Universiteit
Leiden
The Netherlands

Asymptotically good generalized algebraic geometry codes

Chang, H.P.

Citation
Chang, H. P. (2010). *Asymptotically good generalized algebraic geometry codes*.

Version:	Not Applicable (or Unknown)
License:	License to inclusion and publication of a Bachelor or Master thesis in the Leiden University Student Repository
Downloaded from:	https://hdl.handle.net/1887/3597446

Note: To cite this publication please use the final published version (if applicable).

Hilko Peter Chang

Asymptotically Good Generalized Algebraic Geometry Codes

Master thesis, defended on June 11 2010

Thesis advisor: Dr. R.S. de Jong

Mathematisch Instituut, Universiteit Leiden

Preface

In any form of electronic communication, errors can occur and hence there is a need to deal with them. Before error-correcting codes were used, only once a message had been received and could not be understood, one could conclude that errors had occurred. There was no way to resolve these errors other than asking for retransmission.

This changed when Claude Shannon in 1948 proved a theorem[1] which says that even with a noisy channel, there exist ways to encode messages in such a way that they have an arbitrarily good chance of being transmitted safely, provided that one does not exceed the capacity of the channel by trying to transmit too much information too quickly.

This theorem, which marks the start of coding theory, means that with long enough codes we can achieve communication that is as safe as we like. These codes do not have to be linear, and the proof does not construct them. All we know is that they exist. The main problem of coding theory is the construction of these error-correcting codes.

One of the first error-correcting codes was constructed at Bell Labs, by a mathematician named Richard Hamming. He became fed up with a computer which could detect errors in his input during weekend runs, but would then just dump the program, wasting the entire run. He devised ways to encode the input so that the computer could correct isolated errors and continue running, and his work led him to discover what are now called Hamming codes.

Soon after, Marcel Golay generalized Hamming's construction from binary codes to codes using an alphabet of p symbols for p prime. He also constructed two very remarkable codes that correct multiple errors and that now bear his name. However, it is a curious fact of history that one of the very same Golay codes appeared a few years earlier, in a Finnish magazine dedicated to betting on soccer games [2].

This ternary Golay code was first discovered by a Finn who was determining good strategies for betting on blocks of 11 soccer games. Here, one places a bet by predicting a win, lose, or tie for all 11 games, and as long as you do not miss more than two of them, you get a payoff. If a group gets together in a pool and makes multiple bets to cover all the options, so that no

[1] Shannon's theorem states that for any rate R strictly less than the capacity C of the channel and for any $\epsilon > 0$, there exists some code with a sufficiently large length and with rate at least R, such that the probability that an error will occur in the message is less than ϵ.

matter what the outcome, somebody's bet comes within 2 of the actual outcome, then the codewords of a 2-error-correcting perfect code provide a very nice option. The first discoverer of the ternary 'Golay' code, named Juhani Virtakallio, exhibited it merely as a good betting system for football-pools, and its 729 codewords appeared in the football-pool magazine Veikkaaja.

In 1960 Bose and Ray-Chaudhuri and independently Hocquenghem constructed BCH-codes. Ten years later a Russian mathematician Goppa generalized this construction and introduced Goppa codes. These codes are very interesting not only because they allow efficient decoding algorithms, but also because they have good parameters. They are constructed using algebraic curves and hence are also referred to as algebraic geometry codes. The application of algebraic geometry to coding theory is still an interesting topic for research as we will see in this work.

With the advent of digital computing technology the coding and decoding of error-correcting codes became more practical and hence the number of applications of error-correcting codes increased enormously. Perhaps the most familiar application is the spectacularly successful Compact Disc player, which uses Reed-Solomon codes to deliver dramatically clear and error-free sound by correcting errors that occur from dust and scratches. Reed-Solomon codes were also used by the Mariner spacecrafts to send pictures of the planet mars back to earth [5]. They used a (32,6,16) binary code, which means that 26 of every 32 bits sent were redundant, to compensate for the noise from deep-space . Nowadays error-correcting codes are used by satellites, cellular phones, computer hard drives and for almost any form of digital communication.

Summary

Most of the literature on algebraic geometry codes is written in the language of algebraic function fields. However, to get a good understanding of the theory, it is important to understand the relationship between algebraic function fields and algebraic curves. The first chapter contains the definitions and terminology of these two categories and describes the anti-equivalence between them. At the end of this chapter a result is deduced to count in how many places a place of an algebraic function field could split when the base field is extended, which will be used in the last chapter.

The second and third chapter are concerned with coding theory and result in the construction of an asymptotically good sequence of codes at the end of chapter three. The second chapter serves as a preparation for the third. First the standard terminology of coding theory is defined. Then the definition of a generalized algebraic geometry code is given and its properties are studied. At the end it is demonstrated how these codes generalize Goppa codes and Reed-Solomon codes.

The third chapter is about *sequences* of codes. To get an understanding of the challenges of coding theory, we take a look at lower and upper bounds for the rate and relative minimum distance of a sequence of codes. They tell

us that asymptotically good sequences exist and what the limits are of what can be done. We then study the first explicitly constructed asymptotically good sequence of codes and we see that the idea used there is reused at the end of the chapter to construct a more general sequence of asymptotically good codes.

In the final chapter we investigate different variations to the construction of the sequence of codes in chapter three, to see if it is possible to improve the lower bounds for the parameters of the code. The remainder of the chapter is inspired by a recent article (June 2009) [1] about towers of algebraic function fields. We show that asymptotically good sequences of codes can be easily constructed from an exact tower. This leads us to the question of how these exact towers can be constructed. We exhibit the construction of an exact tower of Artin-Schreier extensions and study its properties in detail. Finally we then use this tower to prove that for any given integer m, we can construct a tower for which throughout the tower the number of places of degree m is relatively high compared to the genus.

Acknowledgements

First of all, I am grateful to my advisor Dr. Robin de Jong. His detailed explanations and answers to all the questions that I asked on our regular meetings were extremely helpful and kept me motivated throughout the whole process. I thank him for pointing out many valuable references, for thoroughly reading this text and for making numerous corrections and suggestions, thereby greatly improving the quality of this work.

I also wish to thank Prof. Dr. Bas Edixhoven for his useful comments and Prof. Dr. Ronald Cramer for reading this thesis.

Leiden, May 2010 *H. P. Chang*

Contents

Chapter 1

An Anti-equivalence of Categories

In this chapter we fix a field k. In most applications k will be a finite field $\mathbf{F}_q$ of q elements, where q is a prime power. We define two categories, using this field k. After this we will show that these two categories are anti-equivalent. We end this chapter with some results on the Galois action on places.

1.1 The Category of Algebraic Function Fields

We define the objects in this category as in [10] p.1-2. The objects are called algebraic function fields.

1.1.1 Algebraic Function Fields

Definition 1.1 An *algebraic function field F/k of one variable over k* is an extension field $F \supseteq k$ such that F is a finite algebraic extension of $k(x)$ for some element $x \in F$ wich is transcendental over k.

The set $\tilde{k} = \{z \in F \mid z \text{ is algebraic over } k\}$ is a subfield of F called the *field of constants* of F/k. We have $k \subseteq \tilde{k} \subset F$, and $F/\tilde{k}$ is a function field over $\tilde{k}$. We say that k is algebraically closed in F, or k is the *full constant field* of F, if $k = \tilde{k}$.

The simplest example of a function field is the rational function field $F = k(x)$, for some $x \in F$ which is transcendental over k. An arbitrary function field F/k is often represented as a simple algebraic field extension of a rational function field $k(x)$. For example $F = k(x, y)$ where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in k(x)[T]$.

1.1.2 Morphisms between Function Fields

Let F/k and F'/k be two algebraic function fields. Since both function fields contain the field k, we can consider them as k-algebras.

Definition 1.2 A morphism $\varphi : F/k \to F'/k$ between two algebraic function fields is a k-algebra homomorphism.

In other words, φ is a ring homomorphism that is the identity map on k. Since it is a ring homomorphism between fields, its kernel is zero and therefore it is injective. Hence we can view morphisms between function fields as inclusions.

1.1.3 Places and Divisors

Definition 1.3 Let F be a function field over k. A *valuation ring* $\mathcal{O}$ of F/k is a ring $k \subset \mathcal{O} \subset F$ with the property that for all $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

If $\mathcal{O} \neq F$ we call $\mathcal{O}$ a *discrete valuation ring.*

Note that for any valuation ring the inclusion $k \subset \mathcal{O}$ cannot be an equality. The field F itself is trivially a valuation ring.

Definition 1.4 A *discrete valuation* of F/k is a function $v : F \to \mathbf{Z} \cup \{\infty\}$ with the following properties:

(1) $v(x) = \infty \iff x = 0$.

(2) $v(xy) = v(x) + v(y)$ for any $x, y \in F$.

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$.

(4) There exists an element $z \in F$ with $v(z) = 1$.

(5) $v(a) = 0$ for any $a \in k \setminus \{0\}$.

A function $v : F \to \mathbf{Z} \cup \{\infty\}$ satisfying properties (1),(2),(3) and (5) is called a *valuation.*

The third property in the above definition is called the triangle inequality. Discrete valuations verify another property called the strict triangle inequality.

Lemma 1.5 (Strict Triangle Inequality) *Let v be a discrete valuation of F/k and $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x + y) = \min\{v(x), v(y)\}$.*

Proof For $a \in k \setminus \{0\}$ we have $v(ay) = v(y)$ by property (2) and (5), in particular $v(-y) = v(y)$. Since $v(x) \neq v(y)$ we can assume $v(x) < v(y)$. Suppose that $v(x + y) \neq \min\{v(x), v(y)\}$, so $v(x + y) > v(x)$ by (3), and we obtain $v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x)$, a contradiction. □

Proposition 1.6 *Let $\mathcal{O}$ be a discrete valuation ring of a function field F/k. The following are true.*

- *$\mathcal{O}$ is a local ring and hence has a unique maximal ideal P.*
- *$\mathcal{O}$ is a principal ideal domain with fraction field F.*

- *Let $t \in \mathcal{O}$ be such that $P = t\mathcal{O}$. Then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbf{Z}$ and $u \in \mathcal{O}^*$.*

There are natural bijections between the set of discrete valuation rings of F/k, the set consisting of their maximal ideals and the set of discrete valuations on F/k. In this correspondence a discrete valuation ring $\mathcal{O}$ is mapped to its maximal ideal P. We will often write $\mathcal{O}_P$ instead of $\mathcal{O}$. By the above Proposition P is a principal ideal. A generator $t \in \mathcal{O}_P$ of the maximal ideal P is called a *local coordinate* or *uniformizing parameter* or *local parameter* at P. Since any $0 \neq z \in F$ has a representation of the form $z = t^n u$, we can define a valuation v_P corresponding to P by setting $v_P(0) = \infty$ and $v_P(z) = v_P(t^n u) = n$. This is well defined by the third property of Proposition 1.6. From this discrete valuation we find $\mathcal{O}_P$ and P back via the equations

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

The valuation ring $\mathcal{O} = F$ has maximal ideal (0) and corresponds to the valuation $v_0 : F \to \mathbf{Z} \cup \{\infty\}$ given by $v_0(z) = 0$ for $z \in F^*$ and $v_0(0) = \infty$. Note that v_0 verifies all properties of a discrete valuation except property (4). The valuation v_0 also verifies the strict triangle inequality.

Definition 1.7 A *place* P of a function field F is the maximal ideal of some discrete valuation ring $\mathcal{O}_P \subset F$. We will also use the word place to indicate its corresponding valuation v_P, or discrete valuation ring $\mathcal{O}_P$.

The *residue class field* of a place P is the field $F_P := \mathcal{O}_P/P$, sometimes denoted as $k(P)$. It is a finite field extension of k. If $z \in \mathcal{O}_P$ we write $z(P)$ for the residue class of $z + P \in F_P$. The *degree* of P is $\deg P = [F_P : k]$.

Example 1.8 We take $k = \mathbf{F}_q$, $F = \mathbf{F}_q(X)$ and let P be the place corresponding to an irreducible polynomial $P(X) \in \mathbf{F}_q[X]$. This means the valuation ring of P is the ring $\mathcal{O}_P = \mathbf{F}_q[X]_{P(X)}$ i.e. the ring $\mathbf{F}_q[X]$ localized at the prime ideal generated by $P(X)$. The polynomial $P(X)$ is a local coordinate for $\mathcal{O}_P$. The valuation v_P counts the number of factors $P(X)$ occuring in any given element. If $z \in F^*$ and $v_P(z) = n$ this means that $z = uP(X)^n$ for some unit u of $\mathcal{O}_P$.

The residue class field $F_P = \mathcal{O}_P/P = \mathbf{F}_q[X]_{P(X)}/(P(X))$ is isomorphic to $\mathbf{F}_q[X]/(P(X))$. Therefore its degree is equal to the degree of the polynomial $P(X)$. Let α be a zero of $P(X)$ in some algebraic closure of $\mathbf{F}_q$. Then F_P is isomorphic to $\mathbf{F}_q(\alpha)$. This isomorphism maps $\bar{X}$ to α and for any $z \in \mathcal{O}_P$, $z(P)$ is mapped to $z(\alpha)$. Hence we can interpret the residue class map as evaluation at a chosen zero of $P(X)$.

Definition 1.9 The *divisor group* of a function field F/k is the additively written free abelian group which is generated by the places of F/k and is denoted by $\mathcal{D}_F$. The elements of $\mathcal{D}_F$ are called *divisors* of F/k.

Let $\mathbf{P}_F$ be the set of places of F/k. We can write a divisor $D \in \mathcal{D}_F$ as a formal sum

$$D = \sum_{P \in \mathbf{P}_F} n_P P \qquad \text{with } n_P \in \mathbf{Z}, \quad \text{almost all } n_P = 0.$$

A divisor of the form $D = P$ with $P \in \mathbf{P}_F$ is called a *prime divisor*. The group $\mathcal{D}_F$ is generated by the set of prime divisors. Addition in $\mathcal{D}_F$ is defined coefficient-wise. If $D = \sum_{P \in \mathbf{P}_F} n_P P$ and $D' = \sum_{P \in \mathbf{P}_F} n'_P P$, then

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

The zero element of the group $\mathcal{D}_F$ is the divisor $0 = \sum_{P \in \mathbf{P}_F} n_P P$ with $n_P = 0$ for all P. For $Q \in \mathbf{P}_F$ and $D = \sum_{P \in \mathbf{P}_F} n_P P \in \mathcal{D}_F$ we define $v_Q(D) = n_Q$. This allows us to write

$$D = \sum_{P \in \mathbf{P}_F} v_P(D) P.$$

There is a partial ordering on $\mathcal{D}_F$ given by

$$D_1 \leq D_2 \qquad \Longleftrightarrow \qquad v_P(D_1) \leq v_P(D_2) \quad \text{for all } P \in \mathbf{P}_F.$$

There is a homomorphism $\deg : \mathcal{D}_F \to \mathbf{Z}$ defined by

$$\deg D = \sum_{P \in \mathbf{P}_F} v_P(D) \cdot \deg P.$$

$\deg D$ is called the degree of the divisor D.

Definition 1.10 For a divisor $G \in \mathcal{D}_F$ we define the *Riemann-Roch* space

$$\mathcal{L}(G) = \{z \in F^* \mid v_P(z) \geq -v_P(G) \text{ for all } P \in \mathbf{P}_F\} \cup \{0\}.$$

It is a finite dimensional vectorspace over k.

Example 1.11 Let us calculate the vector space $\mathcal{L}(G)$ for a specific function field F/k and divisor G. We take $k = \mathbf{F}_q$, $F = \mathbf{F}_q(X)$ and $G = P$, where P is the place corresponding to an irreducible polynomial $P(X) \in \mathbf{F}_q[X]$ of degree $d > 0$. Now $\mathcal{L}(G) = \{z \in F^* \mid v_Q(z) \geq -v_Q(G) \text{ for all } Q \in \mathbf{P}_F\} \cup \{0\}$. Because $v_P(G) = 1$ and $v_Q(G) = 0$ for all other places Q, we find that

$$\mathcal{L}(G) = \{z \in F^* \mid v_P(z) \geq -1 \text{ and } v_Q(z) \geq 0 \text{ for all other } Q \in \mathbf{P}_F\} \cup \{0\}.$$

This means that if $z \in \mathcal{L}(G)$ is equal to $z = \frac{f(X)}{g(X)}$ with f, g coprime polynomials in $\mathbf{F}_q[X]$, then up to a scalar in $\mathbf{F}_q^*$, $g(X)$ must be equal to $P(X)$ or 1. The numerator f may be any polynomial of degree less than or equal to d. This is to ensure that $v_\infty(z) = \deg P(X) - \deg f$ is nonnegative. A basis for $\mathcal{L}(G)$ as vector space over $\mathbf{F}_q$ is the set $\{z_0, z_1, \ldots, z_d\}$ with $z_i = \frac{X^i}{P(X)}$.

Let P be a place and t_P a local coordinate for $\mathcal{O}_P$. There is a chain of fractional ideals, extended by the ideals (0) and F

$$(0) \subset \ldots \subset t_P^2\mathcal{O}_P \subset t_P\mathcal{O}_P \subset \mathcal{O}_P \subset t_P^{-1}\mathcal{O}_P \subset t_P^{-2}\mathcal{O}_P \subset \ldots \subset F.$$

For any $z \in F$ and integer n, the condition $v_P(z) \geq n$ is equivalent to $z \in t_P^n\mathcal{O}_P$. Let G be a divisor and define $G_P = v_P(G)$. We can now express $\mathcal{L}(G)$ as an intersection of fractional ideals. If $z \in \mathcal{L}(G)$, then for all places P, $v_P(z) \geq -v_P(G) = -G_P$. Therefore $z \in t_P^{-G_P}\mathcal{O}_P$ for all P. So we conclude that

$$\mathcal{L}(G) = \bigcap_{P \in \mathbf{P}_F} t_P^{-G_P}\mathcal{O}_P.$$

Proposition 1.12 *There is a constant $\gamma \in \mathbf{Z}$ such that for all divisors $G \in \mathcal{D}_F$,*

$$\deg G - \dim \mathcal{L}(G) \leq \gamma.$$

This is Proposition I.4.14 in [10]. It ensures us that we can make the following definition.

Definition 1.13 The *genus* g of a function field F/k is defined as

$$g = \max\{\deg G - \dim \mathcal{L}(G) + 1 \mid G \in \mathcal{D}_F\}.$$

The genus is an important invariant of the function field F/k and it is always a nonnegative integer.

Theorem 1.14 *Let F/k be a function field of genus g. For any divisor $G \in \mathcal{D}_F$,*

$$\dim \mathcal{L}(G) \geq \deg G - g + 1.$$

If $G \in \mathcal{D}_F$ is a divisor of degree $\deg G \geq 2g - 1$, then

$$\dim \mathcal{L}(G) = \deg G - g + 1.$$

The first part of the theorem follows directly from the definition of the genus. The second part is a consequence of the Riemann-Roch Theorem. The bound $2g - 1$ is the best possible bound i.e. there always exists a divisor W with $\deg W = 2g - 2$ and $\dim \mathcal{L}(W) = g > (2g - 2) + 1 - g = g = \deg W + 1 - g$.

1.2 The Category of Normal Projective Curves

We define the objects and morphisms in this category following chapter 2 in [4] and chapter 2.3 in [7]. The objects are normal projective curves.

1.2.1 Projective Curves

Definition 1.15 A topological space X is called *irreducible*, if it cannot be expressed as the union $X = X_1 \cup X_2$ of two proper subsets, each one of which is closed in X. The empty set is not irreducible.

The *Krull dimension* of a topological space X, denoted $\dim X$ is the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ of distinct irreducible closed subsets of X. Note that Z_0 is not the empty set.

Definition 1.16 Let $B = \bigoplus_{i \geq 0} B_i$ be a graded ring. We define Proj B as the set of homogeneous prime ideals of B that do not contain the ideal $B_+ = \bigoplus_{d>0} B_d$. For $f \in B$ we define $B_{(f)}$ as the set of elements of degree zero in B_f. So $B_{(f)} = \{\frac{a}{f^N} \in B_f \mid a \in B_{N \cdot \deg(f)}\}$. The space Proj B has a basis of open sets of the form $D_+(f) = \{\mathfrak{p} \in \text{Proj } B \mid f \notin \mathfrak{p}\}$. We have that $D_+(f) \simeq \text{Spec } B_{(f)}$, and $\mathcal{O}_{\text{Proj } B}(D_+(f)) = B_{(f)}$. So Proj B has a covering by affine open subsets. This covering gives Proj B the structure of a scheme.

