CONSTRUCTIONS OF CODES AND LOW-DISCREPANCY SEQUENCES USING GLOBAL FUNCTION FIELDS

DAVID JOHN STUART MAYOR

(MSci (Hons), ARCS)

A THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

NATIONAL UNIVERSITY OF SINGAPORE

2006

Acknowledgements

First of all, I would like to thank Professor Harald Niederreiter for his strong guidance during the three years he has been gracious enough to supervise me.

I would also like to thank my family for their constant support and encouragement during all stages of my education.

Finally, I would like to state how grateful I am to the National University of Singapore for its generosity in providing me with an NUS Research Scholarship throughout my stay.

Singapore, September 2006 David J. S. Mayor

Contents

Summary

In this thesis we will look at recent developments in the theory of algebraic-geometry codes such as the use of places of arbitrary degree, distinguished divisors, and local expansions. This will lead us to a new construction which will produce an asymptotic coding bound beating all previous efforts. We will also show that the best currently known constructions of algebraic-geometry codes, (t, m, s)-nets, and (t, s)-sequences all have analogous constructions using differentials. Finally, we show that in the decade since the last construction of (t, s)-sequences, new results in the theory of global function fields with many rational places provide improved bounds on the asymptotic properties of (t, s)-sequences, and that this in turn produces a stronger asymptotic bound for the star discrepancy.

Chapter 1

Introduction

This thesis represents a contribution to the theory of global function fields and their applications. Specifically, we will examine codes and low-discrepancy sequences, two seemingly divergent areas of mathematics which have progressively been seen to have closer links than one might initially imagine. We begin by offering a brief outline of their history.

Coding theory was developed by Shannon [47] in 1948 as a means of correcting errors in data transmission. From its beginnings as an area of research solely of interest to discrete mathematicians, the theory branched out in the early 1980s after Goppa wrote a seminal series of papers [11], [12], [13] demonstrating that a new class of codes could be constructed using algebraic curves over finite fields, or equivalently global function fields, where the codes' parameters could be bounded by using methods from algebraic-geometry such as the Riemann-Roch theorem. We refer to such codes as algebraic-geometry codes. The interest in these codes was magnified soon after Goppa introduced them when Tsfasman, Vlăduţ, and Zink [52] demonstrated that algebraic-geometry codes could be shown to produce sequences of codes with the best known asymptotic properties. More recently, it has been shown that there are various generalisations of Goppa's original construction which can be used to produce further asymptotic improvements.

The theory of low-discrepancy sequences has a long and storied history which can be traced back to a celebrated paper of Weyl [56] from 1916. These sequences were themselves of much interest to pure mathematicians before they found practical uses in modern applications such as numerical integration and optimisation. Background on the early developments of this theory is available in the book of Kuipers and Niederreiter [20]. Our research will concentrate on the classes of low-discrepancy point sets and sequences known as (t, m, s)-nets and (t, s)-sequences that were defined by Niederreiter [23]. Just as with coding theory, a significant breakthrough was made in the theory of low-discrepancy sequences when new constructions using global function fields were developed. Niederreiter and Xing collaborated on a series of papers [32], [33], [59], [34] which used global function fields to produce low-discrepancy sequences which were asymptotically optimal.

The fact that the best currently known asymptotic bounds for both codes and low-discrepancy sequences are obtained by using global function fields is not merely coincidence. Recently, Niederreiter and Pirsic [31] have shown that (t, m, s)-nets can be constructed by introducing a minimum distance function on the space $\mathbf{F}_q^{ms}$ which can be seen as a generalisation of the classical Hamming weight from coding theory.

A further similarity between the two areas of research is that both Goppa's introduction of algebraic-geometry codes and Niederreiter and Xing's introduction of low-discrepancy sequences using global function fields sparked searches for global function fields with many places of low degree. This itself is a rich and fascinating area of research which has intrigued a large number of mathematicians from the humble author to the Fields Medal and Abel Prize winning mathematician Jean-Pierre Serre [46]. Our exposure to this research within the thesis will be somewhat limited, but it remains a vital area from which we will draw many results.

The new results that will be presented in the thesis are the following. After a chapter on the preliminaries needed for our work, we begin our original research with a short chapter on the asymptotic properties of algebraic-geometry codes using places of arbitrary degree, and show that for small q we can gain global improvements on the Tsfasman-Vlăduţ-Zink bound. We will also show that for any value of q we can find a small interval where the Tsfasman-Vlăduţ-Zink bound can be improved upon. Unfortunately, these improvements do not lead to improvements on the asymptotic Gilbert-Varshamov bound. However, in the following chapter we construct a new class of algebraic-geometry codes with the explicit intention of breaking the mentioned bound. We do so by combining the ideas of distinguished divisors and local expansions. In Chapter 5 we demonstrate that there is an equivalent construction using differentials to the one in the previous chapter. In Chapter 6 we will show that our new construction of codes can indeed be used to beat all previously known asymptotic coding bounds. In Chapter 7 we turn to the topic of low-discrepancy point sets and introduce a new construction of (t, m, s)-nets using differentials. In Chapter 8 we also use differentials to introduce a new construction of (t, s)-sequences, which is the first in a decade. In Chapter 9 we look at new results that have occurred in the theory of towers of global function fields and then use these to gain improvements in the asymptotic theory of (t, s)-sequences. Finally, we show that these new improvements also have implications for the star discrepancy of low-discrepancy sequences and hence numerical integration.

Chapter 2

Preliminaries

In this chapter we recall some basic facts on global function fields, algebraic coding theory, and low-discrepancy sequences.

2.1 Global Function Fields

We start with a brief recapitulation on the theory of global function fields. The standard text on the subject is the excellent book of Stichtenoth [49].

Let $\mathbf{F}_q$ be the finite field of order q. An extension field F of $\mathbf{F}_q$ is called a **global function field** over $\mathbf{F}_q$ if there exists an element x of F that is transcendental over $\mathbf{F}_q$ and such that F is a finite extension of $\mathbf{F}_q(x)$. Furthermore, $\mathbf{F}_q$ is called the **full constant field** of F if $\mathbf{F}_q$ is algebraically closed in F. For brevity, we simply denote by $F/\mathbf{F}_q$ a global function field F with full constant field $\mathbf{F}_q$.

A **place** P of F is, by definition, the maximal ideal of some valuation ring of F. We denote by O_P the valuation ring corresponding to P and we denote by $\mathbf{P}_F$ the set of places of F.

For a place P of F, we write ν_P for the normalised discrete valuation of F corresponding to P, and any element $t \in F$ with $\nu_P(t) = 1$ is called a **local parameter** at P.

The residue class field O_P/P is denoted by $\tilde{F}_P$ and the **degree** of a place P is defined as

$$\deg(P) = [\tilde{F}_P : \mathbf{F}_q].$$

A place of degree 1 is called a **rational place**.

For a place P of F and $f \in F$ with $\nu_P(f) \geq 0$, the residue class $f + P$ of f in $\tilde{F}_P$ is denoted by $f(P)$.

A **divisor** D of a global function field $F/\mathbf{F}_q$ is a formal sum

$$D = \sum_{P \in \mathbf{P}_F} m_P P$$

with integer coefficients m_P and $m_P \neq 0$ for at most finitely many $P \in \mathbf{P}_F$. We write $\nu_P(D)$ for the coefficient m_P of P. The **support** of D is the set of P for which $\nu_P(D)$ is nonzero and we denote it by $\mathrm{supp}(D)$. We denote by $\mathrm{Div}(F)$ the set of divisors of $F/\mathbf{F}_q$.

The **degree** of a divisor $D = \sum_{P \in \mathbf{P}_F} \nu_P(D)P$ is given by

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

For $f \in F^*$ the **principal divisor** of f is given by

$$\mathrm{div}(f) = \sum_{P \in \mathbf{P}_F} \nu_P(f)P.$$

Since $\deg(\mathrm{div}(f)) = 0$ for any $f \in F^*$, we have

$$\mathrm{Princ}(F) := \{\mathrm{div}(f) : f \in F^*\} \subseteq \mathrm{Div}^0(F) := \{D \in \mathrm{Div}(F) : \deg(D) = 0\}.$$

We let

$$\mathrm{Cl}(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F),$$

which is a finite abelian group and is called the **group of divisor classes of degree 0** of F. The cardinality of $\mathrm{Cl}(F)$ is called the **divisor class number** of F, denoted by $h(F)$.

For a global function field $F/\mathbf{F}_q$ we define its set of **differentials** as

$$\Omega_F = \{x\,dz : x \in F, z \text{ is a separating element for } F/\mathbf{F}_q\},$$

and for any differential $\omega \in \Omega_F$ and separating element z we can write $\omega = x\,dz$ with a unique $x \in F$.

Let P be a rational place of F with a local parameter t. Since any local parameter is a separating element (see [49, Proposition III.9.2]), for a differential ω we can write $\omega = x\,dt$ and furthermore we have a unique expansion of the form

$$x = \sum_{n=r}^{\infty} a_n t^n,$$

where $r \in \mathbf{Z}$ and $a_n \in \mathbf{F}_q$. The residue of ω at P with respect to t is simply the coefficient a_{-1} in the above expansion. Furthermore, this is independent of the choice of t and hence we refer to the **residue** of ω at P, which we denote by $\mathrm{res}_P(\omega)$.

For a place P of F with a local parameter t and a nonzero differential $\omega = x\,dt$ we set $\nu_P((x\,dt)) := \nu_P(x)$. Furthermore, this is independent of the choice of t, hence $\nu_P((\omega))$ is meaningful and defines a divisor (ω).

For any divisor D of F we define the following sets of functions and differentials

$$\mathcal{L}(D) = \{f \in F^* : \mathrm{div}(f) \geq -D\} \cup \{0\},$$
$$\Omega(D) = \{\omega \in \Omega \backslash \{0\} : (\omega) \geq D\} \cup \{0\}.$$

We call $\mathcal{L}(D)$ the **Riemann-Roch space** of D. Both $\mathcal{L}(D)$ and $\Omega(D)$ can be shown to be vector spaces over $\mathbf{F}_q$.

We define the **genus** of F as the integer

$$g := \max_D(\deg(D) - \dim \mathcal{L}(D) + 1),$$

where the maximum is extended over all divisors D of F.

A divisor W of the form (ω) for some nonzero differential ω is called **canonical** and all such divisors satisfy $\deg(W) = 2g - 2$. Furthermore, all canonical divisors of $F/\mathbf{F}_q$ are equivalent, i.e., for divisors D_1, D_2 of F we have $D_1 = D_2 + \mathrm{div}(f)$ for some $f \in F^*$ and in such a case we write

$$D_1 \sim D_2.$$

We also have $\Omega(D) \simeq \mathcal{L}(W - D)$ for any canonical divisor W of F.

Let g be the genus of $F/\mathbf{F}_q$, then we know by the Riemann-Roch theorem that for any divisor D we have

$$\dim \mathcal{L}(D) \begin{cases} = \deg(D) + 1 - g & \text{if } \deg(D) \geq 2g - 1, \\ \geq \deg(D) + 1 - g & \text{if } 0 \leq \deg(D) \leq 2g - 2, \\ = 0 & \text{if } \deg(D) \leq -1. \end{cases}$$

Since

$$\dim \Omega(D) = \dim \mathcal{L}(D) - \deg(D) + g - 1,$$

we also have

$$\dim \Omega(D) \begin{cases} = 0 & \text{if } \deg(D) \geq 2g-1, \\ \geq 0 & \text{if } 0 \leq \deg(D) \leq 2g-2, \\ = g-1-\deg(D) & \text{if } \deg(D) \leq -1. \end{cases}$$

For $k \geq 0$ let $\mathcal{A}_k(F)$ be the set of positive divisors of F of degree k and let $A_k(F) = |\mathcal{A}_k(F)|$. Details for calculating $A_k(F)$ are given in [49, Section V.1] and [39, Section 1.6]. For $r \geq 1$ let $B_r(F)$ be the number of places of F of degree r. Finally, we let $N(F) := A_1(F) = B_1(F)$ be the number of rational places of F.

Definition 2.1. For a given prime power q and an integer $g \geq 0$, let $N_q(g)$ denote the maximum number of rational places that a global function field $F/\mathbf{F}_q$ of genus g can have.

The Hasse-Weil bound implies that $N_q(g) = O(g)$. More specifically, Serre [44] proved that

$$N_q(g) \leq q + 1 + g\lfloor 2q^{1/2} \rfloor,$$

and hence the following definition of Ihara [17] is meaningful.

Definition 2.2. For any prime power q define

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

The following bound due to Vlăduţ and Drinfeld [54] was found soon after the introduction of the previous definition.

Theorem 2.3 (Vlăduţ-Drinfeld Bound). *For every prime power q we have*

$$A(q) \leq q^{1/2} - 1.$$

This remains the best known bound and in fact it is best possible in the case where q is a square, since it was shown by Ihara [17] that we have $A(q) \geq q^{1/2} - 1$ for square q. Garcia and Stichtenoth [9] later introduced explicit towers of function fields obtaining this bound for all square q.

A more recent paper of Bezerra, Garcia, and Stichtenoth [1] showed that

$$A(q) \geq \frac{2(q^{2/3} - 1)}{q^{1/3} + 2}$$

when q is a cube.

2.2 Algebraic Coding Theory

A **code** C over $\mathbf{F}_q$ is a nonempty subset of $\mathbf{F}_q^n$ for some $n \geq 1$. The number n is the **length** of C. An element of C is called a **codeword** and $K := |C|$ is the number of codewords of C. The **information rate** R of the code is defined to be

$$R = \frac{\log_q K}{n}.$$

If a code $C \subseteq \mathbf{F}_q^n$ is a nonzero $\mathbf{F}_q$-linear subspace of $\mathbf{F}_q^n$ then it is called a **linear code** over $\mathbf{F}_q$ and its dimension over $\mathbf{F}_q$ is called the **dimension** of C which we denote by k.

For $\mathbf{x} \in \mathbf{F}_q^n$ the **(Hamming) weight** $w(\mathbf{x})$ is the number of nonzero coordinates of $\mathbf{x}$. For $\mathbf{x}, \mathbf{y} \in \mathbf{F}_q^n$ the **(Hamming) distance** $d(\mathbf{x}, \mathbf{y})$ is given by

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}).$$

For a code C with $K \geq 2$, we define its **minimum distance**

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

and its **relative minimum distance**

$$\delta = \frac{d}{n}.$$

We refer to (n, K, d) codes and linear $[n, k, d]$ codes.

For a given prime power q, let U_q be the set of points (δ, R) in the unit square $[0, 1]^2$ for which there exists a sequence of (n_i, K_i, d_i) codes over $\mathbf{F}_q$ with $i \geq 1$ such that $n_i \to \infty$ as $i \to \infty$ and

$$\lim_{i\to\infty} \frac{d_i}{n_i} = \delta, \quad \lim_{i\to\infty} \frac{\log_q K_i}{n_i} = R.$$

The following nonincreasing continuous function was introduced by Manin [22] for linear $[n_i, k_i, d_i]$ codes over $\mathbf{F}_q$. He later refined the idea [55, Chapter I] to include sequences of nonlinear codes in U_q, which is the definition we have taken.

Definition 2.4. For a given prime power q, put

$$\alpha_q(\delta) = \sup\{R \in [0, 1] : (\delta, R) \in U_q\} \quad \text{for } 0 \leq \delta \leq 1.$$

The classical lower bound on α_q is the following theorem.

Theorem 2.5 (Asymptotic Gilbert-Varshamov Bound). *For any prime power q we have*

$$\alpha_q(\delta) \geq R_{\mathrm{GV}}(q, \delta) := 1 - \delta \log_q(q - 1) + \delta \log_q \delta + (1 - \delta) \log_q(1 - \delta)$$

for $0 < \delta \leq (q - 1)/q$ and $\alpha_q(0) = R_{\mathrm{GV}}(q, 0) := 1$.

As we mentioned in the introduction, a major breakthrough was made by Goppa when he introduced the following class of codes.

Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let G be a divisor of F with $\operatorname{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Then it is meaningful to define an $\mathbf{F}_q$-linear map $\psi : \mathcal{L}(G) \to \mathbf{F}_q^n$ by

$$\psi(f) = (f(P_1), \ldots, f(P_n)) \quad \text{for all } f \in \mathcal{L}(G).$$

The image of ψ is denoted by $C(P_1, \ldots, P_n; G)$ and we call this class of codes **Goppa's algebraic-geometry codes**. These codes' parameters can be bounded by the following theorem (see, for example, [49, Corollary II.2.3]).

Theorem 2.6. *Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least $n \geq g+1$ distinct rational places $P_1, \ldots, P_n$. Let G be a divisor of F with $g \leq \deg(G) < n$ and $\operatorname{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Then $C(P_1, \ldots, P_n; G)$ is a linear $[n, k, d]$ code over $\mathbf{F}_q$ with*

$$k \geq \deg(G) - g + 1, \quad d \geq n - \deg(G).$$

Goppa's algebraic-geometry codes are not the only class of codes to make use of algebraic geometry. For example, we have the following generalisation due to Xing, Niederreiter, and Lam [61].

Let $F/\mathbf{F}_q$ be a global function field of genus g and with r distinct places $P_1, \ldots, P_r$. Let G be a divisor of F with $\operatorname{supp}(G) \cap \{P_1, \ldots, P_r\} = \emptyset$. For $i = 1, \ldots, r$, let C_i be a linear $[n_i, k_i \geq \deg(P_i), d_i]$ code over $\mathbf{F}_q$ and let ϕ_i be a fixed $\mathbf{F}_q$-linear monomorphism from the residue class field of P_i to the linear code C_i. Put

$$n = \sum_{i=1}^{r} n_i.$$

Then it is meaningful to define an $\mathbf{F}_q$-linear map $\beta : \mathcal{L}(G) \to \mathbf{F}_q^n$ by

$$\beta(f) = (\phi_1(f(P_1)), \ldots, \phi_r(f(P_r))) \quad \text{for all } f \in \mathcal{L}(G).$$

The image of β is denoted by $C(P_1, \ldots, P_r; G; C_1, \ldots, C_r)$ and we call this class of codes **XNL codes**.

Theorem 2.7. *Let $F/\mathbf{F}_q$ be a global function field of genus g and let $P_1, \ldots, P_r$ be distinct places of F. For $i = 1, \ldots, r$, let C_i be a linear $[n_i, k_i \geq \deg(P_i), d_i]$ code over $\mathbf{F}_q$. Let G be a divisor of F with $\operatorname{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$ and*

$$g \leq \deg(G) < \sum_{i=1}^{r} \deg(P_i).$$

Then $C(P_1, \ldots, P_n; G; C_1, \ldots, C_r)$ is a linear $[n, k, d]$ code over $\mathbf{F}_q$ with

$$n = \sum_{i=1}^{r} n_i, \quad k \geq \deg(G) - g + 1, \quad d \geq d_0,$$

where d_0 is the minimum of $\sum_{i \in M'} d_i$ taken over all subsets M of $\{1, \ldots, r\}$ for which $\sum_{i \in M} \deg(P_i) \leq \deg(G)$, with M' denoting the complement of M in $\{1, \ldots, r\}$.

The question as to whether it was possible to construct sequences of codes which beat the asymptotic Gilbert-Varshamov bound was an open problem for many years, and some mathematicians believed it to be impossible. It was thus a major result when Tsfasman, Vlăduţ, and Zink [52] demonstrated that Goppa's algebraic-geometry codes produced the bound

$$\alpha_q(\delta) \geq R_{\mathrm{TVZ}}(q, \delta) := 1 - \frac{1}{A(q)} - \delta \quad \text{for } 0 \leq \delta \leq 1,$$

which improves on the asymptotic Gilbert-Varshamov bound for some interval for all square prime powers $q \geq 49$.

The next improvements were made by Vlăduţ [53] and Xing [57] who introduced the ideas of considering distinguished line bundles and distinguished divisors, respectively. These improvements occur around the two intersection points of the Gilbert-Varshamov and Tsfasman-Vlăduţ-Zink bounds and are not global.

The development which led to global improvements on the Tsfasman-Vlăduţ-Zink bound was the consideration of nonlinear algebraic-geometry codes, which was instigated by Elkies [5]. This was later refined by Xing [58] who introduced the idea of using local expansions to create nonlinear codes which produced the bound

$$\alpha_q(\delta) \geq R_{\mathrm{X}}(q,\delta) := 1 - \frac{1}{A(q)} - \delta + \sum_{i=2}^{\infty} \log_q \left(1 + \frac{q-1}{q^{2i}}\right) \quad \text{for } 0 \leq \delta \leq 1.$$

Niederreiter and Özbudak [29] then expanded on Xing's idea by using more terms in the local expansion to produce nonlinear codes with the bound

$$\alpha_q(\delta) \geq R_{\mathrm{N\ddot{O}}}(q,\delta) := 1 - \frac{1}{A(q)} - \delta + \log_q \left(1 + \frac{1}{q^3}\right) \quad \text{for } 0 \leq \delta \leq 1.$$

This was also shown in the case where q is a square by Elkies [6], and Stichtenoth and Xing [50] later gave a simpler proof of Niederreiter and Özbudak's bound.

More recently, Niederreiter and Özbudak [30] introduced a construction which combines Xing's idea of considering two terms of the local expansion of functions in a Riemann-Roch space with the idea of using a distinguished divisor. It can be shown that this improves on Xing's construction using distinguished divisors. We note that Vlăduţ's bound based on distinguished line bundles is in some instances better than Niederreiter and Özbudak's bounds. Thus, for any values of q and δ, the best known bound can be obtained by considering the Gilbert-Varshamov, Vlăduţ [53], and Niederreiter-Özbudak [29], [30] bounds.

