# ON LATTICES FROM FUNCTION FIELDS

by

LEYLA ATEŞ

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University
April 2017

ON LATTICES FROM FUNCTION FIELDS

APPROVED BY

Prof. Dr. Cem Güneri ..............................................
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu ..............................................

Prof. Dr. Albert Levi ..............................................

Asst. Prof. Dr. Seher Tutdere ..............................................

A.Bassa

Assoc. Prof. Dr. Alp Bassa ..............................................

DATE OF APPROVAL: 25/04/2017

# ON LATTICES FROM FUNCTION FIELDS

Leyla Ateş

Mathematics, PhD Thesis, 2017

Thesis Supervisor: Prof. Dr. Cem Güneri

Thesis Co-supervisor: Prof. Dr. Henning Stichtenoth

Keywords: function field lattices, well-roundedness, kissing number

## Abstract

In this thesis, we study the lattices $\Lambda_{\mathcal{P}}$ associated to a function field $F/\mathbb{F}_q$ and a subset $\mathcal{P} \subseteq \mathbb{P}(F)$, which are the so-called function field lattices. We mainly explore the well-roundedness property of $\Lambda_{\mathcal{P}}$.

In previous papers, $\mathcal{P}$ is always chosen to be the set of all rational places of $F$. We extend the definition of function field lattices to the case where $\mathcal{P}$ may contain places of any degree. We investigate the basic properties of $\Lambda_{\mathcal{P}}$ such as rank, determinant, minimum distance and kissing number.

It is well-known that lattices from elliptic or Hermitian function fields are well-rounded. We show that, in contrast, well-roundedness does not hold for lattices associated to a large class of function fields, including hyperelliptic function fields.

# FONKSİYON CİSİMLERİNDEN ELDE EDİLEN LATİSLER ÜZERİNE

Leyla Ateş

Matematik, Doktora Tezi, 2017

Tez Danışmanı: Prof. Dr. Cem Güneri

Tez Yardımcı Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: fonksiyon cismi latisleri, lineer bağımsız ve minimal vektörler, minimal vektör sayısı

## Özet

Bu tezde, bir fonksiyon cismi $F/\mathbb{F}_q$ ve yerlerinin altkümesi $\mathcal{P} \subseteq \mathbb{P}(F)$ kullanılarak oluşturulan latisler, $\Lambda_{\mathcal{P}}$, çalışıldı. Fonksiyon cismi latisleri olarak anılan bu latislerin, minimal vektörlerinin gerdiği alt latisin mertebesiyle ilgilenildi.

Daha önceki çalışmalarda $\mathcal{P}$ kümesi $F$'in derecesi 1 olan yerlerinden oluşuyordu. Biz fonksiyon cismi latislerinin tanımını $\mathcal{P}$'nin herhangi bir derecedeki yeri içermesi durumuna genişlettik. Bu tanıma göre, fonksiyon cismi latislerinin mertebe, determinant, minimum uzaklık, minimal vektör sayısı gibi bazı temel özelliklerini inceledik.

Eliptik ya da Hermitian fonksiyon cisimlerinden elde edilen latislerin minimal vektörlerinin gerdiği alt latisin mertebesi tamdır. Ancak, hipereliptik fonksiyon cisimlerini de içeren, geniş bir fonksiyon cismi sınıfı ile ilişkili latislerin bu özelliği taşımadığını gösterdik.

*To my parents Meryem&Selim Parlar*
*and my husband İbrahim*

# Acknowledgments

In the first place, I gratefully acknowledge Prof. Dr. Henning Stichtenoth for being a tremendous mentor for me throughout my graduate study. Without his supervision and invaluable guidance, this Ph.D. would not have been achievable.

I would also like to express my sincere gratitude to my thesis advisor Prof. Dr. Cem Güneri.

I would like to thank all my friends in Sabancı University, especially Funda Özdemir, Selcen Sayıcı, Burçin Güneş, Dilek Çakıroğlu and Gamze Kuruk for all the moments that we shared.

I am thankful to my primary school teacher Nafiye Çınar, who sparked my interest in mathematics and encouraged me to learn more about it.

I am deeply grateful to my parents, Meryem and Selim Parlar, and my sisters, Betül and Neslihan, for their endless love and care. They have built up a warm family full of love and laughter.

Last, but certainly not least, I would like to give my sincere thanks to my husband İbrahim. Without his love, support and understanding, I would not have been able to overcome the difficulties of the graduate school and my personal life.

This work has been supported by the Science Fellowships and Grant Programs Department (BİDEB) of the Scientific and Technological Research Council of Turkey (TÜBİTAK), under the National Scholarship Program for PhD Students (2211-A).

# Table of Contents

# CHAPTER 1

## Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements and $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. In this thesis, we study lattices from function fields over $\mathbb{F}_q$ by focusing on the well-roundedness property.

Around 1990, M.Y. Rosenbloom and M.A. Tsfasman [10], and independently H.-G. Quebbemann [9] introduced the notion of a function field lattice. They used function field lattices in order to obtain asymptotically dense lattice sphere packings. It was proven that asymptotically good towers of function fields give rise to asymptotically dense families of lattice sphere packings.

Recently, function field lattices have been studied in terms of well-roundedness property ( a lattice is well-rounded if its minimal vectors generate a sublattice of full rank). In 2014, L. Fukshansky and H. Maharaj [5] proved that lattices from elliptic function fields over $\mathbb{F}_q$ are generated by their minimal vectors (with one exceptional case). M. Sha [11], in 2015, improved this result by showing that lattices from elliptic function fields over $\mathbb{F}_q$ have a basis consisting of minimal vectors (with one exceptional case). Lattices from Hermitian function fields over $\mathbb{F}_q$ are also found to be generated by their minimal vectors by Böttcher et al. [3], in 2016. These results imply that lattices from elliptic and Hermitian function fields over $\mathbb{F}_q$ are well-rounded.

In this thesis, we seek an answer to the question whether being well-rounded is a typical feature of function field lattices. While answering this question, we deal with function field lattices which are constructed in a more general way than the ones in the literature. That is to say, in the construction we make use of any subsets of the set of places of $F$, rather than only the set of all rational places.

Denote the set of places of $F$ by $\mathbb{P}(F)$.

The organization of this thesis is as follows:

In Chapter 2, after fixing some notations that we use throughout the thesis, we define lattices $\Lambda_{\mathcal{P}}$ associated to $F$ and $\mathcal{P} \subseteq \mathbb{P}(F)$, and give some parameters of them. As a preliminary step, we present some results from the literature on function field lattices.

In Chapter 3, we consider the lattice $\Lambda_{\mathcal{P}}$ from a function field $F/\mathbb{F}_q$ with gonality $\gamma(F) = \gamma$. The minimum distance $d(\Lambda_{\mathcal{P}})$ always satisfies the inequality

$$d(\Lambda_{\mathcal{P}}) \geq \sqrt{2\gamma},$$

and we focus on the case where this lower bound is attained, i.e. $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. We determine sufficient conditions on $F$ and $\mathcal{P} \subseteq \mathbb{P}(F)$ to ensure that the lattice $\Lambda_{\mathcal{P}}$ is not well-rounded. We find the rank of the sublattice generated by the minimal vectors of $\Lambda_{\mathcal{P}}$. We also give a formula for the kissing number of $\Lambda_{\mathcal{P}}$.

In Chapter 4, we investigate the well-roundedness property of the lattices from a hyperelliptic function field $F/\mathbb{F}_q$. For a specific subset $\mathcal{Q} \subseteq \mathbb{P}(F)$, we show that the lattice $\Lambda_{\mathcal{Q}}$ is well-rounded. We classify the situations in which the lattice $\Lambda_{\mathcal{Q}}$ is generated by its minimal vectors.

In Chapter 5, we give some examples illustrating the results obtained in the previous chapters.

# CHAPTER 2

# Preliminaries

## 2.1. Basic Concepts of Function Fields and Lattices

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is a power of a prime number, and $F/\mathbb{F}_q$ be a function field of one variable over $\mathbb{F}_q$. As a general reference for function fields, see [14]. Throughout this thesis, we assume that $\mathbb{F}_q$ is algebraically closed in $F$.

Let us use the following notations.

- $g = g(F)$ and $\mathbb{P}(F)$ are the *genus* of $F$ and the *set of places* of $F$, respectively.
- $N(F)$ is the *number of rational places* (places of degree one) of $F$ and $\mathbb{P}^1(F)$ is the *set of rational places* of $F$.
- $h := |\mathrm{Cl}^0(F)| = |\mathrm{Div}^0(F)/\mathrm{Princ}(F)|$ is the *class number* of $F$, where $\mathrm{Div}^0(F)$ is the group of *divisors of degree zero* and $\mathrm{Princ}(F)$ is the group of *principal divisors* of $F$.
- $\mathcal{L}(D)$ is the *Riemann-Roch space* associated to the divisor $D$.
- $\mathrm{supp}(D)$ and $\deg(D)$ are the *support* and the *degree* of a divisor $D$, respectively.
- $v_P$ is the *discrete valuation* of $F/\mathbb{F}_q$ associated to the place $P$.
- For a nonzero element $z \in F$, $(z) := (z)_0 - (z)_\infty$ is the *principal divisor* of $z$, where $(z)_0$ and $(z)_\infty$ are the *zero divisor* and the *pole divisor* of $z$, respectively.

- For a nonzero element $z \in F \setminus \mathbb{F}_q$, the *degree* of $z$ is

$$\deg(z) := \deg((z)_0) = \deg((z)_\infty) = \frac{1}{2} \sum_{P \in \mathbb{P}(\mathbb{F})} |v_P(z)| \deg P = [F : \mathbb{F}_q(z)].$$

- $\gamma = \gamma(F) := \min\{[F : E] : E \text{ is a rational subfield, } \mathbb{F}_q \subset E \subset F\}$ is the *gonality* of $F$.

- In the rational function field $\mathbb{F}_q(z)$, the rational places

  $(z = \alpha)$ denotes the zero of $z - \alpha \in \mathbb{F}_q[z]$ and

  $(z = \infty)$ denotes the pole of $z$.

- For an algebraic extension $F'/\mathbb{F}_{q'}$ of $F/\mathbb{F}_q$, if $P'|P$, i.e. $P' \in \mathbb{P}(F')$ lies over $P \in \mathbb{P}(F)$, denote by

  $e(P'|P)$ the *ramification index* of $P'$ over $P$ and

  $f(P'|P)$ the *relative degree* of $P'$ over $P$.

Now, let us define a lattice in $\mathbb{R}^n$ and some important notions about lattices. For detailed information about lattices, see [4].

- A $\mathbb{Z}$-module $L = \bigoplus_{i=1}^{k} \mathbb{Z}\gamma_i \subseteq \mathbb{R}^n$ is a called a *lattice* if the vectors $\gamma_1, \ldots, \gamma_k \in \mathbb{R}^n$ are linearly independent over $\mathbb{R}$.

- Equivalently, lattices can be described as discrete subgroups of $\mathbb{R}^n$.

- By using the definition above, we say that the *rank* of $L$ is $k$ and $\{\gamma_1, \ldots, \gamma_k\}$ forms a *basis* for $L$. We write $\mathrm{rank}(L) = k$.

- If $\{\gamma_1, \ldots, \gamma_k\}$ is a basis for $L$, then the $k \times n$ matrix $B$ whose $i^{\text{th}}$ row vector is $\gamma_i \in \mathbb{R}^n$, is called a *basis matrix.*

- Associated to the basis matrix $B$, the *fundamental parallelotope* of $L$ is defined as the set of points

$$P(B) = \Big\{ \sum_{i=1}^{k} x_i \gamma_i : x_i \in \mathbb{R} \text{ and } 0 \leq x_i < 1 \Big\} \subseteq \mathbb{R}^n.$$

- $\det(L)$ is the $k$-dimensional volume of $P(B)$ for a basis matrix $B$ of $L$.

- $\det(L)$ does not depend on the choice of $B$ and it can be calculated by the formula $\det(L) := \sqrt{\det BB^{\mathrm{T}}}$ for any basis matrix $B$ of $L$.

- The *length* of a vector $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ is given by

$$\|v\| := \sqrt{v_1^2 + \cdots + v_n^2}.$$

- The *minimum distance* of $L$ is defined as

$$d(L) := \min\{\|v\| : v \neq 0, v \in L\}$$

- $S(L) := \{v \in L : \|v\| = d(L)\}$ is the *set of minimal vectors* in $L$. The number of elements of $S(L)$ is called the *kissing number* of $L$, which is denoted by $\kappa(L)$.

- The *sphere packing problem* in $\mathbb{R}^n$ is to find out how densely identical spheres can be packed in $n$-dimensional space.

- The arrangement of open spheres of radius $d(L)/2$, which are centered at the points of a lattice $L$, is called the *lattice (sphere) packing* associated to $L$.

- In this packing, the number of spheres that touch a given one is equal to the number of minimal vectors of $L$. From this, the term kissing number originates.

- The *sphere packing density* $\Delta(L)$ of a lattice packing is the proportion of the space that is occupied by the spheres. Thus,

$$\Delta(L) = \frac{\text{volume of one sphere}}{\text{volume of a fundamental parallelotope}} = \frac{d(L)^k V_k}{2^k \det(L)},$$

  where $V_k$ is the volume of the $k$-dimensional unit sphere.

- A lattice $L$ is said to be *well-rounded* if the set $S(L)$ contains $k$ linearly independent vectors over $\mathbb{R}$. Well-roundedness will play an important role in this thesis.

- $S(L)$ generates a sublattice $L' := \text{span}_{\mathbb{Z}} S(L)$ in $L$.

- $L$ is said to be *generated by its minimal vectors* if $L' = L$.

- Clearly, if $L' = L$, then $L$ is well-rounded. However, the converse does not hold in general.