Definition 1.17 We define $\mathbf{P}^n_k = \text{Proj } k[x_0, \ldots, x_n]$ and call this scheme the n-dimensional projective space over k.

A projective scheme over k is a scheme over k that is isomorphic as scheme over k, to a closed subscheme of $\mathbf{P}^n_k$ for some $n \geq 0$.

If I is a homogeneous ideal of $k[x_0, \ldots, x_n]$, then we can view $B = k[x_0, \ldots, x_n]/I$ as a graded ring in a natural way. It is shown in [7] that projective schemes over k can be characterized as follows.

Theorem 1.18 *Every nonempty projective scheme over k is of the form* Proj $k[x_0, \ldots, x_n]/I$ *for some homogeneous ideal I that does not contain the ideal $(x_0, \ldots, x_n)$ and for some $n \geq 0$.*

Definition 1.19 A projective curve over k is a one dimensional irreducible projective scheme over k.

Normal Curves

Definition 1.20 Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $L = A/\mathfrak{m}$. The ring A is a *regular local ring* if $\dim_L \mathfrak{m}/\mathfrak{m}^2 = \dim A$.

Definition 1.21 Let X be a projective curve. We say X is *regular* or *non-singular* at a point $P \in X$ if the local ring $\mathcal{O}_{X,P}$ is a regular local ring. A curve is *regular* if it is regular at every point. A curve is *singular* if it is not regular.

Definition 1.22 Let X be a scheme. Then X is *integral* if and only if $\mathcal{O}_X(U)$ is an integral domain for every nonempty open subset U of X.

This is Proposition 4.17 in Chapter 2 of [7] which we use here as a definition of integral scheme.

Let us recall that an integral domain is called *normal* if it is integrally closed in its fraction field.

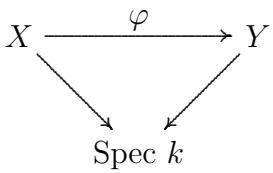
Definition 1.23 Let X be an integral scheme. We say that X is *normal at* $x \in X$ if $\mathcal{O}_{X,x}$ is normal. We say that X is normal if it is irreducible and normal at all of its points.

1.2.2 Morphisms between Curves

Definition 1.24 Let X and Y be projective curves over k. A *morphism* $\varphi : X \to Y$ is a morphism of schemes over k.

Recall that a morphism of schemes consists of a continuous map φ between the topological spaces of X and Y and a morphism $\varphi^{\#}$ of sheaves on Y, from the structure sheaf of Y to the direct image of the structure sheaf of X under φ. That is $\varphi^{\#} : \mathcal{O}_Y \to \varphi_* \mathcal{O}_X$.

Recall that a morphism of schemes over k is a morphism of schemes that is compatible with the structure morphisms. In other words a morphism of schemes $\varphi : X \to Y$ is a morphism of schemes over k if and only if the following diagram commutes.



We call a morphism $\varphi : X \to Y$ *dominant* if its image is dense in Y, i.e. if $\overline{\mathrm{Im}(\varphi)} = Y$. For projective curves this is the same as saying that φ is surjective.

1.3 Anti-equivalence of categories

In this section we will define two contravariant functors between the category of algebraic function fields and the category of normal projective curves. First we define these functors in general. Later we will see that the restrictions of these two functors to function fields in which the constant field is algebraically closed and to curves that are geometrically irreducible will be an anti-equivalence. We start by giving a contravariant functor K that assigns an algebraic function field $K(X)$ to every normal projective curve X.

1.3.1 The function field of a projective curve

Let X be a normal projective curve. Let ξ be the generic point of X. We define the functor K by

$$K(X) = \mathcal{O}_{X,\xi} = \{\langle U, f\rangle \mid \emptyset \neq U \subset X \text{ open}, f \in \mathcal{O}_X(U)\}/\sim .$$

Here $\sim$ is defined by $\langle U, f\rangle \sim \langle V, g\rangle$ if $f = g$ on $U \cap V$. Addition and multiplication of two pairs is defined pointwise.

Now we need to verify that $K(X)$ is an algebraic function field. First we can check that $K(X)$ is indeed a field. For $\langle U, f\rangle \in K(X)$, with $f \neq 0$, the set $V = U \setminus Z(f)$ is open in X and nonempty. Here $1/f$ is defined and regular on V and hence $\langle V, 1/f\rangle$ is an inverse for $\langle U, f\rangle$.

It is clear that $K(X)$ contains the field k as the set of all constant functions $\langle X, a\rangle,\ a \in k$. From Theorem 3.2 d) in [4] we know that $K(X)$ is a finitely generated extension field of k of transcendence degree one, hence an algebraic function field.

Next we need to define what the functor K does with morphisms. Let $\varphi : X \to Y$ be a dominant morphism between two normal projective curves and let η and ξ be the generic points of Y and X respectively. We need to give a k-algebra homomorphism $K(\varphi) : K(Y) = \mathcal{O}_{Y,\eta} \to K(X) = \mathcal{O}_{X,\xi}$. Let $\langle V, f\rangle \in \mathcal{O}_{Y,\eta}$. There is an inclusion $\mathcal{O}_Y(V) \subset \mathcal{O}_{Y,\eta}$ and a ring homomorphism $\varphi^{\#}(V) : \mathcal{O}_Y(V) \to \varphi_*\mathcal{O}_X(V) = \mathcal{O}_X(\varphi^{-1}(V))$. Now $f \in \mathcal{O}_Y(V)$ and hence $\varphi^{\#}(V)(f) \in \mathcal{O}_X(\varphi^{-1}(V)) \subset \mathcal{O}_{X,\xi}$. So we can define $K(\varphi) : \mathcal{O}_{Y,\eta} \to \mathcal{O}_{X,\xi}$ as follows

$$K(\varphi) : \langle V, f\rangle \longmapsto \langle \varphi^{-1}(V), \varphi^{\#}(V)(f)\rangle.$$

Note that $\varphi^{-1}(V)$ is an open set in X, because φ is continuous and $\phi^{-1}(V)$ is not empty because ϕ is dominant. For every open set V of Y the map $\varphi^{\#}(V)$ is a ring homomorphism, therefore $K(\varphi)$ is a ring homomorphism. Since $k = \mathcal{O}_Y(Y) = \mathcal{O}_X(\varphi^{-1}(Y))$ the map $K(\varphi)$ is the identity on k and hence is a k-algebra homomorphism.

We verify that K is functorial. It is clear that $K(\mathrm{id}_X) = \mathrm{id}_{K(X)}$. Now let $\psi : X \to Y$ and $\varphi : Y \to Z$ be two morphisms between normal projective curves and let $\langle W, f\rangle \in K(Z)$. Then

$$\begin{aligned} K(\psi) \circ K(\varphi)(\langle W, f\rangle) &= K(\psi)(\langle \varphi^{-1}(W), \varphi^{\#}(W)(f)\rangle) = \\ &\langle \psi^{-1}\varphi^{-1}(W), \psi^{\#}(\varphi^{-1}(W))(\varphi^{\#}(W)(f))\rangle = \\ &\langle (\varphi \circ \psi)^{-1}(W), (\varphi \circ \psi)^{\#}(W)(f)\rangle = K(\varphi \circ \psi)(\langle W, f\rangle). \end{aligned}$$

We conclude that K is functorial.

1.3.2 The curve associated to a function field

Before we give a contravariant functor L in the other direction, that assigns a normal projective curve $L(F)$ to every algebraic function field F, we give two definitions.

Recall that a ring homomorphism $f : A \to B$ is called *integral* if B is integral over the subring $f(A)$.

Definition 1.25 We say that a morphism $\pi : X' \to X$ between two schemes X' and X is *integral* if for every affine open subset U of X, $f^{-1}(U)$ is affine and $\mathcal{O}_X(U) \to \mathcal{O}_{X'}(f^{-1}(U))$ is integral[1].

Definition 1.26 Let X be an integral scheme, and let F be an algebraic extension of the function field $K(X)$. We define the *normalization of* X *in* F to be an integral morphism $\pi : X' \to X$ with X' normal, $K(X') = F$ and such that π extends the canonical morphism $\operatorname{Spec} F \to X$.

It is shown in [7] Ch. 4.1 that the normalization $\pi : X' \to X$ of X in F exists and is unique up to isomorphism. If furthermore $K(X) \subset F$ is finite and separable, then the normalization is a finite morphism.

We are going to define the functor L using Definition 1.26. Let F/k be an algebraic function field. By definition 1.1, F/k is a finite algebraic extension of the rational function field. We know that the function field $K(\mathbf{P}^1_k)$ of the projective line $\mathbf{P}^1_k$ is rational. Now we define the functor L by taking $L(F)$ to be the normalization of $\mathbf{P}^1_k$ in F, see the diagram below. Then $K(L(F)) = F$ and $L(F)$ is normal. It is shown in [7] that $L(F)$ is also projective, irreducible and one dimensional.

$$\begin{array}{ccc} L(F) = X' & \overset{\pi}{\dashrightarrow} & X = \mathbf{P}^1_k \\ \uparrow & & \uparrow \\ \operatorname{Spec} F & \longrightarrow & \operatorname{Spec} K(X) \end{array}$$

Next we need to define what the functor L does with morphisms. Let $f : G/k \to F/k$ be a k-algebra homomorphism. We define the morphism $L(f) : L(F) \to L(G)$ to be the normalization map π in definition 1.26, where we take $X = L(G)$, hence $K(X) = G$ and $X' = L(F)$.

Let $\pi_F : L(F) \to \mathbf{P}^1_k$ and $\pi_G : L(G) \to \mathbf{P}^1_k$ be the normalizations of $\mathbf{P}^1$ in F and G respectively. Then $L(f)$ is the morphism such that $\pi_F \circ L(f) = \pi_G$, i.e. the following diagram commutes.

$$\begin{array}{ccc} L(F) & \overset{L(f)}{\dashrightarrow} & L(G) \\ & {\scriptstyle \pi_F} \searrow \quad \swarrow {\scriptstyle \pi_G} & \\ & \mathbf{P}^1_k & \end{array}$$

The commutativity of this diagram follows from the definition of normalization and is analogous to the fact that taking integral closures of a ring in the tower of fields $K(\mathbf{P}^1) \subset G \subset F$ is transitive. In the next paragraphs we describe more explicitly what the functor L does.

[1] Note that there are at least three different notions of *integral*. One can speak of an integral *scheme*, an integral *ring homomorphism* and of an integral *morphism* between schemes.

The topological space

We can identify the topological space of $L(F)$ with the set of valuation rings of F that contain k. The field F itself is trivially a valuation ring over k. This valuation ring is the generic point of $L(F)$. The other valuation rings $k \subsetneq \mathcal{O}_P \subsetneq F$ are subrings of F and are *discrete* valuation rings. The subset of discrete valuation rings forms the set $L(F)^0$ of closed points of $L(F)$. We give this subset the cofinite topology. This is the topology where the closed sets are exactly the finite sets and the whole space. So the closed sets of $L(F)$ are finite subsets of $L(F)^0$ of discrete valuation rings and the whole space. Therefore the only closed set that contains the generic point is the whole space $L(F)$. So the generic point is dense.

It is clear that a finite closed set in this space is irreducible if and only if it consists of a single point. The whole space $L(F)$ is irreducible. For if $L(F)$ were reducible it could be expressed as the union of two finite sets and would be finite. This gives a contradiction with Corollary I.3.2 in [10], which states that any function field has infinitely many places. For function fields defined over an infinite field it is clear that they have infinitely many places. If F/k is a function field with $k = \mathbf{F}_q$ finite, we can see this as follows. The field F is an extension of the rational function field $\mathbf{F}_q(X)$. Every place in $\mathbf{F}_q(X)$ has at least one extension in F, so we only need to show that $\mathbf{F}_q(X)$ has infinitely many places. Every irreducible polynomial in $\mathbf{F}_q[X]$ corresponds to a place and for any integer $d \geq 1$ there exists an irreducible polynomial of degree d. Therefore $\mathbf{F}_q(X)$ and hence any function field has infinitely many places.

We have a chain $Z_0 \subset L(F)$, where Z_0 is a single place. The only set smaller than Z_0 is the empty set, which is not irreducible. Any closed subset in between Z_0 and $L(F)$ is finite and has more than one place and is therefore not irreducible. We conclude that the dimension of $L(F)$ is one.

The structure sheaf

The structure sheaf $\mathcal{O}_{L(F)}$ of $L(F)$ looks like this. Let $\mathcal{O}_P \subset F$ be a discrete valuation ring, corresponding to a closed point P of $L(F)$. Then we take $\mathcal{O}_{L(F),P}$ to be $\mathcal{O}_P$ and for the generic point ξ corresponding to the valuation ring F we have $\mathcal{O}_{L(F),\xi} = F$. For every nonempty open subset $U \subset L(F)$, we take $\mathcal{O}_{L(F)}(U) = \cap_{P \in U} \mathcal{O}_{L(F),P}$. This is a sheaf and gives $L(F)$ the structure of a locally ringed topological space. By definition $\mathcal{O}_{L(F),P}$ is normal for every place P, so the resulting scheme is normal.

The associated morphisms

Next we give a description of what the functor L does with morphisms. Let $f : F/k \to F'/k$ be a morphism between two algebraic function fields. The morphism $L(f)$ must map places to places. Let P' be a place of F'. Then P' is the maximal ideal of some discrete valuation ring $\mathcal{O}_{P'} \subset F'$. The morphism of projective curves $L(f) : L(F') \to L(F)$ is given by $L(f)(P') = f^{-1}(P')$.

We see that L is a contravariant functor. The set $f^{-1}(P')$ is a maximal ideal of a discrete valuation ring in F and so it is a place of F. If we consider F as a subfield of F', then f is just the inclusion $F \subset F'$ and $f^{-1}(P') = P' \cap F$. Every place P of F is covered by a place of F' in this way, so $L(f)$ is surjective. In other words, the functor L maps k-algebra homomorphisms to dominant rational maps.

Remark 1.27 A normal locally Noetherian scheme is regular at all points of codimension ≤ 1. Since for a curve all points have codimension ≤ 1, it follows that a normal locally Noetherian[2] curve is regular. Conversely, any regular scheme is normal. We conclude that a curve over a field is normal if and only if it is regular.

1.3.3 Geometrically irreducible curves

The two functors K and L just described give a correspondence between the two categories. Function fields F over k can have the property that k is the full constant field of F. One might ask if there is a corresponding property for projective curves such that the correspondence lets curves with this property correspond to function fields in which k is algebraically closed.

Let X be a normal projective curve over k and let L/k be a field extension of k. The inclusion $k \subset L$ induces a morphism Spec $L \to$ Spec k. We can use this to make a base change from X to $X_L := X \times_k$ Spec L. There are projections $\rho : X_L \to X$ and $X_L \to$ Spec L. The last one gives X_L the structure of an L-scheme. There is an easy interpretation of X_L. It is the curve that is defined as the curve X except with k replaced by the larger base field L. For example if X is a curve and $U \subset X$ is a nonempty affine open subset with affine coordinate ring $A(U)$, then $A(U) \otimes_k L$ is isomorphic to the affine coordinate ring of an open subset in X_L. At the level of function fields we have that if $F/k = K(X)$ is the function field of F, then the function field of X_L is FL/L, the compositum of F and L considered as a function field over L. If we are given X explicitly as $X =$ Proj $k[x_0, \ldots, x_n]/I$ then $X_L =$ Proj $L[x_0, \ldots, x_n]/I'$, where $I' = IL[x_0, \ldots, x_n]$.

Definition 1.28 Let $\bar{k}$ be an algebraic closure of k. Let X be a projective curve over k. We say that X is *geometrically irreducible* if $X_{\bar{k}}$ is irreducible.

Proposition 1.29 *Let k be a perfect field. A curve X over k is geometrically irreducible if and only if k is the full constant field of $K(X)$.*

Proof For a perfect field k every algebraic extension is separable. Therefore the separable closure k^s is equal to the algebraic closure $\bar{k}$. The result now follows from Ch.4 Corollary 2.14 (d) in [7]. □

Instead of providing all the details of the proof, let us look at some examples. The first one demonstrates that if k is not the full constant field of $K(X)$, then X over k is not geometrically irreducible.

[2] A scheme of finite type over a field is Noetherian.

Example 1.30 Let $k = \mathbf{R}$ and $F = \mathbf{C}(X)$. Then $F \cong \mathbf{R}(X)[Y]/(Y^2+1)$ is clearly a finite algebraic extension of $\mathbf{R}(X)$, so it is a function field over $\mathbf{R}$. The field $\mathbf{R}$ is not the full constant field of F, since i with $i^2 = -1$, in $\mathbf{C}(X)$ is algebraic over $\mathbf{R}$. Let $X = L(F)$ be the corresponding projective curve. Now we wish to show that X is not geometrically irreducible.
The curve X contains an affine subset U such that $U = \text{Spec } \mathbf{R}[X,Y]/(Y^2+1)$ and therefore $U_{\mathbf{C}} = \text{Spec } \mathbf{R}[X,Y]/(Y^2+1) \otimes_{\mathbf{R}} \mathbf{C} = \text{Spec } \mathbf{C}[X,Y]/(Y^2+1) = \text{Spec } \mathbf{C}[X,Y]/(Y+i)(Y-i)$.

The closure of the prime ideal $(Y+i) \in U_{\mathbf{C}}$ is the set $\{(X-\alpha, Y+i) \mid \alpha \in \mathbf{C}\}$ and is isomorphic to the affine line $\mathbf{A}^1_{\mathbf{C}}$. We see that $X_{\mathbf{C}}$ is the disjoint union of two copies of $\mathbf{A}^1_{\mathbf{C}}$ and hence is reducible. Therefore X is not geometrically irreducible.

The next example suggests that if X is not geometrically irreducible, then k is not algebraically closed in $K(X)$.

Example 1.31 Let $k = \mathbf{Q}$ and let $X = \text{Proj } \mathbf{Q}[X,Y,Z]/(Y^2 - 2X^2)$. The ideal (Y^2-2X^2) is a homogeneous prime ideal, so X is irreducible. However, X is not geometrically irreducible, since (Y^2-2X^2) factors as $(Y-\sqrt{2}X)(Y+\sqrt{2}X)$ over the algebraic closure of $\mathbf{Q}$.

We find the function field $K(X)$ by setting $Z = 1$ and then taking the fraction field, so $K(X) = \mathbf{Q}(X,Y)/(Y^2-2X^2)$. In $K(X)$ we have for $t = \frac{Y}{X}$ the relation $t^2 = 2$ and hence $K(X) = \mathbf{Q}(X,tX) = \mathbf{Q}(X,t) \cong \mathbf{Q}(\sqrt{2},X)$. The function t is algebraic over $\mathbf{Q}$ and $t \notin \mathbf{Q}$, so $\mathbf{Q}$ is not the full constant field of $K(X)$.

The result of Proposition 1.29 can be made more general.

Theorem 1.32 *Let k be a perfect field and $\bar{k}$ an algebraic closure of k. Let X be an integral projective curve over k and let L/k be the full constant field of $K(X)$ over k. Then the number of irreducible components of $X_{\bar{k}}$ is equal to the degree $[L:k]$.*

Instead of a proof, we illustrate this phenomenon with an example.

Example 1.33 Let $k = \mathbf{Q}$ and $A = \mathbf{Q}[X,Y]/(X^3-2Y^3)$ and $X = \text{Spec } A$. Because $X^3 - 2Y^3$ is irreducible in $\mathbf{Q}[X,Y]$, A is a domain. We have X irreducible and $K(X) = \text{Frac}(A)$. We calculate the base change to the base field $\mathbf{C}$.

$$X_{\mathbf{C}} = \text{Spec } A \otimes_{\mathbf{Q}} \mathbf{C} = \text{Spec } \mathbf{C}[X,Y]/(X^3-2Y^3) = \\ \text{Spec } \mathbf{C}[X,Y]/(X-\alpha)(X-\zeta\alpha)(X-\zeta^2\alpha),$$

where α satisfies $\alpha^3 = 2Y$ and ζ is a primitive third root of unity, i.e. $\zeta^2 + \zeta + 1 = 0$. Note that $A \otimes_{\mathbf{Q}} \mathbf{C}$ is not a domain and hence does not have a field of fractions. We see that the curve $X_{\mathbf{C}}$ has three irreducible components corresponding to the three irreducible factors $(X-\alpha), (X-\zeta\alpha), (X-\zeta^2\alpha)$ of (X^3-2Y^3). The function field $K(X)$ is isomorphic to $\mathbf{Q}(\sqrt[3]{2})(Y)$, because

the rational function $\frac{X}{Y} \in K(X)$ satisfies $(\frac{X}{Y})^3 = 2$. It is now clear that the full constant field of $K(X)$ is $L = \mathbf{Q}(\sqrt[3]{2})$. This is consistent with the theorem, since $[L : k] = [\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ is equal to the number of irreducible components of $X_{\mathbf{C}}$.

