf{b}}) = n - \#\{j \ : \ a_j = b_j = 0\}.$$

Now we are ready to define the meaning of minimum distance of quantum code: a quantum code Q of length n *detects* $d'-1$ quantum digits of errors if for every orthogonal pair of quantum states $|\varphi\rangle$ and $|\psi\rangle$ in Q, and for every error E in the error group G_n of weight less than d', the quantum states $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal.

The *minimum distance* of a quantum code Q is the largest integer d' such that Q detects $d'-1$ quantum digits of errors. We denote by $[[n, K, d]]_q$ a q-ary quantum code of length n, dimension K and minimum distance d, or simply $[[n, k, d]]_q$ whenever $k = \log_q(K)$ is an integer.

A quantum code of length n is called *stabilizer* if it is a joint of eigenspaces of operators

in an abelian subgroup of G_n. The stabilizer quantum codes form a notable class among the quantum codes since they have very special properties, for instance, every quantum code is contained in a stabilizer quantum code.

In what follows we are mainly interested in quantum codes obtained from classical algebraic geometry codes by the so-called CSS construction. The idea behind this procedure is to consider the map $g : \mathbb{F}_q^{2n} \to G_n$ given by $(\mathbf{a}|\mathbf{b}) \mapsto E_{\mathbf{a},\mathbf{b}}$ and the isomorphism $\mathbb{F}_{q^2}^n \to \mathbb{F}_q^{2n}$ of $\mathbb{F}_q$-vector spaces given by $\mathbf{x} = (a_1 + b_1\omega, \ldots, a_n + b_n\omega) \mapsto (\mathbf{a}|\mathbf{b})$, where ω is a primitive element to the quadratic extension $\mathbb{F}_{q^2}|\mathbb{F}_q$. Hence, taking classical codes either over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ with special properties, it is possible to obtain quantum codes from eigenspaces of their image under g. Thus quantum codes constructed in this way have the property of being stabilizer. For further details concerning the mathematical model for quantum error-correction and how to derive quantum codes from classical codes, we refer to [AK01; Got02; GB99; KW08; KM08].

4.1.1 Quantum codes from linear codes over $\mathbb{F}_q$

We recall that for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, the usual (Euclidean) inner product $\sum a_i b_i$ is denoted by $\langle \mathbf{a}, \mathbf{b} \rangle$. Moreover, given a linear code C over $\mathbb{F}_q$, C is called *self-dual* if $C = C^\perp$, and *self-orthogonal* if $C \subseteq C^\perp$, that is if $\langle \mathbf{a}, \mathbf{b} \rangle = 0$ for all $\mathbf{a}, \mathbf{b} \in C$, where $C^\perp$ is the dual code of C as in (1.1.2). The so-called *CSS code construction* allows obtaining quantum codes through of inclusions of classical codes over $\mathbb{F}_q$ as follows.

Theorem 4.1.1. ([GBR04; KW08]) Let C_1, C_2 be two linear codes over $\mathbb{F}_q$ of length n and dimensions k_1 and k_2 respectively with $C_1 \subseteq C_2$. Then there exists a $[[n, k_2 - k_1, d]]_q$ code with minimum distance $d = \min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in (C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$.

In particular, we have the following useful outcome which has been extensively used to provide the existence of many quantum codes.

Corollary 4.1.2. ([MU00]) Let C be a self-orthogonal $[n, k, d]$ code over $\mathbb{F}_q$. Then there exists a $[[n, n - 2k, d]]_q$ code with minimum distance $d = \min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in (C^\perp \setminus C)\} \geq d(C^\perp)$.

Jin and Xing [JX12] showed that when q is even, the self-orthogonality condition can be weakened in the sense that we can obtain self-orthogonal codes from other codes "close" to be self-orthogonal. To be precise, remember that given an n-tuple $\mathbf{x}$ of nonzero elements in $\mathbb{F}_q$, the coordinate-wise multiplication by $\mathbf{x}$ map given by $\mathbf{a} \mapsto \mathbf{x}*\mathbf{a} = (x_1a_1, \ldots, x_na_n)$ gives an isometry for the Hamming metric and for a linear code C over $\mathbb{F}_q$, we shall write $\mathbf{x}*C = \{\mathbf{x}*\mathbf{c} \ : \ \mathbf{c} \in C\}$. Next we shall expose a construction of this type for sequences of codes.

Let $C_0 = (0) \subseteq C_1 \subseteq \ldots \subseteq C_n = \mathbb{F}_q^n$ be an increasing sequence of $n + 1$ linear codes in $\mathbb{F}_q^n$, where C_i has dimension i and minimum distance $d(C_i)$. This sequence is called *self-dual* if

$C_i^\perp = C_{n-i}$ for all i, and *formally self-dual* if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_i^\perp = \mathbf{x} * C_{n-i}$ for all i. In this case, note that for i, j, with $1 \leq i \leq j \leq n$ we have

$$C_i^\perp \setminus C_j^\perp = \mathbf{x} * C_{n-i} \setminus \mathbf{x} * C_{n-j} = \mathbf{x} * (C_{n-i} \setminus C_{n-j});$$

moreover, since the coordinate-wise multiplication by $\mathbf{x}$ is an isometry,

$$\min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in \mathbf{x} * (C_{n-i} \setminus C_{n-j})\} = \min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in (C_{n-i} \setminus C_{n-j})\}.$$

Now, by applying Theorem 4.1.1, we obtain a quantum $[[n, j-i, d]]_q$ code with minimum distance

$$d = \min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in (C_j \setminus C_i) \cup (C_{n-i} \setminus C_{n-j})\} \geq \min\{d(C_j), d(C_{n-i})\}.$$

4.1.2 Quantum codes from linear codes over $\mathbb{F}_{q^2}$

Let $\langle -, - \rangle_H$ denote the Hermitian inner product in $\mathbb{F}_{q^2}^n$ given by $\langle \mathbf{a}, \mathbf{b} \rangle_H = \langle \mathbf{a}, \mathbf{b}^q \rangle$. The dual of a linear code $C \subseteq \mathbb{F}_{q^2}^n$ relative to the Hermitian inner product (or the *Hermitian dual* of C) is

$$C^{\perp H} = \{\mathbf{v} \in \mathbb{F}_{q^2}^n \ : \ \langle \mathbf{v}, \mathbf{c}^q \rangle = 0 \text{ for all } \mathbf{c} \in C\} = (C^q)^\perp.$$

We say that C is *Hermitian self-orthogonal* if $C \subseteq C^{\perp H}$, or equivalently if $C^q \subseteq C^\perp$. Raising to the q-th power we find that $\langle \mathbf{v}, \mathbf{c}^q \rangle = 0$ if and only if $\langle \mathbf{v}^q, \mathbf{c} \rangle = 0$. Hence $(C^q)^\perp = (C^\perp)^q$ and therefore $d(C^{\perp H}) = d(C^\perp)$. We can derive quantum codes from classical codes over $\mathbb{F}_{q^2}$ as follows.

Theorem 4.1.3. ([AK01]) Let C be a linear code over $\mathbb{F}_{q^2}$ of parameters $[n, k, d]$ which is self-orthogonal with respect to the Hermitian inner product. Then there exists a $[[n, n-2k, d]]_q$ quantum code with minimum distance $d = \min\{\mathrm{wt}(\mathbf{c}) \ : \ \mathbf{c} \in (C^{\perp H} \setminus C)\} \geq d(C^\perp)$.

Let $C_0 = (0) \subseteq C_1 \subseteq \ldots \subseteq C_n = \mathbb{F}_{q^2}^n$ be an increasing sequence of $n+1$ linear codes in $\mathbb{F}_{q^2}^n$. From Theorem 4.1.3 we have the following three procedures to obtain q-ary quantum codes from a such sequence:

(A) When the sequence is self-dual then the theorem can be applied. As $C_n = \mathbb{F}_{q^2}^n$, for given i let $q(i)$ be the smallest index such that $C_i^q \subseteq C_{q(i)}$. When $i + q(i) \leq n$ we have $C_i^q \subseteq C_{q(i)} \subseteq C_{n-i} = C_i^\perp$, and hence we get a $[[n, n-2i, \geq d(C_{n-i})]]_q$ code. In Section 4.3, we will get sequences of one-point AG codes for which it is possible to give an estimate of $q(i)$ and consequently obtain quantum codes by this procedure.

(B) When the sequence is formally self-dual but not self-dual, there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_i^\perp = \mathbf{x} * C_{n-i}$ for all $i = 0, \ldots, n$. Following the aforementioned ideas of Jin and Xing

[JX12], we can still derive quantum codes in some cases by slightly modifying the codes. Since the elements of $\mathbb{F}_q$ are precisely the $(q+1)$-th powers in $\mathbb{F}_{q^2}$, there exists $\mathbf{y} \in \mathbb{F}_{q^2}^n$ such that $\mathbf{y}^{q+1} = \mathbf{x}$, or equivalently $\mathbf{y}^q = \mathbf{y}^{-1} * \mathbf{x}$. Consider the sequence $\mathbf{y} * C_0 = (0) \subseteq \mathbf{y} * C_1 \subseteq \ldots \subseteq \mathbf{y} * C_n = \mathbb{F}_{q^2}^n$. As $\mathbf{x} * C^\perp = (\mathbf{x}^{-1} * C)^\perp$ by Lemma 1.1.1, whenever $i + q(i) \leq n$ we have

$$(\mathbf{y} * C_i)^q = \mathbf{y}^q * C_i^q = \mathbf{y}^{-1} * \mathbf{x} * C_i^q \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{q(i)} \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{n-i} = (\mathbf{y} * C_i)^\perp$$

and we can apply Theorem 4.1.3 to get a $[[n, n-2i, \geq d(C_{n-i})]]_q$ quantum code.

(C) To give a concrete example in which the condition $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ holds, we can consider the case in which there exists a self-dual sequence $C'_0 = (0) \subseteq C'_1 \subseteq \ldots \subseteq C'_n = \mathbb{F}_q^n$ of codes over $\mathbb{F}_q$ with $C_i'^\perp = \mathbf{x} * C'_{n-i}$ and such that $C_0, C_1, \ldots, C_n$ are the codes over $\mathbb{F}_{q^2}$ spanned by $C'_0, C'_1, \ldots, C'_n$, respectively. In this situation it is clear that C_i and C'_i have the same parameters, $C_i^\perp = \mathbf{x} * C_{n-i}$ and $(C_i)^q = C_i$. Let $\mathbf{y} \in \mathbb{F}_{q^2}^n$ such that $\mathbf{y}^{q+1} = \mathbf{x}$ and consider now the sequence $\mathbf{y} * C_0 = (0) \subseteq \mathbf{y} * C_1 \subseteq \ldots \subseteq \mathbf{y} * C_n = \mathbb{F}_{q^2}^n$. For $2i \leq n$ we have

$$(\mathbf{y} * C_i)^q = \mathbf{y}^q * C_i = \mathbf{y}^{-1} * \mathbf{x} * C_i \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{n-i} = \mathbf{y}^{-1} * C_i^\perp = (\mathbf{y} * C_i)^\perp$$

so we can apply Theorem 4.1.3 to get a $[[n, n-2i, \geq d(C_{n-i})]]_q$ code.

4.2 CSS constructions from Castle codes

As we have seen in the previous section, to obtain a quantum code from a linear classical code C by the CSS-construction, we must verify the self-orthogonality property of classical code C with respect to the Euclidean or the Hermitian inner-product and compute its dual distance $d(C^\perp)$. Both tasks are difficult in general and, for this reason, among all linear codes producing quantum codes, the class of Algebraic Geometry (AG) codes has received considerable attention [GH15; GHR15; Jin14; JX12; KM08; Sha08]. For these codes there is a simple criterion for the self-orthogonality. In addition, certain families of AG codes allow efficient methods to estimate their minimum distances [Gei+11; HVP98; OM13; Sti09].

Let us briefly remember the construction of AG codes from Section 1.3. We pay particular attention to AG codes coming from Castle and weak Castle curves, that produce self-dual and formally self-dual sequences of codes in a natural way.

Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible algebraic curve of genus g defined over $\mathbb{F}_q$. Take two rational divisors D and G on $\mathcal{X}$ with disjoint supports and such that D is the sum of n rational distinct points, $D = P_1 + \cdots + P_n$. In the following we further assume $n > 2g$. From Section 1.3, the AG code $C_{\mathcal{L}}(D, G)$ has dimension and minimum distance satisfying

$$k = \ell(G) - \ell(G - D) \qquad \text{and} \qquad d \geq n - \deg(G) + \lambda_{a+1},$$

where a is the abundance of C and λ_r is the r-th gonality of $\mathcal{X}$.

By Proposition 1.3.4, $C_{\mathcal{L}}(, D, G)^{\perp} = C_{\mathcal{L}}(D, \mathrm{div}(\eta) - G + D)$, where η is a differential form ω with simple poles and residue 1 at every point P_i in the support of D. Thus $C_{\mathcal{L}}(D, G)$ is self orthogonal if $G \leq D + W - G$. When $C_{\mathcal{L}}(D, G)$ is defined over the field $\mathbb{F}_{q^2}$, and since $C(\mathcal{X}, D, G)^q \subseteq C_{\mathcal{L}}(D, qG)$, the code $C_{\mathcal{L}}(D, G)$ is Hermitian self-orthogonal if $qG \leq D+W-G$. More generally, if ω is a differential form with simple poles at every point P_i in $\mathrm{Supp}(D)$, it follows from Proposition 1.3.3 that $C_{\mathcal{L}}(D, D + \mathrm{div}(\omega) - G) = \mathbf{x} * C_{\mathcal{L}}(D, G)^{\perp}$, where $x_i \neq 0$ is the residue of ω at P_i.