We illustrate the above notions by an example:

**Example 2.1.1** *$A_{n-1}$ denotes the following lattice*

$$\left\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i = 0\right\}.$$

*Let us list some important properties of this lattice.*

**(i)** *The vectors $b_i := (1, 0, \ldots, 0, -1, 0, \ldots, 0)$, where $-1$ is positioned at the $i$-th coordinate for $i = 2, \ldots, n$, form a basis for $A_{n-1}$. Thus,*

$$\text{rank}(A_{n-1}) = n - 1.$$

**(ii)** *Let $B$ be the basis matrix of $A_{n-1}$ associated to the basis $\{b_2, \ldots, b_n\}$. Then the determinant of $A_{n-1}$ is*

$$\det(A_{n-1}) = \sqrt{\det(BB^T)} = \begin{vmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{vmatrix}^{1/2} = \sqrt{n}, \tag{2.1}$$

*as the size of the matrix in Equation* (2.1) *is* $(n-1) \times (n-1)$.

**(iii)** *The minimal vectors of $A_{n-1}$ have the form $\pm(0, \ldots, 0, 1, 0, \ldots, 0, -1, 0, \ldots, 0)$. Thus, the minimum distance in $A_{n-1}$ is*

$$d(A_{n-1}) = \sqrt{1^2 + (-1)^2} = \sqrt{2},$$

*and the kissing number of $A_{n-1}$ is*

$$\kappa(A_{n-1}) = 2 \cdot \binom{n}{2} = n(n-1).$$

**(iv)** *Since the vectors $b_i$ have length $\|b_i\| = \sqrt{2}$, $A_{n-1}$ has a basis consisting of its minimal vectors. Hence, it is well-rounded.*

## 2.2. Function Field Lattices

Let $F$ be a function field over $\mathbb{F}_q$ with genus $g(F) = g$. We fix an $n$-tuple

$$\mathcal{P} = (P_1, \ldots, P_n)$$

of $n$ distinct places $P_i \in \mathbb{P}(F)$. By abuse of notation, we will also consider $\mathcal{P}$ as a subset of $\mathbb{P}(F)$, i.e. $\mathcal{P} \subseteq \mathbb{P}(F)$. Often, $\mathcal{P}$ will consist of all rational places of $F$. In order to avoid trivial cases, we will always assume that $n \geq 2$. Define the set

$$\mathcal{O}_{\mathcal{P}}^* := \{0 \neq z \in F \mid \operatorname{supp}(z) \subseteq \mathcal{P}\},$$

which is an abelian group with respect to multiplication. Consider the map

$$\phi_{\mathcal{P}} : \begin{cases} \mathcal{O}_{\mathcal{P}}^* & \to \mathbb{R}^n \\ z & \mapsto \big(v_{P_1}(z) \cdot \deg P_1, \ldots, v_{P_n}(z) \cdot \deg P_n\big), \end{cases}$$

and define

$$\Lambda_{\mathcal{P}} := \operatorname{Image}(\phi_{\mathcal{P}}).$$

**Definition 2.2.1** $\Lambda_{\mathcal{P}}$ *is called the* function field lattice *associated to* $F$ *and* $\mathcal{P}$.

Let us fix some notations that we use throughout this thesis. For $\mathcal{P} = (P_1, \ldots, P_n)$, we say that $P_i$ is an element of $\mathcal{P}$, $P_i \in \mathcal{P}$, where $i = 1, \ldots, n$. For $z \in \mathcal{O}_{\mathcal{P}}^*$, we sometimes identify the principal divisor $(z)$ with its image $\phi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$. In addition, we define the *length* of $z$ as the length of $\phi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ and denote this length by

$$\|z\| := \|\phi_{\mathcal{P}}(z)\|.$$

We recall that a lattice $L \subseteq \mathbb{R}^n$ is called *even*, if $\|v\|^2$ is an even integer for any vector $v$ in $L$ .

In Proposition 2.2.1 and Proposition 2.2.2, we state some basic facts about the parameters of function field lattices.

**Proposition 2.2.1**

**(i)** *For all* $z \in \mathcal{O}_{\mathcal{P}}^*$, $\|z\|^2 \equiv 0 \bmod 2$, *i.e.* $\Lambda_{\mathcal{P}}$ *is an even lattice.*

**(ii)** *Let* $z \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q$. *Then* $\|z\| \geq \sqrt{2\deg(z)}$, *where equality holds if and only if the zero and the pole of* $z$ *in* $\mathbb{F}_q(z)$ *split completely in the extension* $F/\mathbb{F}_q(z)$.

**(iii)** *The minimum distance* $d(\Lambda_{\mathcal{P}})$ *satisfies* $d(\Lambda_{\mathcal{P}}) \geq \sqrt{2\gamma}$, *where* $\gamma$ *is the gonality of* $F$.

**Proof**:

**(i)** Take $z \in \mathcal{O}_{\mathcal{P}}^*$ and let $z$ have the principal divisor

$$(z) = a_1P_1 + \cdots + a_nP_n, \quad a_i \in \mathbb{Z}, \quad i = 1, \ldots, n.$$

The square of the length of $z$ is

$$\begin{aligned}\|z\|^2 &= a_1^2\deg(P_1)^2 + \cdots + a_n^2\deg(P_n)^2 \\ &\equiv a_1\deg(P_1) + \cdots + a_n\deg(P_n) \bmod 2, \quad \text{as } c^2 \equiv c \bmod 2 \quad \forall c \in \mathbb{Z} \\ &\equiv 0 \bmod 2, \text{ as the degree of any principal divisor is equal to zero.}\end{aligned}$$

**(ii)** Since $z \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q$, the degree $[F : \mathbb{F}_q(z)] = \deg(z)$ is finite. Let the zero and the pole divisor of $z$ be

$$\begin{aligned}(z)_0 =& b_1Q_1 + \cdots + b_sQ_s \\ (z)_\infty =& c_1R_1 + \cdots + c_tR_t, \text{ respectively,}\end{aligned}$$

where $Q_i, R_j$ are distinct places in $\mathcal{P}$, $b_i, c_j \in \mathbb{Z}^{>0}$ for $i = 1, \ldots, s$ and $j = 1, \ldots, t$. Then,

$$\begin{aligned} \|z\|^2 &= \sum_{i=1}^{s} b_i^2 \mathrm{deg}(Q_i)^2 + \sum_{j=1}^{t} c_j^2 \mathrm{deg}(R_j)^2 \\ &\geq \sum_{i=1}^{s} b_i \mathrm{deg}(Q_i) + \sum_{j=1}^{t} c_j \mathrm{deg}(R_j) \\ &= 2\mathrm{deg}(z). \end{aligned}$$

Equality holds if and only if

$$b_i = c_j = 1 \quad \text{and} \quad \mathrm{deg}(Q_i) = \mathrm{deg}(R_j) = 1,$$

for all $i, j$, which proves that the zero and the pole of $z$ in $\mathbb{F}_q(z)$ split completely in the extension $F/\mathbb{F}_q(z)$.

**(iii)** As $\gamma \leq \mathrm{deg}(z)$ for all $z \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q$, the result follows from part (ii).

□

**Proposition 2.2.2** *Let $d_i := \mathrm{deg} P_i$ for $i = 1, \ldots, n$, and $k$ be the greatest common divisor of $d_1, \ldots, d_n$. Let $h$ be the class number of $F$. Then the following hold:*

**(i)** *$\Lambda_{\mathcal{P}}$ is a sublattice of the lattice $A_{n-1}$.*

**(ii)** *The rank of $\Lambda_{\mathcal{P}}$ is equal to* $\mathrm{rank}(\Lambda_{\mathcal{P}}) = n - 1$.

**(iii)** *The index $(A_{n-1} : \Lambda_{\mathcal{P}})$ is given by*

$$(A_{n-1} : \Lambda_{\mathcal{P}}) = \frac{d_1 d_2 \cdots d_n}{k} \cdot h_0,$$

*where $h_0$ is a positive integer that divides $h$.*

**(iv)** *The determinant of $\Lambda_{\mathcal{P}}$ is given by*

$$\det(\Lambda_{\mathcal{P}}) = \sqrt{n} \cdot \frac{d_1 d_2 \cdots d_n}{k} \cdot h_0,$$

*where $h_0$ is a positive integer that divides $h$.*

**Proof**:

**(i)** The result follows from the fact that any principal divisor has degree zero.

**(ii)** Since the divisors $d_iP_1 - d_1P_i$ of $F$ have degree zero for $i = 2, \ldots, n$, we get

$$h \cdot (d_iP_1 - d_1P_i) \in \operatorname{Princ}(F),$$

as $h = \big(\operatorname{Div}^0(F) : \operatorname{Princ}(F)\big)$ is the class number of $F$. Corresponding to these principal divisors, the vectors

$$\begin{array}{llllll}
\big(hd_2d_1, & -hd_1d_2, & 0 & ,0, \ldots, & 0 & \big), \\
\big(hd_3d_1, & 0 & ,-hd_1d_3, & 0, \ldots, & 0 & \big), \\
\ \vdots & & & \ddots & & \\
\big(hd_nd_1, & 0 & , \quad 0 & , \ldots, 0, & -hd_1d_n\big) &
\end{array}$$

are contained in $\Lambda_{\mathcal{P}}$. These vectors provide $n-1$ linearly independent lattice vectors over $\mathbb{R}$. By (i), $\operatorname{rank}(\Lambda_{\mathcal{P}}) \leq \operatorname{rank}(A_{n-1}) = n-1$. Hence, $\operatorname{rank}(\Lambda_{\mathcal{P}}) = n-1$.

**(iii)** Note that the index $(A_{n-1} : \Lambda_{\mathcal{P}})$ is finite since $A_{n-1}$ and $\Lambda_{\mathcal{P}}$ have the same rank by part (ii).

Define the sublattices $B \subseteq A_{n-1}$ and $C \subseteq \mathbb{Z}^n$ as

$$B := \Big\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_i \equiv 0 \bmod d_i, i = 1, \ldots, n, \ \sum_{i=1}^{n} x_i = 0\Big\} \text{ and}$$

$$C := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_i \equiv 0 \bmod d_i, i = 1, \ldots, n\}.$$

**Step 1:** Calculate the index $(A_{n-1} : B)$.

By the second isomorphism theorem for modules,

$$(A_{n-1} : B) = \Big|A_{n-1}\Big/(A_{n-1} \cap C)\Big| = \Big|(A_{n-1} + C)\Big/C\Big| \tag{2.2}$$

as

$$B = A_{n-1} \cap C.$$

Since we have the inclusion

$$C \subseteq (A_{n-1} + C) \subseteq \mathbb{Z}^n \text{ and}$$

the index of $C$ in $\mathbb{Z}^n$ is equal to

$$\big(\mathbb{Z}^n : C\big) = d_1d_2 \cdots d_n, \tag{2.3}$$

we focus on computing the index $\big(\mathbb{Z}^n : (A_{n-1} + C)\big)$.

Let $\tau$ be the homomorphism defined as

$$\tau : \begin{cases} \mathbb{Z}^n & \to \mathbb{Z}/k\mathbb{Z} \\ (x_1, \ldots, x_n) & \mapsto (x_1 + \cdots + x_n) \bmod k. \end{cases}$$

**Step 1.a:** Show that the kernel of $\tau$ is $\operatorname{Ker}(\tau) = A_{n-1} + C$ to find the index $\big(\mathbb{Z}^n : (A_{n-1} + C)\big)$.

Clearly, $A_{n-1}$ lies in the kernel of $\tau$. Let $(x_1, \ldots, x_n)$ be an element of $C$. Then

$$\begin{aligned} x_i \equiv 0 \bmod d_i &\Longrightarrow x_i \equiv 0 \bmod k \\ &\Longrightarrow \sum_{i=1}^{n} x_i \equiv 0 \bmod k \Longrightarrow C \subseteq \operatorname{Ker}(\tau). \end{aligned}$$

Hence $A_{n-1}+C$ is contained in the kernel of $\tau$. Conversely, assume that $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ satisfies the congruence relation

$$x_1 + \cdots + x_n \equiv 0 \bmod k.$$

Then

$$\begin{aligned} &x_1 + \cdots + x_n = rk \text{ for some } r \in \mathbb{Z} \text{ and} \\ &x_1 + \cdots + x_n = r(s_1 d_1 + \cdots + s_n d_n), \end{aligned}$$

where $s_1 d_1 + \cdots + s_n d_n = k$ for some $s_1, \ldots, s_n \in \mathbb{Z}$ as $k$ is the greatest common divisor of $d_1, \ldots, d_n$. Thus, an element $(x_1, \ldots, x_n)$ from the kernel of $\tau$ can be written as

$$(x_1, \ldots, x_n) = (x_1 - r s_1 d_1, \ldots, x_n - r s_n d_n) + (r s_1 d_1, \ldots, r s_n d_n),$$

which is the sum of two elements from $A_{n-1}$ and $C$. Therefore,

$$\operatorname{Ker}(\tau) = A_{n-1} + C$$

and, since $\tau$ is onto,

$$\big(\mathbb{Z}^n : (A_{n-1} + C)\big) = \big|\mathbb{Z}/k\mathbb{Z}\big| = k. \tag{2.4}$$

By Equations 2.2, 2.3 and 2.4, we obtain the index

$$\big(A_{n-1} : B\big) = \frac{d_1 d_2 \cdots d_n}{k}. \tag{2.5}$$

**Step 2:** Show that the index $h_0 := \big(B : \Lambda_{\mathcal{P}}\big)$ divides $h$.

Consider the group homomorphism

$$\sigma : \begin{cases} B & \to \mathrm{Div}^0(F)/\mathrm{Princ}(F) \\ (x_1, \dots, x_n) & \mapsto \frac{x_1}{d_1} P_1 + \dots + \frac{x_n}{d_n} P_n + \mathrm{Princ}(F). \end{cases}$$

The kernel of $\sigma$ satisfies

$$\begin{aligned} \mathrm{Ker}(\sigma) &= \Big\{ (x_1, \dots, x_n) \in B : \quad \frac{x_1}{d_1} P_1 + \dots + \frac{x_n}{d_n} P_n \in \mathrm{Princ}(F) \Big\} \\ &= \Big\{ (x_1, \dots, x_n) \in B : \quad \frac{x_1}{d_1} P_1 + \dots + \frac{x_n}{d_n} P_n = (z),\ z \in \mathcal{O}_{\mathcal{P}}^* \Big\} \\ &= \{ \phi_{\mathcal{P}}(z) : \ z \in \mathcal{O}_{\mathcal{P}}^* \} \\ &= \Lambda_{\mathcal{P}}. \end{aligned}$$

Hence the index $h_0$ divides the index $h = \big(\mathrm{Div}^0(F) : \mathrm{Princ}(F)\big)$.