Theorem 1.34 *The functors K and L give an anti-equivalence between the category of normal projective geometrically irreducible curves over k and algebraic function fields over k with full constant field k.*

Proof We need to show that the composition functors $L \circ K$ and $K \circ L$ are each isomorphic to the identity functor.

It is clear from Proposition 1.29 that K maps a geometrically irreducible curve X over k to a function field with full constant field k. After applying L again to this function field we get again a projective curve. Since L is defined using Definition 1.26 this curve normal. Furthermore by Proposition 1.29 $L(K(X))$ is also geometrically irreducible. So $L(K(X))$ is just like X a normal projective geometrically irreducible curve with function field $K(X)$. Moreover, $L(K(X))$ is uniquely determined by $K(X)$ up to isomorphism and therefore $L(K(X))$ is isomorphic to X.

On the other hand, by Definition 1.26 and the definition of L we have $K(L(F)) = F$ for any algebraic function field F. We conclude that $L \circ K$ is isomorphic to the identity functor and $K \circ L$ is the identity functor. □

1.4 Galois action on places

Definition 1.35 Let X be a normal projective curve over k and let L/k be a field extension of k. Let $\rho : X_L \to X$ be the projection on X. Let $x \in X$ and $y \in X_L$. We say that y extends x if $\rho(y) = x$.
In the context of function fields let $F = K(X)$ and let $F' = K(X_L) = LF$. If $\mathcal{O}_y \subset F'$ and $\mathcal{O}_x \subset F$ are places, we say $\mathcal{O}_y$ extends $\mathcal{O}_x$ if $\mathcal{O}_x = \mathcal{O}_y \cap F$.

As the projection ρ is surjective, every $x \in X$ has an extension in X_L and every $y \in X_L$ is the extension of some $x \in X$.

In the case that the field extension L/k is Galois, we have the following result ([10] Theorem III.7.1).

Theorem 1.36 *Let $x \in X$ and let $\rho^{-1}(x)$ be the set of extensions of x in X_L. The Galois group of L over k acts transitively on $\rho^{-1}(x)$.*

Definition 1.37 Let X be a normal projective curve over k and let L/k be a field extension. We let $X(L)$ denote the set of morphisms of k-schemes from Spec L to X. The elements of $X(L)$ are called *L-valued points of X*.

Proposition 1.38 *Let X be a normal projective curve over k and let L/k be a field extension. The following properties are true.*

(a) We have a canonical bijection $X(L) \to X_L(L)$.

(b) *Any element of $X(L)$ is uniquely determined by the data consisting of a point $x \in X$ and a homomorphism of k-algebras $k(x) \to L$.*

(c) *For any extension L' of L, we have a natural inclusion $X(L) \subset X(L')$.*

(d) *Let $B = k[x_0, \ldots, x_n]$. If $X = V_+(I) = \{\mathfrak{p} \in \text{Proj } B \text{ with } I \subset \mathfrak{p}\}$ is a closed subvariety of* Proj B*, then we can identify $X(L)$ with $\{(t_0, \ldots, t_n) \in \mathbf{P}(L^{n+1}) \mid F(t_0, \ldots, t_n) = 0, \text{for all } F \in I\}$.*

Let X be a normal projective curve over k and let L/k be a finite Galois extension with group G. The group G acts on L as the group of automorphisms of L that leave k fixed. This induces an action on $X(L)$ via 1.38 (b).

Proposition 1.39 *Let $H \subset G$ be a normal subgroup. There is a bijection between the set of orbits $(G/H) \backslash X(L^H)$ and $X(k)$. The set of fixed points $X(L)^H$ can be identified with $X(L^H)$.*

Proof The Galois group of L^H over $k = L^G$ is G/H, so as above G/H acts on $X(L^H)$. By 1.38 (a) we may identify $X(L^H)$ with $X_{L^H}(L^H)$. Let $\rho : X_{L^H} \to X$ be the projection and let $x \in X(k)$. By 1.38 we can identify $\rho^{-1}(x)$ with $\text{Hom}_{k-\text{alg}}(k(x), L^H)$. The action of G/H on $\rho^{-1}(x)$ is transitive. So we can identify the orbits $(G/H) \backslash X(L^H)$ with $X(k)$.
An element of $X(L)$ is a pair (x, f) with $x \in X$ and $f : k(x) \to L$. This is fixed by the action of H if and only if f factors through L^H as $k(x) \to L^H \to L$, where the last arrow is just the inclusion. Finally, (x, f) is fixed by the action of H if and only if the image of f is contained in L^H if and only if (x, f) corresponds to a point in $X(L^H)$. □

For the last part one could also say that the bijection $X(L)^H$ to $X(L^H)$ is a consequence of the bijection $\text{Hom}_{k-\text{alg}}(k(x), L^H) \to \text{Hom}_{k-\text{alg}}(k(x), L)^H$ induced by the inclusion $L^H \subset L$.

Proposition 1.40 *Let k be a perfect field. Let X be a normal projective curve over k and let L/k be a finite (separable) algebraic extension. Let $x \in X$ and let $y_1, \ldots, y_m$ be the extensions of x in X_L. Then*

$$\deg_k x = \sum_{i=1}^{m} \deg_L y_i.$$

Proof First we note that by definition $\deg_k x = [k(x) : k]$ and $\deg_L y_i = [k(y) : L]$. Let ξ and η be the generic points of X and X_L respectively. We denote their function fields by $F = \mathcal{O}_{X,\xi}$ and $F' = \mathcal{O}_{X_L,\eta}$. For $1 \leq i \leq m$ let $f_i = f(y_i|x) := [k(y_i) : k(x)]$ and let $e_i = e(y_i|x)$ be the ramification index of y_i over x. We will deduce the result from theorem III.1.11 in [10], which states that

$$\sum_{i=1}^{m} e_i f_i = [F' : F]. \tag{1.1}$$

Theorem III.6.3(a) in [10] says that algebraic constant field extensions are unramified. So $e_i = 1$ for all i. From lemma III.6.2 in [10] we can conclude that $[F' : F] = [L : k]$. Substituting this in equation 1.1 We get

$$\sum_{i=1}^{m} [k(y_i) : k(x)] = [L : k]. \tag{1.2}$$

Now let us compute $[k(y_i) : k(x)]$ in another way. We have two sets of field inclusions $k \subset k(x) \subset k(y_i)$ and $k \subset L \subset k(y_i)$. This gives us

$$[k(y_i) : k] = [k(y_i) : k(x)][k(x) : k] = [k(y_i) : L][L : k],$$

from which we conclude that $[k(y_i) : k(x)] = \dfrac{[k(y_i) : L][L : k]}{[k(x) : k]}$. Substituting this in the left hand side of equation 1.2 gives

$$\sum_{i=1}^{m} \frac{[k(y_i) : L][L : k]}{[k(x) : k]} = [L : k]. \tag{1.3}$$

We cancel $[L : k]$ on both sides and move $[k(x) : k]$ to the other side to get

$$\sum_{i=1}^{m} \deg_L y_i = \sum_{i=1}^{m} [k(y) : L] = [k(x) : k] = \deg_k x.$$

This is what we needed to prove. □

Corollary 1.41 *Let $k = \mathbf{F}_q$ and $L = \mathbf{F}_{q^m}$. Let X be a projective curve over k and $x \in X$ a place of degree l. Let $d = \gcd(l, m)$. Then x extends into exactly d places of degree $\frac{l}{d}$ in X_L.*

Proof As L/k is Galois, all the places y extending x have the same relative degree $f(y|x)$, hence they also all have the same degree $\deg_L y = [k(y) : L]$. Let n be the number of extensions of x in X_L. From the theorem we know that $m = n \deg_L y$. Therefore we only need to show that $\deg_L y = \frac{m}{d} = \frac{m}{\gcd(l,m)}$. The residue class field $k(y)$ is the compositum of $k(x) \cong \mathbf{F}_{q^l}$ and $L = \mathbf{F}_{q^m}$, so $k(y) \cong \mathbf{F}_{q^{\mathrm{lcm}(m,l)}} \cong \mathbf{F}_{q^{ml/d}}$. Hence $\deg_L y = [\mathbf{F}_{q^{ml/d}} : \mathbf{F}_{q^l}] = \frac{m}{d}$. Now it follows that $n \cdot \frac{m}{d} = m$, and therefore x extends into exactly $n = d$ places. □

Corollary 1.42 *Let $k = \mathbf{F}_q$ and $L = \mathbf{F}_{q^m}$. Let X be a projective curve over k and $x \in X$ a place of degree m. Then x extends into exactly m L-rational places in X_L.*

Chapter 2

Generalizing Reed Solomon and Goppa codes

2.1 Basic contructions

Let q be a prime power and let $\mathbf{F}_q$ be a finite field with q elements.

Definition 2.1 A *linear error correcting code over* $\mathbf{F}_q$ of length n and dimension k is a $\mathbf{F}_q$-linear subspace of $\mathbf{F}_q^n$ of dimension k.

Definition 2.2 Let $v \in \mathbf{F}_q^n$. We define the weight $w(v)$ of v as the number of nonzero coordinates of v. In other words

$$w(v) = |\{1 \leq i \leq n \mid \ v_i \neq 0\}|.$$

Definition 2.3 Let C be a linear error correcting code over $\mathbf{F}_q$ of length n and dimension k. The *minimum distance* d of C is defined by

$$d = \min\{w(v) \mid v \in C \text{ and } v \neq 0\}.$$

A code C with these parameters is denoted as a linear $[n, k, d]_q$-code or sometimes as a $[n, k, d]$-code.

Example 2.4 The space $\mathbf{F}_q^n$ is a $[n, n, 1]_q$-code. The space with basis $(1, 1, 1, 1)$ is a $[4, 1, 4]_q$-code.

There are several ways to combine codes into a new code.

Definition 2.5 Let C_i be a linear $[n_i, k_i, d_i]_q$-code for $i = 1, 2$. The *product* $C_1 \times C_2$ of C_1 and C_2 is the code defined by

$$C_1 \times C_2 = \{(x_1, x_2) \mid x_1 \in C_1 \text{ and } x_2 \in C_2\} \subset \mathbf{F}_q^{n_1+n_2}.$$

It has parameters $[n, k, d]$ where $n = n_1+n_2, \quad k = k_1+k_2, \quad d = \min\{d_1, d_2\}$. This is easy to see because the dimension of the product of two linear subspaces is the sum of their dimensions. For the weight we have $w(x_1, x_2) = w(x_1) + w(x_2)$. To make this minimal we may assume $d_1 \leq d_2$ and can take x_2 with weight zero and x_1 with weight equal to d_1.
The t-fold product C_1^t has parameters $[tn_1, tk_1, d_1]$.

Definition 2.6 Let C_1 and C_2 be two linear codes of the same dimension k. Say C_i is a linear $[n_i, k, d_i]_q$-code for $i = 1, 2$. Let $C_1 \times C_2$ be their product. Both codes have the same dimension so we can choose a linear isomorphism $\gamma : C_1 \to C_2$. We define the *concatenation* C_1C_2 of C_1 and C_2 as the graph of γ, so

$$C_1C_2 = \{(a, \gamma(a)) \mid a \in C_1\} \subset C_1 \times C_2.$$

It has parameters $[n_1 + n_2, k, d]$ with $d \geq d_1 + d_2$. The length of the code is $n_1 + n_2$, because it is a subspace of the product. The dimension is k, because γ is injective. For the minimal weight consider a nonzero code word $(a, \gamma(a))$. We have $w(a, \gamma(a)) = w(a) + w(\gamma(a))$. Since γ is linear, both a and $\gamma(a)$ are not zero. So they must have weight at least d_1 and d_2 respectively. We conclude $d \geq d_1 + d_2$.

Definition 2.7 Let C_1 be a linear $[n_1, k_1, d_1]_q$-code and t a positive integer. The *diagonal* code $\mathrm{diag}(C_1^t)$ is the diagonal of the t-fold product C_1^t.

$$\mathrm{diag}(C_1^t) = \{(x, x, \ldots x) \mid x \in C_1\} \subset \mathbf{F}_q^{tn_1}.$$

It has parameters $[tn_1, k_1, td_1]$. This is easy to see because it is just C_1 concatenated with itself t times. So the dimension does not change and $w(x, x, \ldots, x) = w(x) + w(x) + \cdots + w(x) = tw(x)$. So the minimal weight is td_1.

2.2 Generalized Algebraic Geometry Codes

In 1970 Goppa introduced his classical Goppa codes, also called algebraic geometry codes. These Goppa codes generalize the BCH-codes that were invented by Bose and Ray-Chaudhuri and independently by Hocquenghem around 1960. Because these codes have good coding and decoding algorithms, they are important for practical use.

The construction we give here originates from [13] and generalizes the notion of a Goppa code, hence the name: generalized algebraic geometry code. These codes are interesting not only because, like Goppa codes, they allow efficient coding and decoding algorithms, but also because these codes have a relatively high dimension and minimum distance. This makes them very suitable for constructing sequences of asymptotically good codes which we will see in the next chapters. In preparation for the construction of these sequences of codes we define generalized algebraic geometry codes here and study some of their properties. In particular we determine lower bounds for their parameters. We will also see how they generalize Goppa codes.

To define a generalized algebraic geometry code we need the following:

- A finite field $\mathbf{F}_q$ and an algebraic function field $F/\mathbf{F}_q$ of genus g with full constant field $\mathbf{F}_q$.
- A natural number N. Distinct places $P_1, \ldots P_N$ of F, each P_i has degree k_i. We define the divisor $D = P_1 + P_2 + \ldots P_N$.

- A set of linear codes $C_1, \ldots, C_N$ over $\mathbf{F}_q$, each C_i has parameters $[n_i, k_i, d_i]$. We set $n = \sum_{i=1}^{N} n_i$.
- For every place P_i a $\mathbf{F}_q$-linear isomorphism $\phi_i : F_{P_i} \to C_i \subset \mathbf{F}_q^{n_i}$, where $F_{P_i} = \mathcal{O}_{P_i}/P_i$ is the residue class field of P_i.
- A divisor G, such that $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset$.

Recall definition 1.10 of the Riemann-Roch space $\mathcal{L}(G)$. We define a map $\phi : \mathcal{L}(G) \to \mathbf{F}_q^n$ by setting

$$\phi(z) = (\phi_1(z(P_1)), \phi_2(z(P_2)), \ldots, \phi_N(z(P_N))) \ \in \mathbf{F}_q^n \tag{2.1}$$

for all $z \in \mathcal{L}(G)$.

Definition 2.8 The image of ϕ is called a *generalized algebraic geometry code* and we denote it by $C(D, G, \phi)$.

2.2.1 Parameters of a generalized algebraic geometry code

From [9] we have the following Proposition stated without proof. We include a proof here.

Proposition 2.9 *The code $C(D, G, \phi)$ is a linear $[n, k, d]$-code over $\mathbf{F}_q$ with*

- $n = \sum_{i=1}^{N} n_i$
- $k = \dim \mathcal{L}(G) \geq \deg G + 1 - g \qquad$ *if* $\deg G < \sum_{i=1}^{N} k_i$
- $d \geq \min\{\sum_{i \notin S} d_i \mid S \subseteq \{1, \ldots, N\}$ *is such that* $\sum_{i \in S} k_i \leq \deg G\}$.

Proof Since every ϕ_i has image in $\mathbf{F}_q^{n_i}$, the image of ϕ is in $\prod_{i=n}^{N} \mathbf{F}_q^{n_i} \cong \mathbf{F}_q^n$, so the code has length n. Furthermore, ϕ is a linear map, because ϕ_i is linear for all i. So the code is linear.

For $z \in \mathcal{L}(G)$, $\phi(z)$ can only be zero if $\phi_i(z(P_i)) = 0$ for every i. Since ϕ_i is injective, this is the same as saying that $v_{P_i}(z) \geq 1$ for all $P_i \in \operatorname{supp} D$. Hence $\operatorname{Ker} \phi = \mathcal{L}(G - D)$. If $\deg G < \sum_{i=1}^{N} k_i = \deg D$, then $\deg(G - D) < 0$, hence ϕ is injective and therefore its image has the same dimension as $\mathcal{L}(G)$. The inequality $\dim \mathcal{L}(G) \geq \deg G + 1 - g$ is a consequence of the Riemann-Roch Theorem.

The last part asks us to find a lower bound for d. Because the code is linear $d = \min\{w(\phi(z)) \mid z \in \mathcal{L}(G)\}$. Now fix z in $\mathcal{L}(G) \setminus \{0\}$. We have

$$w(\phi(z)) = w((\phi_1(z), \phi_2(z), \ldots, \phi_N(z))) = \sum_{i \in R_z} w(\phi_i(z(P_i))) \geq \sum_{i \in R_z} d_i,$$

where $R_z = \{i \in \{1, \ldots, N\} \mid z(P_i) \neq 0\}$. Here the last equality follows from the fact that for $i \notin R_z$, $\phi_i(z(P_i))$ has weight zero and does not contribute to

the sum. The inequality holds, because ϕ_i maps injectively into a $[n_i, k_i, d_i]$-code and therefore any nonzero code word has weight at least d_i. Now we have that $d \geq \min\{\sum_{i \in R_z} d_i \mid z \in \mathcal{L}(G) \setminus \{0\}\}$.

We define $S_z = \{1, \ldots, N\} \setminus R_z = \{i \in \{1, \ldots, N\} \mid z(P_i) = 0\}$. We will show that $\sum_{i \in S_z} k_i \leq \deg G$. For all $i \in S_z$, $v_{P_i}(z) \geq 1$, so $z \in \mathcal{L}(G - \sum_{i \in S} P_i)$, so $\dim(G - \sum_{i \in S} P_i) \neq 0$. Now Proposition I.4.2b in [10] implies that $\deg(G - \sum_{i \in S} P_i) \geq 0$, hence we can conclude that $\deg G - \sum_{i \in S_z} \deg P_i \geq 0$. Using $k_i = \deg P_i$ we find $\sum_{i \in S_z} k_i \leq \deg G$.

Finally we note that the set $\{S_z \mid z \in \mathcal{L}(G) \setminus \{0\}\}$ is a subset of the set $\{S \subseteq \{1, \ldots, N\} \mid S \text{ is such that } \sum_{i \in S} k_i \leq \deg G\}$. Since the minimum will not increase, when S runs through a bigger set, we get the result. □

We can find another lower bound for the minimum distance of a generalized algebraic geometry code.

Lemma 2.10 *Let d be the minimum distance of a generalized algebraic geometry code. Then*

$$d \geq \min\{\sum_{i=1}^{N} d_i - \deg G - \sum_{i \in S} (d_i - k_i)\}$$

where the minimum is taken over all sets $S \subseteq \{1, \ldots, N\}$ such that $\sum_{i \in S} k_i \leq \deg G$.