2.3 Low-Discrepancy Sequences

The most powerful known methods for the construction of low-discrepancy point sets and sequences are based on the theory of (t, m, s)-nets and (t, s)-sequences, which are point sets, respectively sequences, satisfying strong uniformity properties in the half-open s-dimensional unit cube $[0, 1)^s$. We note that by a point set we mean a multiset, i.e., a set in which multiplicities of elements are allowed and taken into account.

For a subinterval J of $[0, 1)^s$ and for a point set P consisting of N points $\mathbf{x}_1, \ldots, \mathbf{x}_N \in [0, 1)^s$ we write $A(J; P)$ for the number of integers n with $1 \leq n \leq N$ for which $\mathbf{x}_n \in J$. We then put

$$R(J; P) = \frac{A(J; P)}{N} - \mathrm{Vol}(J).$$

Definition 2.8. The **star discrepancy** $D_N^*(P)$ of the point set P is defined by

$$D_N^*(P) = \sup_J |R(J; P)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^s$ with one vertex at the origin. For a sequence S of points in $[0, 1)^s$, the **star discrepancy** $D_N^*(S)$ is meant to be the star discrepancy of the first N terms of S.

Definition 2.9. A sequence S of points in $[0,1)^s$ is called a **low-discrepancy sequence** if

$$D_N^*(S) = O(N^{-1}(\log N)^s) \qquad \text{for all } N \geq 2.$$

The desire to minimise the star discrepancy and produce low-discrepancy sequences led to the introduction of (t,m,s)-nets and (t,s)-sequences. Sobol' [48] first constructed (t,s)-sequences in base 2 and Faure [8] later considered $(0,s)$-sequences in prime base $b \geq s$. The following general definitions were given by Niederreiter [23].

Definition 2.10. For integers $b \geq 2$, $s \geq 1$, and $0 \leq t \leq m$, a (t,m,s)**-net in base** b is a point set P consisting of b^m points in $[0,1)^s$ such that every subinterval of $[0,1)^s$ of the form

$$\prod_{i=1}^{s}[a_i b^{-d_i}, (a_i+1)b^{-d_i})$$

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$, and of volume b^{t-m} contains exactly b^t points of P.

For a base $b \geq 2$ we write $Z_b = \{0,1,\ldots,b-1\}$ for the set of digits in base b. Given a real number $x \in [0,1)$, let

$$x = \sum_{j=1}^{\infty} y_j b^{-j} \quad \text{with all } y_j \in Z_b$$

be a b-adic expansion of x, where the case $y_j = b-1$ for all but finitely many j is allowed. For an integer $m \geq 1$ we define the truncation

$$[x]_{b,m} = \sum_{j=1}^{m} y_j b^{-j}.$$

If $\mathbf{x} = (x^{(1)}, \dots, x^{(s)}) \in [0,1)^s$ and the $x^{(i)}$, $1 \le i \le s$, are given by prescribed b-adic expansions, then we define

$$[\mathbf{x}]_{b,m} = \Big([x^{(1)}]_{b,m}, \dots, [x^{(s)}]_{b,m}\Big).$$

Definition 2.11. Let $s \ge 1$, $b \ge 2$, and $t \ge 0$ be integers. A sequence $\mathbf{x}_0, \mathbf{x}_1, \dots$ of points in $[0,1)^s$ is a (t,s)**-sequence in base** b if for all integers $k \ge 0$ and $m > t$ the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \le n < (k+1)b^m$ form a (t,m,s)-net in base b.

The following theorem is due to Niederreiter [23].

Theorem 2.12. *The star discrepancy $D_N^*(S)$ of the first N terms of a (t,s)-sequence S in base b satisfies*

$$D_N^*(S) \le \frac{b^t}{s!} \cdot \frac{b-1}{2\lfloor b/2 \rfloor}\left(\frac{\lfloor b/2 \rfloor}{\log b}\right)^s \frac{(\log N)^s}{N} + O\left(\frac{b^t (\log N)^{s-1}}{N}\right) \quad \text{for all } N \ge 2.$$

Hence, it is clear that any (t,s)-sequence in base b is a low-discrepancy sequence.

Low-discrepancy sequences were of interest from a purely academic point of view. However, it was after Koksma [18] showed that there were important applications to numerical analysis that interest really peaked. The following important theorem was proved by Koksma [18] for $s = 1$ and by Hlawka [16] for general s.

Theorem 2.13 (Koksma-Hlawka Inequality). *If f has bounded variation $V(f)$ on $[0,1]^s$ in the sense of Hardy and Krause, then, for any $\mathbf{x}_1, \dots, \mathbf{x}_N \in [0,1)^s$, we have*

$$\left| \int_{[0,1]^s} f(\mathbf{u})\, d\mathbf{u} - \frac{1}{N}\sum_{n=1}^{N} f(\mathbf{x}_n) \right| \le V(f) D_N^*(P),$$

where $D_N^*(P)$ is the star discrepancy of the point set P formed by $\mathbf{x}_1, \ldots, \mathbf{x}_N$.

If $V(f)$ is finite and we have a sequence S in $[0,1)^s$ such that

$$\lim_{N\to\infty} D_N^*(S) = 0,$$

then we get a convergent numerical integration scheme, i.e.,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\mathbf{x}_n) = \int_{[0,1]^s} f(\mathbf{u})\, d\mathbf{u}.$$

It is clear by Theorem 2.12 that (t,s)-sequences (and indeed all low-discrepancy sequences) satisfy the condition $\lim_{N\to\infty} D_N^*(S) = 0$.

For a (t,s)-sequence in base b, smaller values of t provide smaller upper bounds on the star discrepancy. This leads us to the following definition first given by Niederreiter [23].

Definition 2.14. For given integers $b \geq 2$ and $s \geq 1$, let $t_b(s)$ be the least value of t for which there exists a (t,s)-sequence in base b.

In practical problems such as option pricing in mathematical finance, the dimension of the integration domain may be large. Thus, we would like to be able to bound $t_b(s)$ for arbitrarily large s. This was first done by Niederreiter [24] who showed that we have

$$t_b(s) = O(s \log s).$$

This was later improved by Niederreiter and Xing [33], who used global function fields to show that

$$t_b(s) = O(s).$$

In view of the fact that Niederreiter and Xing [34, Theorem 8] proved that

$$t_b(s) \geq \frac{s}{b} - \log_b \frac{(b-1)s+b+1}{2},$$

we see that $t_b(s) = O(s)$ is the best bound possible.

Most of the known constructions of (t,m,s)-nets and (t,s)-sequences are based on the so-called digital method. We refer to (t,m,s)-nets and (t,s)-sequences which are constructed via the digital method as digital (t,m,s)-nets and digital (t,s)-sequences. The method was developed by Niederreiter [23] and we do not replicate it here. Suitable expositions are available in the books of Niederreiter [25, Chapter 4] and Niederreiter and Xing [39, Chapter 8]. For our new constructions in Chapters 7 and 8 we will, however, need some results.

Niederreiter and Pirsic [31] showed that the problem of constructing a digital (t,m,s)-net over $\mathbf{F}_q$ can be reduced to the problem of constructing certain $\mathbf{F}_q$-linear subspaces of $\mathbf{F}_q^{ms}$. For this purpose, $\mathbf{F}_q^{ms}$ is endowed with a weight function which then determines the quality parameter t of the digital net.

First, we define a weight function v on $\mathbf{F}_q^m$ by putting $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0} \in \mathbf{F}_q^m$, and for $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbf{F}_q^m$ with $\mathbf{a} \neq \mathbf{0}$ we set

$$v(\mathbf{a}) = \max\{j : a_j \neq 0\}.$$

Then we extend this definition to $\mathbf{F}_q^{ms}$ by writing a vector $\mathbf{A} \in \mathbf{F}_q^{ms}$ as the concatenation of s vectors of length m, i.e.,

$$\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathbf{F}_q^{ms} \quad \text{with} \quad \mathbf{a}^{(i)} \in \mathbf{F}_q^m \quad \text{for} \quad 1 \leq i \leq s,$$

and putting

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}).$$

Definition 2.15. For any nonzero $\mathbf{F}_q$-linear subspace $\mathcal{N}$ of $\mathbf{F}_q^{ms}$ we define the **minimum distance**

$$\delta_m(\mathcal{N}) = \min_{\mathbf{A}\in\mathcal{N}\setminus\{\mathbf{0}\}} V_m(\mathbf{A}).$$

Theorem 2.16. *Let q be a prime power and let $m \geq 1$ and $s \geq 2$ be integers. Then from any $\mathbf{F}_q$-linear subspace $\mathcal{N}$ of $\mathbf{F}_q^{ms}$ with $\dim(\mathcal{N}) \geq ms - m$ we can construct a digital (t, m, s)-net over $\mathbf{F}_q$ with $t = m + 1 - \delta_m(\mathcal{N})$.*

We can construct digital (t, s)-sequences over $\mathbf{F}_q$ using the following method.

Let $s \geq 1$ and choose elements $c_{r,j}^{(i)} \in \mathbf{F}_q$ for $1 \leq i \leq s$, $j \geq 1$, and $r \geq 0$. Let

$$\mathbf{c}_j^{(i)} = (c_{0,j}^{(i)}, c_{1,j}^{(i)}, \ldots) \in \mathbf{F}_q^{\infty} \quad \text{for } 1 \leq i \leq s \text{ and } j \geq 1,$$

which are collected in the two-parameter system

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} \in \mathbf{F}_q^{\infty} : 1 \leq i \leq s \text{ and } j \geq 1\}.$$

For $m \geq 1$ we define the projection

$$\pi_m : (c_0, c_1, \ldots) \in \mathbf{F}_q^{\infty} \mapsto (c_0, \ldots, c_{m-1}) \in \mathbf{F}_q^{m},$$

and we put

$$C^{(m)} = \{\pi_m(\mathbf{c}_j^{(i)}) \in \mathbf{F}_q^{m} : 1 \leq i \leq s, 1 \leq j \leq m\}.$$

Then we have the following theorem.

Theorem 2.17. *The system $C^{(\infty)}$ can be used to create a digital (t, s)-sequence if, for any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = m - t$, the vectors $\pi_m(\mathbf{c}_j^{(i)})$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, are linearly independent for all $m > t$.*

Finally, we give the following definition which is analogous to Definition 2.14.

Definition 2.18. For a given prime power q and any integer $s \geq 1$, let $d_q(s)$ be the least value of t for which there exists a digital (t, s)-sequence constructed over $\mathbf{F}_q$.

Chapter 3

Asymptotic Bounds for XNL Codes

The idea of using places of arbitrary degree to construct algebraic-geometry codes is due to Niederreiter, Xing, and Lam [41] who introduced a class of codes which we call NXL codes. This was followed by a paper of Xing, Niederreiter, and Lam [61] which introduced the XNL codes detailed in Section 2.2. It was later shown by Özbudak and Stichtenoth [42] that the NXL codes can be viewed as a special case of the more general XNL code construction. In fact, the XNL codes can be viewed as a special case of the class of codes known as function-field codes, which were defined by Hachenberger, Niederreiter, and Xing [14].

The main motivation for these codes is the fact that for small values of q, global function fields $F/\mathbf{F}_q$ generally have few rational places relative to the genus of F. Ding, Niederreiter, and Xing [3] carried out a search for XNL codes which produced many good results. However, as yet there has been no examination of the asymptotic properties of these codes. In this chapter we fill that void by demonstrating that, for small q, XNL codes do indeed produce global improvements upon the Tsfasman-Vlăduţ-Zink bound. Furthermore, we show that for any q there is a range where XNL codes beat the Tsfasman-Vlăduţ-Zink bound.

3.1 The General Asymptotic Bound

Before gaining specific bounds on α_q we must decide which places we wish to use. For presentational purposes, we will use all places of degree l and m for our definitions and theorem. However, analogous results obviously hold if we choose only rational places, only places of degree 2, or places of degree l, m, and n, etc.

We emphasise that throughout this section we fix positive integers l and m. Now fix a prime power q. For a global function field $F/\mathbf{F}_q$ let us associate all places of degree l with a fixed linear $[\overline{n}_l, \overline{k}_l \geq l, \overline{d}_l]$ code over $\mathbf{F}_q$ and all places of degree m with a fixed linear $[\overline{n}_m, \overline{k}_m \geq m, \overline{d}_m]$ code over $\mathbf{F}_q$. Suppose that we have $\gamma := l/\overline{d}_l = m/\overline{d}_m$, then we proceed as follows.

Definition 3.1. For the given prime power q and an integer $g \geq 1$, let $M_q(g)$ denote the maximum value of

$$\frac{\overline{n}_l B_l(F) + \overline{n}_m B_m(F)}{g(F) + (\overline{n}_l - \gamma\overline{d}_l)B_l(F) + (\overline{n}_m - \gamma\overline{d}_m)B_m(F)}$$

that a global function field $F/\mathbf{F}_q$ of genus g can have.

Definition 3.2. For the given prime power q define

$$B(q) = \limsup_{g\to\infty} M_q(g).$$

Then we have the following theorem.

Theorem 3.3. *For the given prime power q we have*

$$\alpha_q(\delta) \geq 1 - \frac{1}{B(q)} - \gamma\delta \qquad for\ 0 \leq \delta \leq 1.$$

Proof. Assume $B(q) > 1$ and $0 < \gamma\delta < 1 - B(q)^{-1}$, for otherwise it is trivial. Let $F_1, F_2, ...$ be a sequence of global function fields over $\mathbf{F}_q$ satisfying

$$\lim_{i\to\infty} g(F_i) = \infty \quad \text{and}$$

$$\lim_{i\to\infty} \frac{\overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i)}{g(F_i) + (\overline{n}_l - \gamma\overline{d}_l)B_l(F_i) + (\overline{n}_m - \gamma\overline{d}_m)B_m(F_i)} = B(q).$$

Note that

$$\lim_{i\to\infty} \frac{g(F_i) - \gamma(\overline{d}_l B_l(F_i) + \overline{d}_m B_m(F_i))}{\overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i)} = \frac{1}{B(q)} - 1 < -\gamma\delta < 0$$

Therefore, for sufficiently large i, we may choose integers r_i where $g(F_i) < r_i < \gamma(\overline{d}_l B_l(F_i) + \overline{d}_m B_m(F_i))$ and

$$\lim_{i\to\infty} \frac{r_i - \gamma(\overline{d}_l B_l(F_i) + \overline{d}_m B_m(F_i))}{\overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i)} = -\gamma\delta.$$

For sufficiently large i, we let G_i be a divisor of F_i with $\deg(G_i) = r_i$ where the support of G_i is disjoint from the places of degree l and m of F_i. Then, for sufficiently large i, we can associate each global function field F_i with an XNL code $C(P_1, ..., P_{B_l(F_i)+B_m(F_i)}; G_i; [\overline{n}_l, \overline{k}_l, \overline{d}_l], ..., [\overline{n}_m, \overline{k}_m, \overline{d}_m])$. Thus, for sufficiently large i, we obtain a sequence of linear $[n_i, k_i, d_i]$ codes over $\mathbf{F}_q$ with

$$n_i = \overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i),$$

$$k_i \geq r_i - g(F_i) + 1,$$

$$d_i \geq \overline{d}_l B_l(F_i) + \overline{d}_m B_m(F_i) - r_i/\gamma.$$

By passing, if necessary, to a subsequence, we can assume that the limits

$$R := \lim_{i\to\infty} \frac{k_i}{n_i} \quad \text{and} \quad \delta' := \lim_{i\to\infty} \frac{d_i}{n_i}$$

exist. It follows that

$$R \geq \lim_{i\to\infty} \frac{r_i - g(F_i) + 1}{\overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i)} = 1 - \frac{1}{B(q)} - \gamma\delta \quad \text{and}$$

$$\delta' \geq \lim_{i\to\infty} \frac{\overline{d}_l B_l(F_i) + \overline{d}_m B_m(F_i) - r_i/\gamma}{\overline{n}_l B_l(F_i) + \overline{n}_m B_m(F_i)} = \delta.$$

Therefore

$$\alpha_q(\delta) \geq \alpha_q(\delta') \geq R \geq 1 - \frac{1}{B(q)} - \gamma\delta$$

since α_q is nonincreasing. □

3.2 Explicit Asymptotic Bounds

We now provide some explicit bounds by specifically choosing places and codes.

Example 3.4. Let us associate all the places of degree 2 with the $[2, 2, 1]$ code that exists for all q. Then $\gamma = 2$ and

$$M_q(g) = \max_F \frac{2B_2(F)}{g(F)}.$$

If we combine results on constant field extensions [49, Lemma V.1.9] with a tower of function fields due to Garcia and Stichtenoth [9], it is clear that for all prime powers q there exists a tower of function fields $\mathcal{F} = (F_1, F_2, ...)$ over $\mathbf{F}_q$ satisfying

$$\lim_{i\to\infty} \frac{N(F_i) + 2B_2(F_i)}{g(F_i)} = q - 1.$$

Therefore, in this case

$$B(q) \geq q - 1 - (q^{1/2} - 1) = q - q^{1/2},$$

and hence for all prime powers q we have

$$\alpha_q(\delta) \geq R_{\mathrm{XNL1}}(q, \delta) := 1 - \frac{1}{q - q^{1/2}} - 2\delta,$$

for $0 \leq \delta \leq 1$.

This bound is meaningful for all values of q except the binary case. Clearly we have $R_{\mathrm{XNL1}}(q, \delta) > R_{\mathrm{TVZ}}(q, \delta)$ for $\delta < q^{-1/2}$, so the Tsfasman-Vlăduţ-Zink bound can always be improved upon for some interval.

Example 3.5. Let us associate all the places of degree 1 with the $[1, 1, 1]$ code that exists for all q and all the places of degree 2 with the $[3, 2, 2]$ code that exists for all q. Then $\gamma = 1$ and

$$M_q(g) = \max_F \frac{N(F) + 3B_2(F)}{g(F) + B_2(F)}.$$

We know that for all prime powers q there exists a tower of function fields $\mathcal{F} = (F_1, F_2, ...)$ over $\mathbf{F}_q$ satisfying

$$\lim_{i \to \infty} \frac{N(F_i) + 2B_2(F_i)}{g(F_i)} = q - 1.$$

Hence, for all prime powers q, there exists a tower of function fields $\mathcal{F} = (F_1, F_2, ...)$ over $\mathbf{F}_q$ satisfying

$$\begin{aligned}\lim_{i \to \infty} \frac{N(F_i) + 3B_2(F_i)}{g(F_i) + B_2(F_i)} &= 1 + \lim_{i \to \infty} \frac{N(F_i) + 2B_2(F_i) - g(F_i)}{g(F_i) + B_2(F_i)} \\ &= 1 + \lim_{i \to \infty} \frac{\frac{N(F_i)+2B_2(F_i)}{g(F_i)} - 1}{1 + \frac{B_2(F_i)}{g(F_i)}} \\ &\geq 1 + \frac{q-2}{1 + \frac{q-1}{2}} \\ &= \frac{3(q-1)}{q+1}.\end{aligned}$$

Therefore, in this case

$$B(q) \geq \frac{3(q-1)}{q+1},$$

and hence for all prime powers q we have

$$\alpha_q(\delta) \geq R_{\mathrm{XNL2}}(q,\delta) := 1 - \frac{q+1}{3(q-1)} - \delta$$

for $0 \leq \delta \leq 1$.

This bound is meaningful for all values of q except the binary case. It also offers a global improvement on the Tsfasman-Vlăduţ-Zink bound in the cases $q = 3$, 4, 5, 7, 8, 9, and 11.

Chapter 4

A New Construction of Algebraic-Geometry Codes

In this chapter we introduce a new construction of algebraic-geometry codes by combining two ideas. Firstly, we use the idea of considering a distinguished divisor, as in previous constructions due to Vlăduţ [53], Xing [57], and Niederreiter and Özbudak [30]. Secondly, we consider local expansions of certain functions, as in previous constructions due to Xing [58] and Niederreiter and Özbudak [29], [30]. We note that a paper of Niederreiter and Özbudak [30] uses both distinguished divisors and local expansions. However, it only uses the first two terms in the expansion, whereas we will generalise the idea by using arbitrarily many terms.

4.1 Distinguished Divisors for Algebraic-Geometry Codes

In this section we introduce the distinguished divisor we will need for our new construction of algebraic-geometry codes. We begin by extending [30, Proposition 2.1] with the following proposition, both of which can be viewed as special cases of [28, Lemma 5.1]. We include the proof for completeness.

