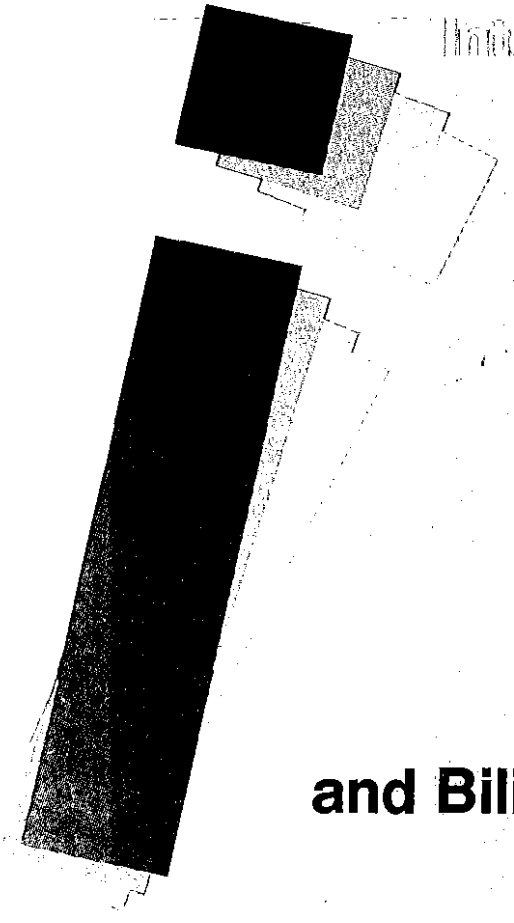
FORSCHUNGSZENTRUM JÜLICH GmbH



Coding Theory and Bilinear Complexity

S. Shokranian
M.A. Shokrollahi

Forschungszentrum Jülich GmbH
Scientific Series of the International Bureau

Coding Theory and Bilinear Complexity

Salahoddin Shokranian

Departamento de Matemática, Universidade de Brasilia, 70910 Brasilia-DF (Brasil)
Department of Mathematics, Purdue University, West Lafayette, Indiana 47907 (USA)

Mohammad Amin Shokrollahi

Institut für Informatik, Universität Bonn, 53117 Bonn (Germany)

German-Brasilian-Cooperation
in Scientific Research and Technological Development

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Shokranian, Salahoddin:
Coding theory and bilinear complexity : German Brasilian cooperation in scientific research and technological development / Salahoddin Shokranian ; Mohammad Amin Shokrollahi. [Hrsg.: Forschungszentrum Jülich GmbH, Zentralbibliothek]. - Jülich : Forschungszentrum Jülich, Zentralbibliothek, 1993
(Scientific series of the International Bureau / Forschungszentrum Jülich GmbH ; Vol. 21)
ISBN 3-89336-123-5
NE: Shokrollahi, Mohammad Amin:; Forschungszentrum <Jülich> / Internationales Büro: Scientific series of ...

Herausgeber und Vertrieb:	Forschungszentrum Jülich GmbH ZENTRALBIBLIOTHEK D-52425 Jülich Telefon (02461) 61-5368 · Telefax (02461) 61-6103
Druck:	Graphische Kunstanstalt Dieter Gehler, Düren-Birkesdorf
Copyright:	Forschungszentrum Jülich 1993

Scientific Series of the International Bureau, Volume 21

ISSN 0938-7676

ISBN 3-89336-123-5

Contents

Preface

The subject of the present book is naturally divided into three parts. The first part (Chapter 1) deals with the theory of *linear error correcting codes.* Here one is interested in the mathematical theory of secure information transmission, e.g., satellite communication. This should not be confused with cryptology where the aim is to guard information against unauthorized access. The second part of the book (Chapters 3, 5, 6, and 7) deals with the theory of *algebraic function fields* and applies this theory to the so-called *modular function fields.* These function fields—or equivalently, algebraic curves—arise from compactifications of the fundamental domain of the action of certain subgroups of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane. Reductions of these curves modulo primes p (outside a finite set of special primes) yields series of algebraic curves over finite fields with many rational points. Finally, the last part of this book (Chapters 8–10) is devoted to a treatment of bilinear complexity theory. Here one is interested in the minimal number of multiplications necessary to compute bilinear forms. One of the most famous representatives of this class of problems is that of determining the asymptotic complexity of matrix multiplication.

The first two subjects merge to the theory of "Geometric Goppa-Codes", also known as "Algebraic-Geometric Codes" which is discussed in Chapter 3. There exists excellent literature on this subject, among which we only mention [42]. For obtaining asymptotically good linear codes from geometric Goppa codes, the main problem is the construction of sequences of curves with many rational points, as is described in Chapter 4.

On the contrary to the theory of error-correcting codes or that of algebraic curves over finite fields, there does not yet exist an up to date concise treatment of the theory of bilinear complexity [1]. Therefore we have decided to give a brief account of the theory which meets our demands in Chapter 8. With the tools developed there we shall see in Chapter 9 that coding theory can be applied to obtain lower bounds in complexity theory in the following sense: one can translate the complexity of a given bilinear map into the problem of determining a linear code of minimal block length when the dimension and the minimum distance are

[1] The forthcoming book [8] will contain the first such attempt

given. The latter problem has been studied by coding theorists extensively. Their results can be used to give lower bounds for the complexity of bilinear maps over finite fields. This is the main subject of Chapter 9.

Last but not least, following CHUDNOVSKY and CHUDNOVSKY, the theory of algebraic function fields can be utilized to obtain interpolation algorithms for multiplication in finite fields. Specializing to elliptic function fields, these algorithms turn out to be even optimal (in the sense of bilinear complexity). Specializing to modular function fields, the theory yields (asymptotically) good algorithms for multiplication in finite fields (Chapter 10).

In writing this book, it has been in the foreground of our attention to provide the interested beginner with a basic knowledge of coding and complexity, their interrelations, as well as their relation to algebraic curves. For a better understanding we have provided exercises at the end of most of the chapters. We consider this book as a first step towards more advanced literature.

This book is based on lectures given by the second author during his visits in Brasilia in summer 1991 and summer 1992 and in the "XII Escola de Álgebra" in Diamantina 1992. It would have not been created without the German-Brazilian-conventions through which an interaction of the authors was made possible. We therefore would like to thank the German organizations KFA-INT and GMD and the Brazilian organizations CNPq and FINEP which made this project possible.

Salahoddin Shokranian and *Mohammad Amin Shokrollahi*

CHAPTER 1

Linear Codes

1.1 Introduction

This chapter contains introductory subjects on linear error correcting codes, which are selected to serve only for the understanding of the book.

The origin of coding theory lies in the practical problem of secure information transmission. Here, in contrary to cryptography where one tries to make information secure against unauthorized use, coding theorists want to guard against damagement of the information (which has in almost all cases natural sources). So the aim of coding theory is to present methods for recovering errors which occur in the transmission of information through a disturbed channel. What is the idea behind these methods? Of course, if one sends information without any type of preprocessing, one very unlikely is capable of correcting any errors. So the idea is to add redundant information and hope that this makes error recovery easier. Suppose for example that the information consists of four bits (i.e., a string consisting of 0's and 1's) and person A wants to send the string $(0,1,0,1)$ to person B. He can repeat the first four bits two more times and send instead the string $(0,1,0,1,0,1,\ldots,0,1)$. It is easy to see that person B can recover one error. So if person A has the additional information that the transmission channel is very unlikely to cause more than one error in twelve bits, he has solved the problem of secure information transmission. A closer look at this so-called "repetition coding" of person A reveals that he now has to spend three times as more transmission energy, but is capable of guarding against just one error. Can he do better?

This is the central problem of coding theory: *Add as few as possible redundant information but do it in such a way that you are capable of guarding against as many errors as possible.* Of course one cannot fulfill both of these conditions at the same time. So the problem which arises is how good one can reconciliate these aims.

In order to be able to give a mathematical foundation to coding theory, we first have to agree upon the transmission alphabet. Originally, this used to be

the alphabet consisting of 0 and 1, i.e., the finite field $\mathbf{F}_2$. As a generalization we consider the alphabet to be an arbitrary finite field $\mathbf{F}_q$. A *code* of *block length* n is then defined to be a subset of $\mathbf{F}_q^n$. We are not going to study codes in this generality in these notes. Instead we want the codes to have an additional structure more accessible to (linear) algebra. The next section will clarify our intention.

1.2 Linear Codes

We start with a definition:

(1.1) Definition. A *linear code* of *dimension* k and *block length* n over the finite field $\mathbf{F}_q$ is a k-dimensional subspace of $\mathbf{F}_q^n$. The elements of C are called *codewords.* $\diamond$

Let us assume for the rest of these notes that whenever we speak of the vector space $\mathbf{F}_q^m$ we think of this vector space as equipped with the standard basis. Let C be linear code of dimension k and block length n over $\mathbf{F}_q$. Since any two vector spaces of dimension k over $\mathbf{F}_q$ are isomorphic, there is an embedding, call it ϕ, of $\mathbf{F}_q^k$ into $\mathbf{F}_q^n$ such that the image of ϕ is C. Hence, ϕ can be described by a matrix $G = G_C \in \mathbf{F}_q^{k\times n}$ (with respect to the standard bases in $\mathbf{F}_q^k$ and $\mathbf{F}_q^n$).

(1.2) Definition. The matrix G_C is called a *generator matrix* for the code C. $\diamond$

Thus the rows of G_C generate the code C and hence, C can be uniquely described by G_C. Equivalently, we can describe C as the null-space of a matrix H_C in the following way: Let $\langle .,. \rangle$ denote the usual scalar product on $\mathbf{F}_q^n$. By $C^\perp$ we denote the following subspace of $\mathbf{F}_q^n$:

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

Then $C^\perp$ is a code of dimension $n - k$ and block length n. H_C is defined to be a generator matrix for $C^\perp$.

(1.3) Definition. Let C be a linear code of dimension k and block length n over $\mathbf{F}_q$. The code $C^\perp$ as constructed above is called the *dual code* to C and H_C is called a *parity check matrix* for C. $\diamond$

H_C is indeed a *check*-matrix for C since $\mathbf{c}$ belongs to C if and only if $\mathbf{c}H_C = \mathbf{0}$.

Let us clarify these concepts with some examples.

(1.4) Example. Consider the repetition code introduced in the introduction. In this case the code—call it C_1—is of dimension 4 and has block length 12. It is defined over $\mathbf{F}_2$. A generator matrix for C_1 is given by

$$G = (I_4 \mid I_4 \mid I_4)$$

where I_4 is the 4×4 identity matrix over $\mathbf{F}_2$. •

(1.5) Example. Consider the code C_2 defined over F_2 having the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Clearly $C_2 = \{(0,0,0,0),(1,1,1,1),(0,1,0,1),(1,0,1,0)\}$. C_2 has dimension 2 and block length 4 and is defined over F_2. •

The block length and the dimension are two fundamental parameters of a linear code which specify the information rate and the length of the words transmitted. In the next section we introduce another fundamental parameter which measures the error correction capacity.

1.3 Error Correction

Up to now we have not told anything about the error correction capacity of a linear code. In order to motivate the definitions which will follow now, let us make a fundamental assumption on the nature of errors which can happen during the transmission. Among various kinds of possible errors we are only interested in those which convert one coordinate symbol into another. In addition, we require that the probability that a symbol α is converted into a symbol β is the same for all α and β. In the binary case for example, we consider only those errors which convert a 0 into a 1 and vice versa. Now it is intuitively reasonable to say that a code has high error correction capacity if one has to change many coordinate symbols to get from one codeword to another. This intuitive idea is made precise by the following definitions.

(1.6) Definition. The metric $d : \mathsf{F}_q^n \times \mathsf{F}_q^n \to \mathbf{N}$ given by

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

is called the *Hamming metric* on F_q^n; $d(\mathbf{x},0)$ is called the *(Hamming) weight* of $\mathbf{x}$. ◇

This metric is very well suited to the study of error correction capacity of a linear code since it measures how many coordinate symbols are to be changed in order to get from one vector to another.

(1.7) Definition. The value $\min_{\mathbf{x}\neq\mathbf{y}\in C} d(\mathbf{x},\mathbf{y})$ is called the *minimum distance* of C. A linear code of dimension k, block length n and minimum distance d is called an $[n,k,d]$-code. ◇

Alternatively, the minimum distance of a linear code C is the minimum of the weights of the nonzero codewords (why?).

Equipped with the Hamming metric we can now formulate an abstract decoding procedure for linear codes: If $\mathbf{u} \in \mathsf{F}_q^n$ is the received word, decode $\mathbf{u}$ to a codeword $\mathbf{c} \in C$ having the smallest Hamming-distance to $\mathbf{u}$.

We want to note that the above abstract decoding procedure is not a suggestion for an algorithm since it is by no means efficient. In general, giving efficient decoding procedures is very hard and it is conjectured that decoding a given linear code is NP-complete (which means that to the present state of knowledge, there is no "efficient" algorithm for decoding a linear code given by its generator matrix [4]). (See [14] for an exact definition of an NP-complete decision problem.)

It is easy to see that a linear code is capable of correcting up to e errors if its minimum distance d satisfies $d \geq 2e + 1$ (This is left as an exercise). Hence the minimum distance is a good measure for the error correction capacity of a linear code.

1.4 Cyclic Codes

This section is devoted to a brief description of a very important class of linear codes, the class of *cyclic codes*. The aim of this section is to show how imposing algebraic conditions on the code makes the description and the study of the code easier. We want to emphasize that this section by no means provides a complete treatment of cyclic codes.

(1.8) Definition. A linear code C of block length n over F_q is called cyclic if $(c_{n-1}, c_0, \ldots, c_{n-2})$ belongs to C whenever $(c_0, \ldots, c_{n-1})$ belongs to C. $\diamond$

In other words, a code C is called cyclic iff it is invariant under cyclic permutation of the coordinate places.

Cyclic codes can be described very nicely with the help of the group algebra $\mathsf{F}_q[C_n]$ where C_n is the cyclic group of order n. To this end, note first that this group algebra is isomorphic to the residue class ring $\mathsf{F}_q[x]/(x^n - 1)$ where we denote by $(x^n - 1)$ the principal ideal generated by $x^n - 1$ in $\mathsf{F}_q[x]$. The isomorphism is described by mapping the residue class of x to the generator of C_n and extending this mapping linearly. We can embed C as a vector space into $\mathsf{F}_q[x]/(x^n - 1)$ by mapping the codeword $(c_0, \ldots, c_{n-1})$ to the residue class of the polynomial $c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$. Thus we can identify C with a subspace of $\mathsf{F}_q[x]/(x^n - 1)$. But C has even more structure. One can easily verify that the condition of being cyclic equips C with the structure of an ideal of the ring $\mathsf{F}_q[x]/(x^n - 1)$. For this one only needs to see that if $c(x) := c_0 + \ldots + c_{n-1}x^{n-1} \in C$ then $xc(x) \bmod (x^n - 1)$ also belongs to C (why?). But this is just the condition of being cyclic stated in (1.8).

As an epimorphic image of the PID $\mathsf{F}_q[x]$, the ring $\mathsf{F}_q[x]/(x^n - 1)$ is itself a PID. Thus there is a polynomial $g(x)$ which generates C as an ideal. If we take $g(x)$ among the generators of C to have the least possible degree, we immediately see that $g(x)$ divides $x^n - 1$ (see the exercises). The auxiliary assumption that $g(x)$

has highest coefficient equal to 1 makes this polynomial unique. In order to be able to speak about this polynomial, let us agree upon the following definition:

(1.9) Definition. The polynomial $g(x)$ the existence of which was shown above, is called the *generator polynomial* for C. The polynomial $h(x) := (x^n - 1)/g(x)$ is called the *check polynomial* for C. $\diamond$

For several reasons, it is very desirable that the polynomial $x^n - 1$ is separable over $\mathbf{F}_q$ which means that it has different linear factors over an extension field of $\mathbf{F}_q$. This condition is always satisfied when n and q are coprime[1]. We want to assume this from now on. If ω is a primitive nth root of unity over $\mathbf{F}_q$, the set of zeros of the polynomial $x^n - 1$ consists of $1, \omega, \ldots, \omega^{n-1}$ and the set of zeros of $g(x)$ is a subset of this. We denote the zero-set of $g(x)$ by $\mathrm{Var}(g)$. It is clear that $\mathrm{Var}(g)$ contains all information about the code C, since the polynomial $g(x)$ and hence the code C can be uniquely determined by $\mathrm{Var}(g)$. How can one read off the parameters of the code C from $\mathrm{Var}(g)$ or equivalently from $g(x)$? We are going to give a partial answer to this in the following.

First of all, the block length of C is given by n. This needs no further comment. The determination of the dimension of C is not very hard either. Indeed, the code C consists of the polynomials $g(x)f(x) \bmod (x^n - 1)$ where $f(x)$ is a polynomial over $\mathbf{F}_q$. Since $g(x)h(x) = x^n - 1$, we can reduce $f(x)$ modulo $h(x)$. Thus C consists of the elements $g(x)f(x)$ where the degree of f is smaller than the degree of h (observe that reduction mod $x^n - 1$ is not necessary since now $\deg(g(x)f(x)) < n$). Thus the dimension of C equals the degree of h, i.e., $n - \deg(g)$.

The determination of the minimum distance of the code C is more difficult. Up to now there is no way to compute efficiently from $\mathrm{Var}(g)$ the actual value of the minimum distance of C for arbitrary cyclic codes. (We call a method efficient if it runs in time polynomial in n.) But there is a very nice result which gives a lower estimate of the minimum distance of C using some data of the set $\mathrm{Var}(g)$.

(1.10) Theorem (BCH-BOUND). *Let C be a cyclic code of block length n over $\mathbf{F}_q$ and $g(x)$ be the generator polynomial for C. Further let ω be a primitive nth root of unity over $\mathbf{F}_q$. If there exist natural numbers i_0 and l such that $\{\omega^{i_0}, \omega^{i_0+1}, \ldots, \omega^{i_0+l-1}\} \subseteq \mathrm{Var}(g)$, then the minimum distance d of C satisfies $d \geq l + 1$.*

The reader may consult [24] or [23] for a proof of this theorem.
let us clarify the subject with some examples:

(1.11) Example. Consider the cyclic code C defined over $\mathbf{F}_2$ having block length 7 and generator polynomial $g(x) = x^3 + x + 1$. Let us compute the zero-set $\mathrm{Var}(g)$:

[1] The reader familiar with the theory of representations of finite groups immediately sees that this condition is equivalent to semisimplicity of the ring $\mathbf{F}_q[C_n]$.

Let ω be a root of $g(x)$ in an extension field of $\mathbf{F}_2$ (in fact $\mathbf{F}_8$ will do, since $g(x)$ is irreducible). Then $\mathrm{Var}(g) = \{\omega, \omega^2, \omega^4\}$. Hence (1.10) asserts that the minimum distance of C is at least 3 (Take $i_0 = 1$ and $l = 2$). The dimension of C is equal to $7 - \deg(g) = 4$. A generator matrix of C is given by

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

In fact, up to a permutation of the coordinates, this code is equal to the $[7, 4, 3]$-Hamming code. •

(1.12) Example. The polynomial $x^{23} - 1$ decomposes over $\mathbf{F}_2$ in the following way:

$$x^{23} - 1 = (x + 1)g(x)f(x)$$

where g and f are irreducible polynomials of degree 11 over $\mathbf{F}_2$. Let ω be a primitive 23^{rd} root of unity over $\mathbf{F}_2$. It is easy to see that one of these polynomials, say g, has the zero-set $\{\omega^k \mid 1 \leq k \leq 22, \left(\frac{k}{23}\right) = 1\}$, where $(..)$ is the Legendre symbol. Let C be the code generated by g. The block length of C equals 23 and its dimension is 12. Since $\{\omega, \omega^2, \omega^3, \omega^4\} \subseteq \mathrm{Var}(g)$, the BCH-bound asserts that the minimum distance d of C satisfies $d \geq 5$. In fact one can prove that $d = 7$. This code is the well-known $[23, 12, 7]$-Golay-Code. •

There are very efficient decoding algorithms for cyclic codes which are able to correct errors up to the BCH-bound (but unfortunately not further). These algorithms heavily rely on the special structure of the cyclic codes. We are not going to discuss them here, since this will lead us too much apart.

1.5 The Parameters of a Linear Code

One of the major questions in coding theory is the following: Given n, k, d, and q, does there exist a linear $[n, k, d]$-code over $\mathbf{F}_q$?

One step towards the solution of this problem is given by the following procedure with which one can construct new codes from given linear codes.

Suppose C is a linear $[n, k, d]$-code over $\mathbf{F}_q$. Let $i \leq n$ be an integer and C_i be the linear code obtained from C by setting the ith coordinate of any codeword in C equal to 0. In other words, if $(e_1, \ldots, e_n)$ is the standard basis of $\mathbf{F}_{q^n}$ and π_i is the projection along e_i onto $\sum_{j \neq i} \mathbf{F}_q e_j$, then $C_i := \pi_i(C)$. C_i is called the *ith punctured code of* C. What can we say about the parameters of C_i?

(1.13) Lemma. *Let C_i be the ith punctured code of an $[n,k,d]$-code C, $d \geq 2$. Then C_i is an $[n,k,d']$-code where $d' = d$ if all minimum weight codewords in C vanish at coordinate position i, and $d' = d-1$ otherwise.*

PROOF. Since π_i is a linear map and $C_i = \pi_i(C)$, C_i is a linear code of block length n. Clearly, $\dim(C_i) = \dim(C) - \dim(C \cap \ker \pi_i)$. Now $\ker \pi_i = \mathsf{F}_q e_i$, hence, since $d \geq 2$ is assumed, $C \cap \ker \pi_i = 0$ which shows that C_i has dimension $\dim(C) = k$. The assertion on the minimum distance of C_i is easy to see. □

With the help of this procedure it is now straightforward that a complete solution to the question stated at the beginning of this section can be given once the exact values of the following function are known:

(1.14) Definition. $N_q[k,d] := \min\{n \mid \exists\ [n,k,d]\text{-code over } \mathsf{F}_q\}$. ◇

In general, finding the exact value of $N_q[k,d]$ for given k, d, and q is very hard. In the next section we shall learn some asymptotic results about this function.

One of the most basic properties of the function N_q is that it is increasing in the second variable.

(1.15) Lemma. *If $\delta \leq d$, then $N_q[k,\delta] \leq N_q[k,d]$ for all $k \geq 1$.*

PROOF. Clearly it suffices to prove the assertion for $\delta = d-1$. Let an $[N_q[k,d],k,d]$ code C over F_q be given. We can construct from this code an $[N_q[k,d],d-1,k]$-code by puncturing it at an appropriate position. This proves $N_q[k,d-1] \leq N_q[k,d]$. □

The *Singleton Inequality* asserts that $N_q[k,d] \geq k+d-1$ for all q (See Exercise 1.2). A more useful bound is the following.

(1.16) Theorem (GRIESMER-BOUND). *We have*

$$N_q[k,d] \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil x \rceil$ is the smallest integer greater or equal to x.

We omit the elementary proof and refer the reader to [24].

1.6 Asymptotic Bounds

Although, as stated in the last section, very little is known about the exact behavior of the function N_q, one has powerful techniques for obtaining asymptotic assertions about this function. This section serves as a brief introduction to the topic of asymptotic studies in the theory of error-correcting codes. We are not going to

motivate this topic, since this is done in a very satisfactory way in different textbooks (such as [23, 24, 42]).

Let q be a prime power and C be a linear $[n,k,d]$-code over $\mathbf{F}_q$. We define $\delta(C) := d/n$ and $R(C) := d/n$. We can associate to every linear code C over $\mathbf{F}_q$ the point $(\delta(C), R(C))$ in $\mathbf{S} := [0,1]^2 \subseteq \mathbf{R}^2$. We are interested in the set Σ_q of accumulation points of the image U_q of this extended mapping. We shall first show that this is equal to the set of all limit points of sequences of linear codes. In other words, we show that Σ_q is the set of those points $(\delta, R) \in \mathbf{S}$ such that there exists a sequence of pairwise different (n_i, k_i, d_i)-codes C_i with the property that $\delta = \lim \delta(C_i)$ and $R = \lim R(C_i)$: for this it is necessary to show that the limit point of any such sequence is an element of Σ_q. Suppose that (C_i) is a sequence of $[n_i, k_i, d_i]$-codes such that $R(C_i) = R$ and $\delta(C_i) = \delta$ are constant. Then (δ, R) is the limit point of a sequence of codes, but not necessarily a point in Σ_q since it may be an isolated point of U_q. But by puncturing the codes C_i at appropriate positions, we obtain a sequence of $[n_i, k_i, d_i - 1]$-codes. Since $k_i/n_i = R$ and $(d_i - 1)/n_i \to \delta$ as i goes to ∞, we see that (δ, R) is also an accumulation point of U_q, hence belongs to Σ_q.

If (C_i) is a sequence of different $[n_i, k_i, d_i]$-codes, the n_i have to go to infinity for increasing i, hence this justifies the notion of "asymptotic studies". The following nice result due to MANIN [25] gives some information about the set Σ_q.

(1.17) Theorem. *There exists a continuous and decreasing function* $\alpha_q : [0,1] \to [0,1]$ *such that* $\alpha_q(0) = 1$, $\alpha_q(x) = 0$ *for* $(q-1)/q \le x \le 1$ *and*

$$\Sigma_q = \{(\delta, R) \mid 0 \le R \le \alpha_q(\delta)\}.$$

One of the central problems in coding theory is the determination of the function α_q (which is equivalent to the asymptotic determination of the function N_q). This seems to be very difficult. Up to now the exact value of α_q is not known even for a single $\delta \in (0, (q-1)/q)$.

Because of lack of knowledge about the function α_q it is desirable to have at least lower and upper estimates for this function. In other words, we are looking for functions (desirably given by explicit formulae) f such that $\alpha_q(x) \le f(x)$ or $\alpha_q(x) \ge f(x)$ for x belonging to a certain interval in $[0, (q-1)/q]$. Among the various results in this direction we just confine ourselves to present three; more information on this topic can be found in [23] and [24].