Therefore, by Equation 2.5 we conclude that

$$\begin{aligned} \big(A_{n-1} : \Lambda_{\mathcal{P}}\big) &= \big(A_{n-1} : B\big) \cdot \big(B : \Lambda_{\mathcal{P}}\big) \\ &= \frac{d_1 d_2 \dots d_n}{k} \cdot h_0, \end{aligned}$$

where $h_0$ is a positive integer that divides $h$.

**(iv)** Since the index $\big(A_{n-1} : \Lambda_{\mathcal{P}}\big)$ is finite by part (iii), the following equality holds:

$$\begin{aligned} \det(\Lambda_{\mathcal{P}}) &= \det(A_{n-1}) \cdot \big(A_{n-1} : \Lambda_{\mathcal{P}}\big) \\ &= \sqrt{n} \cdot \big(A_{n-1} : \Lambda_{\mathcal{P}}\big), \quad \text{by Example 2.1.1} \\ &= \sqrt{n} \cdot \frac{d_1 d_2 \cdots d_n}{k} \cdot h_0, \end{aligned}$$

where $h_0$ is a positive integer that divides $h$ by part (iii).

□

## 2.3. Previous Results about Function Field Lattices

In this section, we give a brief overview over what is known about function field lattices.

### 2.3.1. Lattices from Rational Function Fields

Let $F := \mathbb{F}_q(z)$ be a rational function field over $\mathbb{F}_q$. Consider an $n$-tuple

$$\mathcal{P} = (P_1, \ldots, P_{n-1}, P_\infty),$$

where $P_\infty$ is the pole of $z$ and $P_i$ is the place whose prime element is the monic irreducible polynomial $p_i(z) \in \mathbb{F}_q[z]$, for $i = 1, \ldots, n-1$. Let

$$\deg(P_i) = \deg\,(p_i(z)) =: d_i \text{ for all } i.$$

Then, the vectors

$$\phi_{\mathcal{P}}(p_i(z)) = (0, \ldots, 0, d_i, 0, \ldots, 0, -d_i) \in \Lambda_{\mathcal{P}}$$

have length

$$\|p_i(z)\| = d_i\sqrt{2}.$$

**Special Case:** Assume that all places $P_1, \ldots, P_{n-1}$ are rational places (different from $P_\infty$) of $\mathbb{F}_q(z)$ with the prime elements $z - \alpha_1, \ldots, z - \alpha_{n-1}$, respectively ($\alpha_i \in \mathbb{F}_q$). Then the vectors

$$\begin{aligned}
\phi_{\mathcal{P}}(z - \alpha_1) &= (1, 0, 0, \ldots, 0, -1), \\
\phi_{\mathcal{P}}(z - \alpha_2) &= (0, 1, 0, \ldots, 0, -1), \\
&\vdots \\
\phi_{\mathcal{P}}(z - \alpha_{n-1}) &= (0, 0, \ldots, 0, 1, -1)
\end{aligned}$$

are in $\Lambda_{\mathcal{P}}$. Since these vectors generate the lattice $A_{n-1}$, we conclude that

$$\Lambda_{\mathcal{P}} = A_{n-1}.$$

Now we can state the following result about lattices from rational function fields.

**Theorem 2.3.3** *Assume that $F$ is a rational function field over $\mathbb{F}_q$ and the $n$-tuple $\mathcal{P}$ contains at least two rational places of $F$. Then the lattice $\Lambda_{\mathcal{P}}$ is well-rounded if and only if $\mathcal{P}$ contains only rational places.*

**Proof**: Let $\mathcal{P} = (P_1, \ldots, P_n)$, with $P_1, P_2 \in \mathbb{P}^1(F)$. By using the prime elements of $P_1$ and $P_2$, one can obtain vectors in $\Lambda_{\mathcal{P}}$ of the form

$$\pm(1, -1, 0, \ldots, 0),$$

which have length $\sqrt{2}$. Since this is the smallest possible non-zero length in $\Lambda_{\mathcal{P}}$, the minimum distance in $\Lambda_{\mathcal{P}}$ is

$$d(\Lambda_{\mathcal{P}}) = \sqrt{2}.$$

Assume that $\Lambda_{\mathcal{P}}$ is well-rounded. Then there exist vectors $v_1, \ldots, v_{n-1}$ in $\Lambda_{\mathcal{P}}$ which are linearly independent over $\mathbb{R}$ and of the minimum length in $\Lambda_{\mathcal{P}}$, as $\operatorname{rank}(\Lambda_{\mathcal{P}}) = n-1$. Suppose that, without loss of generality, the degree of $P_n$ is greater than 1. Since the vectors $v_i$ have length $\|v_i\| = \sqrt{2}$, there must be 0 in their $n$-th components. Then the vectors $v_1, \ldots, v_{n-1}$ cannot be linearly independent. Therefore, $\mathcal{P}$ contains only rational places.

Assume that $P_1, \ldots, P_n$ are all rational. Then, as explained in the special case above, $\Lambda_{\mathcal{P}} = A_{n-1}$. Hence it is well rounded, by Example 2.1.1.

□

### 2.3.2. Lattices from Elliptic Function Fields

Lattices from elliptic function fields have been studied in detail in [5] and [11]. We compile their main results in Theorem 2.3.4 below.

Recall that a function field $F/\mathbb{F}_q$ is called elliptic, if it has genus $g = 1$. We fix a rational place $Q_\infty$ of $F/\mathbb{F}_q$ (its existence follows from the Hasse-Weil Bound, see [14, Theorem 5.2.3]). Then the set

$$\mathcal{P} = \mathbb{P}^1(F)$$

of all rational places of $F$ carries the structure of an abelian group $(\mathcal{P}, \oplus, Q_\infty)$ where $Q_\infty$ is the neutral element of $\mathcal{P}$, see [12].

**Theorem 2.3.4** *(See [5], [11].) Let $F/\mathbb{F}_q$ be an elliptic function field and*

$$\mathcal{P} = \mathbb{P}^1(F) = (P_1, \ldots, P_{n-1}, P_n = Q_\infty).$$

*Assume that $n \geq 4$. Then the function field lattice $\Lambda_{\mathcal{P}}$ has the following properties:*

**(i)** *The minimal length of $\Lambda_{\mathcal{P}}$ is $d(\Lambda_{\mathcal{P}}) = 2$.*

**(ii)** *The minimal vectors of $\Lambda_{\mathcal{P}}$ are exactly the vectors $P+Q-R-S$, where $P, Q, R, S \in \mathcal{P}$ are distinct and $P \oplus Q = R \oplus S$.*

**(iii)** *For $n \geq 5$, $\Lambda_{\mathcal{P}}$ has a basis of minimal vectors; in particular, $\Lambda_{\mathcal{P}}$ is well-rounded.*

**(iv)** *The determinant of $\Lambda_{\mathcal{P}}$ is $\det(\Lambda_{\mathcal{P}}) = n\sqrt{n}$.*

**(v)** *The kissing number of $\Lambda_{\mathcal{P}}$ is*

$$\kappa(\Lambda_{\mathcal{P}}) = \frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4} + \Big(n - \frac{n}{\epsilon}\Big) \cdot \frac{n(n-2)}{4},$$

*where $\epsilon$ is the number of 2-torsion rational points of $F$.*

Observe that the structure of $\Lambda_{\mathcal{P}}$ is also known for $n \leq 4$, see [11]. We remark that lattices from elliptic function fields attain the lower bound $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$, where $\gamma = 2$ is the gonality of $F$. (See Proposition 2.2.1(iii).)

The proof of Theorem 2.3.4 is rather long. Its principal tool is the following observation which describes the generators of $\Lambda_{\mathcal{P}}$ in terms of the group structure $\oplus$.

**Lemma 2.3.5** *(See [5, Theorem 2.3].) ($g = 1, \mathcal{P} = \mathbb{P}^1(F), n \geq 4$) The lattice $\Lambda_{\mathcal{P}}$ is generated by vectors of the form*

$$P + Q - R - Q_\infty \text{ such that } P \oplus Q = R,$$

*where $P, Q, R \in \mathcal{P}$ and $Q_\infty$ is the neutral element of $\mathcal{P}$.*

### 2.3.3. Lattices from Hermitian Function Fields

Let $q := \ell^2$ and $H := \mathbb{F}_q(x, y)$ be the Hermitian function field with the defining equation

$$y^\ell + y = x^{\ell+1}$$

over $\mathbb{F}_q$. Recall that the genus, the gonality and the number of rational places of $H$ are given by $g(H) = \ell(\ell-1)/2$, $\gamma(H) = \ell$ and $|\mathbb{P}^1(H)| = \ell^3 + 1$, respectively.

In the following theorem, we assemble some results of [3].

**Theorem 2.3.6** *(See [3].) Let $H/\mathbb{F}_q$ be the Hermitian function field and $\mathcal{P} = \mathbb{P}^1(H)$. Then the function field lattice $\Lambda_{\mathcal{P}}$ has the following properties:*

**(i)** *The minimal length of $\Lambda_{\mathcal{P}}$ is $d(\Lambda_{\mathcal{P}}) = \sqrt{2\ell}$.*

**(ii)** *$\Lambda_{\mathcal{P}}$ is generated by its minimal vectors. Hence, it is well-rounded.*

**(iii)** *The determinant of $\Lambda_{\mathcal{P}}$ is $\det(\Lambda_{\mathcal{P}}) = \sqrt{\ell^3+1}(\ell+1)^{\ell^2-\ell}$.*

**(iv)** *The kissing number of $\Lambda_{\mathcal{P}}$ satisfies $\kappa(\Lambda_{\mathcal{P}}) \geq \ell^7 - \ell^5 + \ell^4 - \ell^2$.*

Note that, like lattices from elliptic function fields, lattices from Hermitian ones also attain the lower bound $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma(H)} = \sqrt{2\ell}$.

The proof of Theorem 2.3.6 is essentially based on the following fact, which provides a set of generators for $\Lambda_{\mathcal{P}}$.

**Lemma 2.3.7** *(See [7, Corollary 7.5].) ($H = \mathbb{F}_q(x,y)$ is Hermitian, $\mathcal{P} = \mathbb{P}^1(H)$) Every function in $\mathcal{O}^*_{\mathcal{P}}$ is the product of functions of the form $ax + by + c$ and their inverses ($a, b, c \in \mathbb{F}_q$).*

## CHAPTER 3

# A Class of Function Field Lattices which are not Well-rounded

As we noted in the previous section, lattices from elliptic and Hermitian function fields are found to be well-rounded for a suitable choice of $\mathcal{P}$. These results lead to a natural question whether being well-rounded is a typical property of all function field lattices. In this chapter, we answer this question negatively by presenting a class of function fields providing lattices which fail to be well-rounded.

Recall our notations that $F/\mathbb{F}_q$ is a function field with $g(F) = g$ and $\gamma(F) = \gamma$, and $\mathcal{P}$ is an $n$-tuple of places of $F$; $\Lambda_{\mathcal{P}}$ is the function field lattice associated to $F$, $\|z\|$ is the length of the vector in the lattice associated to the element $z \in \mathcal{O}_{\mathcal{P}}^*$ and $d(\Lambda_{\mathcal{P}})$ is the minimum distance in $\Lambda_{\mathcal{P}}$.

## 3.1. Function Fields with 'Short' Lattice Vectors

We showed that the minimum distance in $\Lambda_{\mathcal{P}}$ satisfies $d(\Lambda_{\mathcal{P}}) \geq \sqrt{2\gamma}$, see Proposition 2.2.1. The lattices from elliptic and Hermitian function fields attain this lower bound and they are well-rounded. (See Theorem 2.3.4 and Theorem 2.3.6.) Below, we give a characterization of function fields $F/\mathbb{F}_q$ where

$$d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}, \tag{3.1}$$

for an appropriate $n$-tuple $\mathcal{P}$.

In the next sections, we describe some function fields such that Equation (3.1) holds but $\Lambda_{\mathcal{P}}$ is not well-rounded (opposite to the lattices from elliptic and Hermitian function fields).

Let us initially determine the elements $z \in \mathcal{O}_{\mathcal{P}}^*$ with length $\|z\| = \sqrt{2\gamma}$.

**Proposition 3.1.1** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$ and $\mathcal{P} \subseteq \mathbb{P}(F)$. Let $z \in \mathcal{O}_{\mathcal{P}}{}^* \setminus \mathbb{F}_q$. Then, $||z|| = \sqrt{2\gamma}$ if and only if the following conditions hold:*

**(i)** *$[F : \mathbb{F}_q(z)] = \gamma$, and*

**(ii)** *the zero and the pole of $z$ in $\mathbb{F}_q(z)$ split completely in the extension $F/\mathbb{F}_q(z)$.*

Proposition 3.1.1 follows immediately from Proposition 2.2.1(ii).