Proposition 4.1. *Let $F/\mathbf{F}_q$ be a global function field of divisor class number h and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \ldots, x_m$ be positive real numbers. Let $s \leq (m+1)n$ be an integer. Let r be an integer with $r \geq s$. Let $\mathcal{U}(n, s, x_1, \ldots, x_m)$ be the set of divisors of F defined by*

$$\mathcal{U}(n, s, x_1, \ldots, x_m) = \Bigg\{ \sum_{i=1}^{n} l_i P_i : \sum_{i=1}^{n} l_i = s, 0 \leq l_i \leq m+1,$$
$$|\{i : l_i = 0\}| \leq 2\lfloor x_m n \rfloor, |\{i : l_i = 1\}| \leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor,$$
$$\ldots, |\{i : l_i = m-1\}| \leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor \Bigg\}.$$

Suppose that

$$|\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{r-s}(F) < h.$$

Then there exists a divisor G of F such that $\deg(G) = r$ *and* $\mathcal{L}(G - U) = \{0\}$ *for all $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$.*

Proof. Let Q be a rational place of F. Let $\mathcal{D}$ be the set of degree zero divisors given by

$$\mathcal{D} = \{U + A - rQ : U \in \mathcal{U}(n, s, x_1, \ldots, x_m), A \in \mathcal{A}_{r-s}(F)\}.$$

Note that

$$|\mathcal{D}| \leq |\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{r-s}(F) < h.$$

Therefore there exists a degree zero divisor D_0 of F such that

$$D_0 \not\sim D \quad \text{for all } D \in \mathcal{D}.$$

Let $G := D_0 + rQ$. We claim that

$$\mathcal{L}(G - U) = \{0\}$$

for all $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$. Suppose, on the contrary, that there exists $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$ and $f \in \mathcal{L}(G - U) \backslash \{0\}$. Then

$$E := \operatorname{div}(f) + G - U$$

is a positive divisor of degree $r - s$. Thus, $E \in \mathcal{A}_{r-s}(F)$ and

$$D_0 + \operatorname{div}(f) = U + E - rQ \in \mathcal{D},$$

which is a contradiction to the choice of D_0. □

Corollary 4.2. *Let $F/\mathbf{F}_q$ be a global function field of divisor class number h and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \ldots, x_m$ be positive real numbers. Let s be an integer with*

$$mn \leq s \leq (m+1)n$$

and r be an integer with $r \geq s$. Let $\mathcal{V}(n, s, x_1, \ldots, x_m)$ be the set of divisors of F defined by

$$\mathcal{V}(n, s, x_1, \ldots, x_m) = \Bigg\{ \sum_{i=1}^{n} l_i P_i : \sum_{i=1}^{n} l_i \geq s, 0 \leq l_i \leq m+1,$$
$$|\{i : l_i = 0\}| \leq 2\lfloor x_m n \rfloor, |\{i : l_i = 1\}| \leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor,$$
$$\ldots, |\{i : l_i = m-1\}| \leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor \Bigg\}.$$

Suppose that

$$|\mathcal{U}(n,s,x_1,\dots,x_m)|\cdot A_{r-s}(F)<h.$$

Then there exists a divisor G of F such that $\deg(G)=r$*,* $\mathcal{L}(G-V)=\{0\}$ *for all $V\in\mathcal{V}(n,s,x_1,\dots,x_m)$, and* $\operatorname{supp}(G)\cap\{P_1,\dots,P_n\}=\emptyset$*.*

Proof. Let G_1 be a divisor of degree r obtained by Proposition 4.1. Suppose that we have $V=\sum_{i=1}^{n}l_iP_i\in\mathcal{V}(n,s,x_1,\dots,x_m)$ of degree $s+t$. Then

$$\begin{aligned}|\{i:l_i=m+1\}|&=s+t-mn+m|\{i:l_i=0\}|+\cdots+|\{i:l_i=m-1\}|\\&\geq t.\end{aligned}$$

Hence, for t places P_i with coefficient $l_i=m+1$, we can change the coefficient to $l_i=m$ and find a divisor $U\in\mathcal{U}(n,s,x_1,\dots,x_m)$ such that $U\leq V$. Then $\mathcal{L}(G_1-V)\subseteq\mathcal{L}(G_1-U)=\{0\}$ and therefore

$$\mathcal{L}(G_1-V)=\{0\}\quad\text{for all } V\in\mathcal{V}(n,s,x_1,\dots,x_m).$$

Using the weak approximation theorem [49, Theorem I.3.1], for $1\leq i\leq n$ we obtain $f_i\in F$ such that

$$\nu_{P_j}(f_i)=\begin{cases}0 & \text{if } j\neq i,\\ 1 & \text{if } j=i.\end{cases}$$

Let $f=\prod_{i=1}^{n}f_i^{-\nu_{P_i}(G_1)}\in F^*$ and

$$G=G_1+\operatorname{div}(f).$$

As $G\sim G_1$, we get $\mathcal{L}(G-V)=\{0\}$ for all $V\in\mathcal{V}(n,s,x_1,\dots,x_m)$. Moreover, we have $\operatorname{supp}(G)\cap\{P_1,\dots,P_n\}=\emptyset$. □

4.2 The Basic Construction of Algebraic-Geometry Codes

We now give the new construction of nonlinear codes. Let $n \geq 1$ and $m \geq 1$ be integers. For $\mathbf{a} = (a_1^{(1)}, \ldots, a_m^{(1)}, \ldots, a_1^{(n)}, \ldots, a_m^{(n)}) \in \mathbf{F}_q^{mn}$, we define the subsets $I_m(\mathbf{a}), I_{m-1}(\mathbf{a}), \ldots, I_1(\mathbf{a})$ of $\{1, \ldots, n\}$ as

$$\begin{aligned} I_m(\mathbf{a}) &= \{i \in \{1, \ldots, n\} : a_m^{(i)} \neq 0\}, \\ I_{m-1}(\mathbf{a}) &= \{i \in \{1, \ldots, n\} : a_m^{(i)} = 0,\ a_{m-1}^{(i)} \neq 0\}, \\ &\vdots \\ I_1(\mathbf{a}) &= \{i \in \{1, \ldots, n\} : a_m^{(i)} = \cdots = a_2^{(i)} = 0,\ a_1^{(i)} \neq 0\}. \end{aligned}$$

For positive real numbers $x_1, \ldots, x_m$ with $x_1 + \cdots + x_m < 1$, let $M_{q,n}(x_1, \ldots, x_m)$ be the subset of $\mathbf{F}_q^{mn}$ defined as

$$M_{q,n}(x_1, \ldots, x_m) = \{\mathbf{a} \in \mathbf{F}_q^{mn} : |I_1(\mathbf{a})| = \lfloor x_1 n \rfloor, \ldots, |I_m(\mathbf{a})| = \lfloor x_m n \rfloor\}.$$

Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. For $i = 1, \ldots, n$, let t_i be a local parameter of F at P_i. Let G be a divisor of F of degree $r \geq mn + 2g - 1$ with $\mathrm{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Then for $f \in \mathcal{L}(G)$ and $i = 1, \ldots, n$, we have $\nu_{P_i}(f) \geq 0$ and hence the local expansion

$$f = f^{(0)}(P_i) + f^{(1)}(P_i)t_i + \cdots .$$

Let Φ be the linear map defined by

$$\begin{aligned} \Phi : \mathcal{L}(G) &\to \mathbf{F}_q^{mn} \\ f &\mapsto (f^{(m-1)}(P_1), \ldots, f^{(0)}(P_1), \ldots, f^{(m-1)}(P_n), \ldots, f^{(0)}(P_n)). \end{aligned}$$

Note that $\operatorname{Ker}\Phi = \mathcal{L}(G - m(P_1 + \cdots + P_n))$ and

$$\dim \operatorname{Ker}\Phi = r - mn + 1 - g.$$

Furthermore,

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

and hence Φ is surjective.

Let $N_{\mathcal{L}}(P_1, \ldots, P_n; G; x_1, \ldots, x_m) := \Phi^{-1}(M_{q,n}(x_1, \ldots, x_m))$ and note that

$$|N_{\mathcal{L}}(P_1, \ldots, P_n; G; x_1, \ldots, x_m)| = q^{r+1-g-mn}|M_{q,n}(x_1, \ldots, x_m)|.$$

Finally, let ϕ be the map defined by

$$\begin{aligned} \phi : N_{\mathcal{L}}(P_1, \ldots, P_n; G; x_1, \ldots, x_m) &\to \mathbf{F}_q^n \\ f &\mapsto (f^{(m)}(P_1), \ldots, f^{(m)}(P_n)). \end{aligned}$$

Theorem 4.3. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \ldots, x_m$ be positive real numbers with*

$$2\sum_{j=1}^{m}(j+1)x_j \leq 1.$$

Let s be an integer with

$$mn \leq s \leq (m+1)n - 2\sum_{j=1}^{m}(j+1)\lfloor x_j n \rfloor$$

and r be an integer with $r \geq s$. We assume further that

$$r \geq mn + 2g - 1$$

and

$$|\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{r-s}(F) < h.$$

Then there exists a divisor G of F with $\deg(G) = r$ *and* $\mathrm{supp}(G) \cap \{P_1, \dots, P_n\} = \emptyset$ *such that*

$$C_{\mathcal{L}}(P_1, \dots, P_n; G; x_1, \dots, x_m) := \phi(N_{\mathcal{L}}(P_1, \dots, P_n; G; x_1, \dots, x_m))$$

is a q-ary (n, K, d) code with

$$K = q^{r+1-g-mn} |M_{q,n}(x_1, \dots, x_m)|$$

and

$$d \geq (m+1)n + 1 - s - 2\sum_{j=1}^{m} (j+1) \lfloor x_j n \rfloor.$$

Proof. We know by Corollary 4.2 that there exists a divisor G of F with $\deg(G) = r$ and $\mathrm{supp}(G) \cap \{P_1 \dots, P_n\} = \emptyset$ such that

$$\mathcal{L}(G - V) = \{0\} \text{ for all } V \in \mathcal{V}(n, s, x_1, \dots, x_m).$$

Let $f_1, f_2 \in N_{\mathcal{L}}(P_1, \dots, P_n; G; x_1, \dots, x_m)$ be two distinct functions. Since $\mathrm{supp}(G) \cap \{P_1 \dots, P_n\} = \emptyset$, we have $\nu_{P_i}(f_1 - f_2) \geq 0$ for $1 \leq i \leq n$. Let $l_i(f_1 - f_2) = \min(m+1, \nu_{P_i}(f_1 - f_2))$ for $1 \leq i \leq n$. Let $V = l_1(f_1 - f_2)P_1 + \cdots + l_n(f_1 - f_2)P_n$.

Note that

$$\begin{aligned}
|\{i : l_i(f_1 - f_2) = 0\}| &= |\{i : \nu_{P_i}(f_1 - f_2) = 0\}| \\
&\leq |\{i : \nu_{P_i}(f_1) = 0\}| + |\{i : \nu_{P_i}(f_2) = 0\}| \\
&= 2\lfloor x_m n \rfloor, \\
|\{i : l_i(f_1 - f_2) = 1\}| &= |\{i : \nu_{P_i}(f_1 - f_2) = 1\}| \\
&\leq |\{i : \nu_{P_i}(f_1) = 1\}| + |\{i : \nu_{P_i}(f_2) = 1\}| \\
&\quad + |\{i : \nu_{P_i}(f_1) = \nu_{P_i}(f_2) = 0\}| \\
&\leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor, \\
&\vdots \\
|\{i : l_i(f_1 - f_2) = m - 1\}| &= |\{i : \nu_{P_i}(f_1 - f_2) = m - 1\}| \\
&\leq |\{i : \nu_{P_i}(f_1) = m - 1\}| \\
&\quad + |\{i : \nu_{P_i}(f_2) = m - 1\}| \\
&\quad + |\{i : \nu_{P_i}(f_1) = \nu_{P_i}(f_2) = m - 2\}| \\
&\quad + \cdots + |\{i : \nu_{P_i}(f_1) = \nu_{P_i}(f_2) = 0\}| \\
&\leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor.
\end{aligned}$$

Moreover, $f_1 - f_2 \in \mathcal{L}(G - V)\backslash\{0\}$ and hence we obtain

$$l_1(f_1 - f_2) + \cdots + l_n(f_1 - f_2) \leq s - 1.$$

Therefore, we obtain the following bound on $w(\phi(f_1 - f_2))$. Note that in our evaluation we will use a new calculation rather than the above individual results.

$$
\begin{aligned}
&(m+1)n+1-s\\
&\leq \sum_{i=1}^{n}(m+1-l_i(f_1-f_2))\\
&= |\{i : l_i(f_1-f_2)=m\}| + \sum_{\substack{i=1\\ l_i(f_1-f_2)\leq m-1}}^{n} (m+1-l_i(f_1-f_2))\\
&= |\{i : l_i(f_1-f_2)=m\}| + \sum_{\substack{i=1\\ l_i(f_1-f_2)\leq m-1\\ l_i(f_1)=l_i(f_2)}}^{n} (m+1-l_i(f_1-f_2))\\
&\quad + \sum_{\substack{i=1\\ l_i(f_1-f_2)\leq m-1\\ l_i(f_1)\neq l_i(f_2)}}^{n} (m+1-l_i(f_1-f_2))\\
&= |\{i : l_i(f_1-f_2)=m\}| + \sum_{\substack{i=1\\ l_i(f_1-f_2)\leq m-1\\ l_i(f_1)=l_i(f_2)}}^{n} (m+1-l_i(f_1-f_2))\\
&\quad + \sum_{\substack{i=1\\ l_i(f_1)\leq m-1\\ l_i(f_2)\geq l_i(f_1)+1}}^{n} (m+1-l_i(f_1)) + \sum_{\substack{i=1\\ l_i(f_2)\leq m-1\\ l_i(f_1)\geq l_i(f_2)+1}}^{n} (m+1-l_i(f_2)).
\end{aligned}
$$

Note that

$$
\sum_{\substack{i=1\\ l_i(f_1-f_2)\leq m-1\\ l_i(f_1)=l_i(f_2)}}^{n} (m+1-l_i(f_1-f_2)) \leq \sum_{\substack{i=1\\ l_i(f_1)\leq m-1\\ l_i(f_1)=l_i(f_2)}}^{n} (m+1-l_i(f_1)).
$$

Therefore

$$
\begin{aligned}
&(m+1)n+1-s\\
&\leq |\{i : l_i(f_1-f_2)=m\}| + \sum_{\substack{i=1\\ l_i(f_1)\leq m-1\\ l_i(f_1)=l_i(f_2)}}^{n} (m+1-l_i(f_1))\\
&\quad + \sum_{\substack{i=1\\ l_i(f_1)\leq m-1\\ l_i(f_2)\geq l_i(f_1)+1}}^{n} (m+1-l_i(f_1)) + \sum_{\substack{i=1\\ l_i(f_2)\leq m-1\\ l_i(f_1)\geq l_i(f_2)+1}}^{n} (m+1-l_i(f_2))\\
&\leq |\{i : l_i(f_1-f_2)=m\}|\\
&\quad + \sum_{\substack{i=1\\ l_i(f_1)\leq m-1}}^{n} (m+1-l_i(f_1)) + \sum_{\substack{i=1\\ l_i(f_2)\leq m-1}}^{n} (m+1-l_i(f_2))\\
&= |\{i : l_i(f_1-f_2)=m\}| + 4\lfloor x_1 n\rfloor + \cdots + 2(m+1)\lfloor x_m n\rfloor\\
&\leq w(\phi(f_1-f_2)) + 4\lfloor x_1 n\rfloor + \cdots + 2(m+1)\lfloor x_m n\rfloor,
\end{aligned}
$$

and hence

$$d \geq (m+1)n+1-s-2\sum_{j=1}^{m}(j+1)\lfloor x_j n\rfloor \geq 1.$$

Therefore, ϕ is injective and

$$K = |N_{\mathcal{L}}(P_1,\ldots,P_n;G;x_1,\ldots,x_m)| = q^{r+1-g-mn}|M_{q,n}(x_1,\ldots,x_m)|.$$

□

Chapter 5

Algebraic-Geometry Codes Using Differentials

When Goppa introduced his construction of algebraic-geometry codes, he did so using differentials. It later became convention to construct the dual of Goppa's codes by considering functions in a Riemann-Roch space, which was the approach we used in Chapter 2. More recently, new constructions of algebraic-geometry codes were introduced by Lam, Niederreiter, and Xing. Namely, NXL codes [41] and XNL codes [61], the latter being a generalisation of the former. After these new codes were introduced in 1999, an open question was whether there was an equivalent construction using differentials. This was independently shown to be true by Heydtmann [15] and Dorfer and Maharaj [4]. In this chapter we demonstrate that there is an equivalent construction using differentials to our construction in Chapter 4, which is of interest since it can be viewed as the most general currently known construction of algebraic-geometry codes using rational places.

5.1 Distinguished Divisors for Algebraic-Geometry Codes Using Differentials

In Section 4.1 we produced a distinguished divisor for functions in a Riemann-Roch space. We now prove the existence of a similar distinguished divisor for differentials.

Proposition 5.1. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \ldots, x_m$ be positive real numbers. Let $s \leq (m+1)n$ be an integer. Let r be an integer with $r \leq n - s + 2g - 2$. Let $\mathcal{U}(n, s, x_1, \ldots, x_m)$ be the set of divisors of F defined by*

$$\mathcal{U}(n, s, x_1, \ldots, x_m) = \Bigg\{ \sum_{i=1}^{n} l_i P_i : \sum_{i=1}^{n} l_i = s, 0 \leq l_i \leq m+1,$$

$$|\{i : l_i = 0\}| \leq 2\lfloor x_m n \rfloor, |\{i : l_i = 1\}| \leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor,$$

$$\ldots, |\{i : l_i = m-1\}| \leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor \Bigg\}.$$

Suppose that

$$|\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{n-r-s+2g-2}(F) < h.$$

Then there exists a divisor G of F of degree r such that

$$\Omega\Big(G - \sum_{i=1}^{n} P_i + U\Big) = \{0\}$$

for all $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$.

Proof. Let Q be a rational place of F. Let $\mathcal{D}$ be the set of degree zero divisors given by

$$\mathcal{D} = \{U + A - (n - r + 2g - 2)Q : U \in \mathcal{U}(n, s, x_1, \ldots, x_m), A \in \mathcal{A}_{n-r-s+2g-2}(F)\}.$$

Note that

$$|\mathcal{D}| \leq |\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{n-r-s+2g-2}(F) < h.$$

Therefore there exists a degree zero divisor D_0 of F such that

$$D_0 \not\sim D \quad \text{for all } D \in \mathcal{D}.$$

Let ω_1 be a nonzero differential of F and put

$$G := (\omega_1) - D_0 + \sum_{i=1}^{n} P_i - (n - r + 2g - 2)Q.$$

We claim that

$$\Omega\bigg(G - \sum_{i=1}^{n} P_i + U\bigg) = \{0\}$$

for all $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$. Suppose, on the contrary, that there exists $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$ and ω_2 such that

$$\omega_2 \in \Omega\bigg(G - \sum_{i=1}^{n} P_i + U\bigg)\backslash\{0\}.$$

Note that

$$\Omega\bigg(G - \sum_{i=1}^{n} P_i + U\bigg) \simeq \mathcal{L}\bigg((\omega_2) - G + \sum_{i=1}^{n} P_i - U\bigg)$$

and hence there exists a nonzero $f_1 \in F$ such that

$$f_1 \in \mathcal{L}\bigg((\omega_2) - G + \sum_{i=1}^{n} P_i - U\bigg).$$

Then

$$E := \text{div}(f_1) + (\omega_2) - G + \sum_{i=1}^{n} P_i - U$$

is a positive divisor of degree $n - r - s + 2g - 2$. Note that all canonical divisors are equivalent. Therefore

$$(\omega_2) = (\omega_1) + \text{div}(f_2)$$

for some $f_2 \in F$ and so

$$D_0 + \mathrm{div}(f_1 f_2) = U + E - (n - r + 2g - 2)Q \in \mathcal{D},$$

which is a contradiction to the choice of D_0. □

Corollary 5.2. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $n \geq 1$ distinct rational places $P_1, \dots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \dots, x_m$ be positive real numbers. Let s be an integer with*

$$mn \leq s \leq (m+1)n$$

and r be an integer with $r \leq n - s + 2g - 2$. Let $\mathcal{V}(n, s, x_1, \dots, x_m)$ be the set of divisors of F defined by

$$\mathcal{V}(n, s, x_1, \dots, x_m) = \Bigg\{ \sum_{i=1}^{n} l_i P_i : \sum_{i=1}^{n} l_i \geq s, 0 \leq l_i \leq m+1,$$
$$|\{i : l_i = 0\}| \leq 2\lfloor x_m n \rfloor, |\{i : l_i = 1\}| \leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor,$$
$$\dots, |\{i : l_i = m-1\}| \leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor \Bigg\}.$$

Suppose that

$$|\mathcal{U}(n, s, x_1, \dots, x_m)| \cdot A_{n-r-s+2g-2}(F) < h.$$

Then there exists a divisor G of F such that $\deg(G) = r$, $\mathrm{supp}(G) \cap \{P_1, \dots,$ $P_n\} = \emptyset$, and

$$\Omega\Big(G - \sum_{i=1}^{n} P_i + V\Big) = \{0\}$$

for all $V \in \mathcal{V}(n, s, x_1, \dots, x_m)$.