Proof Assume $S \subseteq \{1, \ldots, N\}$ is such that $-\sum_{i \in S} k_i \geq -\deg G$.
Then $\sum_{i \notin S} d_i = \sum_{i=1}^{N} d_i - \sum_{i \in S} d_i + \sum_{i \in S}(k_i - k_i) = \sum_{i=1}^{N} d_i - \sum_{i \in S} k_i - \sum_{i \in S}(d_i - k_i) \geq \sum_{i=1}^{N} d_i - \deg G - \sum_{i \in S}(d_i - k_i)$. The result now follows from Proposition 2.9. □

Corollary 2.11 *If $d_i = k_i$ for all i, then $d \geq \deg D - \deg G$.*

Proof This follows from substituting $\sum_{i=1}^{N} d_i = \sum_{i=1}^{N} k_i = \deg D$ in the above lemma. □

Corollary 2.12 *Let $C(D, G, \phi)$ be a generalized algebraic geometry code with $k_u = \min\{k_i \mid 1 \leq i \leq N\}$ and $d_v = \min\{d_i \mid 1 \leq i \leq N\}$ and minimum distance d. Then*

$$d \geq d_v(N - \frac{\deg G}{k_u}).$$

Proof By Proposition 2.9 $d \geq \min\{\sum_{i \notin S} d_i\}$, where the minimum is taken over all sets S for which $\sum_{i \in S} k_i \leq \deg G$. Let $S' \subset \{1, \ldots, N\}$ be such a set with maximal cardinality. Then $d \geq \min\{\sum_{i \notin S} d_i\} \geq (N - |S'|)d_v$. We find an upper bound for $|S'|$. We have $|S'|k_u = \sum_{i \in S'} k_u \leq \sum_{i \in S'} k_i \leq \deg G$. So $|S'| \leq \frac{\deg G}{k_u}$ and therefore $d \geq (N - |S'|)d_v \geq d_v(N - \frac{\deg G}{k_u})$. □

Lemma 2.13 *Let C be a generalized algebraic geometry code with $k_u = \min\{k_i \mid 1 \leq i \leq N\}$. Let $z \in \mathcal{L}(G)$ and let d' be the number of indices i for which $\phi_i(z(P_i))$ is nonzero. Then $d' \geq N - \frac{\deg G}{k_u}$.*

Proof From the proof of Proposition 2.9 we have $d' = |R_z|$ and $d \geq \min_z\{\sum_{i \in R_z} d_i\}$. Since $d_i \geq 1$ for all i we find that $d' \geq \min\{\sum_{i \notin S} 1 \mid S \subseteq \{1, \ldots, N\}$ is such that $\sum_{i \in S} k_i \leq \deg G\}$. Now Corollary 2.12 with $d_v = 1$ gives the result. □

Let us now consider a linear error correcting code over $\mathbf{F}_{q^m}$. We can identify the field $\mathbf{F}_{q^m}$ with $\mathbf{F}_q^m$ in the following way. Let $\alpha \in \mathbf{F}_{q^m}^*$ be a generator of the cyclic group $\mathbf{F}_{q^m}^*$, then $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$. Consider the map $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^m$ given by

$$\psi(a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}) = (a_0, a_1, \ldots, a_{m-1}).$$

Using this map we can view a code defined over $\mathbf{F}_{q^m}$ as a code over $\mathbf{F}_q$. This raises the question how parameters change when we view a code over $\mathbf{F}_{q^m}$ as a code over $\mathbf{F}_q$.

Lemma 2.14 *Let C be a linear $[n, k, d']_{q^m}$-code. Then via ψ, C becomes a linear $[nm, km, d]_q$-code, with $d' \leq d \leq md'$.*

Proof Let $v = (v_1, \ldots, v_n) \in C \subset \mathbf{F}_{q^m}^n$. The isomorphism ψ extends naturally to an isomorphism $\psi : \mathbf{F}_{q^m}^n \to \mathbf{F}_q^{mn}$ (also denoted ψ) by setting $\psi(v) = (\psi(v_1), \ldots, \psi(v_n))$. We see that the length of C over $\mathbf{F}_q$ is nm. If $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, then all the vectors $\alpha^i v$ are in C, since C is linear. The vectors $\psi(\alpha^i v)$ are all linearly independent over $\mathbf{F}_q$, therefore the dimension of C as a code over $\mathbf{F}_q$ is km.

Let $v = (v_1, \ldots, v_n) \in \mathbf{F}_{q^m}^n$ have weight 1 over $\mathbf{F}_{q^m}$, in other words v has exactly 1 nonzero coordinate, say v_1. Now v_1 is mapped by ψ to m coordinates in $\mathbf{F}_q$ and since ψ maps only zero to zero, at least one and at most m of these m coordinates are nonzero. Therefore the weight of $\psi(v)$ over $\mathbf{F}_q$ is at least one and at most m. Since any vector is a sum of vectors of weight one, it follows that $d' \leq d \leq md'$. □

For example the field $\mathbf{F}_{q^m}$ can be viewed as a $[1, 1, 1]_{q^m}$-code and also as a $[m, m, 1]_q$-code.

2.2.2 Relation with Goppa codes

Let us recall the definition of a Goppa code. Let $F/\mathbf{F}_q$ be a function field, $P_1, \ldots, P_N$ distinct rational places of F of degree one. $D = P_1 + \cdots + P_N$. Let G be a divisor of F such that Supp $G \cap$ Supp $D = \emptyset$.

Definition 2.15 The *geometric Goppa code* associated with the divisors D and G is defined by

$$C(D, G) = \{(z(P_1), z(P_2), \ldots, z(P_N)) \mid z \in \mathcal{L}(G)\} \subset \mathbf{F}_q^N.$$

We will show that generalized algebraic geometry codes generalize the definition of a Goppa code. Let F, D, G be as above. For each i we define the linear code C_i to be the $[1, 1, 1]_q$-code $\mathbf{F}_q$. For every place P_i the residue field $F_{P_i} = \mathbf{F}_q$. Therefore we can take $\phi_i : F_{P_i} \to C_i$ the identity map. The

generalized algebraic geometry code $C(D, G, \phi)$ is equal to the Goppa code $C(D, G)$. From Proposition 2.9 this is a code of length N and if $\deg G < N$ the dimension is equal to the dimension of $\mathcal{L}(G)$. Corollary 2.11 tells us that the minimum distance d satisfies $d \geq N - \deg G$.

2.3 Goppa codes and Reed-Solomon codes

We have seen that Goppa codes are generalized algebraic geometry codes. In this section we will give two definitions of Reed-Solomon codes. The first definition defines a Reed-Solomon code as a Goppa code, the second is the original definition. We show that they are equivalent and thereby Goppa codes and hence generalized algebraic geometry codes generalize Reed-Solomon codes.

Definition 2.16 A code of length n over $\mathbf{F}_q$ is *cyclic* if for any codeword $c = (c_1, c_2, \ldots, c_n) \in C$ also $(c_n, c_1, c_2, \ldots, c_{n-1}) \in C$.

It is well known that the canonical isomorphism $\mathbf{F}_q^n \cong \mathbf{F}_q[X]/(X^n - 1)$ gives a bijection between cyclic codes of length n and ideals of $\mathbf{F}_q[X]/(X^n - 1)$. Via this isomorphism we can write codewords $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ as polynomials $c(X) = \sum_{i=0}^{n-1} c_i X^i \in \mathbf{F}_q[X]/(X^n - 1)$. Since cyclic codes correspond to ideals and every ideal in $\mathbf{F}_q[X]/(X^n - 1)$ is principal because $\mathbf{F}_q[X]$ is a principal ideal domain, we can define a *generator polynomial* of a code as a generator of the corresponding ideal in $\mathbf{F}_q[X]$.

Definition 2.17 Let α be a primitive element of $\mathbf{F}_q$. Then α has order $n = q - 1$. Let $0 < k \leq n$. Let $D = P_{\alpha^0} + P_\alpha + \cdots + P_{\alpha^{n-1}}$ and let $G = (k-1)P_\infty$ be divisors of the rational function field $\mathbf{F}_q(X)$. The code

$$C = C(D, G) = \{c_f = (f(\alpha^0), f(\alpha), \ldots, f(\alpha^{n-1})) \mid f \in \mathbf{F}_q[X] \text{ and } \deg f \leq k - 1\} \subseteq \mathbf{F}_q^n$$

is called a Reed-Solomon code, or RS-code. It has parameters $[n, k, n + 1 - k]_q$.

Definition 2.18 Let α be a primitive element of $\mathbf{F}_q$. Then α has order $n = q - 1$. Let $0 \leq l \leq n + 1$ and $2 - l \leq \delta \leq n + 1 - l$ be nonnegative integers. An RS-code is a cyclic code over $\mathbf{F}_q$ of length $n = q - 1$, for which the generator polynomial g is the least common multiple of the generator polynomials of $\alpha^l, \alpha^{l+1}, \ldots, \alpha^{l+\delta-2}$. It has parameters $[n, n + 1 - \delta, \delta]_q$.

Theorem 2.19 *The two definitions of RS-code above are equivalent. More precisely, the code $C(D, G)$ in definition 2.17 with $k = n + 1 - \delta$ is equal to the code in definition 2.18 with $l = 1$.*

Proof Let $g(X) = (X - \alpha^l)(X - \alpha^{l+1}) \cdots (X - \alpha^{l+\delta-2})$ be the generator polynomial of $\alpha^l, \alpha^{l+1}, \ldots, \alpha^{l+\delta-2}$. We wish to show that any codeword $c_f = c_f(X) = f(\alpha^0) + f(\alpha)X + \cdots + f(\alpha^{n-1})X^{n-1}$ of the code C in definition

2.17 is a multiple of $g(X)$. We will do this by showing that $g(x) = 0$ implies $c_f(x) = 0$ for any $x \in \mathbf{F}_q$.

Let $x = \alpha^t$ be a zero of $g(X)$. Then $l \leq t \leq l + \delta - 2$. Say $f = \sum_{j=0}^{k-1} b_j X^j$ and let $\Phi(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{n-1}) = \frac{X^n - 1}{X - 1}$. We have

$$c_f(\alpha^t) = \sum_{i=0}^{n-1} \alpha^{ti} f(\alpha^i) = \sum_{i=0}^{n-1} \alpha^{ti} \sum_{j=0}^{k-1} b_j \alpha^{ij} = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} b_j \alpha^{ti+ji} =$$

$$\sum_{j=0}^{k-1} \sum_{i=0}^{n-1} b_j \alpha^{(t+j)i} = \sum_{j=0}^{k-1} b_j \Phi(\alpha^{t+j}) = 0.$$

Note that $\Phi(\alpha^{t+j}) = 0$ whenever $t+j \neq 0$ or n. Since $l+j \leq t+j \leq l+\delta-2+j$ and $0 \leq j \leq k-1 = n-\delta$, we get $l \leq t+j \leq l+n-2$ and so if $l = 1$ we can conclude that $t + j \neq 0$ or n. Hence $c_f(X)$ is a multiple of $g(X)$. So the code $C(D, G)$ is contained in the ideal generated by g. The code $C(D, G)$ has dimension $k = n + 1 - \delta = n - \deg g$. Therefore the two codes have the same dimension and are equivalent. □

Remark 2.20 The parameters of the RS-code in definition 2.18 do not depend on l. Therefore any two of such RS-codes with generator polynomials of the same degree have the same parameters and are equivalent. By the above theorem these are equivalent to the Goppa code in 2.17. We conclude that Goppa codes are a generalization of RS-codes.

Chapter 3

Asymptotically good codes

Definition 3.1 Let C be an $[n,k,d]_q$-code. The *rate* of C is the ratio

$$R = R(C) = \frac{k}{n}$$

and the *relative minimum distance* of C is the ratio

$$\delta = \delta(C) = \frac{d}{n}.$$

Let $(C_m)_{m\geq 0}$ be a sequence of codes over $\mathbf{F}_q$, where each C_m is a $[n_m,k_m,d_m]_q$-code. We say that the sequence of codes $(C_m)_{m\geq 0}$ is *asymptotically good* if

$$\liminf_{m\to\infty} R(C_m) > 0 \qquad \text{and} \qquad \liminf_{m\to\infty} \delta(C_m) > 0.$$

3.1 Bounds for the rate of a code

There is a balance between rate and minimum distance. Codes with a high rate will have a small relative minimum distance and vice versa. To make this more precise we define

$$V_q = \{(\delta(C), R(C)) \in [0,1]^2 \mid C \text{ is a linear code over } \mathbf{F}_q\}$$

and $U_q \subset [0,1]^2$ is the set of limit points of V_q.

Proposition 3.2 *There is a continuous function $\alpha_q : [0,1] \to [0,1]$ such that*

$$U_q = \{(\delta, R) \mid 0 \leq \delta \leq 1 \text{ and } 0 \leq R \leq \alpha_q(\delta)\}.$$

Moreover, $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ for $1 - \frac{1}{q} \leq \delta \leq 1$, and α_q is decreasing on the interval $0 \leq \delta \leq 1 - \frac{1}{q}$.

This is proved in [8]. This Proposition says that $\alpha_q(\delta)$ is the maximum possible rate for a code with relative minimum distance δ. The exact value of $\alpha_q(\delta)$ is unknown for $0 < \delta < 1 - \frac{1}{q}$.

The higher both $\delta(C)$ and $R(C)$ are, the better is the performance of a code C. For any code C the rate $R(C) = \alpha_q(\delta(C))$ is the highest possible

rate. To be able to evaluate the performance or efficiency of code, we need to know more about the function α_q. There are several upper and lower bounds for α_q. We state some of them here, for a proof we refer the reader to [10] and the references therein.

The q-ary entropy function $H_q : [0, 1 - \frac{1}{q}] \to \mathbf{R}$ is defined by $H_q(0) = 0$ and

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x) \quad \text{for } 0 \leq x \leq 1 - 1/q.$$

(Plotkin Bound) For $0 \leq \delta \leq 1 - \frac{1}{q}$,

$$\alpha_q(\delta) \leq 1 - \tfrac{q}{q-1}\delta.$$

(Hamming Bound) For $0 \leq \delta \leq 1$,

$$\alpha_q(\delta) \leq 1 - H_q(\tfrac{\delta}{2}).$$

(Bassalygo-Elias Bound) For $0 \leq \delta \leq 1 - \frac{1}{q}$ and $\theta = 1 - \frac{1}{q}$,

$$\alpha_q(\delta) \leq 1 - H_q(\theta - \sqrt{\theta(\theta - \delta)}).$$

(Gilbert-Varshamov Bound) For $0 \leq \delta \leq 1 - \frac{1}{q}$,

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Of the three upper bounds, the Bassalygo-Elias Bound is always best. The Gilbert-Varshamov Bound is a lower bound for α_q. It implies that asymptotically good codes exist. The proof of the Gilbert-Varshamov Bound is not constructive, i.e. it does not tell one how to construct such a sequence of codes.

There is another lower bound for a_q. To formulate it we make a definition.

Definition 3.3 Let $N_q(g)$ be the maximum number of rational places that a function field of genus g defined over $\mathbf{F}_q$ can have. We define

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

(Tsfasman-Vladut-Zink Bound) For $0 \leq \delta \leq 1$,

$$\alpha_q(\delta) \geq 1 - \delta - \tfrac{1}{A(q)}.$$

The Tsfasman-Vladut-Zink bound improves the Gilbert-Varshamov bound in some range of δ for all $q \geq 49$. In [10] Theorem V.3.6 it is shown that $A(q) \leq \sqrt{q} - 1$. Ihara, Tsfasman, Vladut and Zink used methods from algebraic geometry and number theory to show that equality holds if q is a square [11]. In other words $A(q^2) = q - 1$. Let $B_1(F)$ denote the number of rational places of a function field F. In section 4.2 we give a construction of a tower of function fields $(F_n)_{n \geq 1}$ over $\mathbf{F}_{q^2}$ for which $\lim_{n \to \infty} \frac{B_1(F_n)}{g(F_n)} = A(q^2) = q - 1$.

3.1.1 A first attempt

One of the main problems in coding theory is the construction of asymptotically good codes. To demonstrate that this is not an easy problem, we will start with a simple construction of a sequence of codes that turns out to be not asymptotically good.

We have seen that by taking products and concatenations of a code we can increase its dimension and minimum distance. Therefore a first idea may be to construct a sequence of codes by taking repeated concatenations and products.

Let C_0 be a $[n_0, k_0, d_0]_q$-code and let $(b_i)_{i\geq 1}$ with $b_i \in \{0, 1\}$ for all i, be a sequence of zeroes and ones. We construct a sequence of codes $(C_m)_{m\geq 0}$ recursively.

$$C_m = \begin{cases} C_{m-1}^2 & \text{if} \quad b_m = 0 \\ \operatorname{diag}(C_{m-1}^2) & \text{if} \quad b_m = 1 \end{cases}$$

Proposition 3.4 *The sequence of codes constructed above is not asymptotically good.*

Proof We compute the parameters $[n_m, k_m, d_m]$ using 2.5 and 2.7. For each $m, n_m = 2n_{m-1}$. So $n_m = 2^m n_0$. Let $x_m = |\{1 \leq i \leq m \mid b_i = 0\}|$ be the number of zeroes occuring in the first m entries in the sequence and similarly let y_m be the number of ones. Then $x_m + y_m = m$. We have $k_m = 2k_{m-1}$ if $b_m = 0$ and $k_m = k_{m-1}$ if $b_m = 1$, so $k_m = 2^{x_m} k_0$. In a similar way we find that $d_m = 2d_{m-1}$ if $b_m = 1$ and $d_m = d_{m-1}$ if $b_m = 0$, so $d_m = 2^{y_m} d_0$. From this it is easy to compute that $r_m = \dfrac{k_m}{n_m} = \dfrac{2^{x_m} k_0}{2^m n_0} = \dfrac{r_0}{2^{m-x_m}}$ and $\delta_m = \dfrac{d_m}{n_m} = \dfrac{2^{y_m} d_0}{2^m n_0} = \dfrac{\delta_0}{2^{x_m}}$. Now it follows that $\lim r_m \cdot \lim \delta_m = \lim r_m \delta_m = \lim \frac{r_0 \delta_0}{2^m} = 0$, here lim is the limit where m tends to infinity. Hence $\lim r_m = 0$ or $\lim \delta_m = 0$ and therefore the code is not asymptotically good. □

Note that in fact both limits are zero unless the sequence $(b_i)_{i\geq 1}$ eventually becomes constant. Furthermore this result does not depend on the sequence $(b_i)_{i\geq 1}$, therefore we see that any sequence of codes constructed by repeatedly taking diagonals and products is not asymptotically good.

3.2 MGAG codes

Now we present the construction of a family of asymptotically good codes that was given by Spera in [9]. He starts with a generalized algebraic geometry code where all the codes C_i have the same parameters and modifies this to prove that the resulting code is asymptotically good. We will refer to these codes as MGAG codes (Modified Generalized Algebraic Geometry codes). Next we show that these MGAG codes generalize the codes that were constructed in [6] by Justesen.

Fix a prime power $q > 16$ and a rational number R with $0 < R < \frac{1}{2}$. We fix an algebraic function field $F/\mathbf{F}_q$ of genus g. For every $m \in \mathbf{N}$ such that $2mR$ is an integer we construct a generalized algebraic geometry code using the following data:

- A positive integer $N = N_m$ with $a^m\sqrt{q}^m \leq N_m \leq B_m$[1]. Here a is a positive integer such that $16 \leq a^2 < q$ and B_m is the number of places of F of degree m.
- Distinct places $P_1, \ldots P_N$ of degree m. $D = P_1 + \cdots + P_N$.
- A divisor G, such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$ and $\deg G = 2RmN_m$.
- For $1 \leq i \leq N_m$, we take $C_i = \mathbf{F}_q^m$ the linear $[m, m, 1]_q$-code and $\phi_i : F_{P_i} \to \mathbf{F}_q^m$ a linear isomorphism.

Now the code $C'_m = C(D, G, \phi)$ where $\phi = (\phi_i)_{i=1}^N$ is as before, has parameters $[n_m, k_m, d_m]_q$ with $n_m = mN_m$, $k_m = \dim \mathcal{L}(G) \geq 2RmN_m + 1 - g$ and $d_m \geq N_m(1-2R)$. This all comes from Proposition 2.9. $d_m \geq \min \sum_{i \notin S} 1 = N_m - |S|$, where S is the largest set such that $|S|m \leq \deg G$, so $-|S| \geq -\frac{\deg G}{m} = -2RN_m$.

As m tends to infinity, the family of generalized algebraic geometry codes C'_m does not appear to be asymptotically good. Let R_m be the rate and δ_m the relative minimum distance of C'_m.

$$R_m = \frac{k_m}{n_m} \geq \frac{\deg G}{mN_m} + \frac{1-g}{mN_m} \longrightarrow \frac{\deg G}{mN_m} = \frac{2RmN_m}{mN_m} = 2R.$$

$$\delta_m = \frac{d_m}{n_m} \geq \frac{N_m(1-2R)}{mN_m} = \frac{1}{m}(1-2R).$$

Although the above does not imply that the relative minimum distance tends to zero, we cannot conclude that the relative minimum distance stays positive. Therefore we need to modify the construction.