4.2.1 Castle codes and sufficient conditions for their self-orthogonality

Let $\mathcal{X}$ be a curve as in previous section and let Q be a rational point on $\mathcal{X}$. We recall from Section 3.1 that a pointed curve $(\mathcal{X}, Q)$ is said to be Castle if it satisfies the conditions

(C1) The Weierstrass semigroup $H(Q)$ of $\mathcal{X}$ at Q is symmetric; and

(C2) $\#\mathcal{X}(\mathbb{F}_q) = q\rho(Q) + 1$, where $\rho(Q)$ is the multiplicity of $H(Q)$.

A pointed curve $(\mathcal{X}, Q)$ is called weak Castle if it satisfies the condition (C1) and

(C2′) There exist a morphism $f : \mathcal{X} \to \mathbb{P}^1$ with $\mathrm{div}_{\infty}(f) = dQ$, and a set $U = \{\alpha_1, \ldots, \alpha_h\} \subseteq \mathbb{F}_q$ such that for all $i = 1, \ldots, h$, we have $f^{-1}(\alpha_i) \subseteq \mathcal{X}(\mathbb{F}_q)$ and $\#f^{-1}(\alpha_i) = d$.

Example 4.2.1. Let q be odd. A hyperelliptic curve $\mathcal{X}$ over $\mathbb{F}_q$ is given by an equation $y^2 = F(x)$, where F is a squareless polynomial. If $\deg(F) = 2g+1$ then $\mathcal{X}$ has genus g and one hyperelliptic point at infinity, Q. Then $\mathcal{X}$ is Castle if and only if $F(\alpha)$ is a nonzero square for all $\alpha \in \mathbb{F}_q$. For example, the curve $y^2 = x^q - x + 1$ has $2q + 1$ points and it is Castle for all q. Otherwise, if $\mathcal{X}$ is not Castle, take $U = \{\alpha \in \mathbb{F}_q : F(\alpha) \text{ is a nonzero square in } \mathbb{F}_q\}$. Whenever $U \neq \emptyset$, $(\mathcal{X}, Q)$ is a weak Castle curve and provides codes of length $n = 2\#U$. Similarly, if q is even, a hyperelliptic curve $\mathcal{X}$ of genus g over $\mathbb{F}_q$ is given by an equation $y^2 + y = F(x)$, where $F(x)$ is a rational function with $\deg(\mathrm{div}_0(F)), \deg(\mathrm{div}_{\infty}(F)) \leq 2g + 2$. If F is a polynomial there is one hyperelliptic point at infinity Q and $\mathcal{X}$ is Castle or complete weak Castle. For example, the curves $y^2 + y = x^u$, where $q + 1|u$ and $0 < u \leq q^2 - 1$ are Castle over $\mathbb{F}_{q^2}$.

For $i = 1, \ldots, n$, let $m_i = \min\{m : \ell(mQ) - \ell((m - n)Q) \geq i\}$. Then $C_i = C_{\mathcal{L}}(\mathcal{X}, D, m_iQ)$ has dimension i and the sequence

$$C_0 = (0) \subseteq C_1 \subseteq \ldots \subseteq C_n = \mathbb{F}_q^n \tag{4.2.1}$$

is a formally self-dual sequence of codes. Thus, from a weak Castle curve we obtain in a natural manner a formally self-dual sequence of codes and consequently, by applying the procedures explained in Sections 4.1.1 and 4.1.2, a set of quantum stabilizer codes. To be precise, we have the following results.

Corollary 4.2.2. Let $(\mathcal{X}, Q)$ be a weak Castle curve over $\mathbb{F}_q$ and let $C_0 = (0) \subseteq C_1 \subseteq \ldots \subseteq C_n = \mathbb{F}_q^n$ be the sequence of codes from (4.2.1). If $2i \leq n$ then we have a quantum code of parameters $[[n, n-2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \lambda_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$ is the abundance of C_{n-i}.

Proof. Notice that we have a formally self-dual sequence $C_0 \subseteq \ldots \subseteq C_n$ and we can thus apply the construction (C) of Section 4.1.2. The estimate on the minimum distance follows from the improved Goppa bound stated in equation (1.3.1). □

Corollary 4.2.3. Let $(\mathcal{X}, Q)$ be a weak Castle curve over $\mathbb{F}_{q^2}$ such that the sequence $C_0 = (0) \subseteq C_1 \subseteq \ldots \subseteq C_n = \mathbb{F}_{q^2}^n$ obtained as in (4.2.1) is self-dual. If $qm_i \leq m_{n-i}$ then we have a quantum code over $\mathbb{F}_q$ of parameters $[[n, n-2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \lambda_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$.

Proof. Taking into account that $C(\mathcal{X}, D, m_i Q)^q \subseteq C(\mathcal{X}, D, q m_i Q)$, the proof is similar to the previous corollary, now applying construction (A) of Section 4.1.2. □

To obtain quantum codes using the procedure (A) of Section 4.1.2, formal self-orthogonality is not enough. In what follows we shall provide some sufficient conditions on curves verifying Castle assumptions in order to obtain codes satisfying the self-duality property. Given a pointed curve $(\mathcal{X}, Q)$ of genus g, satisfying the condition (C2′), we consider the divisor

$$D := \sum_{P \in f^{-1}(U)} P$$

and the intrinsic rational function $\varphi := \prod_{i=1}^{h}(f - \alpha_i)$ related to f. As a notation, given an integer m, we write $m^{\perp} = n + 2g - 2 - m$.

Lemma 4.2.4. Let $(\mathcal{X}, Q)$ be a pointed curve satisfying (C2′). If $\mathrm{div}(d\varphi) = (2g-2)Q$, then $C_{\mathcal{L}}(D, mQ)^{\perp} = C_{\mathcal{L}}(D, m^{\perp}Q)$.

Proof. Consider the differential form $\eta = d\varphi/\varphi$. From hypothesis we get $\mathrm{div}(\eta) = (n + 2g - 2)Q - D$ since $\mathrm{div}(\varphi) = D - nQ$. Hence, η has simple poles and residue 1 at $P \in \mathrm{Supp}(D)$. □

Proposition 4.2.5. Let $(\mathcal{X}, Q)$ be a pointed curve satisfying (C2) and let $f \in \mathcal{L}(\infty Q)$ such that $v_Q(f) = \rho(Q)$. If $\mathrm{div}(df) = (2g-2)Q$, then $C_{\mathcal{L}}(D, mQ)^{\perp} = C_{\mathcal{L}}(D, m^{\perp}Q)$.

Proof. As in this case $\varphi = f^q - f$ because $U = \mathbb{F}_q$, we obtain $\mathrm{div}(d\phi) = \mathrm{div}(df)$ and thus the result follows from the previous lemma. □

Corollary 4.2.6. Let $(\mathcal{X}, Q)$ be a pointed curve in the conditions of Lemma 4.2.4 or Proposition 4.2.5. Then $C_{\mathcal{L}}(D, mQ)$ is Euclidean self-orthogonal if $2m \leq n + 2g - 2$. If q is a square, $C_{\mathcal{L}}(D, mQ)$ is Hermitian self-orthogonal if $(\sqrt{q} + 1)m \leq n + 2g - 2$.

Remark 4.2.7. Note that the conditions required by Proposition 4.2.5 are not verified by all Castle curves. Consider, for example, the hyperelliptic curve $\mathcal{X}$ of equation $y^2 = x^q - x + 1$ over $\mathbb{F}_q$, q odd of Example 4.2.1. Here $\rho(Q) = 2$ which is the pole order of x at Q, and $\mathcal{X}$ is Castle with $f = x$ in the notation of Proposition 4.2.5. As the points P over the $x = \alpha$, for α a root of $x^q - x + 1$ in $\overline{\mathbb{F}}_q$, are also ramified, we have $\mathrm{div}(dx) \neq (2g-2)Q$. On the contrary, for the curves $y^2 + y = x^u$, where $q+1|u$, over $\mathbb{F}_{q^2}$ of Example 4.2.1, a simple computation shows that $\mathrm{div}(dx) = (2g-2)Q$, hence they provide self-dual sequences of codes.

Corollary 4.2.8. Let $(\mathcal{X}, Q)$ be a pointed curve over $\mathbb{F}_{q^2}$ in the conditions of Lemma 4.2.4 or Proposition 4.2.5. Let M be the dimension set of $(\mathcal{X}, Q)$. If $(q+1)m_i \leq n+2g-2$ then we have a quantum code over $\mathbb{F}_q$ of parameters $[[n, n-2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \lambda_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$.

4.2.2 Curves defined by separated variable equations

Next we consider the family of curves having a plane model given by a separated variable equation $F(y) = G(x)$, where F and G are univariate polynomials of coprime degrees. The particular case in which one of the polynomials is linearized is interesting since it contains many of the most relevant curves for Coding Theory purposes. For instance, several of the curves studied below were already treated in [Sti88]. Remember that a polynomial F is called *linearized* (or a q-polynomial) if the exponents of all monomials are powers of q, i.e. a polynomial of shape

$$\sum_{i=0}^{n} a_i x^{q^i} \in \mathbb{F}_{q^r}[x].$$

Furthermore, it is said *separable* if $a_0 \neq 0$. The following properties hold true for this type of curves.

Proposition 4.2.9. Let $\mathcal{X}$ be the curve defined over $\mathbb{F}_q$ by the equation $F(y) = G(x)$, where F and G are polynomials of degrees $a = \deg(F), b = \deg(G)$ with $\gcd(a, b) = 1$ and F is a linearized separable polynomial. Let Q be the common pole of x and y and $\rho(Q)$ the multiplicity of $H(Q)$. Then

(1) The genus of $\mathcal{X}$ is $g = (a-1)(b-1)/2$.

(2) The Weierstrass semigroup $H(Q)$ of $\mathcal{X}$ at Q is $\langle a, b\rangle$. In particular, $H(Q)$ is symmetric and $\rho(Q) = \min\{a, b\}$.

(3) $\mathrm{div}(dx) = (2g-2)Q$. If $b > a$ then $\rho(Q) = a$ and there exists $f : \mathcal{X} \to \mathbb{P}^1$ with $\mathrm{div}_\infty(f) = \rho(Q)Q$ and $\mathrm{div}(df) = (2g-2)Q$.

Proof. (1) It follows from the Riemann-Hurwitz-Zeuthen genus formula (Theorem 1.2.11) by noticing that, being F linearized and separable, Q is the only ramification point of $\mathcal{X}$ over the

morphism x. (2) From the equation of $\mathcal{X}$ we have $av_Q(y) = bv_Q(x)$ and since $(a, b) = 1$ we conclude that $v_Q(y) = b, v_Q(x) = a$, hence $H(Q) \supseteq \langle a, b\rangle$. Since the genus of $\langle a, b\rangle$ is g we get equality. As all semigroups generated by two elements are symmetric, the statement follows. (3) Again, since F is linearized and separable, its derivative is a constant, which implies that Q is the only point of $\mathcal{X}$ which ramifies over the morphism x. Using $\operatorname{div}(dx) = -2\operatorname{div}_\infty(x) + B_x$, where B_x is the ramification divisor of the morphism x, we obtain the equality between the divisors. To see the last statement it is enough to take $f = x$. □

Proposition 4.2.9 gives a large family of curves verifying the conditions of Proposition 4.2.5, and hence providing self-dual sequences of Castle and weak Castle codes. Concrete examples of relevant Castle curves used in Coding Theory belonging to this family include those already mentioned above: Hermitian curve, Norm-Trace curve, etc. Recall, however, that not all Castle curves satisfying the conditions of Proposition 4.2.5 belong to this family. For instance, this happens to the Ree curve [MST09] whose plane models known so far are not given by a separated variable equation.

Next we show some examples of curves in the conditions of Lemma 4.2.4.

Example 4.2.10. Let $\mathcal{X}$ be the curve given by

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = x^u \tag{4.2.2}$$

defined over $\mathbb{F}_{q^r}$ with $u \mid (q^r - 1)/(q - 1)$. We shall see that it is a weak Castle curve with $q^{r-1}(u(q-1)+1)+1$ rational points and genus $g = (u-1)(q^{r-1}-1)/2$. Note that this curve is covered by the Norm-Trace curve over $\mathbb{F}_{q^r}$; indeed, it is a quotient curve of the Norm-Trace curve by the cyclic group of automorphisms generated by $(x, y) \mapsto (\zeta x, y)$, where ζ is a primitive u-th root of unity. Also this equation includes many other interesting curves as the Hermitian curve and its quotients in case of $r = 2$. Now, consider the multiplicative subgroup of $\mathbb{F}_{q^r}^\times$

$$U^\times = \{\beta \in \mathbb{F}_{q^r}^\times \ : \ \beta^u \in \mathbb{F}_q\} \tag{4.2.3}$$

of cardinality $u(q-1)$ and set $U = U^\times \cup \{0\}$. Observe that the elements of U are the elements of $\mathbb{F}_{q^r}$ which split totally over the morphism $x : \mathcal{X} \to \mathbb{P}^1$. Now take

$$\varphi = \prod_{\beta \in U}(x - \beta) = x \prod_{\beta \in U^\times}(x - \beta) = x(x^{u(q-1)} - 1) = x^{u(q-1)+1} - x. \tag{4.2.4}$$

Since from Proposition 4.2.9 we have $\operatorname{div}(dx) = (2g-2)Q$, where Q is the unique pole of x, a sufficient condition to have $\operatorname{div}(d\varphi) = (2g-2)Q$ is that $u \equiv 1 \pmod{p}$, where p is the characteristic of $\mathbb{F}_q$. Notice that this always happens in characteristic 2.