Proof. Let G_1 be a divisor of degree r obtained by Proposition 5.1. Suppose that we have $V \in \mathcal{V}(n, s, x_1, \ldots, x_m)$ of degree $s+t$. Then

$$\begin{aligned} |\{i : l_i = m+1\}| &= s + t - mn + m|\{i : l_i = 0\}| + \cdots + |\{i : l_i = m-1\}| \\ &\geq t. \end{aligned}$$

Hence, for t places P_i with coefficient $l_i = m+1$, we can change the coefficient to $l_i = m$ and find a divisor $U \in \mathcal{U}(n, s, x_1, \ldots, x_m)$ such that $U \leq V$. Then $\Omega(G_1 - \sum_{i=1}^{n} P_i + V) \subseteq \Omega(G_1 - \sum_{i=1}^{n} P_i + U) = \{0\}$ and therefore

$$\Omega\left(G_1 - \sum_{i=1}^{n} P_i + V\right) = \{0\} \quad \text{for all } V \in \mathcal{V}(n, s, x_1, \ldots, x_m).$$

Let ω be a nonzero differential of F, then

$$\mathcal{L}\left((\omega) - G_1 + \sum_{i=1}^{n} P_i - V\right) = \{0\}$$

for all $V \in \mathcal{V}(n, s, x_1, \ldots, x_m)$. Using the weak approximation theorem [49, Theorem I.3.1], for $1 \leq i \leq n$ we obtain $f_i \in F$ such that

$$\nu_{P_j}(f_i) = \begin{cases} 0 & \text{if } j \neq i, \\ 1 & \text{if } j = i. \end{cases}$$

Let $f = \prod_{i=1}^{n} f_i^{-\nu_{P_i}(G_1)} \in F^*$ and

$$G = G_1 + \mathrm{div}(f).$$

As $G \sim G_1$, we have

$$\mathcal{L}\left((\omega) - G + \sum_{i=1}^{n} P_i - V\right) = \{0\}$$

for all $V \in \mathcal{V}(n, s, x_1, \ldots, x_m)$ and hence

$$\Omega\left(G - \sum_{i=1}^{n} P_i + V\right) = \{0\}$$

for all $V \in \mathcal{V}(n, s, x_1, \ldots, x_m)$. Moreover, we have $\mathrm{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. □

5.2 The Basic Construction of Algebraic-Geometry Codes Using Differentials

For integers $m, n \geq 1$ and $\mathbf{a} \in \mathbf{F}_q^{mn}$, let $x_1, \ldots, x_m, I_m(\mathbf{a}), I_{m-1}(\mathbf{a}), \ldots, I_1(\mathbf{a})$, and $M_{q,n}(x_1, \ldots, x_m)$ be defined as in Section 4.2.

Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least n distinct rational places $P_1, \ldots, P_n$. For $i = 1, \ldots, n$, let t_i be a local parameter of F at P_i. Let G be a divisor of F of degree $r \leq (1-m)n - 1$ with $\text{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Then for $\omega \in \Omega(G - \sum_{i=1}^n P_i)$ and $i = 1, \ldots, n$, we have $\nu_{P_i}((\omega)) \geq -1$ and hence $\omega = x_i\, dt_i$ where x_i is given by the expansion

$$x_i = \text{res}_{P_i}(\omega) t_i^{-1} + \text{res}_{P_i}(\omega t_i^{-1}) + \text{res}_{P_i}(\omega t_i^{-2}) t_i + \cdots .$$

Let $\Psi : \Omega(G - \sum_{i=1}^n P_i) \rightarrow \mathbf{F}_q^{mn}$ be the $\mathbf{F}_q$-linear map given by

$$\Psi(\omega) = (\text{res}_{P_1}(\omega t_1^{-(m-1)}), \ldots, \text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega t_n^{-(m-1)}), \ldots, \text{res}_{P_n}(\omega)).$$

Note that $\text{Ker}\, \Psi = \Omega(G + (m-1) \sum_{i=1}^n P_i)$ and

$$\dim \text{Ker}\, \Psi = (1-m)n - r + g - 1$$

since $r \leq (1-m)n - 1$. Furthermore

$$\dim \Omega(G - \sum_{i=1}^{n} P_i) = n - r + g - 1$$

and hence Ψ is surjective.

Let $N_\Omega(P_1, \ldots, P_n; G; x_1, \ldots, x_m) := \Psi^{-1}(M_{q,n}(x_1, \ldots, x_m))$ and note that

$$|N_\Omega(P_1, \ldots, P_n; G; x_1, \ldots, x_m)| = q^{(1-m)n-r+g-1} |M_{q,n}(x_1, \ldots, x_m)|.$$

Finally, let ψ be the map defined by

$$\begin{aligned} \psi : N_\Omega(P_1, \ldots, P_n; G; x_1, \ldots, x_m) &\to \mathbf{F}_q^n \\ \omega &\mapsto \big(\mathrm{res}_{P_1}(\omega t_1^{-m}), \ldots, \mathrm{res}_{P_n}(\omega t_n^{-m})\big). \end{aligned}$$

Theorem 5.3. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $n \geq 1$ distinct rational places $P_1, \ldots, P_n$. Let $m \geq 1$ be an integer and let $x_1, \ldots, x_m$ be positive real numbers with*

$$2 \sum_{j=1}^{m} (j+1) x_j \leq 1.$$

Let s be an integer with

$$mn \leq s \leq (m+1)n - 2 \sum_{j=1}^{m} (j+1) \lfloor x_j n \rfloor$$

and r be an integer with $r \leq n - s + 2g - 2$. We assume further that

$$r \leq (1-m)n - 1$$

and

$$|\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{n-r-s+2g-2}(F) < h.$$

Then there exists a divisor G of F with $\deg(G) = r$ *and* $\mathrm{supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$ *such that*

$$C_\Omega(P_1, \ldots, P_n; G; x_1, \ldots, x_m) := \psi(N_\Omega(P_1, \ldots, P_n; G; x_1, \ldots, x_m))$$

is a q-ary (n, K, d) code with

$$K = q^{(1-m)n-r+g-1} |M_{q,n}(x_1, \ldots, x_m)|$$

and

$$d \geq (m+1)n + 1 - s - 2 \sum_{j=1}^{m} (j+1) \lfloor x_j n \rfloor.$$

Proof. We know by Corollary 5.2 that there exists a divisor G of F with $\deg(G) = r$ and $\operatorname{supp}(G) \cap \{P_1 \dots, P_n\} = \emptyset$ such that

$$\Omega(G - \sum_{i=1}^{n} P_i + V) = \{0\} \text{ for all } V \in \mathcal{V}(n, s, x_1, \dots, x_m).$$

Let $\omega_1, \omega_2 \in N_\Omega(P_1, \dots, P_n; G; x_1, \dots, x_m)$ be two distinct differentials. Since $\operatorname{supp}(G) \cap \{P_1 \dots, P_n\} = \emptyset$, we have $\nu_{P_i}((\omega_1 - \omega_2)) \geq -1$ for $1 \leq i \leq n$. Let $l_i(\omega_1 - \omega_2) = \min(m + 1, \nu_{P_i}((\omega_1 - \omega_2)) + 1)$ for $1 \leq i \leq n$. Let $V = l_1(\omega_1 - \omega_2)P_1 + \cdots + l_n(\omega_1 - \omega_2)P_n$. Note that

$$\begin{aligned}
|\{i : l_i(\omega_1 - \omega_2) = 0\}| &= |\{i : \nu_{P_i}((\omega_1 - \omega_2)) = -1\}| \\
&\leq |\{i : \nu_{P_i}((\omega_1)) = -1\}| \\
&\quad + |\{i : \nu_{P_i}((\omega_2)) = -1\}| \\
&= 2\lfloor x_m n \rfloor, \\
|\{i : l_i(\omega_1 - \omega_2) = 1\}| &= |\{i : \nu_{P_i}((\omega_1 - \omega_2)) = 0\}| \\
&\leq |\{i : \nu_{P_i}((\omega_1)) = 0\}| + |\{i : \nu_{P_i}((\omega_2)) = 0\}| \\
&\quad + |\{i : \nu_{P_i}((\omega_1)) = \nu_{P_i}((\omega_2)) = -1\}| \\
&\leq 2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor, \\
&\vdots \\
|\{i : l_i(\omega_1 - \omega_2) = m - 1\}| &= |\{i : \nu_{P_i}((\omega_1 - \omega_2)) = m - 2\}| \\
&\leq |\{i : \nu_{P_i}((\omega_1)) = m - 2\}| \\
&\quad + |\{i : \nu_{P_i}((\omega_2)) = m - 2\}| \\
&\quad + |\{i : \nu_{P_i}((\omega_1)) = \nu_{P_i}((\omega_2)) = m - 3\}| \\
&\quad + \cdots + |\{i : \nu_{P_i}((\omega_1)) = \nu_{P_i}((\omega_2)) = -1\}| \\
&\leq 2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor.
\end{aligned}$$

Moreover, $\omega_1 - \omega_2 \in \Omega(G - \sum_{i=1}^{n} P_i + V)\backslash\{0\}$ and hence we obtain

$$l_1(\omega_1 - \omega_2) + \cdots + l_n(\omega_1 - \omega_2) \leq s - 1.$$

Therefore, we obtain the following bound on $w(\psi(\omega_1 - \omega_2))$. Note that in our evaluation we will use a new calculation rather than the above individual results.

$$\begin{aligned}
&(m+1)n + 1 - s \\
&\leq \sum_{i=1}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \\
&= |\{i : l_i(\omega_1 - \omega_2) = m\}| + \sum_{\substack{i=1 \\ l_i(\omega_1-\omega_2)\leq m-1}}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \\
&= |\{i : l_i(\omega_1 - \omega_2) = m\}| + \sum_{\substack{i=1 \\ l_i(\omega_1-\omega_2)\leq m-1 \\ l_i(\omega_1)=l_i(\omega_2)}}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \\
&\quad + \sum_{\substack{i=1 \\ l_i(\omega_1-\omega_2)\leq m-1 \\ l_i(\omega_1)\neq l_i(\omega_2)}}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \\
&= |\{i : l_i(\omega_1 - \omega_2) = m\}| + \sum_{\substack{i=1 \\ l_i(\omega_1-\omega_2)\leq m-1 \\ l_i(\omega_1)=l_i(\omega_2)}}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \\
&\quad + \sum_{\substack{i=1 \\ l_i(\omega_1)\leq m-1 \\ l_i(\omega_2)\geq l_i(\omega_1)+1}}^{n} (m + 1 - l_i(\omega_1)) + \sum_{\substack{i=1 \\ l_i(\omega_2)\leq m-1 \\ l_i(\omega_1)\geq l_i(\omega_2)+1}}^{n} (m + 1 - l_i(\omega_2)).
\end{aligned}$$

Note that

$$\sum_{\substack{i=1 \\ l_i(\omega_1-\omega_2)\leq m-1 \\ l_i(\omega_1)=l_i(\omega_2)}}^{n} (m + 1 - l_i(\omega_1 - \omega_2)) \leq \sum_{\substack{i=1 \\ l_i(\omega_1)\leq m-1 \\ l_i(\omega_1)=l_i(\omega_2)}}^{n} (m + 1 - l_i(\omega_1)).$$

Therefore

$$\begin{aligned}
&(m+1)n+1-s \\
&\leq |\{i : l_i(\omega_1-\omega_2)=m\}| + \sum_{\substack{i=1 \\ l_i(\omega_1)\leq m-1 \\ l_i(\omega_1)=l_i(\omega_2)}}^{n} (m+1-l_i(\omega_1)) \\
&\quad + \sum_{\substack{i=1 \\ l_i(\omega_1)\leq m-1 \\ l_i(\omega_2)\geq l_i(\omega_1)+1}}^{n} (m+1-l_i(\omega_1)) + \sum_{\substack{i=1 \\ l_i(\omega_2)\leq m-1 \\ l_i(\omega_1)\geq l_i(\omega_2)+1}}^{n} (m+1-l_i(\omega_2)) \\
&\leq |\{i : l_i(\omega_1-\omega_2)=m\}| \\
&\quad + \sum_{\substack{i=1 \\ l_i(\omega_1)\leq m-1}}^{n} (m+1-l_i(\omega_1)) + \sum_{\substack{i=1 \\ l_i(\omega_2)\leq m-1}}^{n} (m+1-l_i(\omega_2)) \\
&= |\{i : l_i(\omega_1-\omega_2)=m\}| + 4\lfloor x_1 n\rfloor + \cdots + 2(m+1)\lfloor x_m n\rfloor \\
&\leq w(\psi(\omega_1-\omega_2)) + 4\lfloor x_1 n\rfloor + \cdots + 2(m+1)\lfloor x_m n\rfloor,
\end{aligned}$$

and hence

$$d \geq (m+1)n+1-s-2\sum_{j=1}^{m}(j+1)\lfloor x_j n\rfloor \geq 1.$$

Therefore ψ is injective and

$$K = |N_\Omega(P_1,\ldots,P_n;G;x_1,\ldots,x_m)| = q^{(1-m)n-r+g-1}|M_{q,n}(x_1,\ldots,x_m)|.$$

□

Chapter 6

An Improved Asymptotic Bound for Codes

In Section 2.2 we mentioned that, aside from the asymptotic Gilbert-Varshamov bound, the strongest currently known global bound for asymptotic codes is

$$\alpha_q(\delta) \geq R_{\text{NÖ}}(q,\delta) := 1 - \frac{1}{A(q)} - \delta + \log_q\left(1 + \frac{1}{q^3}\right) \quad \text{for } 0 \leq \delta \leq 1,$$

which was shown by Niederreiter and Özbudak [29]. Later, Niederreiter and Özbudak [30] also demonstrated that this bound could be improved upon for certain values of δ. For example, it was shown [30, Example 5.2] that for $q = 2^6$ and

$$\delta = \frac{137638684432502389295215039848333815977314125590\,44}{460650978313429323655319854867676493473213186057\,09}$$

we get an improvement on $R_{\text{NÖ}}(q,\delta)$ which is significant as it occurs in a range where $R_{\text{NÖ}}(q,\delta) > R_{\text{GV}}(q,\delta)$. Unfortunately, we note that it should have been mentioned that Vlăduţ's implicit bound is even better for these values of q and δ.

A limitation of Vlăduţ's bound is that it is only valid in the case where q is a square. Hence, another example presented by Niederreiter and Özbudak [30, Example 5.4] where $q = 2^{21}$ and

$$\delta = \frac{1034323484865452473463726110309814032498446010098}{99621193732964014413326435515634059733734238550355}$$

provides the best known bound.

In this chapter we show that the new construction of algebraic-geometry codes introduced in Chapter 4 can improve upon the results of Niederreiter and Özbudak and hence produce the best known bounds for $\alpha_q(\delta)$ for certain values of q and δ.

6.1 Some Limit Computations

Let $\mathcal{U}(n, s, x_1, \ldots, x_m)$ be defined as in Proposition 4.1 and recall that a global function field $F/\mathbf{F}_q$ has divisor class number $h(F)$ and $A_k(F)$ positive divisors of degree k. It is clear that the major challenge in providing an asymptotic bound for our new class of codes lies in bounding the terms of the fundamental equation

$$|\mathcal{U}(n, s, x_1, \ldots, x_m)| \cdot A_{r-s}(F) < h(F),$$

as the genus of the underlying global function field tends to infinity. In this section we will recall results on $A_{r-s}(F)$ and $h(F)$, but we begin with a new bound for $|\mathcal{U}(n, s, x_1, \ldots, x_m)|$.

Proposition 6.1. *Let $x_1, \ldots, x_m$ be positive real numbers and let y be a real* *number such that*

$$0 \leq y < 1 - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j$$

and

$$\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)^{l+1} \geq \left(x_l + \sum_{k=l}^{m} x_k\right)\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right)^{l}$$

for $1 \leq l \leq m$. *Then we have*

$$\begin{aligned}
&\lim_{n\to\infty}\frac{\log_q|\mathcal{U}(n, s = mn + \lfloor yn \rfloor, x_1, \dots, x_m)|}{n} = \\
&-2x_m \log_q(2x_m) - (2x_{m-1}+x_m)\log_q(2x_{m-1}+x_m) \\
&- \cdots - (2x_1+x_2+\cdots+x_m)\log_q(2x_1+x_2+\cdots+x_m) \\
&-\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right)\log_q\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right) \\
&-\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)\log_q\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right).
\end{aligned}$$

Proof. Note that for a divisor $\sum_{i=1}^{n} l_i P_i \in \mathcal{U}(n, s, x_1, \dots, x_m)$ we have

$$\begin{aligned}
|\{i : l_i = m\}| &= (m+1)n - s - 2|\{i : l_i = m-1\}| - \cdots - (m+1)|\{i : l_i = 0\}| \\
&\geq (m+1)n - s - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)\lfloor x_j n \rfloor.
\end{aligned}$$

A consequence of the inequality

$$y < 1 - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j$$

is that for $s = mn + \lfloor yn \rfloor$ we have

$$s \leq (m+1)n - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)\lfloor x_j n \rfloor.$$

This shows that all values of $k_1, \ldots, k_m$ in the following summation are valid.

$$\begin{aligned}
&|\mathcal{U}(n, s = mn + \lfloor yn \rfloor, x_1, \ldots, x_m)| \\
&= \sum_{k_m=0}^{2\lfloor x_m n \rfloor} \sum_{k_{m-1}=0}^{2\lfloor x_{m-1} n \rfloor + \lfloor x_m n \rfloor} \cdots \sum_{k_1=0}^{2\lfloor x_1 n \rfloor + \lfloor x_2 n \rfloor + \cdots + \lfloor x_m n \rfloor} \\
&\binom{n}{k_m} \binom{n - k_m}{k_{m-1}} \cdots \binom{n - k_m - \cdots - k_2}{k_1} \\
&\binom{n - k_m - \cdots - k_1}{n - 2k_1 - \cdots - (m+1)k_m - \lfloor yn \rfloor}.
\end{aligned}$$

Note that for any term in the above summation once we have chosen $k_1 + \cdots + k_m$ places with coefficients $l_i = 0, \ldots, m-1$, we have

$$n - k_1 - \cdots - k_m \geq n - \sum_{j=1}^{m} (j+1) \lfloor x_j n \rfloor > 0$$

places left to choose from. We need to choose

$$\begin{aligned}
|\{i : l_i = m\}| &= (m+1)n - s - 2|\{i : l_i = m-1\}| - \cdots - (m+1)|\{i : l_i = 0\}| \\
&= n - \lfloor yn \rfloor - 2k_1 - \cdots - (m+1)k_m \\
&\geq n - \lfloor yn \rfloor - \frac{1}{2} \sum_{j=1}^{m} (j^2 + 5j + 2) \lfloor x_j n \rfloor \\
&\geq 0
\end{aligned}$$

places with coefficient $l_i = m$, which provides the final binomial coefficient.

Now note that

$$\begin{aligned}
&\max_{\substack{0\le k_m\le 2\lfloor x_m n\rfloor \\ \vdots \\ 0\le k_1\le 2\lfloor x_1 n\rfloor+\lfloor x_2 n\rfloor+\cdots+\lfloor x_m n\rfloor}} \binom{n}{k_m}\cdots\binom{n-k_m-\cdots-k_1}{n-2k_1-\cdots-(m+1)k_m-\lfloor yn\rfloor} \\
&\le |\mathcal{U}(n, s=mn+\lfloor yn\rfloor, x_1,\ldots,x_m)| \\
&\le (2\lfloor x_m n\rfloor+1)\cdots(2\lfloor x_1 n\rfloor+\lfloor x_2 n\rfloor+\cdots+\lfloor x_m n\rfloor+1) \\
&\qquad \max_{\substack{0\le k_m\le 2\lfloor x_m n\rfloor \\ \vdots \\ 0\le k_1\le 2\lfloor x_1 n\rfloor+\lfloor x_2 n\rfloor+\cdots+\lfloor x_m n\rfloor}} \binom{n}{k_m}\cdots\binom{n-k_m-\cdots-k_1}{n-2k_1-\cdots-(m+1)k_m-\lfloor yn\rfloor}.
\end{aligned}$$

Since

$$\lim_{n\to\infty}\frac{\log_q((2\lfloor x_m n\rfloor+1)\cdots(2\lfloor x_1 n\rfloor+\lfloor x_2 n\rfloor+\cdots+\lfloor x_m n\rfloor+1))}{n}=0,$$

we obtain that

$$\begin{aligned}
&\lim_{n\to\infty}\frac{\log_q|\mathcal{U}(n,s=mn+\lfloor yn\rfloor,x_1,\ldots,x_m)|}{n} \\
&=\lim_{n\to\infty}\max_{\substack{0\le k_m\le 2\lfloor x_m n\rfloor \\ \vdots \\ 0\le k_1\le 2\lfloor x_1 n\rfloor+\lfloor x_2 n\rfloor+\cdots+\lfloor x_m n\rfloor}}\frac{\log_q\left\{\binom{n}{k_m}\cdots\binom{n-k_m-\cdots-k_1}{n-2k_1-\cdots-(m+1)k_m-\lfloor yn\rfloor}\right\}}{n}.
\end{aligned}$$

Let $0<t_1\le 2x_1+x_2+\cdots+x_m,\ldots,0<t_m\le 2x_m$ be real numbers. We note that the ranges of $\lfloor t_1 n\rfloor,\ldots,\lfloor t_m n\rfloor$ include all the values for $k_1,\ldots,k_m$ in the above equation.