All the ϕ_i have image in $\mathbf{F}_q^m$. We give $\mathbf{F}_q^m$ the structure of a field by identifying it with $\mathbf{F}_{q^m}$. Let α be a primitive element of $\mathbf{F}_{q^m}$, such that $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$. Now we define a map $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^m$ by

$$\psi(a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}) = (a_0, a_1, \ldots, a_{m-1}). \tag{3.1}$$

We set $\xi = \psi(\alpha)$. Note that in the multiplicative structure we have now given to $\mathbf{F}_q^m$, multiplication of an element $x \in \mathbf{F}_q^m$ by ξ is given by $\xi \cdot x = \psi(\alpha \cdot \psi^{-1}(x))$. We define a $\mathbf{F}_q$-linear isomorphism $\sigma_\xi : (\mathbf{F}_q^m)^N \to (\mathbf{F}_q^m)^N$ by

$$\sigma_\xi(x_0, x_1, \ldots, x_{N-1}) = (x_0, \xi x_1, \ldots, \xi^{N-1} x_{N-1}) \qquad \text{for } x_i \in \mathbf{F}_q^m.$$

It is easy to verify that σ_ξ is indeed an $\mathbf{F}_q$-linear isomorphism and that its inverse is $\sigma_{\xi^{-1}}$. From now on we assume $N \leq q^m - 1$, then all powers $\xi^0, \xi, \ldots \xi^{N-1}$ are distinct, since α is a primitive element and has order $q^m - 1$. Applying σ_ξ to the code C'_m gives a code $\sigma_\xi C'_m$ with the same parameters.

[1] See Lemma 3.7

Definition 3.5 The MGAG code C_m is the concatenation, see Definition 2.6, of C'_m and $\sigma_\xi C'_m$, i.e. $C_m = C'_m \sigma_\xi C'_m$. It consists of all code words of the form $(\phi(z), \sigma_\xi \phi(z)) =$

$$(\phi_1(z(P_1)), \ldots, \phi_N(z(P_N)), \phi_1(z(P_1)), \xi\phi_2(z(P_2)), \ldots, \xi^{N-1}\phi_N(z(P_N))) \tag{3.2}$$

with $z \in \mathcal{L}(G)$.

These MGAG codes $(C_m)_m$ can be used to construct asymptotically good sequences of codes, as we will show in the next sections.

3.3 The first asymptotically good code

The first asymptotically good sequence of codes, constructed by Justesen [6] is closely related to the MGAG codes defined above. We will define Justesen's code J_m using our MGAG codes above. For every m the code J_m in the sequence is a MGAG code over $\mathbf{F}_q$. But as opposed to the sequence of codes defined above, in this sequence the function field F is not fixed. It will vary with m. For m a positive integer and a fixed prime power q we take the function field $F = \mathbf{F}_{q^m}(X)$, so the function field itself depends on m.

Now there are two equivalent ways to construct a sequence of codes over $\mathbf{F}_q$. Both constructions yield a code of the same length with coordinates in $\mathbf{F}_q$. For both ways we let α be a primitive element of $\mathbf{F}_{q^m}$ and apply the isomorphism ψ given in equation 3.1 to each coordinate to obtain a code over $\mathbf{F}_q$.

In the first construction we consider F as function field over $\mathbf{F}_{q^m}$. The code C_m will turn out to be a modified Reed-Solomon code over $\mathbf{F}_{q^m}$. We expand this code using ψ to get a code over $\mathbf{F}_q$. In the second construction we consider $F = \mathbf{F}_{q^m}(X)$ as function field over $\mathbf{F}_q$.

3.3.1 Justesen's code over $\mathbf{F}_{q^m}$

We consider $F = \mathbf{F}_{q^m}(X)$ as function field over $\mathbf{F}_{q^m}$. We fix R with $0 < R < \frac{1}{2}$ and we take k the smallest integer greater than or equal to $2RN$, where $N = q^m - 1$. Now we take $G = (k-1)P_\infty$. Let α be a generator for the multiplicative group $\mathbf{F}^*_{q^m}$. The divisor D is the set of all rational places corresponding to powers of α, so these are all the rational places except the two places corresponding to zero and infinity. In short $D = P_1 + P_\alpha + \cdots + P_{\alpha^{N-1}}$. For $0 \leq i \leq N-1$ we let $C_i = \mathbf{F}_q(\alpha)$ be the linear $[1,1,1]_{q^m}$-code and $\phi_i : F_{P_{\alpha^i}} \to C_i$ the identity.

Let C_m be the MGAG code with the divisors D and G and map ϕ as above. So

$$C_m = \{\phi(z) = (z(1), z(\alpha), \ldots z(\alpha^{N-1}), z(1), \alpha z(\alpha), \ldots, \alpha^{N-1} z(\alpha^{N-1})) \\ \mid z \in \mathbf{F}_q(\alpha)[X] \text{ and } \deg(z) \leq k-1\} \subset \mathbf{F}_q(\alpha)^{2N}.$$

Note that in this case $\xi = \alpha$, because we have identified $\mathbf{F}_{q^m}$ with $\mathbf{F}_q(\alpha)$. Remark that the first N coordinates of C_m form a Reed-Solomon code over q^m of dimension k. Hence we see that C_m is a $[2N, k, 2(N+1-k)]_{q^m}$-code.

Definition 3.6 *Justesen's code* J_m is the code C_m considered as a vector space over $\mathbf{F}_q$. In other words it is C_m expanded as q-ary code by applying ψ to each coordinate. It is a $[2mN, mk, d]_q$-code with $d \geq 2(N+1-k)$.

Justesen did this construction for $q = 2$ and showed that the family of codes $(C_m)_m$ is asymptotically good. A proof of a more general case is given in section 3.4.

3.3.2 Justesen's code over $\mathbf{F}_q$

Now we repeat this construction, but we consider $F = \mathbf{F}_{q^m}(X)$ as function field over $\mathbf{F}_q$. As before, fix R with $0 < R < \frac{1}{2}$ and take k the smallest integer greater than or equal to $2RN$. Let $N = q^m - 1$. We take $G = (k-1)P_\infty$. Let $\alpha \in \mathbf{F}_{q^m}^*$ as before be an element of order $q^m - 1$. The divisor D is the set of all places corresponding to powers of α, so $D = P_1 + P_\alpha + \cdots + P_{\alpha^{N-1}}$. We write P_i for P_{α^i}. Remark that in general the places are not rational over $\mathbf{F}_q$. For example $F_{P_i} \cong \mathbf{F}_q(\alpha^i)$ and has degree $k_i = [\mathbf{F}_q(\alpha^i) : \mathbf{F}_q]$.

For $0 \leq i \leq N-1$ we let $C_i = \mathbf{F}_q(\alpha^i) \subset \mathbf{F}_q(\alpha)$ be a linear $[m, k_i, 1]_q$-code and $\phi_i : F_{P_i} \to \mathbf{F}_q^m$ is the composition of the isomorphism $F_{P_i} \cong C_i$ followed by the inclusion $\mathbf{F}_q(\alpha^i) \subset \mathbf{F}_q(\alpha)$, followed by ψ .

Let C_m be the MGAG code as in definition 3.5 with the divisors D and G and map ϕ above. The code C_m is a q-ary code of length $2N$ and dimension k. It cannot be equal to the code J_m of definition 3.6, since the dimension is k and J_m has dimension mk. However, we can show that it is a subspace of J_m and we can construct the code J_m out of m copies of C_m.

We will write P' for a place in F over $\mathbf{F}_{q^m}$ and we denote its restriction to F over $\mathbf{F}_q$ by P. We have $G' = (k-1)P'_\infty$ and $\mathcal{L}(G') = \{z \in \mathbf{F}_q(\alpha)[X] \mid \deg z < k\}$ and $\mathcal{L}(G) = \{z \in \mathbf{F}_{q^X} \mid \deg z < k\}$. First we note that for $P_i = P_{\alpha^i}$ and $z \in \mathcal{L}(G)$ the identification $F_{P_i} \cong \mathbf{F}_q(\alpha^i)$ maps $z(P_i)$ to $z(\alpha^i)$. It is easy to see that $\mathcal{L}(G') \cong \bigoplus_{i=0}^{m-1} \alpha^i \mathcal{L}(G)$. This shows that there is an isomorphism

$$\bigoplus_{i=1}^{m} C_m \longrightarrow J_m \subset (\mathbf{F}_q^{2N})^m \qquad \text{given by} \qquad (\phi(z_i), \sigma_\xi\phi(z_i))_{i=1}^m \longmapsto$$
$$((\phi(z_1), \sigma_\xi\phi(z_1)) + (\phi(\alpha z_2), \sigma_\xi\phi(\alpha z_2)) + \cdots + (\phi(\alpha^{m-1} z_m), \sigma_\xi\phi(\alpha^{m-1} z_m))).$$

3.4 A renewed MGAG code

In this section we generalize the construction of a MGAG code to include places of varying degrees. We start with a Lemma.

Lemma 3.7 *Let F be an algebraic function field over $\mathbf{F}_q$ of genus g. Let a be a positive integer such that $a^2 < q$. For every positive integer m, we define N_m to be the smallest integer greater than or equal to $a^m\sqrt{q}^m$. Then for m sufficiently large there exist at least N_m places of F of degree m.*

Proof Let B_m denote the number of places of degree m in F. All we need to show is that for large enough m we have $N_m \leq B_m$. From Corollary V.2.10 in [10] it follows that

$$B_m > \frac{q^m}{m} - (2+7g)\cdot\frac{\sqrt{q}^m}{m} = a^m\sqrt{q}^m\left(\frac{\sqrt{q}^m}{ma^m} - \frac{2+7g}{ma^m}\right).$$

By assumption $\frac{\sqrt{q}}{a} > 1$, therefore as m goes to infinity also $\frac{\sqrt{q}^m}{ma^m}$ will grow to infinity. On the other hand $\frac{2+7g}{ma^m}$ goes to zero, because the function field and hence its genus, is fixed. So for m sufficiently large $\left(\frac{\sqrt{q}^m}{ma^m} - \frac{2+7g}{ma^m}\right) > 1$, from which it follows that $B_m > N_m$. □

Now we will construct our renewed MGAG code. Choose a prime power $q > 16$. Let $F/\mathbf{F}_q$ be an algebraic function field of genus g. We fix a rational number R with $0 < R < \frac{1}{2}$ and a small positive real number ϵ with $0 < \epsilon < 1 - 2R$. We let m run through the set of positive integers for which $2Rm$ is an integer. If $R = \frac{s}{t}$ for $s, t \in \mathbf{N}$ relatively prime and $t \neq 0$, then $m = t, 2t, 3t, \ldots$ and so on. For each such m we construct a code C_m with the following data.

- Let $N = N_m$ with $a^m\sqrt{q}^m \leq N_m \leq B_m$ be defined as in Lemma 3.7. Here a is a positive integer such that $16 \leq a^2 < q$ and B_m is the number of places of F of degree m.
- Distinct places $P_1, \ldots, P_N$, each place P_i has degree k_i, where k_i is such that $\frac{k_i}{m} > 2R + \epsilon$. The degrees are such that their least common multiple is equal to m, i.e. $lcm(k_i : 1 \leq i \leq N) = m$. A divisor $D = P_1 + \cdots + P_N$.
- A divisor G, such that $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset$ and $\deg G = 2RmN_m$.
- For $1 \leq i \leq N_m$, we take C_i a linear $[m, k_i, d_i]_q$-code and $\phi_i : F_{P_i} \to C_i \subset \mathbf{F}_q^m$. Note that as vector spaces $\dim_{\mathbf{F}_q} F_{P_i} = \dim_{\mathbf{F}_q} C_i = k_i$, so ϕ_i is an isomorphism of vector spaces. Since C_i has length m, we can consider the image of ϕ_i as a subspace of $\mathbf{F}_q^m$.

Remark 3.8 The condition $k_i > 2Rm$ ensures that $\deg D = \sum_{i=1}^{N} k_i > 2RmN = \deg G$. This condition says that each code C_i has rate greater than $2R$. Later on this will be used to prove that the sequence of codes we have constructed is asymptotically good.

Since the least common multiple of all the k_i is m, every k_i is a divisor of m. Therefore the residue class field $F_{P_i} \cong \mathbf{F}_{q^{k_i}}$ can be embedded as a subfield of $\mathbf{F}_{q^m}$. Another consequence of $\frac{k_i}{m} > 2R$ is that if $2R \geq \frac{1}{2}$ then $k_i > \frac{1}{2}m$

and k_i divides m, therefore $k_i = m$ for all i, and all places must have the same degree m. Hence to construct codes with places of different degrees it is necessary that $R < \frac{1}{4}$.

We let $C'_m = C(D, G, \phi)$ be the generalized algebraic geometry code on the above data. It consists of all codewords of the form

$$\phi(z) = (\phi_1(z(P_1)), \phi_2(z(P_2)), \ldots, \phi_N(z(P_N))) \ \in (\mathbf{F}_q^m)^N$$

with $z \in \mathcal{L}(G)$. Let $k_u = \min\{k_i \mid 1 \leq i \leq N\}$ and $d_v = \min\{d_i \mid 1 \leq i \leq N\}$. Then by Corollary 2.12 C'_m is a $[mN, \dim \mathcal{L}(G), d]_q$-code with $d \geq d_v(N - \frac{\deg G}{k_u})$.

All the ϕ_i have image in $\mathbf{F}_q^m$. As before we give $\mathbf{F}_q^m$ the structure of a field by identifying it with $\mathbf{F}_{q^m}$. Let $\alpha \in \mathbf{F}_{q^m}$ be such that $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$. Now we define a map $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^m$ by

$$\psi(a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}) = (a_0, a_1, \ldots, a_{n-1}).$$

We set $\xi = \psi(\alpha)$. We define a linear isomorphism $\sigma_\xi : (\mathbf{F}_q^m)^N \to (\mathbf{F}_q^m)^N$ by

$$\sigma_\xi(x_0, x_1, \ldots, x_{N-1}) = (x_0, \xi x_1, \ldots, \xi^{N-1} x_{N-1}) \qquad \text{for } x_i \in \mathbf{F}_q^m.$$

We assume $N \leq q^m - 1$, then all powers $\xi^0, \xi, \ldots \xi^{N-1}$ are distinct, since α is a primitive element and has order $q^m - 1$. Applying σ_ξ to the code C'_m gives a code $\sigma_\xi C'_m$, with the same parameters.

Now we define C_m as the concatenation of C'_m and $\sigma_\xi C'_m$, i.e. $C_m = C'_m \sigma_\xi C'_m$. It consists of all code words of the form $(\phi(z), \sigma_\xi \phi(z)) =$

$$(\phi_1(z(P_1)), \ldots, \phi_N(z(P_N))), \phi_1(z(P_1)), \xi\phi_2(z(P_2)), \ldots, \xi^{N-1}\phi_N(z(P_N)))$$

with $z \in \mathcal{L}(G)$.

Lemma 3.9 *Let $N \leq q^m - 1$ and let $1 \leq i, j \leq N_m$ be such that $\phi_i(z(P_i)) \neq 0$ and $\phi_j(z(P_j)) \neq 0$. Then*

$$(\phi_i(z(P_i)), \xi^{i-1}\phi_i(z(P_i))) = (\phi_j(z(P_j)), \xi^{j-1}\phi_j(z(P_j))) \iff i = j.$$

Proof Suppose the two pairs are equal. Then since $\phi_i(z(P_i)) = \phi_j(z(P_j)) \neq 0$, we can divide it out in the second coordinate, yielding $\xi^{i-1} = \xi^{j-1}$. Both i and j are less than or equal to N and hence less than or equal to $q^m - 1$ which is the order of ξ. Therefore $i = j$. The other implication is trivial. □

Corollary 3.10 *Let $v \in C_m$. Then v has at least $d' \geq N - \frac{\deg G}{k_u}$ distinct nonzero pairs of the form $(\phi_i(z(P_i)), \xi^{i-1}\phi_i(z(P_i)))$.*

Proof This is immediate from the above lemma and lemma 2.13. □

Definition 3.11 Let λ and L be two integers with $0 < \lambda \leq L$. We define $M = \sum_{i=1}^{\lambda} (q-1)^i \binom{L}{i}$. To give a vector of weight i in $\mathbf{F}_q^L$ we must choose i out of L coordinates to be nonzero and for every nonzero coordinate there are $q-1$ possible values. Therefore the number of vectors in $\mathbf{F}_q^L$ of weight exactly i is $(q-1)^i \binom{L}{i}$. In this way we see that M is the number of nonzero vectors in $\mathbf{F}_q^L$ of weight $\leq \lambda$.

Let $v \in (\mathbf{F}_q^L)^N$. We denote the number of nonzero L-strings in v by $w_{q^L}(v)$ and the number of nonzero coordinates in $\mathbf{F}_q$ of v by $w(v)$. In other words $w(v)$ is the usual weight of v over $\mathbf{F}_q$.

Proposition 3.12 *Let $v = (v_1, \ldots, v_N) \in (\mathbf{F}_q^L)^N$ with $w_{q^L}(v) = d'$ be such that all nonzero v_i are distinct. Let $0 < \lambda \leq L$ be an integer. Then $\lambda(d' - M) \leq w(v) \leq Ld'$.*

Proof Remark that if $d' < M$ the first inequality is trivial. Let $v = (v_1, \ldots, v_N)$ with $v_i \in \mathbf{F}_q^L$. Let $R = \{i \mid v_i \neq 0\}$, let $R_{\leq\lambda} = \{i \in R \mid w(v_i) \leq \lambda\}$ and let $S = R \setminus R_{\leq\lambda}$. Then $|R| = d'$ and because all v_i with $i \in R$ are distinct it follows that $|R_{\leq\lambda}| \leq M$. Hence $|S| = d' - |R_{\leq\lambda}| \geq d' - M$. Now we have $w(v) = \sum_{i=1}^{N} w(v_i) = \sum_{i \in R} w(v_i) = \sum_{i \in R_{\leq\lambda}} w(v_i) + \sum_{i \in S} w(v_i) \geq \sum_{i \in S} w(v_i) > \lambda |S| \geq \lambda(d' - M)$.
Since $w(v_i) \leq L$ for all i we find that $w(v) \leq Ld'$. □

In the following $H_q(\mu)$ denotes the entropy function. From [9] we have the following lemma, which we will not prove here.

Lemma 3.13 *If $0 \leq \mu \leq \frac{1}{q}$ and L is a positive integer such that μL is an integer, then*

$$\sum_{i=0}^{\mu L} (q-1)^i \binom{L}{i} \leq q^{LH_q(\mu)} (1 + \mu(q-2))^L.$$

This lemma says that for $\mu = \frac{\lambda}{L} \leq \frac{1}{q}$ the number M of nonzero vectors in $\mathbf{F}_{q^L}$ of weight less than or equal to λ is bounded by $q^{LH_q(\mu)}(1 + \mu(q-2))^L$.

We fix a real number ϵ' satisfying $0 < \epsilon' \leq \frac{1}{q}$. We let λ depend on m such that $\epsilon' \leq \frac{\lambda}{2m} \leq \frac{1}{q}$. Note that M depends on λ and therefore also depends on m.

Proposition 3.14 *The limit of M/N tends to zero, as m tends to infinity.*

Proof Recall that $N \geq a^m q^{\frac{m}{2}}$. Let $\beta = 1 + \frac{\lambda}{2m}(q-2)$. By the above lemma with $L = 2m$ we have $M \leq q^{2mH_q(\frac{\lambda}{2m})} \beta^{2m}$. Now

$$\frac{M}{N} \leq \frac{q^{2mH_q(\frac{\lambda}{2m})} \beta^{2m}}{a^m q^{\frac{m}{2}}} = q^{m(2H_q(\frac{\lambda}{2m}) - \frac{1}{2})} \left(\frac{\beta^2}{a}\right)^m .$$

Since $\frac{\lambda}{2m} \leq \frac{1}{q}$ we have $\beta < 2$ and hence $\beta^2 < 4 \leq a$. Therefore $\left(\frac{\beta^2}{a}\right)^m$ tends to zero as m tends to infinity. It remains to show that $2H_q(\frac{\lambda}{2m}) < \frac{1}{2}$, or in other words that $H_q(\frac{\lambda}{2m}) < \frac{1}{4}$ for $\frac{\lambda}{2m} \leq \frac{1}{q}$. This is shown in [9]. □

Theorem 3.15 *The sequence of codes $(C_m)_m$ is asymptotically good.*

Proof First we compute the rate of C_m. This is

$$R(C_m) = \frac{\dim \mathcal{L}(G)}{2mN} \geq \frac{\deg G + 1 - g}{2mN} = \frac{2RmN}{2mN} + \frac{1-g}{2mN} = R + \frac{1-g}{2mN}.$$

Therefore as m tends to infinity, $\liminf R(C_m) \geq R > 0$.