4.2.3 Maximal Curves

Recall that a curve $\mathcal{X}$ of genus g over a field $\mathbb{F}_{q^{2r}}$ is maximal if it attains equality in

$$\#\mathcal{X}(\mathbb{F}_{q^{2r}}) = q^{2r} + 1 + 2gq^r; \qquad \text{(Hasse-Weil bound)}$$

see [HKT08, Sec. 9.2] for details. Maximal curves often provide AG codes with good parameters. In this subsection we shall give examples of maximal Castle curves verifying the conditions of Proposition 4.2.9. In particular, the examples we present are curves defined over $\mathbb{F}_{q^{2r}}$ by plane models of type $F(y) = G(x)$, where $F(y)$ is linearized and separable of degree ρ a power of $p = \mathrm{char}(\mathbb{F}_q)$, and $G(x)$ of degree $q^r + 1$, bigger than ρ. Thus these curves have genus $2g = (\rho - 1)q^r$ and the Weierstrass semigroup $H(Q)$ of $\mathcal{X}$ at Q is generated by ρ and $q^r + 1$. In this situation, maximality implies the Castle condition $\#\mathcal{X}(\mathbb{F}_{q^{2r}}) = q^{2r}\rho + 1$. We present a couple of examples.

Example 4.2.11. Let $a \in \mathbb{F}_{q^2}$ such that $a^q + a = 0$ and consider the curve $\mathcal{X}$ defined over $\mathbb{F}_{q^2}$ by

$$y^{q/p} + y^{q/p^2} + \cdots + y = ax^{q+1} \tag{4.2.5}$$

where $p = \mathrm{char}(\mathbb{F}_q)$. To check the maximality of $\mathcal{X}$ we note that it is covered by the Hermitian curve $\mathcal{H} : w^q + w = z^{q+1}$ via the morphism $x = z$, $y = (-aw)^p + aw$. The cardinality of $\mathcal{X}(\mathbb{F}_{q^2})$ can be computed from this fact by taking into account that its genus g satisfies $2g = (q/p-1)q$.

Example 4.2.12. Let $\mathcal{X}$ be the curve over $\mathbb{F}_{q^{2r}}$, r odd, defined by

$$y^q + y = x^{q^r+1}. \tag{4.2.6}$$

As in the previous example, $\mathcal{X}$ is maximal as it is covered by the Hermitian curve $\mathcal{H} : w^{q^r} + w = z^{q^r+1}$ over $\mathbb{F}_{q^{2r}}$. A covering is given by $x = z$, $y = w^{q^{r-1}} - w^{q^{r-2}} + \cdots + w$.

4.3 Some Examples of quantum codes

In this Section we shall show a few examples of quantum codes obtained from the curves treated in the above Section. Computations have been done by using the computer system Magma [BCP97]. In order to compare the quality of the obtained parameters we shall use the tables [Ede; Gra] and the quantum Gilbert-Varshamov bound.

Theorem 4.3.1. ([FM04]) Suppose that $n > k \geq 2$, $d \geq 2$ and $n \equiv k (\mathrm{mod}\ 2)$. Then there exists a stabilizer quantum code $[[n, k, d]]_q$ provided that

$$\frac{q^{n-k+2} - 1}{q^2 - 1} > \sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i}. \tag{4.3.1}$$

We shall use the following notation: given a code $[[n,k,d]]_q$, we write $[[n,k,d]]_q^\dagger$ when the parameters n,k,d meet the Gilbert-Varshamov bound with equality. We write $[[n,k,d]]_q^\ddagger$ when the parameters n,k,d strictly improve on the Gilbert-Varshamov bound.

Codes from the Suzuki curve

The curve $\mathcal{X}$ of equation $y^q+y=x^{q_0}(x^q+x)$ over $\mathbb{F}_q$, where $q_0=2^s$ and $q=2q_0^2$ is called the *Suzuki* curve. It has genus $g=q_0(q-1)$ and q^2+1 rational points. Let Q be the common pole of x and y. Then the Weierstrass semigroup $H(Q)$ is generated by $\langle q, q+1, q+2q_0, q+2q_0+1\rangle$ (see [OM13] and the references therein), so $\mathcal{X}$ is a Castle curve. Codes arising from this curve have been extensively studied and their parameters are rather well known. In particular, the conditions stated in Proposition 4.2.5 and Corollary 4.2.6 holds, so that the duals of one point Suzuki codes are again one-point Suzuki codes. We can use them to obtain quantum codes from construction (C) of Section 4.1.2.

Example 4.3.2. For $q=8$, $C_{\mathcal{L}}(D,mQ)$ has length 64 and is self-orthogonal whenever $m\leq 45$. Then we get quantum codes over $\mathbb{F}_8$ of parameters $[[64,62,2]]_8^\dagger$, $[[64,54,3]]_8$, $[[64,52,4]]_8^\dagger$, $[[64,42,5]]_8$, $[[64,40,6]]_8$, $[[64,38,7]]_8$, $[[64,36,8]]_8$. These are good parameters compared with those listed in [Ede].

Codes from elliptic and hyperelliptic curves

Example 4.3.3. Consider the family of hyperelliptic curves $y^2+y=x^u$, where $q+1|u$ and $u\leq q^2-1$ over $\mathbb{F}_{q^2}$, q even, of Example 4.2.1. In Remark 4.2.7 we noted that they are Castle and verify $\operatorname{div}(dx)=(2g-2)Q$. Since they have genus $g=\lfloor u-1\rfloor/2$, the code $C_{\mathcal{L}}(D,mQ)$ is self-orthogonal whenever $2m\leq 2q^2+u-3$ and Hermitian self-orthogonal whenever $(q+1)m\leq 2q^2+u-3$. We find quantum codes with parameters $[[8,6,2]]_2^\ddagger$, $[[32,30,2]]_4^\ddagger$, $[[32,24,4]]_4^\ddagger$, $[[128,126,2]]_8^\ddagger$, $[[128,116,4]]_8^\dagger$, $[[128,112,6]]_8^\ddagger$, $[[128,108,8]]_8^\ddagger$ among others. The particular case $u=q+1$ was studied in [Jin14, Sec. III (A)].

Example 4.3.4. Here we show an example of a complete weak Castle curve which is not Castle. When $q\equiv 3 \pmod 4$ then -1 is not a square, hence the elliptic curve $\mathcal{X}: y^2=x^3+ax$ has $q+1$ rational points over $\mathbb{F}_q$. Consequently it has $q^r+1+2\sqrt{q^r}$ rational points over $\mathbb{F}_{q^r}$ for $r\equiv 2 \pmod 3$. To give a concrete example take $q=3, r=2$. A simple computation shows that $\rho(Q)=2$ and $\mathcal{X}$ is not Castle. However $\mathcal{X}$ is a complete weak Castle curve with respect the morphism $f=y$. We obtain codes with the following parameters over $\mathbb{F}_9$: $[[15,13,2]]_9^\dagger$, $[[15,7,4]]_9^\dagger$, $[[15,5,5]]_9^\dagger$, $[[15,3,6]]_9^\dagger$, $[[15,1,7]]_9$. Quantum codes from elliptic curves have been treated in [JX12].

Codes from Hermitian, Norm-Trace and related curves

Quantum codes arising from Hermitian curves have been extensively treated, [KM08; SK06]. Here we shall consider the related more general curves $\mathcal{X}$ of Example 4.2.10 given by an equation of the form

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = x^u \tag{4.3.2}$$

over $\mathbb{F}_{q^r}$ with $u \mid (q^r-1)/(q-1)$. We saw that when $u \equiv 1 \pmod{p}$ then $\mathcal{X}$ satisfies the conditions of Lemma 4.2.4, where p is the characteristic of $\mathbb{F}_{q^r}$. Note that when $u = (q^r-1)/(q-1)$, then $\mathcal{X}$ is the Norm-Trace curve, and if $r = 2$ then $\mathcal{X}$ is the Hermitian curve. In both cases such conditions are also automatically satisfied.

Example 4.3.5. For $q = 2$, $r = 4$ and $u = 3$, from Corollary 4.2.6 the codes $C_{\mathcal{L}}(D, mQ)$ of length 32 over $\mathbb{F}_{16}$ are Hermitian self-orthogonal whenever $m \leq 8$. The quantum codes over $\mathbb{F}_4$ obtained from these have parameters $[[32, 30, 2]]_4^{\ddagger}$ and $[[32, 24, 3]]_4^{\dagger}$.

Example 4.3.6. For $q = 2$, $r = 3$ and $u = 7$, we obtain the Norm-Trace curve. The codes $C_{\mathcal{L}}(D, mQ)$ of length 32 over the field $\mathbb{F}_8$ are self-orthogonal if $m \leq 24$. We obtain $[[32, 28, 2]]_8^{\dagger}$, $[[32, 26, 3]]_8^{\ddagger}$, $[[32, 18, 4]]_8$ quantum codes.

Example 4.3.7. For $r = 2$ we obtain the Hermitian curves and quotients $y^q + y = x^u$ with $u \mid q+1$, over $\mathbb{F}_{q^2}$, which are $\mathbb{F}_{q^2}$-maximal. The case where q is an odd power of 2 and $u = 3$ was considered in [Jin14, Sec. III (B)]. We obtain codes $[[8, 6, 2]]_2^{\ddagger}$, $[[64, 54, 3]]_4^{\dagger}$, $[[64, 52, 4]]_4^{\dagger}$, $[[176, 162, 3]]_8$, $[[176, 156, 5]]_8$, $[[176, 154, 6]]_8$, $[[176, 150, 8]]_8^{\dagger}$, $[[176, 146, 9]]_8^{\dagger}$.

Codes from maximal curves

To end this section, let us see some quantum codes arising from maximal curves as the ones considered in Section 4.2.3.

Example 4.3.8. Let $\mathcal{X}$ be the curve over $\mathbb{F}_{q^2}$ of Example 4.2.11

$$y^{q/p} + y^{q/p^2} + \cdots + y = ax^{q+1} \tag{4.3.3}$$

where $a \in \mathbb{F}_{q^2}$ verifies $a^q + a = 0$ and p is the characteristic of $\mathbb{F}_q$. For $q = 9$ let us take the curve $y^3 + y = \alpha^5 x^{10}$ over $\mathbb{F}_{81}$, where α is a primitive element of $\mathbb{F}_{81}$. It has 244 rational points and genus 9. The codes $C_{\mathcal{L}}(D, mQ)$ are Hermitian self-orthogonal if $m \leq 25$, by Corollary 4.2.6. For these values we obtain quantum codes with the following parameters: $[[243, 241, 2]]_9^{\ddagger}$, $[[243, 233, 3]]_9^{\dagger}$, $[[243, 219, 6]]_9$ and $[[243, 213, 9]]_9^{\dagger}$. For $q = 8$ take $a = 1$. The curve has 257 rational points and genus 12. From Corollary 4.2.6, the codes $C_{\mathcal{L}}(D, mQ)$ are Hermitian self-orthogonal if $m \leq 30$. With these values we can provide quantum codes with the following parameters: $[[256, 254, 2]]_8^{\ddagger}$, $[[256, 248, 3]]_8^{\dagger}$, $[[256, 238, 4]]_8$ and $[[256, 224, 8]]_8$. These quantum codes have good parameters compared to similar quantum codes in [Ede].

Example 4.3.9. This is a particular case of the curve given in Example 4.2.12. Take $r = 3$ in that example and let $\mathcal{X}$ be the curve over $\mathbb{F}_{q^6}$ given by the equation

$$y^q + y = x^{q^3+1}. \tag{4.3.4}$$

When $q = 2$, $\mathcal{X}$ has genus 4 and 129 rational points. From Corollary 4.2.6, the codes $C_{\mathcal{L}}(D, mQ)$ are Hermitian self-orthogonal if $m \leq 14$. With these values we obtain the following quantum codes: $[[128, 126, 2]]_8^{\ddagger}$, $[[128, 116, 4]]_8^{\dagger}$, $[[128, 112, 6]]_8^{\ddagger}$ and $[[128, 108, 8]]_8^{\ddagger}$.

4.4 Traces of Castle codes

Some of the codes we have obtained in the previous sections are defined over large extensions of $\mathbb{F}_q$. However, in practice we can be interested in codes defined over smaller fields. Such codes can be obtained from the formers by two ways by Definition 1.1.2: given a code C over $\mathbb{F}_{q^r}$, we can consider its subfield subcode $C|\mathbb{F}_q$ over $\mathbb{F}_q$ and its trace code $\mathrm{tr}(C)$. Both codes over $\mathbb{F}_q$ are closely related by Delsarte's theorem 1.1.3. Nevertheless, as we shall see, at least for AG codes the way of using trace maps is simpler. Remark however that quantum codes from subfield subcodes of affine variety codes have been studied in [GH15; GHR15].