Note that Stirling's formula can be used to show that

$$\frac{\log_q \binom{n}{\lfloor t_m n\rfloor}}{n}$$

$$= -t_m \log_q(t_m) - (1-t_m)\log_q(1-t_m) + O\left(\frac{\log n}{n}\right),$$

$$\frac{\log_q \binom{n-\lfloor t_m n\rfloor}{\lfloor t_{m-1} n\rfloor}}{n}$$

$$\begin{aligned}&= (1-t_m)\log_q(1-t_m) - t_{m-1}\log_q(t_{m-1})\\ &\quad - (1-t_m-t_{m-1})\log_q(1-t_m-t_{m-1}) + O\left(\frac{\log n}{n}\right),\end{aligned}$$

$$\vdots$$

$$\frac{\log_q \binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_2 n\rfloor}{\lfloor t_1 n\rfloor}}{n}$$

$$\begin{aligned}&= (1-t_m-\cdots-t_2)\log_q(1-t_m-\cdots-t_2) - t_1\log_q(t_1)\\ &\quad - (1-t_m-\cdots-t_1)\log_q(1-t_m-\cdots-t_1) + O\left(\frac{\log n}{n}\right),\end{aligned}$$

$$\frac{\log_q \binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_1 n\rfloor}{n-\lfloor yn\rfloor-2\lfloor t_1 n\rfloor-\cdots-(m+1)\lfloor t_m n\rfloor}}{n}$$

$$\begin{aligned}&= (1-t_m-\cdots-t_1)\log_q(1-t_m-\cdots-t_1)\\ &\quad - (y+t_1+\cdots+mt_m)\log_q(y+t_1+\cdots+mt_m)\\ &\quad - (1-y-2t_1-\cdots-(m+1)t_m)\log_q(1-y-2t_1-\cdots-(m+1)t_m)\\ &\quad + O\left(\frac{\log n}{n}\right).\end{aligned}$$

Therefore

$$\frac{\log_q\left(\binom{n}{\lfloor t_m n\rfloor}\binom{n-\lfloor t_m n\rfloor}{\lfloor t_{m-1} n\rfloor}\cdots\binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_2 n\rfloor}{\lfloor t_1 n\rfloor}\binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_1 n\rfloor}{n-2\lfloor t_1 n\rfloor-\cdots-(m+1)\lfloor t_m n\rfloor-\lfloor yn\rfloor}\right)}{n}$$

$$\begin{aligned}
&= -t_m\log_q(t_m)-\cdots-t_1\log_q(t_1)\\
&\quad-(y+t_1+\cdots+mt_m)\log_q(y+t_1+\cdots+mt_m)\\
&\quad-(1-y-2t_1-\cdots-(m+1)t_m)\log_q(1-y-2t_1-\cdots-(m+1)t_m)\\
&\quad+O\left(\frac{\log n}{n}\right).
\end{aligned}$$

Let $b_y(t_1,\ldots,t_m)$ be the function defined as

$$\begin{aligned}
&b_y(t_1,\ldots,t_m)\\
&= -t_m\log_q(t_m)-\cdots-t_1\log_q(t_1)\\
&\quad-(y+t_1+\cdots+mt_m)\log_q(y+t_1+\cdots+mt_m)\\
&\quad-(1-y-2t_1-\cdots-(m+1)t_m)\log_q(1-y-2t_1-\cdots-(m+1)t_m).
\end{aligned}$$

Note that for $1\le l\le m$ we have

$$\begin{aligned}
\frac{\partial b_y(t_1,\ldots,t_m)}{\partial t_l} &= -\log_q(t_l)-l\log_q(y+t_1+\cdots+mt_m)\\
&\quad+(l+1)\log_q(1-y-2t_1-\cdots-(m+1)t_m)\\
&= \log_q\frac{(1-y-2t_1-\cdots-(m+1)t_m)^{l+1}}{t_l(y+t_1+\cdots+mt_m)^l}.
\end{aligned}$$

Note that, for $l=1,\ldots,m$, we have

$$\frac{\partial b_y(t_1,\ldots,t_m)}{\partial t_l}\ge 0$$

for $0<t_m\le 2x_m,...,0<t_1\le 2x_1+x_2+\cdots+x_m$.

Therefore we have

$$
\begin{aligned}
&\lim_{n\to\infty} \frac{\log_q |\mathcal{U}(n, s = mn + \lfloor yn \rfloor, x_1, \ldots, x_m)|}{n} \\
&= \lim_{n\to\infty} \max_{\substack{0 \le k_m \le 2\lfloor x_m n\rfloor \\ \vdots \\ 0\le k_1 \le 2\lfloor x_1 n\rfloor + \lfloor x_2 n\rfloor + \cdots + \lfloor x_m n\rfloor}} \frac{\log_q \left(\binom{n}{k_m} \cdots \binom{n-k_m-\cdots-k_1}{n-2k_1-\cdots-(m+1)k_m-\lfloor yn\rfloor} \right)}{n} \\
&= \lim_{n\to\infty} \max_{\substack{0 \le \lfloor t_m n\rfloor \le 2\lfloor x_m n\rfloor \\ \vdots \\ 0\le \lfloor t_1 n\rfloor \le 2\lfloor x_1 n\rfloor + \lfloor x_2 n\rfloor + \cdots + \lfloor x_m n\rfloor}} \frac{\log_q \left(\binom{n}{\lfloor t_m n\rfloor} \cdots \binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_1 n\rfloor}{n-2\lfloor t_1 n\rfloor-\cdots-(m+1)\lfloor t_m n\rfloor-\lfloor yn\rfloor} \right)}{n} \\
&= \lim_{n\to\infty} \max_{\substack{0 < t_m \le 2x_m \\ \vdots \\ 0< t_1 \le 2x_1 + x_2 + \cdots + x_m}} \frac{\log_q \left(\binom{n}{\lfloor t_m n\rfloor} \cdots \binom{n-\lfloor t_m n\rfloor-\cdots-\lfloor t_1 n\rfloor}{n-2\lfloor t_1 n\rfloor-\cdots-(m+1)\lfloor t_m n\rfloor-\lfloor yn\rfloor} \right)}{n} \\
&= \lim_{n\to\infty} \max_{\substack{0 < t_m \le 2x_m \\ \vdots \\ 0< t_1 \le 2x_1 + x_2 + \cdots + x_m}} b_y(t_1, \ldots, t_m) + O\left(\frac{\log n}{n}\right) \\
&= \lim_{n\to\infty} b_y(2x_1 + x_2 + \cdots x_m, \ldots, 2x_m) + O\left(\frac{\log n}{n}\right) \\
&= b_y(2x_1 + x_2 + \cdots x_m, \ldots, 2x_m) \\
&= -2x_m \log_q(2x_m) - (2x_{m-1} + x_m)\log_q(2x_{m-1} + x_m) \\
&\quad - \cdots - (2x_1 + x_2 + \cdots + x_m)\log_q(2x_1 + x_2 + \cdots + x_m) \\
&\quad - \left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right)\log_q\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right) \\
&\quad - \left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)\log_q\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right).
\end{aligned}
$$

□

The following bound was proved for $0 < \sigma < 2/(q^{1/2}+1)$ by Xing [57, Proposition 3.4] and extended by Niederreiter and Özbudak [30, Proposition

4.5].

Proposition 6.2. *Let $\{F_i/\mathbf{F}_q\}_{i=1}^{\infty}$ be a sequence of global function fields with genus $g(F_i) \to \infty$ as $i \to \infty$. Then*

$$\limsup_{i\to\infty} \frac{\log_q A_{\lfloor \sigma g(F_i)\rfloor}(F_i)}{g(F_i)} \leq I(\sigma) :=$$

$$\begin{cases} \frac{\sigma}{2} + \log_q 4 - \sigma \log_q \sigma \\ \qquad\qquad - (2-\sigma)\log_q(2-\sigma) & \textit{if } 0 < \sigma \leq \frac{2}{q^{1/2}+1}, \\ \sigma - 1 + 2\log_q(q^{1/2}+1) & \textit{if } \frac{2}{q^{1/2}+1} \leq \sigma < 3 - 2\log_q(q^{1/2}+1). \end{cases}$$

Note that $I(\sigma)$ is a strictly increasing function mapping the interval $(0, 3-2\log_q(q^{1/2}+1)$ onto the interval $(0,2)$.

Finally, to bound the divisor class number relative to the genus, we have the following proposition due to Vlăduţ [53] (see also [51, Proposition 2.3.26]).

Proposition 6.3. *Let $\{F_i/\mathbf{F}_q\}_{i=1}^{\infty}$ be a sequence of global function fields with genus $g(F_i) \to \infty$ as $i \to \infty$ and*

$$\lim_{i\to\infty} \frac{N(F_i)}{g(F_i)} = A > 0.$$

Then

$$\liminf_{i\to\infty} \frac{\log_q h(F_i)}{g(F_i)} \geq 1 + A \cdot \log_q \left(\frac{q}{q-1}\right).$$

6.2 The Improved Asymptotic Bound

In this section we combine the asymptotic bounds on $|\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)|$, $A_{r_i - s_i}(F_i)$, and $h(F_i)$ to obtain a new asymptotic coding bound.

Let $x_1, \ldots, x_m$ be positive real numbers and let y be a real number such that

$$0 \le y < 1 - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j$$

and

$$\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)^{l+1} \ge \left(x_l + \sum_{k=l}^{m} x_k\right)\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right)^{l}$$

for $1 \le l \le m$. Let $G(x_1, \ldots, x_m, y)$ be the function defined as

$$\begin{aligned}
&G(x_1, \ldots, x_m, y) \\
&= 1 + A(q)\log_q \frac{q}{q-1} \\
&\quad + A(q)\Bigg(2x_m \log_q(2x_m) + (2x_{m-1}+x_m)\log_q(2x_{m-1}+x_m) \\
&\quad + \cdots + (2x_1 + x_2 + \cdots + x_m)\log_q(2x_1 + x_2 + \cdots + x_m) \\
&\quad + \left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right)\log_q\left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right) \\
&\quad + \left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)\log_q\left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)\Bigg)
\end{aligned}$$

and let $\Psi(x_1, \ldots, x_m, y)$ be the function defined as

$$\Psi(x_1, \ldots, x_m, y) = \begin{cases} I^{-1}(G(x_1, \ldots, x_m, y)) & \text{if } 0 < G(x_1, \ldots, x_m, y) < 2, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 6.4. *Let $\{F/\mathbf{F}_q\}_{i=1}^{\infty}$ be a sequence of global function fields with $g_i \to \infty$ as $i \to \infty$ and*

$$\lim_{i\to\infty} \frac{N_i}{g_i} = A(q) > 0,$$

where N_i and g_i denote the number of rational places and the genus of F_i, *respectively. Then for positive real numbers* $x_1, \ldots, x_m, \delta$ *with*

$$\frac{1}{2}\sum_{j=1}^{m}(j^2+j-2)x_j < \delta \leq 1 - \frac{2}{A(q)} - 2\sum_{j=1}^{m}(j+1)x_j,$$

and

$$\left(\delta - \frac{1}{2}\sum_{j=1}^{m}(j^2+j-2)x_j\right)^{l+1} \geq \left(x_l + \sum_{k=l}^{m} x_k\right)\left(1 + \frac{1}{2}\sum_{j=1}^{m}(j^2-j-4)x_j - \delta\right)^{l}$$

for $1 \leq l \leq m$*, we have*

$$\begin{aligned}\alpha_q(\delta) \geq R_{x_1,\ldots,x_m}(q,\delta) := 1 &- \frac{1}{A(q)} - \delta \\ &- \sum_{j=1}^{m} x_j \log_q x_j - \left(1 - \sum_{j=1}^{m} x_j\right)\log_q\left(1 - \sum_{j=1}^{m} x_j\right) \\ &+ \left(\sum_{j=1}^{m} x_j\right)\log_q(q-1) - \sum_{j=1}^{m}(j+3)x_j \\ &+ \frac{1}{A(q)}\Psi\left(x_1,\ldots,x_m, 1 - 2\sum_{j=1}^{m}(j+1)x_j - \delta\right).\end{aligned}$$

Proof. Let $y := 1-2\sum_{j=1}^{m}(j+1)x_j-\delta$. We can assume $\sigma := \Psi(x_1,\ldots,x_m,y)$ > 0 as the result is already known otherwise [29]. Note that

$$y > \frac{2-\sigma}{A(q)}.$$

Let $\varepsilon > 0$ be a sufficiently small real number such that $\varepsilon < \sigma$ and

$$y > \frac{2-(\sigma-\varepsilon)}{A(q)}$$

hold.

For $i \geq 1$, let $n_i = N_i$, $s_i = mn_i + \lfloor yn_i \rfloor$ and $r_i = s_i + \lfloor(\sigma-\varepsilon)g_i\rfloor$. Then we have

$$\begin{aligned}
&\lim_{i\to\infty} \frac{\log_q |\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)|}{g_i} \\
&= A(q)\Bigg(- 2x_m \log_q(2x_m) - (2x_{m-1} + x_m) \log_q(2x_{m-1} + x_m) \\
&\quad - \cdots - (2x_1 + x_2 + \cdots + x_m) \log_q(2x_1 + x_2 + \cdots + x_m) \\
&\quad - \left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right) \log_q \left(y + \frac{1}{2}\sum_{j=1}^{m}(j^2+3j)x_j\right) \\
&\quad - \left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right) \log_q \left(1 - y - \frac{1}{2}\sum_{j=1}^{m}(j^2+5j+2)x_j\right)\Bigg). \\
&= 1 + A(q)\log_q \frac{q}{q-1} - G(x_1, \ldots, x_m, y).
\end{aligned}$$

Therefore

$$\begin{aligned}
&\limsup_{i\to\infty} \frac{\log_q \left(|\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)| \cdot A_{r_i - s_i}(F_i)\right)}{g_i} \\
&\le \limsup_{i\to\infty} \frac{\log_q |\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)|}{g_i} + \limsup_{i\to\infty} \frac{\log_q A_{r_i - s_i}(F_i)}{g_i} \\
&\le \limsup_{i\to\infty} \frac{\log_q |\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)|}{g_i} + I(\sigma - \varepsilon) \\
&= 1 + A(q)\log_q \frac{q}{q-1} - G(x_1, \ldots, x_m, y) + I(\sigma - \varepsilon) \\
&< 1 + A(q)\log_q \frac{q}{q-1} \\
&\le \liminf_{i\to\infty} \frac{\log_q h(F_i)}{g_i},
\end{aligned}$$

where we have applied Proposition 6.3 in the final inequality. Therefore, for sufficiently large i, we have

$$|\mathcal{U}(n_i, s_i, x_1, \ldots, x_m)| \cdot A_{r_i - s_i}(F_i) < h(F_i).$$

Note that

$$\lim_{i\to\infty} \frac{r_i + 1 - 2g_i}{n_i} = m + y - \frac{2 - (\sigma - \varepsilon)}{A(q)} > m$$

and so, for sufficiently large i, we have

$$r_i + 1 - 2g_i > mn_i.$$

Note that, as was mentioned in [29, Lemma 4.2], we have

$$\begin{aligned}
&\lim_{n\to\infty} \frac{\log_q |M_{q,n}(x_1,\ldots,x_m)|}{n} \\
&= -\sum_{j=1}^{m} x_j \log_q x_j - \left(1 - \sum_{j=1}^{m} x_j\right) \log_q \left(1 - \sum_{j=1}^{m} x_j\right) \\
&\quad + \left(\sum_{j=1}^{m} x_j\right) \log_q (q-1) + \sum_{j=2}^{m} (j-1) x_j.
\end{aligned}$$

We now apply Theorem 4.3. By passing, if necessary, to a subsequence this yields a sequence $\{C_i\}_{i=i_0\geq 1}^{\infty}$ of q-ary (n_i, K_i, d_i) codes satisfying

$$\begin{aligned}
\lim_{i\to\infty} \frac{\log_q K_i}{n_i} \geq\ & y + \frac{\sigma - \varepsilon - 1}{A(q)} \\
& - \sum_{j=1}^{m} x_j \log_q x_j - \left(1 - \sum_{j=1}^{m} x_j\right) \log_q \left(1 - \sum_{j=1}^{m} x_j\right) \\
& + \left(\sum_{j=1}^{m} x_j\right) \log_q (q-1) + \sum_{j=2}^{m} (j-1) x_j \\
=\ & 1 + \frac{\sigma - \varepsilon - 1}{A(q)} - \delta - 2\sum_{j=1}^{m} (j+1) x_j \\
& - \sum_{j=1}^{m} x_j \log_q x_j - \left(1 - \sum_{j=1}^{m} x_j\right) \log_q \left(1 - \sum_{j=1}^{m} x_j\right) \\
& + \left(\sum_{j=1}^{m} x_j\right) \log_q (q-1) + \sum_{j=2}^{m} (j-1) x_j
\end{aligned}$$

and

$$\lim_{i\to\infty} \frac{d_i}{n_i} \geq 1 - y - 2\sum_{j=1}^{m} (j+1) x_j = \delta.$$

Letting ε tend to 0, we obtain the desired result. □

6.3 Explicit Asymptotic Bounds

In this section we compare our bound with various others for some values of q and δ analysed by Niederreiter and Özbudak [30]. We note that in the case $m = 1$, the bound $R_{x_1}(q, \delta)$ corresponds to their construction.

Our first example will demonstrate that increasing the value of m produces stronger bounds. The second example will show that our new code construction can indeed be used to produce the strongest currently known asymptotic coding bound for certain values of q and δ.

Let $R_{\mathrm{V}}(q, \delta)$ be the bound obtained by Vlăduţ [53] using distinguished line bundles and $R_{\mathrm{Xing}}(q, \delta)$ be the bound obtained by Xing [57] using distinguished divisors.

Example 6.5. Let $q = 2^6$ and

$$\begin{aligned}\delta &= \frac{1376386844325023892952150398483338159773141255904}{46065097831342932365531985486767649347321318605709} \\ &= 0.29879169026501515839\ldots.\end{aligned}$$

We note that with $x_1 = 10^{-13}$, $R_{x_1}(q, \delta)$ has been analysed by Niederreiter and Özbudak [30, Example 5.2]. For these values of q and δ, the crucial inequalities are

$$R_{\mathrm{V}}(q, \delta) > R_{x_1}(q, \delta) > R_{\mathrm{Xing}}(q, \delta) > R_{\mathrm{N\ddot{O}}}(q, \delta) > R_{\mathrm{GV}}(q, \delta).$$

More specifically, we have

$$\begin{aligned}
R_{\mathrm{V}}(q,\delta) - R_{x_1}(q,\delta) &\geq 2.4136 \cdot 10^{-7},\\
R_{x_1}(q,\delta) - R_{\mathrm{Xing}}(q,\delta) &\geq 7.3387 \cdot 10^{-15},\\
R_{\mathrm{Xing}}(q,\delta) - R_{\mathrm{N\ddot{O}}}(q,\delta) &\geq 1.6317 \cdot 10^{-6},\\
R_{\mathrm{N\ddot{O}}}(q,\delta) - R_{\mathrm{X}}(q,\delta) &\geq 1.4111 \cdot 10^{-8},\\
R_{\mathrm{X}}(q,\delta) - R_{\mathrm{TVZ}}(q,\delta) &\geq 9.0312 \cdot 10^{-7},\\
R_{\mathrm{TVZ}}(q,\delta) - R_{\mathrm{GV}}(q,\delta) &\geq 2.6462 \cdot 10^{-3}.
\end{aligned}$$

We begin our analysis by noting that for $m = 1$ there are better choices of x_1 than Niederreiter and Özbudak's choice of $x_1 = 10^{-13}$. For example, with $x_1 = 7.9957147039 \cdot 10^{-14}$ we obtain

$$R_{x_1}(q,\delta) - R_{\mathrm{Xing}}(q,\delta) \geq 7.55856972571591107037 \cdot 10^{-15}$$

and furthermore

$$R_{\overline{x}_1}(q,\delta) - R_{\mathrm{Xing}}(q,\delta) \leq 7.55856972571591107038 \cdot 10^{-15}$$

for all $\overline{x}_1$.

We now show that if we increase m, we gain improvements. With

$$\begin{aligned}
x_1 &= 7.99571470394199455365697316 7 \cdot 10^{-14},\\
x_2 &= 1.32992085858119073001 1 \cdot 10^{-27}
\end{aligned}$$

we obtain

$$\begin{aligned}
R_{x_1,x_2}(q,\delta) - R_{\mathrm{Xing}}(q,\delta) \geq 7.5585697257160367914878980072686924 0\\
284332089 \cdot 10^{-15}
\end{aligned}$$

and therefore

$$R_{x_1,x_2}(q,\delta) - R_{\overline{x}_1}(q,\delta) \geq 1.2572 \cdot 10^{-28}.$$

for all $\overline{x}_1$. Furthermore

$$\begin{aligned} R_{\overline{x}_1,\overline{x}_2}(q,\delta) - R_{\text{Xing}}(q,\delta) \leq\ & 7.55856972571603679148789800726869240 \\ & 284332090 \cdot 10^{-15} \end{aligned}$$

for all $\overline{x}_1$ and $\overline{x}_2$. With

$$\begin{aligned} x_1 &= 7.995714703941994550636124043092191470796649418 \cdot 10^{-14}, \\ x_2 &= 1.329920858581190729623007049896058553827 \cdot 10^{-27}, \\ x_3 &= 9.91712573491320911997279876 \cdot 10^{-52} \end{aligned}$$

we obtain

$$\begin{aligned} R_{x_1,x_2,x_3}(q,\delta) - R_{\text{Xing}}(q,\delta) \geq\ & 7.75585697257160367914878980072686924 \\ & 03476522521372777458540297087276489 \\ & 33738325264175327945 \cdot 10^{-15} \end{aligned}$$

and therefore

$$R_{x_1,x_2,x_3}(q,\delta) - R_{\overline{x}_1,\overline{x}_2}(q,\delta) \geq 6.3320 \cdot 10^{-52}$$

for all $\overline{x}_1$ and $\overline{x}_2$. Furthermore

$$\begin{aligned} R_{\overline{x}_1,\overline{x}_2,\overline{x}_3}(q,\delta) - R_{\text{Xing}}(q,\delta) \leq\ & 7.55856972571603679148789800726869240 \\ & 34765225213727774585402970872764893 \\ & 3738325264175327946 \cdot 10^{-15} \end{aligned}$$

for all $\overline{x}_1$, $\overline{x}_2$, and $\overline{x}_3$. With

$$\begin{aligned}
x_1 &= 7.99571470394199455063612404309219147079664941 8 \cdot 10^{-14},\\
x_2 &= 1.32992085858119072962300704989605855382 7 \cdot 10^{-27},\\
x_3 &= 9.917125734913209119972798 76 \cdot 10^{-52},\\
x_4 &= 3.41883 \cdot 10^{-94}
\end{aligned}$$

we obtain

$$\begin{aligned}
R_{x_1,x_2,x_3,x_4}(q,\delta) - R_{\text{Xing}}(q,\delta) \geq 7.&558569725716036791487898007268692 40\\
&34765225213727774585402970872764893\\
&3738325267407239318 \cdot 10^{-15}
\end{aligned}$$

and therefore

$$R_{x_1,x_2,x_3,x_4}(\delta) - R_{\overline{x}_1,\overline{x}_2,\overline{x}_3}(\delta) \geq 3.2319 \cdot 10^{-95}$$

for all $\overline{x}_1$, $\overline{x}_2$, and $\overline{x}_3$.