(1.18) Theorem. *Let* $H_q(x) := x \log_q(q-1) - x \log_q(x) - (1-x)\log_q(1-x)$ *and* $\theta := (q-1)/q$. *If* $0 \le x \le \theta$, *we have:*

(1) *(*PLOTKIN*-Bound)* $\alpha_q(x) \le 1 - x/\theta$.

(2) *(*MCELIECE*-*RODEMICH*-*RAMSEY*-*WELCH*-Bound)*

$$\alpha_2(x) \le H_2\left(\frac{1}{2}\sqrt{x(1-x)}\right),$$

(3) *(GILBERT-VARSHAMOV-Bound)* $\alpha_q(x) \geq 1 - H_q(x)$.

Over two decades of research made it plausible to think that the Gilbert-Varshamov-curve $1 - H_q(x)$ was equal to $\alpha_q(x)$, but the construction of codes via algebraic curves lead to codes exceeding the Gilbert-Varshamov-bound (for square q greater than or equal to 49). This construction will be discussed in Chapter 3.

1.7 Exercises

1.1. Let $H \in \mathbf{F}_q^{(n-k)\times n}$ be the parity check matrix of the $[n, k, d]$-code C. Show that if every l columns of H are linearly independent, then $d \geq l + 1$.

1.2. Show that the parameters of a linear $[n, k, d]$-code satisfy the *Singleton-inequality* $k + d \leq n + 1$.

1.3. Show that the Hamming metric is indeed a metric on $\mathbf{F}_q^n$.

1.4. Show that if the minimum distance d of a code C satisfies $d \geq 2e + 1$, then C is capable of correcting up to e errors.

1.5. Show that the minimum distance of a linear code C is equal to the minimum of the weights of the nonzero codewords of C.

1.6. Let C have the parity check matrix

$$H := \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Compute the minimum distance of C. How many errors can be corrected by C?

1.7. Let q be a power of a prime, n a natural number prime to q and $g_1(x), g_2(x)$ be two polynomials in $\mathbf{F}_q[x]$ dividing $x^n - 1$ such that the quotient $g_1(x)/g_2(x)$ is not constant. Show that the ideals generated by $g_1(x)$ and $g_2(x)$ in $\mathbf{F}_q[x]/(x^n - 1)$ are different.

1.8. Compute the number of different cyclic codes of length n over the field $\mathbf{F}_q$ (under the assumption $\gcd(n, q) = 1$) in terms of the number of irreducible factors of $x^n - 1$. How many cyclic codes of length 9 exist over $\mathbf{F}_2$?

1.9. Let $\omega \in \mathbf{F}_q$ be a primitive nth root of unity and consider the cyclic code C of length n over $\mathbf{F}_q$ having $(x - \omega^1) \ldots (x - \omega^l)$ as a generator polynomial, where l is an arbitrary natural number less or equal to n. Compute the parameters of this code and compare these with the Singleton-inequality.

CHAPTER 2

Algebraic Function Fields

2.1 Introduction

In this chapter we are going to introduce the reader with a basic knowledge about algebraic function fields of one variable. This introduction will be very brief and we are going to emphasize only those subjects which will be relevant for future use. Let us first explain what an algebraic function field of one variable is:

(2.1) Definition. Let k be a field and x an indeterminate over k. An *algebraic function field K of one variable* is a finite extension of $k(x)$. The elements in K which are transcendental over k are called *variables* and the elements of K algebraic over k are called *constants*. The algebraic closure of k in K is called the *field of constants of K/k*. The field $k(x)$ is called the *rational function field of one variable over k*. $\diamond$

Since we are not going to study function fields of several variables, we shall omit in future the extension "of one variable". Moreover, we want to assume that k is algebraically closed in K whenever we speak of the function field K/k.

If k is a perfect field, a given algebraic function field K can be described by an equation $f(x, y) = 0$ where f is a polynomial of two variables with coefficients in k [16]. This reveals to some extent the connection of function fields and algebraic curves. Of course, this is merely a motivation and not an exact formulation. The latter can be found in any textbook on commutative algebra or algebraic geometry.

The main aim of this chapter is to formulate the Theorem of Riemann-Roch. For this, we shall first introduce the concept of a prime divisor by studying valuations on the rational function field. We shall then be able to introduce the group of divisors and the appropriate concepts relevant to the "Riemann-part" of the Theorem of Riemann-Roch. Introducing the canonical class, we will then be able to complete the formulation of this famous theorem.

2.2 Valuations

(2.2) Definition. Let K be a field and L a subfield of K. A *multiplicative (additive) valuation* on K is a nonzero mapping $v: K \to \mathbf{R}_{\geq 0}$ ($v: K^\times \to \mathbf{R}$) with the following properties:

(1) $\forall a, b \in K:\ v(ab) = v(a)v(b)$ ($\forall a, b \in K:\ v(ab) = v(a) + v(b)$),

(2) $\forall a, b \in K:\ v(a+b) \leq \max(v(a), v(b))$ ($\forall a, b \in K:\ v(ab) \geq \min(v(a), v(b))$).

A multiplicative (additive) valuation is called *trivial* if $v(a) = 1$ for all $a \in K^\times$ ($v(a) = 0$ for all $a \in K^\times$). In the sequel we shall only study nontrivial valuations (unless otherwise stated). A *valuation of K/L* is a valuation of K trivial on L. An additive valuation v is called *discrete* if its image is isomorphic to $\mathbf{Z}$. Two multiplicative (additive) valuations v_1 and v_2 on K are called *equivalent* if $v_1(x) < 1$ ($v_1(x) < 0$) implies $v_2(x) < 1$ ($v_2(x) < 0$) for all $x \in K$ (for all $x \in K^\times$). $\diamond$

Let us extend the set $\mathbf{R}$ of real numbers by an element ∞ with the assumption that $\infty > x$ and $x \pm \infty = \infty$ as well as $x \cdot \infty = \infty$ for all $x \in \mathbf{R}$. One easily sees that any additive valuation on $K^\times$ can be extended to a valuation on K by setting $v(0) := \infty$.

The following are examples of valuations:

(2.3) Example. Let us study valuations on the field $\mathbf{Q}$ of rational numbers. If p is a prime, we denote by $\mathrm{ord}_p(z)$ the highest power of p which divides the integer z. Thus we have for example $\mathrm{ord}_2(6) = 1$, $\mathrm{ord}_3(18) = 2$, $\mathrm{ord}_5(9) = 0$. We can extend $\mathrm{ord}_p(.)$ uniquely to the field $\mathbf{Q}$ by setting $\mathrm{ord}_p(\frac{z}{u}) := \mathrm{ord}_p(z) - \mathrm{ord}_p(u)$. Now it is easily seen that for any prime p the mapping $\mathrm{ord}_p(.)$ is a discrete additive valuation on $\mathbf{Q}$. Indeed, since the additivity of $\mathrm{ord}_p(.)$ is clear (note that this need not be the case when p is not a prime), it suffices to show that $\mathrm{ord}_p(a+b) \geq \max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$. But this follows easily from the fact that the ring $\mathbf{Z}$ of integers is a UFD (Unique Factorization Domain), i.e., the factorization into powers of primes is (up to ordering) unique.

Now fix a real number $\sigma > 1$ and set $|a|_p := \sigma^{-\mathrm{ord}_p(a)}$. It is easily verified that $|.|_p$ is a discrete multiplicative valuation on $\mathbf{Q}$. If we choose $\sigma = p$, then we call this valuation the *normalized p-adic valuation* on $\mathbf{Q}$. •

(2.4) Example. Now let R be any UFD and π a prime element in R. Then we can repeat the construction of the previous example to get an additive valuation $\mathrm{ord}_\pi(.)$ and a multiplicative valuation $|.|_\pi$ on R. These valuations can be uniquely extended to the quotient field K of R in the same manner as for the ring $\mathbf{Z}$ and the field $\mathbf{Q}$.

We want to emphasize the case $R = k[x]$, i.e., the case where R is the polynomial ring of one variable over the field k. Here the prime elements correspond to irreducible polynomials and we speak of $\mathrm{ord}_{p(x)}(.)$ for an irreducible polynomial $p(x)$.

It is clear that for two different irreducible polynomials $p(x)$ and $q(x)$ the valuations $\mathrm{ord}_{p(x)}(.)$ and $\mathrm{ord}_{(q(x)}(.)$ are inequivalent: We have for example $\mathrm{ord}_{p(x)}(p(x)) = 1$ but $\mathrm{ord}_{q(x)}(p(x)) = 0$. •

(2.5) Example. The rational function field $K = k(x)$ possesses another additive valuation which is not equivalent to any of the valuations $\mathrm{ord}_{p(x)}(.)$. This is constructed as follows: Let $h(x) := \frac{f(x)}{g(x)} \in k(x)$. Then we define $\mathrm{ord}_\infty(h(x)) := \deg(g(x)) - \deg(f(x))$. Note that this is a valuation and that it is well defined (why?). •

To any valuation v of K (additive or multiplicative), one can associate a certain subring of K defined in the following way:

(2.6) Definition. Let v be a multiplicative valuation of K. The ring $\mathcal{O}_v := \{x \in K \mid v(x) \leq 1\}$ is called *the valuation ring* associated to v. (In the case v is additive, the condition ≤ 1 is replaced by ≥ 0). ◇

Note that two valuations are equivalent if and only if the corresponding valuation rings are equal. In fact, this explains why valuation rings are more natural objects than the valuations. Let us study the basic structure of valuation rings. In the sequel we suppose that v is a multiplicative valuation, the case of additive valuations being similar. The elements of the set $\{x \in K \mid v(x) = 1\}$ are invertible in $\mathcal{O}_v$ since $v(x) = 1$ implies $v(1/x) = 1/1 = 1$. By the same argument we see that the elements of $\{x \in K \mid v(x) < 1\}$ are not invertible. Hence we have computed the set of invertible elements of $\mathcal{O}_v$.

(2.7) Lemma. $\mathcal{O}_v^\times = \{x \in K \mid v(x) = 1\}$.

The set $\mathcal{M}_v := \{x \in K \mid v(x) < 1\}$ is easily seen to be an ideal of $\mathcal{O}_v$. In fact it is the only maximal ideal of $\mathcal{O}_v$. It is an elementary exercise in algebra to see that in this case $\mathcal{O}_v/\mathcal{M}_v$ is a field.

(2.8) Definition. $K(v) := \mathcal{O}_v/\mathcal{M}_v$ is called the *residue class field* of the valuation v and the corresponding canonical homomorphism is called the *evaluation map* (or *residue class mapping*) at v. ◇

Let us compute the valuation rings and residue class fields for the valuations introduced in the last examples:

(2.9) Example. Denote by $\mathbf{Z}_{(p)}$ the valuation ring of $\mathrm{ord}_p(.)$. A rational number a/b belongs to $\mathbf{Z}_{(p)}$ if and only if $\mathrm{ord}_p(a) \geq \mathrm{ord}_p(b)$. Thus if we assume a and b to be coprime, a/b belongs to $\mathbf{Z}_{(p)}$ if and only if $\mathrm{ord}_p(b) = 0$, i.e., if and only if p does not divide b. Hence we get

$$\mathbf{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbf{Z},\ b \not\equiv 0 \bmod p \right\}.$$

For example we get $\frac{2}{3} \in \mathbf{Z}_{(2)}$ and $\frac{3}{5} \notin \mathbf{Z}_{(5)}$. If $\frac{a}{b} \in \mathbf{Z}_{(p)}$ and a, b are coprime, we have $\mathrm{ord}_p(a/b) = \mathrm{ord}_p(a)$. Hence, if $M_{(p)}$ denotes the maximal ideal in $\mathbf{Z}_{(p)}$, we have

$$M_{(p)} = \left\{ \frac{a}{b} \;\middle|\; \frac{a}{b} \in \mathbf{Z}_{(p)},\ \mathrm{ord}_p(a) \geq 1 \right\} = p\mathbf{Z}_{(p)}.$$

It is easy to show that $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)} \simeq \mathbf{Z}/p\mathbf{Z}$. Thus the residue class field of the prime p is the finite field with p elements. •

(2.10) Example. Let $p(x) \in k[x]$ be an irreducible polynomial and $\mathcal{O}_{p(x)}$ and $\mathcal{M}_{p(x)}$ denote the valuation ring and the residue class field of the valuation $\mathrm{ord}_{p(x)}(.)$. In exactly the same way as above one shows that

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in k[x],\ \mathrm{ord}_{p(x)}(g(x)) = 0 \right\}$$

and

$$\mathcal{M}_{p(x)} = p(x)\mathcal{O}_{p(x)}.$$

Again it is an elementary exercise to show that $\mathcal{O}_{p(x)}/\mathcal{M}_{p(x)} = k[x]/p(x)k[x]$, hence the residue class field of $\mathrm{ord}_{p(x)}(.)$ is an extension of degree $\deg(p(x))$ of k.

As for the valuation $\mathrm{ord}_\infty(.)$ one can be easily show that the residue class field of this valuation coincides with k. (See the exercises.) •

There is a simple correspondence between additive and multiplicative valuations in an algebraic function field K/k which may have been suggested by the examples above: If v is an additive valuation in K/k, we get a multiplicative valuation v' defined by $v'(x) := a^{-v(x)}$ where a is a positive real number greater than one. On the other hand, if v' is a multiplicative valuation on K/k, we get an additive valuation v by setting $v(x) := -\log(v'(x))$, where log is the logarithm to any base greater than one.

2.3 Relation of Valuations and Points in the Rational Case

This section is meant to serve as a motivation for the future identification of valuation rings and points of an algebraic curve.

For the sake of simplicity let k be an algebraically closed field (for example equal to $\mathbf{C}$). We have already computed a set of inequivalent valuations of the field $k(x)/k$: All the inequivalent valuations but ord_∞ are in one to one correspondence with the irreducible polynomials in $k[x]$. Since k is algebraically closed, the irreducible polynomials in $k[x]$ are of the form $x - \alpha$ for some $\alpha \in k$. So all the inequivalent valuations in $k(x)/k$ but ord_∞ are in one to one correspondence with the elements of k.

Let us extend k by an element ∞ and agree upon the fact that the valuation ord_∞ corresponds to ∞ (this might look quite artificial but it has a rigorous

justification). Then we see that the valuation rings in $k(x)/k$ are in one to one correspondence with $k \cup \{\infty\}$, i.e., with the projective line over k.

Regarding the projective line as the most simple algebraic curve, this might serve as a motivation for identifying valuation rings with points of a curve. (Note that we have not defined the notion of an algebraic curve. We are just speaking about the intuitive understanding of curve, for example as the set of zeros of a polynomial in two variables.)

2.4 Extension of Valuations

Let K be a field and v a valuation on K. Further let L be a subfield of K. Then the restriction of v to L is clearly a valuation on L. If $\mathcal{O}_v$ is the corresponding valuation ring in K, it is not difficult to see that the valuation ring corresponding to the restriction of v on L is given by $\mathcal{O}_v \cap L$.

(2.11) Definition. Let L be a field and K an extension of L. Further let w be a valuation on L. The valuation v on K is said to be an *extension of w to K*, if the restriction of v to L equals w. $\diamond$

We have by now studied the valuations in the rational function field $k(x)$ over a field k. In order to be able to perform arithmetics in algebraic function fields, we have to know the valuations of these fields trivial over the constant field k. Since the restriction of any valuation of an algebraic function field to a rational subfield yields (up to equivalence) one of the known valuations, we have therefore to ask whether the valuations of $k(x)$ can be extended to an extension field.

This question can be stated in the affirmative: Given a field extension K of $k(x)$ and a valuation v of $k(x)$ there always exists an extension of v to K. The extension of the valuation in $k(x)/k$ to K is generally not unique. We are not going to discuss the various ways of extending valuations to a field extension. We confine ourselves to the fact that there exist different techniques for calculating these extensions [1, 16].

2.5 The Set of Prime Divisors

In this section we want to introduce a standard terminology used in the rest of these notes.

(2.12) Definition. Let K be an algebraic function field over k. We call a valuation ring of K associated to a valuation of K/k a *prime divisor* of K/k. $\diamond$

We denote prime divisors by capital letters such as $P, Q, \ldots$. If a valuation ring $\mathcal{O}$ is identified with the prime divisor P, we speak of $\mathcal{O}$ as the valuation ring corresponding to P. The *residue class field* of a prime divisor is defined to be

the residue class field of the corresponding valuation ring. The same holds for the *evaluation map* at a prime divisor. If P is a prime divisor of L/k, K is an extension of L and Q is a prime divisor of K such that its valuation extends the valuation corresponding to P, we say that Q *is less or equal to* P: $Q \leq P$. (This means that the reverse order holds for the valuation rings.) If P is a prime divisor, we denote by ord_P resp. $|.|_P$ the additive resp. multiplicative valuation corresponding to P. (Note that there exist infinitely many equivalent valuations corresponding to P. Unless stated otherwise, we take one valuation from each equivalence class in an arbitrary manner.)

The notion of a prime divisor comes from the correspondence between a valuation ring and prime elements in appropriate rings (for example prime numbers in case of $\mathbf{Q}$ and prime (irreducible) polynomials in the case of a rational function fields).

Let P be a prime divisor of the algebraic function field K and $\mathcal{K}_P$ its residue class field. One can show that the constant field k of K can be embedded in $\mathcal{K}_P$ and that the degree $(\mathcal{K}_P : k)$ is finite. This can easily be seen in the case $K = k(x)$.

(2.13) Definition. $(\mathcal{K}_P : k)$ is called the *degree* of the divisor P. $\diamond$

We denote the set of prime divisors of K/k by $\mathbf{P}(K/k)$. Let us state some fundamental properties of this set:

(1) For any algebraic function field K/k the set of prime divisors $\mathbf{P}(K/k)$ is infinite. In fact, since every valuation of $k(x)$ can be extended to a valuation of K and there are infinitely many inequivalent valuations in $k(x)$, the assertion follows.

(2) If $x \in K$ satisfies $\mathrm{ord}_P(x) = 0$ for all $P \in \mathbf{P}(K/k)$, then x is a constant.

(3) (Finiteness property) If $f \in K^\times$, then the number of prime divisors P such that $\mathrm{ord}_P(f) \neq 0$ is finite.

(4) ("Product Formula") For every P there exists a valuation $|.|_P$ corresponding to P such that for every nonzero $x \in K$ we have $\sum_{P \in \mathbf{P}(K/k)} \mathrm{ord}_P(x) \deg(P) = 0$.

The set of representatives of valuations stated in (4) is called a set of *normalized valuations.*

2.6 The Group of Divisors

The group of invertible elements of the field $k(x)$ of rational functions in the indeterminate x over the field k is generated by the set of irreducible polynomials in $k[x]$. In fact, one can write any rational function as the product of integral powers of irreducible polynomials. Since $k[x]$ is a UFD (which means that the representation as a product of powers of irreducible polynomials is essentially unique) and

$k(x)$ is the quotient field of $k[x]$, one can regard $k(x)^\times$ as the free abelian group over the set of the irreducible polynomials. If K is an algebraic function field, one can always find in K a (unique) subring sharing the properties of $k[x]$ in $k(x)$ (the *integral closure* of $k[x]$ in K). But this ring is usually no longer a UFD. In order to deal with this problem, one can introduce the following group:

(2.14) Definition. Let K be an algebraic function field and $\mathbf{P}(K/k)$ the set of prime divisors of K. The *divisor group* $\mathbf{D}(K/k)$ of K/k is defined to be the free abelian group over $\mathbf{P}(K/k)$. $\diamond$

We shall obey the notations of algebraic geometry (rather that of number theory) and assume $\mathbf{D}(K/k)$ to be an additive group. Then by definition every divisor A has a unique representation $A = \sum_P a_P P$ where P runs over all elements of $\mathbf{P}(K/k)$ and the a_P's are integers vanishing for almost all P.

(2.15) Example. Let $K = \mathbf{F}_2(x)$. We denote by (∞) the prime divisor corresponding to ord_∞ and by $(p(x))$ the prime divisor corresponding to $\mathrm{ord}_{p(x)}$ where $p(x)$ is an irreducible polynomial over $\mathbf{F}_2$. The following are examples of divisors over $\mathbf{F}_2$:

$$A := 2(x) - 5(x^2 + x + 1), \quad B := 2(x^3 + x + 1) - 3(x + 1) - 3(\infty).$$

•

Let f be a non-vanishing function belonging to the algebraic function field K. Because of the finiteness property of the set of prime divisors stated in the previous section, we can associate to f a divisor (f) defined by $(f) := \sum_P \mathrm{ord}_P(f)P$.

(2.16) Definition. (f) is called the *principal divisor* associated to f. $\diamond$

(2.17) Example. Let $K = \mathbf{F}_2(x)$ and $f = x(x^3+x+1)/(x^2+x+1)$. Then we have

$$\mathrm{ord}_x(f) = \mathrm{ord}_{x^3+x+1}(f) = -\mathrm{ord}_{x^2+x+1}(f) = 1, \ \mathrm{ord}_\infty(f) = -2.$$

Hence we have $(f) = (x) + (x^3 + x + 1) - (x^2 + x + 1) - 2\infty$. The divisor B of the previous example satisfies $B = (g)$ where $g = (x^3 + x + 1)^2/(x + 1)^3$. To the divisor A of the previous example there corresponds no principal divisor, since any function $f \in K$ satisfying $\mathrm{ord}_x(f) = 2$, $\mathrm{ord}_{x^3+x+1}(f) = -5$, $\mathrm{ord}_p(f) = 0$ for any irrducible polynomial p in $k[x]$ different from x and x^2+x+1, and $\mathrm{ord}_\infty(f) = 0$, is a constant multiple of $x^2/(x^2 + x + 1)^5$, but for this function we have $\mathrm{ord}_\infty(f) = 8 \neq 0$. •

(2.18) Definition. Two divisors A and B of the algebraic function field are called *equivalent* if $A = B + (f)$ for some function $f \in K$. The set of all divisors equivalent to a given divisor A is called the *class* of A (Sometimes denoted by $[A]$). $\diamond$

(2.19) Example. Let again $K = \mathbf{F}_2(x)$. Further let $A = (x) + 2(x+1)$ and $B = (x^3 + x + 1)$. Then A and B are equivalent since $A = B + (f)$ where $f = x(x+1)^2/(x^3+x+1)$. •

The notion of the degree of a prime divisor was defined in the last section. We can extend this to get the concept of the degree of a divisor:

(2.20) Definition. Let $A = \sum_P a_P P$ be a divisor of the algebraic function field K/k. The integer $\deg(A) := \sum_P a_P \deg(P)$ is called the *degree* of the divisor A. ◇

The product formula in the last section forces the degree of principal divisors to be equal to 0 (why?). Hence we can extend the definition of the degree to divisor classes: $\deg([A]) := \deg(A)$. The set of divisors of degree 0 in an algebraic function field forms a group. The quotient of this group by the group of principal divisors is called the class group of the field. It is of extreme importance for the arithmetic of the function field and plays the same role as the class group in number fields.

2.7 The Linear Space of a Divisor

We can define a partial order on the group of divisors of an algebraic function field in the following way: If $A = \sum_P a_P P$ and $B = \sum_P b_P P$, we define $A \leq B$ if and only if $a_P \leq b_P$ for all P. Note that if we had written the operation in the divisor group multiplicatively, this would have lead to the normal definition of divisibility. Note also that this partial order is compatible with the operation in the divisor group, i.e., $A \leq B$ implies $A + C \leq B + C$ for any divisor C.

(2.21) Example. The divisors $A = (x^2+x+1) - 3(\infty)$ and $B = (x+1) + (\infty)$ are not comparable in $\mathbf{F}_2(x)$ while $A \leq (f)$ where $f = x^2 + x + 1$. •

Given a divisor A in an algebraic function field K/k, we can associate to A the vector space $L(A) := \{f \in K^\times \mid (f) \geq -(A)\} \cup \{0\}$. One can show that $L(A)$ is a finite dimensional vector space over the field k.

(2.22) Definition. $L(A)$ is called the *linear space of* A. Its dimension is denoted by $\dim(A)$ and is called the *dimension* of A. ◇

It can be shown that the dimension is constant on the divisor classes so we can define $\dim([A]) := \dim(A)$.

The computation of the dimension of a divisor A will be the topic of the discussions following. The linear space of certain divisors will be used later to construct geometric Goppa codes.

The problem of determination of $\dim(A)$ for a divisor A can easily be solved some cases (see for instance [16]):

(2.23) Theorem. *Let A be a divisor of the algebraic function field K/k. Then* $\dim(A) = 0$ *whenever* $\deg(A) < 0$. *If* $\deg(A) = 0$, *then* $\dim(A) = 0$ *if A is not principal. If A is principal then* $\dim(A) = 1$.

The nontrivial part of the problem is to determine $\dim(A)$ for divisors of positive degree.

2.8 The Theorem of Riemann-Roch

For computing the dimension of a divisor, we first have to introduce a fundamental invariant of the function field K/k. Suppose that A is a divisor of positive degree of K/k. Then $\dim(A) - \deg(A)$ can be proved to be at most equal to 1. So let us define $\sigma(A)$ by $\dim(A) - \deg(A) = 1 - \sigma(A)$. Hence $\sigma(A)$ is a nonnegative integer. The first question which arises is how big $\sigma(A)$ can get. It can be proved that there exists a constant $g = g(K/k)$ depending only on the field K/k such that $\sigma(A) \leq g$ for all divisors A (see [1]).

(2.24) Definition. $g = g(K/k) := \max_A \sigma(A)$ is called the *genus* of K/k. $\diamond$

The genus of a function field has many equivalent definitions. The one we have depicted has the advantage to make the following "almost trivial":

(2.25) Theorem (THEOREM OF RIEMANN). *Let K/k be an algebraic function field of genus g and A a divisor of positive degree in K/k. Then* $\dim(A) \geq \deg(A) + 1 - g$. *Moreover, we have equality if* $\deg(A) \geq 2g - 1$.