Let $E$ be a rational subfield of $F$ with $[F : E] = \gamma$ and $P$ be a rational place of $E$. Define the following conditions:

$$P \text{ splits completely in the extension } F/E, \text{ and} \tag{1}$$

$$\text{for all } P' \in \mathbb{P}^1(F) \text{ with } P' \text{ lying over } P, \text{ the tuple } \mathcal{P} \text{ contains } P'. \tag{2}$$

The next corollary characterizes the function fields satisfying Equation (3.1).

**Corollary 3.1.2** *For a function field $F$ over $\mathbb{F}_q$ with $\gamma(F) = \gamma$ and $\mathcal{P} \subseteq \mathbb{P}(F)$, the following are equivalent:*

**(i)** *$d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$.*

**(ii)** *There exists a rational subfield $E \subseteq F$ with $[F : E] = \gamma$ such that the number of rational places of $E$ satisfying conditions* (1) *and* (2) *is at least two.*

**Proof**: Assume that there is an element $z \in \mathcal{O}_{\mathcal{P}}^*$ with $\|z\| = \sqrt{2\gamma}$. Let $E := \mathbb{F}_q(z)$. By Proposition 3.1.1, $[F : E] = \gamma$ and the rational places $(z = 0)$ and $(z = \infty)$ satisfy condition (1). As $z \in \mathcal{O}_{\mathcal{P}}^*$, these two places also satisfy condition (2).

Now assume the part (ii). Let $P$ and $Q$ be distinct rational places of $E$ for which conditions (1) and (2) hold. There is an element, say $z$, of $E$ such that the zero and the pole of $z$ in $E$ are $P$ and $Q$, respectively. From condition (1), $[F : \mathbb{F}_q(z)] = \gamma$; hence $E = \mathbb{F}_q(z)$. From condition (2), $z$ belongs to $\mathcal{O}_{\mathcal{P}}^*$. Then by Proposition 3.1.1, $z$ has length $\|z\| = \sqrt{2\gamma}$. Therefore, $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$.

□

### 3.2. $F/\mathbb{F}_q$ with a Unique Rational Subfield of Degree $\gamma(F)$

It is well-known that a hyperelliptic function field $F/\mathbb{F}_q$ has gonality $\gamma(F) = 2$, and there is a *unique* rational subfield $E \subseteq F$ with $[F : E] = 2$, see [14, Proposition 6.2.4].

This motivates us to consider function fields $F/\mathbb{F}_q$ which satisfy the following condition:

$$\text{There is a unique rational subfield } E \subseteq F \text{ with } [F : E] = \gamma(F). \tag{$*$}$$

Denote by $\Delta_{\mathcal{P}}$ the sublattice of $\Lambda_{\mathcal{P}}$ generated by the minimal vectors of $\Lambda_{\mathcal{P}}$. By definition, $\Lambda_{\mathcal{P}}$ is well-rounded if and only if

$$\operatorname{rank}(\Delta_{\mathcal{P}}) = \operatorname{rank}(\Lambda_{\mathcal{P}}).$$

In the next theorem, an expression for the rank of $\Delta_{\mathcal{P}}$ is given, when $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$ and condition $(*)$ holds.

Recall that if $E$ is a rational subfield of $F$ with $[F : E] = \gamma$, for a rational place $P$ of $E$, we define conditions (1) and (2) as follows:

$$P \text{ splits completely in the extension } F/E, \text{ and} \tag{1}$$

$$\text{for all } P' \in \mathbb{P}^1(F) \text{ with } P'|P, \text{ the place } P' \text{ belongs to } \mathcal{P}. \tag{2}$$

**Theorem 3.2.3** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$, $g(F) \geq 2$ and $\mathcal{P} \subseteq \mathbb{P}(F)$. Suppose that $F/\mathbb{F}_q$ satisfies condition $(*)$ and $\Lambda_{\mathcal{P}}$ has minimum distance $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Let $E \subseteq F$ be the unique rational subfield with $[F : E] = \gamma$ and consider the set*

$$S := \{P \in \mathbb{P}(E) : \deg(P) = 1 \textit{ and } P \textit{ satisfies conditions } (1) \textit{ and } (2)\}.$$

*Let $m := |S|$. Then the following hold:*

**(i)** $m \geq 2$.

**(ii)** $\operatorname{rank}(\Lambda_{\mathcal{P}}) \geq m\gamma - 1$.

**(iii)** *The vectors in $\Lambda_{\mathcal{P}}$ of minimal length span a sublattice of rank $m - 1$, i.e.,*

$$\operatorname{rank}(\Delta_{\mathcal{P}}) = m - 1.$$

**(iv)** *$\Lambda_{\mathcal{P}}$ is not well-rounded.*

**Proof**:

**(i)** Since $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$ and $E$ is the unique rational subfield with $[F : E] = \gamma$, the result directly follows from Corollary 3.1.2.

**(ii)** By Proposition 2.2.2,

$$\operatorname{rank}(\Lambda_{\mathcal{P}}) = |\mathcal{P}| - 1.$$

Since above every place $P \in S$ there are $\gamma$ rational places of $F$, all of which are contained in $\mathcal{P}$, the cardinality of $\mathcal{P}$ satisfies the inequality

$$|\mathcal{P}| \geq m\gamma.$$

Hence, $\operatorname{rank}(\Lambda_{\mathcal{P}}) \geq m\gamma - 1$.

**(iii)** Let $P \in S$ and $x \in E$ be such that $P$ is the pole of $x$ in $E$. Since $P$ splits completely in $F/E$, the degree of $F/\mathbb{F}_q(x)$ is $[F : \mathbb{F}_q(x)] = \gamma$, and thus $E = \mathbb{F}_q(x)$. Then $S$ can be expressed as

$$S = \{(x = \infty), (x = a_1), \dots, (x = a_{m-1})\},$$

where the elements $a_1, \dots, a_{m-1} \in \mathbb{F}_q$ are pairwise distinct. We claim:

**(a)** The elements $x - a_i$ belong to $\mathcal{O}_{\mathcal{P}}^*$, and the vectors $\phi_{\mathcal{P}}(x - a_i) \in \Lambda_{\mathcal{P}}$ are linearly independent of the minimal length $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$.

**(b)** Every minimal vector in $\Lambda_{\mathcal{P}}$ is a $\mathbb{Z}-$linear combination of $\phi_{\mathcal{P}}(x - a_i)$, $i = 1, \dots, m-1$.

**Proof of (a):** Since the elements of $S$ fulfill condition (1), the pole divisor of $x$ and the zero divisor of $x - a_i$ in $F$ are of the form

$$(x)_\infty = Q_1 + \dots + Q_\gamma \text{ and}$$

$$(x - a_i)_0 = P_1^{(i)} + \dots + P_\gamma^{(i)},$$

respectively, where $Q_j, P_k^{(i)}$ are pairwise distinct rational places in $\mathbb{P}^1(F)$. By condition (2), $Q_j, P_k^{(i)} \in \mathcal{P}$. Hence $x - a_i \in \mathcal{O}_{\mathcal{P}}^*$. Let $\mathcal{P}$ be the $n$-tuple

$$\mathcal{P} = (Q_1, \dots, Q_\gamma, P_1^{(1)}, \dots, P_\gamma^{(1)}, \dots, P_1^{(m-1)}, \dots, P_\gamma^{(m-1)}, \dots).$$

Then the vectors $\phi(x - a_i)$ have the form

$$(\underbrace{-1, \dots, -1}_{Q_j}, 0, \dots, 0, \underbrace{1, \dots, 1}_{P_k^{(i)}}, 0, \dots, 0).$$

These vectors have length $\sqrt{2\gamma}$, and they are obviously linearly independent.

**Proof of (b):** Let $z \in \mathcal{O}_{\mathcal{P}}{}^*$ with $||z|| = \sqrt{2\gamma}$, then $[F : \mathbb{F}_q(z)] = \gamma$ by Proposition 3.1.1. Thus $\mathbb{F}_q(z) = \mathbb{F}_q(x)$ by condition $(*)$. Therefore,

$$\text{either } z = \alpha x - \beta \text{ with } \alpha, \beta \in \mathbb{F}_q \text{ and } \alpha \neq 0 \text{ (case 1)},$$

$$\text{or } z = \frac{\alpha x - \beta}{x - \delta} \text{ with } \alpha, \beta, \delta \in \mathbb{F}_q \text{ and } \alpha\delta \neq \beta \text{ (case 2)}.$$

Again by Proposition 3.1.1, the zero and the pole of $z$ split completely in $F/\mathbb{F}_q(z)$. Since $z$ is an element of $\mathcal{O}_{\mathcal{P}}^*$, all places of $F$ lying over the zero or the pole of $z$ belong to $\mathcal{P}$. Thus, the zero and the pole of $z$ in $\mathbb{F}_q(z)$ are contained in the set $S$.

In case 1, we can assume that $z = x - \beta$ (since $\phi_{\mathcal{P}}(z) = \phi_{\mathcal{P}}(\alpha^{-1}z)$). It follows that $(x = \beta) \in S$. Hence,

$$\phi_{\mathcal{P}}(z) = \phi_{\mathcal{P}}(x - \beta) = \phi_{\mathcal{P}}(x - a_i) \tag{3.2}$$

for some $i \in \{1, \ldots, m-1\}$.

In case 2, we have to distinguish two subcases: $\alpha = 0$ or $\alpha \neq 0$. In the first subcase, we can assume that $z = 1/(x-\delta)$. Then $(x = \delta) \in S$. As above, we conclude that

$$\phi_{\mathcal{P}}(z) = -\phi_{\mathcal{P}}(x-\delta) = -\phi_{\mathcal{P}}(x-a_i) \tag{3.3}$$

for some $i \in \{1, \ldots, m-1\}$. In the second subcase, without loss of generality, $z = (x-\beta)/(x-\delta)$, and it follows $(x=\beta), (x=\delta) \in S$. Therefore,

$$\begin{aligned} \phi_{\mathcal{P}}(z) =& \phi_{\mathcal{P}}(x-\beta) - \phi_{\mathcal{P}}(x-\delta) \\ =& \phi_{\mathcal{P}}(x-a_j) - \phi_{\mathcal{P}}(x-a_i) \end{aligned} \tag{3.4}$$

for some $i \neq j \in \{1, \ldots, m-1\}$.

Consequently, the rank of $\Delta_{\mathcal{P}}$ is

$$\operatorname{rank}(\Delta_{\mathcal{P}}) = m-1.$$

**(iv)** As $g(F) \geq 2$, the gonality of $F$ is greater than 1. Then from parts (ii) and (iii),

$$\begin{aligned} \operatorname{rank}(\Lambda_{\mathcal{P}}) &\geq m\gamma - 1 \\ &> m-1 = \operatorname{rank}(\Delta_{\mathcal{P}}), \end{aligned}$$

which implies that $\Lambda_{\mathcal{P}}$ does not contain enough linearly independent minimal vectors to be well-rounded.

□

In the setting of Theorem 3.2.3, we find a formula for the kissing number of $\Lambda_{\mathcal{P}}$.

**Corollary 3.2.4** *Under the assumptions of Theorem 3.2.3, the kissing number of $\Lambda_{\mathcal{P}}$ is given by*

$$\kappa(\Lambda_{\mathcal{P}}) = m(m-1).$$

**Proof**: By the proof of Theorem 3.2.3(iii), we observed that if $z \in \mathcal{O}_{\mathcal{P}}^*$ gives a minimal vector in $\Lambda_{\mathcal{P}}$, then the vector $\phi_{\mathcal{P}}(z)$ must have one of the following forms (using the same notations as in the proof of the theorem):

- By the Equation (3.2), $\phi_{\mathcal{P}}(z) = \phi_{\mathcal{P}}(x-a_i)$, for $i = 1, \ldots, m-1$, which is the vector

  $$(\underbrace{-1, \ldots, -1}_{Q_j}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{P_k^{(i)}}, 0, \ldots, 0).$$

  There are $m-1$ vectors of this form.

- By the Equation (3.3), $\phi_{\mathcal{P}}(z) = -\phi_{\mathcal{P}}(x - a_i)$, for $i = 1, \ldots, m-1$, which is the vector
$$(\underbrace{1, \ldots, 1}_{Q_j}, 0, \ldots, 0, \underbrace{-1, \ldots, -1}_{P_k^{(i)}}, 0, \ldots, 0).$$
There are $m - 1$ vectors of this form.

- By the Equation (3.4), $\phi_{\mathcal{P}}(z) = \phi_{\mathcal{P}}(x-a_j) - \phi_{\mathcal{P}}(x-a_i)$, for $i \neq j \in \{1, \ldots, m-1\}$, which is the vector
$$(0, \ldots, 0, \underbrace{1, \ldots, 1}_{P_k^{(j)}}, 0, \ldots, 0, \underbrace{1-, \ldots, -1}_{P_k^{(i)}}, 0, \ldots, 0).$$
There are $(m-1)(m-2)$ vectors of this form.

In total, the number of minimal vectors of $\Lambda_{\mathcal{P}}$ is
$$\kappa(\Lambda_{\mathcal{P}}) = m(m-1).$$

□

Now we consider the special case that $\mathcal{P}$ consists of all rational places of $F$, i.e. $\mathcal{P} = \mathbb{P}^1(F)$.

**Corollary 3.2.5** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$ and $g(F) \geq 2$. Let*
$$\mathcal{P} = \mathbb{P}^1(F).$$
*Suppose that $F/\mathbb{F}_q$ satisfies condition $(*)$ and $\Lambda_{\mathcal{P}}$ has minimum distance $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Let $E \subsetneq F$ be the unique rational subfield with $[F : E] = \gamma$ and consider the set*
$$S' := \{P \in \mathbb{P}(E) : \deg(P) = 1 \textit{ and } P \textit{ splits completely in the extension } F/E\}.$$
*Let $m := |S'|$. Then the conclusions of Theorem 3.2.3 hold.*

**Proof**: Since $\mathcal{P} = \mathbb{P}^1(F)$, each place in $S'$ satisfies condition (2). Thus, the hypothesis of Theorem 3.2.3 is satisfied.