In summary, we have shown that for $m = 2$, 3, and 4 we can gain consecutive improvements on Niederreiter and Özbudak's construction for $m = 1$.

Example 6.6. Let $q = 2^{21}$ and

$$\begin{aligned}
\delta &= \frac{1034323484865452473463726110309814032498446010098}{99621193732964014413326435515634059733734238550355}\\
&= 0.010382564654243863 59\ldots.
\end{aligned}$$

Recalling the result of Bezerra, Garcia, and Stichtenoth [1] that was mentioned in Section 2.1, we see that

$$A(2^{21}) \geq \frac{16383}{65}.$$

Since we do not know the exact value of $A(2^{21})$, we cannot calculate the exact value of, for example, $R_{\mathrm{TVZ}}(q,\delta)$. We fix this problem by replacing $R_{\mathrm{TVZ}}(q,\delta)$ with the bound

$$R'_{\mathrm{TVZ}}(q,\delta) := 1 - \frac{65}{16383} - \delta \quad \text{for } 0 \leq \delta \leq 1.$$

Similarly we replace $A(2^{21})$ with $\frac{16383}{65}$ in the other bounds involving $A(q)$ and in these cases we again replace R with R'.

We note that with $x_1 = 10^{-60}$, $R'_{x_1}(q,\delta)$ has been analysed by Niederreiter and Özbudak [30, Example 5.4]. Since Vlăduţ's bound is only valid in the case where q is a square, we see that, for these values of q and δ, the crucial inequalities are

$$R'_{x_1}(q,\delta) > R'_{\mathrm{Xing}}(q,\delta) > R'_{\mathrm{N\ddot{O}}}(q,\delta) > R_{\mathrm{GV}}(q,\delta).$$

More specifically, we have

$$\begin{aligned}
R'_{x_1}(q,\delta) - R'_{\mathrm{Xing}}(q,\delta) &\geq 2.1335 \cdot 10^{-61}, \\
R'_{\mathrm{Xing}}(q,\delta) - R'_{\mathrm{N\ddot{O}}}(q,\delta) &\geq 1.2865 \cdot 10^{-18}, \\
R'_{\mathrm{N\ddot{O}}}(q,\delta) - R'_{\mathrm{X}}(q,\delta) &\geq 3.5516 \cdot 10^{-27}, \\
R'_{\mathrm{X}}(q,\delta) - R'_{\mathrm{TVZ}}(q,\delta) &\geq 7.4484 \cdot 10^{-21}, \\
R'_{\mathrm{TVZ}}(q,\delta) - R_{\mathrm{GV}}(q,\delta) &\geq 3.2418 \cdot 10^{-8}.
\end{aligned}$$

We begin our analysis by noting that for $m = 1$ there are better choices of x_1 than Niederreiter and Özbudak's choice of $x_1 = 10^{-60}$. For example, with

$$x_1 = 4.159479366046034067199662818967840675643 \cdot 10^{-57}$$

we obtain

$$\begin{aligned} R'_{x_1}(q,\delta) - R'_{\text{Xing}}(q,\delta) \geq 9.&5086274720972276882500356453238812 2\\ &6284907268317219108910765130352926 5\\ &0919079801 \cdot 10^{-59} \end{aligned}$$

and furthermore

$$\begin{aligned} R'_{\overline{x}_1}(q,\delta) - R'_{\text{Xing}}(q,\delta) \leq 9.&5086274720972276882500356453238812 2\\ &6284907268317219108910765130352926 5\\ &0919079802 \cdot 10^{-59} \end{aligned}$$

for all $\overline{x}_1$.

Now let $m = 2$. With

$$\begin{aligned} x_1 &= 4.1594793660460340671996628189678406756432 \cdot 10^{-57},\\ x_2 &= 2.3336 \cdot 10^{-128} \end{aligned}$$

we obtain

$$\begin{aligned} R'_{x_1,x_2}(q,\delta) - R'_{\text{Xing}}(q,\delta) \geq 9.&5086274720972276882500356453238812 2\\ &6284907268317219108910765130352926 5\\ &6253716970 \cdot 10^{-59} \end{aligned}$$

and therefore

$$R'_{x_1,x_2}(q,\delta) - R'_{\overline{x}_1}(q,\delta) \geq 5.3346 \cdot 10^{-130}.$$

for all $\overline{x}_1$.

In summary, we have shown that for $m = 2$ we gain an improvement on Niederreiter and Özbudak's construction for $m = 1$. This is significant as Niederreiter and Özbudak's bound is the best in the literature for these values of q and δ. Hence, we have shown that our new construction can produce best known asymptotic coding bounds.

Chapter 7

A New Construction of (t,m,s)-Nets

When Niederreiter and Xing introduced the idea of using global function fields to produce low-discrepancy point sets and sequences, digital (t, m, s)-nets were obtained by simply considering digital $(t, s-1)$-sequences. An interesting development was the introduction by Niederreiter and Pirsic [31] of the concept of duality theory, which endows the vector space $\mathbf{F}_q^{ms}$ with a weight function which is a generalisation of the classical Hamming weight, in order to produce digital (t, m, s)-nets.

The switch to a more coding-theoretic viewpoint allows us to import an important idea from the theory of algebraic-geometry codes. Goppa's algebraic-geometry codes are dependent upon a divisor G of particular degree whose support is disjoint from a set $P_1, \ldots, P_n$ of rational places. It is a fact that some such divisors will produce codes with better parameters than other divisors of the same degree. It was shown independently by Vlăduţ [53] (see also [51]) and then Xing [57] that this fact could be utilised to produce improvements on the asymptotic bounds of linear codes.

The introduction of a more direct way to produce digital (t, m, s)-nets using global function fields means that we can transfer the distinguished divisor method from coding theory to the low-discrepancy sequences setting. This was first demonstrated by Niederreiter and Xing [40] and reproduced in [60]. A more generalised version using arbitrary places was given by Niederreiter and Özbudak [28], and this produces the best known (t, m, s)-nets.

For our construction we will restrict ourselves to using rational places, but we will use differentials.

7.1 Distinguished Divisors for (t, m, s)-Nets Using Differentials

We begin by introducing the distinguished divisor that we will need. The following proposition is simply a slight modification of Proposition 5.1.

Proposition 7.1. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $s \geq 2$ distinct rational places $P_1, \ldots, P_s$. Let $m \geq 1$ and $0 \leq l \leq \min\{ms, ms - m + g - 1\}$ be integers. Let $\mathcal{U}(s, l, m)$ be the set of divisors of F defined by*

$$\mathcal{U}(s, l, m) = \left\{ \sum_{i=1}^{s} w_i P_i : \sum_{i=1}^{s} w_i = l, 0 \leq w_i \leq m \right\}.$$

Suppose that

$$|\mathcal{U}(s, l, m)| \cdot A_{ms-m+g-1-l}(F) < h.$$

Then there exists a divisor G of F such that $\deg(G) = m + s - ms + g - 1$ *and*

$$\Omega\Big(G - \sum_{i=1}^{s} P_i + U\Big) = \{0\}$$

for all $U \in \mathcal{U}(s, l, m)$.

Proof. Let Q be a rational place of F. Let $\mathcal{D}$ be the set of degree zero divisors given by

$$\mathcal{D} = \{U + A - (ms - m + g - 1)Q : U \in \mathcal{U}(s, l, m), A \in \mathcal{A}_{ms-m+g-1-l}(F)\}.$$

Note that

$$|\mathcal{D}| \leq |\mathcal{U}(s, l, m)| \cdot A_{ms-m+g-1-l}(F) < h.$$

Therefore there exists a degree zero divisor D_0 of F such that

$$D_0 \not\sim D \quad \text{for all } D \in \mathcal{D}.$$

Let ω_1 be a nonzero differential of F and put

$$G := (\omega_1) - D_0 + \sum_{i=1}^{s} P_i - (ms - m + g - 1)Q.$$

We claim that

$$\Omega\Big(G - \sum_{i=1}^{s} P_i + U\Big) = \{0\}$$

for all $U \in \mathcal{U}(s, l, m)$. Suppose, on the contrary, that there exists $U \in \mathcal{U}(s, l, m)$ and ω_2 such that

$$\omega_2 \in \Omega\Big(G - \sum_{i=1}^{s} P_i + U\Big)\backslash\{0\}.$$

Note that

$$\Omega\Big(G - \sum_{i=1}^{s} P_i + U\Big) \simeq \mathcal{L}\Big((\omega_2) - G + \sum_{i=1}^{s} P_i - U\Big)$$

and hence there exists a nonzero $f_1 \in F$ such that

$$f_1 \in \mathcal{L}\Bigg((\omega_2) - G + \sum_{i=1}^{s} P_i - U\Bigg).$$

Then

$$E := \mathrm{div}(f_1) + (\omega_2) - G + \sum_{i=1}^{s} P_i - U$$

is a positive divisor of degree $ms - m + g - 1 - l$. Note that all canonical divisors are equivalent. Therefore

$$(\omega_2) = (\omega_1) + \mathrm{div}(f_2)$$

for some $f_2 \in F$ and so

$$D_0 + \mathrm{div}(f_1 f_2) = U + E - (ms - m + g - 1)Q \in \mathcal{D}$$

which is a contradiction to the choice of D_0. □

7.2 The Basic Construction of (t, m, s)-Nets Using Differentials

We now define our construction of (t, m, s)-nets. Let $F/\mathbf{F}_q$ be a global function field. For a given dimension $s \geq 2$, we assume that $N(F) \geq s$ and let $P_1, \ldots, P_s$ be distinct rational places of F. For $i = 1, \ldots, s$, let $t_i \in F$ be a local parameter at P_i. Now choose an arbitrary divisor G of F and put

$$n_i = \nu_{P_i}(G) \quad \text{for } 1 \leq i \leq s.$$

For $1 \leq i \leq s$ and $\omega \in \Omega(G - \sum_{i=1}^{s} P_i)$ note that $\nu_{P_i}((\omega)) \geq n_i - 1$. Therefore for $m \geq 1$ we can let $\omega = x_i\, dt_i$, where

$$x_i = \mathrm{res}_{P_i}(\omega t_i^{-n_i}) t_i^{n_i - 1} + \ldots + \mathrm{res}_{P_i}(\omega t_i^{-(n_i + m - 1)}) t_i^{n_i + m - 2} + \ldots$$

and $\mathrm{res}_{P_i}(\omega t_i^{-n_i}), \mathrm{res}_{P_i}(\omega t_i^{-(n_i+1)}), \ldots$ are uniquely determined constants in $\mathbf{F}_q$. Finally, we define

$$\mathbf{c}_\omega^{(i)} = (\mathrm{res}_{P_i}(\omega t_i^{-(n_i+m-1)}), \ldots, \mathrm{res}_{P_i}(\omega t_i^{-n_i})) \quad \text{for } 1 \leq i \leq s,$$

$$\mathbf{C}_\omega = (\mathbf{c}_\omega^{(1)}, \ldots, \mathbf{c}_\omega^{(s)}) \in \mathbf{F}_q^{ms},$$

and let $\mathbf{C}_\Omega^m(P_1, \ldots, P_s; G)$ be the image of the following $\mathbf{F}_q$-linear map:

$$\begin{array}{rcl} \phi : \Omega\left(G - \sum_{i=1}^{s} P_i\right) & \rightarrow & \mathbf{F}_q^{ms} \\ \omega & \mapsto & \mathbf{C}_\omega. \end{array}$$

The minimum distance of $\mathbf{C}_\Omega^m(P_1, \ldots, P_s; G)$ is provided by the following theorem.

Theorem 7.2. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $s \geq 2$ distinct rational places $P_1, \ldots, P_s$. Let $m \geq 1$ and $0 \leq l \leq \min\{ms, ms - m + g - 1\}$ be integers. Suppose further that*

$$|\mathcal{U}(s, l, m)| \cdot A_{ms-m+g-1-l}(F) < h.$$

Then there exists a divisor G of F with $\deg(G) = m + s - ms + g - 1$ such that $\mathbf{C}_\Omega^m(P_1, \ldots, P_s; G)$ is an $\mathbf{F}_q$-linear subspace of $\mathbf{F}_q^{ms}$ with

$$\dim(\mathbf{C}_\Omega^m(P_1, \ldots, P_s; G)) \geq ms - m$$

and

$$\delta_m(\mathbf{C}_\Omega^m(P_1, \ldots, P_s; G)) \geq ms - l + 1.$$

Proof. Let G be a divisor of the form given in Proposition 7.1. Let $\omega \in \Omega(G - \sum_{i=1}^{s} P_i)$ be a nonzero differential and put

$$w_i(\omega) = \min(m, \nu_{P_i}((\omega)) - n_i + 1) \quad \text{for} \quad 1 \leq i \leq s.$$

Then, using the notation from Section 2.3, we have

$$v(\mathbf{c}_\omega^{(i)}) = m - w_i(\omega) \quad \text{for} \quad 1 \leq i \leq s.$$

Therefore

$$V_m(\mathbf{C}_\omega) = \sum_{i=1}^{s} v(\mathbf{c}_\omega^{(i)}) = ms - \sum_{i=1}^{s} w_i(\omega).$$

For $i = 1, \dots, s$, we have $\nu_{P_i}((\omega)) \geq n_i - 1 + w_i(\omega)$, and so

$$\omega \in \Omega\left(G - \sum_{i=1}^{s} P_i + \sum_{i=1}^{s} w_i(\omega) P_i\right).$$

Since $\omega \neq 0$, it follows that we must have

$$\sum_{i=1}^{s} w_i(\omega) \leq l - 1,$$

hence

$$V_m(\mathbf{C}_\omega) \geq ms - l + 1 \geq 1.$$

This shows that the $\mathbf{F}_q$-linear map $\phi : \Omega(G - \sum_{i=1}^{s} P_i) \mapsto \mathbf{C}_\omega$ is injective. Thus,

$$\begin{aligned}
\dim(\mathbf{C}_\Omega^m(P_1, \dots, P_s; G)) &= \dim \Omega(G - \sum_{i=1}^{s} P_i) \\
&= \dim \mathcal{L}(G - \sum_{i=1}^{s} P_i) - \deg(G - \sum_{i=1}^{s} P_i) + g - 1 \\
&\geq s - \deg(G) + g - 1 = ms - m
\end{aligned}$$

and also

$$\delta_m(\mathbf{C}_\Omega^m(P_1, \dots, P_s; G)) \geq ms - l + 1.$$

□

Corollary 7.3. *Let $F/\mathbf{F}_q$ be a global function field of genus g, divisor class number h, and with at least $s \geq 2$ distinct rational places $P_1, \dots, P_s$. Let $m \geq 1$ and $0 \leq l \leq \min\{ms, ms - m + g - 1\}$ be integers. Suppose further that*

$$|\mathcal{U}(s, l, m)| \cdot A_{ms-m+g-1-l}(F) < h.$$

Then there exists a digital $(m - ms + l, m, s)$-net over $\mathbf{F}_q$.

Proof. This follows by Theorem 2.16. □

Example 7.4. Let F be the Hermitian function field [49, Example VI.3.6] over $\mathbf{F}_{25}$. Then $g(F) = 10$, $h(F) = 6^{20}$, $A_1(F) = N(F) = 126$, $A_2(F) = 8001$, $A_3(F) = 347376$, and $A_4(F) = 11859876$. Let $s = 126$.

Suppose $l = ms - m + g - 1 = 125m + 9$ where $m \geq 9$. Note that the condition

$$|\mathcal{U}(126, 125m + 9, m)| = \binom{116 + m}{125} < 6^{20}$$

is satisfied for $9 \leq m \leq 19$ and so there exist digital $(9, m, 126)$-nets over $\mathbf{F}_{25}$ for these values of m. Furthermore, a comparison with the information available at [43] shows that for $m = 18$ and 19 these digital nets have quality parameter t matching the best known value.

Suppose $l = ms - m + g - 2 = 125m + 8$ where $m \geq 8$. Note that the condition

$$|\mathcal{U}(126, 125m + 8, m)| \cdot 126 = \binom{117 + m}{125} \cdot 126 < 6^{20}$$

is satisfied for $8 \leq m \leq 16$ and so there exist digital $(8, m, 126)$-nets over $\mathbf{F}_{25}$ for these values of m. Furthermore, a comparison with the information available at [43] shows that for $m = 16$ this digital net has quality parameter t matching the best known value.

Suppose $l = ms - m + g - 3 = 125m + 7$ where $m \geq 7$. Note that the condition

$$|\mathcal{U}(126, 125m + 7, m)| \cdot 8001 = \binom{118 + m}{125} \cdot 8001 < 6^{20}$$

is satisfied for $7 \leq m \leq 14$ and so there exist digital $(7, m, 126)$-nets over $\mathbf{F}_{25}$ for these values of m. Furthermore, a comparison with the information available at [43] shows that for $m = 14$ this digital net has quality parameter t matching the best known value.

Suppose $l = ms - m + g - 4 = 125m + 6$ where $m \geq 6$. Note that the condition

$$|\mathcal{U}(126, 125m + 6, m)| \cdot 347376 = \binom{119 + m}{125} \cdot 347376 < 6^{20}$$

is satisfied for $6 \leq m \leq 12$ and so there exist digital $(6, m, 126)$-nets over $\mathbf{F}_{25}$ for these values of m. Furthermore, a comparison with the information available at [43] shows that for $m = 12$ this digital net has quality parameter t matching the best known value.

Suppose $l = ms - m + g - 5 = 125m + 5$ where $m \geq 5$. Note that the condition

$$|\mathcal{U}(126, 125m + 5, m)| \cdot 11859876 = \binom{120 + m}{125} \cdot 11859876 < 6^{20}$$

is satisfied for $5 \leq m \leq 10$ and so there exist digital $(5, m, 126)$-nets over $\mathbf{F}_{25}$ for these values of m. Furthermore, a comparison with the information available at [43] shows that for $m = 10$ this digital net has quality parameter t matching the best known value.

Chapter 8

A New Construction of (t,s)-Sequences

In this chapter we introduce the first new construction of (t, s)-sequences using global function fields since the fourth and final construction of Niederreiter and Xing [34] in 1996. Our construction is the first to make use of differentials, and it is based on the construction of Xing and Niederreiter [59] which provides the best known parameters and also the most general construction, since it uses places of arbitrary degree.

8.1 The Basic Construction of (t,s)-Sequences Using Differentials

Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least one rational place P_∞, let D be a divisor of F with $\deg(D) = -2$ and $P_\infty \notin \operatorname{supp}(D)$, let $P_1, \ldots, P_s$ be distinct places of F with $P_i \neq P_\infty$ for $1 \leq i \leq s$, and put

$e_i = \deg(P_i)$ for $1 \le i \le s$.

Note that we have $\dim \Omega(D) = g+1$, $\dim \Omega(D+P_\infty) = g$, and $\dim \Omega(D + (2g+1)P_\infty) = 0$, hence there exist integers $0 = n_0 < n_1 < \cdots < n_g \le 2g$ such that

$$\dim \Omega(D + n_u P_\infty) = \dim \Omega(D + (n_u+1)P_\infty) + 1 \qquad \text{for } 0 \le u \le g.$$

Now we choose

$$w_u \in \Omega(D + n_u P_\infty) \backslash \Omega(D + (n_u+1)P_\infty) \qquad \text{for } 0 \le u \le g.$$

It is easily seen that $\{w_0, w_1, \ldots, w_g\}$ is a basis of $\Omega(D)$. For $i = 1, \ldots, s$, consider the chain

$$\Omega(D) \subset \Omega(D - P_i) \subset \Omega(D - 2P_i) \subset \ldots$$

of vector spaces over $\mathbf{F}_q$. By starting from the basis $\{w_0, w_1, \ldots, w_g\}$ of $\Omega(D)$ and successively adding basis vectors at each step of the chain, we obtain for each $n \ge 1$ a basis

$$\{w_0, w_1, \ldots, w_g, \omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_{ne_i}^{(i)}\}$$

of $\Omega(D - nP_i)$. Now let z be a local parameter at P_∞. For $r = 0, 1, \ldots$ we put

$$z_r = \begin{cases} z^r dz & \text{if } r \notin \{n_0, n_1, \ldots, n_g\}, \\ w_u & \text{if } r = n_u \text{ for some } u \in \{0, 1, \ldots, g\}. \end{cases}$$

Note that $\nu_{P_\infty}((z_r)) = r$ for all $r \ge 0$. For $1 \le i \le s$ and $j \ge 1$ we have $\omega_j^{(i)} \in \Omega(D - kP_i)$ for some $k \ge 1$ and also $P_\infty \notin \text{supp}(D - kP_i)$, hence $\nu_{P_\infty}((\omega_j^{(i)})) \ge 0$. Thus, we have expansions at P_∞ of the form

$$\omega_j^{(i)} = \sum_{r=0}^{\infty} a_{r,j}^{(i)} z_r \qquad \text{for } 1 \le i \le s \text{ and } j \ge 1,$$

where all coefficients $a_{r,j}^{(i)} \in \mathbf{F}_q$. For $1 \le i \le s$ and $j \ge 1$ we define the sequence of elements $c_{r,j}^{(i)} \in \mathbf{F}_q$, $r = 0, 1, \ldots$, by considering the sequence of elements $a_{r,j}^{(i)}$, $r = 0, 1, \ldots$, and then deleting the terms with $r = n_u$ for some $u \in \{0, 1, \ldots, g\}$. Finally, we set up the system

$$C^{(\infty)} = \{\mathbf{c}_j^{(i)} = (c_{0,j}^{(i)}, c_{1,j}^{(i)}, \ldots) \in \mathbf{F}_q^\infty : 1 \le i \le s \text{ and } j \ge 1\}.$$

We write $S_\Omega(P_\infty, P_1, \ldots, P_s; D)$ for a sequence obtained from this system by the digital method.