The study of the defect $\delta(A) := \dim(A) - \deg(A) - 1 + g$ (also called the *index of specialty of A*) leads to the Theorem of Riemann-Roch:

(2.26) Theorem (THEOREM OF RIEMANN-ROCH). *Let K/k be a function field of genus g. There exists a unique class $W = W(K/k)$ of divisors in $\mathbf{D}(K/k)$ such that* $\deg(W) = 2g - 2$ *and* $\dim(W) = g$ *and*

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

We are not going to talk about the so-called *canonical class* W the existence of which is claimed in the last Theorem. We just note that divisors of degree greater than $2g-2$ are *nonspecial*, i.e., their index of specialty is equal to 0. On the contrary, divisors for which the index of specialty is not 0 are called *special divisors*. Let us clarify the subject by some examples:

(2.27) Example. Let $K = \mathsf{F}_2(x)$ be a rational function field over F_2. Consider the divisor $A = 2(x) + 2(x+1) - (x^2 + x + 1)$. Let $f \in L(A)$. Then $f = g \cdot (x^2 + x + 1/(x(x+1))^2$ where g is a polynomial of degree at most 2. To see this, note that f can have poles of order at most 2 in x and $(x+1)$ which forces the denominator of f to be of the form given; furthermore, $\mathrm{ord}_\infty(f)$ should be nonnegative which yields the condition on the degree of g. Therefore we get $\dim(A) = 3$. $\bullet$

(2.28) Example. By the same argumentation as above one can prove that if $k(x)/k$ is a rational function field and A is a divisor of positive degree in K/k, then $\dim(A) = \deg(A) + 1$. Hence $\dim(A) - \deg(A) = 1$ for all divisors of positive degree, which shows that the genus of $k(x)/k$ is equal to 0. •

(2.29) Example. Now that we have learned about function fields of genus 0, let us see how function fields of genus 1 look like. So assume that K/k is a function field of genus one and that there exists a prime divisor P of degree one in K/k. These fields are called *elliptic function fields*. By the Theorem of Riemann-Roch we have $\dim(P) = 1$. Since the constants clearly belong to $L(P)$, we have $L(P) = k$. Applying again the theorem we get $\dim(2P) = 2$, hence there exists a function x such that $L(2P) = \langle 1, x \rangle$. In the same way we get the existence of a function y such that $L(3P) = \langle 1, x, y \rangle$. Since for $f, g \in L(3P)$ we have $fg \in L(6P)$ we get

$$\langle 1, x, y, x^2, xy, y^2, x^3 \rangle \subseteq L(6P).$$

But $\dim(6P) = 6$. Thus there exist $a_0, \ldots, a_6 \in k$ such that

$$a_0 y^2 + (a_1 x + a_2) y = a_3 x^3 + a_4 x^2 + a_5 x + a_6.$$

So the field K is generated by the equation given above. •

2.9 Exercises

2.1. Show that any valuation on a finite field is trivial.

2.2. Let v be a multiplicative valuation of K. Show that $v(0) = 0$ and $v(\pm 1) = 1$.

2.3. Let v be a multiplicative valuation on K. For $a, b \in K$ show that if $v(a) \neq v(b)$ then $v(a + b) = \max\{v(a), v(b)\}$.

2.4. Show that two valuations of a field K are equivalent if and only if the corresponding valuation rings are equal.

2.5. Show that $\mathcal{M}_v$ is the unique maximal ideal of $\mathcal{O}_v$.

2.6. Let R be a commutative ring with 1 and M be a maximal ideal of R. Show that R/M is a field.

2.7. Show that $\mathrm{ord}_\infty(.)$ is a well defined valuation on $k(x)$.

2.8. Show that the residue class field of the valuation ord_∞ on $k(x)$ equals k.

2.9. Prove the product formula in the case of the rational function field.

2.10. Show that in the case of a rational function field a divisor is principal if and only if it is of degree 0.

CHAPTER 3

Geometric Goppa Codes

In this chapter we shall introduce Goppa's construction of codes over function fields or equivalently codes on algebraic curves [15]. The first section describes the construction of these codes while the next sections are devoted to the discussion of examples.

3.1 Construction of Geometric Goppa Codes

Let $K/\mathbf{F}_q$ be an algebraic function field of genus g. Further let $P_1, \ldots, P_n$ be different prime divisors of degree 1 of $K/\mathbf{F}_q$. Choose a divisor G of $K/\mathbf{F}_q$ satisfying $2g-2 < \deg(G) < n$ and $\mathrm{ord}_{P_i}(G) = 0$ for $i = 1, \ldots, n$. If $f \in \mathcal{O}_{P_i}$ and $\mathcal{M}_{P_i}$ denotes the maximal ideal of $\mathcal{O}_{P_i}$ we set $f(P_i) := f + \mathcal{M}_{P_i}$. Note that $f(P_i) \in \mathbf{F}_q$ for $i = 1, \ldots, n$, since the P_i are assumed to be of degree one. Consider the following mapping:

$$\begin{array}{rccl} \gamma\colon & L(G) & \to & \mathbf{F}_q^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

γ is a well defined mapping: since $\mathrm{ord}_{P_i}(G) = 0$, we have $\mathrm{ord}_{P_i}(f) \geq \mathrm{ord}_{P_i}(G) = 0$ for all $i = 1, \ldots, n$, hence $f \in \mathcal{O}_{P_i}$ for $i = 1, \ldots, n$, which implies that $f(P_i)$ is defined and belongs to $\mathbf{F}_q$. The second trivial observation is that γ is in fact a homomorphism of $\mathbf{F}_q$-spaces. Hence the image $C = C_K(G; P_1, \ldots, P_n)_q$ of γ is a linear subspace of $\mathbf{F}_q^n$, so it is a linear code.

(3.1) Definition. $C_K(G; P_1, \ldots, P_n)_q$ is called a *geometric Goppa code.* $\diamond$

The point now is that the parameters of C can be estimated by the Theorem of Riemann-Roch:

(3.2) Theorem. *If $K/\mathbf{F}_q$ is of genus g, then $C_K(G; P_1, \ldots, P_n)_q$ is an $[n, k, d]$-code with $k = \deg(G) - g + 1$ and $d \geq n - \deg(G)$.*

PROOF. The assertion about the block length of $C_K(G; P_1, \ldots, P_n)_q$ is obvious. For computing k, we have to compute $\dim(G)$ and $\dim\ker\gamma$ since $k = \dim(G) - \dim\ker\gamma$. The Theorem of Riemann-Roch yields $\dim(G) = \deg(G) - g + 1$. If $f \in \ker\gamma$, then $f(P_i) = 0$ for $i = 1, \ldots, n$. So $\mathrm{ord}_{P_i}(f) \geq 1$ which means that $f \in L(P_1 + \ldots P_n)$. This implies that $\ker\gamma \subseteq L(G - (P_1 + \ldots + P_n))$. But since $\deg(G) < n$, the degree of $G - (P_1 + \ldots + P_n)$ is negative, so the corresponding linear space is trivial. It follows that $\ker\gamma$ is trivial, i.e., γ is an embedding. So $k = \dim(G) = \deg(G) - g + 1$.

Now let $\mathbf{c}$ be an element of $C_K(G; P_1, \ldots, P_n)_q$ of weight $d \neq 0$. So there exists a function $f \in L(G)$ such that $\gamma(f) = \mathbf{c}$. Since $\mathbf{c}$ has weight d, it has $n-d$ zero coordinates which means that $f(P_i) = 0$ for $n - d$ of the prime divisors $P_1, \ldots, P_n$. Reordering these if necessary we may assume that f vanishes on $P_1, \ldots, P_{n-d}$. But this means that $f \in L(G - \sum_{i=1}^{n-d} P_i)$. Since $d \neq 0$, we have that $\mathbf{c} \neq 0$ and so $f \neq 0$. It follows that $L(G - \sum_{i=1}^{n-d} P_i) \neq \{0\}$. So we conclude that $\deg(G - \sum_{i=1}^{n-d} P_i) \geq 0$, so $d \geq n - \deg(G)$. □

3.2 Codes in the rational function field

Now let $K = \mathbf{F}_q(x)$. As we have seen, the prime divisors of degree 1 of K correspond to the elements of $\mathbf{F}_q \cup \{\infty\}$. Let $\alpha_1, \ldots, \alpha_n$ be elements of $\mathbf{F}_q$ and $G = m(\infty)$ where $0 < m < n$. If we denote by $P_1, \ldots, P_n$ the prime divisors $(x - \alpha_1), \ldots, (x - \alpha_n)$, we want to study the code $C_K(G; P_1, \ldots, P_n)_q$. Of course it suffices to compute the images of the basis elements of $L(G)$ under the mapping γ. For this we need a basis of $L(G)$. Now $G = m(\infty)$, so $1, x, \ldots, x^m \in L(G)$ since $\mathrm{ord}_\infty(x^k) = -k \geq -m$ for $k = 0, \ldots, m$. By the theorem of Riemann-Roch (note that $g = 0$ in this case) we get $\dim(G) = m + 1$. Since $1, x, \ldots, x^m$ are apparently linearly independent over $\mathbf{F}_q$, we conclude that they form a basis of $L(G)$. Now observe that $x^k(P_i) = x^k \bmod (x - \alpha_i) = \alpha_i^k$. So a generator matrix for $C_K(G; P_1, \ldots, P_n)_q$ is the following:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^m & \alpha_2^m & \ldots & \alpha_n^m \end{pmatrix}.$$

It is also possible to give explicit formulae for the generator matrices of the codes obtained from rational function fields for arbitrary G. Since it is only a matter of uninteresting computations, we just give an example:

(3.3) Example. Let $K = \mathbf{F}_7(x)$, $P_1 = (x)$, $P_2 = (x-1)$, $P_3 = (x-3)$, $P_4 = (x-5)$ and $P_5 = (\infty)$. Further let $G = 2(x-2) + (x-4)$. We have $\deg(G) = 3 < n = 5$. We can thus apply the construction of Section 3.1. We first compute a basis of $L(G)$: We can verify immediately that $g_1 := 1$, $g_2 := 1/(x-2)$, $g_3 := 1/(x-2)^2$ and $g_4 := 1/(x-4)$ belong to $L(G)$ (partial fraction decomposition). They are easily seen to be linearly independent too. Since $\dim(G) = \deg(G) + 1 = 4$ by the Theorem of Riemann-Roch, they form a basis for $L(G)$. We get the following generator matrix for the code obtained from these data:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 6 & 1 & 5 & 0 \\ 2 & 1 & 1 & 4 & 0 \\ 5 & 2 & 6 & 1 & 0 \end{pmatrix}.$$

This matrix is obtained as follows: The (i,j)-entry of this matrix is $g_i(P_j)$. If $P = (x-\alpha)$, $g(P) = g \bmod (x-\alpha) = g(\alpha)$. This explains the computation of the numbers in the first four columns of the matrix. If $P = (\infty)$, then $g(P) = 0$ whenever $\mathrm{ord}_\infty(g) \geq 1$. Since $\mathrm{ord}_\infty(g_i) \geq 1$ for $i = 2,3,4$, we get the zeros in the last column of the matrix. Further, the function 1 evaluated at any prime divisor equals 1, so the first row of the matrix is the all-one-vector. •

An interesting property of geometric codes over the rational function field is given in the exercises.

3.3 A Nontrivial Example

In this section we want to construct a code over a function field of genus greater than 0. Although we have not developed all the necessary tools for describing all the steps of the construction in these notes, we think that this example can nevertheless serve for the clarification of the subject. Let $\mathbf{F}_4 := \{0, 1, \omega, \overline{\omega}\}$ be the field with 4 elements. Define the function field K by $K = \mathbf{F}_4(x,y)$ with $x^3 + y^3 = 1$. This function field belongs to the class of the so-called "Hermitian function fields". The "curve" described by the equation $x^3 + y^3 = 1$ is called the "Hermitian curve". Without giving any computational details we remark that the genus of this function field equals 1. (See, e.g., [34].)

We have pointed out in Section 2.3 the connection between prime divisors and points of the corresponding curve. In particular we saw that (at least in the case of the rational function field) there is a correspondence between the prime divisors of degree one and the points of the projective line over the constant field. So in order to get a description of the prime divisors of degree one of K we first have to compute the points of the corresponding curve over $\mathbf{F}_4$, i.e., the set of pairs $(a,b) \in \mathbf{F}_4^2$ such that $a^3 + b^3 = 1$. But in order to get all the points we should work in the *projective plane* over $\mathbf{F}_4$ rather than in the affine plane. The *projective n-space* over a field k is

constructed as follows: Let ${}^*k^{n+1}$ denote the set of nonzero vectors in k^{n+1}. We can define on ${}^*k^{n+1}$ an equivalence relation by calling two vectors $\mathbf{x}$ and $\mathbf{y}$ equivalent if there exists a nonzero $\lambda \in k$ such that $\mathbf{x} = \lambda\mathbf{y}$. The set of equivalence classes under this relation is called a projective n-space over k. The coordinates of a point in the projective space are called *homogeneous coordinates.* If $n = 1$ we call this space the projective line and if $n = 2$ we call it the projective plane. What are the points of the projective line over a field k? If (x, y) belongs to the projective line and $y \neq 0$, we see that (x, y) and $(x/y, 1)$ represent the same point and if $y = 0$, (x, y) is equivalent to $(1, 0)$. Hence the points of the projective line consist of $(\alpha, 1)$ and $(1, 0)$ where α runs over the elements of k. If we call $(1, 0)$ the *point at infinity*, we get the known correspondence between prime divisors of degree one and the points of the projective line. Since we are working with homogeneous coordinates, we have to homogenize our equation, i.e., we should look for points satisfying the equation

$$x^3 + y^3 = z^3.$$

A short computation yields that there are nine points satisfying this equation:

$$\begin{array}{lll} Q = (1,0,1) & P_1 = (\omega,0,1) & P_2 = (\overline{\omega},0,1) \\ P_3 = (1,1,0) & P_4 = (\omega,1,0) & P_5 = (\overline{\omega},1,0) \\ P_6 = (0,1,1) & P_7 = (0,\omega,1) & P_8 = (0,\overline{\omega},1). \end{array}$$

Let α be an integer satisfying $0 < \alpha < 8$ and define the divisor G_α by $G_\alpha = \alpha Q$. We want to construct the code $C_K(G_\alpha; P_1, \ldots, P_8)_4$. For this we need first a basis of the space $L(G)$.

Consider the function $x - 1$. In order to be able to evaluate this function at the projective points, we have first to homogenize it. This yields the function $f = x - z$. We see that $f(Q) = 0$ and $1/f(P_3) = 1/f(P_4) = 1/f(P_5) = 0$. Hence $(f) \geq Q - P_3 - P_4 - P_5$. Now we use the following well known theorem [1].

(3.4) Theorem. *Let K/k be an algebraic function field and $f \in K$. If $(f) = A - B$ where A and B are integral divisors, then* $\deg(A) = \deg(B) = (K : k(f))$.

In our case $k(f) = \mathbf{F}_4(x - 1) = \mathbf{F}_4(x)$, hence $(K : k(f)) = 3$. Since by the above considerations $B := P_3 + P_4 + P_5$ is an integral divisor with $(x - 1) \geq -B$ and $\deg(B) = 3$ we deduce that $(x - 1) = A - (P_1 + P_2 + P_3)$ where A is an integral divisor of degree 3 and $A \geq Q$. But since $(x - 1)$ does not vanish at any other point, we see that $(x - 1) = 3Q - (P_3 + P_4 + P_5)$.

The same reasoning yields $(x - \omega) = 3P_1 - (P_3 + P_4 + P_5)$ and $(x - \overline{\omega}) = 3P_2 - (P_3 + P_4 + P_5)$. Now $y^3 + x^3 = 1$, so $y^3 = (x^3 - 1) = (x - 1)(x - \omega)(x - \overline{\omega})$. Since the function y vanishes at Q, P_1, P_2 we deduce that $(y) = Q + P_1 + P_2 - (P_3 + P_4 + P_5)$. Now a basis for $L(G_\alpha)$ can be obtained very easily. Since $f_1 := 1 \in L(G_\alpha)$ for all α, and $\dim(G_\alpha) = \alpha$ by the Theorem of Riemann-Roch, a basis for $L(G_1)$ is 1.

The function $f_2 := y/(x-1)$ has the principal divisor $P_1 + P_2 - 2Q$, so a basis for $L(G_2)$ is $1, y/(x-1)$. Further, the function $f_3 := 1/(x-1)$ has the divisor $(P_3 + P_4 + P_5) - 3Q$, so $1/(x-1) \in L(3G)$. On the same way we get:

$$f_4 := (y/(x-1))^2 \in L(4G), \quad f_5 := (y/(x-1)^2) \in L(5G),$$
$$f_6 := (y/(x-1))^3 \in L(6G), \quad f_7 := (y^2/(x-1)^3) \in L(7G).$$

Now we use the following lemma:

(3.5) Lemma. *Suppose K/k is an algebraic function field, P is a prime divisor of K/k and $f_1, \ldots, f_m$ are nonzero functions in K. If $\mathrm{ord}_P(f_i) \neq \mathrm{ord}_P(f_j)$ for $i \neq j$, the functions $f_1, \ldots, f_m$ are linearly independent.*

PROOF. Let x and y be nonzero functions in K such that $\mathrm{ord}_P(x) \neq \mathrm{ord}_P(y)$. By Exercise 2.3 $\mathrm{ord}_P(x+y) = \min(\mathrm{ord}_P(x), \mathrm{ord}_P(y))$. Repeating this reasoning we get with the assumptions of the lemma: $\mathrm{ord}_P(\sum_{i=1}^m \alpha_i f_i) = \min\{\mathrm{ord}_P(f_i) \mid i = 1, \ldots, m\}$ where α_i are arbitrary elements of k. Now suppose that $\sum_{i=1}^m \alpha_i f_i = 0$ for elements $\alpha_1, \ldots, \alpha_m \in k$ not all equal to 0. Without loss of generality we may assume that α_1 is not zero. We get $-\alpha_1 f_1 = \sum_{i=2}^m \alpha_i f_i$. Taking ord_P on both sides of this equation we obtain $\mathrm{ord}_P(f_1) = \min\{\mathrm{ord}_P(f_i) \mid i = 2, \ldots, m\}$. This is a contradiction since the $\mathrm{ord}_P(f_i)$ were assumed to be different. □

Since in our case $\mathrm{ord}_Q(f_i) = i$ for $i > 1$ and $\mathrm{ord}_P(f_1) = 0$, we can apply this lemma for $P := Q$ to get that $f_1, \ldots, f_7$ are linearly independent.

(3.6) Theorem. $L(G_\alpha) = (f_1, \ldots, f_\alpha)$.[1].

In order to compute generator matrices for the codes $C_K(G_\alpha; P_1, \ldots, P_8)_4$ we have to know how to evaluate the functions f_j at the points P_i. For this we have to homogenize the functions, i.e. replace x by x/z and y by y/z. This gives

$$\begin{array}{lll} f_1 = 1, & f_2 = y/(x-z), & f_3 = 1/(x-z), \\ f_4 = (y/(x-z))^2 & f_5 = yz/(x-z)^2 & f_6 = (y/(x-z))^3 \\ f_z = y^2 z/(x-z)^3. & & \end{array}$$

Now evaluations of these functions at the points is trivial. We just give as an example a generator matrix for the code $C_K(G_4; P_1, \ldots, P_8)_4$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \overline{\omega} & \omega & 1 & \omega & \overline{\omega} \\ \omega & \overline{\omega} & 1 & \overline{\omega} & \omega & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega & \overline{\omega} & 1 & \overline{\omega} & \omega \end{pmatrix}.$$

[1] By $(x_1, \ldots, x_n)$ we denote the span of $x_1, \ldots, x_n$

Observe an interesting property of this code: With respect to the symmetric bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{8} x_i y_i$ every codeword is orthogonal to every other codeword!

What about the parameters of the above code? Of course the dimension equals $\deg(G_4) = 4$. By (3.2) the minimum distance d of this code satisfies $d \geq 8 - \deg(G_4) = 4$. It turns out that the minimum distance of this code is 4.

3.4 Exercises

3.1. If $C_K(G; P_1, \ldots, P_n)_q$ is a geometric Goppa code over the rational function field $K = \mathbf{F}_q(x)$, prove that its minimum distance d satisfies $d = n - \deg(G)$.

CHAPTER 4

Codes above the Gilbert-Varshamov-Bound

In this chapter we shall show how one can construct codes which asymptotically lie above the Gilbert-Varshamov-bound.

4.1 Asymptotics

In this section we want to investigate the asymptotic properties of geometric Goppa codes.

For the rest of this section we fix a finite field $\mathbf{F}_q$. Let K be an algebraic function field of genus g over $\mathbf{F}_q$ having at least $n+1$ prime divisors of degree one, which we denote by $P_1, \ldots, P_n, Q$. Further let $G := \alpha Q$ for some natural number α satisfying $2g-2 < \alpha < n$. Let $C := C_K(G; P_1, \ldots, P_n)_q$ be the geometric Goppa code as constructed in 3.1. Denote by d the minimum distance and by k the dimension of C. Then, by (3.2) we have

$$\begin{aligned} d &\geq n - \alpha \\ k &= \alpha - g + 1. \end{aligned}$$

Hence we obtain:

(4.1) $$\delta(C) + R(C) \geq 1 - g/n + 1/n.$$

(See Section 1.6 for the definition of $\delta(C)$ and $R(C)$.) Now consider the set S of sequences of function fields such that for every sequence σ in S the number of prime divisors of degree one of K goes to infinity as K runs through the elements of σ. For each such sequence σ we define $\gamma_\sigma := \liminf_{K \in \sigma} g(K)/n(K)$, where $g(K)$ denotes the genus of the function field K and $n(K)+1$ is the number of prime divisors of degree one of K.

(4.2) Lemma. *For $\sigma \in S$ let L_σ denote the line segment $L_\sigma := \{(\delta, R) \mid \delta + R = 1 - \gamma_\sigma, \delta \in (0, 1-\gamma_\sigma)\}$. Then $L_\sigma \subset \Sigma_q$.*

PROOF. Let $\sigma \in S$ be fixed. We may assume that $\lim_{K \in \sigma} g(K)/n(K) = \gamma_\sigma$. Let $\delta \in (0, 1 - \gamma_\sigma)$ be given. For $K \in \sigma$ let $\alpha = \alpha(K) := \lfloor (1-\delta)n(K) \rfloor$[1]. Let C_K be the geometric Goppa code constructed over K as above. By puncturing the code if necessary, we may assume that C_K has minimum distance $n(K) - \alpha$ and dimension $\alpha(K) - g(K) + 1$. Hence, $\lim_{K \in \sigma}(\delta(C_K), R(C_K)) = (\delta, 1 - \gamma_\sigma - \delta)$, as was to be proved. □

4.2 Codes Beyond the Gilbert-Varshamov-Bound

Let us consider a sequence $\sigma \in S$. Since the Gilbert-Varshamov curve (see Section 1.6)

$$G(x) := 1 - x \log_q(q-1) + x \log_q(x) + (1-x) \log_q(1-x)$$

is convex, the line L_σ either intersects $G(x)$ in the interval $(0,1)$ in two points (counting multiplicities) δ_1, δ_2 and is above $G(x)$ for $\delta \in (\delta_1, \delta_2)$, or L_σ does not intersect $G(x)$ in the interval $(0,1)$. Thus, if we find sequences σ, such that L_σ intersects $G(x)$, we have found sequences of linear codes which are asymptotically above the Gilbert-Varshamov-bound.

When does L_σ intersect $G(x)$?

(4.3) Lemma. *L_σ intersects $G(x)$ if and only if $\gamma_\sigma < \log_q(2q-1) - 1$.*

PROOF. Let us first compute when L_σ is tangent to $G(x)$. We have

$$G'(X) = -\log_q(q-1) - \log_q(x) + \log_q(1-x).$$

Hence, $G'(\delta_0) = -1$ for $\delta_0 = (q-1)/(2q-1)$. So L_σ is tangent to $G(x)$ if $\gamma_\sigma = \phi(\delta_0) - \delta_0 = \log_q(2q-1) - 1$. This proves the result. □

Our task is now to find sequences σ which satisfy the above inequality. In the next chapters we shall sketch how to find such sequences.

[1] $\lfloor x \rfloor$ is defined to be the largest integer $\leq x$.

CHAPTER 5

Modular Function Fields

5.1 Introduction

In the previous chapters we have given an introduction to the theory of algebraic geometric codes. One of the most striking facts about this class of codes is their asymptotic significance, first realized by TSFASMAN, VLADUT, and ZINK [43]. They showed that the class of algebraic geometric codes contains sequences of codes which lie asymptotically above the Gilbert-Varshamov bound. As we saw in the previous chapter, one can manage in proving such a theorem by considering sequences of function fields over finite fields having many prime divisors of degree one relative to their genus. In the following chapters we shall introduce the function fields used in this context.

5.2 Congruence Subgroups

The main purpose of this section is to explain the construction of modular function fields. Throughout this chapter G denotes the group $\mathrm{GL}_2(\mathbf{R})^+$ of real (2×2)-matrices of positive determinant. It is clear that under the usual topology of $\mathbf{R}^4$ the group G becomes a topological group (which means that inversion and multiplication in G are continuous operations) and that $\mathrm{SL}_2(\mathbf{Z})$ is a discrete subgroup of G, i.e., every element of $\mathrm{SL}_2(\mathbf{Z})$ has a neighborhood in G which does not contain any other element of $\mathrm{SL}_2(\mathbf{Z})$.

(5.1) Definition. Let N be a positive integer. The *Hecke-subgroup* $\Gamma_0(N)$ is defined by

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}.$$

$\diamond$

The geometric structure of G is best reflected by its action on the upper half plane $\mathbf{H} := \{z \in \mathbf{C} \mid \operatorname{Im} z > 0\}$ given in the following: for $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and $z \in \mathbf{H}$ we define the action of A on z by

$$Az := \frac{az+b}{cz+d}.$$

It is easily seen that this action of G on $\mathbf{H}$ is transitive. However, this is not true for the restricted action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{H}$ (compare the exercises).