As in the last sections, let $(\mathcal{X}, Q)$ be a pointed curve, now defined over $\mathbb{F}_{q^r}$. Remember from Section 1.1 that the trace map $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ and its extension coordinate-wise to $\mathbb{F}_{q^r}^n$ are surjective $\mathbb{F}_q$-linear maps. Letting $\mathcal{L}(\infty Q) = \cup_{i=0}^{\infty} \mathcal{L}(iQ)$ the space of rational functions on $\mathcal{X}$ having possible poles only at Q, we can also extend tr to $\mathcal{L}(\infty Q)$ by $\mathrm{tr}(f) = f + f^q + \cdots + f^{q^{r-1}}$. Here we list some properties of these extensions.

Lemma 4.4.1. The following properties hold.

(a) If $f \in \mathcal{L}(\infty Q)$ then $v_Q(\mathrm{tr}(f)) = q^{r-1} v_Q(f)$. Thus, if f is nonconstant then $\mathrm{tr}(f) \neq 0$.

(b) For all $f \in \mathcal{L}(\infty Q)$ we have $\mathrm{tr}(\mathrm{ev}(f)) = \mathrm{ev}(\mathrm{tr}(f)) = \mathrm{ev}(\mathrm{tr}(f^q))$.

Let $\mathcal{V}$ be the set of functions in $\mathcal{L}(\infty Q)$ evaluating to $\mathbb{F}_q^n$, $\mathcal{V} = \{f \in \mathcal{L}(\infty Q) : \mathrm{ev}(f) \in \mathbb{F}_q^n\}$. $\mathcal{V}$ is a $\mathbb{F}_q$-linear subspace of $\mathcal{L}(\infty Q)$ containing $\ker(\mathrm{ev})$. As a consequence of Lemma 4.4.1(c), $\mathcal{V}$ also contains $\mathrm{tr}(\mathcal{L}(\infty Q))$. The next proposition explains why trace codes are simpler to handle than subfield subcodes.

Proposition 4.4.2. $\mathcal{V} = \mathrm{tr}(\mathcal{L}(\infty Q)) + \ker(\mathrm{ev})$.

Proof. Since $\mathrm{tr} \circ \mathrm{ev}$ is surjective (as both maps are so), if $f \in \mathcal{V}$ there exists $g \in \mathcal{L}(\infty Q)$ such that $\mathrm{ev}(f) = \mathrm{tr}(\mathrm{ev}(g)) = \mathrm{ev}(\mathrm{tr}(g))$, hence $f - \mathrm{tr}(g) \in \ker(\mathrm{ev})$. The converse is clear. □

Thus $\mathrm{ev}(\mathcal{V}) = \mathrm{ev}(\mathrm{tr}(\mathcal{L}(\infty Q))$ and henceforth we will only consider trace codes. However, note that for Castle codes, we can also give a basis of $\ker(\mathrm{ev})$ over $\mathbb{F}_{q^r}$. For all $m > 0$ we have

$$\ker(\mathrm{ev}) \cap \mathcal{L}(mQ) = \mathcal{L}(mQ - D).$$

Let $\varphi = f_2^{q^r} - f_2$. Since $\mathcal{X}$ is Castle, we have $\mathrm{div}(\varphi) = D - nQ$. Consequently, there is an isomorphism $\mathcal{L}((n-m)Q) \to \mathcal{L}(mQ - D)$ given by $f \mapsto \varphi f$ and the set $\{\varphi f_1, \varphi f_2, \dots\}$ is a basis of $\ker(\mathrm{ev})$.

The following results allows us to obtain self-orthogonal trace codes over $\mathbb{F}_q$ when the pointed curve $(\mathcal{X}, Q)$ of genus g over $\mathbb{F}_{q^r}$ has the self-dual property. Writing $H(Q) = \{0 = \rho_1 < \rho_2 < \dots\}$, let $f_i \in \mathcal{L}(\infty Q)$ such that $v_Q(f_i) = \rho_i$ for $i = 1, 2, \dots$. In view of Lemma 4.4.1(c), if $\rho_i = q\rho_t$ then we take $f_i = f_t^q$. Then $L = \{f_1, f_2, \dots\}$ is a basis of $\mathcal{L}(\infty Q)$ over $\mathbb{F}_{q^r}$ verifying $L^q \subseteq L$, and the sets $L_m = \{f_i \in L : \rho_i \leq m\}$ are bases of $\mathcal{L}(mQ)$ for all $m \geq 0$. Let α be a primitive element of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Then $\{1, \alpha, \dots, \alpha^{r-1}\}$ is a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ and every element $a \in \mathbb{F}_{q^r}$ can be written as $a = \lambda_1 + \lambda_2\alpha + \cdots + \lambda_r\alpha^{r-1}$ with $\lambda_1, \dots, \lambda_r \in \mathbb{F}_q$.

Proposition 4.4.3. The set $\mathcal{B} = \{1\} \cup \{\mathrm{tr}(\alpha^j f_i) : j = 0, \dots, r-1, f_i \in L \text{ for } i > 1\}$ is a basis of $\mathrm{tr}(\mathcal{L}(\infty Q))$ over $\mathbb{F}_q$. The set $\mathcal{B}_m = \{1\} \cup \{\mathrm{tr}(\alpha^j f_i) : j = 0, \dots, r-1, f_i \in L_m \text{ for } i > 1\}$ is a basis of $\mathrm{tr}(\mathcal{L}(mQ))$ over $\mathbb{F}_q$.

Proof. It suffices to show the first statement. That $\mathcal{B}$ is a generator set follows from the $\mathbb{F}_q$-linearity of tr and the fact that L is a basis of $\mathcal{L}(\infty Q)$ over $\mathbb{F}_{q^r}$. To see that $\mathcal{B}$ is an independent set, and since $v_Q(\mathrm{tr}(f_i)) \neq v_Q(\mathrm{tr}(f_t))$ if $i \neq t$, it suffices to show that $\mathrm{tr}(f_i), \mathrm{tr}(\alpha f_i), \dots, \mathrm{tr}(\alpha^{r-1} f_i)$ are independent for all $i > 1$. If $0 = \sum_j \lambda_j \mathrm{tr}(\alpha^{j-1} f_i) = \mathrm{tr}(\sum_j \lambda_j \alpha^{j-1} f_i)$ then $\mathrm{tr}(a f_i) = 0$, where $a = \sum_j \lambda_j \alpha^{j-1}$. By Lemma 4.4.1(b), we have $a f_i = 0$ hence $a = 0$ and $\lambda_j = 0$ for all j. □

For $j = 0, \dots, r-1$, let $\beta_j \in \mathbb{F}_{q^r}$ such that $\beta_j^q = \alpha^j$. Then, if $f_i = f_t^q$ we have $\mathrm{ev}(\mathrm{tr}(\alpha^j f_i)) = \mathrm{ev}(\mathrm{tr}((\beta_j f_t)^q)) = \mathrm{ev}(\mathrm{tr}(\beta_j f_t))$ by Lemma 4.4.1(c). Consider the sets $L' = \{1\} \cup (L \setminus L^q)$ and $L'_m = L' \cap L_m$. Define accordingly the sets $\mathcal{B}'$ and $\mathcal{B}'_m$ by substituting L by L' and L_m by L'_m.

Corollary 4.4.4. The set $\mathrm{ev}(\mathcal{B}')$ generates $\mathrm{ev}(\mathrm{tr}(\mathcal{L}(\infty Q)))$ over $\mathbb{F}_q$. The set $\mathrm{ev}(\mathcal{B}'_m)$ generates $\mathrm{tr}(C_{\mathcal{L}}(D, mQ))$ over $\mathbb{F}_q$.

In order to ensure the self-orthogonality of trace codes, we shall use the following fact.

Lemma 4.4.5. Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^r}^n$. We have $\langle \mathrm{tr}(\mathbf{x}), \mathrm{tr}(\mathbf{y}) \rangle = \mathrm{tr}(\langle \mathbf{x}, \mathrm{tr}(\mathbf{y}) \rangle)$.

Proof. For $\mathbf{x}, \mathbf{z} \in \mathbb{F}_{q^r}^n$ and $0 \leq i \leq r$ we have $\langle \mathbf{x}^{q^i}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{z}^{q^{r-i}} \rangle^{q^i}$. Take $\mathbf{z} = \mathrm{tr}(\mathbf{y})$. Note that $\mathbf{z} \in \mathbb{F}_q^n$ and hence $\mathbf{z}^{q^{r-i}} = \mathbf{z}$. Thus

$$\langle \mathrm{tr}(\mathbf{x}), \mathrm{tr}(\mathbf{y}) \rangle = \sum_{i=0}^{r-1} \langle \mathbf{x}^{q^i}, \mathrm{tr}(\mathbf{y}) \rangle = \sum_{i=0}^{r-1} \langle \mathbf{x}, \mathrm{tr}(\mathbf{y}) \rangle^{q^i} = \mathrm{tr}(\langle \mathbf{x}, \mathrm{tr}(\mathbf{y}) \rangle).$$

□

Remember that given an integer m, with $0 \leq m \leq n + 2g - 2$, we write $m^\perp = n + 2g - 2 - m$. The self-orthogonality and the parameters of trace codes can be checked by using the following result.

Proposition 4.4.6. Let $(\mathcal{X}, Q)$ be a pointed curve of genus g over $\mathbb{F}_{q^r}$ verifying the self-dual property.

(1) If $mq^{\lfloor r/2 \rfloor} \leq m^{\perp}$ then $\mathrm{tr}(C_{\mathcal{L}}(D, mQ))$ is self-orthogonal over $\mathbb{F}_q$.

(2) If $mq^{r-1} < n$ then $\mathrm{ev}(\mathrm{tr}(f)) \neq 0$ for all $f \in \mathcal{L}(mQ)$.

(3) $d(\mathrm{tr}(C_{\mathcal{L}}(D, mQ))^{\perp}) = d(C_{\mathcal{L}}(D, m^{\perp}Q)|\mathbb{F}_q) \geq d(C_{\mathcal{L}}(D, m^{\perp}Q))$.

Proof. (1) Assume r is even. If $mq^{r/2} \leq m^{\perp}$ then for all $i = 0, \ldots, r/2$, we have

$$C_{\mathcal{L}}(D, mQ)^{q^i} \subseteq C_{\mathcal{L}}(D, mq^iQ) \subseteq C_{\mathcal{L}}(D, mQ)^{\perp}. \tag{4.4.1}$$

Let $f, g \in \mathcal{L}(mQ)$. According to Lemma 4.4.5, we have

$$\begin{aligned} \langle \mathrm{tr}(\mathrm{ev}(f)), \mathrm{tr}(\mathrm{ev}(g)) \rangle &= \mathrm{tr}(\sum_{j=0}^{r-1} \langle \mathrm{ev}(f), \mathrm{ev}(g)^{q^j} \rangle) \\ &= \mathrm{tr}(\sum_{j=0}^{r/2-1} \langle \mathrm{ev}(f), \mathrm{ev}(g)^{q^j} \rangle) + \mathrm{tr}(\sum_{j=r/2}^{r-1} \langle \mathrm{ev}(f), \mathrm{ev}(g)^{q^j} \rangle). \end{aligned} \tag{4.4.2}$$

By eq. (4.4.1) all summands in the first sum of eq. (4.4.2) are zero and so its trace is zero. For the second sum note that as seen in the proof of Lemma 4.4.5 we can write $\langle \mathrm{ev}(f), \mathrm{ev}(g)^{q^j} \rangle = \langle \mathrm{ev}(f)^{q^{r-j}}, \mathrm{ev}(g) \rangle^{q^j}$, with $r - j \leq r/2$. Then $\langle \mathrm{ev}(f)^{q^{r-j}}, \mathrm{ev}(g) \rangle = 0$ and the second trace is also 0. The case r odd is similar. (2) Let $f \in \mathcal{L}(mQ)$. It holds that $v_Q(\mathrm{tr}(f)) \leq mq^{r-1} < n$, hence $\mathrm{ev}(\mathrm{tr}(f)) \neq \mathbf{0}$. (3) Follows from Delsarte's theorem. □

Example 4.4.7. Consider the Suzuki curve with 65 rational points and genus 14 over $\mathbb{F}_8$. According to Proposition 4.4.6(1), the traces $\mathrm{tr}(C_{\mathcal{L}}(D, mQ))$ over $\mathbb{F}_2$ are self-orthogonal for $0 \leq m \leq 30$. Furthermore since $\dim(\mathrm{tr}(C_{\mathcal{L}}(D, 30Q))) = 32$, this code is self-dual. Thus the bound stated in item (1) is sharp in this case. From these traces, we derive quantum codes with parameters $[[64, 62, 2]]_2^{\ddagger}$, $[[64, 50, 4]]_2^{\ddagger}$, where the notation $[[n, k, d]]_q^{\dagger\ddagger}$ is as in Section 4.3.

Let us consider the case $r = 2$ and let $C = C_{\mathcal{L}}(D, mQ)$ be a code over $\mathbb{F}_{q^2}$. Note that the condition on m stated in Corollary 4.2.6 to ensure the Hermitian self-orthogonality of C, is exactly the same as the condition of Proposition 4.4.6(1), to ensure the self-orthogonality of $\mathrm{tr}(C)$. Thus, in some sense, the construction of quantum codes from traces of self-orthogonal codes extends to $r > 2$ the construction of quantum codes from Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$. Note also that besides considering traces $\mathrm{tr}(C_{\mathcal{L}}(D, mQ))$, we can use 'incomplete' traces, that is subcodes generated by some (but not all) elements of $\mathrm{ev}(\mathcal{B}'_m)$. In many cases these subcodes can provide quantum codes with better parameters than trace codes themselves.