Theorem 8.1. *Let $F/\mathbf{F}_q$ be a global function field of genus g and with at least one rational place P_∞, let D be a divisor of F with $\deg(D) = -2$ and $P_\infty \notin \operatorname{supp}(D)$, and let $P_1, \ldots, P_s$ be distinct places of F with $P_i \neq P_\infty$ for $1 \le i \le s$. Then $S_\Omega(P_\infty, P_1, \ldots, P_s; D)$ is a digital (t, s)-sequence constructed over $\mathbf{F}_q$ with*

$$t = g + \sum_{i=1}^{s} (e_i - 1),$$

where $e_i = \deg(P_i)$ for $1 \le i \le s$.

Proof. By Theorem 2.17, it suffices to show that for any $m > t$ and any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^s d_i = m - t$, the vectors

$$\pi_m(\mathbf{c}_j^{(i)}) = (c_{0,j}^{(i)}, \ldots, c_{m-1,j}^{(i)}) \in \mathbf{F}_q^m \quad \text{for } 1 \le j \le d_i, 1 \le i \le s,$$

are linearly independent over $\mathbf{F}_q$. Fix a set of integers $m, d_1, \ldots, d_s$ satisfying the above conditions. Let H be the set of i with $1 \le i \le s$ for which $d_i \ge 1$, and suppose that we have

$$\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} \pi_m(\mathbf{c}_j^{(i)}) = \mathbf{0} \in \mathbf{F}_q^m$$

for some $b_j^{(i)} \in \mathbf{F}_q$. With $R = \{n_0, n_1, \ldots, n_g\}$ this means that

$$\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} a_{r,j}^{(i)} = 0$$

for the first m nonnegative integers r that are not in R. Now consider the differential ω of F given by

$$\omega = \sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} \Big(\omega_j^{(i)} - \sum_{u=0}^{g} a_{n_u,j}^{(i)} w_u \Big) = \sum_{\substack{r=0 \\ r \notin R}}^{\infty} \Big(\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} a_{r,j}^{(i)} \Big) z_r.$$

Since $n_g \leq 2g$ and $g \leq m-1$ we have $\nu_{P_\infty}((\omega)) \geq m+g+1$, and together with the choice of the $\omega_j^{(i)}$ this shows that

$$\omega \in \Omega\Big(D - \sum_{i=1}^{s} \Big(\Big\lfloor \frac{d_i - 1}{e_i} \Big\rfloor + 1 \Big) P_i + (m+g+1) P_\infty \Big).$$

Note that

$$\begin{aligned} \deg \Big(D - \sum_{i=1}^{s} \Big(\Big\lfloor \frac{d_i - 1}{e_i} \Big\rfloor + 1 \Big) P_i + (m+g+1) P_\infty \Big) \\ &= -2 - \sum_{i=1}^{s} \Big(\Big\lfloor \frac{d_i - 1}{e_i} \Big\rfloor + 1 \Big) e_i + (m+g+1) \\ &\geq m - t - \sum_{i=1}^{s} d_i + 2g - 1 \\ &= 2g - 1. \end{aligned}$$

Therefore $\omega = 0$, and we have

$$\sum_{i \in H} \sum_{j=1}^{d_i} b_j^{(i)} \omega_j^{(i)} =: w \in \Omega(D).$$

Fix an $h \in H$. We claim that $b_j^{(h)} = 0$ for $1 \leq j \leq d_h$. Suppose, on the contrary, that some $b_j^{(h)} \neq 0$, then by the choice of the $\omega_j^{(h)}$ we have

$$\sum_{j=1}^{d_h} b_j^{(h)} \omega_j^{(h)} \in \Omega(D - kP_h) \backslash \Omega(D) \qquad \text{for some } k \geq 1,$$

and so

$$\nu_{P_h}\left(\left(\sum_{j=1}^{d_h} b_j^{(h)}\omega_j^{(h)}\right)\right) \leq \nu_{P_h}(D) - 1.$$

However, we also know that

$$\nu_{P_h}\left(\left(\sum_{j=1}^{d_h} b_j^{(h)}\omega_j^{(h)}\right)\right) = \nu_{P_h}\left(\left(w - \sum_{i\in H\setminus\{h\}}\sum_{j=1}^{d_i} b_j^{(i)}\omega_j^{(i)}\right)\right) \geq \nu_{P_h}(D),$$

a contradiction. Thus, for any $i \in H$, $b_j^{(i)} = 0$ for $1 \leq j \leq d_i$. □

Note that the only different condition in our construction to that of Xing and Niederreiter is that we use a divisor D with $\deg(D) = -2$, whereas they use a divisor D' with $\deg(D') = 2g$. Such divisors can always be found and hence any global function field $F/\mathbf{F}_q$ with places $P_\infty, P_1, \ldots, P_s$ can be used to construct two different digital (t,s)-sequences over $\mathbf{F}_q$, where $t = g + \sum_{i=1}^{s}(\deg(P_i) - 1)$.

A project of cataloging upper bounds on $d_q(s)$ for $q = 2, 3, 5$ and $1 \leq s \leq 50$ was begun by Niederreiter and Xing [34, Table 4], [36, Table 2], [38, Table 3], [37, Table 5], and has been continued by Niederreiter [26, Table 1], [27, Table 1]. We now provide an example which demonstrates that it is possible to use nonrational places to gain improved bounds on $d_q(s)$.

Example 8.2. Let $F/\mathbf{F}_5$ be the global function field given in [35, Example 4], i.e., $F = \mathbf{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x^2 - 2), \qquad y_2^5 - y_2 = \frac{x^4 - 1}{y_1 - 1},$$

$g(F/\mathbf{F}_5) = 11$ and $N(F/\mathbf{F}_5) = 32$. Consider the place in $\mathbf{F}_5(x)$ corresponding to $x^2 + 2x - 2$, this splits completely in the extension $K/\mathbf{F}_5(x)$ where $K = \mathbf{F}_5(x, y_1)$, and one of the places in K lying above $x^2 + 2x - 2$ splits completely in F/K. Therefore F contains at least 5 places of degree 2. Combining this with Theorem 8.1 (or [59, Theorem 2]) we obtain

$$d_5(32) \leq 12,$$

which is an improvement on the current bound $d_5(32) \leq 13$ given in [27, Table 1].

Chapter 9

Improved Bounds for (t,s)-Sequences

In this chapter, for certain values of b, we will improve the upper bound on the quantity

$$\limsup_{s\to\infty} \frac{t_b(s)}{s}$$

whose existence is implied by the previously mentioned result $t_b(s) = O(s)$.

We begin by recalling the definition of the quantity $X_q(s)$ that was introduced in [39, Section 8.4].

For a global function field $F/\mathbf{F}_q$ with $N(F) \geq 1$, exclude one rational place of F and list all other places according to nondecreasing degrees. If $P_1, \ldots, P_s$ are the first s places in the list, then put

$$\delta_s(F) = \sum_{i=1}^{s} (\deg(P_i) - 1).$$

Now define

$$X_q(s) = \min_F (g(F) + \delta_s(F)),$$

where the minimum is extended over all global function fields $F/\mathbf{F}_q$ with $N(F) \geq 1$. We know by Theorem 8.1 (and also by [59, Theorem 2]) that we have

$$d_q(s) \leq X_q(s) \quad \text{for all } s \geq 1.$$

The above result is based on the strongest known construction of (t,s)-sequences. Hence, we can bound $d_q(s)$ by finding towers of function fields with many places of small degree. Niederreiter and Xing [33], [59] made use of the tower of global function fields due to Garcia and Stichtenoth [9] which was the first explicit tower of function fields that was asymptotically good, i.e., it is a tower $\mathcal{F} = (F_1, F_2, \ldots)$ of function fields over $\mathbf{F}_q$ satisfying the condition

$$\lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} > 0.$$

In the decade since the last construction of (t,s)-sequences in [34], Garcia, Stichtenoth, and Thomas [10], Li, Maharaj, and Stichtenoth [21], and Bezerra, Garcia, and Stichtenoth [1] have all constructed new towers which are asymptotically good. In addition, Elkies *et al.* [7] have proved the existence of curves of every genus with many rational points. In the next four sections we will utilise these new results to produce improvements in the asymptotic theory of (t,s)-sequences. In Section 9.5 we investigate what these new results imply for the star discrepancy of sequences.

9.1 A Theorem of Garcia, Stichtenoth, and Thomas

We start with the following theorem of Garcia, Stichtenoth, and Thomas [10, Theorem 2.1], which makes use of tame towers of function fields.

Theorem 9.1. *Let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be a tower of function fields over $\mathbf{F}_q$ satisfying the following conditions:*

(i) All extensions F_{n+1}/F_n are tame.

(ii) The set $R = \{P \in \mathbf{P}_{F_1} : P$ is ramified in F_n/F_1 for some $n \geq 2\}$ is finite.

(iii) The set $T = \{P \in \mathbf{P}_{F_1} : \deg(P) = 1$ and P splits completely in all extensions $F_n/F_1\}$ is nonempty.

Then $\mathcal{F}$ is asymptotically good, and one has the estimate

$$\lim_{n\to\infty} \frac{N(F_n)}{g(F_n)} \geq \frac{2t}{2g(F_1) - 2 + r} =: \lambda(\mathcal{F})$$

where $t := |T|$ and $r := \sum_{P\in R} \deg(P)$.

For our purposes, we need to know the bounds for the number of rational places and the genus at each individual n. So we note that in the proof of the above theorem it is shown that

$$2g(F_n) \leq [F_n : F_1](2g(F_1) - 2 + r) + 2$$

and

$$N(F_n) \geq t \cdot [F_n : F_1].$$

We now introduce two propositions which make use of Theorem 9.1. Firstly, we use the rational places of one of Garcia, Stichtenoth, and Thomas's towers of function fields over $\mathbf{F}_q$ to bound $d_q(s)$.

Proposition 9.2. *Let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be a tower of function fields over $\mathbf{F}_q$ satisfying the conditions of Theorem 9.1. Assume further that F_1 is the rational function field and $[F_{n+1} : F_n] = m \geq 2$ for all $n \geq 1$. Then we have*

$$d_q(s) \leq \frac{m}{\lambda(\mathcal{F})} s + 1.$$

for all $s \geq 1$.

Proof. First let $1 \leq s \leq q$. Then

$$N(F_1/\mathbf{F}_q) = q + 1 \geq s + 1$$

and hence

$$d_q(s) \leq g(F_1) = 0.$$

Now let $s \geq q + 1$. Note that this implies $s \geq t$ and therefore

$$t \cdot m^{n-2} \leq s \leq t \cdot m^{n-1} - 1$$

for some integer $n \geq 2$. We know that

$$N(F_n/\mathbf{F}_q) \geq t \cdot m^{n-1}$$

and

$$g(F_n/\mathbf{F}_q) \leq \frac{m^{n-1}(r-2)+2}{2}.$$

Therefore

$$d_q(s) \leq g(F_n/\mathbf{F}_q) \leq \frac{m^{n-1}(r-2)+2}{2} \leq \frac{m(r-2)}{2t} s + 1 = \frac{m}{\lambda(\mathcal{F})} s + 1.$$

□

In the second proposition of this section we use the rational places of Garcia, Stichtenoth, and Thomas's towers of function fields over $\mathbf{F}_{q^2}$ to bound $d_q(s)$.

Proposition 9.3. *Let $\mathcal{E} = (E_1, E_2, ...)$ be a tower of function fields over $\mathbf{F}_q$ such that by setting $F_n := E_n \cdot \mathbf{F}_{q^2}$ we obtain a tower of function fields $\mathcal{F} = (F_1, F_2, ...)$ over $\mathbf{F}_{q^2}$ satisfying the conditions of Theorem 9.1. Assume further that E_1 is the rational function field, $[F_{n+1} : F_n] = m \geq 2$ for all $n \geq 1$, and $N(E_n/\mathbf{F}_q) \geq 1$ for all $n \geq 1$. Then if $t \cdot m$ is even we have*

$$d_q(s) \leq \left(\frac{2m}{\lambda(\mathcal{F})} + 1\right) s + 1 - \frac{2m}{\lambda(\mathcal{F})}$$

and if $t \cdot m$ is odd we have

$$d_q(s) \leq \left(\frac{2m}{\lambda(\mathcal{F})} + 1\right) s + 1 - \frac{m}{\lambda(\mathcal{F})}$$

for all $s \geq 1$.

Proof. First let $1 \leq s \leq q$. Then

$$N(E_1/\mathbf{F}_q) = q + 1 \geq s + 1$$

and hence

$$d_q(s) \leq g(E_1/\mathbf{F}_q) = 0.$$

Next let $q + 1 \leq s \leq \frac{1}{2}(q^2 + q)$. Then using all the rational places of $E_1/\mathbf{F}_q$ and $s - q$ places of degree 2 we obtain

$$d_q(s) \leq s - q \leq \left(\frac{2m}{\lambda(\mathcal{F})} + 1\right) s + 1 - \frac{2m}{\lambda(\mathcal{F})}.$$

Finally, let $s \geq \frac{1}{2}(q^2 + q) + 1$. If $t \cdot m$ is even we have

$$\frac{t \cdot m^{n-2} + 2}{2} \leq s \leq \frac{t \cdot m^{n-1} + 2}{2} - 1$$

for some integer $n \geq 2$, and if $t \cdot m$ is odd we have

$$\frac{t \cdot m^{n-2} + 1}{2} \leq s \leq \frac{t \cdot m^{n-1} + 1}{2} - 1$$

for some integer $n \geq 2$.

Results on constant field extensions [49, Lemma V.1.9] tell us that

$$g(E_n/\mathbf{F}_q) = g(F_n/\mathbf{F}_{q^2}) \leq \frac{m^{n-1}(r-2)+2}{2}$$

and

$$N(E_n/\mathbf{F}_q) + 2B_2(E_n/\mathbf{F}_q) = N(F_n/\mathbf{F}_{q^2}) \geq t \cdot m^{n-1}.$$

Clearly if $t \cdot m$ is even we have

$$N(E_n/\mathbf{F}_q) + B_2(E_n/\mathbf{F}_q) \geq \frac{t \cdot m^{n-1} + 2}{2}$$

and if $t \cdot m$ is odd we have

$$N(E_n/\mathbf{F}_q) + B_2(E_n/\mathbf{F}_q) \geq \frac{t \cdot m^{n-1} + 1}{2}.$$

Therefore when $t \cdot m$ is even we have

$$\begin{aligned} d_q(s) \leq g(E_n/\mathbf{F}_q) + s &\leq \frac{m^{n-1}(r-2)+2}{2} + s \\ &\leq \frac{m(s-1)(r-2)}{t} + 1 + s \\ &= \left(\frac{2m}{\lambda(\mathcal{F})} + 1\right)s + 1 - \frac{2m}{\lambda(\mathcal{F})} \end{aligned}$$

and when $t \cdot m$ is odd we have

$$\begin{aligned} d_q(s) \leq g(E_n/\mathbf{F}_q) + s &\leq \frac{m^{n-1}(r-2)+2}{2} + s \\ &\leq \frac{(2s-1)m(r-2)}{2t} + 1 + s \\ &= \left(\frac{2m}{\lambda(\mathcal{F})} + 1\right)s + 1 - \frac{m}{\lambda(\mathcal{F})}. \end{aligned}$$

□

9.2 Li, Maharaj, and Stichtenoth's Towers of Function Fields

The paper of Garcia, Stichtenoth, and Thomas [10] was followed by a paper of Li, Maharaj, and Stichtenoth [21] which made a systematic attempt to find optimal towers of function fields. The optimal towers that were found in [21] can be summarised as follows.

q	recursive polynomial	$\lambda(\mathcal{F})$
4	$x_n^2x_{n+1}^3 + (x_n^3 + x_n^2 + x_n)x_{n+1}^2 + (x_n + 1)x_{n+1} + x_n^3 + x_n = 0$	1
9	$2x_nx_{n+1}^2 + (x_n^2 + x_n + 1)x_{n+1} + x_n^2 + x_n + 2 = 0$	2
25	$(4x_n + 1)x_{n+1}^2 + (x_n^2 + x_n + 2)x_{n+1} + x_n + 3 = 0$	4
49	$(x_n^2 + 6)x_{n+1}^2 + x_nx_{n+1} + x_n^2 + 4 = 0$	6

Example 9.4. Applying Proposition 9.2 to the above towers, we obtain

$$\begin{aligned} d_4(s) &\leq 3s + 1, \\ d_9(s) &\leq s + 1, \\ d_{25}(s) &\leq \frac{s}{2} + 1, \\ d_{49}(s) &\leq \frac{s}{3} + 1. \end{aligned}$$

For $q = 9$, 25, and 49, these bounds represent improvements on the previous known theory, which was a result due to Xing and Niederreiter [59]. Namely, for any prime p and integer $e \geq 1$ we have

$$d_{p^{2e}}(s) \leq \frac{p}{p^e - 1}s,$$

whereas we have

$$d_{p^{2e}}(s) \leq \frac{2}{p^e - 1}s + 1$$

for $p^{2e} = 9$, 25, and 49. We note that as the bounds for these values of q are based on optimal towers of function fields whose polynomial is quadratic, they are the best bounds obtainable by Proposition 9.2.

Remark 9.5. It is possible to obtain the new bound $d_9(s) \leq s + 1$ using a different tower of function fields over $\mathbf{F}_9$ [10, Example 2.4].

Example 9.6. Let us consider Li, Maharaj, and Stichtenoth's tower of function fields $\mathcal{F} = \{\mathbf{F}_9(x_1 \ldots, x_n) : n \geq 1\}$ over $\mathbf{F}_9$, but with $\mathbf{F}_9$ replaced by $\mathbf{F}_3$, i.e., consider $\mathcal{E} = \{\mathbf{F}_3(x_1 \ldots, x_n) : n \geq 1\}$. Li, Maharaj, and Stichtenoth show that for $n \geq 2$ the place representing $x_1^4 + x_1^2 + x_1 + 1$ is totally ramified in the extension $\mathbf{F}_3(x_1 \ldots, x_n)/\mathbf{F}_3(x_1)$. Therefore, $\mathbf{F}_3$ is the full constant field of $\mathbf{F}_3(x_1 \ldots, x_n)$ for all $n \geq 1$. Note that for $n \geq 1$ the rational place of $\mathbf{F}_3(x_1, \ldots, x_{n+1})$ representing the zero of $x_{n+1} + 2$ lies over the rational place of $\mathbf{F}_3(x_1, \ldots, x_n)$ representing the zero of $x_n + 2$, and therefore $N(\mathbf{F}_3(x_1, \ldots, x_n)/\mathbf{F}_3) \geq 1$ for all $n \geq 1$. Then, considering the constant field extension $\mathbf{F}_3(x_1, \ldots, x_n)/\mathbf{F}_3 \cdot \mathbf{F}_9 = \mathbf{F}_9(x_1, \ldots, x_n)/\mathbf{F}_9$, we see that we can use Proposition 9.3 to obtain the bound

$$d_3(s) \leq 3s - 1.$$

For $q = 5$ and 7, Li, Maharaj, and Stichtenoth do not determine whether $\mathbf{F}_q$ is the full constant field of $\mathbf{F}_q(x_1 \ldots, x_n)$ for all $n \geq 1$. Instead they show that $\mathbf{F}_{q^2}$ is the full constant field of $\mathbf{F}_{q^2}(x_1 \ldots, x_n)$ by providing a place of $\mathbf{F}_{q^2}(x_1)$ which is totally ramified in $\mathbf{F}_{q^2}(x_1 \ldots, x_n)$ for all $n \geq 1$. Note that we could obtain a strong bound on $d_5(s)$ if $\mathbf{F}_5$ is the full constant field of $\mathbf{F}_5(x_1 \ldots, x_n)$, since the rational place of $\mathbf{F}_5(x_1, \ldots, x_{n+1})$ representing the zero of $x_{n+1}+2$ lies over the rational place of $\mathbf{F}_5(x_1, \ldots, x_n)$ representing the zero of $x_n + 2$ for all $n \geq 1$.

It would be nice if we could determine the full constant field of the above tower, but it is not overly important since we can gain bounds on $t_q(s)$, as opposed to $d_q(s)$, by using the following technique.