Now let Γ be a Hecke-subgroup or $\mathrm{SL}_2(\mathbf{Z})$. Γ acts on $\mathbf{H}$ as a subgroup of G.

(5.2) Definition. Let Γ be any discrete subgroup of $\mathrm{SL}_2(\mathbf{R})$. Then $F = F(\Gamma)$ is called a *fundamental domain for* $\Gamma\backslash\mathbf{H}$ if

(i) F is a connected open subset of $\mathbf{H}$,

(ii) no two points of F are equivalent under Γ,

(iii) every point of $\mathbf{H}$ is equivalent to some point of the closure of F under Γ.

◇

(5.3) Example. A fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{H}$ is given by the following set [31]:

$$F(\mathrm{SL}_2(\mathbf{Z})) = \left\{ z \in \mathbf{H} \;\middle|\; -\frac{1}{2} < \operatorname{Re}(z) < \frac{1}{2},\ |z| > 1 \right\}.$$

The closure of $F(\mathrm{SL}_2(\mathbf{Z}))$ under $\mathrm{SL}_2(\mathbf{Z})$ is given by

$$\begin{aligned} F'(\mathrm{SL}_2(\mathbf{Z})) \;=\; & F(\mathrm{SL}_2(\mathbf{Z})) \cup \{z \in \mathbf{H} \mid |z| \geq 1,\ \operatorname{Re}(z) = -1/2\} \\ & \cup \{z \in \mathbf{H} \mid |z| = 1, -1/2 \leq \operatorname{Re}(z) \leq 0\}. \end{aligned}$$

•

Our aim now is to associate to every Hecke-subgroup a function field of one variable over $\mathbf{C}$. For this we review first some basic topological facts.

Let X be a topological space. A *complex analytic structure* S on X is a set S such that

(i) S is a collection of pairs (U_i, p_i) with i in a set I of indices, where $\{U_i\}_{i \in I}$ is an open covering of X and p_i is a homeomorphism of U_i onto an open subset of $\mathbf{C}$,

(ii) if $U_i \cap U_j \neq \emptyset$, the map

$$p_j p_i^{-1}\colon \quad p_i(U_i \cap U_j) \to p_j(U_i \cap U_j)$$

is holomorphic, and

(iii) S is maximal under the conditions (i) and (ii).

(See [32, §1.5].)

(5.4) Definition. A connected Hausdorff topological space with a complex analytic structure is called a *Riemann surface.* ◇

Now let X be a Riemann surface and consider the set $K(X)$ of meromorphic functions $f: X \to \mathbf{C}$. This set forms a field which contains a rational function field over $\mathbf{C}$. Once one can prove that $K(X)$ is a finite extension of this rational function field, one obtains that $K(X)$ is a field of algebraic functions of one variable over $\mathbf{C}$. The finiteness is in general not guaranteed. However, one can force the finiteness by assuming that X be compact. The following theorem is classical. For a proof the reader is referred to [28, §9.6].

(5.5) Theorem. *The field of meromorphic functions on a compact Riemann surface is an algebraic function field of one variable over* $\mathbf{C}$.

We would like to associate a compact Riemann surface to a Hecke-subgroup $\Gamma_0(N)$. Let us study first the case of $\mathrm{SL}_2(\mathbf{Z})$. A good candidate for a topological space associated to $\mathrm{SL}_2(\mathbf{Z})$ would be the set of orbits $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$. We define a topology on this set in the following manner: if $\overline{z}$ is the orbit of the element $z \in \mathbf{H}$, the set of open neighborhoods of $\overline{z}$ is defined to consist of all $\mathrm{SL}_2(\mathbf{Z})U$, where U runs over the open neighborhoods of z in $\mathbf{H}$. But with this topology the set $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$ is not compact: for instance, the sequence of orbits of the elements $1 + in$, where n runs over the positive integers, does not have a limit in $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$. But by considering the set $F'(\mathrm{SL}_2(\mathbf{Z}))$ it is easily seen that only sequences which converge to ∞ do not have a limit in $F'(\mathrm{SL}_2(\mathbf{Z}))$. So it is possible to compactify $F'(\mathrm{SL}_2(\mathbf{Z}))$ by adding to it $\overline{\infty}$ and defining an appropriate system of open neighborhoods for this new point. We take the sets $\{\infty\} \cup \{z \in \mathbf{H} \mid \mathrm{Im}(z) > r\}$ for all positive numbers r as a fundamental system of open neighborhoods of ∞. The action of $\mathrm{SL}_2(\mathbf{Z})$ on ∞ can be defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty := a/c$; hence $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathbf{H} \cup \mathbf{Q} \cup \{\infty\}$. The fundamental system of neighborhoods of the orbit $\overline{\infty}$ of ∞ is the set of all $\mathrm{SL}_2(\mathbf{Z})U$ where U runs over the fundamental set of open neighborhoods of ∞. With this topology, $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H} \cup \{\overline{\infty}\}$ is seen to be a compact topological space (isomorphic to the Riemann sphere).

Defining an analytic structure on $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H} \cup \{\infty\}$ which turns this topological space into a compact Riemann surface needs some work. We just mention that this is possible and refer the reader to [32, §1.5].

Now let us discuss the general case. In general, the fundamental domain $F(\Gamma_0(N))$ of a Hecke-subgroup $\Gamma_0(N)$ is not compact. To compactify this set we have to add to it a finite number of additional points in $\mathbf{Q} \cup \{\infty\}$ for which the system of neighborhoods are to be defined properly.

In the sequel, we denote by $\mathbf{H}^*$ the set $\mathbf{H} \cup \mathbf{R} \cup \{\infty\}$. The action of G on $\mathbf{H}$ can be extended in a straightforward manner to an action on $\mathbf{H}^*$. We call a non-identity

element α of G parabolic if $\mathrm{tr}(\alpha)^2 = 4\det(\alpha)$, or what is the same, if α has exactly one real eigenvalue (of multiplicity two). We leave it as an exercise to the reader to prove that an element $\alpha \in G$ is parabolic if and only if α has a unique fixed point in $\mathbf{R} \cup \{\infty\}$.

(5.6) Definition. A fixed point $c \in \mathbf{R} \cup \{\infty\}$ of a parabolic element of a Hecke-subgroup $\Gamma_0(N)$ is called a *cusp* of $\Gamma_0(N)$. Two cusps of $\Gamma_0(N)$ are called *equivalent* if there is an element of $\Gamma_0(N)$ which maps one of these cusps to another. $\diamond$

(5.7) Example. Let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ be parabolic, i.e., $(d+a)^2 - 4(ad-bc) = (d-a)^2 + 4bc = 0$, and z be a fixed point of α. If $c = 0$, then $a = d = \pm 1$ and $z = \infty$. Otherwise $cz^2 + (d-a)z - b = 0$, which implies $z = (a-d)/c \in \mathbf{Q}$. Hence the set $C(\mathrm{SL}_2(\mathbf{Z}))$ of cusps of $\mathrm{SL}_2(\mathbf{Z})$ is contained in $\mathbf{Q}^* := \mathbf{Q} \cup \{\infty\}$. We want to show that $\mathbf{Q}^* = C(\mathrm{SL}_2(\mathbf{Z}))$. Since $\infty \in C(\mathrm{SL}_2(\mathbf{Z}))$, it is fixed under the parabolic element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let p/q be an arbitrary element of $\mathbf{Q}$ and suppose that p and q are coprime. It suffices to show that there exists $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ such that $\alpha\infty = p/q$: then, since ∞ is a cusp, there exists a parabolic element $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ such the $\gamma\infty = \infty$. Hence the parabolic element $\alpha\gamma\alpha^{-1}$ fixes p/q which shows that $p/q \in C(\mathrm{SL}_2(\mathbf{Z}))$. Since p and q are coprime, there exist $u, v \in \mathbf{Z}$ such that $up - vq = 1$. The matrix $\alpha := \left(\begin{smallmatrix} p & v \\ q & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ satisfies $\alpha\infty = p/q$. Hence $C(\mathrm{SL}_2(\mathbf{Z})) = \mathbf{Q}^*$. We also see that all the cusps of $\mathrm{SL}_2(\mathbf{Z})$ are equivalent. $\bullet$

(5.8) Remark. The above example shows that the set of cusps of any Hecke-subgroup is a subset of $\mathbf{Q}^*$. $\bullet$

As in the case of $\mathrm{SL}_2(\mathbf{Z})$, we can compactify the fundamental domain of any Hecke-subgroup by adding to it a finite set of inequivalent cusps. For the fundamental domain of the action of $\Gamma_0(N)$ on $\mathbf{H}^*$, which we shall denote by $\Gamma_0(N)\backslash\mathbf{H}^*$, we introduce the following fundamental system of neighborhoods for each point:

- If $z \in \mathbf{H}$, the fundamental system of neighborhoods of z is the usual system of Euclidean neighborhoods given by

$$U_r(w) = \{w \in \mathbf{H} \mid |w - z| < r\},$$

  where r runs over the set of positive real numbers.

- If $z = \infty$, a fundamental system of neighborhoods of ∞ is given by

$$U_r(\infty) = \{w \in \mathbf{H} \mid \mathrm{Im}\, w > r\},$$

  where again r runs over the set of positive real numbers.

- If $z \in \mathbf{Q}$, a fundamental system of neighborhoods of z is defined by the set consisting of z and the interiors of the circles in $\mathbf{H}$ which are tangent to z.

We do not define neighborhoods for non-rational elements of $\mathbf{R}$, since we shall only add cusps of $\Gamma_0(N)$ to the fundamental domain $F(\Gamma_0(N))$ and these cusps are either rational numbers or ∞, see (5.8). It turns out that under the topology defined above, the set $\Gamma_0(N)\backslash\mathbf{H}^*$ becomes a locally compact Hausdorff topological space [32, pp. 12]. Furthermore, this space can be endowed with a complex analytic structure, such that under this structure $\Gamma_0(N)\backslash\mathbf{H}^*$ is a compact Riemann surface [32, §1.5].

(5.9) Theorem. *Let $\Gamma = \Gamma_0(N)$ for some natural number N. Then $\Gamma\backslash\mathbf{H}^*$ is a compact Riemann surface, i.e., an algebraic function field of one variable over the field $\mathbf{C}$ of complex numbers.*

(5.10) Definition. The function field of the compact Riemann surface $\Gamma_0(N)\backslash\mathbf{H}^*$ is denoted by $K_0(N)$, and is called the *modular function field.* $\diamond$

By considering the arithmetic of the modular function fields, one obtains formulas for the genus of the function fields $K_0(N)$. For future applications we confine ourselves to stating the result only in the case where N is a prime [32].

(5.11) Theorem. *Let $g_0(N)$ denote the genus of $K_0(N)$. If N is a prime greater than 3, we have:*

$$g_0(N) = \begin{cases} \dfrac{N-13}{12} & \text{if } N \equiv 1 \bmod 12, \\ \dfrac{N-5}{12} & \text{if } N \equiv 5 \bmod 12, \\ \dfrac{N-7}{12} & \text{if } N \equiv 7 \bmod 12, \\ \dfrac{N+1}{12} & \text{if } N \equiv 11 \bmod 12. \end{cases}$$

The function fields $K_0(N)$ are defined over the complex numbers. As algebraic function fields of one variable they are finite extensions of a rational function field $\mathbf{C}(t)$ over $\mathbf{C}$, i.e., $K_0(N) = \mathbf{C}(t)(\omega)$ where ω and t are related by an equation $f(t,\omega) = 0$ for some $f \in \mathbf{C}[X,Y]$. Now suppose that $f \in \mathbf{Z}[X,Y]$. What can we say about the function field $\mathbf{Q}(t)(\omega)$ where ω and t are related by the same equation $f(t,\omega) = 0$? We could also go one step further and reduce the coefficients of f modulo some prime number p and ask about the function field $\mathbf{F}_p(t,\omega)$ where t and ω are related by $f_p(t,\omega) = 0$, f_p denoting the reduction of f modulo p.

In general, if an algebraic function field K is defined over some field k of characteristic 0 by an equation of the type $f(x,y) = 0$, $f \in \mathbf{Z}[X,Y]$, the arithmetic properties are changed if one considers the function field over $\mathbf{F}_p$ generated by the reduction of f modulo p.

(5.12) Example. Consider the elliptic function field $K = \mathbf{Q}(x, y)$, $y^2 = x^3 - 3x - 3$. Reduction modulo 3 yields the function field $\mathbf{F}_3(x, y)$, $y^2 = x^3$, which is of genus zero. •

One of the most remarkable facts about the modular function fields $K_0(N)$ is the following theorem due to IGUSA [18] (we just state a weak version of this theorem).

(5.13) Theorem. *$K_0(N)$ contains a rational subfield $\Omega_0(N)$ such that $K_0(N)$ is generated over $K_0(N)$ by an equation $f(x, y) = 0$, $f \in \mathbf{Z}[X, Y]$, and such that for all p not dividing N the function field $K_0^p(N) := \mathbf{F}_p(x, y)$, $f_p(x, y) = 0$, has genus $g_0(N)$, f_p denoting the reduction of f modulo p.*

We call the function fields $K_0^p(N)$ generated by the polynomials f_p of the previous theorem *p-modular function fields.*

There remain a lot of unanswered questions at this stage, one of the most important being the question of the uniqueness of f upon imposing further conditions on the p-modular function fields to be obtained by the reduction of f. These questions can be best answered by using the language of algebraic geometry, which we have not developed here. For our purposes it is sufficient to know that these function fields exist and that their genus as well as their number of rational points can be obtained by analytic arguments carried out in characteristic 0.

These function fields will be used to prove the existence of linear codes above the Gilbert-Varshamov-bound. What we still have to compute is the number of rational points of p-modular curves over $\mathbf{F}_p$ or an extension of $\mathbf{F}_p$. It is a remarkable fact that this number, similar to the genus, can be computed using the analytic structure of the modular function fields $K_0(N)$ over the field $\mathbf{C}$. We shall describe this method in the next chapters.

5.3 Exercises

5.1. Show that the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{H}$ is not transitive.

5.2. Show that with the topology described above, the fundamental domain $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$ is not compact.

5.3. Prove that an element $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ is parabolic if and only if it has a unique fixed point in $\mathbf{R} \cup \{\infty\}$.

CHAPTER 6

The Space of Cusp Forms

6.1 Introduction

As described at the end of the last chapter, we can employ analytic techniques to obtain the number of rational points of a p-modular curve over $\mathbf{F}_p$. This will be done in the following way: let Γ denote a Hecke-subgroup or $\mathrm{SL}_2(\mathbf{Z})$. We first define for Γ a finite dimensional $\mathbf{C}$-vector space, the space $S_2(\Gamma)$ of cusp forms of weight 2, of holomorphic functions from $\mathbf{H}^*$ to $\mathbf{C}$ which satisfy certain transformation properties and regularity conditions. Next we introduce on this finite dimensional vector space a linear operator, the Hecke operator, the trace of which is fundamental in the theory. The trace of the Hecke operators on the space of cusp forms is computed via the Eichler-Selberg trace formula, which we shall only refer. The main fact is now that the number of rational points of p-modular function fields over extensions of $\mathbf{F}_p$ is closely related to the traces of Hecke operators on $S_2(\Gamma)$. In this way we shall be able to compute this number and proceed with the proof of the theorem of TSFASMAN, VLADUT, and ZINK.

6.2 The Space of Cusp Forms

For a matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we put $j(\alpha, z) = cz + d$ for $z \in \mathbf{H}$. It is clear that $j(\alpha, z)$ is a holomorphic function on $\mathbf{H}$, and the relation

$$j(\alpha\beta, z) = j(\alpha, \beta z) j(\beta, z),$$

can be verified quickly.

(6.1) Definition. Let k be an integer and Γ be a Hecke-subgroup or $\mathrm{SL}_2(\mathbf{Z})$. A holomorphic function $f: \mathbf{H}^* \to \mathbf{C}$ is called a *modular form of weight k with respect to Γ* if

$$\forall \alpha \in \Gamma \, \forall z \in \mathbf{H}: \qquad f(z) = j(\alpha, z)^{-k} f(\alpha z).$$

A modular form of weight k with respect to Γ which vanishes at all cusps of Γ is called a *cusp form of weight k with respect to Γ*. $\diamond$

When Γ is a Hecke-subgroup, one can compute the dimension of the space of cusp forms $S_k(\Gamma)$ by studying the arithmetic of automorphic forms. The interested reader is referred to [32, §2]. We focus our interest on the following fact.

(6.2) Theorem. *Let Γ be a Hecke-subgroup. For every natural number k the set $S_k(\Gamma)$ is a finite-dimensional $\mathbf{C}$-vector space. Further, the dimension of $S_2(\Gamma)$ equals the genus of the modular function field associated to Γ.*

6.3 Hecke Operators

In this section we introduce linear operators on the vector space of cusp forms of weight k. It turns out that in the case $k = 2$ the traces of these operators as endomorphisms of $S_2(\Gamma)$ play an important role in the determination of the number of prime divisors of degree one of the p-modular function fields $K_0^p(N)$ over $\mathbf{F}_{p^2}$.

To begin with, let Γ denote a Hecke-subgroup $\Gamma_0(N)$ for some N and

$$\Delta := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid c \equiv 0 \bmod N, \gcd(a, N) = 1, ad - bc > 0 \right\}.$$

One can prove that for every $\alpha \in \Delta$ the double coset $\Gamma\alpha\Gamma$ has a decomposition

$$\Gamma\alpha\Gamma = \cup_i \Gamma\alpha\gamma_i$$

where $\{\gamma_i\}$ is a finite set of representatives of the quotient $\Gamma/(\Gamma \cap \alpha^{-1}\Gamma\alpha)$. Let $R(N)$ be the free abelian group generated by the double cosets $\Gamma\alpha\Gamma$ for $\alpha \in \Delta$, i.e., $R(N)$ is the set of all formal sums

$$\sum_{\alpha \in \Delta} m_\alpha \Gamma\alpha\Gamma,$$

where $m_\alpha \in \mathbf{Z}$ for all $\alpha \in \Delta$ and $m_\alpha = 0$ for all but finitely many α.

We can impose a structure of a $\mathbf{Z}$-algebra on $R(N)$ in the following manner: let $\alpha, \beta \in \Delta$, $\Gamma\alpha\Gamma = \cup_i \Gamma\alpha_i$, and $\Gamma\beta\Gamma = \cup_j \Gamma\beta_j$. We define the multiplication of these double cosets by

$$(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma) := \sum_{\gamma \in \Delta} c_\gamma \Gamma\gamma\Gamma,$$

where for every $\gamma \in \Delta$ we have $c_\gamma := \#\{(i, j) \mid \Gamma\alpha_i\beta_j = \Gamma\gamma\}$. It can be shown that this multiplication is well-defined [32]. Extending this multiplication linearly, we obtain a structure of a $\mathbf{Z}$-algebra on $R(N)$.

(6.3) Definition. The algebra $R(N)$ is called the *Hecke algebra of the pair* (Γ, Δ). The elements of $R(N)$ are called *Hecke operators*. $\diamond$

To see why the elements of $R(N)$ are called operators, we define an action of $R(N)$ on $S_k(\Gamma)$ as follows: For a double coset $\Gamma\alpha\Gamma = \cup_{i=1}^{d}\Gamma\alpha_i \in R(N)$ and a cusp form $f \in S_k(\Gamma)$ we define

$$((\Gamma\alpha\Gamma)f)(z) := \det(\alpha)^{k/2-1}\sum_{i=1}^{d} j(\alpha_i, z)^{-k} f(\alpha_i z).$$

It can be shown that this action is independent of the decomposition of $\Gamma\alpha\Gamma$, and $(\Gamma\alpha\Gamma)f \in S_k(\Gamma)$ [32]. Extending this action to $R(N)$, we see that for every k, $R(N)$ can be viewed as an algebra of $S_k(\Gamma)$-operators. This gives rise to $\mathbf{C}$-representations of $R(N)$.

In the following we want to describe the structure of $R(N)$. Using the theory of elementary divisors we see that for every double coset $\Gamma\alpha\Gamma$ there exist uniquely determined $l, m \in \mathbf{Z}$, $l, m > 0$, $\gcd(l, N) = 1$, $l|m$, such that

$$\Gamma\alpha\Gamma = \Gamma\begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix}\Gamma.$$

Now set

$$T(l, m) := \Gamma\begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix},$$

and

$$T(n) := \sum_{\substack{lm=n \\ l,m \text{ as above}}} T(l, m).$$

Then one has the following theorem.

(6.4) Theorem. *The Hecke algebra $R(N)$ is the polynomial ring over $\mathbf{Z}$ generated by $T(p)$, $T(p,p)$, $T(q)$, where p runs over the primes not dividing N and q runs over the prime divisors of N. In other words,*

$$R(N) = \mathbf{Z}[T(p), T(p,p), T(q) \mid p, q \text{ prime}, p \nmid N, q|N].$$

A proof of this theorem is given in [32] or [26]. In particular, it can be shown that $R(N)$ is a commutative and associative algebra [32].

As was indicated before, the traces of Hecke operators acting on the space $S_2(\Gamma_0(N))$ play an important role in the determination of the number of prime divisors of degree one of a p-modular function field. We omit the difficult computations concerning these traces and state only the result for prime N. The formula obtained is a special case of the so-called *Eichler-Selberg trace formula* [22].

(6.5) Theorem. *Let N be a prime number and p be a prime different from N. Then the trace of the Hecke operator $T(p^2)$ on $S_2(\Gamma)$ is given by*

$$\operatorname{tr}(T(p^2)) = -\sum_{s,f} \frac{h(D)}{w(D)} \left(1 + \left(\frac{D}{N}\right)\right) + p^2 + 1 + g_0(N),$$

where s runs over the integers satisfying $-2p < s < 2p$, f runs over the positive integers such that f^2 is a divisor of $D := s^2 - 4p^2$ and such that $(s^2 - 4p^2)/f^2 \equiv 0$ or $1 \bmod 4$, $h(D)$ is the class number of the order $\mathcal{O}_D$ of discriminant D of $\mathbb{Q}(\sqrt{D})$, $w(D)$ is the number of roots of unity of $\mathcal{O}_D$, and $\left(\frac{D}{N}\right)$ is the Jacobi symbol.

A proof of this theorem can be found for instance in [17] (see also [27]). Also the *Selberg trace formula* [33] can be applied to obtain this result.

CHAPTER 7

Number of Prime Divisors of p-modular Fields

7.1 Relation to the Traces of Hecke Operators

Let $K/\mathbf{F}_q$ be an algebraic function field of one variable and for every n, let a_n denote the number of prime divisors of degree one of the field $K\mathbf{F}_{q^n}/\mathbf{F}_{q^n}$. The *Z-function* of K is defined by

$$Z(K;u) := \exp(\sum_{i=1}^{\infty} a_i \frac{u^i}{i}).$$

It is related to the usual ζ-function of $K/\mathbf{F}_q$ in the following way: the ζ-function $\zeta(K;s)$ of $K/\mathbf{F}_q$ is defined by $\zeta(K;s) = \sum_A \frac{1}{N(A)}$ where the sum runs over all integral divisors A of $K/\mathbf{F}_q$ and $N(A)$ denotes the norm of the divisor A. Then $Z(K;q^{-s}) = \zeta(K;s)$.

(7.1) Example. Let $K = \mathbf{F}_q(x)$ be a rational function field over $\mathbf{F}_q$. The number of prime divisors of degree one of $K\mathbf{F}_{q^n}/\mathbf{F}_{q^n}$ is $q^n + 1$. Now observe that

$$\begin{aligned} -\log(1-u) - \log(1-qu) &= \sum_{i=1}^{\infty} \frac{u^i}{i} + \sum_{i=1}^{\infty} \frac{q^i u^i}{i} \\ &= \sum_{i=1}^{\infty} (q^i + 1)\frac{u^i}{i}. \end{aligned}$$

Hence we see that

$$Z(\mathbf{F}_q(x);u) = \frac{1}{(1-u)(1-qu)}.$$

•

The above example is in some sense characteristic. One can show the following [29].

(7.2) Theorem. *For every algebraic function field of one variable $K/\mathbf{F}_q$ of genus g, there exists a polynomial $L(K;u) \in \mathbf{Z}[u]$ of degree $2g$ such that*

$$Z(K;u) = \frac{L(K;u)}{(1-u)(1-qu)}.$$

Many fundamental properties of the function field K are encoded in the polynomial $L(K;u)$. In particular, for any n the number a_n is related to the zeros of L. Note that $L(K;0) = Z(K;0) = 1$, hence $L(K;u) = \prod_{i=1}^{2} g(1-\alpha_i u)$ for some $\alpha_1, \ldots, \alpha_{2g} \in \mathbf{C}$.

(7.3) Theorem. *Let $\alpha_1, \ldots, \alpha_{2g}$ be such that $L(K;u) = \prod_{i=1}^{2g}(1-\alpha_i u)$. Then*

$$\forall\, n \geq 1: \qquad a_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^m.$$

PROOF. Let $E(u) := \log Z(K;u) = \sum_{n=1}^{\infty} a_n x^n/n$. Then

$$E(u) = \sum_{i=1}^{2g} \log(1-\alpha_i u) - \log(1-u) - \log(1-qu).$$

Hence, if $E^{(n)}(u)$ denotes the nth formal derivative of $E(u)$, we obtain

$$E^{(n)}(u) = (n-1)!\left(-\sum_{i=1}^{2g} \frac{\alpha_i^n}{(1-\alpha_i u)^n} + \frac{1}{(1-u)^n} + \frac{q^n}{(1-qu)^n}\right).$$

Now, since $E^{(n)}(0) = (n-1)!a_n$, we obtain the assertion. □

Let us now go back again to Hecke operators. Let N be a prime. For a prime p different from N we define the *pth Hecke polynomial of* $S_2(\Gamma_0(N))$ by

$$H_p(u) := \det(\mathrm{id} - T(p)u + p\,\mathrm{id}\,u^2).$$

The connection between the p-modular function fields and Hecke operators is now given by the following fundamental theorem.