Example 4.4.8. Consider the elliptic Hermitian curve $\mathcal{X} : y^2 + y = x^3$ with 9 rational points over $\mathbb{F}_4$ and let α be a primitive element of $\mathbb{F}_4$ over $\mathbb{F}_2$. The trace code $\mathrm{tr}(C_{\mathcal{L}}(D, 3Q)) =$

$\langle \mathbf{1}, \mathrm{ev}(\mathrm{tr}(x)), \mathrm{ev}(\mathrm{tr}(\alpha x)), \mathrm{ev}(\mathrm{tr}(y)), \mathrm{ev}(\mathrm{tr}(\alpha y)) \rangle$ has dimension 5 and dual distance 4. Thus it cannot be self-orthogonal. Remove the generator $\mathrm{ev}(\mathrm{tr}(y))$. Then we get a self-dual code of dimension 4 whose dual distance is also 4, that gives a quantum $[[8, 0, 4]]_2$ code whose parameters cannot be improved [Gra]. Furthermore this code cannot be obtained from $\mathcal{X}$ by using Hermitian self-orthogonality and construction (A). In the same way, consider the Hermitian curve over $\mathbb{F}_{q^{2r}}$ with $q^{3r} + 1$ points. The dual distance of the code $C_{\mathcal{L}}(D, (q^r + 1)Q)$ can be computed by using the order bound. Consider the trace $\mathrm{tr}(C_{\mathcal{L}}(D, (q^r + 1)Q))$ of this code over $\mathbb{F}_q$ of dimension $2r + 1$ and remove at most $r - 1$ generators from $\mathrm{ev}(\mathrm{tr}(y)), \ldots, \mathrm{ev}(\mathrm{tr}(\alpha^{r-1}y))$ in order to obtain a self-orthogonal code with the same dual distance as $\mathrm{tr}(C_{\mathcal{L}}(D, (q^r + 1)Q))$. Direct computations show that we get quantum codes $[[64, 50, 4]]_2^{\ddagger}$, $[[512, 492, 4]]_2^{\ddagger}$, $[[27, 19, 3]]_3^{\dagger}$, $[[729, 715, 3]]_3^{\dagger}$, $[[64, 56, 3]]_4^{\dagger}$, $[[125, 117, 3]]_5^{\dagger}$, $[[343, 335, 3]]_7^{\dagger}$, $[[512, 504, 3]]_8^{\dagger}$, $[[729, 721, 3]]_9^{\dagger}$, reaching good parameters in all cases. The same procedure can be carried out by using codes from other curves. For example, from the Norm-Trace curve over $\mathbb{F}_{q^r}$ we obtain quantum codes $[[32, 20, 4]]_2^{\ddagger}$, $[[128, 112, 4]]_2^{\ddagger}$, etc.

Chapter 5

Locally recoverable codes from algebraic curves

The modern distributed and cloud storage data systems aim the high data availability and, at the same time, the reliability of these data. However, to ensure that these systems can develop all their potential of performance, it is necessary to deal with the failures which are commonly part of their operations. In this direction, the use of coding techniques in these systems has played an important role in the protection against possible failures. These methods arose as an alternative to the replication technique, and recently much research has been done in this field; see [Gop+12; PHO13; TB14; BTV15; BTV16].

In this setting, motivated by significant improvements in terms of redundancy and reliability in storage systems, Gopalan et al. introduced in [Gop+12] the concept of *locality* in coding theory, and consequently the notion of locally recoverable codes (or LRC codes), the error-correcting codes to be used to ensure the fast recovery information in storage systems. Roughly speaking, local repair techniques deal with the recovery of lost encoded data by a local procedure, which means making use of small amount of data to repair a failure.

MDS codes (and Reed-Solomon codes in particular) are examples of LRC codes but they are not interesting in the viewpoint of local properties since they have the largest possible locality. In [TB14] a variation of Reed-Solomon codes (RS codes) for local recoverability purposes was introduced by Tamo and Barg. These so-called LRC-RS codes can have much smaller locality. However, it is well known that one of the main drawbacks of RS codes for practical applications relies on their small length. The same happens for LRC-RS codes. A classical way to overcome this problem is to consider codes from algebraic curves with many rational points. In this way, the above construction of LRC-RS codes was extended by Barg, Tamo, and Vlăduţ in [BTV16; TB14] to the so-called LRC-Algebraic Geometry codes (or LRC-AG codes), obtaining larger and powerful LRC codes.

In this chapter, we present some observations on the construction and properties concerning LRC-AG codes. We introduce the concepts related to LRC codes in Section 5.1, where we

present the Reed-Solomon-like construction given in [TB14] by Tamo and Barg. In Subsection 5.2.1 we slightly generalize the original construction LRC codes arising from AG codes given by Barg, Tamo, and Vlăduţ in [BTV15]. This generalization expands the family of LRC-AG codes so that we can get some codes with better parameters. In particular, some of these new LRC codes are in fact algebraic-geometric codes as shown in Subsection 5.2.2. Finally, in Subsection 5.2.3 we deal with local recovery. We prove that some LRC-AG codes admit a simplified recovering method by simple checksum and propose a family of curves that provide codes with this property.

5.1 Preliminaries on codes with locality

Let C be a code of length n and cardinality q^k over $\mathbb{F}_q$. A coordinate $i \in \{1, \ldots, n\}$ of C is said to have *locality* r if there exist $R_i \subseteq \{1, \ldots, n\} \backslash \{i\}$ of cardinality r and a map $\varphi_i : C_{R_i} \to \mathbb{F}_q$ such that for all $\mathbf{x} \in C$, the symbol x_i is equal to $\varphi_i(\mathbf{x}_{R_i})$, where $\mathbf{x}_{R_i}$ denotes the projection of $\mathbf{x}$ on the coordinates in R_i and $C_{R_i} = \{\mathbf{x}_{R_i} \ : \ x \in C\}$. That is to say, if for all $\mathbf{x}, \mathbf{y} \in C$, $\mathbf{x}_{R_i} = \mathbf{y}_{R_i}$ implies $x_i = y_i$, which is equivalent to say that the code $C_{R_i \cup \{i\}}$ has minimum distance at least 2. The code C is said to have *locality* r (or *all-symbol locality* r), if each coordinate $i \in \{1, \ldots, n\}$ has locality at most r.

The locality property of a code C means that any symbol x_i of a codeword $\mathbf{x}$ in C can be recovered from the symbols in $\mathbf{x}_{R_i}$ by $\varphi_i(\mathbf{x}_{R_i})$, the local recovery procedure. For this reason, the map φ_i and the set R_i are respectively called *recovering map* and *recovering set* for the coordinate i. We call a code with locality of *locally recoverable code*, or *LRC code* for short. We use the notation $(n, k, r)_q$ to refer to a q-ary linear code with length n, dimension k and locality r.

An example of $(n, k, 1)$ code is the replication code where each coordinate of an $[n/2, k]$ code is repeated. On the other hand, MDS codes are systematic at every k positions, hence they attain locality k. In particular, the locality parameter r of an (n, k, r) code satisfies $1 \leq r \leq k$.

The minimum distance of an (n, k, r) code is bounded by the Singleton-like relation

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2; \tag{5.1.1}$$

see [Gop+12]. Codes reaching such equality are called *optimal* LCR codes. Observe that this bound generalizes the Singleton bound (1.1.1) for the case $k = r$. Hence MDS codes (and Reed-Solomon codes in particular) are optimal LRC codes.

In what follows we present the construction due to Barg and Tamo [TB14] of optimal linear LRC codes attaining locality in the range $(1, k)$. Their construction relies on Reed-Solomon codes.

5.1.1 Reed-Solomon-like construction

As mentioned before, Reed-Solomon codes constitute a family of optimal LRC codes with the largest possible locality. Since the purpose of locality theory is to repair failures with small amount of data, it is desirable to derive codes with small locality. To this aim, we recall the Reed-Solomon code construction to expose the method obtained in [TB14].

Let q be a prime power. Remember that given a set $\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$ we have the evaluation map at $P_1, \ldots, P_n$

$$\begin{array}{rccc} \mathrm{ev} & : & \mathbb{F}_q[x] & \longrightarrow & \mathbb{F}_q^n \\ & & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array},$$

where $\mathbb{F}_q[x]$ denotes the set of univariate polynomials with coefficients in $\mathbb{F}_q$. For k a positive integer such that $k < n$, consider the set $V_k = \{f \in \mathbb{F}_q[x] \ : \ \deg(g) \leq k-1\}$. The linear code C obtained as the image of V_k by ev is called a Reed-Solomon code, which is an $[n, k, n-k+1]_q$ code. Since two polynomials of degree less than k are equal if any k of their values coincide, each polynomial in V_k can be obtained from any k symbols of codeword $\mathrm{ev}(f)$ by performing polynomial interpolation, and this is exactly the idea used in [TB14] to construct LRC codes, which we next present.

Let r be a positive integer and consider $\mathcal{P}_1, \ldots, \mathcal{P}_m \subseteq \mathbb{F}_q$ be $m \geq 2$ pairwise distinct subsets of cardinality $r+1$ such that there exists a polynomial $h \in \mathbb{F}_q[x]$ of degree $r+1$ that is constant over each subset $\mathcal{P}_i = \{P_{ij} \ : \ j = 1, \ldots, r+1\}$ for $i = 1, \ldots, m$. Notice that these choices can be done by using the group structure of $\mathbb{F}_q^\times$.

Let $\mathcal{P} = \cup_{i=1}^m \mathcal{P}_i$ and $n = \#\mathcal{P} = m(r+1)$. For an integer k satisfying $r \mid k$ and $k + \frac{k}{r} \leq n$, let L_h denote the $\mathbb{F}_q$-linear space of polynomials spanned by $1, h, \ldots, h^{\frac{k}{r}-1}$, and consider the linear space of polynomials

$$V = \bigoplus_{i=0}^{r-1} L_h x^i \subseteq \mathbb{F}_q[x]. \tag{5.1.2}$$

The linear code obtained by the image of the evaluation map at $\mathcal{P}$

$$\begin{array}{rccc} \mathrm{ev}_{\mathcal{P}} & : & V & \longrightarrow & \mathbb{F}_q^n \\ & & f & \mapsto & (f(P_{ij}) \ : \ i = 1, \ldots, m \ , \ j = 1, \ldots, r+1) \end{array}$$

is called the *LRC Reed-Solomon code*, or *LRC-RS code*, denoted by $C(\mathcal{P}, V)$.

As the degree of polynomials in V are at most $k + \frac{k}{r} - 2 < n$, the map $\mathrm{ev}_{\mathcal{P}}$ is injective, and thus the dimension of C equals k. Moreover, for any polynomial $f \in V$ and $i = 1, \ldots, m$, there exists a polynomial $\delta_i(x)$ of degree at most $r-1$ such that $\delta_i(P_{ij}) = f(P_{ij})$ for $j = 1, \ldots, r+1$. Such δ_i's can be computed through interpolation at any r points of $\mathcal{P}_i$ and consequently a recovering set for this local recovery procedure of the coordinate corresponding to a point P_{ij}

is $R_{ij} = \mathcal{P}_i \setminus \{P_{ij}\}$ with the recovery map written explicitly as

$$\varphi_{ij}(\mathrm{ev}_{\mathcal{P}}(f)_{R_{ij}}) = \sum_{\substack{t \\ t \neq j}} f(P_{it}) \prod_{\substack{s \\ s \neq t}} \frac{P_{ij} - P_{is}}{P_{it} - P_{is}}.$$

The properties of $C(\mathcal{P}, V)$ are summarized as follows.

Theorem 5.1.1. ([TB14, Th. 3.1]) The linear code $C(\mathcal{P}, V)$ is an optimal $(n, k, r)_q$ LRC code whose local recovery is performed by polynomial interpolation.

Despite the RS-like construction provides optimal LRC codes, its main drawback is the codes obtained are short compared with the size of the alphabet. Addressing this issue, Barg, Tamo, and Vladut [BTV15] provided an alternative construction from algebraic curves, which extends the aforementioned one. In next section we present their method to obtain larger LRC codes and point out some improvements on their approach.

5.2 Locally recoverable codes from algebraic curves

Let $\mathcal{X}$ and $\mathcal{Y}$ be two (projective, non-singular, geometrically irreducible) algebraic curves defined over $\mathbb{F}_q$. Given $\phi : \mathcal{X} \to \mathcal{Y}$ a separable covering of degree $r+1$, let us consider $\mathcal{S} \subseteq \mathcal{Y}(\mathbb{F}_q)$ a set of cardinality s consisting of rational totally split points of ϕ in $\mathcal{Y}$ whose fibres are rational points of $\mathcal{X}$ and $\mathcal{P} = \phi^{-1}(\mathcal{S}) \subseteq \mathcal{X}(\mathbb{F}_q)$.