□

The following is a remarkable application of Theorem 3.2.3.

**Corollary 3.2.6** *Let $F/\mathbb{F}_q$ be a hyperelliptic function field. Then $\gamma(F) = 2$ and $g(F) \geq 2$. Let $\mathcal{P} = \mathbb{P}^1(F)$ and $E \subsetneq F$ be the unique rational subfield with $[F : E] = 2$. Assume the following condition:*
$$\textit{At least two rational places of } E \textit{ split in } F/E. \qquad (**)$$
*Then, the function field lattice $\Lambda_{\mathcal{P}}$ is not well-rounded.*

**Proof**: Since $\mathcal{P} = \mathbb{P}^1(F)$ and condition $(**)$ holds, Corollary 3.1.2 applies; the minimum distance of $\Lambda_{\mathcal{P}}$ is equal to $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma(F)} = 2$. Then the result follows by Corollary 3.2.5.

□

Note that the lattices associated to hyperelliptic function fields are studied in detail in Chapter 4. Also, a sufficient criterion to obtain condition $(**)$ for hyperelliptic function fields is given in Chapter 5 to produce examples of lattices which are not well-rounded.(See Example 5.0.3 in Chapter 5.)

We complete this section by showing that there are many function fields that satisfy condition $(*)$:

**Proposition 3.2.7** *Suppose that $E \subseteq F$ is a rational subfield of $F$ such that $r := [F : E]$ is a prime number and*

$$g(F) > (r-1)^2.$$

*Then the gonality of $F$ is $\gamma(F) = r$, and $E$ is the unique rational subfield of $F$ with $[F : E] = r$.*

**Proof**: Assume that there is a rational subfield $\bar{E} \subseteq F$ of degree $[F : \bar{E}] \leq r$ and $\bar{E} \neq E$. Then $F$ is the compositum of $E$ and $\bar{E}$, and by Riemann's inequality (see [14, Corollary 3.11.4]) we obtain

$$g(F) \leq ([F:E]-1)([F:\bar{E}]-1) \leq (r-1)^2,$$

a contradiction.

□

## 3.3. $F/\mathbb{F}_q$ with Many Rational Subfields of Degree $\gamma(F)$

Now we give a generalization of the results in Section 3.2, by omitting condition $(*)$, which allows $F$ to have only one rational subfield $E \subseteq F$ with $[F : E] = \gamma(F)$. In Corollary 3.3.10, a class of function fields $F/\mathbb{F}_q$ is presented where $\Lambda_{\mathcal{P}}$ is not well-rounded and

$$d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma(F)}.$$

Our reference for this section is [1].

Let us recall conditions (1) and (2), again for this section. If $E$ is a rational subfield of $F$ with $[F : E] = \gamma(F)$, for a rational place $P$ of $E$, define conditions:

$$P \text{ splits completely in the extension } F/E, \text{ and} \tag{1}$$

$$\text{for all } P' \in \mathbb{P}^1(F) \text{ with } P'|P, \text{ the place } P' \text{ belongs to } \mathcal{P}. \tag{2}$$

**Lemma 3.3.8** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$ and $\mathcal{P} \subseteq \mathbb{P}(F)$. Suppose that $\Lambda_{\mathcal{P}}$ has minimum distance $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Let $E \subseteq F$ be a rational subfield with $[F : E] = \gamma$ and consider the set*

$$S(E) := \{P \in \mathbb{P}(E) : \deg(P) = 1 \text{ and } P \text{ satisfies conditions } (1) \text{ and } (2)\}.$$

*Assume that $|S(E)| =: m \geq 2$. Then the following hold:*

**(i)** *The vectors $\phi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ of minimal length where $z \in E \cap \mathcal{O}_{\mathcal{P}}^*$ span a sublattice of $\Lambda_{\mathcal{P}}$ of rank $m - 1$.*

**(ii)** *The number of the minimal vectors $\phi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ where $z \in E \cap \mathcal{O}_{\mathcal{P}}^*$ is given by $m(m-1)$.*

**Proof**: Corollary 3.1.2 guarantees the existence of a rational subfield $E \subseteq F$ with $[F : E] = \gamma$ and $|S(E)| \geq 2$. Let $S(E) = \{P_1, \ldots, P_m\}$.

**(i)** Let $z \in E \cap \mathcal{O}_{\mathcal{P}}^*$ with $\|z\| = \sqrt{2\gamma}$. By Proposition 3.1.1,

$$[F : \mathbb{F}_q(z)] = \gamma \implies E = \mathbb{F}_q(z),$$

and the zero and the pole of $z$ in $E$ satisfy (1). Since $z \in \mathcal{O}_{\mathcal{P}}^*$, these two places also satisfy (2). Thus,

$$(z)^E = P_i - P_j \text{ for some } i \neq j \text{ with } i, j \in \{1, \ldots .m\},$$

where $(z)^E$ denotes the principal divisor of $z$ in $E$. Let us denote $z$ by $z_{i,j}$ if $(z)^E = P_i - P_j$. Then,

$$\begin{aligned}(z_{i,j})^E &= P_i - P_j \\ &= (z_{i,1})^E - (z_{j,1})^E \text{ for } i, j \in \{2, \ldots, m\}.\end{aligned}$$

Thus,

$$\phi_{\mathcal{P}}(z_{i,j}) = \phi_{\mathcal{P}}(z_{i,1}) - \phi_{\mathcal{P}}(z_{j,1}), \text{ and also}$$
$$\phi_{\mathcal{P}}(z_{1,j}) = -\phi_{\mathcal{P}}(z_{j,1}).$$

Hence, the set

$$\{\phi_{\mathcal{P}}(z_{j,1}) : j = 2, \ldots, m\}$$

generates the sublattice of $\Lambda_{\mathcal{P}}$ spanned by all $\phi_{\mathcal{P}}(z)$, where $\|z\| = \sqrt{2\gamma}$, $z \in E \cap \mathcal{O}_{\mathcal{P}}^*$. Since (for a suitable ordering of $\mathcal{P}$) $\phi_{\mathcal{P}}(z_{j,1})$ has the form

$$\phi_{\mathcal{P}}(z_{j,1}) = (0, \ldots, 0, \underbrace{-1, \ldots, -1}_{\text{above } P_1}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{\text{above } P_j}, 0, \ldots, 0),$$

the vectors $\phi_{\mathcal{P}}(z_{j,1})$ are linearly independent for $j = 2, \ldots, m$.

**(ii)** By part (i), we count the elements $z_{i,j}$, with $i, j \in \{1, \dots, m\}$ and $i \neq j$. Obviously, there are $m(m-1)$ such elements.

□

The next theorem gives an interval in which the rank of $\Delta_{\mathcal{P}}$ lies.

**Theorem 3.3.9** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$ and $\mathcal{P} \subseteq \mathbb{P}(F)$. Suppose that $\Lambda_{\mathcal{P}}$ has minimum distance $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Let $E_1, \dots, E_s$ be all rational subfields of $F$ with $[F : E_i] = \gamma$ and consider the sets*

$$S(E_i) := \{P \in \mathbb{P}(E_i) : \deg(P) = 1 \textit{ and } P \textit{ satisfies conditions } (1) \textit{ and } (2)\},$$

*for $i = 1, \dots, s$. Let $m_i := |S(E_i)|$ and $m := \max\{m_i : 1 \leq i \leq s\}$. Then the following hold:*

**(i)** $m \geq 2$.

**(ii)** $\operatorname{rank}(\Lambda_{\mathcal{P}}) \geq m\gamma - 1$.

**(iii)** *The rank of the sublattice $\Delta_{\mathcal{P}}$, generated by the minimal vectors of $\Lambda_{\mathcal{P}}$, satisfies*

$$m - 1 \leq \operatorname{rank}(\Delta_{\mathcal{P}}) \leq s(m-1).$$

**Proof**:

**(i)** The result follows from Corollary 3.1.2.

**(ii)** See the proof of part (ii) of Theorem 3.2.3.

**(iii)** If $\phi_{\mathcal{P}}(z)$ is a minimal vector, then $\mathbb{F}_q(z) = E_i$ for some $i \in \{1, \dots, s\}$ such that $m_i \geq 2$, by Corollary 3.1.2. Thus, $z \in E_i \cap \mathcal{O}_{\mathcal{P}}^*$ where $m_i \geq 2$, $1 \leq i \leq s$. On the other hand, if $m_i \geq 2$, then there are $m_i - 1$ linearly independent vectors $\phi_{\mathcal{P}}(z)$ of minimal length, where $z \in E_i \cap \mathcal{O}_{\mathcal{P}}^*$, by Lemma 3.3.8. Therefore, the number of linearly independent minimal vectors in $\Lambda_{\mathcal{P}}$, $\operatorname{rank}(\Delta_{\mathcal{P}})$, satisfies the inequalities

$$m - 1 \leq \operatorname{rank}(\Delta_{\mathcal{P}}) \leq \sum_{i=1}^{s} (m_i - 1) \leq s(m-1).$$

□

Now we obtain a class of function fields which yields lattices that are not well-rounded.

**Corollary 3.3.10** *Under the assumptions of Theorem 3.3.9, assume further that $g(F) > 0$ and $s \leq \gamma$. Then, $\Lambda_{\mathcal{P}}$ is not well-rounded.*

**Proof**: As $g(F) > 0$, the gonality of $F$ is greater than 1. Then,

$$\begin{aligned} \operatorname{rank}(\Delta_{\mathcal{P}}) \leq s(m-1) \leq \gamma(m-1) = \gamma m - \gamma \\ < \gamma m - 1 \leq \operatorname{rank}(\Lambda_{\mathcal{P}}). \end{aligned}$$

Therefore, the number of linearly independent minimal vectors is less than the rank of $\Lambda_{\mathcal{P}}$, i.e. $\Lambda_{\mathcal{P}}$ is not well-rounded.

□

The following corollary presents an expression for the kissing number of $\Lambda_{\mathcal{P}}$.

**Corollary 3.3.11** *Under the assumptions of Theorem 3.3.9, the kissing number of $\Lambda_{\mathcal{P}}$ is given by*

$$\kappa(\Lambda_{\mathcal{P}}) = \sum_{i=1}^{s} m_i(m_i - 1).$$

**Proof**: By Corollary 3.1.2, any $z \in \mathcal{O}_{\mathcal{P}}^*$ with minimal length belongs to $E_i \cap \mathcal{O}_{\mathcal{P}}^*$ for some $i \in \{1, \ldots, s\}$ such that $m_i \geq 2$. Then the result follows from the second part of Lemma 3.3.8.

□

As a final observation, we can discard condition (2) if $\mathcal{P}$ consists of all rational places of $F$.

**Corollary 3.3.12** *Let $F/\mathbb{F}_q$ be a function field with $\gamma(F) = \gamma$. Let*

$$\mathcal{P} = \mathbb{P}^1(F).$$

*Suppose that $\Lambda_{\mathcal{P}}$ has minimum distance $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Let $E_1, \ldots, E_s$ be all rational subfields of $F$ with $[F : E_i] = \gamma$ and consider the sets*

$$S'(E_i) := \{P \in \mathbb{P}(E_i) : \deg(P) = 1 \text{ and } P \text{ splits completely in the extension } F/E_i\},$$

*for $i = 1, \ldots, s$. Let $m_i := |S'(E_i)|$ and $m := \max\{m_i : 1 \leq i \leq s\}$. Then, the conclusions of Theorem 3.3.9 hold.*

**Proof**: See the proof of Corollary 3.2.5.

□

# CHAPTER 4

## Lattices from Hyperelliptic Function Fields

In the previous chapter we showed that for some natural choice of $\mathcal{P}$, lattices from hyperelliptic function fields are not well-rounded (see Theorem 3.2.3 or Corollary 3.2.6). In this chapter, we study lattices from hyperelliptic function fields in detail for a different choice of the set $\mathcal{P}$.

### 4.1. Some Basic Facts about Hyperelliptic Function Fields

We present some preliminary information on hyperelliptic function fields based on [14, §6.2].

Let $K$ be a perfect field.

**Definition 4.1.1** *A* hyperelliptic function field *over $K$ is an algebraic function field $F/K$ of genus $g(F) \geq 2$ which contains a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$.*

**Lemma 4.1.1**

**(i)** *A function field $F/K$ of genus $g(F) \geq 2$ is hyperelliptic if and only if there exists a divisor $A \in \mathrm{Div}(F)$ where $\deg(A) = 2$ and the dimension of $\mathcal{L}(A)$ is at least 2.*

**(ii)** *Every function field $F/K$ of genus 2 is hyperelliptic.*

If $F/K$ is hyperelliptic and $K(x)$ is a subfield of $F$ with $[F : K(x)] = 2$, then the extension $F/K(x)$ is separable. Hence $F/K(x)$ is a cyclic extension of degree 2.

**Proposition 4.1.2** *Assume that* $\mathrm{char}(K) \neq 2$*. Then the following hold:*

**(i)** *Let $F/K$ be a hyperelliptic function field of genus $g$. Then there exist $x, y \in F$ such that $F = K(x, y)$ and*

$$y^2 = f(x) \in K[x] \tag{4.1}$$

*with a square-free polynomial $f(x)$ of degree $2g + 1$ or $2g + 2$.*

**(ii)** *Conversely, if $F = K(x, y)$ and $y^2 = f(x) \in K[x]$ with a square-free polynomial $f(x)$ of degree $m > 4$, then $F/K$ is hyperelliptic of genus*

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

**(iii)** *Let $F = K(x, y)$ with $y^2 = f(x)$ as in Equation (4.1). Then the places $P \in \mathbb{P}(K(x))$ which ramify in $F/K(x)$ are the following:*

$$\text{all zeros of } f(x), \ \text{if } \deg(f(x)) \equiv 0 \bmod 2,$$

$$\text{all zeros of } f(x) \text{ and the pole of } x, \ \text{if } \deg(f(x)) \equiv 1 \bmod 2.$$

*Hence, if $f(x)$ decomposes into linear factors, then exactly $2g + 2$ places of $K(x)$ are ramified in $F/K(x)$.*

In the case of $\mathrm{char}(K) = 2$, the number $r$ of ramified places in $F/K(x)$ lies in the interval

$$1 \leq r \leq g + 1. \tag{4.2}$$

Later we will use the following property of hyperelliptic function fields.