(7.4) Theorem. *Let N be a prime number and p be a prime different from N; further let $K = K_0^p(N)$ be the p-modular function field over $\mathbf{F}_p$. Then we have*

$$Z(K;u) = \frac{H_p(u)}{(1-u)(1-qu)};$$

Hence, $L(K;u) = H_p(u)$.

For a proof of this theorem, the reader is referred to [13]. (See also [19] for another type of discussion. Note that the number of prime divisors of degree one of the p-modular function field equals the number of F_p-rational points of a smooth curve corresponding to this field.)

To obtain a formula for the number of prime divisors of degree one of $K_0^p(N)\mathsf{F}_{p^2}$, we have to make some remarks.

Let $d := \dim S_2(\Gamma_0(N))$ and $a_1, \ldots, a_d$ be the eigenvalues of $T(p)$. Further define for $1 \leq i \leq d$ the numbers α_i and α_i' by

$$1 - a_i u + p u^2 = (1 - \alpha_i u)(1 - \alpha_i' u).$$

This implies $\alpha_i \alpha_i' = p$ and $\alpha_i + \alpha_i' = a_i$ for all i. By the definition of $H_p(u)$ we obtain $H_p(u) = \prod_{i=1}^{d}(1 - \alpha_i u)(1 - \alpha_i' u)$. By (7.3) and (7.4) we know that the number of prime divisors of degree one of $K_0^p(N)\mathsf{F}_{p^2}$ is given by $p^2 + 1 - \sum_{i=1}^{d}(\alpha_i^2 + \alpha_i'^2)$. We want to relate the latter summand with traces of Hecke operators.

Clearly, $T(p)^2$ has eigenvalues $a_1^2, \ldots, a_d^2$, hence $\operatorname{tr}(T(p)^2) = \sum_{i=1}^{d} a_i^2$. But $a_i = \alpha_i + \alpha_i'$, thus $a_i^2 = \alpha_i + \alpha_i'^2 + 2p$, since $\alpha_i \alpha_i' = p$. We obtain

$$\sum_{i=1}^{d}(\alpha_i^2 + \alpha_i'^2) = \operatorname{tr}(T(p)^2) - 2pd.$$

Now we have [32]

$$T(p^2) = T(p)^2 - p\,\mathrm{id}\,.$$

This yields

$$\begin{aligned} \operatorname{tr}(T(p^2)) &= \operatorname{tr}(T(p)^2) - pd \\ &= \sum_{i=1}^{d}(\alpha_i^2 + \alpha_i'^2) + pd. \end{aligned}$$

Now noting that $d = \dim S_2(\Gamma_0(N)) = g_0(N)$ by (6.2), we obtain the following.

(7.5) Theorem. *The number of prime divisors of degree one of the p-modular function field $K_0^p(N)\mathsf{F}_{p^2}/\mathsf{F}_{p^2}$ is given by $p^2 + 1 - \operatorname{tr}(T(p^2)) + pg_0(N)$.*

Applying now the formula for the trace of $T(p^2)$ from (6.5), we get our final result.

(7.6) Theorem. *Let N and p be primes, $p \neq N$. The number of prime divisors of degree one of $K_0^p(N)\mathsf{F}_{p^2}$ is given by*

$$\sum_{s,f} \frac{h(D)}{w(D)}\left(1 + \left(\frac{D}{N}\right)\right) + g_0(N)(p-1),$$

where s, f, and D are as in (6.5).

Since the first term in the above formula is bounded as N goes to infinity, we see that the number of prime divisors of degree one of $K_0^p(N)\mathbf{F}_{p^2}$ is almost equal to $g_0(N)(p-1)$ as N becomes large.

7.2 Codes Beyond the Gilbert-Varshamov-Bound

Let p be a fixed prime number. For every prime number N let $K_N := K_0^p(N)\mathbf{F}_{p^2}$ and σ be the sequence of function fields K_N where N runs over the set of prime numbers different from p. Let $n(K_N)+1$ be the number of prime divisors of degree one of $K_N/\mathbf{F}_{p^2}$. By (7.6) $\lim_N g(K_N)/n(K_N) = \frac{1}{p-1}$, which shows that $\gamma_\sigma = 1/(p-1)$. It is easily seen that for $p \geq 7$ we have $\gamma_\sigma < \log_{p^2}(2p^2-1)-1$, hence (4.3) implies the following theorem, see [43].

(7.7) Theorem (TSFASMAN, VLADUT, ZINK). *Let $p \geq 7$. Then there exists a sequence of linear codes over $\mathbf{F}_{p^2}$ which asymptotically lie above the Gilbert-Varshamov-bound.*

Using other techniques, it is possible to prove the above theorem over any field $\mathbf{F}_{p^{2m}}$ where m is any positive integer and $p \geq 7$, see [42].

The function fields considered here are the best possible: one can show that for any sequence σ of function fields over $\mathbf{F}_q$, q a square, such that the number $n(K)+1$ of rational points of K goes to infinity as K runs through the elements of σ, we have that $\gamma_\sigma \geq 1/(\sqrt{q}-1)$, see [42].

CHAPTER 8

An Introduction to the Theory of Bilinear Complexity

8.1 Introduction

In the course of these notes we shall investigate the problem, how many arithmetic operations are necessary to compute a finite set of multivariate polynomials over a field. One can assign different weights to different arithmetic operations; if, for example, large integers are involved in the computation, then it makes more sense to give more weight to the multiplication of these numbers than to the addition. This stems from the fact that the best known algorithms for the multiplication of two numbers having n binary digits require $O(n \log n \log\log n)$ operations [30], whereas addition of two such numbers requires only $O(n)$ arithmetic operations. On the other side, if only computations with small rational numbers are involved, one should assign the same weight to addition and multiplication/division.

Different weightings of arithmetic operations lead usually to different theories. If, e.g., one wants to obtain the minimal number of additions necessary to compute a set of polynomials, one often uses different tools than those necessary for the study of the number of multiplications, say. The situation changes even more if one is interested in both of these numbers at the same time, i.e., if one is interested in the minimum (weighted) number of additions *and* multiplications necessary to compute a set of polynomials.

Before making things more precise, it is useful to clarify the problem we are interested in with the aid of some examples.

(8.1) Example. (*Multiplication of polynomials of degree* 1)

Here we are interested in an algorithm, which, given a pair of polynomials $p = p_1 x + p_0$ and $q = q_1 x + q_0$ over a field K, computes (the coefficients of) their

product $pq =: f = f_2x^2 + f_1x + f_0$ where

$$f_2 = p_1q_1,$$
$$f_1 = p_1q_0 + p_0q_1,$$
$$f_0 = p_0q_0.$$

Furthermore, this algorithm should use the minimum number of arithmetic operations. Since the coefficients of the polynomials p and q are not determined a priori and since the algorithm we are interested in should work for every set of coefficients in K, we can regard the coefficients as further indeterminates over K. Because of notational reasons, we change the variables p_i to x_i and q_i to y_i. The computational problem is now to compute the set of polynomials

$$f_2 = x_1y_1,$$
$$f_1 = x_1y_0 + x_0y_1,$$
$$f_0 = x_0y_0,$$

using the least number of arithmetic operations. •

(8.2) Example. (*Multiplication of complex numbers*)

In this case, the problem is to give an algorithm to compute the product $c_3 = f_1 + if_2$ of two arbitrary complex numbers $c_1 = x_1 + iy_1$ and $c_2 = x_2 + iy_2$. Then

$$f_1 = x_1x_2 - y_1y_2$$
$$f_2 = x_1y_2 + x_2y_1.$$

Again, we can regard the coefficients of c_1 and c_2 as indeterminates over the field $\mathbf{R}$ of real numbers. The computation problem is to give an algorithm to compute the polynomials $f_1, f_2 \in \mathbf{R}[x_1, x_2, y_1, y_2]$, which uses the minimum number of arithmetic operations. •

(8.3) Example. (*Multiplication of* 2×2*-matrices*)

Given two arbitrary 2×2-matrices $X = (x_{ij})$ and $Y = (y_{ij})$ over a field K, compute their product $Z = XY = (z_{ij})$ using the minimum number of arithmetic operations. Applying the rules for matrix multiplication, the problem consists of computing the following set of polynomials over K using the minimum number of arithmetic operations:

$$z_{ij} = x_{i1}y_{1j} + x_{i2}y_{2j}, \quad i,j \in \{1,2\}.$$

•

The problems introduced in the examples above may be stated in the following unified way:

> Let $x_1, \ldots, x_s$ be indeterminates over a field K. Further let $f_1, \ldots, f_m \in K[x_1, \ldots, x_s]$. It is required to give an optimal computation of $f_1, \ldots, f_m$ under the assumption that the elements of $K \cup \{x_1, \ldots, x_s\}$ can be computed without any cost.

8.2 Computation Sequences and Multiplicative Complexity

The problem at the end of the last section cannot be attacked yet, since it is by no means precisely stated. It is, for instance, not clear what is meant by a computation. In this section we shall make the concepts introduced intuitively in the last section more precise.

The following definition will clarify the concept of the "computation of polynomials".

(8.4) Definition. Let $x_1, \ldots, x_s$ be indeterminates over the field K. A sequence $(g_1, \ldots, g_r)$ in $K(x_1, \ldots, x_s)$ is called *a computation sequence of length* r if for all $\rho \leq r$ we have

$$\exists\, u_\rho, v_\rho \in K + \sum_{i \leq s} Kx_i + \sum_{\sigma < \rho} Kg_\sigma : \quad g_\rho = u_\rho v_\rho \text{ or } g_\rho = u_\rho / v_\rho, v_\rho \neq 0.$$

If $f_1, \ldots, f_l$ are polynomials in $K[x_1, \ldots, x_s]$ and $(g_1, \ldots, g_r)$ is a computation sequence such that

$$\{f_1, \ldots, f_l\} \subseteq K + \sum_{i \leq s} Kx_i + \sum_{\rho \leq r} Kg_\rho,$$

then we say that $(g_1, \ldots, g_r)$ *computes* the set $\{f_1, \ldots, f_l\}$ over K. A computation sequence $(g_1, \ldots, g_r)$ is called *division-free* if, with the above notations, each g_ρ is of the form $g_\rho = u_\rho v_\rho$. $\diamond$

The length of a computation sequence is a measure for the cost of this sequence and hence may be used to define the concept of an optimal computation of a set of polynomials. But before going into details, let us say some words about the problem of weighting arithmetic operations in the model of computation induced by (8.4). As is apparent from this definition, a computation sequence $(g_1, \ldots, g_r)$ computes any finite set of polynomials in

$$K + \sum_{i \leq s} Kx_i + \sum_{\rho \leq r} Kg_\rho.$$

This means that scalar multiplications or K-linear combinations of polynomials does not effect the cost of computation of these polynomials in the above model. Only when two nonconstant polynomials in the above set are multiplied or divided, one needs a longer computation sequence. If we denote this type of multiplications/divisions by *essential multiplications/divisions*[1] (as opposed to *scalar multiplications*, i.e., multiplication with elements of K), then the length of a computation sequence equals the number of essential multiplications/divisions in this sequence. The weighting of arithmetic operations is such that essential multiplications/divisions are weighted with 1 and scalar multiplications are weighted with 0, as are additions and subtractions.

[1] In the sequel, we shall denote essential multiplications by $*$.

(8.5) Definition. Let $F := \{f_1, \ldots, f_l\} \subset K[x_1, \ldots, x_s]$. A computation sequence of minimal length for F is called an *optimal computation* for F. The length of an optimal computation for F is called the *(non-scalar) complexity of* F and is denoted by $L_{\{*,/\}}(F)$. The length of an optimal division-free computation sequence for F is called the *multiplicative complexity* of F and is denoted by $L_{\{*\}}(F)$ or merely by $L(F)$. $\diamond$

Note that we have suppressed the dependency of $L_{\{*,/\}}$ and L on the underlying field. See (8.9) for an example.

(8.6) Example. (*Multiplication of polynomials of degree* 1)
We have already seen that computing the product of two polynomials of degree one over K is equivalent to computing the set $F = \{f_0, f_1, f_2\}$ of polynomials in $K[x_0, x_1, y_0, y_1]$ where

$$f_0 = x_0 y_0, \quad f_1 = x_1 y_0 + x_0 y_1, \quad f_2 = x_1 y_1.$$

A possible computation sequence for F is $(g_1, \ldots, g_4)$ where

$$\begin{aligned} g_1 &= x_0 * y_0 = f_0, \\ g_2 &= x_1 * y_0, \\ g_3 &= x_0 * y_1, \\ g_4 &= x_1 * y_1 = f_2. \end{aligned}$$

Since $f_1 = g_2 + g_3$, we have $L(F) \leq 4$. $\bullet$

(8.7) Example. (*Multiplication of complex numbers*)
As we have seen, this problem is equivalent to compute the polynomials

$$f_1 = x_1 x_2 - y_1 y_2, \quad f_2 = x_1 y_2 + x_2 y_1$$

in $\mathbf{R}[x_1, x_2, y_1, y_2]$. A possible computation sequence is $(g_1, \ldots, g_4)$ where

$$\begin{aligned} g_1 &= x_1 * x_2, \\ g_2 &= y_1 * y_2, \\ g_3 &= x_1 * y_2, \\ g_4 &= x_2 * y_1. \end{aligned}$$

Since $f_1 = g_1 - g_2$ and $f_2 = g_3 + g_4$, we have $L(\{f_1, f_2\}) \leq 4$. $\bullet$

(8.8) Example. (*Multiplication of* 2×2*-matrices*)
The problem is to compute the polynomials

$$f_{ij} = x_{i1} y_{1j} + x_{i2} y_{2j}, \quad i, j \in \{1, 2\},$$

in $K[x_{ij}, y_{ij} \mid i, j \in \{1, 2\}]$. A possible computation sequence is given by

$$g_{ijk} := x_{ik} * y_{kj}, \quad i, j, k \in \{1, 2\}.$$

Since $f_{ij} = g_{ij1} + g_{ij2}$, we have $L(f_{ij} \mid i, j \in \{1, 2\}) \leq 8$. $\bullet$

(8.9) Example. Usually, the complexity of a set of polynomials depends heavily on the field K. Consider for instance the polynomial $f := x_1^2 + x_2^2 \in \mathbf{R}[x_1, x_2]$. Let us compute the length $L_{\mathbf{R}}(f)$ of an optimal division-free computation sequence for f over $\mathbf{R}$. We claim that $L_{\mathbf{R}}(f) \geq 2$. Suppose not; then $L_{\mathbf{R}}(f) \leq 1$ and since $f \notin \mathbf{R} + \mathbf{R}x_1 + \mathbf{R}x_2$ we have $L_{\mathbf{R}}(f) = 1$. Hence, there exist $a_i, b_i, c_i \in \mathbf{R}, i = 1, 2, 3$ such that

$$x_1^2 + x_2^2 = (a_1 + b_1x_1 + c_1x_2)(a_2 + b_2x_1 + c_2x_2) + a_3 + b_3x_1 + c_3x_2.$$

Comparing coefficients we get

$$b_1b_2 = c_1c_2 = 1,\ b_1c_2 + c_1b_2 = 0.$$

This implies that $(b_1c_2)^2 + 1 = 0$, which is impossible (over $\mathbf{R}$). Hence $L_{\mathbf{R}}(f) \geq 2$. On the other hand, the computation sequence

$$g_1 := x_1 * x_1, g_2 := x_2 * x_2$$

clearly computes f, i.e., $L_{\mathbf{R}}(f) = 2$. What about $L_{\mathbf{C}}(f)$? Note that over $\mathbf{C}$ we have $f = (x_1 + ix_2)(x_1 - ix_2)$, hence $L_{\mathbf{C}}(f) = 1$. This result may also be extended to any field: If K contains a primitive fourth root of unity, then $L_K(f) = 1$, otherwise $L_K(f) = 2$. •

It may look strange that divisions may help when computing a set of polynomials. The following example shows that this indeed may be the case.

(8.10) Example. Consider the polynomial $f = x^{31}$ over any field K. The following computation sequence of length 7 computes f:

$$g_1 := x * x, \quad g_2 = g_1 * x, \quad g_3 := g_1 * g_2, \quad g_4 := g_3 * g_1,$$
$$g_5 := g_4 * g_4, \quad g_6 := g_5 * g_5, \quad g_7 := g_6 * g_1,$$

since $g_7 = x^{31}$. It can be shown that $L(x^{31}) = 7$. On the other hand, computing x^{32} by squaring x five times and then dividing x^{32} by x gives a computation sequence of length 6 for the computation of x^{31}. The division step thus gives a better computation. •

We may ask how much divisions may help or even, whether there exist classes of polynomials such that for their computation divisions do not help at all?

This question has been answered by STRASSEN [40]. Before stating (a simplified version of) his result, we need a definition.

(8.11) Definition. Let $x_1, \ldots, x_s$ be indeterminates over the field K. A computation sequence $(g_1, \ldots, g_r)$ in $K(x_1, \ldots, x_s)$ is called *quadratic* if

$$\forall i \leq r\ \exists u_i, v_i \in \sum_{i=1}^{s} Kx_i: \qquad g_i = u_iv_i.$$

In this case we shall also write $((u_1, v_1), \ldots, (u_r, v_r))$ for $(g_1, \ldots, g_r)$. ◇

(8.12) Theorem (STRASSEN). *Let K be an infinite field and $F \subseteq K[x_1, \ldots, x_s]$ be a finite set of* quadratic polynomials. *Then there exists a quadratic computation sequence of length $L_{\{*,/\}}(F)$ which computes F. In particular, $L_{\{*,/\}}(F) = L(F)$.*

The reader may verify that the computation sequences given so far for the multiplication of polynomials, multiplication of complex numbers and multiplication of 2×2-matrices, are all quadratic.

We may still ask for simpler algorithms for computing quadratic polynomials. To obtain simpler algorithms, we have to restrict ourselves to a subclass of quadratic polynomials.

(8.13) Definition. Let K be a field and $x_1, \ldots, x_s, y_1, \ldots, y_m$ be indeterminates over K. A polynomial $p \in K[x_1, \ldots, x_s, y_1, \ldots, y_m]$ is called *bilinear (with respect to $\underline{x} := (x_1, \ldots, x_s)$ and $\underline{y} := (y_1, \ldots, y_m)$)* if

$$p(\underline{x}, \underline{y}) = \sum_{i,j} a_{ij} x_i y_j,$$

where $a_{ij} \in K$. $\diamond$

Bilinear polynomials may be computed by simpler computation sequences than quadratic ones.

(8.14) Definition. Let K be a field and $x_1, \ldots, x_s, y_1, \ldots, y_m$ be indeterminates over K. A quadratic computation sequence $((u_1, v_1), \ldots, (u_r, v_r))$ in $K[x_1, \ldots, x_s, y_1, \ldots, y_m]$ is called *bilinear* if for all $i = 1, \ldots, r$ the u_i, resp. v_i are linear homogeneous in $x_1, \ldots, x_s$, resp. $y_1, \ldots, y_m$. $\diamond$

For any finite set F of bilinear polynomials over K there exists a bilinear computation sequence which computes F: there exists by (8.12) a quadratic computation sequence $((U_1, V_1), \ldots, (U_q, V_q))$ for the computation of F. Hence $F \subset \sum_{i=1}^{q} KU_iV_i$. Now let for every $i = 1, \ldots, r$ $U_i = u_i + u_i'$, $V_i = v_i + v_i'$ where u_i, v_i are linear homogeneous in $x_1, \ldots, x_s$ and u_i', v_i' are linear homogeneous in $y_1, \ldots, y_l$. Then, since F is a set of bilinear polynomials, we have $F \subset \sum_{i=1}^{q} Ku_iv_i' + \sum_{i=1}^{q} Ku_i'v_i$. This shows that $((u_1, v_1'), \ldots, (u_q, v_q'), (u_1', v_1), \ldots, (u_q', v_q))$ is a bilinear computation sequence for F. The following definition thus makes sense.

(8.15) Definition. Let F be a finite set of bilinear polynomials over K. The minimum length of a bilinear computation sequence for F is called the *bilinear complexity* (or *rank*) of F and is denoted by $R(F)$. $\diamond$

Clearly, $L(F) \leq R(F)$ for a set F of bilinear polynomials, since bilinear computation sequences form a subset of quadratic computation sequences. But the foregoing argumentation also shows the following.

(8.16) Lemma. *Let F be a finite set of bilinear polynomials over K. Then*

$$L(F) \leq R(F) \leq 2L(F).$$

We finish this section with a couple of examples.

(8.17) Example. (*Multiplication of polynomials of degree* 1)
We want to give an upper estimate for $R = R(f_0, f_1, f_2)$ where

$$f_0 = x_0y_0, \quad f_1 = x_1y_0 + x_0y_1, \quad f_2 = x_1y_1.$$

The trivial algorithm leads to $R \leq 4$, as was shown before (It is easy to check that the trivial algorithm is bilinear). The following bilinear computation sequence shows that $R \leq 3$:

$$\begin{aligned} g_1 &= x_0 * y_0 = f_0, \\ g_2 &= (x_0 + x_1) * (y_0 + y_1), \\ g_3 &= x_1 * y_1 = f_2. \end{aligned}$$

Since $f_1 = g_2 - g_1 - g_3$, the g_i constitute a bilinear computation sequence for $\{f_0, f_1, f_2\}$ of length 3. •

(8.18) Example. (*Multiplication of complex numbers*)
Again, let

$$f_1 = x_1x_2 - y_1y_2, \quad f_2 = x_1y_2 + x_2y_1$$

be the bilinear polynomials corresponding to the multiplication of complex numbers. The bilinear computation sequence

$$\begin{aligned} g_1 &= x_1 * (x_2 + y_2) \\ g_2 &= y_2 * (x_1 + y_1) \\ g_3 &= x_2 * (y_1 - x_1) \end{aligned}$$

computes $\{f_1, f_2\}$, since $f_1 = g_1 - g_2$ and $f_2 = g_1 + g_3$. Hence $R(\{f_1, f_2\}) \leq 3$. •

(8.19) Example. (*Multiplication of* 2×2*-matrices*)
Let again f_{ij} denote the bilinear polynomials corresponding to the multiplication of 2×2-matrices. We have already seen that $R(\{f_{ij} \mid i, j = 1, 2\}) \leq 8$. Consider the following computation sequence:

$$\begin{aligned} g_1 &= (x_{11} + x_{22}) * (y_{11} + y_{22}) & g_2 &= (x_{21} + x_{22}) * y_{11} \\ g_3 &= x_{11} * (y_{12} - y_{22}) & g_4 &= x_{22} * (-y_{11} + y_{21}) \\ g_5 &= (x_{11} + x_{12}) * y_{22} & g_6 &= (-x_{11} + x_{21}) * (y_{11} + y_{12}) \\ g_7 &= (x_{12} - x_{22}) * (y_{21} + y_{22}). \end{aligned}$$

Since

$$f_{11} = g_1 + g_4 - g_5 + g_7 \quad f_{12} = g_3 + g_5$$
$$f_{21} = g_2 + g_4 \quad f_{22} = g_1 - g_2 + g_3 + g_6,$$

this sequence computes f_{ij} over any field (even over any ring!). The corresponding bilinear algorithm is known as STRASSEN's matrix multiplication algorithm [41]. The major point of this algorithm is that it is valid over any ring. Hence one may interpret x_{ij} and y_{ij} as matrices over a field K and use the algorithm recursively. This gives an algorithm for multiplying $n \times n$-matrices which uses asymptotically $O(n^{\log_2 7}) = O(n^{2.80735\ldots})$ multiplications (which is better than the naive algorithm which needs $O(n^3)$ multiplications). •

In the examples above we have only given upper bounds for the bilinear complexities of the corresponding bilinear polynomials. The major problem is now to give good or even matching lower bounds for these quantities. This will be done in the next sections.

8.3 Rank of Bilinear Mappings

Bilinear polynomials in $(s+l)$ indeterminates over a field K can be viewed as bilinear forms of the vector space $K^s \times K^l$. Indeed, if

$$p(x_1, \ldots, x_s, y_1, \ldots, y_l) = \sum_{i,j} a_{ij} x_i y_j$$

is a bilinear polynomial over K, then for the pair $(e_1, \ldots, e_s)$ and $(e'_1, \ldots, e'_l)$ of natural bases of K^s, resp. K^l, p induces a bilinear form ϕ_p defined by $\phi_p(e_i, e'_j) := a_{ij}$. Analogously, linear homogeneous polynomials in m indeterminates may be viewed as linear forms of K^m.

A sequence $(z_1, \ldots, z_n)$ of bilinear polynomials (with respect to $x_1, \ldots, x_s$ and $y_1, \ldots, y_l$) over K induces a bilinear mapping of $\Phi: K^s \times K^l \to K^n$ by requiring that the kth coordinate of Φ be equal to the bilinear form induced by z_k. In this way, bilinear polynomials induce bilinear mappings. It is also possible to speak about bilinear algorithms for bilinear mappings. The next definition makes this concept precise.

(8.20) Definition. Let U, V, and W be finite dimensional vector spaces over the field K and $\Phi: U \times V \to W$ be a bilinear mapping. Denote by U^*, resp. V^*, the dual spaces of U, resp. V. The *bilinear complexity* or *rank* $R(\Phi)$ of Φ is the minimal number r such that there exist $u_1, \ldots, u_r \in U^*$, $v_1, \ldots, v_r \in V^*$, and $w_1, \ldots, w_r \in W$, satisfying

$$\forall x \in U, y \in V: \quad \Phi(x, y) = \sum_{i=1}^{r} u_i(x) v_i(y) w_i.$$

◇

The proof of many results on the rank of bilinear mappings become more transparent if one uses the terminology of tensors and tensor product.

(8.21) Definition. A tensor product $(U \otimes V, \tau)$ of U and V consists of a vector space $U \otimes V$ over K and a bilinear map $\tau: U \times V \to U \otimes V$ such that

(1) The K-span of the image of τ equals $U \otimes V$,

(2) (Universal mapping property) For every vector space W and every bilinear map $\Phi: U \times V \to W$ there exists a linear map $\phi: U \otimes V \to W$ such that $\Phi = \phi\tau$.