Since the pullback map $\phi^* : \mathbb{F}_q(\mathcal{Y}) \to \mathbb{F}_q(\mathcal{X})$ provides a separable extension of fields $\mathbb{F}_q(\mathcal{X})|\phi^*(\mathbb{F}_q(\mathcal{Y}))$ of degree $r+1$, there exists an element $y \in \mathbb{F}_q(\mathcal{X})$ satisfying $\mathbb{F}_q(\mathcal{X}) = \phi^*(\mathbb{F}_q(\mathcal{Y}))(y)$. Hence, taking D' a divisor on $\mathcal{Y}$ with support disjoint to $\mathcal{S}$, we can consider the $\mathbb{F}_q$-linear space of rational functions on $\mathcal{X}$

$$V = \bigoplus_{i=0}^{r-1} \phi^*(\mathcal{L}(D'))y^i \subseteq \mathbb{F}_q(\mathcal{X}).$$

Observe that, owing to y being a primitive element to the field extension $\mathbb{F}_q(\mathcal{X})|\phi^*(\mathbb{F}_q(\mathcal{Y}))$ of degree $r+1$, the elements $1, y, \ldots, y^r$ are linearly independent over $\phi^*(\mathbb{F}_q(\mathcal{Y}))$ and consequently the space V is well-defined.

The code defined as the image of V by the evaluation map at $\mathcal{P}$

$$\begin{array}{rccl} \mathrm{ev}_{\mathcal{P}} & : & V & \longrightarrow & \mathbb{F}_q^n \\ & & f & \mapsto & (f(P) \ : \ P \in \mathcal{P}) \end{array},$$

with $n = \#\mathcal{P}$, is called the *LRC algebraic-geometric code* (or *LRC-AG codes*) denoted by $C(\mathcal{P}, V, \phi)$.

Notice that any rational function in $\phi^*(\mathcal{L}(D'))$ is constant on each fibre $\phi^{-1}(S)$ for $S \in \mathcal{S}$. Hence, the local recovery of an erased coordinate $f(P)$ of a codeword $\mathrm{ev}_{\mathcal{P}}(f)$, for $f \in V$, can be

performed by Lagrangian interpolation at the remaining r coordinates of $\mathrm{ev}_{\mathcal{P}}(f)$ corresponding to points in the fibre $\phi^{-1}(\phi(P))$ of P, since over the points of $\phi^{-1}(\phi(P))$ the function f becomes a polynomial over y.

Theorem 5.2.1. [BTV15, Th. 3.1] If $\mathrm{ev}_{\mathcal{P}}$ is injective then $C(\mathcal{P}, V, \phi) \subseteq \mathbb{F}_q^n$ is a linear (n, k, r) LRC code with parameters

$$n = s(r+1), \qquad k = r\ell(D'), \qquad \text{and} \qquad d \geq n - \deg(D')(r+1) - (r-1)\deg(y).$$

Note that $C = C(\mathcal{P}, V, \phi)$ is a subcode of the algebraic geometry code $C_{\mathcal{L}}(\mathcal{X}, D, G)$, where $D = \sum_{P \in \mathcal{P}} P$ and G is the smallest divisor on $\mathcal{X}$ with respect to $\geq$ whose Riemann-Roch space $\mathcal{L}(G)$ contains V. We in particular have

$$d(C) \geq d(C_{\mathcal{L}}(\mathcal{X}, D, G)) \geq n - \deg(G).$$

Example 5.2.2. In [BTV15] Barg and Tamo presented two families of LRC codes arising from the Hermitian curve $\mathcal{H}$ defined by $x^{q+1} = y^q + y$ over $\mathbb{F}_{q^2}$.

(a) The first considers the rational function $\phi = x : \mathcal{H} \to \mathbb{P}^1$ of degree q. Since x has only the point at infinity Q as ramification point, we take $\mathcal{S} = \mathbb{A}^1(\mathbb{F}_{q^2}) \subseteq \mathbb{P}^1$ and thus $x^{-1}(\mathcal{S}) = \mathcal{H}(\mathbb{F}_{q^2}) \backslash \{Q\}$. If $D' = l\infty$ then $V = \bigoplus_{i=0}^{q-2} \langle 1, x, x^2, \ldots, x^l \rangle y^i \subseteq \mathbb{F}_{q^2}(\mathcal{H})$. We get LRC codes with locality $q-1$ and parameters $n = q^3$, $k = r(l+1)$, and $d \geq n - \deg(G)$, where $G = -v_Q(x^l y^{r-1})Q = (lq + (r-1)(q+1))Q$.

(b) The second family is obtained by the morphism $\phi = y$ of degree $q+1$. The branch points of y are exactly the points in the set $M = \{b \in \mathbb{A}(\mathbb{F}_{q^2}) : b^q + b = 0\} \cup \{\infty\}$ and thus we take $\mathcal{S} = \mathbb{P}^1 \setminus M$. For $D' = l\infty$, we get $V = \bigoplus_{i=0}^{q-1} \langle 1, y, y^2, \ldots, y^l \rangle x^i \subseteq \mathbb{F}_{q^2}(\mathcal{H})$. Hence, we obtain LRC codes with locality q and parameters $n = q^3 - q$, $k = r(l+1)$ and $d \geq n - \deg(G)$, where $G = -v_Q(y^l x^{r-1})Q = (l(q+1) + (r-1)q)Q$.

Example 5.2.3. Following similar ideas as in the previous example, Ballico and Marcola [BM16] provide LRC-AG codes from the Norm-Trace curve $x^{1+q+\cdots+q^{u-1}} = y + y^q + \cdots + y^{q^{u-1}}$ defined over $\mathbb{F}_{q^u}$. They obtain two families of LRC codes:

(a) a family of LRC codes of locality $r = q^{u-1} - 1$ and parameters $n = q^{2u-1}, k = (t+1)(q^{u-1} - 1), d \geq n - tq^{u-1} - (q^{u-1} - 1)(1 + q + \cdots + q^{u-1})$; and

(b) a family of LRC codes of locality $r = q + \cdots + q^{u-1}$ and parameters $n = q^{2u-1} - q^{u-1}, k = (t+1)(q + \cdots + q^{u-1}), d \geq n - tq^{u-1} - (q + \cdots + q^{u-1}) - q^{u-1}(-1 + q + \cdots + q^{u-1})$.

Furthermore, in that paper a detailed analysis on the distance of Hermitian LRC codes given in Example 5.2.2 is done.

Example 5.2.4. Constructions (a) in the previous examples can be generalized to any Castle curve $(\mathcal{X}, Q)$; see Section 3.1. Take $\phi \in \mathcal{L}(\infty Q)$ such that $-v_Q(\phi) = \rho(Q)$, the multiplicity of $H(Q)$. Under the Castle conditions it holds that for every $a \in \mathbb{F}_q$ the fibre $\phi^{-1}(a)$ consists of $m = \rho(Q)$ points. Then, by taking $\mathcal{S} = \mathbb{F}_q$ and $D' = l\infty$ we can construct LRC codes of length $n = qm = \#\mathcal{X}(\mathbb{F}_q) - 1$ and locality $r = m - 1$. Another possible generalization of these constructions will be given in Section 5.2.3.

5.2.1 Improved parameters

In this section we propose a slight variation on the definition of LRC-AG codes that may lead to improvements on the parameters k and d of the obtained codes without affecting neither the locality nor the recovering method. As LRC codes are designed to be used in large storage systems, improvements on the dimension could be of practical interest.

Keeping the notation used at the beginning of the current section, $\mathcal{X}$ and $\mathcal{Y}$ stand for algebraic curves over $\mathbb{F}_q$, and $\phi : \mathcal{X} \to \mathcal{Y}$ denotes a separable covering of degree $r+1$. Rather than considering an unique divisor D on $\mathcal{Y}$, we may regard r distinct rational divisors $D'_0, \ldots, D'_{r-1}$ on $\mathcal{Y}$ with support disjoint from $\mathcal{S}$. Thus we can consider the space of rational functions on $\mathcal{X}$

$$V' := \bigoplus_{i=0}^{r-1} \phi^*(\mathcal{L}(D'_i))y^i \subseteq \mathbb{F}_q(\mathcal{X}) \tag{5.2.1}$$

and define the code $C = \mathrm{ev}_{\mathcal{P}}(V') \subseteq \mathbb{F}_q^n$.

Theorem 5.2.5. The code $C = \mathrm{ev}_{\mathcal{P}}(V') \subseteq \mathbb{F}_q^n$ is a linear (n, k, r) LRC code with parameters

$$n = s(r+1), \qquad k = \sum_{i=0}^{r-1} \ell(D'_i) \quad \text{and} \quad n - \deg(G) \leq d \leq \min_{0 \leq i \leq r-1}\{d_i\}$$

provided $\mathrm{ev}_{\mathcal{P}}|_{V'}$ is injective, where G is the smallest rational divisor with respect to $\leq$ whose Riemann-Roch space $\mathcal{L}(G)$ contains V', and d_i is the minimum distance of $C_i = \mathrm{ev}_{\mathcal{P}}(\phi^*(\mathcal{L}(D'_i)y^i)$, $i = 0, \ldots, r-1$. The local recovery of an erased coordinate $f(P)$ of $\mathrm{ev}_{\mathcal{P}}(f)$ can be performed by Lagrangian interpolation at the remaining r coordinates of $\mathrm{ev}_{\mathcal{P}}(f)$ corresponding to points in the fibre $\phi^{-1}(\phi(P))$ of P.

Proof. The statement on the parameters follows from construction. Since the functions in $\phi^*(\mathcal{L}(D'_i))$, $i = 0, \ldots, r-1$, are constant over each fibre of ϕ, for any codeword in C the coordinates corresponding to points in such a fibre can be seen as evaluations of polynomials of degree $r-1$ in the variable y, which can be retrieved from any r coordinates in the fibre through interpolation. □

Remark 5.2.6. Observe that $n > \deg(G)$ implies $\mathrm{ev}_{\mathcal{P}}|_{V'}$ is injective.

Remark 5.2.7. Codes arising from evaluation of spaces of rational functions of type (5.2.1) were considered by Maharaj in [Mah05] using the language of function fields. In that paper, the divisor G giving the lower bound on the minimum distance in the Theorem 5.2.5 is explicitly described as

$$G = \max\{\phi^*(D'_i) - \operatorname{div}(y^i) \ : \ 0 \leq i \leq r-1\},$$

where $\max(H, H') = \sum_{P \in \mathcal{X}} \max\{v_P(H), v_P(H')\}P$.

Employing a sequence of divisors $D'_0, \ldots, D'_{r-1}$ instead of a single divisor D provides greater flexibility to the construction. Typically, we can take $D'_0 \geq \ldots \geq D'_{r-1}$ since codewords of smaller weight come from evaluation of functions $f \in \phi^*(\mathcal{L}(D'_i))y^i$ with large i. This strategy allows increasing the dimension of C without decreasing its minimum distance. For example, if $\mathcal{Y} = \mathbb{P}^1$ and $Q = \phi^{-1}(\infty)$, instead of $V = \bigoplus_{i=0}^{r-1} \phi^*(\mathcal{L}(l\infty))y^i$ we can consider the space $V' = \bigoplus_{i=0}^{r-1} \phi^*(\mathcal{L}(l_i\infty))y^i$. Whenever $-v_Q(x^{l_i}y^i) \leq -v_Q(x^l y^{r-1})$, it holds that $V \subseteq \mathcal{L}(G)$ for every divisor G such that $V \subseteq \mathcal{L}(G)$, so that we increase the dimension without affecting the estimate on the minimum distance. We next give some examples of how this variation can provide LRC-AG codes with better parameters.

Example 5.2.8. Consider the Hermitian LRC code $C = \operatorname{ev}_{\mathcal{P}}(V)$ of Example 5.2.2(a), where

$$V = \bigoplus_{i=0}^{r-1} x^*(\mathcal{L}(l\infty))y^i = \bigoplus_{i=0}^{r-1} \langle 1, x, x^2, \ldots, x^l \rangle y^i.$$

Since $-v_Q(x^{l_i}y^i) \leq -v_Q(x^l y^{r-1})$ is now equivalent to $l_i q + i(q+1) \leq lq + (r-1)(q+1)$, this condition holds true by taking $l_{r-i-1} = l + i - 1$ for $i = 0, \ldots, r-1$. Hence with the code $C' = \operatorname{ev}_{\mathcal{P}}(V')$ for

$$V' = \bigoplus_{i=0}^{r-1} x^*(\mathcal{L}(l_i\infty))y^i,$$

we can increase the dimension by $(r-1) + \cdots + 1 = r(r-1)/2$ units without affecting the estimate on the minimum distance. For example, if $q = 5$ then $r = 4$. For any value of l whenever $\operatorname{ev}_{\mathcal{P}}$ is injective, the dimension increases by 6 units while the Singleton-optimal defect $n - k - \left\lceil \frac{k}{r} \right\rceil + 2 - d$ decreases by 8 units. For example, for $l = 2$ this defect is reduced from 15 to 7. For codes on other curves for which the order of y is much larger than the order of x the increase on the dimension may be higher.

Example 5.2.9. In this example we take the opposite way and construct Hermitian LRC codes with improved minimum distance and the same dimension. Let $q = 3$. Rather than consider

$$V = x^*(\mathcal{L}(l\infty)) \oplus x^*(\mathcal{L}(l\infty))y,$$

we shall take

$$V' = x^*(\mathcal{L}((l+1)\infty)) \oplus x^*(\mathcal{L}((l-1)\infty))y.$$

l	1	2	3	4	5	6
k	4	6	8	10	12	14
d	20	17	14	11	8	6
d'	21	18	15	12	9	6

Table 5.1: Dimension and minimum distance of codes C and C' for $q = 3$.

l	1	2	3	4	5	6	7	8	9	10	11	12	13
k	6	9	12	15	18	21	24	27	30	33	36	39	42
d	50	46	42	38	34	30	26	22	18	14	10	8	6
d'	54	50	46	42	38	34	30	26	22	18	14	10	8

Table 5.2: Parameters of C and C' in Example 5.2.9 for $q = 4$.