To estimate the relative minimum distance δ_m, we recall that by lemma 2.13 any codeword v has at least $d' = N - \frac{\deg G}{k_u}$ nonzero strings of length $2m$. Using Proposition 3.12 with $L = 2m$, we find that $d = w(v) \geq \lambda(d' - M)$. Therefore the relative minimum distance is $\delta_m = \frac{d}{2mN} \geq \frac{\lambda(d'-M)}{2mN} = \frac{\lambda}{2m}(\frac{d'}{N} - \frac{M}{N})$. We choose λ such that $\frac{1}{q} \geq \frac{\lambda}{2m} \geq \epsilon' > 0$, for some fixed $\epsilon' > 0$. Note that λ, d', M and N all depend on m.

Now $\lim \frac{\lambda}{2m} \geq \epsilon' > 0$ and by Proposition 3.14 we have $\lim \frac{M}{N} = 0$. Now we compute $\lim \frac{d'}{N} \geq \lim \frac{1}{N}(N - \frac{\deg G}{k_u}) = 1 - \lim \frac{2RmN}{Nk_u} = 1 - \lim \frac{2Rm}{k_u}$. All the k_i satisfy $\frac{k_i}{m} > 2R + \epsilon$ for some $\epsilon > 0$. Therefore $\lim 1 - \frac{2Rm}{k_u} > \lim \frac{m}{k_u}\epsilon > 0$. We conclude that $\lim \delta_m \geq \epsilon'(\epsilon - 0) > 0$ and so the sequence of codes C_m is asymptotically good. □

Corollary 3.16 *If $\epsilon' \leq \lim_{m\to\infty} \frac{\lambda}{2m} \leq \frac{1}{q}$ and $\lim_{m\to\infty} \frac{k_u}{m} - 2R > \epsilon$, then the asymptotic rate of the above code is R and the asymptotic relative minimum distance satisfies*

$$\delta \geq \epsilon'\epsilon.$$

The highest lower bounds are achieved when all places have the same degree $k_i = m$ for all i and when we take λ such that $\epsilon' = \frac{\lambda}{2m} = \frac{1}{q}$ for all m. Then the code will satisfy

$$\lim_{m\to\infty} R(C_m) \geq R > 0 \qquad \text{and} \qquad \lim_{m\to\infty} \delta(C_m) \geq \frac{1}{q}(1 - 2R) > 0.$$

Chapter 4

Towers of algebraic function fields

Definition 4.1 *A tower of algebraic function fields over* $\mathbf{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_i over $\mathbf{F}_q$ with the following properties:

- For all i, $\mathbf{F}_q$ is the full constant field of F_i.
- For all i, $F_i \subset F_{i+1}$ is a finite separable algebraic extension of degree $[F_{i+1} : F_i] > 1$.
- The genus $g(F_i)$ tends to infinity as i tends to infinity.

Definition 4.2 A tower $\mathcal{F}$ of algebraic function fields over $\mathbf{F}_q$ is called *asymptotically exact* if for all $m \geq 1$ the following limit exists:

$$\beta_m(\mathcal{F}) = \lim_{i \to \infty} \frac{B_m(F_i)}{g(F_i)}$$

where $B_m(F_i)$ denotes the number of places of degree m on F_i. The sequence of real numbers $(\beta_1, \beta_2, \ldots)$ is called the *type* of the asymptotically exact tower.

The following theorem demonstrates the relevance of asymptotically exact towers in coding theory.

Theorem 4.3 *Let $r \geq 1$ be an integer and let $\mathcal{F}$ be a tower of algebraic function fields such that $\beta_r(\mathcal{F}) = \beta > 1$. Then there is an asymptotically good sequence of codes $(C_k)_{k \geq 1}$ associated to $\mathcal{F}$.*

Proof Let $\mathcal{F} = (F_k/\mathbf{F}_q)_{k \geq 1}$ be as above. Fix a number R with $\frac{1}{\beta} < R < 1$. Now for every k we take the following:

- Take $N_k = B_r(F_k)$ and let $D = D_k = \sum_{i=1}^{N_k} P_i$ be the divisor that is the sum of all places of degree r in F_k. Then $\deg D = rN_k$.
- Take $G = G_k$ a divisor of degree $\deg G = \lceil RN_k \rceil$ and such that Supp $G \cap$ Supp $D = \emptyset$.

- Let C_i for $1 \leq i \leq N_k$ be the linear $[r, r, 1]_q$-code $\mathbf{F}_{q^r} = C_i$ and let $\phi_i : F_{kP_i} \to \mathbf{F}_{q^r} \to \mathbf{F}_q^r$. be an isomorphism.

Now let C_k be the generalized algebraic geometry code $C_k = C(D, G, \phi)$. The code C_k has parameters $[rN_k, \dim \mathcal{L}(G_k), d_k]_q$, where $d_k \geq N_k - \frac{\deg G}{r}$ by Corollary 2.9. By the Riemann-Roch Theorem $\dim \mathcal{L}(G_k) \geq \deg G_k + 1 - g_k$. Now we compute the asymptotic parameters of the code.

$$\lim_{k\to\infty} \frac{\dim \mathcal{L}(G_k)}{rN_k} \geq \lim_{k\to\infty} \frac{\deg G_k + 1 - g_k}{rN_k} = \lim_{k\to\infty} \left(\frac{RN_k}{rN_k} + \frac{1}{rN_k} - \frac{g_k}{rN_k} \right) = \frac{1}{r}(R - \frac{1}{\beta}) > 0. \quad (4.1)$$

Here we have used that $N_k = B_r(F_k)$ and the last inequality is our assumption on R. For the relative minimum distance we find

$$\lim_{k\to\infty} \frac{d_k}{rN_k} \geq \lim_{k\to\infty} \frac{N_k}{rN_k} - \frac{\deg G}{r^2 N_k} = \lim_{k\to\infty} \frac{1}{r} - \frac{RN_k}{r^2 N_k} = \frac{1}{r}(1 - \frac{R}{r}) > 0. \quad (4.2)$$

We conclude that the sequence of codes is asymptotically good. □

It is remarkable that this proof is so straightforward, in contrast with the previous chapter where a lot of work was needed to prove that the asymptotic minimum distance is positive. In particular we did not need the modification of the GAG code, where the code is doubled and the last part is multiplied by powers of ξ. It seems that all the difficulties are taken away by using an asymptotically exact tower. Hence we can expect that if such a tower exists, its construction will be a difficult problem. We prove the existence of asymptotically exact towers in Theorem 4.15. However this proof is not constructive. An explicit construction of an asymptotically exact tower will be given in Section 4.2. The above theorem not only assumes that an asymptotically exact tower exists, but also that for at least one integer r it has $\beta_r > 1$. It is therefore an important question if we can construct exact towers with this property. We will look at this in Section 4.3.1.

One might ask if the parameters of a sequence of codes can be improved by combining the construction in Section 3.2 with the use of an asymptotically exact tower. In the next section we will see if this is indeed the case and we will also look at other variations of MGAG codes to see if they can lead to improvement.

4.1 Variations on MGAG codes

We start by analyzing how the parameters of a MGAG code change, when the underlying function field is not fixed, but varies within an exact tower of function fields. Later on we study codes using a fixed function field F, where the places do not have a fixed degree m, but instead we use *all* places of degree less than or equal to m. In other words we take the maximum possible number of places of degree less than m. Finally we look at a code having only m places, one for each integer less than or equal to m.

4.1.1 MGAG codes in a tower

Let $r \geq 1$ be an integer and let $\mathcal{F} = (F_k)_{k\geq 1}$ be an exact tower of algebraic function fields with $\beta_r(\mathcal{F}) = \beta > 1$. Let $\frac{1}{\beta} < R < 1$.

- $N = B_r(F_k)$. (If $q^r < B_r(F_k)$, we take $N = q^r - 1$.)
- $D = \sum_{i=1}^{N} P_i$ with $\deg P_i = r$ is the divisor that is the sum of all places of degree r. $\deg D = rN$.
- G a divisor disjoint from D with $\deg G = \lceil RN \rceil$.
- $C_i = \mathbf{F}_q^r$ is a linear $[r, r, 1]_q$-code. $\phi_i : F_{kP_i} \to C_i = \mathbf{F}_q^r$ an $\mathbf{F}_q$-linear isomorphism.

Let $C'_k = C(D, G, \phi)$ denote the generalized algebraic geometry code with divisors D and G as defined in definition 2.8. Let α be an element of order $q^r - 1$ in $\mathbf{F}_{q^r}$ such that $\mathbf{F}_{q^r} \cong \mathbf{F}_q(\alpha)$. Let $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^r$ be defined as in equation 3.1 (with $m = r$). We take $\xi = \psi(\alpha)$ and σ_ξ as before. Let $C_k = C'_k \sigma_\xi C'_k$. We compute the parameters of C_k and compare these with the code in section 3.2.

The dimension of C_k is equal to $\dim \mathcal{L}(G) \geq \deg G + 1 - g_k$ and therefore the rate is

$$\frac{\dim \mathcal{L}(G)}{2rN} \geq \frac{\deg G + 1 - g_k}{2rN} = \frac{R}{2r} - \frac{1}{2r}\frac{g_k}{N} + \frac{1}{2rN}.$$

When k tends to infinity the limit of the rate is $\frac{1}{2r}(R - \frac{1}{\beta}) > 0$. For the minimum distance we first note that the number of distinct nonzero pairs of the form $(\phi_i(z(P_i)), \xi^{i-1}\phi_i(z(P_i)))$ is at least $d' \geq N - \frac{\deg G}{r}$ by corollary 3.10. Then from Proposition 3.12 and lemma 3.13 it follows that for any integer $\lambda \leq \frac{2r}{q}$ the weight $w(v)$ of any $v \in C_k$ satisfies

$$w(v) \geq \lambda(d' - M) \geq \lambda d' - \lambda q^{2rH_q(\frac{\lambda}{2r})}(1 + \frac{\lambda}{2r}(q-2))^{2r}.$$

Here M is the number of vectors in $\mathbf{F}_q^{2r}$ of weight less than or equal to λ. The relative minimum distance is $\delta \geq \frac{\lambda(d'-M)}{2rN} = \frac{\lambda}{2r}(\frac{d'}{N} - \frac{M}{N})$. We choose λ such that $\frac{1}{q} \geq \frac{\lambda}{2r} > \epsilon' > 0$, for some fixed $\epsilon' > 0$. The limit of M/N is zero by Proposition 3.14. The other limit is

$$\lim \frac{d'}{N} = \lim \frac{N - \frac{\deg G}{r}}{2rN} = \frac{1}{2r}(1 - \frac{R}{r}) > 0.$$

We conclude that for this code the rate and relative minimum distance satisfy

$$\lim_{m\to\infty} R(C_k) \geq \frac{1}{2r}(R - \frac{1}{\beta}) > 0 \qquad \text{and} \qquad \lim_{m\to\infty} \delta(C_k) \geq \frac{\epsilon'}{2r}(1 - \frac{R}{r}) > 0.$$

We conclude that the sequence of codes is asymptotically good, for a fixed r. We can also see that the parameters of the code depend on r and decrease

when r increases. Comparing these bounds with equations 4.1 and 4.2 we see that the rate is reduced by a factor $\frac{1}{2}$ and the relative minimum distance is reduced by a factor $\frac{\epsilon'}{2} \leq \frac{1}{2q}$. Comparing these bounds to section 3.2 we see that for a large enough value of r we get $\frac{1}{2r}(R - \frac{1}{\beta}) < R$ and $\frac{\epsilon'}{2r}(1 - \frac{R}{r}) < \frac{1}{q}(1 - 2R)$. Hence the modification of the construction does not give better lower bounds for the parameters.

4.1.2 A code using many places

Let F be an algebraic function field of genus g. We wish to explore if it is possible to construct a MGAG code using not just places in F of some fixed degree m, but using *all* places of degree less than or equal to m. If such a construction is possible, we will try to use it for constructing a sequence of codes. Furthermore, we wish to find reasonable bounds for the parameters of such a sequence and see if it is asymptotically good.

Keeping in mind that the function field F is fixed, we write B_r for $B_r(F)$, the number of places of F of degree r.

- Fix a real number R with $0 < R < 1$ and an integer $m \geq 1$.
- Let $N = \sum_{i=1}^{m} B_i$ be the number of places of degree $\leq m$.
- Let D be the divisor of F that is the sum of all places of degree $\leq m$, so $D = \sum_{i=1}^{N} P_i$ with $\deg P_i \leq m$ and all the P_i distinct. $\deg D = \sum_{i=1}^{m} iB_i$.
- Take G a divisor of degree $\lfloor RN \rfloor$, the largest integer smaller than or equal to RN.

Let α be a generating element for $\mathbf{F}_{q^m}$ of order $q^m - 1$, so $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$. We use this element α as in equation 3.1 to fix an isomorphism $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^m$. For $1 \leq j \leq m$ we take $C_j = \mathbf{F}_{q^j}$. So C_j is a $[j, j, 1]_q$-code. If j does not divide m we cannot embed $\mathbf{F}_{q^j}$ as a subfield of $\mathbf{F}_{q^m}$. However it is always possible to choose a $\mathbf{F}_q$-linear injection of vector spaces $\iota_j : \mathbf{F}_{q^j} \to \mathbf{F}_q^m$. For every place P_i of degree j we choose a linear isomorphism $\tau_i : F_{P_i} \to C_j$ and we define $\phi_i = \iota_j \circ \tau_i$ to be the composition $F_{P_i} \to C_i \to \mathbf{F}_q^m$ of these two maps. We define a map $\phi : \mathcal{L}(G) \to (\mathbf{F}_q^m)^N$ by setting

$$\phi(z) = (\phi_1(z(P_1)), \phi_2(z(P_2)), \ldots, \phi_N(z(P_N))) \quad \text{for all } z \in \mathcal{L}(G).$$

Let $C_m = C(D, G, \phi)$ denote the generalized algebraic geometry code that is the image of ϕ. It has length $mN = m\sum_{i=1}^{m} B_i$. Its dimension is equal to the dimension of $\mathcal{L}(G)$, since the map ϕ is injective when $\deg G < \deg D$. So by the Riemman-Roch Theorem its dimension is at least $\deg G + 1 - g$. Its minimum distance d satisfies $d \geq N - \deg G = N - \lfloor RN \rfloor \geq N(1 - R)$. The rate is

$$R(C_m) \geq \frac{\deg G + 1 - g}{mN} \geq \frac{RN}{mN} - \frac{g}{mN} = \frac{1}{m}(R - \frac{g}{N}).$$

The relative minimum distance is

$$\delta(C_m) \geq \frac{N - \deg G}{mN} \geq \frac{1}{m}(1 - R).$$

When the function field F is fixed, the only possible way to let the lengths of the codes tend to infinity is by having places of arbitrary high degree m. Therefore also m must tend to infinity. The lower bounds for the parameters of these codes tend to zero as m tends to infinity. So we cannot say that the code is asymptotically good. However if m is bounded or fixed, then the lower bounds for the rate and relative minimum distance guarantee that the code is asymptotically good. To let the length of the code still tend to infinity we need infinitely many places of degree less than or equal to m. We can only achieve this by using an asymptotically exact tower $\mathcal{F}$, such that the genus tends to infinity and $\lim_{g_k \to \infty} \frac{\sum_{i=1}^{m} B_i}{g_k} = \sum_{i=1}^{m} \beta_i(\mathcal{F}) > 1$. Then it is necessary to take $1 < \frac{1}{R} < \sum_{i=1}^{m} \beta_i(\mathcal{F})$.

4.1.3 A code using very few places

Let F be an algebraic function field of genus g. Instead of using all places of degree m, we investigate the construction and parameters of a MGAG code using only one place of degree i for each $i \leq m$. A first problem that arises is that for small i, there may not exist any place of degree i. For large enough i we do not have this problem, because Corollary V.2.10 c) in [10] tells us that for $i \geq 4g + 3$ there is at least one place of degree i.

We now construct a code with no more than one place of each degree. Let us define $l = 4g + 3$.

- Fix a real number R with $0 < R < \frac{1}{2}$ and integers $m \geq l$ and $a \geq 2$.
- Let D be the divisor of F that is defined by $D = \sum_{i=l}^{m} P_i$ with $\deg P_i = i$. Then all the P_i are distinct. $\deg D = \sum_{i=l}^{m} i = \frac{1}{2}m(m+1) - \frac{1}{2}l(l-1)$.
- Take G a divisor with $\deg G = \lfloor Rm^2 \rfloor$. Then $\deg G < \frac{1}{2}m(m+1)$. For m sufficiently large we will have $\deg G < \deg D$, because l is fixed.

Let α be a generating element for $\mathbf{F}_{q^m}$ of order $q^m - 1$, so $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$. We use this element α as in equation 3.1 to fix an isomorphism $\psi : \mathbf{F}_q(\alpha) \to \mathbf{F}_q^m$. For $l \leq i \leq m$ we take $C_i = \mathbf{F}_{q^i}$ a $[i, i, 1]_q$-code. If i does not divide m we cannot embed $\mathbf{F}_{q^i}$ as a subfield of $\mathbf{F}_{q^m}$. However we always have a $\mathbf{F}_q$-linear injection of vector spaces $\iota_i : \mathbf{F}_{q^i} \to \mathbf{F}_q^m$. For every place P_i of degree i we choose a linear isomorphism $F_{P_i} \to C_i$ and we write $\phi_i : F_{P_i} \to \mathbf{F}_q^m$ for the composition of this isomorphism with ι_i. We define a map $\phi : \mathcal{L}(G) \to (\mathbf{F}_q^m)^{m-l}$ by setting

$$\phi(z) = (\phi_l(z(P_l)), \phi_{l+1}(z(P_{l+1})), \ldots, \phi_m(z(P_m))) \quad \text{for all } z \in \mathcal{L}(G).$$

Let $C_m = C(D, G, \phi)$ denote the generalized algebraic geometry code that is the image of ϕ. It has length $m(m - l)$. Since the map ϕ is injective when $\deg G < \deg D$, its dimension is equal to $\dim \mathcal{L}(G)$ and therefore, by

the Riemman-Roch theorem, greater then or equal to $\deg G + 1 - g$. Its minimum distance d satisfies $d \geq m - \deg G \geq m(1 - Rm)$ The rate is

$$R(C_m) \geq \frac{\deg G + 1 - g}{m^2} \geq \frac{Rm^2}{m^2} - \frac{g}{m^2} = R - \frac{g}{m^2}.$$

The relative minimum distance is

$$\delta(C_m) \geq \frac{m - \deg G}{m^2} = \frac{1}{m}(1 - mR).$$

Here we immediately see a problem. As soon as m becomes greater than $\frac{1}{R}$ this lower bound becomes trivial, because then $(1 - mR) < 0$. To make an asymptotically good code a modification is necessary. A first idea is to modify the code in such a way that Proposition 3.12 can be used. However, this will only give an improvement of the lower bound if $d' > M$. In this case that would mean that we require $m(1 - Rm) > (q - 1)2m$, where we have taken $M = (q - 1)2m$ the number of vectors of weight one in $\mathbf{F}_q^{2m}$. It is obvious that this inequality never holds. Therefore the method of section 3.2 will not give any improvement.

Both the asymptotically good sequence of codes in Theorem 4.3 and the sequence in the previous chapter are constructed using generalized algebraic geometry codes. The difference is that in the construction using a tower, the function field varies and the degree of the places remains fixed, whereas in the previous chapter the function field is fixed and the degree of the places increases.

Questions that now arise are: Do these asymptotically exact towers exist? How can they be constructed? We will see the construction of an asymptotically exact tower in the next section.

4.2 A tower of Artin-Schreier extensions

We give an example of an asymptotically exact tower $\mathcal{F}$ defined over $\mathbf{F}_{q^2}$, with $\beta_1(\mathcal{F}) = q - 1$. The definition of this tower and more details about its properties can be found in [3]. Extensions $F \subset F(T)$ where T satisfies an equation of the form $T^q - T = w$ for some $w \in F$ are called Artin-Schreier extensions. If, as in our case, the base field is $\mathbf{F}_{q^2}$, then extensions given by an equation of the form $T^q + T = w$ for some $w \in F$ are also called Artin-Schreier extensions.