◇

While the uniqueness of the tensor product (up to isomorphism) follows directly from the definition, the proof of the existence involves a certain construction which can be read in any book on multilinear algebra or algebra (see, e.g., [21]). It can be proved easily that the tensor product is associative, i.e.,

$$(U \otimes V) \otimes W \simeq U \otimes (V \otimes W) \simeq: U \otimes V \otimes W.$$

for K-spaces U, V, and W.

The connection between the K-space $\mathrm{Bil}(U \times V, W)$ and tensor products is given by the following isomorphism.

(8.22) Lemma. $\mathrm{Bil}(U \times V, W) \simeq U^* \otimes V^* \otimes W$, *where* U^* *and* V^* *denote the dual spaces of* U *and* V.

PROOF. (Sketch) It can be proved that the homomorphism $h: U^* \otimes V^* \otimes W \to \mathrm{Bil}(U \times V, W)$ defined by $u^* \otimes v^* \otimes w \mapsto ((a,b) \mapsto u^*(a)v^*(b)w)$ is an isomorphism [21]. □

To $\Phi \in \mathrm{Bil}(U \times V, W)$ corresponds a unique tensor $t \in U^* \otimes V^* \otimes W$ according to (8.22). Further, if $\Phi(a,b) = \sum_{\rho \le r} u_\rho(a)v_\rho(b)w_\rho$ for all $(a,b) \in U \times V$, we have in view of the above isomorphism $t = \sum_{\rho \le r} u_\rho \otimes v_\rho \otimes w_\rho$. If we call an element $u \otimes v \otimes w \in U^* \otimes V^* \otimes W$ a *triad*, we obtain that the rank of a bilinear mapping Φ is the minimum number r such that the tensor corresponding to Φ can be represented as a sum of r triads. One can thus also speak of the *rank* of a tensor in $U^* \otimes V^* \otimes W$ defined as the rank of the associated bilinear map. The rank of the bilinear mapping Φ is sometimes also called the *tensor rank* of Φ. In the sequel we shall make frequent implicit use of the above isomorphism and mix up tensors and bilinear mappings.

(8.23) Example. Here we want to show that the rank of a bilinear mapping is a generalization of the concept of the rank of a linear map. Let U and V be K-spaces. If $\phi \in \mathrm{Bil}(U \times V, K)$, then for $a \in U$ the mapping ϕ_a which assigns to $b \in V$ the value $\phi_a(b) := \phi(a,b)$ is a linear form on V, i.e., $\phi_a \in V^*$. Then

$\mathrm{Bil}(U \times V, K) \simeq \mathrm{Hom}(U, V^*)$ under the isomorphism $\phi \mapsto (h_\phi\colon a \mapsto \phi_a)$. We claim that $R(\phi) = \mathrm{rk}(h_\phi)$.

Suppose that $\phi = \sum_{\rho \le r} u_\rho \otimes v_\rho$, where $u_\rho \in U^*$, and $v_\rho \in V^*$ (we may suppose that all the $w_\rho = 1$ and $r = R(\phi)$). Then for any $a \in U$ we have

$$h_\phi(a) = \phi_a \in \sum_{\rho \le r} u_\rho(a) v_\rho,$$

hence $\mathrm{rk}(h_\phi) \le r$.

On the other hand, let $\mathrm{rk}(h_\phi) = r$ and $v_1, \ldots, v_r$ be a basis of the image of h_ϕ. Then, for any $a \in U$ there exist $u_1(a), \ldots, u_r(a) \in K$ such that $h_\phi(a) = \sum_{\rho \le r} u_\rho(a) v_\rho$. For the linear forms u_ρ thus defined we obtain: $\phi = \sum_{\rho \le r} u_\rho \otimes v_\rho$, which shows that $R(\phi) \le \mathrm{rk}(h_\phi)$. •

In the rest of this section we shall develop a simple but powerful tool for proving lower or upper bounds for the bilinear complexity of a bilinear mapping, by reducing it to the bilinear complexity of some other bilinear mapping. We have first to recall some basic facts.

Suppose that U_i, V_i, $i = 1, 2$, are finite dimensional K-spaces and $f \in \mathrm{Hom}(U_1, U_2)$, $g \in \mathrm{Hom}(V_1, V_2)$. Let $(U_i \otimes V_i, \tau_i)$, $i = 1, 2$ be the tensor product of U_i and V_i. Then $\tau_2(f \times g)$ is a bilinear mapping from $U_1 \times V_1$ to $U_2 \otimes V_2$, hence there exists a unique homomorphism h from $U_1 \otimes V_1$ to $U_2 \otimes V_2$ such that $h(u_1 \otimes v_1) = f(u_1) \otimes g(v_1)$. We denote this homomorphism by $f \otimes g$.

We recall a definition. Let U and V be K-spaces and $\varphi \in \mathrm{Hom}(U, V)$. Then $\varphi^*\colon V^* \to U^*$ defined by $\varphi^*(\lambda) := \lambda\varphi$ is a homomorphism.

(8.24) Lemma. *Let U_i, V_i, W_i, $i = 1, 2$, be finite dimensional K-spaces and $\phi \in U_1^* \otimes V_1^* \otimes W_1$. Suppose that $\varphi^* \in \mathrm{Hom}(U_1^*, U_2^*)$, $\psi^* \in \mathrm{Hom}(V_1^*, V_2^*)$, and $\eta \in \mathrm{Hom}(W_1, W_2)$. Then $R((\varphi^* \otimes \psi^* \otimes \eta)(\phi)) \le R(\phi)$.*

PROOF. Let $\phi = \sum_{\rho \le r} u_\rho \otimes v_\rho \otimes w_\rho$, where $r = R(\phi)$, $u_\rho \in U_1^*$, $v_\rho \in V_1^*$, and $w_\rho \in W_1^*$. Then $(\varphi^* \otimes \psi^* \otimes \eta)(\phi) = \sum_{\rho \le r} \varphi^*(u_\rho) \otimes \psi^*(v_\rho) \otimes \eta(w_\rho)$, which proves the assertion. □

The following lemma shows how this reduction technique can be used.

(8.25) Lemma. *Let U_i, V_i, W_i, $i = 1, 2$, be finite dimensional K-spaces and $\phi_i \in \mathrm{Bil}(U_i \times V_i, W_i)$, $i = 1, 2$. Further let $\varphi \in \mathrm{Hom}(U_1, U_2)$, $\psi \in \mathrm{Hom}(V_1, V_2)$, and $\eta \in \mathrm{Hom}(W_1, W_2)$ be such that the following diagram commutes:*

$$\begin{array}{ccccc} U_1 & \times & V_1 & \xrightarrow{\phi_1} & W_1 \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\eta} \\ U_2 & \times & V_2 & \xrightarrow{\phi_2} & W_2 \end{array}.$$

Then we have:

(1) *If φ and ψ are surjective, then $R(\phi_2) \leq R(\phi_1)$.*

(2) *If η is injective, then $R(\phi_1) \leq R(\phi_2)$.*

PROOF. The condition that the above diagram commutes translates to

$$(\mathrm{id} \otimes \mathrm{id} \otimes \eta)(\phi_1) = (\varphi^* \otimes \psi^* \otimes \mathrm{id})(\phi_2). \tag{8.26}$$

(1) The surjectivity of φ and ψ implies that there exist $\varphi^{-1} \in \mathrm{Hom}(U_2, U_1)$, $\psi^{-1} \in \mathrm{Hom}(V_2, V_1)$ such that $\varphi\varphi^{-1} = \mathrm{id}_{U_2}$ and $\psi\psi^{-1} = \mathrm{id}_{V_2}$. Application of $((\varphi^{-1})^* \otimes (\psi^{-1})^* \otimes \mathrm{id})$ to (8.26) yields

$$((\varphi^{-1})^* \otimes (\psi^{-1})^* \otimes \eta)(\phi_1) = \phi_2.$$

Now (8.24) implies that $R(\phi_2) \leq R(\phi_1)$.

(2) The injectivity of η implies that there exists $\eta^{-1} \in \mathrm{Hom}(W_2, W_1)$ such that $\eta^{-1}\eta = \mathrm{id}_{W_1}$. Application of $(\mathrm{id} \otimes \mathrm{id} \otimes \eta^{-1})$ to (8.26) yields

$$\phi_1 = (\varphi^* \otimes \psi^* \otimes \eta^{-1})(\phi_2).$$

Hence (8.24) implies that $R(\phi_1) \leq R(\phi_2)$. □

We shall use the above methods in the next chapter.

8.4 Concise bilinear mappings

For the construction of linear codes from bilinear algorithms it is important that the underlying bilinear form is in some sense "nondegenerate". The precise meaning of this is given by the following. As usual, U, V, and W denote finite dimensional vector spaces over a field K.

(8.27) Definition. Let $\Phi \in \mathrm{Bil}(U \times V; W)$. Then

(1) Φ is called 1-*concise* if $\{u \in U \mid \Phi(u, V) = 0\} = \{0\}$.

(2) Φ is called 2-*concise* if $\{v \in V \mid \Phi(U, v) = 0\} = \{0\}$.

(3) Φ is called 3-*concise* if $\langle \Phi(U, V) \rangle = W$.

(4) Φ is called *concise* if Φ is i-concise for $i = 1, 2, 3$.

◇

For studying the bilinear complexity of a bilinear mapping Φ, it is not a restriction of generality if we assume that Φ is concise. This is the content of the following simple lemma the proof of which is left to the reader.

(8.28) Lemma. *For* $\Phi \in \mathrm{Bil}(U \times V; W)$ *let* $U' := \{u \in U \mid \Phi(u, V) = 0\}$, $V' := \{v \in V \mid \Phi(U, v) = 0\}$, *and* $W' := \langle \Phi(U, V) \rangle$. *Then*

$$\begin{aligned} \Phi' \colon\ U/U' \times V/V' &\to W' \\ (u + U', v + V') &\mapsto \Phi(u, v) \end{aligned}$$

is a well defined concise bilinear mapping and $R(\Phi') = R(\Phi)$.

In the sequel we shall make use of the following fact.

(8.29) Remark. Let $\phi \in \mathrm{Bil}(U \times V; W)$ and suppose that ϕ has a representation of the form $\phi = \sum_{\rho \le r} u_\rho \otimes v_\rho \otimes w_\rho$. Then we have:

(1) If ϕ is 1-concise, then $\langle u_1, \ldots, u_r \rangle = U^*$.

(2) If ϕ is 2-concise, then $\langle v_1, \ldots, v_r \rangle = V^*$.

(3) If ϕ is 3-concise, then $\langle w_1, \ldots, w_r \rangle = W$.

In particular, if ϕ is concise, then $R(\phi) \ge \max\{\dim U, \dim V, \dim W\}$. •

8.5 Lower Bounds for some Computational Problems

As was said before, the aim of (algebraic) complexity theory is to give in some way the minimum number of operations necessary to compute (algebraic) quantities. Hence, one tries to make assertions about *all possible* algorithms for the problem to solve.

To determine the exact minimum number of operations necessary to compute an algebraic problem, one has—in some way—to estimate from below this number and at the same time to find a *matching upper bound*, i.e., to give an algorithm (or prove the existence of an algorithm) which uses this number of arithmetic operations. So the problem is divided into two parts: Proving *lower bounds* and finding (matching) *upper bounds*. The second problem is usually connected to the design of algorithms and is generally considered to be easier than the first, for which only a few general techniques are known. Proving (nontrivial) lower bounds for algebraic computation problems is one of the most challenging topics in complexity theory.

Below we shall discuss some bilinear problems and give nontrivial lower bounds for their bilinear complexity. Since we have not developed the tools for proving most of these bounds, we shall content ourselves to the proofs of the most simple lower bounds.

Let K be a field and D be a finite dimensional division algebra over K. We consider the bilinear mapping $\mu \colon D \times D \to D$ defined by $\mu(a, b) := ab$, i.e., we consider the multiplication in D, where D is regarded as a vector space over K.

(8.30) Definition. The multiplicative complexity, resp. rank of the bilinear mapping μ as above is called the *multiplicative complexity, resp. rank of* D/K and is denoted by $L(D/K)$, resp. $R(D/K)$ or merely $L(D)$, resp. $R(D)$ if K is clear from the context. $\diamond$

We identify μ with the tensor in $D^* \otimes D^* \otimes D$ under the isomorphism given in (8.22). Suppose that there exists a bilinear algorithm of length r for μ. We can thus represent μ as a sum of r triads:

$$\mu = \sum_{i=1}^{r} u_i \otimes v_i \otimes w_i,$$

where $u_i, v_i \in D^*$ and $w_i \in D$. Let x be a nonzero element of K. Then

$$\mu(x, D) = xD \subseteq \sum_{i=1}^{r} u_i(x) v_i(D) w_i.$$

Denote the dimension of D over K by n. There exists a nonzero x in L such that $u_1(x) = \cdots = u_{n-1}(x) = 0$ (why?). For this x we have $xD \subseteq \sum_{i=n}^{r} u_i(x) v_i(D) w_i \subseteq \sum_{i=n}^{r} K w_i$. Since D is a division algebra and x is nonzero, $xD = D$ and hence the K-dimension of xD is n. We see that $r - n + 1 \geq n$, hence $r \geq 2n - 1$. We have thus proved the following:

(8.31) Theorem. *Let K be a field and D be a division algebra of degree n of K. Then we have $R(D/K) \geq 2n - 1$.*

We remark without proof that even $L(D/K) \geq 2n - 1$. The proof of this assertion is more complicated than that of (8.31).

What is $R(D/K)$ for a finite dimensional division algebra D over K? Let us first discuss the case where D is a simple field extension of K. The question of upper bounds for the rank $R(D/K)$ is very much related to the rank of polynomial multiplication. To be more precise, for a natural number l let $K[x]_l$ denote the K-space of polynomials of degree less than l over K. Let $\Phi_K^{l,m} \in \mathrm{Bil}(K[x]_l \times K[x]_m, K[x]_{l+m-1})$ be the polynomial multiplication map. Then $R(D/K)$ is related to $R(\Phi_K^{n,n})$. This is the context of the following lemmas.

(8.32) Lemma. *Let D be a simple field extension of degree n of the field K. Then $R(D/K) \leq R(\Phi_K^{n,n})$.*

PROOF. Let $p(x)$ be a monic irreducible polynomial of degree n over K such that $D \simeq K[x]/(p(x))$ and κ be the residue class mapping $K[x] \to K[x]/(p(x)) \simeq D$. We

obtain the following commutative diagram

$$\begin{array}{ccccc} K[x]_n & \times & K[x]_n & \xrightarrow{\Phi_K^{n,n}} & K[x]_{2n-1} \\ \downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_2} \\ D & \times & D & \xrightarrow{\nu} & D \end{array}$$

where ν is the multiplication in D, κ_1 is the restriction of κ to $K[x]_n$, and κ_2 is the restriction of κ to $K[x]_{2n-1}$. Since κ_1 is surjective, (8.25)(1) implies that $R(D/K) = R(\nu) \leq R(\Phi_K^{n,n})$. □

(8.33) Lemma. *Let l and m be positive integers and K be a field such that $|K| \geq l + m - 2$. Then $R(\Phi_K^{l,m}) \leq l + m - 1$.*

PROOF. Let $\alpha_1, \ldots, \alpha_{l+m-2}$ be pairwise different elements of K. For $k \geq 1$ we define $\gamma_k : K[x]_k \to K^{l+m-1}$ by $\gamma_k(f) := (f(\alpha_1), \ldots, f(\alpha_{l+m-2}), f(\infty))$, where $f(\infty)$ stands for the coefficient of x^{k-1} of f. It is clear that γ_k is injective if and only if $k \leq l + m - 1$ and surjective if and only if $k \geq l + m - 1$. Now consider the following commutative diagram

$$\begin{array}{ccccc} K[x]_l & \times & K[x]_m & \xrightarrow{\Phi_K^{l,m}} & K[x]_{l+m-1} \\ \downarrow{\scriptstyle \gamma_l} & & \downarrow{\scriptstyle \gamma_m} & & \downarrow{\scriptstyle \gamma_{l+m-1}} \\ K^{l+m-1} & \times & K^{l+m-1} & \xrightarrow{\mu} & K^{l+m-1} \end{array}$$

where μ is component-wise multiplication. Since γ_{l+m-1} is bijective,we obtain $R(\Phi_K^{l,m}) \leq R(\mu) \leq l + m - 1$ by (8.25)(2). □

As a corollary we obtain from (8.31), (8.32), and (8.33) the following.

(8.34) Corollary. *Let D be a simple field extension of K of degree n and $|K| \geq 2n - 2$. Then $R(D/K) = 2n - 1$.*

Applying this corollary to the case $K = \mathbf{R}$ and $D = \mathbf{C}$, we see that the bilinear algorithm for multiplication of complex numbers introduced in (8.18) is optimal (in the sense of bilinear complexity) and that $R(\mathbf{C}/\mathbf{R}) = 3$. Also, application of (8.33) to the multiplication of polynomials of degree less or equal to one shows that the bilinear computation introduced in (8.17) is optimal and that $R(\Phi_K^{2,2}) = 3$ for any field K.

The reader can consult the exercises for further relations between polynomial multiplication and the rank of simple field extensions.

Now the question arises what happens when $|K| < 2n - 2$. One result is the following [11, 44]

(8.35) Theorem. *If $|K| < 2n-2$, and D is a simple field extension of K of degree n, then $R(D/K) > 2n-1$.*

In the next chapters we shall make more accurate assertions about $R(D/K)$ in the case of small finite fields with the aid of algebraic curves. There exist also assertions about the bilinear complexity of non-simple field extensions and skew fields over given fields. The interested reader may consult the forthcoming book [8] on these subjects.

The leading problem of bilinear complexity is that of matrix multiplication. Here one wants to compute the rank of the bilinear mapping which assigns to a pair of square matrices their product. More precisely, if n is a positive integer, we define $L(K^{n\times n})$, resp. $R(K^{n\times n})$ as the multiplicative complexity, resp. rank of the multiplication map in $K^{n\times n}$. Concerning lower bounds for $R(K^{n\times n})$ we have the following.

(8.36) Theorem. *For any field K we have $R(K^{n\times n}) \geq 2n^2 - 1$.*

PROOF. The following proof has been taken from [3]. During this proof we denote by A the ring $K^{n\times n}$. We shall need the following facts about A.

(i) Any minimal left (right) ideal of A has K-dimension n.

(ii) Any maximal left (right) ideal of A has K-dimension $n^2 - n$.

(iii) No right ideal $R \neq 0$ of A is contained in a left ideal $L \neq A$ of A.

The proofs of these assertions are left as an exercise.

Suppose that $r := R(K^{n\times n}) < 2n^2 - 1$. For $\rho = 1, \ldots, r$, let $u_\rho, v_\rho \in A^*$, and $w_\rho \in A$ be such that

$$\forall\, a, b \in A: \quad ab = \sum_{\rho=1}^{r} u_\rho(a) v_\rho(b) w_\rho. \tag{8.37}$$

Observe first that $\sum_{\rho=1}^{r} K u_\rho = A^*$ since the multiplication map is concise, see Remark (8.29) We may assume w.l.o.g. that $u_1, \ldots, u_{n^2}$ are linearly independent (note that A has dimension n^2 over K). Since $r < 2n^2 - 1$, $\sum_{\rho=n^2}^{r} K v_\rho \neq A^*$. Hence, there exists $0 \neq b \in A$ such that $v_{n^2}(b) = \cdots = v_r(b) = 0$. By (8.37) we have then $Ab \subseteq \sum_{\rho=1}^{n^2-1} K w_\rho$. Thus, Ab is a proper left ideal of A, hence it is contained in a maximal left ideal L of A. Again by the conciseness of the multiplication map, $v_1, \ldots, v_r$ generate A^*, hence we may assume that $v_n, \ldots, v_{n^2-1}$ are linearly independent over L, since L has K-dimension $n^2 - n$ by (ii) (note that after this choice, $u_1, \ldots, u_{n^2}$ need not be linearly independent anymore, but we don't need this in the sequel). This implies that for any $y \in A$ there exists $c \in L$ such that

$$v_n(c) = v_n(y), \ldots, v_r(c) = v_r(y).$$

Since $r < 2n^2 - 1$, there exists $0 \neq a \in A$ such that $u_{n^2}(a) = \cdots = u_r(a) = 0$. Hence, (8.37) implies

$$\forall y \in A \; \exists c \in L: \quad ay - ac = a(y - c) \in \sum_{\rho=1}^{n-1} K w_\rho \subseteq L.$$

Thus we have $ay \in L$ for all $y \in A$, hence $aA \subseteq L$, a contradiction to (iii). □

BROCKETT and DOBKIN [5] as well as LAFON and WINOGRAD[20] have proved that even $L(K^{n\times n}) \geq 2n^2 - 1$ over any field K. Their proof is beyond the scope of these notes.

Applying (8.36) to the case $n = 2$, we get $R(K^{2\times 2}) \geq 7$. On the other hand, STRASSEN's algorithm introduced in (8.19) implies $R(K^{2\times 2}) \leq 7$ which shows that $R(K^{2\times 2}) = 7$ and that STRASSEN's algorithm for multiplication of 2×2-matrices is optimal. In Section 9.2 we shall see that the bound in (8.36) is not sharp (at least for $K = \mathbf{F}_2$).

The *asymptotic* bilinear complexity of matrix multiplication is characterized by the so called *exponent of matrix multiplication*, usually denoted by ω_K, which is defined as

$$\omega_K := \inf\{\gamma \mid R(K^{n\times n}) = O(n^\gamma)\}.$$

Note that by (8.16) we have $R(K^{n\times n}) \geq L(K^{n\times n}) \geq R(K^{n\times n})/2$, hence $R(K^{n\times n})$ and $L(K^{n\times n})$ are asymptotically equal. It is known that ω_K at most depends on the characteristic of K [12].

Although the model of bilinear complexity neglects operations in the field of scalars, one can show that the number of all arithmetic operations for multiplication of $n \times n$-matrices is of the same order of magnitude as $R(K^{n\times n})$, i.e., if we denote by $M_K(n)$ the minimum number of arithmetic operations necessary to multiply two $n \times n$-matrices over K, then $M_K(n) = O(R(K^{n\times n}))$ (see for instance [12, p. 57–58]). Hence $\omega_K = \inf\{\gamma \mid M_K(n) = O(n^\gamma)\}$.

The trivial algorithm for multiplying matrices implies $\omega_K \leq 3$ over any field K. Recursion of STRASSEN's algorithm for 2×2-matrix multiplication shows that $\omega_K \leq \log_2 7$ for any field. The present world record for ω_K is held by COPPERSMITH and WINOGRAD [10] who have shown that $\omega_K \leq 2.38$ over any field K; (8.36) implies that $\omega_K \geq 2$ over any field K.

The complexity of many problems in linear algebra, like inversion of non-singular matrices or solving systems of linear equations is directly related to the complexity of matrix multiplication. Knowing the latter is therefore of fundamental interest.

We can now generalize the problems introduced in this section in the following way: let K be a field and A be a finite dimensional associative algebra over K, i.e., A is a finite dimensional vector space over K endowed with a multiplication which is bilinear and associative. We consider the bilinear map from $A \times A$ to A which

assigns to every pair of elements in A their product, and ask for the multiplicative complexity $L(A/K)$ or the rank $R(A/K)$ of this bilinear map. (We may also write $L(A)$ or $R(A)$ if K is known from the context.) We mention without proof a general lower bound due to ALDER and STRASSEN [2]:

(8.38) Theorem (ALDER-STRASSEN). *Let A be a finite dimensional associative algebra over K. Then*

$$L(A/K) \geq 2\dim_K(A) - t,$$

where t is the number of maximal two-sided ideals of A.

The proof of this theorem is beyond the scope of these notes. Let us apply (8.38) to the problems stated before: If A is a division algebra of dimension n over K, then the only maximal two-sided ideal of A is the zero ideal, hence $L(A/K) \geq 2n - 1$, in accordance with (8.31).

Let A be the ring of $n \times n$-matrices over K. It is an easy exercise to prove that the only maximal two-sided ideal of A is the zero ideal. Since the dimension of A over K is n^2, we obtain $L(K^{n\times n}/K) \geq 2n^2 - 1$.

Another application of (8.38) is as follows:

Let G be a finite group. The group ring $\mathbf{C}[G]$ of G is defined to be the ring of all complex valued functions on G. For all elements $\sigma \in G$ we identify σ with the characteristic function of $\{\sigma\}$. Then it is clear that every element $f \in \mathbf{C}[G]$ has a unique representation as $f = \sum_{\sigma\in G} a_\sigma \sigma$ where $a_\sigma \in \mathbf{C}$. Extending the multiplication of G by linearity, $\mathbf{C}[G]$ becomes a $\mathbf{C}$-algebra of dimension $|G|$, where $|G|$ denotes the number of elements in G. By Wedderburn's theorem, the number of maximal two-sided ideals of $\mathbf{C}[G]$ equals the number $h(G)$ of conjugacy classes of G, hence, $L(\mathbf{C}[G]/\mathbf{C}) \geq 2|G| - h(G)$.

In the next chapter we shall see how coding theory can be used to obtain lower bounds for the rank of bilinear maps over finite fields.

Acknowledgement. The content of this chapter was presented by the second author during the 12th school of Algebra of the Brazilian Mathemtical Organization. We acknowledge the remarks of an anonymous referee of an expository article based on these talks (submitted by the second author to *matematmatica contemporanea*) which improved the presentation of this chapter.

8.6 Exercises

8.1. Suppose that l and m are positive integers, K is a field and D is a simple field extension of K of dimension at least $l + m - 1$. Prove that $R(\Phi_K^{l,m}) \leq R(D/K)$.

8.2. Let $U' \leq U$, $V' \leq V$, and W be finite dimensional K-spaces and $\Phi \in \mathrm{Bil}(U \times V; W)$. Further let Φ' be the restriction of Φ to $U' \times V'$. Show that $R(\Phi') \leq R(\Phi)$.