Example 9.7. We note a result of Niederreiter and Xing [33, Proposition 4] which states that for all integers $b \geq 2$, $h \geq 1$, and $s \geq 1$ we have

$$t_b(s) \leq ht_{b^h}(s) + (h-1)s.$$

Hence, we know that

$$t_5(s) \leq 2t_{25}(s) + s \leq 2d_{25}(s) + s \leq 2s + 2$$

and

$$t_7(s) \leq 2t_{49}(s) + s \leq 2d_{49}(s) + s \leq \frac{5}{3}s + 2.$$

For $q = 3$, 5, and 7, these bounds represent asymptotic improvements on the previous known theory. For $q = 3$ and 7, this was a result due to Xing and Niederreiter [59]. Namely, for any prime power q and integer $s \geq 1$ we have

$$d_q(s) \leq \frac{3q-1}{q-1}(s-1) - \frac{(2q+4)(s-1)^{1/2}}{(q^2-1)^{1/2}} + 2.$$

In particular,

$$d_3(s) \leq 4s - \frac{5}{2^{1/2}}(s-1)^{1/2} - 2 \qquad \text{for all } s \geq 1,$$

$$d_7(s) \leq \frac{10}{3}s - \frac{3^{3/2}}{2}(s-1)^{1/2} - \frac{4}{3} \qquad \text{for all } s \geq 1.$$

For $q = 5$, the previous best bound was obtained by Niederreiter and Xing [39, Remark 8.4.5] who used the rational places of a Hilbert class field tower to obtain the bound

$$d_5(s) \leq \frac{11}{4}s + 1 \qquad \text{for all } s \geq 1.$$

9.3 Curves of Every Genus with Many Rational Places Due to Elkies *et al.*

In all previous attempts to use global function fields to bound $d_q(s)$, the method has involved using towers of function fields. However, it is apparent that if we can find global function fields of every genus with many rational places, then we can also gain bounds on $d_q(s)$. When Niederreiter and Xing obtained their last construction of (t, s)-sequences, this was a barren area of research. Serre [45] had previously posed the question as to whether

$$\liminf_{g \to \infty} \frac{N_q(g)}{g} > 0,$$

but it was only recently that Elkies *et al.* [7] showed that the above inequality holds for every prime power q. Furthermore, in the case where q is a square, strong explicit bounds [7, Theorem 1.2 and Corollary 6.2] were obtained which we now reproduce.

Theorem 9.8. *We have*

$$\liminf_{g\to\infty}\frac{N_q(g)}{g}\geq\begin{cases}\dfrac{q^{1/2}-1}{2+\log_q 2} & \textit{if } q \textit{ is an even square,}\\ \dfrac{q^{1/2}-1}{2+\log_q 4} & \textit{if } q \textit{ is an odd square,}\\ \dfrac{2(q^{1/2}-1)}{2+(q^{1/2}+1)\cdot\log_q 2} & \textit{if } q \textit{ is an odd square.}\end{cases}$$

Whilst this theorem does not provide bounds on $d_q(s)$ for individual s, it does provide strong bounds on the asymptotic properties of $d_q(s)$. Namely, we have the following corollary.

Corollary 9.9. *We have*

$$\limsup_{s\to\infty}\frac{d_q(s)}{s}\leq\begin{cases}\dfrac{2+\log_q 2}{q^{1/2}-1} & \textit{if } q \textit{ is an even square,}\\ \dfrac{2+\log_q 4}{q^{1/2}-1} & \textit{if } q \textit{ is an odd square,}\\ \dfrac{2+(q^{1/2}+1)\cdot\log_q 2}{2(q^{1/2}-1)} & \textit{if } q \textit{ is an odd square.}\end{cases}$$

Proof. Let $q+1\leq s_1<s_2<\cdots$ be a sequence of integers such that

$$\lim_{i\to\infty}\frac{d_q(s_i)}{s_i}=\limsup_{s\to\infty}\frac{d_q(s)}{s}.$$

For any $i\geq 1$, let g_i be the least nonnegative integer such that $N_q(g_i)\leq s_i$ and $N_q(g_i+1)\geq s_i+1$. Then $d_q(s_i)\leq g_i+1$, and so

$$\frac{d_q(s_i)}{s_i}\leq\frac{g_i+1}{N_q(g_i)}.$$

Since $g_i\to\infty$ as $i\to\infty$, we obtain the desired result by letting $i\to\infty$. □

We know by the previously mentioned result of Xing and Niederreiter that if we have $q=p^{2e}$ where p is a prime and $e\geq 1$ is an integer then

$$d_q(s)\leq\frac{p}{q^{1/2}-1}s\quad\text{for all } s\geq 1.$$

Hence, we gain no improvement for even values of q. However, for odd values of q we have

$$\limsup_{s\to\infty} \frac{d_q(s)}{s} \leq \frac{2 + (q^{1/2}+1)\cdot \log_q 2}{2(q^{1/2}-1)}.$$

In particular,

$$\begin{aligned}
\limsup_{s\to\infty} \frac{d_9(s)}{s} &\leq \frac{1}{2} + \log_9 2 = 0.8154\ldots, \\
\limsup_{s\to\infty} \frac{d_{25}(s)}{s} &\leq \frac{1}{4} + \frac{3}{4}\log_{25} 2 = 0.4115\ldots, \\
\limsup_{s\to\infty} \frac{d_{49}(s)}{s} &\leq \frac{1}{6} + \frac{2}{3}\log_{49} 2 = 0.2854\ldots.
\end{aligned}$$

These bounds offer asymptotic improvements on the new results presented in Section 9.2.

We again note the result of Niederreiter and Xing which states that for all integers $b \geq 2$, $h \geq 1$, and $s \geq 1$ we have

$$t_b(s) \leq h t_{b^h}(s) + (h-1)s.$$

Hence, we also gain the bounds

$$\begin{aligned}
\limsup_{s\to\infty} \frac{t_3(s)}{s} &\leq 2(1 + \log_9 2) = 2.6309\ldots, \\
\limsup_{s\to\infty} \frac{t_5(s)}{s} &\leq \frac{3}{2}(1 + \log_{25} 2) = 1.8230\ldots, \\
\limsup_{s\to\infty} \frac{t_7(s)}{s} &\leq \frac{4}{3}(1 + \log_{49} 2) = 1.5708\ldots.
\end{aligned}$$

These bounds again offer asymptotic improvements on the new results presented in Section 9.2.

9.4 Bezerra, Garcia, and Stichtenoth's Towers of Function Fields

Recently, Bezerra, Garcia, and Stichtenoth [1] have constructed an explicit tower of function fields $\mathcal{F} = (F_1, F_2, \ldots)$ over $\mathbf{F}_{q^3}$ such that

$$\lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} \geq \frac{2(q^2-1)}{q+2}.$$

More specifically, we have

$$g(F_n) \leq \frac{(q+2)q^n}{2(q-1)}$$

and

$$N(F_n) \geq (q+1)q^n.$$

This provides the following proposition.

Proposition 9.10. *For any prime power q we have*

$$d_{q^3}(s) \leq \frac{q(q+2)}{2(q^2-1)} s$$

for all $s \geq 1$.

Proof. First let $1 \leq s \leq q^3$. Then

$$N(\mathbf{F}_{q^3}(x)/\mathbf{F}_{q^3}) = q^3 + 1$$

and hence

$$d_{q^3}(s) \leq g(\mathbf{F}_{q^3}(x)/\mathbf{F}_{q^3}) = 0.$$

Now let $s \geq q^3 + 1$ and let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be Bezerra, Garcia, and Stichtenoth's tower of function fields over $\mathbf{F}_{q^3}$. We have

$$(q+1)q^{n-1} \leq s \leq (q+1)q^n - 1$$

for some integer $n \geq 1$. We know that

$$g(F_n/\mathbf{F}_{q^3}) \leq \frac{q+2}{2(q-1)}q^n$$

and

$$N(F_n/\mathbf{F}_{q^3}) \geq (q+1)q^n.$$

Therefore

$$d_{q^3}(s) \leq g(F_n/\mathbf{F}_{q^3}) \leq \frac{q+2}{2(q-1)}q^n \leq \frac{q(q+2)}{2(q^2-1)}s.$$

□

Example 9.11. Proposition 9.10 provides the bounds

$$d_8(s) \leq \frac{4}{3}s$$

and

$$d_{27}(s) \leq \frac{15}{16}s.$$

It was shown by Niederreiter and Xing [37, Theorem 7] that by using the rational places of a Hilbert class field tower, it is possible to obtain the bound

$$d_{27}(s) \leq \frac{12}{5}s + 1 \quad \text{for all } s \geq 1.$$

Our new bound for $d_{27}(s)$ is clearly much stronger.

There is a well-known website of Brouwer [2] which lists the best possible linear $[n, k, d]$ codes for various values of q. Recently, a new website has been launched by Schürer and Schmid [43] with the similar aim of cataloging (t, m, s)-nets and (t, s)-sequences. The values of q for which the website is valid are 2, 3, 4, 5, 7, 8, 9, 16, 25, 27, and 32.

We note that in Sections 9.2-9.4 we have introduced improved bounds on $t_q(s)$ for all the odd prime powers mentioned above. Namely, $q = 3$, 5, 7, 9, 25, and 27. Furthermore, we improved the bound for $q = 8$. The known bounds for $q = 2$, 4, and 16 seem strong, whilst the known bound for $q = 32$ is weak due to the lack of knowledge about towers of function fields over $\mathbf{F}_q$ in the case where q is quintic.

9.5 Implications for Star Discrepancy

As we mentioned in Section 2.3, Niederreiter [23] showed that for any (t, s)-sequence S in base b we have

$$D_N^*(S) \leq C_b(s,t)N^{-1}(\log N)^s + O(b^t N^{-1}(\log N)^{s-1}) \quad \text{for all } N \geq 2,$$

where

$$C_b(s,t) = \frac{b^t}{s!} \cdot \frac{b-1}{2\lfloor b/2 \rfloor} \left(\frac{\lfloor b/2 \rfloor}{\log b} \right)^s.$$

We know that since $t_b(s) = O(s)$, $C_b(s, t_b(s))$ tends to 0 as $s \to \infty$ for all integers $b \geq 2$. In this section we examine which values of b provide the fastest convergence rates. It is easily seen that

$$\limsup_{s\to\infty} \frac{\log C_b(s, t_b(s)) + s(\log s - 1)}{s} = \log \left(\frac{\lfloor b/2 \rfloor}{\log b} \right) + \log b \cdot \limsup_{s\to\infty} \frac{t_b(s)}{s}.$$

Thus, it is clear that finding the value of b which provides the strongest bound on the star discrepancy for high dimensions is equivalent to bounding the following function.

Definition 9.12. For a given integer $b \geq 2$ we define

$$C(b) = \log \left(\frac{\lfloor b/2 \rfloor}{\log b} \right) + \log b \cdot \limsup_{s\to\infty} \frac{t_b(s)}{s}.$$

Example 9.13. There is currently no research on the quantity $C(b)$ available in the literature. However, using previously known bounds on $t_b(s)$, the best bound we can obtain for $C(b)$ is in the case $b = 16$, where we have

$$\limsup_{s\to\infty} \frac{t_{16}(s)}{s} \leq \frac{2}{3}$$

and hence

$$C(16) \leq \frac{11}{3}\log 2 - \log\log 2 = 2.9080\ldots.$$

The new bound for $t_9(s)$ from Section 9.3 gives us

$$C(9) \leq \log 12 - \log\log 3 = 2.3908\ldots.$$

Therefore, for large s, the case $b = 9$ provides the best currently known bound for the star discrepancy of a (t, s)-sequence.

Remark 9.14. Note that the weaker bound for $d_9(s)$ presented in Section 9.2 would also have produced a stronger bound than for $b = 16$.

Remark 9.15. Recently, the function $C_b(s, t)$ that was provided by Niederreiter [23] has been improved upon by Kritzer [19], who replaced $C_b(s, t)$ with a function $F_b(s, t)$ which provides a stronger bound. However, this does not affect the asymptotic analysis in this section, as it is easily seen that

$$\limsup_{s\to\infty} \frac{\log C_b(s, t_b(s)) + s\log s}{s} = \limsup_{s\to\infty} \frac{\log F_b(s, t_b(s)) + s\log s}{s}.$$

Bibliography

[1] J. Bezerra, A. Garcia, and H. Stichtenoth, An explicit tower of function fields over cubic finite fields and Zink's lower bound, *J. Reine Angew. Math.* **589**, 159–199 (2005).

[2] A.E. Brouwer, Bounds on minimum distance of linear codes, available online at `http://www.win.tue.nl/∼aeb/voorlincod.html`.

[3] C.S. Ding, H. Niederreiter, and C.P. Xing, Some new codes from algebraic curves, *IEEE Trans. Inform. Theory* **46**, 2638–2642 (2000).

[4] G. Dorfer and H. Maharaj, Generalized AG codes and generalized duality, *Finite Fields Appl.* **9**, 194–210 (2003).

[5] N.D. Elkies, Excellent nonlinear codes from modular curves, *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pp. 200–208, ACM, New York, 2001.

[6] N.D. Elkies, Still better nonlinear codes from modular curves, preprint, 2003.

[7] N.D. Elkies, E.W. Howe, A. Kresch, B. Poonen, J.L. Wetherell, and M.E. Zieve, Curves of every genus with many points. II. Asymptotically good families, *Duke Math. J.* **122**, 399–422 (2004).

[8] H. Faure, Discrépance de suites associées à un système de numération (en dimension s) (French), *Acta Arith.* **41**, 337–351 (1982).

[9] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121**, 211–222 (1995).

[10] A. Garcia, H. Stichtenoth, and M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3**, 257–274 (1997).

[11] V.D. Goppa, Codes that are associated with divisors (Russian), *Problemy Peredači Informacii* **13**, 33–39 (1977).

[12] V.D. Goppa, Codes on algebraic curves (Russian), *Dokl. Akad. Nauk SSSR* **259**, 1289–1290 (1981).

[13] V.D. Goppa, Algebraic-geometric codes (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **46**, 762–781 (1982).

[14] D. Hachenberger, H. Niederreiter, and C.P. Xing, Function-field codes, submitted.

[15] A.E. Heydtmann, Generalized geometric Goppa codes, *Comm. Algebra* **30**, 2763–2789 (2002).

[16] E. Hlawka, Funktionen von beschränkter Variation in der Theorie der Gleichverteilung (German), *Ann. Mat. Pura Appl. (4)* **54**, 325–333 (1961).

[17] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**, 721–724 (1981).

[18] J.F. Koksma, A general theorem from the theory of uniform distribution modulo 1 (Dutch), *Mathematica, Zutphen. B.* **11**, 7–11 (1942).

[19] P. Kritzer, Improved upper bounds on the star discrepancy of (t, m, s)-nets and (t, s)-sequences, *J. Complexity* **22**, 336–347 (2006).

[20] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.

[21] W.-C.W. Li, H. Maharaj, and H. Stichtenoth, New optimal tame towers of function fields over small finite fields, *Algorithmic Number Theory* (C. Fieker and D.R. Kohel, eds.), Lecture Notes in Comput. Sci., Vol. 2369, pp. 372–389, Springer, Berlin, 2002.

[22] Yu.I. Manin, What is the maximum number of points on a curve over $\mathbf{F}_2$?, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**, 715–720 (1981).

[23] H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104**, 273–337 (1987).

[24] H. Niederreiter, Low-discrepancy and low-dispersion sequences, *J. Number Theory* **30**, 51–70 (1988).

[25] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[26] H. Niederreiter, Constructions of (t, m, s)-nets, *Monte Carlo and Quasi-Monte Carlo Methods 1998* (H. Niederreiter and J. Spanier, eds.), pp. 70–85, Springer, Berlin, 2000.

[27] H. Niederreiter, Constructions of (t, m, s)-nets and (t, s)-sequences, *Finite Fields Appl.* **11**, 578–600 (2005).

[28] H. Niederreiter and F. Özbudak, Constructions of digital nets using global function fields, *Acta Arith.* **105**, 279–302 (2002).

[29] H. Niederreiter and F. Özbudak, Constructive asymptotic codes with an improvement on the Tsfasman-Vlăduţ-Zink and Xing bounds, *Coding, Cryptography and Combinatorics* (K.Q. Feng, H. Niederreiter, and C.P. Xing, eds.), Progr. Comput. Sci. Appl. Logic, Vol. 23, pp. 259–275, Birkhäuser, Basel, 2004.

[30] H. Niederreiter and F. Özbudak, Further improvements on asymptotic bounds for codes using distinguished divisors, *Finite Fields Appl.*, to appear.

[31] H. Niederreiter and G. Pirsic, Duality for digital nets and its applications, *Acta Arith.* **97**, 173–182 (2001).

[32] H. Niederreiter and C.P. Xing, Low-discrepancy sequences obtained from algebraic function fields over finite fields, *Acta Arith.* **72**, 281–298 (1995).

[33] H. Niederreiter and C.P. Xing, Low-discrepancy sequences and global function fields with many rational places, *Finite Fields Appl.* **2**, 241–273 (1996).

[34] H. Niederreiter and C.P. Xing, Quasirandom points and global function fields, *Finite Fields and Applications* (S. Cohen and H. Niederreiter, eds.), London Math. Soc. Lecture Note Ser., Vol. 233, pp. 269–296, Cambridge University Press, Cambridge, 1996.

[35] H. Niederreiter and C.P. Xing, Global function fields with many rational places over the quinary field, *Demonstratio Math.* **30**, 919–930 (1997).

[36] H. Niederreiter and C.P. Xing, The algebraic-geometry approach to low-discrepancy sequences, *Monte Carlo and Quasi-Monte Carlo Methods 1996* (H. Niederreiter *et al.*, eds.), Lecture Notes in Statist., Vol. 127, pp. 139–160, Springer, New York, 1998.

[37] H. Niederreiter and C.P. Xing, Nets, (t, s)-sequences, and algebraic geometry, *Random and Quasi-Random Point Sets* (P. Hellekalek and G. Larcher, eds.), Lecture Notes in Statist., Vol. 138, pp. 267–302, Springer, New York, 1998.

[38] H. Niederreiter and C.P. Xing, Global function fields with many rational places and their applications, *Finite Fields: Theory, Applications, and Algorithms* (R.C. Mullin and G.L. Mullen, eds.), Contemp. Math., Vol. 225, pp. 87–111, Amer. Math. Soc., Providence, RI, 1999.

[39] H. Niederreiter and C.P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge University Press, Cambridge, 2001.

[40] H. Niederreiter and C.P. Xing, A construction of digital nets with good asymptotic behavior, Technical Report, Temasek Laboratories, National University of Singapore, 2001.

[41] H. Niederreiter, C.P. Xing, and K.Y. Lam, A new construction of algebraic-geometry codes, *Appl. Algebra Engrg. Comm. Comput.* **9**, 373–381 (1999).

[42] F. Özbudak and H. Stichtenoth, Constructing codes from algebraic curves, *IEEE Trans. Inform. Theory* **45**, 2502–2505 (1999).

[43] R. Schürer and W.Ch. Schmid, MinT: A database for optimal net parameters, *Monte Carlo and Quasi-Monte Carlo Methods 2004* (H. Niederreiter and D. Talay, eds.), pp. 457–469, Springer, Berlin, 2006; updated online at `http://mint.sbg.ac.at`.

[44] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini (French), *C. R. Acad. Sci. Paris Sér. I Math.* **296**, 397–402 (1983).

[45] J.-P. Serre, Nombres de points des courbes algébriques sur $\mathbf{F}_q$ (French), *Séminaire de théorie des nombres. 1982–1983*, Exp. No. 22, Université de Bordeaux I, Talence, 1983.

[46] J.-P. Serre, *Rational Points on Curves over Finite Fields*, Lecture Notes, Harvard University, 1985.

[47] C.E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* **27**, 379–423 (1948).

[48] I.M. Sobol', Distribution of points in a cube and approximate evaluation of integrals (Russian), *Ž. Vyčisl. Mat. i Mat. Fiz.* **7**, 784–802 (1967).

[49] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[50] H. Stichtenoth and C.P. Xing, Excellent nonlinear codes from algebraic function fields, *IEEE Trans. Inform. Theory* **51**, 4044–4046 (2005).

[51] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[52] M.A. Tsfasman, S.G. Vlăduţ, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109**, 21–28 (1982).

[53] S.G. Vlăduţ, An exhaustion bound for algebro-geometric "modular" codes (Russian), *Problemy Peredachi Informatsii* **23**, 28–41 (1987).

[54] S.G. Vlăduţ and V.G. Drinfeld, The number of points of an algebraic curve (Russian), *Funktsional. Anal. i Prilozhen.* **17**, 68–69 (1983).

[55] S.G. Vlăduţ and Yu.I. Manin, Linear codes and modular curves (Russian), *Current Problems in Mathematics. Vol. 25* (R.V. Gamkrelidze,

ed.), Progress in Science and Technology, pp. 209–257, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[56] H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins (German), *Math. Ann.* **77**, 313–352 (1916).

[57] C.P. Xing, Algebraic-geometry codes with asymptotic parameters better than the Gilbert-Varshamov and the Tsfasman-Vlăduţ-Zink bounds, *IEEE Trans. Inform. Theory* **47**, 347–352 (2001).

[58] C.P. Xing, Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound, *IEEE Trans. Inform. Theory* **49**, 1653–1657 (2003).

[59] C.P. Xing and H. Niederreiter, A construction of low-discrepancy sequences using global function fields, *Acta Arith.* **73**, 87–102 (1995).

[60] C.P. Xing and H. Niederreiter, Digital nets, duality, and algebraic curves, *Monte Carlo and Quasi-Monte Carlo Methods 2002* (H. Niederreiter, ed.), pp. 155–166, Springer, Berlin, 2004.

[61] C.P. Xing, H. Niederreiter, and K.Y. Lam, A generalization of algebraic-geometry codes, *IEEE Trans. Inform. Theory* **45**, 2498–2501 (1999).