**Proposition 4.1.3** *Consider a hyperelliptic function field $F/K$ of genus $g$ and a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$. Then, all rational subfields $K(z) \subseteq F$ with $[F : K(z)] \leq g$ are contained in $K(x)$. In particular, $K(x)$ is the only rational subfield of $F$ with $[F : K(x)] = 2$.*

## 4.2. The Group $\mathcal{O}^*_{\mathcal{Q}}$ for Hyperelliptic Function Fields

We consider a hyperelliptic function field $F/\mathbb{F}_q$ with genus $g = g(F)$ and denote by $\mathbb{F}_q(x)$ its unique rational subfield of degree $[F : \mathbb{F}_q(x)] = 2$. We assume that the pole of $x$ is ramified in $F/\mathbb{F}_q(x)$ and denote by $P_\infty$ the unique pole of $x$ in $\mathbb{P}(F)$. Throughout Sections 4.2-4.4, we fix the tuple $\mathcal{Q} \subseteq \mathbb{P}(F)$ as follows:

$$\mathcal{Q} = (P_\infty, P_2, \ldots, P_r, Q_1, \ldots, Q_s), \text{ where}$$

- $P_2, ..., P_r$ are all rational places of $F$ which are ramified over $\mathbb{F}_q(x)$ and are different from $P_\infty$, and

- $Q_1, ..., Q_s$ are all places of $F$ of degree 2, which are inert over $\mathbb{F}_q(x)$.

We set, throughout Sections 4.2-4.4,

$$\alpha_i := x(P_i) \in \mathbb{F}_q \text{ (for } i = 2, ..., r) \text{ and } \beta_j := x(Q_j) \in \mathbb{F}_q \text{ (for } j = 1, ..., s).$$

We study the lattice $\Lambda_\mathcal{Q}$. Clearly the rank of $\Lambda_\mathcal{Q}$ is

$$\text{rank}(\Lambda_\mathcal{Q}) = |\mathcal{Q}| - 1 = r + s - 1.$$

In this section we find the form of elements of the group $\mathcal{O}_\mathcal{Q}^*$, which leads to determine a generating set for $\Lambda_\mathcal{Q}$.

**Lemma 4.2.4** *Let $z \in \mathcal{O}_\mathcal{Q}^*$. Then there exist $a_i, b_j \in \mathbb{Z}$ such that the element*

$$t := z \prod_{i=2}^{r} (x - \alpha_i)^{a_i} \prod_{j=1}^{s} (x - \beta_j)^{b_j} \in \mathcal{O}_\mathcal{Q}^*$$

*has the divisor*

$$(t) = \nu_\infty P_\infty + \nu_2 P_2 + \cdots + \nu_r P_r \text{ with } \nu_i \in \{0, 1\}, i = 2, \ldots, r. \tag{4.3}$$

**Proof**: The valuations of $x - \alpha_i$ and $x - \beta_j$ are

$$v_{P_\infty}(x - \alpha_i) = v_{P_\infty}(x - \beta_j) = -2, \quad v_{P_i}(x - \alpha_i) = 2 \text{ and } v_{Q_j}(x - \beta_j) = 1,$$

for all $i, j$, and zero at all other places. Thus by assigning the values

$$a_i := -\left\lfloor \frac{v_{P_i}(z)}{2} \right\rfloor \text{ and } b_j := -v_{Q_j}(z),$$

$t$ has the principal divisor $(t)$ given in Equation (4.3).

□

**Lemma 4.2.5** *Let $z$ be an element of $\mathcal{O}_\mathcal{Q}^*$ and define the element*

$$t := z \prod_{i=2}^{r} (x - \alpha_i)^{a_i} \prod_{j=1}^{s} (x - \beta_j)^{b_j} \in \mathcal{O}_\mathcal{Q}^*$$

*as in Lemma 4.2.4. Then,*

**(i)** *$t$ can be written as*

$$t = cy + \sum_{k=0}^{g} c_k x^k, \tag{4.4}$$

*where $c, c_k \in \mathbb{F}_q$, $g = g(F)$ and $y$ is an element of $F$ with the pole divisor*

$$(y)_\infty = (2g + 1)P_\infty.$$

**(ii)** *In Equation* (4.4)*, if* $c = 0$ *then* $t$ *is a non-zero constant in* $\mathbb{F}_q$*.*

**(iii)** *In Equation* (4.4)*, if* $c \neq 0$ *then the characteristic of* $\mathbb{F}_q$ *is odd and the number of ramified places in* $F/\mathbb{F}_q(x)$ *is* $2g + 2$*.*

**Proof**:

**(i)** It is clear that $t$ is in the Riemann-Roch space $\mathcal{L}((r-1)P_\infty)$ associated to the divisor $(r-1)P_\infty$. By Proposition 4.1.2 and Equation (4.2), the number of ramified places in $F/\mathbb{F}_q(x)$ is at most $2g+2$. Then

$$r \leq 2g + 2 \text{ and}$$

$$t \in \mathcal{L}((r-1)P_\infty) \subseteq \mathcal{L}((2g+1)P_\infty).$$

Note that $\mathcal{L}((2g+1)P_\infty)$ has dimension $g+2$ and there exists an element $y \in F$ with pole divisor $(y)_\infty = (2g+1)P_\infty$. (See [14, Theorem 1.5.17] and [14, Proposition 1.6.6].) Thus, the set

$$\{1, x, x^2, \ldots, x^g, y\}$$

forms a basis for $\mathcal{L}((2g+1)P_\infty)$. Therefore, $t$ can be written as in Equation (4.4).

**(ii)** Assume that $c = 0$. Let the degree of $t(x) \in \mathbb{F}_q[x]$ be $\deg(t(x)) = \ell \leq g$. Then the valuation of $t$ at the place $P_\infty$ is

$$v_{P_\infty}(t) = -2\ell,$$

by the Strict Triangle Inequality for valuations of $F/\mathbb{F}_q$ (see [14, Lemma 1.1.11]). It follows that, without loss of generality, the principal divisor $(t)$ has the form

$$(t) = -2\ell P_\infty + P_2 + \cdots + P_{2\ell+1}.$$

Then the places $(x = \alpha_2), \ldots, (x = \alpha_{2\ell+1})$ are the zeros of $t$ in $\mathbb{F}_q(x)$, which results in that the polynomial $t(x)$ has $2\ell$ zeros, $\alpha_2, \ldots, \alpha_{2\ell+1}$, in $\mathbb{F}_q$. It follows that

$$2\ell \leq \deg(t(x)) = \ell \;\Rightarrow\; \ell = 0.$$

Hence

$$t = c_0 \in \mathbb{F}_q^*.$$

**(iii)** If $c \neq 0$, by the Strict Triangle Inequality, the valuation of $t$ at the place $P_\infty$ is

$$v_{P_\infty}(t) = v_{P_\infty}(y) = -(2g+1).$$

Then, without loss of generality, the principal divisor $(t)$ has the form

$$(t) = -(2g+1)P_\infty + P_2 + \cdots + P_{2g+2},$$

which implies that

$$r \geq 2g+2.$$

From Proposition 4.1.2 and Equation (4.2), it follows that

$$\begin{gathered}\operatorname{char}(\mathbb{F}_q) \neq 2 \text{ and} \\ r = 2g+2,\end{gathered}$$

i.e. the number of ramified places in $F/\mathbb{F}_q(x)$ is $2g+2$.

□

In the next theorem, we describe the elements of the group $\mathcal{O}_Q^*$ on a case by case basis.

**Theorem 4.2.6** *Assume that the pole of $x$ is ramified in $F/\mathbb{F}_q(x)$. Then the set $\mathcal{O}_Q^*$ can be described as follows:*

**(i)** *In the case of* $\operatorname{char}(\mathbb{F}_q) = 2$,

$$\mathcal{O}_Q^* = \Big\{\delta \cdot \prod_{i=2}^{r}(x-\alpha_i)^{a_i} \prod_{j=1}^{s}(x-\beta_j)^{b_j} : \delta \in \mathbb{F}_q^*,\ a_i, b_j \in \mathbb{Z}\Big\},$$

**(ii)** *In the case of* $\operatorname{char}(\mathbb{F}_q) \neq 2$, *assume that $F = \mathbb{F}_q(x,u)$ where $u^2 = f(x)$ with a square-free polynomial $f(x) \in \mathbb{F}_q[x]$. There are two subcases:*

**(a)** *If $f(x)$ does not decompose into linear factors over $\mathbb{F}_q$,*

$$\mathcal{O}_Q^* = \Big\{\delta \cdot \prod_{i=2}^{r}(x-\alpha_i)^{a_i} \prod_{j=1}^{s}(x-\beta_j)^{b_j} : \delta \in \mathbb{F}_q^*,\ a_i, b_j \in \mathbb{Z}\Big\}.$$

**(b)** *If $f(x)$ decomposes into linear factors over $\mathbb{F}_q$,*

$$\mathcal{O}_Q^* = \Big\{\delta \cdot u^{\mu} \cdot \prod_{i=2}^{r}(x-\alpha_i)^{a_i} \prod_{j=1}^{s}(x-\beta_j)^{b_j} : \mu \in \{0,1\},\ \delta \in \mathbb{F}_q^*,\ a_i, b_j \in \mathbb{Z}\Big\}.$$

**Proof**: Let $z$ be an arbitrary element of $\mathcal{O}_Q^*$. Applying Lemma 4.2.4 and Lemma 4.2.5, $z$ can be written as

$$z = t\prod_{i=2}^{r}(x-\alpha_i)^{a_i} \prod_{j=1}^{s}(x-\beta_j)^{b_j},\ a_i, b_j \in \mathbb{Z}, \tag{4.5}$$

where $t \in \mathcal{O}_Q^*$ has the form

$$\begin{cases} t = cy + \sum\limits_{k=0}^{g} c_k x^k, \text{ with } c, c_k \in \mathbb{F}_q, g = g(F) \text{ and} \\ y \in F \text{ such that } (y)_\infty = (2g+1)P_\infty. \end{cases} \tag{4.6}$$

**(i)** If $\mathrm{char}(\mathbb{F}_q) = 2$ then in Equation (4.6)

$$c = 0$$

by the third part of Lemma 4.2.5. It follows that $t$ is a non-zero constant in $\mathbb{F}_q$, by the second part of Lemma 4.2.5.

**(ii)** By Proposition 4.1.2, the assumption that the pole of $x$ is ramified in $F/\mathbb{F}_q$ implies that the degree of $f(x) \in \mathbb{F}_q[x]$ is

$$\deg(f(x)) = 2g + 1.$$

**(a)** Suppose that $f(x)$ does not decompose into linear factors in $\mathbb{F}_q[x]$. Then the number of ramified places in $F/\mathbb{F}_q(x)$ is less than $2g + 2$ by Proposition 4.1.2. Thus, in Equation (4.6)

$$c = 0$$

by the third part of Lemma 4.2.5. Hence $t$ is a non-zero constant in $\mathbb{F}_q$, by the second part of Lemma 4.2.5.

**(b)** Suppose that $f(x)$ splits into linear factors over $\mathbb{F}_q$. Then by Proposition 4.1.2, the number of ramified places in $F/\mathbb{F}_q(x)$ is $r = 2g + 2$ and the set of roots of $f(x)$ is

$$\{\alpha_2, \ldots, \alpha_{2g+2}\}.$$

Then the principal divisor of $u$ is

$$(u) = -(2g + 1)P_\infty + P_2 + \cdots + P_{2g+2},$$

which stems from the equality $u^2 = f(x)$.

There are two types of elements in $\mathcal{O}_Q^*$, depending on whether $c$ is zero or not in Equation (4.6).

- If $c = 0$, by the second part of Lemma 4.2.5, $t$ belongs to $\mathbb{F}_q^*$.
- If $c \neq 0$, then the valuation of $t$ at the place $P_\infty$ is

$$v_{P_\infty}(t) = v_{P_\infty}(y) = -(2g + 1).$$

Then, by Equation (4.3), $(t)$ has the form

$$(t) = -(2g + 1)P_\infty + P_2 + \cdots + P_{2g+2}.$$

Hence, the principal divisor of $t$ satisfies the equality

$$(t) = (u),$$

implying that

$$t = \delta u, \ \delta \in \mathbb{F}_q^*.$$

In all of the cases, Equation (4.5) provides the desired form for $z$.

□

Generating sets for $\Lambda_{\mathcal{Q}}$ can easily be derived from Theorem 4.2.6.