8.3. Prove Lemma (8.28).

CHAPTER 9

Bilinear Complexity and Codes

The relation between the bilinear complexity of bilinear mappings over finite fields and the theory of linear codes was first observed by BROCKETT and DOBKIN [5]. The general procedure is as follows: one can assign to any bilinear computation of length r for a bilinear mapping Φ a linear code of block length r with dimension k and minimum distance d, where k and d depend only on Φ (and not on the specific algorithm considered). A lower bound for r is then given by the smallest number n such that there exists an $[n,k,d]$-code over $\mathbf{F}_q$, i.e., by a $N_q[k,d]$ (see Section 1.5).

9.1 Bilinear Complexity and Codes

From now on we only consider bilinear mappings over finite fields. The main theorem of this chapter is given by the following.

(9.1) Theorem. *Let U, V, and W be finite dimensional $\mathbf{F}_q$-spaces, $\Phi \in \mathrm{Bil}(U \times V; W)$ be 1-concise, and $\delta := \min\{\dim \Phi(a,V) \mid 0 \neq a \in U\}$. Further let $\Phi = \sum_{\rho \leq r} u_\rho \otimes v_\rho \otimes w_\rho$, where $u_\rho \in U^*$, $v_\rho \in V^*$, and $w_\rho \in W$ for $1 \leq \rho \leq r$. Then*

$$\begin{array}{rccl} \gamma\colon & U & \to & \mathbf{F}_q^r \\ & a & \mapsto & (u_1(a), \ldots, u_r(a)), \end{array}$$

is a homomorphism and its image is an $[r, \dim U, d]$-code over $\mathbf{F}_q$ where $d \geq \delta$. Thus $R(\Phi) \geq N_q[\dim U, \delta]$.

PROOF. γ certainly is a vector space homomorphism, since the u_ρ are linear forms. Hence the image of γ is a linear code C. Now if $a \in \ker \gamma$, then

$$\Phi(a,V) = \sum_{\rho \leq r} \underbrace{u_\rho(a)}_{=0} v_\rho(V) w_\rho = 0,$$

hence $a = 0$ by the assumption of the 1-conciseness of Φ and thus γ is injective. The dimension of C is therefore equal to $\dim U$. For any $a \in U$ we have

$$\Phi(a, V) \subseteq \sum_{\rho, u_\rho(a) \neq 0} \mathsf{F}_q w_\rho,$$

hence we deduce that $\dim \Phi(a, V) \leq |\{\rho \mid u_\rho(a) \neq 0\}| = \operatorname{wgt}(\gamma(a))$, which shows that the minimum distance d of C satisfies $d \geq \delta$. Hence $r \geq N_q[k, d] \geq N_q[k, \delta]$, since N_q is an increasing function of the second variable by (1.15). □

One can also formulate other versions of this theorem where U is replaced by V or W, and prove them in an analogous way. We leave this as an exercise to the reader.

9.2 A Lower Bound for Matrix Multiplication

As we have already seen, $R(K^{n\times n}) \geq 2n^2 - 1$ by (8.36). The only n for which this bound is known to be sharp is $n = 2$ (over an arbitrary field). In this section we discuss an idea of BSHOUTY [7] to show that for $K = \mathsf{F}_2$ and $n \geq 5$ the bound $2n^2 - 1$ is not sharp. It is based on the following simple result.

(9.2) Lemma. $R(\mathsf{F}_q^{n\times n}) \geq N_q[n, n^2]$.

PROOF. By considering the regular representation we can embed F_{q^n} into $\mathsf{F}_q^{n\times n}$: let $x_1, \ldots, x_n$ be a basis of $\mathsf{F}_{q^n}/\mathsf{F}_q$. For every $\alpha \in \mathsf{F}_{q^n}$ there exists $A_\alpha \in \mathsf{F}_q^{n\times n}$ such that $(\alpha x_1, \ldots, \alpha x_n) = (x_1, \ldots, x_n)A_\alpha$. The mapping ρ: $\mathsf{F}_{q^n} \to \mathsf{F}_q^{n\times n}$, $\alpha \to A_\alpha$ is a ring monomorphism, and $\rho(\mathsf{F}_{q^n}^\times) \subseteq \mathrm{GL}_n(\mathsf{F}_q)$.

Now let Φ be the restriction of the multiplication in $\mathsf{F}_q^{n\times n}$ to $\mathsf{F}_{q^n} \times \mathsf{F}_q^{n\times n}$. Clearly, $R(\mathsf{F}_q^{n\times n}) \geq R(\Phi)$ by Exercise 8.2. Now for any nonzero $\alpha \in \mathsf{F}_{q^n}$ the dimension of $\Phi(\alpha, \mathsf{F}_q^{n\times n}) = \alpha \cdot \mathsf{F}_q^{n\times n}$ is n^2, since α is invertible. Hence, (9.1) implies that $R(\Phi) \geq N_q[n, n^2]$. □

Now let us assume that $q = 2$.

(9.3) Lemma. *We have* $\sum_{i=0}^{n-1} \lceil n^2/2^i \rceil \geq 2n^2 + n - 2 - \lceil 2\log_2 n \rceil$.

PROOF. Let $m := \lceil 2\log_2 n \rceil$. Then $2^{m-1} < n^2 \leq 2^m$ and

$$\begin{aligned}
\sum_{i=0}^{n-1} \left\lceil \frac{n^2}{2^i} \right\rceil &\geq \sum_{i=0}^{m} \frac{n^2}{2^i} + (n - 1 - m) \\
&= 2n^2 - \frac{n^2}{2^m} + (n - 1 - m) \\
&\geq 2n^2 + n - 2 - m \\
&= 2n^2 + n - 2 - \lceil 2\log_2 m \rceil. \quad \square
\end{aligned}$$

As a simple consequence we obtain

(9.4) Corollary. *We have* $R(\mathbf{F}_2^{n\times n}) \geq 2n^2 + n - 2 - \lceil 2\log_2 m\rceil$. *Especially,* $R(\mathbf{F}_2^{n\times n}) > 2n^2 - 1$ *for* $n \geq 5$.

PROOF. By the Griesmer bound (1.16), $N_2[n, n^2] \geq g(n) := \sum_{i=0}^{n-1}\lceil n^2/2^i\rceil$. For $n \geq 7$ we clearly have $2n^2+n-2-\lceil 2\log_2 n\rceil > 2n^2-1$. Further, $g(5) = 51 > 2\cdot 25-1$ and $g(6) = 73 > 2\cdot 36 - 1$, hence $g(n) > 2n^2 - 1$ for $n \geq 5$. Now (9.2) yields the result. □

Combining this result with a projection technique, BSHOUTY has shown that $R(\mathbf{F}_2^{n\times n}) \geq 2\frac{1}{2}n^2 + o(n^2)$ for large n, see [7].

9.3 A Lower Bound for Polynomial Multiplication

We have already discussed the bilinear complexity of the polynomial multiplication map $\Phi_K^{l,m}$ in Section 8.5. We saw in (8.33) that $R(\Phi_K^{l,m}) = l + m - 1$ if K has at least $l + m - 2$ elements. In this section we shall show how to obtain lower bounds for this rank if K is a small finite field, using the theory of linear codes.

For the ease of notation, let us define $\mathcal{R}_q(n) := R(\Phi_{\mathbf{F}_q}^{n,n})$. (In fact, the methods we use here may also be applied to obtain lower bounds for $R(\Phi_{\mathbf{F}_q}^{l,m})$ for $l \neq m$, but we confine ourselves to the case $l = m$.)

Let $0 \neq f \in \mathbf{F}_q[x]_n$. Then the kernel of the multiplication with f is obviously trivial which shows that $\dim(f\mathbf{F}_q[x]_n) = n$. Hence, $\mathcal{R}_q(n) \geq N_q[n, n]$ by (9.1). Applying the Singleton bound $N_q[n, n] \geq 2n - 1$ we obtain $\mathcal{R}_q(n) \geq 2n - 1$.

(9.5) Lemma. $\mathcal{R}_q(n) \geq 2n - 1$.

This lemma is of course also a trivial consequence of (8.31) and (8.32): We know by (8.31) that $R(\mathbf{F}_{q^n}/\mathbf{F}_q) \geq 2n - 1$ and by (8.32) that $R(\mathbf{F}_{q^n}/\mathbf{F}_q) \leq \mathcal{R}_q(n)$.

The Singleton inequality is very poor. Suppose for example that $q = 2$ and $n = 4$. Then the Singleton inequality gives $N_2[4, 4] \geq 7$ but the Griesmer bound gives $N_2[4, 4] \geq 4 + 2 + 1 + 1 = 8$. Is it possible to obtain a better lower bound for $N_q[n, n]$ which is at least valid for large n? In other words, what is a good asymptotic lower bound for $N_q[n, n]$? Here we can apply the asymptotic bounds discussed in Section 1.6 in the following way.

(9.6) Lemma. *Let* R_q *be a continuous monotonically decreasing function in the interval* $[0, \frac{q}{q-1}]$ *such that* $R_q(x) \geq \alpha_q(x)$ *for every* $x \in [0, \frac{q}{q-1}]$, $R_q(0) = 1$, *and* $R_q(\frac{q-1}{q}) = 0$. *Let* ξ *be the unique solution of* $R_q(\xi) = \xi$ *in the interval* $(0, 1)$.

(1) *If* $R_q(\xi) > \alpha_q(\xi)$, *then* $N_q[n, n] > n/\xi$ *for sufficiently large* n.

(2) *If* $R_q(\xi) = \alpha_q(\xi)$, *then there exists for every* $\varepsilon > 0$ *an* n_0 *such that for every* $n \geq n_0$ *we have* $N_q[n, n] \geq n/(\xi + \varepsilon)$.

PROOF. For each n let C_n be an $[N_q[n,n],n,n]$-code. Further, let $\delta := \limsup n/N_q[n,n]$. By the definition of α_q and our assumptions we have $\delta \leq \alpha_q(\delta) \leq R_q(\delta)$. In case (1) we obtain $\delta < R_q(\delta)$, i.e., $\delta < \xi$. In case (2) we obtain $\delta \leq \xi$. □

The following corollaries are immediate.

(9.7) Corollary (BROWN-DOBKIN [6]). *For large n we have $\mathcal{R}_2(n) \geq 3.52n$.*

PROOF. We know already that $\mathcal{R}_2(n) \geq N_2[n,n]$. For estimating the right hand side from below we use (9.6)(2) with $R_2(x) := H_2(\frac{1}{2} - \sqrt{x(1-x)})$ from (1.18). Solving $R_2(\xi) = \xi$ numerically for $\xi \in (0, \frac{1}{2})$ we obtain $\xi \sim 0.283477$, hence $N_2[n,n] \geq n/0.2835 = 3.527n$ for large n. □

(9.8) Corollary. *For large n we have $\mathcal{R}_q(n) > (2 + \frac{1}{q-1})n$.*

PROOF. We use (9.6)(1) with the curve $R_q(x) = 1 - \frac{q}{q-1}x$ from (1.18) and obtain $R_q(\xi) = \xi$ for $\xi = (q-1)/(2q-1)$. This gives the assertion. □

The lower bounds for $\mathcal{R}_q(n)$ given in the last two corollaries are linear in n. Is it also possible to give upper bounds for $\mathcal{R}_q(n)$ linear in n? This would in fact have an interesting coding theoretic application which we want to discuss in the following.

Let us call a sequence C_n of linear codes *good*, if it contains a subsequence C_m such that $\lim \delta(C_m) \neq 0$ and $\lim R(C_m) \neq 0$. Suppose that $\mathcal{R}_q(n) \leq cn$ for infinitely many n for some constant c depending possibly on $\mathbf{F}_q$. Then for every such n there exits by Section 9.1 a linear $[\mathcal{R}_q(n),n,n]$-code. By adding eventually zero coordinates to this code one obtains a $[\lceil cn \rceil,n,n]$-code C_n. The sequence of codes obtained so is a good sequence since $\lim(R(C_n),\delta(C_n)) = (c,c)$ and $c \neq 0$. Hence an asymptotic linear upper bound for $\mathcal{R}_q(n)$ would imply the existence of a family of good codes and the effective construction of algorithms realizing the asymptotic linear upper bound would yield an effective construction of a family of good codes.

As the bilinear complexity of polynomial multiplication and that of multiplication in simple extension fields are related, we may also ask whether an upper bound for $R(\mathbf{F}_{q^n}/\mathbf{F}_q)$ which is linear in n also yields families of good codes. Let a be a nonzero element in $\mathbf{F}_{q^n}$. Then $a\mathbf{F}_{q^n} = \mathbf{F}_{q^n}$, hence by (9.1) $R(\mathbf{F}_{q^n}/\mathbf{F}_q) \geq N_q[n,n]$. This shows that an asymptotic linear upper bound for $R(\mathbf{F}_{q^n}/\mathbf{F}_q)$ also yields a family of good codes.

We have already seen that geometric Goppa codes give rise to sequences of asymptotically good codes. Is it possible to use these codes to obtain linear upper bounds for $\mathcal{R}_q(n)$ or $R(\mathbf{F}_{q^n}/\mathbf{F}_q)$? An answer to this question is given in the next chapter.

9.4 Exercises

9.1. Let U, V, and W be finite dimensional F_q-spaces and $\Phi \in \mathrm{Bil}(U \times V; W)$ be concise. Let $\delta_1 := \min\{\dim \Phi(U, b) \mid 0 \neq b \in V\}$ and $\delta_2 := \min\{\mathrm{rk}(\lambda\Phi) \mid 0 \neq \lambda \in W^*\}$ (note that for $\lambda \in W^*$, $\lambda\Phi$ is a bilinear form on $U \times V$ and it makes sense to speak of the rank of this bilinear form). Show that $R(\Phi) \geq \max\{N_q[\dim V, \delta_1], N_q[\dim W, \delta_2]\}$.

9.2. Show that $N_q[n, n] > 2n$ for $n \geq 3q$ and hence $R(\mathsf{F}_{q^n}/\mathsf{F}_q) > 2n$ for $n \geq 3q$ (Hint: use the Griesmer bound).

CHAPTER 10

Multiplication in finite fields

10.1 The Theorem of Chudnovsky & Chudnovsky

In this section we discuss a connection between the bilinear complexity of multiplication in finite extensions of finite fields and algebraic function fields over finite fields due to D.V. Chudnovsky and G.V. Chudnovsky. Recall that for any prime divisor $\mathfrak{p}$ of and algebraic function field K/k of one variable, the canonical residue class morphism $\kappa_{\mathfrak{p}}: \mathcal{O}_{\mathfrak{p}} \to K(\mathfrak{p})$ (where $\mathcal{O}_{\mathfrak{p}}$ is the valuation ring corresponding to $\mathfrak{p}$ and $K(\mathfrak{p})$ the residue class field of $\mathfrak{p}$) is called the *evaluation map corresponding to* $\mathfrak{p}$. In the sequel we shall, by abuse of notation, denote restrictions of $\kappa_{\mathfrak{p}}$ to subspaces of $\mathcal{O}_{\mathfrak{p}}$ also by $\kappa_{\mathfrak{p}}$. Also, we set $R_q(n) := R(\mathbf{F}_{q^n}/\mathbf{F}_q)$.

(10.1) Theorem. *Let q be a prime power and n be a positive integer. Suppose that there exists an algebraic function field $K/\mathbf{F}_q$ of one variable such that K contains divisors $\mathfrak{p}$ and D with the following properties:*

- *$\mathfrak{p}$ is a prime divisor of degree n,*
- *$L(D) \subset \mathcal{O}_{\mathfrak{p}}$ and the evaluation map $\kappa_{\mathfrak{p}}: L(D) \to K(\mathfrak{p})$ is surjective,*
- *$K/\mathbf{F}_q$ contains more than $2\deg(D)$ prime divisors of degree one.*

Then $R_q(n) \leq \dim(2D)$.

PROOF. Note first that $K(\mathfrak{p}) \simeq \mathbf{F}_{q^n}$, hence for the multiplication ϕ in $K(\mathfrak{p})$ we have $R(\phi) = R_q(n)$. Second, by the theorem of independence of valuations [1], we can find in the class of D a divisor D' such that $\operatorname{ord}_{\mathfrak{p}}(D') = 0$ and such that for all prime divisors P of degree one of $K/\mathbf{F}_q$, $\operatorname{ord}_P(D') = 0$. Because of $\operatorname{ord}_{\mathfrak{p}}(D') = 0$, $\kappa_{\mathfrak{p}}$ is defined on $L(D')$. Its kernel equals $L(D' - \mathfrak{p})$ and hence the dimension of its image is $\dim(D') - \dim(D' - \mathfrak{p}) = \dim(D) - \dim(D - \mathfrak{p}) = n$. By changing D to D' if necessary we may thus suppose that $\operatorname{ord}_P(D) = 0$ for all prime divisors of degree one of $K/\mathbf{F}_q$.

Let ν be the restriction of the multiplication in K to $L(D) \times L(D)$. The following diagram clearly commutes:

$$\begin{array}{ccccc} L(D) & \times & L(D) & \xrightarrow{\nu} & L(2D) \\ \downarrow{\scriptstyle \kappa_\mathfrak{p}} & & \downarrow{\scriptstyle \kappa_\mathfrak{p}} & & \downarrow{\scriptstyle \kappa_\mathfrak{p}} \\ K(\mathfrak{p}) & \times & K(\mathfrak{p}) & \xrightarrow{\phi} & K(\mathfrak{p}) \end{array} .$$

Since by assumption $\kappa_\mathfrak{p}(L(D)) = K(\mathfrak{p})$, (8.25)(1) gives that $R_q(n) = R(\phi) \leq R(\nu)$.

Let $P_1, \ldots, P_N$ be the prime divisors of degree one of $K/\mathbf{F}_q$. Let $\gamma\colon L(2D) \to \oplus_{i=1}^N K(P_i)$ be defined by $\gamma(g) := (g(P_1), \ldots, g(P_N))$ (Compare Chapter 3). Since $N > 2D$ by assumption, γ is injective. Without loss of generality we may assume that the image of γ equals $\oplus_{i=1}^d K(P_i)$ where $d = \dim(2D)$. Denoting by μ the multiplication in the $\mathbf{F}_q$-algebra $\oplus_{i=1}^d K(P_i)$ (with multiplication and addition defined component-wise), the following diagram commutes:

$$\begin{array}{ccccc} L(D) & \times & L(D) & \xrightarrow{\nu} & L(2D) \\ \downarrow{\scriptstyle \tilde{\gamma}} & & \downarrow{\scriptstyle \tilde{\gamma}} & & \downarrow{\scriptstyle \gamma} \\ \bigoplus_{i=1}^d K(P_i) & \times & \bigoplus_{i=1}^d K(P_i) & \xrightarrow{\mu} & \bigoplus_{i=1}^d K(P_i) \end{array} ,$$

where μ is the multiplication in $\oplus_{i=1}^d K(P_i)$ and $\tilde{\gamma}$ is the restriction of γ to $L(D)$. Since γ is injective,we obtain by (8.25)(2) that $R(\nu) \leq R(\mu) = d$, hence $R_q(n) = R(\phi) \leq R(\nu) \leq R(\mu) \leq d$. □

10.2 An Asymptotic Linear Upper Bound

Using p-modular function fields we want to prove the following theorem:

(10.2) Theorem (CHUDNOVSKY, CHUDNOVSKY). *Let $p \geq 5$. There exists an infinite sequence (n_i) of integers such that $R_{p^2}(n_i) \leq 3n_i + o(n_i)$.*

For the proof of this theorem we first need two preliminary lemmas.

(10.3) Lemma. *Let $K/\mathbf{F}_q$ be an algebraic function field of genus g and $\mathfrak{p}$ be a prime divisor of degree n of K. Suppose that K contains a non-special divisor B_0 such that $\deg(B_0) + \deg(\mathfrak{p}) \geq 2g - 1$. Then there exists a divisor D in the class of $B_0 + \mathfrak{p}$ such that the restricted evaluation map $L(D) \to K(\mathfrak{p})$ is surjective.*

PROOF. By the theorem of independence of valuations there exists a divisor D in the class of $B_0 + \mathfrak{p}$ such that $\mathrm{ord}_{\mathfrak{p}}(D) = 0$. Hence $L(D)$ is contained in the valuation ring corresponding to $\mathfrak{p}$ and the restricted evaluation map is defined. The kernel of this map is $L(D - \mathfrak{p})$ and hence the dimension of the kernel is $\dim(D - \mathfrak{p}) = \dim(B_0) = \deg(B_0) - g + 1$. Further, since by assumption $\deg(D) \geq 2g - 1$, D is non-special and $\dim(D) = \deg(D) - g + 1 = \deg(B_0) + \deg(\mathfrak{p}) - g + 1$. This implies that the image of the restricted evaluation map is n-dimensional. □

(10.4) Lemma. *Let $K/\mathbf{F}_q$ be an algebraic function field of one variable and let g denote the genus of K.*

(1) *If an integer n satisfies $n > \log_q g + 6$, then K contains a prime divisor of degree n.*

(2) *If an integer m satisfies $m \geq g + 2\log_q g + 6$, then K contains a non-special divisor of degree m.*

For a proof of this lemma the reader is referred to [9] or [35]. The technique used for the proof is the manipulation of the ζ-function of the function field. As a corollary we obtain:

(10.5) Corollary. *Suppose that there exists an algebraic function field $K/\mathbf{F}_q$ of genus g, and an integer n satisfying $\log_q g + 6 < n \leq g - 2\log_q g - 7$. Suppose further that the number of prime divisors of degree one of $K/\mathbf{F}_q$ is greater than $4g - 2$. Then $R_q(n) \leq 3g - 1$.*

PROOF. (10.4) implies that K contains a prime divisor $\mathfrak{p}$ of degree n. Let $m = 2g - 1 - n$. Then $m \geq g + 2\log_q g + 6$ by assumption, hence by (10.4) $K/\mathbf{F}_q$ contains a non-special divisor of degree m. Thus (10.3) implies that $K/\mathbf{F}_q$ contains a divisor D of degree $2g - 1$ such that the restricted evaluation map $L(D) \to K(\mathfrak{p})$ is surjective. Further, $K/\mathbf{F}_q$ contains more than $4g - 2 = 2\deg(D)$ prime divisors of degree one. By (10.1) we have $R_q(n) \leq \dim(2D) = 4g - 1 - g + 1 = 3g - 1$. □

Proof (of (10.2)). For a prime l different from p let $K_l := K_0^p(l)$. We denote by g_l the genus of K_l (see (5.11) for explicit formulas). Discarding small values of l if necessary, the integer $n_l := g_l - \lceil 2\log_q g_l \rceil - 7$ satisfies $\log_q g_l + 6 < n_l$. Further, by (7.6) the number N_l of prime divisors of degree one of K_l over $\mathbf{F}_{p^2}$ satisfies

$$N_l \geq g_l(p-1) \geq 4g_l > 4g_l - 2,$$

since $p \geq 5$. Hence, by (10.5),

$$\begin{aligned} R_{p^2}(n_l) &\leq 3g_l - 1 \\ &= 3n_l + 3\lceil \log_q g_l \rceil + 20 \\ &= 3n_l + o(n_l). \end{aligned}$$

This proves the theorem. □.

We see that the sequence of codes derived from the above algorithms gives rise to the point $(\frac{1}{3}, \frac{1}{3}) \in \Sigma_{p^2}$. (See Section 9.3.)

10.3 Further Results

Besides the asymptotic result stated in the last section there exist results concerning the exact value $R_q(n)$ for different q and n satisfying $\frac{1}{2}q+1 < n$. They can be derived by applying (10.1) to different function fields.

For q a prime power, let $\varepsilon(q)$ be defined by

$$\varepsilon(q) := \begin{cases} \max\{t \mid t \leq 2\sqrt{q}, (t,q) = 1\}, & \text{if } q \text{ is not a perfect square,} \\ 2\sqrt{q} & \text{if } q \text{ is a perfect square.} \end{cases}$$

Then the following theorem holds [36]

(10.6) Theorem. *For* $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + \varepsilon(q))$ *we have* $R_q(n) = 2n$.

There exist also other ranges for q where the exact value of $R_q(n)$ is (almost known) [37]. We just mention one of the results.

(10.7) Theorem. *Let* p *be a prime number such that* $(16p^2 - 12p + 1)/5$ *is not a square. Then* $R_{p^2}(n) \in \{2n, 2n+1\}$ *if* $\frac{1}{2}p^2 + 1 < n < \frac{1}{2}(p^2 + 4p - 4)$.

Also the complexity of the generation of these bilinear algorithms has been the subject of investigation. We refer the interested reader to [38, 39].

CHAPTER 11

Answers to all Exercises

Chapter 1

1.1. Denote by $H_1, \ldots, H_n$ the columns of H. A word $c = (c_1, \ldots, c_n) \in \mathbf{F}_q^n$ belongs to C if and only if $cH = 0$. But

$$cH = c_1 H_1 + \cdots + c_n H_n = \sum_{\substack{i \\ c_i \neq 0}} c_i H_i.$$

Hence, if every l columns of H are linearly idependent, $cH \neq 0$ for every nonzero $c \in \mathbf{F}_q^n$ of weight less or equal to l and this shows that the minimum distance d of C satisfies $d \geq l + 1$.

1.2. Let C be an $[n, k, d]$-code over $\mathbf{F}_q$ and $H \in \mathbf{F}_q^{(n-k)\times n}$ be a parity-check matrix for C. The rank of H is $n - k$, hence every $n - k + 1$ columns of H are linearly dependent. There exist thus nonzero $c_1, \ldots, c_{n-k+1} \in \mathbf{F}_q$ such that $c_1 H_1 + \cdots + c_{n-k+1} H_{n-k+1} = 0$. Setting $c = (c_1, \ldots, c_{n-k+1}, 0, \ldots, 0)$ we obtain thus $cH = 0$, i.e., $c \in C$, i.e., $d \leq n - k + 1$.

1.3. We have trivially $d(x, x) = 0$ and $d(x, y) = d(y, x)$ for all $x, y \in \mathbf{F}_{q^n}$. It remains to prove the triangle inequality, i.e., for arbitrary $x, y, z \in \mathbf{F}_{q^n}$ we have to prove that $d(x, y) \leq d(x, z) + d(z, y)$. It suffices to show this for $x, y, z \in \mathbf{F}_q$ (why?) and this is trivial.