It is clear that $C = \mathrm{ev}_{\mathcal{P}}(V)$ and $C' = \mathrm{ev}_{\mathcal{P}}(V')$ have the same dimension. But now we have

$$V \subseteq \mathcal{L}((3l+4)Q) \text{ and } V' \subseteq \mathcal{L}((3l+3)Q),$$

which leads to an increment of one unit in the minimum distance. In Table 1 we compare their true minimum distances. For larger values of q, slight modifications like this may provide more significant improvements. Similarly for $q = 4$, evaluating the spaces

$$V = x^*(\mathcal{L}(l\infty)) \oplus x^*(\mathcal{L}(l\infty))y \oplus x^*(\mathcal{L}(l\infty))y^2$$

and

$$V' = x^*(\mathcal{L}((l+1)\infty)) \oplus x^*(\mathcal{L}(l\infty))y \oplus x^*(\mathcal{L}((l-1)\infty))y^2,$$

we get LRC codes over $\mathbb{F}_{16}$ with length $n = 64$ and locality $r = 3$. Here

$$V \subseteq \mathcal{L}((4l+10)Q) \text{ and } V' \subseteq \mathcal{L}((4l+6)Q),$$

so the improvement on the minimum distance should be about 4 units. The dimension k and true minimum distances d, d' of these codes are listed in Table 2. The calculations have been computed with Magma [BCP97].

5.2.2 Locality in AG codes

As in the previous section, let $\mathcal{X}$ and $\mathcal{Y}$ be two curves over $\mathbb{F}_q$ with a separable covering $\phi : \mathcal{X} \to \mathcal{Y}$ of degree $r+1$, $V = \bigoplus_{i=0}^{r-1} \phi^*(\mathcal{L}(D_i'))y^i \subseteq \mathbb{F}_q(\mathcal{X})$ and $C = \mathrm{ev}_{\mathcal{P}}(V)$. The estimative on the minimum distance of C in Theorem 5.2.5 comes from the Goppa bound on the minimum distance of the AG code $C_{\mathcal{L}}(\mathcal{X}, D, G) = \mathrm{ev}_{\mathcal{P}}(\mathcal{L}(G))$, where $D = \sum_{P \in \mathcal{P}} P$ and G is the smallest divisor on $\mathcal{X}$ such that $V \subseteq \mathcal{L}(G)$.

It follows that $C_{\mathcal{L}}(\mathcal{X}, D, G)$ is the smallest AG code containing C. The error correction capa-

bilities of C are estimated through the corresponding capabilities of $C_{\mathcal{L}}(\mathcal{X}, D, G)$. Furthermore, no efficient algorithms for decoding C are currently available, so that we are compelled to decode C as a subcode of $C_{\mathcal{L}}(\mathcal{X}, D, G)$. Consequently, the best results are obtained when C is itself an AG code, that is, when $V = \mathcal{L}(G)$. In general, we can not expect this to happen when $D'_0 = \cdots = D'_{r-1}$, but it is possible when these divisors are suitably chosen.

In what follows we discuss when Hermitian one-point codes with the morphism $\phi = x$ coincides with the LRC codes constructed in the previous section. Note that in this case a function $f \in \mathcal{L}(\infty Q) \subseteq \mathbb{F}_{q^2}(\mathcal{H})$ can be uniquely written as a polynomial $f \in \mathbb{F}_{q^2}[x][y]$ with $\deg_y(f) < q$. Such f may appear in the set V of an LRC code if $\deg_y(f) < q - 1$.

Proposition 5.2.10. Let $\mathcal{H}$ be the Hermitian curve $x^{q+1} = y + y^q$ over $\mathbb{F}_{q^2}$. The space of functions $V = \bigoplus_{i=0}^{t} \langle 1, x, x^2, \ldots, x^{l_i} \rangle y^i \subseteq \mathbb{F}_q(\mathcal{H})$, with $t \leq q-2$ is a Riemann-Roch space $\mathcal{L}(G)$ if and only if there exists j, $0 \leq j \leq t+1$, such that $l_{t-i} = i$ if $i < j$ and $l_{t-i} = i+1$ if $i \geq j$. In this case $G = mQ$, where Q is the point at infinity of $\mathcal{H}$ and $m = (t+1)q + t - j$ if $j \leq t$ or $m = t(q+1)$ if $j = t+1$.

Proof. The smallest Riemann-Roch space containing V is $\mathcal{L}(mQ)$ with $m = \max\{-v_Q(x^{l_i}y^i) : i = 0, \ldots, t\} = \max\{l_i q + i(q+1) : i = 0, \ldots, t\}$. Let us first assume $V = \mathcal{L}(mQ)$. Then for $i = 0, \ldots, t$, we have $l_{t-i} \leq i+1$, since otherwise $-v_q(x^{l_{t-i}}y^{t-i}) > -v_Q(x^{i+2}y^{t-i}) > -v_Q(y^{t+1})$ so $y^{t+1} \in V$. In particular $l_t = 0$ or $l_t = 1$. A similar argument proves that for all $i = 1, \ldots, t$, we have $l_{i-1} \geq l_i + 1$. From these two conditions, we deduce that there exists j, $0 \leq j \leq t+1$, such that $l_{t-i} = i$ if $i < j$ and $l_{t-i} = i+1$ if $i \geq j$. Conversely, it is simple to check that under these conditions we have $m = -v_Q(x^{l_{t-j}}y^{t-j}) = (j+1)q + (t-j)(q+1) = (t+1)q + t - j$ if $j \leq t$ and $m = -v_Q(y^t) = t(q+1)$ if $j = t+1$. In either case it holds that $\dim(V) = \ell(mQ)$, hence we get equality $V = \mathcal{L}(mQ)$. □

Example 5.2.11. Consider the LRC codes obtained from the Hermitian curve with $q = 4$ and the morphism $\phi = x$. There are exactly four among them which are AG codes, namely the evaluation of the following spaces

$$V = \langle 1, x, x^2 \rangle \oplus \langle 1, x \rangle y \oplus \langle 1 \rangle y^2 = \mathcal{L}(-v_Q(y^2)Q) = \mathcal{L}(10Q)$$
$$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x \rangle y \oplus \langle 1 \rangle y^2 = \mathcal{L}(-v_Q(x^3)Q) = \mathcal{L}(12Q)$$
$$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x, x^2 \rangle y \oplus \langle 1 \rangle y^2 = \mathcal{L}(-v_Q(x^2y)Q) = \mathcal{L}(13Q)$$
$$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x, x^2 \rangle y \oplus \langle 1, x \rangle y^2 = \mathcal{L}(-v_Q(xy^2)Q) = \mathcal{L}(14Q).$$

5.2.3 Locally recoverable codes from Artin-Schereier curves

We start this section by presenting a motivate example for what follows. It deals with a property that we shall develop along this section.

Example 5.2.12. Let us consider the Hermitian LRC-AG codes of Example 5.2.2(a) over the field $\mathbb{F}_9$ with locality $r = 2$. For $a \in \mathbb{F}_{q^2}$, each fibre $\phi^{-1}(a)$ is of type $\{P_{ab_1}, P_{ab_2}, P_{ab_3}\}$ with $a^4 = b_i^3 + b_i$ for $i = 1, 2, 3$. Since a function $f \in V$ can be written as $f = g_0(x) + g_1(x)y$, with $g_0, g_1 \in \phi^*(\mathcal{L}(D'))$, we have $f(P_{ab_i}) = g_0(a) + g_1(a)b_i$ and thus

$$f(P_{ab_1}) + f(P_{ab_2}) + f(P_{ab_3}) = 3g_0(a) + g_1(a)(b_1 + b_2 + b_3) = g_1(a)(b_1 + b_2 + b_3) = 0$$

because $b_1 + b_2 + b_3 = 0$ as it is the sum of the roots of the polynomial $t(T) = T^3 + T - a^4$ (that is the coefficient of T^2). Then the coordinate $f(P_{ab_1})$ of the codeword $\mathrm{ev}_{\mathcal{P}}(f)$ can be recovered as $f(P_{ab_1}) = -f(P_{ab_2}) - f(P_{ab_3})$.

Although the construction of LRC-AG codes given in Subsection 5.2.1 ensures a local recovery by polynomial interpolation, the example above shows that in some cases the recovery procedure can be performed also through a simple checksum, which is faster and easier. Furthermore, this property can be viewed as an additional feature of such codes, allowing a simple and fast checking of each block in a codeword for possible errors. In this section we shall provide a wide family of LRC-AG codes satisfying this property. To this end, we first recall some identities regarding roots of univariate polynomials.

Consider the elementary symmetric polynomials on the variables $x_1, \ldots, x_d$ over an arbitrary field

$$\begin{aligned} \sigma_1 = \sigma_1(x_1, \ldots, x_d) &= x_1 + \cdots + x_d \\ \sigma_2 = \sigma_2(x_1, \ldots, x_d) &= x_1x_2 + x_1x_3 + \cdots + x_{d-1}x_d \\ &\vdots \\ \sigma_d = \sigma_d(x_1, \ldots, x_d) &= x_1 \cdots x_d. \end{aligned}$$

They relate the roots of an univariate polynomial to its coefficients by the expression

$$(T - x_1) \cdots (T - x_d) = T^d - \sigma_1 T^{d-1} + \sigma_2 T^{d-2} + \cdots + (-1)^d \sigma_d;$$

see e.g. [CLO92, § 7.1]. In general, for a polynomial $t(T) = t_d T^d + \cdots + t_1 T + t_0$ of degree d, the elementary symmetric polynomials on the roots $x_1, \ldots, x_d$ of t are related to its coefficients by the identities

$$\sigma_i = (-1)^i \frac{t_{d-i}}{t_d}, \qquad i = 1, \ldots, d,$$

also known as the *Vieta's formulae*. Consider now for $s \geq 1$ the symmetric multivariate polynomials on $x_1, \ldots, x_d$

$$\pi_s = \pi_s(x_1, \ldots, x_d) = x_1^s + \cdots + x_d^s,$$

called *power sums polynomials*. They are related to the elementary symmetric polynomials by

the so-called *Newton-Girard identities* [CLO92, § 7.1]: for each integer $1 \leq s \leq d$, we have

$$\begin{aligned} \pi_1 &= \sigma_1 \\ \pi_2 &= \sigma_1\pi_1 - 2\sigma_2 \\ &\vdots \\ \pi_s &= -\left(\textstyle\sum_{j=1}^{s-1}(-1)^j\pi_{s-j}\sigma_j\right) - (-1)^s s\sigma_s. \end{aligned} \quad .$$

Let p be the characteristic of $\mathbb{F}_q$. Remember that a polynomial over $\mathbb{F}_q[x]$ is *linearized* if the exponents of all its nonzero monomials are powers of p. A polynomial of type $L(x) - \alpha$, for L a linearized polynomial over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q$, is called an *affine p-polynomial*.

Lemma 5.2.13. If $x_1, ..., x_d$ are roots of an affine p-polynomial of degree d over $\mathbb{F}_q$, then $\pi_i(x_1, ..., x_d) = 0$ for $i = 1, \ldots, d-2$.

Proof. By induction. Clearly $\pi_1 = \sigma_1 = 0$. Assume $\pi_1 = \cdots = \pi_{i-1} = 0$ for $i \leq d-3$. Then $\pi_i = \pm i\sigma_i$. If $\sigma_i = 0$ we have $\pi_i = 0$. If $\sigma_i \neq 0$ then $d - i = p^h - i$ is a power of p. Thus $i \equiv 0 \pmod{p}$ and again $\pi_i = 0$. Therefore $\pi_1 = \cdots = \pi_{d-2} = 0$. □

Next we extend the idea of Example 5.2.12 to a wide class of curves providing families of LRC codes allowing local recovery by a checksum map. The codes we propose come from the family of Artin-Schereir curves.

Let $\mathcal{X}$ be an algebraic non-singular curve defined over $\mathbb{F}_q$ by an equation of separated variables

$$F(x) = L(y), \tag{5.2.2}$$

where F and L are univariate polynomials over $\mathbb{F}_q$ of coprime degrees and L is a separable linearized polynomial of degree $m = p^h$, where $p = \mathrm{char}(\mathbb{F}_q)$.

Let $\phi : \mathcal{X} \to \mathbb{P}^1$ be the morphism of degree m given by the rational function x and consider the set

$$M = \{a \in \mathbb{F}_q \ : \ \text{there exists } b \in \mathbb{F}_q \text{ with } F(a) = L(b)\}.$$

Note that, by our assumptions on L, for each $a \in M$ the function $x - a$ has m distinct zeroes. Note also that $\mathcal{X}$ has exactly one point at infinity Q which is the common pole of x and y. The point Q is the only point of $\mathcal{X}$ that ramifies over the morphism ϕ. Let $\mathcal{S} \subseteq M$ be a subset of cardinality $s > 0$. For $i = 0, \ldots, m-2$, take a divisor $D'_i = l_i\infty$ of $\mathbb{P}^1$ and consider the space of functions

$$V = \bigoplus_{i=0}^{m-2} \phi^*(\mathcal{L}(D'_i))y^i \subseteq \mathbb{F}_q(\mathcal{X})$$

with $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x)(y)$. From Proposition 4.2.9 it holds that $V \subseteq \mathcal{L}(\infty Q)$ and the Weierstrass semigroup $H(Q)$ of $\mathcal{X}$ at Q is generated by $-v_Q(x) = \deg(L)$ and $-v_Q(y) = \deg(F)$. Consider also the set of points $\mathcal{P} = \phi^{-1}(\mathcal{S})\backslash\{Q\}$. Then we have a code $C = \mathrm{ev}_{\mathcal{P}}(V) \subseteq \mathbb{F}_q^n$ of length

$n = \#\mathcal{P} = ms$. According to the Theorem 5.2.5, C is an LRC code based on polynomial interpolation with locality $r = m - 1$.