Definition 4.4 Let $F_1 = \mathbf{F}_{q^2}(x_1)$ be the rational function field over $\mathbf{F}_{q^2}$. For $n \geq 1$, we set

$$F_{n+1} = F_n(z_{n+1}),$$

where z_{n+1} satisfies the equation

$$z_{n+1}^q + z_{n+1} = x_n^{q+1},$$

with

$$x_n = \frac{z_n}{x_{n-1}} \in F_n \qquad \text{for } n \geq 2.$$

4.2.1 The genus of F_n

For all n let $g_n = g(F_n)$ be the genus of F_n and let $N_n = B_1(F_n)$ be the number of places of F_n of degree one. The tower has the following properties

Theorem 4.5 *The genus g_n is given by the following formula:*

$$g_n = \begin{cases} q^n + q^{n-1} - q^{\frac{n+1}{2}} - 2q^{\frac{n-1}{2}} + 1, & \text{if } n \text{ is odd,} \\ q^n + q^{n-1} - \frac{1}{2}q^{\frac{n}{2}+1} - \frac{3}{2}q^{\frac{n}{2}} - q^{\frac{n}{2}-1} + 1, & \text{if } n \text{ is even.} \end{cases} \tag{4.3}$$

The number N_n satisfies the following inequality:

$$N_n \geq (q^2 - 1)q^{n-1} + 2q \qquad \text{for all } n \geq 3. \tag{4.4}$$

Corollary 4.6

$$\lim_{n\to\infty} \frac{N_n}{g_n} = q - 1.$$

Proof From the above theorem it follows immediately that

$$\liminf_{n\to\infty} \frac{N_n}{g_n} \geq q - 1.$$

Recall Definition 3.3 and the comments following it on page 31. There it was stated that $A(q^2) \leq q - 1$. This implies that

$$\limsup_{n\to\infty} \frac{N_n}{g_n} \leq q - 1.$$

We conclude that $\liminf \frac{N_n}{g_n} = \limsup \frac{N_n}{g_n}$, hence the limit $\lim \frac{N_n}{g_n}$ exists and is equal to $q - 1$. This completes the proof. □

A complete proof of Theorem 4.5 is given in [3]. We will give an overview of the proof given there and its most important ingredients.

The most difficult part is the calculation of the genera. A recursive relation for the genera is found with help of the *Hurwitz genus formula*. From this recursive formula the result in 4.5 is deduced. To use the Hurwitz genus formula one must first know the degrees $[F_{i+1} : F_i]$ and $[K_{i+1} : K_i]$, where K_i is the full constant field of F_i, and the *different* $\mathrm{Diff}(F_{i+1}/F_i)$. For the latter, one needs to determine all the places in F_i that ramify and for each of those places calculate the *different exponent* $d(P'|P)$.

Theorem 4.7 *[Hurwitz Genus Formula] Let F/K be an algebraic function field of genus g and F'/F be a finite separable extension. Let K' denote the constant field of F' and g' the genus of F'/K'. Then we have*

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

This is theorem III.4.12 in [10].

Definition 4.8 The different $\mathrm{Diff}(F'/F)$ is a divisor of F' defined as

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

For the definition of the different exponent we refer to section III.4 in [10]. All we need to know for now is stated in Lemma 4.12.

Outline of the proof of Theorem 4.5

Let us recall that the tower is defined by $F_1 = \mathbf{F}_{q^2}(x_1)$. For $n \geq 1, F_{n+1} = F_n(z_{n+1})$, where $z_{n+1}^q + z_{n+1} = x_n^{q+1}$ and $x_n = \frac{z_n}{x_{n-1}} \in F_n$ for $n \geq 2$.

Lemma 4.9 *Suppose that a place P of F_n is a simple pole of x_n. Then the extension F_{n+1}/F_n has degree $[F_{n+1} : F_n] = q$ and P is totally ramified in F_{n+1}/F_n. The place P' lying above P is a simple pole of x_{n+1}.*

Lemma 4.10 *For all $n \geq 1$, K is algebraically closed in F_n, hence $[K_{n+1} : K_n] = 1$. The degree of the extension F_{n+1}/F_1 is $[F_{n+1} : F_1] = q^{n-1}$.*

Lemma 4.11 *For all $n \geq 1$ there exists a unique place Q_n of F_n of degree one, such that $v_{Q_n}(x_k) = q^{k-1}$ for $1 \leq k \leq n$ and $v_{Q_n}(z_k) > 0$ for $2 \leq k \leq n$. The place Q_n splits into q places of F_{n+1} of degree one, one of them being Q_{n+1}*

Lemma 4.12 *Let P in F_n be a place that is ramified in F_{n+1}. Then P is totally ramified. Denote by P' the unique place of F_{n+1} lying over P. Let m_P be defined by*

$$v_P(x_n^{q+1}) = -m_P, \quad m_P > 0 \text{ and } \gcd(m_P, q) = 1.$$

Then the different exponent $d(P'|P)$ is given by

$$d(P'|P) = (q-1)(m_P + 1).$$

The next step in the proof of Theorem 4.5 is to define recursively for every n a set $S^{(n)}$ of places in F_n. The places in $S^{(n)}$ are all extensions of places in $S^{(n-1)}$ or extensions of the place Q_i for some $i < n$. Later it is shown that $S^{(n)}$ is equal to the set of places in F_n that are ramified.

Lemma 4.13 *For $P \in S^{(n)}$, we have $v_P(x_n) = -1$.*

Hence for $P \in S^{(n)}$, $m_P = v_P(x_n^{q+1}) = -(q+1)$ and therefore

$$d(P'|P) = (q-1)(m_P + 1) = (q-1)(q+2).$$

From this and the Hurwitz Genus Formula and some extra work a recursion formula for the genus g_n follows. The inequality for the number of places of degree one N_n is extracted from results about the sets $S^{(n)}$ along the way. In fact equality holds for 4.4 if q is odd. If q is even and $n \geq 5$, then $N_n = (q^2-1)q^{n-1} + 2q^2$.

4.2.2 Ramification calculations

In this section we give some explicit calculations to demonstrate the phenomenon of ramification and to illustrate the proof of Theorem 4.5. We take $q = 2$. For the first two fields in the tower we will calculate local parameters for the places that ramify. For simplicity let $x = x_1, y = z_2, \frac{y}{x} = x_2, z = z_3$. The first field is just the rational function field $F_1 = \mathbf{F}_4(x)$. The second field F_2 is the function field of an elliptic curve $\mathbf{F}_4[x, y]/(y^2 + y + x^3)$. The third field F_3 is the field $\mathbf{F}_4(x, y, z)$ where x, y, z satisfy the relations $y^2 + y + x^3 = z^2 + z + (\frac{y}{x})^3 = 0$. To study these function fields we look at the following affine coordinate rings:

$$A_1 = \mathbf{F}_4[x] \tag{4.5}$$
$$A_2 = \mathbf{F}_4[x, y]/(y^2 + y + x^3) \tag{4.6}$$
$$A_3 = \mathbf{F}_4[u, x, y, z]/(ux - 1, y^2 + y + x^3, z^2 + z + y^3u^3). \tag{4.7}$$

At each level we will look at the prime ideals that ramify. In F_1, the place at infinity that corresponds to a zero of $\frac{1}{x}$, is the only place that ramifies in F_2. To check this we need to make a change of coordinates. We define

$$u = \frac{1}{x}, \quad v = \frac{y}{x^2}, \quad \text{it then follows that } x = \frac{1}{u}, \quad y = \frac{v}{u^2}.$$

Then we have

$$A_1' = \mathbf{F}_4[u] \quad \text{and} \quad A_2' = \mathbf{F}_4[u, v]/(v^2 + vu^2 + u).$$

We define $P_\infty = P_\infty^{(1)} = uA_1' = (u)$. We look at the factorization of uA_2' in A_2'. Setting $u = 0$ in A_2' we get $\mathbf{F}_4[v]/(v^2)$ from which we can guess that (u) factors as $(v)^2$ in A_2'. Indeed from the relation $v^2 = u(1 + vu)$ we see that $(v)^2 \subset (u)$. For the other inclusion we use $u = v^2 + vu^2$, so $u^2 = v^4 + v^2u^4 = v^2(v^2 + u^4)$. Now $u = v^2 + vu^2 = v^2 + v^3(v^2 + u^4) \in (v)^2$. We conclude that P_∞ ramifies in A_2' as $(v)^2$ with ramification index two and that v is a local parameter for the unique ideal $P_\infty^{(2)}$ above P_∞. Note that $u \in (v)$ and therefore $(v) = (u, v)$ is a maximal ideal.

The places of F_2 that ramify in F_3 are $P_\infty^{(2)} = vA_2'$ and $P_2 = xA_2 + (y + 1)A_2 = (x, y + 1)$. Now we try to find generators and a local parameter for the ideal $P_\infty^{(3)}$ above $P_\infty^{(2)}$. To do this we wish to compute the valuation $v_{3\infty}$ corresponding to $P_\infty^{(3)}$. Let $v_{2\infty}$ be the valuation corresponding to $P_\infty^{(2)}$. Now $v_{2\infty}(v) = 1$, because v is a local parameter. Furthermore $2 = v_{2\infty}(v^2) = v_{2\infty}(vu^2 + u) = v_{2\infty}(u) + v_{2\infty}(1 + vu) = v_{2\infty}(u)$. So $v_{2\infty}(u) = 2$. Using the relations for x and y we easily find that $v_{2\infty}(x) = v_{2\infty}(u^{-1}) = -2$ and $v_{2\infty}(y) = v_{2\infty}(v) - 2v_{2\infty}(u) = 1 - 4 = -3$.

Let $v_{3\infty}$ be the valuation corresponding to $P_\infty^{(3)}$. Now $v_{3\infty}(v) = 2v_{2\infty}(v) = 2$, because the ramification index of $P_\infty^{(3)}$ over $P_\infty^{(2)}$ is two. For the same reason $v_{3\infty}(u) = 4$. In u, v, z coordinates the equation $z^2 + z = \frac{y^3}{x^3}$ becomes $z^2 + z = \frac{v^3}{u^3}$. Therefore $v_{3\infty}(z^2 + z) = 3v_{3\infty}(v) - 3v_{3\infty}(u) = -6$. From

this it follows that $v_{3\infty}(z) = -3$. Now we define $t = \frac{v}{zu}$ and we check that $v_{3\infty}(t) = v_{3\infty}(v) - v_{3\infty}(z) - v_{3\infty}(u) = 2 + 3 - 4 = 1$. So we have found that $t = \frac{v}{zu} = \frac{y}{zx}$ is a local parameter for $P_\infty^{(3)}$.

Now we look for a polynomial equation for t in u and v. We substitute $z = \frac{v}{tu}$ in the equation $z^2 + z + \frac{v^3}{u^3}$ and get $\frac{v^2}{t^2u^2} + \frac{v}{tu} = \frac{v^3}{u^3}$. We multiply by $\frac{u^3t^2}{v}$ and get $vu + u^2t = v^2t^2$. Finally we substitute $v^2 = u(1 + uv)$ on the right hand side and divide by u to get $v + ut = (1 + uv)t^2$. Now we can write down an affine coordinate ring for the open set where t is a regular function, that is where $z \neq 0$ and $u \neq 0$. This is the ring

$$A_3' = \mathbf{F}_4[u, v, t]/(v^2 + vu^2 + u, t^2(1 + uv) + ut + v).$$

We can identify $P_\infty^{(3)}$ with the ideal $(u, v, t) = (t)$ in this ring. Dividing out by the ideal $P_\infty^{(2)} = (u, v)$, that is setting $v = 0$ and $u = 0$, we get $\mathbf{F}_4[t]/(t^2)$. The ideal $P_\infty^{(2)} = (v)$ factors in this ring as $P_\infty^{(2)} = (t)^2 = P_\infty^{(3)2}$.

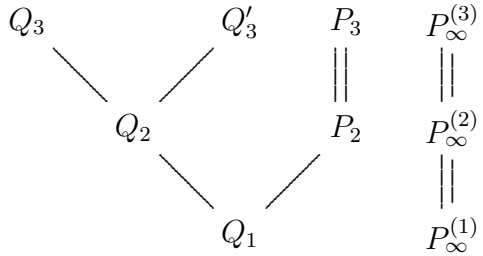
Let P_3 be the place in F_3 that lies above $P_2 = (x, y + 1)$ in F_2. To show that P_2 ramifies, we find a local parameter for P_3. Let v_{P_3} be the valuation of P_3. Since x is a zero of P_2, we know that $v_{P_3}(x) > 0$. Because y is a unit in the local ring $\mathcal{O}_{P_3}$ at P_3, we have $v_{P_3}(y) = 0$. We rewrite the equation $z^2 + z = \frac{y^3}{x^3}$ as $x^3z(z + 1) = y^3$. Applying the valuation v_{P_3} we get $3v_{P_3}(x) + 2v_{P_3}(z) = 0$. If $v_{P_3}(z) \geq 0$, the left hand side would not be equal to zero, therefore $v_{P_3}(z + 1) = v_{P_3}(z) < 0$. From $3v_{P_3}(x) = -2v_{P_3}(z)$ we find that $v_{P_3}(x)$ is divisible by 2 and since it also positive we must have $v_{P_3}(x) = 2$. Hence $v_{P_3}(z) = -3$. It now follows that for $r = \frac{1}{zx}$ we have $v_{P_3}(r) = -v_{P_3}(z) - v_{P_3}(x) = 3 - 2 = 1$, so r is a local parameter for P_3.

Now we look for a polynomial equation for r in x and y. We substitute $z = \frac{1}{rx}$ in the equation $z^2 + z + \frac{y^3}{x^3}$ and get $\frac{1}{r^2x^2} + \frac{1}{rx} = \frac{y^3}{x^3}$. We multiply by x^3r^2 and get $x + rx^2 = r^2y^3$. Now we can write down a new affine coordinate ring for F_3, where r is one of the coordinates.

$$A_3 = \mathbf{F}_4[x, y, r]/(y^2 + y + x^3,\ y^3r^2 + rx^2 + x).$$

We can identify P_3 with the ideal $(x, y+1, r) = (r)$ in this ring. Dividing out by the ideal $P_2 = (x, y+1)$, that is setting $x = 0$ and $y = 1$, we get $\mathbf{F}_4[r]/(r^2)$. We conclude that the ideal P_2 factors in this ring as $P_2 = (r)^2 = P_3^2$.

We summarize our result in the following diagram:



Double edges indicate ramification.

$Q_3 = (x, y, z)$, $Q_3' = (x, y, z+1)$, $P_3 = (x, y+1, r)$, $P_\infty^{(3)} = (t)$.
$Q_2 = (x, y)$, $P_2 = (x, y+1)$, $P_\infty^{(2)} = (v)$
$Q_1 = (x)$, $P_\infty^{(1)} = (u)$.

Now we have found the places that ramify, we can calculate the genera of F_2 and F_3 using Theorem 4.7 and verify formula 4.3 for $q = 2$ and $n = 2, 3$.

We know that $g_1 = 0$, because F_1 is the rational function field. The different exponent for each place that ramifies is given by lemma 4.13 and is equal to 4. So $d(P_\infty^{(2)}|P_\infty^{(1)}) = 4$. Using definition 4.8 we calculate that $\mathrm{Diff}(F_2/F_1) = 4P_\infty^{(2)}$, so $\deg \mathrm{Diff}(F_2/F_1) = 4$. Hence the Hurwitz genus formula 4.7 now gives

$$2g_2 - 2 = 2(2g_1 - 2) + 4,$$

from which it follows that $g_2 = 1$.

Similarly $\mathrm{Diff}(F_3/F_2) = 4P_\infty^{(3)} + 4P_3$, so $\deg \mathrm{Diff}(F_3/F_2) = 8$. Applying theorem 4.7 gives $2g_3 - 2 = 2(2g_2 - 2) + 8$ from which it follows that $g_3 = 5$. We see that these values for g_2 and g_3 are consistent with equation 4.3.

A primitive element for F_3/F_1

It is possible to generate F_3 with two elements x, w as $F_3 = \mathbf{F}_4(x, w)$, where w satisfies a polynomial $\phi_3(T) \in \mathbf{F}_4(x)[T]$. One could take $w = y + z$. Then one can check that w is a root of

$$\phi_3(T) = T^4 + \frac{1}{x^3}T^2 + (1 + \frac{1}{x^3})T + x^6 + 1.$$

To verify that w is a generator we express z and y as rational functions in x and w.

$$w^2 + w = y^2 + y + z^2 + z = x^3 + \frac{y^3}{x^3}.$$

So $y^3 = x^3(w^2 + w + x^3)$

$$y^3 = yy^2 = y(y + x^3) = y^2 + yx^3 = y + x^3 + yx^3 = y(x^3 + 1) + x^3.$$

So $y = \frac{y^3+x^3}{x^3+1}$. Substituting y^3 we can express y as

$$y = \frac{x^3(w^2 + w + x^3) + x^3}{x^3 + 1}.$$

Finally we can express z in x and w using the above equation for y and the relation $z = w + y$. In fact for all q and all n there is a polynomial $\phi_n(T) \in \mathbf{F}_q(x)[T]$ such that $\mathbf{F}_q(x)[T]/\phi_n(T)$ is isomorphic to the field F_n.

4.3 Exact towers

Definition 4.14 Let $\mathcal{F} = (F_k)_{k\geq 1}$ be a tower of algebraic function fields. Let $f : \mathbf{N} \to \mathbf{N}$ be a strictly increasing function, that is $f(i) < f(j)$ for all $i < j$. The tower $(F_{f(k)})_{k\geq 1}$ is called a *subtower* of $\mathcal{F}$.

Theorem 4.15 *Let $\mathcal{F} = (F_k)_{k\geq 1}$ be a tower of algebraic function fields defined over a finite field $\mathbf{F}_q$, for which the genus $g_k = g(F_k)$ tends to infinity as k tends to infinity. Then $\mathcal{F}$ admits an asymptotically exact subtower.*

Proof We start by showing that for every integer r, the sequence $\frac{B_r(F_k)}{g_k}$ with $k \geq 1$ is bounded. From lemma V.2.10 in [10] we can conclude that $B_r < \frac{1}{r}q^r + \frac{1}{r}q^{\frac{r}{2}}(2+7g)$. This bound does not depend on the function field itself, only on its genus g. We divide this inequality by g and let g grow to infinity,

$$\frac{B_r}{g} < \frac{q^r}{rg} + \frac{1}{r}q^{\frac{r}{2}}(7+\frac{2}{g}) < \frac{7}{r}q^{\frac{r}{2}}.$$

Since this holds for all function fields F_k, the sequence $(\frac{B_r(F_k)}{g_k})_{k\geq 1}$ is bounded from above by $\frac{7}{r}q^{\frac{r}{2}}$ and from below by zero. Since any sequence of real numbers contained in a bounded interval admits a convergent subsequence, we can conclude that the tower $\mathcal{F}$ admits a subtower for which $\beta_r(\mathcal{F})$ exists. Moreover $\beta_r \leq \frac{7}{r}q^{\frac{r}{2}}$.

Now we will construct a subtower of $\mathcal{F}$ such that all the limits β_r exist simultaneously for all r. By the above we can find a strictly increasing function $f_1 : \mathbf{N} \to \mathbf{N}$, such that $\mathcal{F}^{(1)} = (F_k^{(1)})_{k\geq 1}$ where $F_k^{(1)} = F_{f_1(k)}$, is a subtower of $\mathcal{F}$ for which the limit β_1 exists. We define towers $\mathcal{F}^{(i)}$ recursively: let $\mathcal{F}^{(i)} = (F_k^{(i)})_{k\geq 1}$ be a tower for which the limits $\beta_1, \ldots, \beta_i$ exist. We define $\mathcal{F}^{(i+1)}$ by taking a strictly increasing function $f_{i+1} : \mathbf{N} \to \mathbf{N}$, such that $\mathcal{F}^{(i+1)} = (F^{(i)}_{f_{i+1}(k)})_{k\geq 1}$ is a subtower of $\mathcal{F}^{(i)}$ for which the limits $\beta_1, \ldots, \beta_{i+1}$ exist. Note that for integers s, t the function field $F_t^{(s)}$ is the t-th function field in $\mathcal{F}^{(s)}$, so $F_t^{(s)} = F_{f_s f_{s-1} \cdots f_1(t)}$.

We now define the diagonal tower $\mathcal{D} = (F_k^{(k)})_{k\geq 1}$. It is a subtower of $\mathcal{F}$, because $F_k^{(k)}$ is a function field that occurs in the tower $\mathcal{F}$ and $F_k^{(k)} \subset F^{(k)}_{f_{k+1}(k)} \subset F^{(k)}_{f_{k+1}(k+1)} = F_{k+1}^{(k+1)}$. Let $r \geq 1$ be an integer. For $k \geq r$ the function fields of $\mathcal{D}$ are a subtower of $\mathcal{F}^{(r)}$, therefore the limit $\beta_r(\mathcal{D})$ exists. This completes the proof. □

The following Proposition is a generalization of Proposition 2.3 in [1].