1.4. Let $c \in C$ be transmitted and u with $d(u, c) \leq e$ be received. We have to show that c is the unique codeword in C having the least distance to u: suppose that there exists another codeword c' different from c such that $d(c', u) \leq e$. Then by the triangle inequality we have $d \leq d(c, c') \leq d(u, c) + d(u, c') \leq 2e < d$ which is a contradiction.

1.5. This is a trivial consequence of $d(x,y) = d(x-y,0)$ where 0 denotes the zero-word.

1.6. A trivial computation shows that the minimum distance of C is 3. Hence C is capable of correcting one error by Exercise 1.4.

1.7. The condition implies that the degrees of g_1 and g_2 are not equal. Hence the dimensions of the ideals generated by g_1 and g_2 are also not equal.

1.8. Since $(n,q) = 1$, we have $x^n - 1 = \prod_{i=1}^{r} h_i(x)$ where $h_i(x)$ are different irreducible polynomials over F_q. The number of different cyclic codes of length n over F_q is equal to the number of different monic divisors of $x^n - 1$ over F_q by the previous exercise. Hence there exist 2^r cyclic codes of length n over F_q.

Now note that over F_2 we have

$$x^9 - 1 = (x+1)(x^2+x+1)(x^6+x^3+1).$$

Hence there exist 8 inequivalent cyclic codes of length 9 over F_2.

1.9. By (1.10) the minimum distance d of C satisfies $d \geq l+1$. On the other side, the dimension of C equals $n-l$, hence $d \geq n-k+1$. The Singleton Inequality implies $d \leq n-k+1$, hence, $d = n-k+1$. This shows that for this code the Singleton Inequality is sharp.

Chapter 2

2.1. Let v be a valuation on F_q and $0 \neq a \in \mathsf{F}_q$. Then $v(a)^{q-1} = v(a^{q-1}) = v(1) = 1$, hence $v(a) = 1$.

2.2. Let $v(0) = r$. Then for all $b \in K$ we have $r = v(0) = v(0 \cdot b) = rv(b)$, hence $r = 0$. Further we have $v(1) = v(1 \cdot 1) = v(1)^2$, hence either $v(1) = 0$ (which is impossible, since for all $b \in K$ we have $v(b) = v(1 \cdot b) = v(1)v(b)$), or $v(1) = 1$. To see that $v(-1) = 1$, note that $1 = v(1) = v((-1)(-1)) = v(-1)^2$.

2.3. Assume that $v(a) < v(b)$ and suppose that $v(a+b) < v(b)$. Then $v(b) = v(a+b-a) \leq \max\{v(a+b), v(a)\} < v(b)$, which is a contradiction.

2.4. We only show this for multiplicative valuations, the case of additive valuations being similar. Let v and v' be multiplicative valuations on K. Suppose that v and v' are equivalent. By symmetry, it is sufficient to show that $\mathcal{O}_v \subseteq \mathcal{O}_{v'}$. Let $x \in \mathcal{O}_v$. Then $v(x) \leq 1$. If $v(x) < 1$, then $v'(x) < 1$ by the equivalence and hence $x \in \mathcal{O}_{v'}$.

If $v(x) = 1$, then by Exercise 2.3, we have $v(x-1) < 1$, hence $v'(x-1) < 1$, hence $x - 1 \in \mathcal{O}_{v'}$, i.e., $x \in \mathcal{O}_{v'}$.

2.5. It is easily checked that $\mathcal{M}_v$ is an ideal of $\mathcal{O}_v$: for $x, y \in \mathcal{M}_v$ we have $v(x+y) \leq \max\{v(x), v(y)\} < 1$, hence $\mathcal{M}_v$ is additively closed. Further, for $r \in \mathcal{O}_v$ and $x \in \mathcal{M}_v$ we have $v(rx) = v(r)v(x) < 1$, hence $rx \in \mathcal{M}_v$. Now note that $\mathcal{M}_v = \mathcal{O}_v \setminus \mathcal{O}_v^\times$, since $\mathcal{O}_v^\times = \{r \in \mathcal{O}_v \mid v(r) = 1\}$. This yields the assertion.

2.6. This is a standard exercise in algebra: If $x + M$ is a nonzero element in R/M, then $x \in R \setminus M$ and the ideal $Rx + M$ generated by x and M contains M properly, hence equals R since M is maximal. Thus there exist $r \in R$, $m \in M$ such that $1 = rx + m$. This shows that $rx + M = 1 + M$, that is $r + M$ is the multiplicative inverse of $x + M$ in R/M.

2.7. If $h(x) = g(x)/f(x) = g'(x)/f'(x)$, then $g(x)g'(x) = f(x)f'(x)$, hence $\deg(g) + \deg(g') = \deg(f) + \deg(f')$, i.e., $\deg(f) - \deg(g) = \deg(f') - \deg(g')$. Thus ord_∞ is well-defined. To see that it is an additive valuation it suffices to note that $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

2.8. It is easily seen that

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; g(x), f(x) \in k[x], g(x) \neq 0, \deg(f) \leq \deg(g) \right\},$$

and

$$\mathcal{M}_\infty := \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_\infty \;\middle|\; \deg(f) < \deg(g) \right\},$$

are the valuation ring, resp. the maximal ideal corresponding to ord_∞ in $k(x)$. We show that for every $h \in \mathcal{O}_\infty$ there exists $a \in k$ such that $h - a \in \mathcal{M}_\infty$. Let $h = f/g \in \mathcal{O}_\infty$. If f and g are not of the same degree, then $h \in \mathcal{M}_\infty$ and we may take $\alpha = 0$. Otherwise, let m be the common degree of f and g and let α be the quotient of the highest coefficients of f and g. It is easily seen that $h - \alpha \in \mathcal{M}_\infty$.

2.9. We have to show that for all $0 \neq h \in k(x)$ we have $\sum_p \mathrm{ord}_p(h)\deg(p) = 0$, where p runs over all irreducible polynomials in $k[x]$ and ∞ and $\deg(\infty) = 1$ by the previous exercise. Let $h := \prod_{i=1}^r p_i^{e_i}$, where p_i are irreducible polynomials and e_i are integers. Then $\sum_p \mathrm{ord}_p(h)\deg(p) = \sum_{i=1}^r \mathrm{ord}_{p_i}(h)\deg(p_i) + \mathrm{ord}_\infty(p) = \sum_{i=1}^r e_i + \mathrm{ord}_\infty(h)$. Now note that $\mathrm{ord}_\infty(h) = -\sum_{i=1}^r e_i$, which yields the assertion.

2.10. Prinicipal divisors are of degree zero by the product formula, hence we have to show that in the case of a rational function field $k(x)$ any divisor of degree zero is principal. Let $A = \sum_p a_p(p) + a_\infty(\infty)$ where p runs over the irreducible polynomials of $k[x]$. Let $h := \prod_p p^{a_p}$. Then it is easily seen that the divisor of h equals A.

Chapter 3

3.1. By (3.2) the dimension k of the code equals $k = \deg(G) + 1$ and its minimum distance d satisfies $d \geq n - \deg(G) = n - k + 1$. On the other side, the Singleton Inequality implies that $d \leq n - k + 1$, hence $d = n - k + 1 = n - \deg(G)$.

Chapter 5

5.1. Let us see whether there exists $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ such that $Ai = 2i$. We obtain $\frac{ai+b}{ci+d} = 2i$, which yields $(b + 2c) + i(a - 2d) = 0$. Noting that $ad - bc = 1$ we obtain $2d^2 + 2c^2 = 1$ which is impossible.

5.2. It is easy to see that the sequence $(\overline{ni})$ does not converge in $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$ and has not any converget subsequences.

5.3. It is shown in (5.7) that a parabolic element $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ has a unique fixed point $\mathbf{R} \cup \{\infty\}$. To show the converse, let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ and $z \in \mathbf{C} \cup \{\infty\}$ be a fixed point of α. If $z = \infty$, then $c = 0$ and $1 = \det \alpha = ad$. This shows that $a = d = \pm 1$, and $\alpha = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$, i.e., α is parabolic. Otherwise $cz^2 + (d - a)z - b = 0$; α has a unique fixed point in $\mathbf{R} \cup \{\infty\}$ if and only if $(d - a)^2 + 4bc = 0$ which is equivalent to $0 = (a + d)^2 - (4ad - 4bc) = \mathrm{tr}\,(\alpha)^2 - 4\det(\alpha)$.

Chapter 8

8.1. Let $D = K[x]/(p(x))$ where p is an irreducible polynomial over K. Consider the following commutative diagram

$$\begin{array}{ccccc} K[x]_l & \times & K[x]_m & \xrightarrow{\Phi_K^{l,m}} & K[x]_{l+m-1} \\ \downarrow{\scriptstyle \kappa_l} & & \downarrow{\scriptstyle \kappa_m} & & \downarrow{\scriptstyle \kappa_{l+m-1}} \\ D & \times & D & \xrightarrow{\mu} & D \end{array}$$

where $\kappa\colon K[x] \to D$ is reduction modulo $p(x)$, κ_k is the restriction of κ to $K[x]_k$, and μ is the multiplication in D. By the assumptions κ_{l+m-1} is injective, hence (8.25)(2) implies the assertion.

8.2. Consider the following commutative diagram

$$\begin{array}{ccccc} U' & \times & V' & \xrightarrow{\Phi'} & W' \\ \downarrow{\scriptstyle \mathrm{id}_{U'}} & & \downarrow{\scriptstyle \mathrm{id}_{V'}} & & \downarrow{\scriptstyle \mathrm{id}_{W'}} \\ U & \times & V & \xrightarrow{\Phi} & W \end{array}$$

where $W' = \langle \Phi'(U', V') \rangle$. Since $\mathrm{id}_{W'}$ is injective, we have $R(\Phi') \leq R(\Phi)$.

8.3. It is easy to see that Φ' is well-defined and concise. Consider the following commutative diagram

$$\begin{array}{ccccc} U & \times & V & \xrightarrow{\Phi} & W' \\ \downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_2} & & \downarrow{\scriptstyle \mathrm{id}_{W'}} \\ U/U' & \times & V/V' & \xrightarrow{\Phi'} & W' \end{array}$$

where κ_1 and κ_2 are the canonical homomorphisms. Since κ_1 and κ_2 are surjective, we have $R(\Phi') \leq R(\Phi)$ and since $\mathrm{id}_{W'}$ is (in particular) injective, we have $R(\Phi) \leq R(\Phi')$ (by Lemma (8.25)).

Chapter 9

9.1. Let $\Phi = \sum_{i=1}^{r} u_i \otimes v_i \otimes w_i$ where $u_i \in U^*$, $v_i \in V^*$ and $w_i \in W$. Analogously to the proof of (9.1) we define linear mappings γ_1 and γ_2 by

$$\begin{array}{rccl} \gamma_1\colon & V & \to & \mathsf{F}_q^r \\ & b & \mapsto & (v_1(b), \ldots, v_r(b)), \end{array}$$

and

$$\begin{array}{rccl} \gamma_2\colon & W^* & \to & \mathsf{F}_q^r \\ & \lambda & \mapsto & (\lambda(w_1), \ldots, \lambda(w_r)). \end{array}$$

The images of γ_1 and γ_2 are linear codes over F_q which we denote by C_1 and C_2. Let us compute the kernel of γ_i: let $b \in \ker \gamma_1$. Then

$$\Phi(U, b) = \sum_{\rho \leq r} u_\rho(U) \underbrace{v_\rho(b)}_{=0} w_\rho = 0,$$

which shows that $b = 0$ since Φ is assumed to be concise (here 2-conciseness of Φ would also suffice). Anlogously, if $\lambda \in \ker \gamma_2$, we obtain $\lambda\Phi(U, V) = 0$ which shows

that $\lambda = 0$, since Φ is concise (3-conciseness would suffice). Hence $\dim C_1 = \dim V$, and $\dim C_2 = \dim W$. Now for any $b \in V$ we have

$$\Phi(U, b) \subseteq \sum_{\rho, v_\rho(b) \neq 0} \mathsf{F}_q w_\rho,$$

hence we deduce that $\dim \Phi(U, b) \leq |\{\rho \mid v_\rho(b) \neq 0\}| = \operatorname{wgt}(\gamma_1(b))$, which shows that the minimum distance d_1 of C_1 satisfies $d_1 \geq \delta_1$. Analogously, for $\lambda \in W^*$ we have

$$\lambda\Phi = \sum_{\rho, \lambda(w_\rho) \neq 0} u_\rho \otimes v_\rho,$$

which shows that $\operatorname{rk} \lambda\Phi \leq |\{\rho \mid \lambda(w_\rho) \neq 0\}| = \operatorname{wgt}(\gamma_2(\lambda))$. This implies that the minimum distance d_2 of C_2 satisfies $d_2 \geq \delta_2$.

9.2. Let $m := \lceil \log_q n \rceil$. Then we have

$$\begin{aligned}
\sum_{i=0}^{n} \left\lceil \frac{n}{q^i} \right\rceil &\geq \sum_{i=0}^{m} \frac{n}{q^i} + (n - m - 1) \\
&= n \frac{q^{m+1} - 1}{q - 1} \frac{1}{q^m} + n - m - 1 \\
&= 2n + n \frac{1 - 1/q^m}{q - 1} - m - 1 \\
&\geq 2n + \frac{n - 1}{q - 1} - m - 1,
\end{aligned}$$

the last inequality being a cosequence of $q^m \geq n$.

Now consider the function $f(x) = \frac{x-1}{q-1} - \log_q x - 1$. By studying the derivative $f'(x) = 1/(q-1) - 1/x \ln q$, we see that $f(x)$ is monotonically increasing for $x \geq q$. Since $n \geq 3q$ is assumed, this shows that

$$\begin{aligned}
\sum_{i=0}^{n} \left\lceil \frac{n}{q^i} \right\rceil &> 2n + \frac{3q - 1}{q - 1} - \lceil \log_q 3q \rceil - 1 \\
&= 2n + 1 + \frac{2}{q - 1} - \lceil \log_q 3 \rceil \\
&> 2n.
\end{aligned}$$

Bibliography

[1] *E. Artin*: *Algebraic Numbers and Algebraic Functions.* Gordon and Breach Science Publishers, 1977.

[2] *A. Alder, V. Strassen*: On the algorithmic complexity of associative algebras. *Theoret. Comp. Sci.*, **15**, 201–211, (1981).

[3] *W. Baur*: Algebraische Berechnungskomplexität. *Lectures at the Mathematics Department of the University of Konstanz,* (unpublished manuscript), 1990.

[4] *E.R. Berlekamp, R. J. McEliece, H. C. A. van Tilborg*: On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, **24**, 384–386, (1978).

[5] *R.W. Brockett, D.P. Dobkin*: On the optimal evaluation of a set of bilinear forms. *Linear Algebra and its Applications*, **19**, 207–235, (1978).

[6] *M.R. Brown, D.P. Dobkin*: An improved lower bound on polynomial multiplication. *IEEE Trans. Computers*, **29**, 337–340, (1980).

[7] *N. Bshouty*: A new lower bound for matrix multiplication. 29th Annual Symposium on Foundations of Computer Science (FOCS), 64–67, (1988).

[8] *P. Bürgisser, M. Clausen, Th. Lickteig, M. A. Shokrollahi*: *Algebraic Complexity Theory.* In preparation.

[9] *D.V. Chudnovsky, G.V. Chudnovsky*: Algebraic complexities and algebraic curves over finite fields. *Proc. Natl. Acad. Sci. USA*, **84**, 1739–1743, (1987).

[10] *D. Coppersmith, S. Winograd*: Matrix multiplication via arithmetic progressions. *Proc. 19th ACM STOC*, New York, 1–6, (1987).

[11] *H.F. de Groote*: Characterization of division algebras of minimal rank and the structure of their algorithm varieties. *SIAM Journal of Computing*, **12**, 101–117, (1983).

[12] *H.F. de Groote*: *Lectures on the Complexity of Bilinear Problems.* Lecture Notes in Computer Science, **245**, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1985.

[13] *M. Eichler*: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, **5**, 355–366, (1954).

[14] *M.R. Garey, D.S. Johnson*: *Computers and Intractability. A Guide to the Theory of NP-Completeness.* Freeman and Company, New York, 1979.

[15] *V. D. Goppa*: A new class of linear error-correcting codes. *Problems of Information Transmission*, **6**, 207–212, (1970).

[16] *H. Hasse*: *Zahlentheorie.* Akademie Verlag, Berlin, 1969.

[17] *H. Hijikata*: Explicit formulas for the traces of Hecke-operators for $\Gamma_0(N)$. *J. Math. Soc. Japan*, **26**, No. 1, 56–82, (1974).

[18] *J. Igusa*: Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, **81**, 561–577, (1959).

[19] *Y. Ihara*: Hecke polynomials as congruence ζ-functions in elliptic mmodular case. *Ann. Math.*, **85**, 267–295, (1967).

[20] *J. C. Lafon, S. Winograd*: A lower bound for the multiplicative complexity of the product of two matrices. *Unpublished manuscript* (1978).

[21] *S. Lang*: *Algebra.* Addison-Wesley, 1984

[22] *S. Lang*: *Introduction to Modular Forms.* Springer Verlag, Berlin, Heidelberg, New York, 1976. (See also the correction of Zagier [45].)

[23] *J.H. van Lint*: *Introduction to Coding Theory.* Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1982.

[24] *F. J. MacWilliams, N. J. A. Sloane*: *The Theory of Error Correcting Codes.* North Holland, Amsterdam, New York, Oxford, 1977.

[25] *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).

[26] *T. Miyake*: *Modular forms*, Springer Verlag, Berlin, Heidelberg, New York, 1989.

[27] *C. Moreno*: *Algebraic Curves over Finite Fields.* Cambridge University Press, 1989.

[28] *R. Narasimhan*: *Complex Analysis of one Variable.* Birkhäuser, Basel, 1985.

[29] *F. K. Schmidt*: Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Zeitschrift*, **33**, 1–32, (1931).

[30] *A. Schönhage, V. Strassen*: Schnelle Multiplikation großer Zahlen. *Computing*, **7**, 281–292, (1971).

[31] *J. P. Serre*: *A Course in Arithmetic.* Springer Verlag, Berlin, Heidelberg, 1973.

[32] *G. Shimura*: *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, 1971.

[33] *S. Shokranian*: *The Selberg-Arthur Trace Formula.* Lecture Notes in Mathematics, **1503**, Springer Verlag, Berlin, Heidelberg, 1992.

[34] *M. A. Shokrollahi*: Codes on Hermitian curves. *Lecture Notes in Computer Science*, **507**, 168–176, 1987.

[35] *M. A. Shokrollahi*: *Beiträge zur Codierungs- und Komplexitätstheorie mittels algebraischer Funktionenkörper.* Bayreuther math. Schriften, *Heft 39*, pp. 236, 1991.

[36] *M. A. Shokrollahi*: Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comp.*, **21**, 1193–1198, (1992).

[37] *M. A. Shokrollahi*: On the rank of certain finite fields. *Computational Complexity*, **1**, 157–181, (1991).

[38] *M. A. Shokrollahi*: Efficient randomized generation of optimal multiplication algorithms in certain finite fields. *Computational Complexity*, **2**, 67–96, (1992).

[39] *M. A. Shokrollahi, K. Werther*: Generation of optimal bilinear multiplication algorithms: theory and implementation, *Research Report No. 8575-CS*, University of Bonn, 1992,

[40] *V. Strassen*: Vermeidung von Divisionen. *Journal für die reine und angewandte Mathematik*, **264**, 184–202, (1973).

[41] *V. Strassen*: Gaussian elimination is not optimal. *Num. Math.*, **13**, 354–356, (1969).

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

[43] *M. A. Tsfasman, S. G. Vladut, Th. Zink*: Modular curves, Shimura curves, and codes better than the Varshamov Gilbert bound. *Math. Nachrichten*, **104**, 13–28, (1982).

[44] *S. Winograd*: On multiplication in algebraic extension fields. *Theoretical Computer Science*, **8**, 359–377, (1979).

[45] *D. Zagier*: Correction to "The Eichler-Selberg trace formula on $\mathrm{SL}_2(\mathbf{Z})$". *Lecture Notes in Mathematics*, **627**, 171–173, (1977).

Index

previously published in this series

Climatic Zones and Rural Housing in India
Editors: N.K. Bansal, G. Minke
GERMAN-INDIAN COOPERATION
ISBN 3-89336-008-5

Titanium Nitride Coatings
Preparations, Characteristics and Applications
S. Marinković, Z. Marinković and H. Kötter
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-010-7

The Nappe Structure of the North Sporades in Greece
The Glossa Unit of Skopelos
V. Jacobshagen and D. Matarangas
GERMAN–GREEK COOPERATION
ISBN 3-89336-015-8

Impact of Green on the Urban Atmosphere in Athens
M. Horbert, A. Kirchgeorg, A. Chronopoulou-Sereli, J. Chronopoulous
GERMAN-GREEK COOPERATION
ISBN 3-89336-016-6

Development and Improvement of Identification Methods for Time Varying and Nonlinear Industrial Processes
Bilateral Cooperation between Technische Hochschule Darmstadt and Univerza "Edvarda Kardelja" Ljubljana
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-022-0

Digital Adaptive Control
edited by: K. Schwamberger, A. Schumann and D. Matko, B. Zupančić
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-021-2

Boron Nitride Coatings
Preparation, Characteristics and Applications
S. Marinković and Z. Marinković with collaboration of H. Kötter and Ch. Meixner
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-024-7

A Test Method for Solar Water Heaters Characterisation
by M. Bosanac
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-032-8

Selected Studies of Adsorption on Metal and Semiconductor Surfaces
by B. Gumhalter, M. Milun and K. Wandelt
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-034-4

Osnovi nauke o materijalima (neue Werkstoffe)
by G. Ondracek and I. Stamenković
GERMAN-YUGOSLAV COOPERATION
ISBN 3-89336-036-0

Scientific Series of the International Bureau

1 Fundamentos do Método de Correntes Parasitas
S. Stegemann (1990)
GERMAN-BRASILIAN COOPERATION

2 Diamond and Diamondlike Coatings
S. Marinković and Z. Marinković with S. Krawczynski (1990)
GERMAN-YUGOSLAV COOPERATION

3 Environmental Research in Aquatic Systems
M. Branica (1990)
GERMAN-YUGOSLAV COOPERATION

4 Volcanic Tremor and Magma Flow
edited by R. Schick and R. Mugiono (1991)
GERMAN-INDONESIAN COOPERATION

5 Petrography, Geochemistry and Petrogenesis of the MIGIF-HAFAFIT GNEISSES at HAFAFIT MINE Area, South Eastern Desert, Egypt
Abdelazeem Ahmed Rashwan (1991)
GERMAN-EGYPTIAN COOPERATION

6 Terpene in Nadeln und Zweigen von Picea abies (L.) Karst
Projektleitung: H. Ziegler, V. Tišler (1991)
GERMAN-YUGOSLAV COOPERATION

7 Titanium Nitride Coatings
Preparations, Characteristics and Applications (2nd edition)
S. Marinković, Z. Marinković and H. Kötter (1991)
GERMAN-YUGOSLAV COOPERATION

8 The Thermal Degradation of Poly(2-Mono-, 2,2-Di- and 2,2,2-Trichloroethyl Methacrylate) – Kinetics and Mechanisms –
I. Popović, L. Katsikas, J. Veličković, W. Schnabel (1991)
GERMAN-YUGOSLAV COOPERATION

9 New Developments in Diamond and Diamondlike Coatings
Preparation, properties and application
S. Marinković and Z. Marinković with S. Krawczynski (1991)
GERMAN-YUGOSLAV COOPERATION

10 Integral Methods for the Calculation of Electric Fields
For Application in High Voltage Engineering (1992)
GERMAN-YUGOSLAV COOPERATION

11 Rechnerunterstützte Montageablaufplanung
M. Rabe, Y. Wang, I. Veza (1992)
GERMAN-CROATIAN COOPERATION

12 Reference Materials and Methods in Environmental and Biological Research
M. Rossbach (1992)
GERMAN-SLOVENIAN-COOPERATION

13 Photoacoustic Spectroscopy with Emphasis to
Application on Solid and Powered Samples
A. Alebić-Juretić, C. Zetzsch (1992)
GERMAN-CROATIAN COOPERATION

14 Fracture Mechanics and Mechanical Testing Laboratory at Inchass
M.M. Ghoneim, A.M. Nasreldin, A.A. Elsayed, D. Pachur (1992)
GERMAN-EGYPTIAN COOPERATION

15 Analysis Methods and Techniques for Hard Thin Layer Coatings Characterization –
in particular on Titanium Nitride –
B. Bliznakovska, M. Miloševski
in cooperation with S. Krawczynski, Ch. Meixner, H.-R. Kötter (1993)
GERMAN COOPERATION with the University "Kiril i Metodij", Skopje

16 Biomaterials
edited by J. Krawczynski, G. Ondracek (1993)
GERMAN COOPERATION with the University of Skopje

17 CVD – Main Concepts, Applications and Restrictions
B. Bliznakovska, M. Miloševski
in cooperation with S. Krawczynski, Ch. Meixner, H.-R. Kötter (1993)
GERMAN COOPERATION with the University "Sv. Kiril i Metodij", Skopje

18 Thessaloniki '91 Field Measurement Campaign
edited by N. Moussiopoulos, G. Kaiser (1993)
GERMAN-GREEK COOPERATION

19 Geochemistry and Tectonic Significance of the
Pan-African El Sibai Window, Central Eastern Desert, Egypt
Gamal Mohamed Kamal El Din Saber (1993)
GERMAN-EGYPTIAN COOPERATION

20 A Transect from a Tectonic Mélange to an Island-Arc in the
Pan-African of SE Egypt (Wadi Ghadir Area)
Hani El-Akhal (1993)
GERMAN-EGYPTIAN COOPERATION

21 Coding Theory and Bilinear Complexity
S. Shokranian, M.A. Shokrollahi (1993)
GERMAN-BRASILIAN COOPERATION

ISBN 3-89336-123-5