Proposition 5.2.14. The linear code $C \subseteq \mathbb{F}_q^n$ described above is an LRC code with locality $m - 1$ allowing a local recovery based on addition.

Proof. For $a \in M$, let $\phi^{-1}(a) = \{P_1, \ldots, P_m\}$ be the fibre of x at a and write $f_{aj} = f(P_j)$ the evaluation at the point $P_j \in \phi^{-1}(a)$ of a function

$$f = \sum_{i=0}^{m-2} g_i y^i \in V.$$

The functions $g_i \in \phi^*(\mathcal{L}(D_i'))$ are constant over each fibre so we can write $g_i = g_i(P_j) \in \mathbb{F}_q$ for any P_j. Then $f_{aj} = g_0 b_j^0 + \cdots + g_{m-2} b_j^{m-2}$ with $b_j = y(P_j)$ and so

$$\sum_{j=1}^{m} f_{aj} = m g_0 + g_1 \pi_1 + \cdots + g_{m-2} \pi_{m-2} = g_1 \pi_1 + \cdots + g_{m-2} \pi_{m-2},$$

where $\pi_i = \pi_i(b_1, \ldots, b_m)$ is the i-th power sum polynomial on the roots $b_1, \ldots, b_m$ of $L(T) - F(a)$. Since $L(T) - F(a)$ is an affine p-polynomial, it follows from Lemma 5.2.13 that $\pi_1 = \cdots = \pi_{m-2} = 0$. Therefore $f_{a1} + \cdots + f_{am} = 0$ and the local recovery of an erased symbol f_{aj} is obtained from the sum of the remaining symbols in the fibre $x^{-1}(a)$. □

Example 5.2.15. LRC codes arising from Hermitian and Norm-Trace curves in Example 5.2.2(a) and Example 5.2.3(a) satisfy the construction above. Hence recovering single erasures on these codes can be performed through addition.

Bibliography

[AK01] A. Ashikhmin and E. Knill. "Nonbinary quantum stabilizer codes." *IEEE Trans. Inform. Theory* 47.7 (2001), pp. 3065–3072.

[Arb+85] E. Arbarello et al. *Geometry of algebraic curves*. Vol. 1. Springer-Verlag, 1985.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language." *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[Bee07] P. Beelen. "The order bound for general algebraic geometric codes." *Finite Fields Appl.* 13.3 (2007), pp. 665–680.

[BK98] E. Ballico and S. J. Kim. "Weierstrass Multiple Loci of n-Pointed Algebraic Curves." *J. Algebra* 199.2 (1998), pp. 455–471.

[BM16] E. Ballico and C. Marcolla. "Higher Hamming weights for locally recoverable codes on algebraic curves." *Finite Fields Appl.* 40 (2016), pp. 61–72.

[BT06] P. Beelen and N. Tutaş. "A generalization of the Weierstrass semigroup." *J. Pure Appl. Algebra* 207.2 (2006), pp. 243–260.

[BTV15] A. Barg, I. Tamo, and S. Vlăduţ. "Locally recoverable codes on algebraic curves." *2015 IEEE International Symposium on Information Theory (ISIT)*. 2015, pp. 1252–1256.

[BTV16] A. Barg, I. Tamo, and S. Vlăduţ. "Locally recoverable codes on algebraic curves." *ArXiv preprint ArXiv:1603.08876* (2016).

[CDK94] A. Campillo, F. Delgado, and K. Kiyek. "Gorenstein property and symmetry for one-dimensional local Cohen-Macaulay rings." *Manuscripta Math.* 83.1 (1994), pp. 405–423.

[Che01] H. Chen. "Some good quantum error-correcting codes from algebraic-geometric codes." *IEEE Trans. Inform. Theory* 47.5 (2001), pp. 2059–2061.

[CLO92] D. Cox, J. Little, and D. O'shea. *Ideals, varieties, and algorithms*. Vol. 3. Springer, 1992.

[CS96] A. R. Calderbank and P. W Shor. "Good quantum error-correcting codes exist." *Phys. Rev. A* 54.2 (1996), pp. 1098–1105.

[CT05] C. Carvalho and F. Torres. "On Goppa codes and Weierstrass gaps at several points." *Des. Codes Cryptography* 35.2 (2005), pp. 211–225.

[Del90] F. Delgado. "The symmetry of the Weierstrass generalized semigroups and affine embeddings." *Proc. Am. Math. Soc.* 108.3 (1990), pp. 627–631.

[DGN08] F. Delgado, C. Galindo, and A. Núñez. "Generating sequences and Poincaré series for a finite set of plane divisorial valuations." *Adv. Math.* 219.5 (2008), pp. 1632–1655.

[DK09] I. Duursma and R. Kirov. "An extension of the order bound for AG codes." *Applied algebra, algebraic algorithms and error-correcting codes. 18th international symposium, AAECC-18, Tarragona, Sapin, June 8–12, 2009. Proceedings.* 2009, pp. 11–22.

[DKP11] I. Duursma, R. Kirov, and S. Park. "Distance bounds for algebraic geometric codes." *J. Pure Appl. Algebra* 215.8 (2011), pp. 1863–1878.

[DP10] I. M. Duursma and S. Park. "Coset bounds for algebraic geometric codes." *Finite Fields Appl.* 16.1 (2010), pp. 36–55.

[Duu08] I. M. Duursma. "Algebraic geometry codes: general theory." *Advances in algebraic geometry codes.* Vol. 5. Ser. Coding Theory Cryptol. World Sci. Publ., Hackensack, NJ, 2008, pp. 1–48.

[Ede] Y. Edel. *Some Good Quantum Twisted Codes.* URL: `http://www.mathi.uni-heidelberg.de/~yves/Matrizen/QTBCH/QTBCHindex.html`.

[FM04] K. Feng and Z. Ma. "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes." *IEEE Trans. Inform. Theory* 50.12 (2004), pp. 3323–3325.

[GB99] M. Grassl and T. Beth. "Relations between classical and quantum errorcorrecting codes." *Proceedings Workshop "Physik und Informatik", DPG-Frhjahrstagung, Heidelberg, Mrz.* 1999, pp. 45–57.

[GBR04] M. Grassl, T. Beth, and M. Roetteler. "On optimal quantum codes." *Int. J. Quantum Inf.* 2.01 (2004), pp. 55–64.

[Gei+11] O. Geil et al. "On the order bounds for one-point AG codes." *Adv. Math. Commun.* 5.3 (2011), pp. 489–504.

[GH15] C. Galindo and F. Hernando. "Quantum codes from affine variety codes and their subfield-subcodes." *Des. Codes Cryptography* 76.1 (2015), pp. 89–100.

[GHR15] C. Galindo, F. Hernando, and D. Ruano. "Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement." *Quantum Inf. Process.* 14.9 (2015), pp. 3211–3231.

[Gop+12] P. Gopalan et al. "On the locality of codeword symbols." *IEEE Trans. Inform. Theory* 58.11 (2012), pp. 6925–6934.

[Gop81] V. D. Goppa. "Codes on algebraic curves." *Soviet Math. Dokl.* Vol. 24. 1981, pp. 170–172.

[Got02] D. Gottesman. "An introduction to quantum error correction." *Proceedings of Symposia in Applied Mathematics.* Vol. 58. 2002, pp. 221–236.

[Gra] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes.* URL: `http://www.codetables.de`.

[HK01] M. Homma and S. J. Kim. "Goppa codes with Weierstrass pairs." *J. Pure Appl. Algebra* 162.2 (2001), pp. 273–290.

[HKT08] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field.* Princeton: Princeton University Press, 2008.

[Hom96] M. Homma. "The Weierstrass semigroup of a pair of points on a curve." *Arch. Math.* 67.4 (1996), pp. 337–348.

[HVP98] T. Høholdt, J. H. Van Lint, and R. Pellikaan. "Algebraic geometry codes." *Handbook of coding theory* 1.Part 1 (1998), pp. 871–961.

[Jin14] L. Jin. "Quantum stabilizer codes from maximal curves." *IEEE Trans. Inform. Theory* 60.1 (2014), pp. 313–316.

[JX12] L. Jin and C. Xing. "Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes." *IEEE Trans. Inform. Theory* 58.8 (2012), pp. 5484–5489.

[Kim94] S. J. Kim. "On the index of the Weierstrass semigroup of a pair of points on a curve." *Arch. Math.* 62.1 (1994), pp. 73–82.

[KM08] J.-L. Kim and G. L. Matthews. "Quantum error-correcting codes from algebraic curves." *Advances in algebraic geometry codes.* Vol. 5. Ser. Coding Theory Cryptol. World Sci. Publ., Hackensack, NJ, 2008, pp. 419–444.

[KW08] J.-L. Kim and J. Walker. "Nonbinary quantum error-correcting codes from algebraic curves." *Discrete Math.* 308.14 (2008), pp. 3115–3124.

[Mah05] H. Maharaj. "Explicit constructions of algebraic-geometric codes." *IEEE Trans. Inform. Theory* 51.2 (2005), pp. 714–722.

[Mat01] G. L. Matthews. "Weierstrass pairs and minimum distance of Goppa codes." *Des. Codes Cryptography* 22.2 (2001), pp. 107–121.

[Mat04] G. L. Matthews. "The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve." *Finite fields and applications. 7th international conference, $\mathbb{F}_{q^7}$, Toulouse, France, May 5–9, 2003.* 2004, pp. 12–24.

[MO15] C. Munuera and W. Olaya-León. "An introduction to algebraic geometry codes." *Algebra for secure and reliable communication modeling*. Vol. 642. Contemp. Math. Amer. Math. Soc., Providence, RI, 2015, pp. 87–117.

[Mor91] C. J. Moreno. *Algebraic curves over finite fields*. 97. Cambridge University Press, 1991.

[Moy11] J. J. Moyano-Fernández. "On Weierstrass semigroups at one and two points and their corresponding Poincaré series." *Abh. Math. Semin. Univ. Hamb.* 81.1 (2011), pp. 115–127.

[Moy15] J. J. Moyano-Fernández. "Poincaré series for curve singularities and its behaviour under projections." *J. Pure Appl. Algebra* 219.6 (2015), pp. 2449–2462.

[MST09] C. Munuera, A. Sepúlveda, and F. Torres. "Castle curves and codes." *Adv. Math. Commun.* 3.4 (2009), pp. 399–408.

[MT16] C. Munuera and W. Tenório. "Some contributions to the construction of Locally Recoverable codes from algebraic curves." *ArXiv preprint ArXiv:1606.09073* (2016).

[MTT16] C. Munuera, W. Tenório, and F. Torres. "Quantum error-correcting codes from algebraic geometry codes of Castle type." *Quantum Inf. Process.* 15.10 (2016), pp. 4071–4088.

[MU00] R. Matsumoto and T. Uyematsu. "Constructing quantum error-correcting codes for p m-state systems from classical error-correcting codes." *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* 83.10 (2000), pp. 1878–1883.

[OM13] W. Olaya-León and C. Munuera. "On the minimum distance of Castle codes." *Finite Fields Appl.* 20 (2013), pp. 55–63.

[PHO13] L. Pamies-Juarez, H. Hollmann, and F. Oggier. "Locally repairable codes with multiple repair alternatives." *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*. IEEE. 2013, pp. 892–896.

[Ser12] J.P. Serre. *Algebraic groups and class fields*. Vol. 117. Springer Science & Business Media, 2012.

[Sha08] T. Shaska. "Quantum codes from algebraic curves with automorphisms." *Condensed Matter Physics* 11.2 (2008), pp. 383–396.

[SK06] P. K. Sarvepalli and A. Klappenecker. "Nonbinary quantum codes from Hermitian curves." *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. Springer. 2006, pp. 136–143.

[Ste96] A. Steane. "Multiple-particle interference and quantum error correction." *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Vol. 452. 1954. 1996, pp. 2551–2577.

[Sti09] H. Stichtenoth. *Algebraic function fields and codes.* 2nd ed. Berlin: Springer, 2009.

[Sti88] H. Stichtenoth. "Self-dual Goppa codes." *J. Pure Appl. Algebra* 55.1-2 (1988), pp. 199–211.

[TB14] I. Tamo and A. Barg. "A family of optimal locally recoverable codes." *IEEE Trans. Inform. Theory* 60.8 (2014), pp. 4661–4676.

[TVN07] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes. Basic notions.* Providence, American Mathematical Society (AMS), 2007.

[vv88] J. H. van Lint and G. van der Geer. *Introduction to coding theory and algebraic geometry. (Based on lectures given in the seminar held at Schloß Mickeln, Düsseldorf, November 16-21, 1987).* Basel: Birkhäuser Verlag, 1988.