**Corollary 4.2.7** *Under the assumptions of Theorem 4.2.6, the function field lattice $\Lambda_{\mathcal{Q}}$ can be generated as follows:*

**(i)** *In the case of* $\mathrm{char}(\mathbb{F}_q) = 2$*,*

$$\Lambda_{\mathcal{Q}} = \Big\langle \phi_{\mathcal{Q}}(x-\alpha_i),\ \phi_{\mathcal{Q}}(x-\beta_j) : i = 2,\dots,r,\ j = 1,\dots,s \Big\rangle.$$

**(ii)** *In the case of* $\mathrm{char}(\mathbb{F}_q) \neq 2$*, assume that $F = \mathbb{F}_q(x,u)$ where $u^2 = f(x)$ with a square-free polynomial $f(x) \in \mathbb{F}_q[x]$. There are two subcases:*

**(a)** *If $f(x)$ does not decompose into linear factors over $\mathbb{F}_q$,*

$$\Lambda_{\mathcal{Q}} = \Big\langle \phi_{\mathcal{Q}}(x-\alpha_i),\ \phi_{\mathcal{Q}}(x-\beta_j) : i = 2,\dots,r,\ j = 1,\dots,s \Big\rangle.$$

**(b)** *If $f(x)$ decomposes into linear factors over $\mathbb{F}_q$,*

$$\Lambda_{\mathcal{Q}} = \Big\langle \phi_{\mathcal{Q}}(x-\alpha_i),\ \phi_{\mathcal{Q}}(x-\beta_j) : i = 2,\dots,r,\ j = 1,\dots,s \Big\rangle + \Big\langle \phi_{\mathcal{Q}}(u) \Big\rangle.$$

## 4.3. Well-roundedness Property of the Lattices from Hyperelliptic Function Fields

Let $F/\mathbb{F}_q$ be a hyperelliptic function field and $\mathbb{F}_q(x) \subseteq F$ be the unique rational subfield of $F$ with $[F : \mathbb{F}_q(x)] = 2$. Recall that, in Chapter 3, we obtained the following result on well-roundedness property of lattices from hyperelliptic function fields:

**Theorem 4.3.8** *Suppose that $\mathcal{P} \subseteq \mathbb{P}(F)$ contains all the extensions of at least two rational places of $\mathbb{F}_q(x)$ which split in $F/\mathbb{F}_q(x)$. Then the lattice $\Lambda_{\mathcal{P}}$ is not well-rounded.*

**Proof**: See Corollary 3.1.2 and Theorem 3.2.3 in Chapter 3.

□

Now, we analyze the case that the extensions of splitting rational places of $\mathbb{F}_q(x)$ are excluded from $\mathcal{P}$. In other words, we consider the tuple

$$\mathcal{Q} = (P_\infty, P_2, \dots, P_r, Q_1, \dots, Q_s) \subseteq \mathbb{P}(F)$$

which is described in Section 4.2.

**Theorem 4.3.9** *Assume that $g(F) \geq 3$ and the pole of $x$ is ramified in $F/\mathbb{F}_q(x)$. Consider the set of vectors*

$$M := \{\phi_{\mathcal{Q}}(x-\alpha_i),\ \phi_{\mathcal{Q}}(x-\beta_j) : i = 2, \ldots, r,\ j = 1, \ldots, s\} \subseteq \Lambda_{\mathcal{Q}}.$$

*Then the following hold:*

**(i)** *The minimum distance of $\Lambda_{\mathcal{Q}}$ is*

$$d(\Lambda_{\mathcal{Q}}) = \sqrt{8}$$

*and the vectors in $M$ have the minimum length.*

**(ii)** *The lattice $\Lambda_{\mathcal{Q}}$ is well-rounded.*

**Proof**:

**(i)** The vectors $\phi_{\mathcal{Q}}(x-\alpha_i)$ and $\phi_{\mathcal{Q}}(x-\beta_j)$ have the form

$$\pm (0, \ldots, 0, -2, 0, \ldots, 0, 2, 0, \ldots, 0), \tag{4.7}$$

and the length

$$\|x-\alpha_i\| = \|x-\beta_j\| = \sqrt{(-2)^2+2^2} = \sqrt{8}.$$

In Proposition 2.2.1, we showed that the square of the length $\|z\|$ is an even integer for any $z \in \mathcal{O}^*_{\mathcal{Q}}$. Suppose that there is an element $z \in \mathcal{O}^*_{\mathcal{Q}}$ with $\|z\| < \sqrt{8}$. Then we have one of the following cases:

- $\|z\| = \sqrt{6}$. Then $\phi_{\mathcal{Q}}(z)$ is either

$$\pm (-2, 1, 1, 0, \ldots, 0) \text{ or}$$

$$\pm (1, 1, 1, -1, -1, -1, 0, \ldots, 0),$$

without loss of generality.

<u>In the first case</u>, the degree of the extension $F/\mathbb{F}_q(z)$ is $[F : \mathbb{F}_q(z)] = 2$. By the uniqueness property of $\mathbb{F}_q(x)$,

$$\mathbb{F}_q(z) = \mathbb{F}_q(x).$$

If the zero or the pole of $z$ split in $F/\mathbb{F}_q(z)$, then $z$ cannot belong to $\mathcal{O}^*_{\mathcal{Q}}$, due to the setting of $\mathcal{Q}$. Thus, the zero and the pole of $z$ are ramified or inert in $F/\mathbb{F}_q(x)$, which implies that $\phi_{\mathcal{Q}}(z)$ has the form as in Equation (4.7).

<u>In the second case</u>, the degree of the extension $F/\mathbb{F}_q(z)$ is $[F : \mathbb{F}_q(z)] = 3$. Then, by Riemann's inequality (see [14, Corollary 3.11.4]),

$$F = \mathbb{F}_q(x, z) \text{ and}$$

$$g(F) \leq ([F : \mathbb{F}_q(x)] - 1)([F : \mathbb{F}_q(z)] - 1) = 2.$$

It follows that $g(F) = 2$, which is not the case.

- $\|z\| = \sqrt{4}$. Then $\phi_{\mathcal{Q}}(z)$, without loss of generality, has the form

  $$\pm(1, 1, -1, -1, 0, \ldots, 0).$$

  Hence, $z$ has degree 2 and $\phi_{\mathcal{Q}}(z)$ must have the form as in Equation (4.7), again.

- $\|z\| = \sqrt{2}$. Then $\phi_{\mathcal{Q}}(z)$, without loss of generality, has the form

  $$\pm(1, -1, 0, \ldots, 0),$$

  which results in that $[F : \mathbb{F}_q(x)] = 1$, i.e. $F$ is a rational function field.

Therefore, the minimum distance of $\Lambda_{\mathcal{Q}}$ is $d(\Lambda_{\mathcal{Q}}) = \sqrt{8}$.

**(ii)** $\mathcal{Q}$ consists of the extensions of $(x = \infty)$, $(x = \alpha_i)$ and $(x = \beta_j)$ in $F/\mathbb{F}_q(x)$. Thus, the set $M$ consists of

$$|\mathcal{Q}| - 1$$

vectors of $\Lambda_{\mathcal{Q}}$, which have the minimum length of $\Lambda_{\mathcal{Q}}$ by the first part. Recall that the rank of the lattice is also $\operatorname{rank}(\Lambda_{\mathcal{Q}}) = |\mathcal{Q}| - 1$ (see Proposition 2.2.2). $M$ is clearly a linearly independent set; therefore, the function field lattice $\Lambda_{\mathcal{Q}}$ is well-rounded.

□

**Corollary 4.3.10** *Under the assumptions of Theorem 4.3.9, $\Lambda_{\mathcal{Q}}$ can be generated by its minimal vectors in the following cases:*

- $\operatorname{char}(\mathbb{F}_q) = 2$.
- $\operatorname{char}(\mathbb{F}_q) > 2$, *and* $F = \mathbb{F}_q(x, u)$ *with the defining equation* $u^2 = f(x) \in \mathbb{F}_q[x]$ *where*

  *$f(x)$ is a square-free polynomial and*

  *$f(x)$ does not decompose into linear factors over $\mathbb{F}_q$.*

**Proof**: The results follow from Corollary 4.2.7 and Theorem 4.3.9.

□

## 4.4. Relatively ‘Short’ Vectors in Hyperelliptic Function Fields

Let $F/\mathbb{F}_q$ be a hyperelliptic function field and $\mathbb{F}_q(x) \subseteq F$ be the unique rational subfield of $F$ with $[F : \mathbb{F}_q(x)] = 2$. Let $\mathcal{Q} \subseteq \mathbb{P}(F)$ be the tuple described in Section 4.2. In the previous section, it was shown that the minimal vectors of $\Lambda_{\mathcal{Q}}$ are associated to certain elements of $\mathbb{F}_q(x)$. Now, we present our result on the smallest length of $z \in \mathcal{O}_{\mathcal{Q}}^*$ where $z$ is not an element of $\mathbb{F}_q(x)$ (which may be useful for future studies on the successive minima for $\Lambda_{\mathcal{Q}}$, see [6, p. 58]).

The following observation holds for any tuple $\mathcal{P}$ of places of $F$.

**Proposition 4.4.11** *Let $g(F) = g$ and $z \in \mathcal{O}_{\mathcal{P}}^*$. If the length of $z$ satisfies the inequality*

$$\|z\| < \sqrt{2g+2},$$

*then $z$ belongs to $\mathbb{F}_q(x)$.*

**Proof**: By Proposition 2.2.1,

$$2g + 2 > \|z\|^2 \geq 2\deg(z)$$

$$\Rightarrow \deg(z) < g + 1.$$

Hence, $z \in \mathbb{F}_q(x)$ by Proposition 4.1.3.

□

In general, the assumption $\|z\| < \sqrt{2g+2}$ in Proposition 4.4.11 cannot be relaxed. We give an example:

**Example 4.4.2** *Let* $\mathrm{char}(\mathbb{F}_q)$ *be odd and $F = \mathbb{F}_q(x, u)$ where $u^2 = f(x)$ with a square-free polynomial $f(x) \in \mathbb{F}_q[x]$. Assume that $f(x)$ splits into linear factors in $\mathbb{F}_q[x]$ and the pole of $x$ is ramified in $F/\mathbb{F}_q(x)$. Then, there exists an element $z$ in $\mathcal{O}_{\mathcal{Q}}^* \setminus \mathbb{F}_q(x)$ with length*

$$\|z\| = \sqrt{2g+2}.$$

**Proof**: Since the pole of $x$ is ramified in $F/\mathbb{F}_q(x)$, the degree of $f(x)$ is $\deg(f(x)) = 2g + 1$ by Proposition 4.1.2. Let $h_1(x)$ and $h_2(x)$ be polynomials in $\mathbb{F}_q(x)$ such that

$$f(x) = h_1(x)h_2(x), \text{ where } \deg(h_1(x)) = g \text{ and } \deg(h_2(x)) = g + 1.$$

By Proposition 4.1.2, the zeros of $f(x)$ and the pole of $x$ are all of the ramified places in $F/\mathbb{F}_q(x)$. Since $f(x)$ decomposes into linear factors over $\mathbb{F}_q$, the principal divisors of $u$ and $h_1$ are found to be

$$\begin{aligned} (u) &= -(2g+1)P_\infty + \sum_{i=2}^{2g+2} P_i, \text{ and} \\ (h_1) &= -2gP_\infty + \sum_{\substack{i \text{ where} \\ h_1(\alpha_i)=0}} 2P_i, \end{aligned}$$

respectively. Hence, the element $uh_1^{-1} \in \mathcal{O}_{\mathcal{Q}}^* \setminus \mathbb{F}_q(x)$, with the principal divisor

$$\left(uh_1^{-1}\right) = -P_\infty - \sum_{\substack{i \text{ where} \\ h_1(\alpha_i)=0}} P_i + \sum_{\substack{i \text{ where} \\ h_2(\alpha_i)=0}} P_i,$$

attains the length $\sqrt{2g+2}$.

□

# CHAPTER 5

## Further Examples of Function Field Lattices

In this chapter, we present several examples which demonstrate some of the results of the previous chapters.

The first example gives a sufficient criterion to check the assumption in Corollary 3.2.6.

**Example 5.0.3** *Let $F/\mathbb{F}_q$ be a hyperelliptic function field with $g = g(F)$ and $\mathbb{F}_q(x) \subseteq F$ be the unique rational subfield of $F$ with $[F : \mathbb{F}_q(x)] = 2$. Let $\mathcal{P}$ consist of all rational places of $F$. Assume that the genus of $F$ satisfies the inequality*

$$g \leq \frac{q-5}{2+2\sqrt{q}}. \tag{5.1}$$

*Then the function field lattice $\Lambda_{\mathcal{P}}$ is not well-rounded.*

**Proof**: Recall that $N(F)$ denotes the number of rational places of $F$. Then by Equation (5.1) and the Hasse-Weil Theorem (see [14, Theorem 5.2.3]), $N(F)$ satisfies the inequality

$$N(F) \geq q + 1 - 2g\sqrt{q} \geq q + 1 + [2g - (q-5)] = 2g + 6.$$

By Proposition 4.1.2, the number of ramified places in $F/\mathbb{F}_q(x)$ is at most $2g + 2$. Consequently, there must be at least two rational places of $\mathbb{F}_q(x)$ which split in $F/\mathbb{F}_q(x)$. Then the result follows from Corollary 3.2.6.