Proposition 4.16 *Let $\mathcal{F}/\mathbf{F}_q = (F_k)_{k\geq 1}$ be an asymptotically exact tower of algebraic function fields defined over $\mathbf{F}_q$. Let $\mathbf{F}_{q^m}\mathcal{F}/\mathbf{F}_{q^m} = (\mathbf{F}_{q^m}F_k)_{k\geq 1}$ be the tower obtained after extending the base field from $\mathbf{F}_q$ to $\mathbf{F}_{q^m}$. Then $\mathbf{F}_{q^m}\mathcal{F}$ is an asymptotically exact tower over $\mathbf{F}_{q^m}$. For r a positive integer*

$$\beta_r(\mathbf{F}_{q^m}\mathcal{F}) = \sum_{l\in T_r} \frac{l}{r}\beta_l(\mathcal{F}),$$

where $T_r = \{l \mid l = r \cdot \gcd(l, m)\}$.

Proof Note that for constant field extensions the genus does not change. This follows from theorem 4.7 and the fact that constant field extensions are unramified. So $g(F_k) = g(\mathbf{F}_{q^m}F_k)$ for all k. From now on we omit the index

k for the field F_k. First we will show that every place y of $\mathbf{F}_{q^m}F$ of degree r is the extension of a place x of F of degree l for some $l \in T_r$. Second we will show that for every $l \in T_r$, a place x of F of degree l extends to a number of places of degree r in $\mathbf{F}_{q^m}F$.

Let y be a place of $\mathbf{F}_{q^m}F$ of degree r and let x be the projection of y in F. Say x has degree l. Then y is an extension of x and by corollary 1.41 all the extensions of x have the same degree $\deg y = r = \frac{l}{\gcd(l,m)}$. Therefore $l \in T_r$. Conversely let x be a place of F of degree l where l satisfies $l = r \cdot \gcd(l, m)$. By corollary 1.41 x extends into $d = \gcd(l, m)$ places of degree $\frac{l}{d} = r$ in $\mathbf{F}_{q^m}F$.

We conclude that for all $k \geq 1$

$$B_r(\mathbf{F}_{q^m}F_k) = \sum_{l \in T_r} \frac{l}{r} B_l(F_k).$$

Dividing both sides by g_k and taking the limit $k \to \infty$ gives the result. □

Remark 4.17 The set $T_r = \{l \mid l = r \cdot \gcd(l, m)\}$ is equal to the set $\{l \mid l = rd,\ d \in S_r\}$, where $S_r = \{d \mid d|m \text{ and } \gcd(r, \frac{m}{d}) = 1\}$. This allows us to rewrite the above result as

$$\beta_r(\mathbf{F}_{q^m}\mathcal{F}) = \sum_{d \in S_r} d\beta_{rd}(\mathcal{F}).$$

Proposition 4.18 *Let r and m be positive integers, such that m divides r. Let $\mathcal{F}/\mathbf{F}_q = (F_k)_{k\geq 1}$ be an asymptotically exact tower of algebraic function fields defined over $\mathbf{F}_q$ for which $\beta_r = \beta > 0$ and $\beta_i = 0$ for all $i \neq r$.*

Then the ascent of the tower $\mathbf{F}_{q^m}\mathcal{F}/\mathbf{F}_{q^m} = (\mathbf{F}_{q^m}F_k)_{k\geq 1}$ is an asymptotically exact tower over $\mathbf{F}_{q^m}$ for which $\beta_{\frac{r}{m}} = m\beta > 0$ and $\beta_i = 0$ for all $i \neq \frac{r}{m}$.

Proof From Proposition 4.16 and the remark above we find that $\beta_{\frac{r}{m}} = m\beta > 0$. For $i \neq \frac{r}{m}$ the limit β_i is a sum of other β's which are all zero. □

4.3.1 Towers of type $\beta_m > 0$

We have proven that asymptotically exact towers exist. This proof was not constructive. In the previous section we gave an example of an asymptotically exact tower over $\mathbf{F}_{q^2}$ for which $\beta_1 = q - 1 > 0$. From Theorem 2.2 in [1] it follows that for this tower $\beta_i = 0$ for all $i > 1$. Hence it is an asymptotically exact tower.

Given a positive integer r, we wish to construct an asymptotically exact tower for which $\beta_r > 0$. We have seen that from a tower with $\beta_r > 0$, we can obtain a tower with $\beta_{\frac{r}{m}} > 0$ by extending the constant field of the tower. Since we already have a tower with $\beta_1 > 0$, and we want to construct one with $\beta_r > 0$, we now want to do the opposite. This gives us the idea of taking the tower with $\beta_1 > 0$ and changing the base field to a smaller constant field.

We call this base change a *descent*. Unfortunately, the descent to a smaller constant field does not always exist. Only under appropriate assumptions taking the descent is possible.

Proposition 4.19 *Let $F = \mathbf{F}_{q^m}(x, y)$ be an algebraic function field over $\mathbf{F}_{q^m}$, where y satisfies $f(y) = 0$ for some polynomial $f \in \mathbf{F}_q(x)[T]$ that is irreducible in $\mathbf{F}_{q^m}(x)[T]$. Then the descent of F to $\mathbf{F}_q$ exists. That is, there exists a function field $G/\mathbf{F}_q$ such that F is the compositum of the field $\mathbf{F}_{q^m}$ and G, that is $F = \mathbf{F}_{q^m}G$.*

Proof From the first chapter we know that the algebraic function field F is the function field of a normal projective curve X over $\mathbf{F}_{q^m}$. This curve contains a dense affine open subset U that has affine coordinate ring $\mathcal{O}_X(U) \cong \mathbf{F}_{q^m}[x, y]/(f)$.

We define $G = \mathbf{F}_q(x, y)$ where y satisfies $f(y) = 0$ for the same polynomial $f \in \mathbf{F}_q(x)[T]$. In the same way G is the function field of a curve Y over $\mathbf{F}_q$ that contains a dense affine open subset V that has affine coordinate ring $\mathcal{O}_Y(V) \cong \mathbf{F}_q[x, y]/(f)$. We will show that the extension of the base field of Y from $\mathbf{F}_q$ to $\mathbf{F}_{q^m}$ gives the curve X. From the properties of the tensor product of $\mathbf{F}_q$-algebras it follows immediately that

$$\mathcal{O}_Y(V) \otimes_{\mathbf{F}_q} \mathbf{F}_{q^m} = \mathcal{O}_X(U).$$

Since both subsets U and V are dense, we conclude that indeed $Y_{\mathbf{F}_{q^m}}$[1] $= X$. We know that F and G are the fraction fields of $\mathcal{O}_X(U)$ and $\mathcal{O}_Y(V)$ respectively. It is also clear that the compositum of G with $\mathbf{F}_{q^m}$ is equal to the field F. □

We have now seen that taking the compositum of a function field with a large constant field in the category of algebraic function fields corresponds to taking the tensor product in the category of normal projective curves.

We will now redefine the tower of Artin-Schreier extensions in section 4.2 over the field $\mathbf{F}_{q^{2m}}$. The polynomials used for defining this tower only have coefficients zero and one and therefore we can take the descent to the constant field $\mathbf{F}_{q^2}$. We will then investigate this new tower and see if it satisfies $\beta_m > 0$.

Definition 4.20 We define the tower $\mathcal{F}/\mathbf{F}_{q^{2m}}$ as follows. Let $F_1 = \mathbf{F}_{q^{2m}}(x_1)$ be the rational function field over $\mathbf{F}_{q^{2m}}$. For $k \geq 1$, we set

$$F_{k+1} = F_k(z_{k+1}),$$

where z_{k+1} satisfies the equation

$$z_{k+1}^{q^m} + z_{k+1} = x_k^{q^m+1},$$

with

$$x_k = \frac{z_k}{x_{k-1}} \in F_k \qquad \text{for } k \geq 2.$$

[1] Recall that by definition $Y_{\mathbf{F}_{q^m}} = Y \times_{\mathbf{F}_q} \operatorname{Spec} \mathbf{F}_{q^m}$. See also section 1.3.3.

Definition 4.21 We define the tower $\mathcal{G}/\mathbf{F}_{q^2}$ as follows. Let $G_1 = \mathbf{F}_{q^2}(x_1)$. For $k \geq 1$, we set

$$G_{k+1} = G_k(z_{k+1}),$$

where z_{k+1} satisfies the equation

$$z_{k+1}^{q^m} + z_{k+1} = x_k^{q^m+1},$$

with

$$x_k = \frac{z_k}{x_{k-1}} \in G_k \qquad \text{for } k \geq 2.$$

It is clear that the tower $\mathcal{F}/\mathbf{F}_{q^{2m}}$ is equal to the constant field extension of the tower $\mathcal{G}/\mathbf{F}_{q^2}$ with the field $\mathbf{F}_{q^{2m}}$. More precisely, for every $k \geq 1$, we have $F_k = \mathbf{F}_{q^{2m}} G_k$.

Lemma 4.22 *Let $F \subset F'$ be an extension of algebraic function fields. If there exists a place of F that is totally ramified in F', then the full constant field of F is algebraically closed in F'.*

Proof Let K and K' be the full constant fields F and F' respectively. We need to show $K' = K$. By hypothesis there is a place Q of F and a place Q' of F' extending Q, such that $e(Q'|Q) = [F' : F]$. It follows from equation 1.1 that $f(Q'|Q) = 1$ and Q' is the only place above Q. We define $F_1 = K'F$ the constant field extension. We have inclusions $F \subset F_1 \subset F'$. There is only one place Q_1 of F_1 extending Q and since F_1 is a constant field extension of F, we have $e(Q_1|Q) = 1$. It follows from $f(Q'|Q) = f(Q'|Q_1)f(Q_1|Q) = 1$ that also $f(Q_1|Q) = 1$. Using equation 1.1 again we find that $e(Q_1|Q)f(Q_1|Q) = [F_1 : F] = 1$, from which we conclude that $[K' : K] = 1$ and hence $K = K'$ is the full constant field of F'. □

We will now investigate the limit $\beta_m(\mathcal{G}) = \lim_{k\to\infty} \frac{B_m(G_k)}{g(G_k)}$. Therefore we need to know the genus of G_k and the number of places $B_m(G_k)$ of G_k of degree m.

We start with the genus. As the tower $\mathcal{F}$ is a constant field extension of $\mathcal{G}$, the fields F_k and G_k have the same genus g_k. It is easily obtained from Theorem 4.5 by replacing q with q^m.

$$g_k = \begin{cases} q^{mk} + q^{m(k-1)} - q^{\frac{m(k+1)}{2}} - 2q^{\frac{m(k-1)}{2}} + 1, & \text{if } k \text{ is odd,} \\ q^{mk} + q^{m(k-1)} - \frac{1}{2}q^{\frac{mk}{2}+1} - \frac{3}{2}q^{\frac{mk}{2}} - q^{\frac{mk}{2}-1} + 1, & \text{if } k \text{ is even.} \end{cases}$$

Computing the number of places of degree m of G_k is a very difficult problem. To avoid having to compute the Zeta function, we will instead try to find an estimate for the number of places of degree m. This is sufficient for showing that the limit β_m is positive.

First we remark that we already know an estimate for the number of places of F_k of degree one. It is also given by Theorem 4.5 after replacing q with q^m.

$$B_1(F_k) \geq (q^{2m} - 1)q^{m(k-1)} + 2q^m \qquad \text{for all } k \geq 3.$$

We can exploit this for bounding $B_m(G_k)$ from below, because there is a relation between the number of places in F_k of degree one and the places of G_k of degree dividing m. From now on we omit the index k for the fields F_k, G_k and the genus g_k.

$$B_1(F) = \sum_{d|m} d \cdot B_d(G).$$

See equation (2.23) p.178 in [10]. We can rewrite this as

$$m \cdot B_m(G) = B_1(F) - \sum_{d|m,\ d\neq m} d \cdot B_d(G).$$

To find a lower bound for the limit $\beta_m(\mathcal{G})$, we need a lower bound for $B_1(F)$ and upper bounds for $B_d(G)$ for all $d < m$ that divide m. We can find these upper bounds using V.2.10(a) p.179 in [10] which states that for any function field $H/\mathbf{F}_q$ with genus $g(H)$,

$$|B_r(H) - \frac{q^r}{r}| < (2 + 7g(H))\frac{q^{r/2}}{r}.$$

After adapting this formula to the present context, where the constant field of G is $\mathbf{F}_{q^2}$ and not $\mathbf{F}_q$, we get

$$B_d(G) < \frac{q^{2d}}{d} + (2 + 7g)\frac{q^d}{d}. \tag{4.8}$$

Putting everything together, and thereby omitting terms that will tend to zero as $k \to \infty$, gives

$$\beta_m(\mathcal{G}/\mathbf{F}_{q^2}) = \lim_{k\to\infty} \frac{B_m(G_k)}{g_k} =$$
$$\lim_{k\to\infty} \frac{1}{m}\left(\frac{B_1(F_k)}{g_k} - \sum_{d|m,\ d\neq m} \frac{d \cdot B_d(G_k)}{g_k}\right) \geq \frac{1}{m}\left((q^m - 1) - \sum_{d|m,\ d\neq m} 7q^d\right).$$

Here we have used Corollary 4.6 to replace the limit $\lim_{k\to\infty} \frac{B_1(F_k)}{g_k}$ with $(q^m - 1)$. Finally, to show that $\beta_m(\mathcal{G}) > 0$, it remains to be checked that the right hand side is positive, i.e. that

$$q^m - 1 > \sum_{d|m,\ d\neq m} 7q^d.$$

For very large q this is obvious, as the left hand side is a polynomial in q of degree m and the right hand side is a polynomial in q of degree $< m$. Unfortunately, for small values of q and m the inequality does not always hold. In fact it is easy to check that the only values of q and m for which the above inequality does not hold are $q = 2, m = 2, 3, 4, 6$ and $q = 3, m = 2, 4$ and $q = 4, 5, 7, m = 2$.

Let us first prove that the inequality holds for all $q \geq 8$ and all m. Recall the geometric sum

$$q^m - 1 = (q-1)\sum_{i=0}^{m-1} q^i.$$

From this we obtain

$$\begin{aligned} q^m - 1 - \sum_{d|m,\ d\neq m} 7q^d &= (q-1)\sum_{i=0}^{m-1} q^i - \sum_{d|m,\ d\neq m} 7q^d \\ &= (q-1)\sum_{i=0,\ i\nmid m}^{m-1} q^i + \sum_{d|m,\ d\neq m} (q-1-7)\,q^d > \sum_{d|m,\ d\neq m} (q-8)\,q^d \geq 0. \end{aligned}$$

The last inequality holds if and only if $q \geq 8$.

Now we investigate if we can improve our lower bound for $\beta_m(\mathcal{G}/\mathbf{F}_{q^2})$. For places of degree one, the well known Hasse-Weil bound is a stronger bound than equation 4.8. In this setting, where the ground field is $\mathbf{F}_{q^2}$ and not $\mathbf{F}_q$ the Hasse-Weil bound gives us

$$B_1(G) < q^2 + 1 + 2gq.$$

See Theorem V.2.3 in [10]. When using this upper bound for B_1 to compute $\beta_m(\mathcal{G}/\mathbf{F}_{q^2})$ for $m = 2, 3$ (or m prime) we get

$$\begin{aligned} m \cdot \beta_m(\mathcal{G}/\mathbf{F}_{q^2}) = \lim_{k\to\infty} \frac{B_m(G_k)}{g_k} &= \lim_{k\to\infty} \frac{B_1(F_k)}{g_k} - \sum_{d|m,\ d\neq m} \frac{B_d(G_k)}{g_k} \\ &\geq (q^m - 1) - \lim_{k\to\infty} \frac{B_1(G_k)}{g_k} \geq q^m - 1 - 2q. \quad (4.9) \end{aligned}$$

Here we have already taken into account that $\lim \frac{q^2+1}{g_k}$ tends to zero. The last expression with $m = 3$ becomes $q^3 - 1 - 2q$. This is positive for all $q \geq 2$. We now see that $\beta_m(\mathcal{G}/\mathbf{F}_{q^2}) > 0$ in the case $q = 2, m = 3$. Here equation 4.9 shows us that $\beta_3(\mathcal{G}/\mathbf{F}_{2^2}) \geq \frac{2^3-1-2\cdot 2}{3} = 1$.

For $m = 2$ we want to know for which prime powers q the expression $q^2 - 1 - 2q$ is positive. This is the case for all $q \geq 3$, but unfortunately not for $q = 2$.

There are now three cases remaining. These are the cases $(q, m) = (2, 4), (2, 6), (3, 4)$. Again using the Hasse-Weil bound, computations similar to equation 4.9 show that

$$4\beta_4(\mathcal{G}/\mathbf{F}_{2^2}) \geq 2^4 - 1 - 2\cdot 2 - 7\cdot 2^2 = -17 \qquad \text{and}$$

$$6\beta_6(\mathcal{G}/\mathbf{F}_{2^2}) \geq 2^6 - 1 - 2\cdot 2 - 7\cdot 2^2 - 7\cdot 2^3 = -25$$

We see that these lower bounds for $\beta_m(\mathcal{G}/\mathbf{F}_{2^2})$ with $m = 4, 6$ are trivial. For the last case $(q, m) = (3, 4)$ we find some improvement,

$$\beta_4(\mathcal{G}/\mathbf{F}_{3^2}) \geq \frac{3^4 - 1 - 2\cdot 3 - 7\cdot 3^2}{4} = \frac{11}{4} > 0.$$

We can summarize this section with the following Theorem that we have now proved.

Theorem 4.23 *For any positive integer m, except possibly for $m = 2, 4$ or 6, there exists a tower of algebraic function fields $\mathcal{G}/\mathbf{F}_4$ with $\beta_m(\mathcal{G}/\mathbf{F}_4) > 0$. For all prime powers $q \geq 3$ and for any positive integer m, there exists a tower of algebraic function fields $\mathcal{G}/\mathbf{F}_{q^2}$ with $\beta_m(\mathcal{G}/\mathbf{F}_{q^2}) > 0$.* □

Remark 4.24 For the cases $q = 2$ with $m = 2, 4$ or 6, the upper and lower bounds we used are not strong enough to conclude that the limit $\beta_m(\mathcal{G}/\mathbf{F}_4)$ is positive. For these three cases a more detailed analysis or an explicit computation of the limit β_m is necessary.

It is interesting to note that in characteristic 2 there does exist a tower with $\beta_2 > 0$ and a different tower with $\beta_4 > 0$. In Proposition 3.1 and 3.3 in [1] these towers, which are very similar to our tower $\mathcal{G}$, are constructed. The same Garcia-Stichtenoth tower is used as in Definition 4.20 and 4.21 with $m = 1$. For $m = 1$ these two definitions are identical. The difference with our construction is that the descent is taken not to a field of which the cardinality is a square, but to the field $\mathbf{F}_2$.

Bibliography

[1] S. Ballet and R. Rolland, *Families of curves over any finite field with a class number greater than the Lachaud-Martin-Deschamps Bounds*, arXiv:0906.5432v1, 30 June 2009.

[2] Barg, Alexander. *At the Dawn of the Theory of Codes*, The Mathematical Intelligencer, Vol. 15 No. 1, 1993 pp. 20-26.

[3] A. Garcia, H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Mathematicae 121 1995 pp. 211-222.

[4] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[5] R. Hill, *A First Course in Coding Theory*, Oxford University Press, 1986.

[6] J. Justesen, *A class of constructive asymptotically good algebraic codes*, IEEE Trans. Inf. Theory Vol. 18 1972 pp. 652-656.

[7] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[8] Y.I. Manin *What is the maximum number of points on a curve over* $\mathbf{F}_2$ *?*, J. Fac. Sci. Univ. Tokyo 28, 715-720, 1981.

[9] A. G. Spera, *Asymptotically Good Codes from Generalized Algebraic-Geometry Codes*, Designs, Codes and Cryptography 37 2005 pp. 305-312.

[10] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin-Heidelberg 1993.

[11] M.A. Tsfasman, S.G.Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.

[12] C.P. Xing, H. Niederreiter and K.Y. Lam, *Construction of algebraic geometry codes*, IEEE Trans. Inf. Theory Vol. 45(4) 1999 pp. 1186-1193.

[13] C.P. Xing, H. Niederreiter and K.Y. Lam, *A generalization of algebraic geometry codes*, IEEE Trans. Inf. Theory Vol. 45(7) 1999 pp. 2498-2501.