□

**Example 5.0.4** *Let $r$ be a prime number with $q \equiv 1 \bmod r$, and let $f(x) = \prod_{i=1}^{k} p_i(x)^{e_i}$ with $k$ distinct irreducible monic polynomials $p_i(x) \in \mathbb{F}_q[x]$ such that $1 \leq e_i \leq r-1$. Assume that $\sum_{i=1}^{k} \deg(p_i(x)) > 2r$ and there exist at least two elements $a_1, a_2 \in \mathbb{F}_q$ such that $f(a_i) \neq 0$ is an $r$-th power in $\mathbb{F}_q$. Let $F/\mathbb{F}_q$ be the function field $F = \mathbb{F}_q(x, y)$ with defining equation*

$$y^r = f(x).$$

*Let $\mathcal{P}$ consist of all rational places of $F$. Then the lattice associated to $F$ is not well-rounded.*

**Proof**: $F/\mathbb{F}_q(x)$ is a Kummer extension of degree $[F:\mathbb{F}_q(x)] = r$ (see [14, Proposition 3.7.3]). Denote by $P_i$ the place of $\mathbb{F}_q(x)$ with prime element $p_i(x)$ and by $P_i'$ the place of $F$ lying over $P_i$, for $i = 1, \ldots, k$. Then the following equality

$$rv_{P_i'}(y) = v_{P_i'}(f(x)) = e(P_i'|P_i)e_i,$$

where $e(P_i'|P_i)$ is the ramification index of $P_i'$ over $P_i$, implies that

$$e(P_i'|P_i) = r.$$

Then the degree of $P_i'$ is equal to

$$\deg(P_i') = \deg(P_i) = \deg(p_i(x)).$$

Applying the Hurwitz Genus Formula (see [14, Theorem 3.4.13]), we get

$$2g - 2 = -2r + \deg(\mathrm{Diff}(F/\mathbb{F}_q(x))), \tag{5.2}$$

where the degree of the different $\mathrm{Diff}(F/\mathbb{F}_q(x))$ satisfies

$$\begin{aligned}\deg(\mathrm{Diff}(F/\mathbb{F}_q(x))) &\geq \sum_{i=1}^{k} d(P_i'|P_i)\deg(P_i') \\ &= \sum_{i=1}^{k} (e(P_i'|P_i) - 1)\deg(p_i(x)) \\ &> (r-1)2r.\end{aligned}$$

Then Equation (5.2) implies that

$$g > (r-1)^2,$$

and consequently Proposition 3.2.7 applies to the function field $F/\mathbb{F}_q$. By the Kummer Theorem, the zeros of the polynomials $x - a_1$ and $x - a_2$ split completely in the extension $F/\mathbb{F}_q(x)$ (see [14, Theorem 3.3.7]). Thus, the minimum distance in $\Lambda_{\mathcal{P}}$ is $d(\Lambda_{\mathcal{P}}) = \sqrt{2r}$ by Corollary 3.1.2.

Then the result follows from Corollary 3.2.5.

□

Recall that the Hermitian function field $H = \mathbb{F}_q(x, y)$ is a function field over a finite field $\mathbb{F}_q$ where $q = \ell^2$ is a square and $x, y \in H$ satisfy the equation

$$y^\ell + y = x^{\ell+1}.$$

Böttcher et al. [3] showed that if $\mathcal{P}$ is taken to be the $n$-tuple of all rational places of $H$, then the lattice associated to $H$ is well-rounded. (See Theorem 2.3.6.) It is known that Hermitian function fields are maximal, i.e. the number of rational places $N(H)$ attains the upper Hasse-Weil bound $N(H) = q + 1 + 2g\sqrt{q}$. The next two examples illustrate that not all lattices associated to maximal function fields are well-rounded.

**Example 5.0.5** *Let $q = \ell^2$ be a square and let $r$ be a prime number with $\ell \equiv -1 \bmod r$ and $r < (\ell+1)/2$. Consider the function field $F = \mathbb{F}_q(u,y)$ with defining equation*

$$y^\ell + y = u^r.$$

*Let $\mathcal{P}$ consist of all rational places of $F$. Then $F/\mathbb{F}_q$ is maximal, and the lattice associated to it is not well-rounded.*

**Proof**: Being a subfield of the Hermitian function field $H = \mathbb{F}_q(x,y)$ where $y^\ell + y = x^{\ell+1}$, the function field $F$ is maximal over $\mathbb{F}_q$ (see [8]). On the other hand, $F/\mathbb{F}_q(y)$ is a Kummer extension of degree $[F : \mathbb{F}_q(y)] = r$ (see [14, Proposition 3.7.3]). Note that

- $(y = \infty)$ and $(y = \alpha)$ such that $\alpha^\ell + \alpha = 0$, $\alpha \in \mathbb{F}_q$, are the ramified places in $F/\mathbb{F}_q(y)$ and
- $(y = \alpha)$ such that $\alpha^\ell + \alpha \in \mathbb{F}_\ell \setminus \{0\}$, $\alpha \in \mathbb{F}_q$, are the completely splitting places in $F/\mathbb{F}_q(y)$ .

Then by the Hurwitz Genus Formula (see [14, Theorem 3.4.13]), the genus of $F$ is equal to

$$g(F) = \frac{(\ell-1)(r-1)}{2}. \tag{5.3}$$

Now Proposition 3.2.7 applies to the function field $F/\mathbb{F}_q$. By Corollary 3.1.2, the minimum distance in $\Lambda_{\mathcal{P}}$ is $d(\Lambda_{\mathcal{P}}) = \sqrt{2r}$. Also by Equation (5.3), the number of rational places of $F$ and the rank of $\Lambda_{\mathcal{P}}$ are found as follows:

> $N(F) = r(\ell^2 - \ell) + \ell + 1$ as $F/\mathbb{F}_q$ is maximal (this can also be computed directly), and
>
> $\operatorname{rank}(\Lambda_{\mathcal{P}}) = N(F) - 1 = r(\ell^2 - \ell) + \ell.$

Denote the number of completely splitting places in $F/\mathbb{F}_q(y)$ by

$$m := \ell(\ell - 1) \geq 2.$$

By Corollary 3.2.4, we can find the number of the minimal vectors in $\Lambda_{\mathcal{P}}$ as

$$\kappa(\Lambda_{\mathcal{P}}) = m(m-1) = (\ell^2 - \ell)(\ell^2 - \ell - 1).$$

Then by Corollary 3.2.5, the rank of the sublattice generated by the minimal vectors of $\Lambda_{\mathcal{P}}$ is equal to

$$\operatorname{rank}(\Delta_{\mathcal{P}}) = m - 1 = \ell^2 - \ell - 1 < \operatorname{rank}(\Lambda_{\mathcal{P}}).$$

Therefore, the lattice $\Lambda_{\mathcal{P}}$ is not well-rounded.

□

**Example 5.0.6** *Let $q = \ell^2$ be a square and let $r$ be a prime number which divides $\ell + 1$. Asssume that $k$ is another divisor of $\ell + 1$ with $r \nmid k$ and $2r \leq k$. Consider the function field $F = \mathbb{F}_q(u, v)$ with defining equation*

$$u^k + v^r = 1.$$

*Let $\mathcal{P}$ consist of all rational places of $F$. Then $F/\mathbb{F}_q$ is maximal, and the lattice associated to it is not well-rounded.*

**Proof**: $F$ is a subfield of the Hermitian function field $H$ over $\mathbb{F}_q$ given by the equation $x^{\ell+1} + y^{\ell+1} = 1$, thus it is maximal over $\mathbb{F}_q$ (see [8]). Note that $F/\mathbb{F}_q(u)$ is a Kummer extension of degree $[F : \mathbb{F}_q(u)] = r$, then the genus of $F$ is calculated as

$$g(F) = \frac{(r-1)(k-1)}{2}$$

(see [14, Proposition 3.7.3]). Now Proposition 3.2.7 applies to the function field $F/\mathbb{F}_q$. Due to Corollary 3.1.2, it is found that $d(\Lambda_{\mathcal{P}}) = \sqrt{2r}$. Then the result follows from Corollary 3.2.5.

□

In Chapter 3, we observed that if a function field lattice is well-rounded, then the associated function field $F$ has sufficiently many rational subfield $E \subsetneq F$ of small degree $[F : E]$. In the next two examples, we show that elliptic and Hermitian function fields have that property. This fact explains why their associated lattices are well-rounded (see Theorem 2.3.4 and Theorem 2.3.6).

**Example 5.0.7** *An elliptic function field $F$ over $\mathbb{F}_q$ with $N$ rational places has exactly $N$ rational subfields of degree 2.*

**Proof**: Fix a rational place $O \in \mathbb{P}^1(F)$. Note that the Riemann-Roch space $\mathcal{L}(P + O)$ has dimension 2 over $\mathbb{F}_q$ where $P \in \mathbb{P}^1(F)$. Let $\{1, x\}$ be a basis of this space. Then

$$\mathcal{L}(P + O) = \mathbb{F}_q + x\mathbb{F}_q \text{ and}$$
$$\mathbb{F}_q(\mathcal{L}(P + O)) = \mathbb{F}_q(x).$$

Consequently,

the pole divisor of $x$ in $F$ is $(x)_\infty = P + O$ and

the degree of the extension $F/\mathbb{F}_q(x)$ is $[F : \mathbb{F}_q(x)] = 2$.

Define the map $\sigma$ as follows:

$$\sigma : \begin{cases} \mathbb{P}^1(F) & \to \{E \mid E \subsetneq F \text{ is a rational subfield of } F \text{ with } [F : E] = 2\} \\ P & \mapsto \mathbb{F}_q(\mathcal{L}(P + O)). \end{cases}$$

$\sigma$ is a one-to-one map:
Let $P, Q \in \mathbb{P}^1(F)$ such that

$$\sigma(P) = \mathbb{F}_q(x)$$
$$\sigma(Q) = \mathbb{F}_q(y)$$

for some $x, y \in F$. Then $(y)_\infty = Q + O$ and the valuations of $x$ and $y$ at the place $O$ are

$$v_O(x) = -1 = v_O(y).$$

If $\mathbb{F}_q(x) = \mathbb{F}_q(y)$, then $y$ can be written as

$$y = \frac{ax+b}{cx+d} \quad \text{where} \quad ad - bc \neq 0, a, b, c, d \in \mathbb{F}_q.$$

The valuations at the place $O$ are as the following:

$$v_O(ax+b) : \begin{cases} 0 & \text{if } a = 0 \\ -1 & \text{if } a \neq 0 \end{cases} \quad \text{and} \quad v_O(cx+d) : \begin{cases} 0 & \text{if } c = 0 \\ -1 & \text{if } c \neq 0. \end{cases}$$

Since the assumption $c \neq 0$ implies that $v_O(y) \geq 0$, we can write $y$ as

$$y = ax + b, \ a \neq 0.$$

Then $v_P(y) = -1$ and

$$(y)_\infty = P + O \Longrightarrow P = Q.$$

$\sigma$ is onto:
Let $E \subseteq F$ be a rational subfield of $F$ with $[F : E] = 2$. Denote by $O_E := O \cap E$ the rational place of $E$ over which $O$ lies. Let $z$ be an element of $E$ whose pole is $O_E$. Then one can choose $z$ as the defining element of $E$, i.e.

$$E = \mathbb{F}_q(z).$$

Then the degree of $z$ is

$$\deg(z) = [F : E] = 2,$$

which implies that there exists a rational place $P$ of $F$ such that the pole divisor of $z$ in $F$ is

$$(z)_\infty = O + P.$$

Thus we conclude that

$$E = \mathbb{F}_q(z) = \mathbb{F}_q(\mathcal{L}(O + P))$$
$$= \sigma(P).$$

□

**Example 5.0.8** *Let $q = \ell^2$ be a square and $H = \mathbb{F}_q(x, y)$ be the Hermitian function field given by the equation $y^\ell + y = x^{\ell+1}$. Then there are at least $\ell^3+1$ rational subfields $E \subseteq H$ with degree $[H : E] = \gamma(H)$. The kissing number of $\Lambda_{\mathcal{P}}$, where $\mathcal{P} = \mathbb{P}^1(H)$, satisfies the inequality*

$$\kappa(\Lambda_{\mathcal{P}}) \geq \ell^2(\ell^2 - 1)(\ell^3 + 1).$$

**Proof**: The gonality of $H$ is $\gamma(H) = \ell$ and the group $G$ of automorphisms of $H$ over $\mathbb{F}_q$ has order $\ell^3(\ell^2 - 1)(\ell^3 + 1)$ (see [13]). The degree of the extension $H/\mathbb{F}_q(x)$ is

$$[H : \mathbb{F}_q(x)] = \ell$$

and there are $\ell^3 + 1$ subfields of $H$ conjugate to $\mathbb{F}_q(x)$ under $G$. Thus, one obtains at least $\ell^3 + 1$ rational subfields $E$ of $H$ of degree $[H : E] = \ell$. The last assertion in the example follows from the fact that in each of these extensions $H/E$, there are exactly $\ell^2$ rational places which split completely in $H/E$. Applying Corollary 3.3.11 gives the result, which was also obtained in [3, Theorem 8.1], by a different method.

□

# Bibliography

[1] L. Ateş, H. Stichtenoth, *A note on short vectors in lattices from function fields*, Finite Fields Appl., **39** (2016), 264-271.

[2] A. Böttcher, L. Fukshansky, S.R. Garcia, H. Maharaj, *On lattices generated by finite Abelian groups*, SIAM Journal on Discrete Mathematics, **29** (2015), 382-404.

[3] A. Böttcher, L. Fukshansky, S.R. Garcia, H. Maharaj, *Lattices from Hermitian function fields*, J. Algebra, **447** (2016), 560-579.

[4] J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices, and groups*, 3rd Edition, Springer-Verlag, 1999.

[5] L. Fukshansky, H. Maharaj, *Lattices from elliptic curves over finite fields*, Finite Fields Appl., **28** (2014), 67-78.

[6] P.M. Gruber, C.G. Lekkerkerker, *Geometry of numbers*, 2nd Edition, North-Holland, Amsterdam, 1987.

[7] G. Hiss, *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups*, Indag. Math. (N.S.), **15** (2004), 223-243.

[8] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris, **305** (1987), 729-732.

[9] H.-G. Quebbemann, *Lattices from curves over finite fields*, 1989, unpublished manuscript.

[10] M.Y. Rosenbloom, M.A. Tsfasman, *Multiplicative lattices in global fields*, Invent. Math. **101** (1990), 687-696.

[11] M. Sha, *On the lattices from elliptic curves over finite fields*, Finite Fields Appl., **31** (2015), 84-107.

[12] J.H. Silverman, *The arithmetic of elliptic curves*, 2nd Edition, Springer-Verlag, 2009. Graduate Texts in Mathematics No. **106**.

[13] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, Teil II, Arch. Math. (Basel) **24** (1973), 615-631 (in German).

[14] H. Stichtenoth, *Algebraic function fields and codes*, $2^{\text{nd}}$ Edition, Springer-Verlag, 2009. Graduate Texts in Mathematics No. **254**.