Some New Constructions of Asymptotically Good Code Sequences

Nils Henry Williams Rasmussen

Master's Thesis in
Algebraic Geometry

Department of Mathematics
University of Bergen
Norway

30 May 2006

Acknowledgements

I first of all want to thank my advisor, Professor Trygve Johnsen, for introducing me to the field of algebraic-geometric codes. His suggestions on topics of interest have been most valuable for the way this thesis has developed.

I also want to thank everybody else at Pure Mathematics who have in some way contributed to this thesis.

Contents

Chapter 1

Introduction

1.1 Asymptotic Properties of Codes

Let n be a positive integer and q a prime power. A q-ary code C of length n is a nonempty subset of $\mathbb{F}_q^n$ with at least two elements. The elements of C will be called *codewords*. The *distance* between two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is $d(x, y) := |\{i \in \{1, \ldots, n\} \,|\, x_i \neq y_i\}|$. The *weight* of a vector x is $\mathrm{wt}(x) := d(x, 0)$. The *minimum distance* of C is the smallest positive integer $d \leq n$ such that there exist two elements $x, y \in C$ satisfying $d(x, y) = d$. The dimension of C is $k := \log_q(|C|)$. A q-ary code of length n, dimension k, and minimum distance d is called an $[n, k, d]_q$ code. If it is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$, we say that C is an $[n, k, d]_q$-linear code. Note that in that case, the minimum distance of C is the same as the minimum weight among the nonzero codewords.

We furthermore define the *relative minimum distance* $\delta := d/n$ and the *coderate* $R := k/n$.

In this thesis we will be interested in infinite sequences $(C_i)_{i=1}^{\infty}$ of codes where the length approaches infinity. Given $\delta \in [0, 1]$, we are interested in finding an infinite sequence $(C_i)_{i=1}^{\infty}$ of $[n_i, k_i, d_i]_q$ codes C_i with $\delta = \liminf_{i\to\infty} d_i/n_i$ such that $R = \liminf_{i\to\infty} k_i/n_i$ is nonzero. If the code sequence satisfies $\liminf_{i\to\infty} d_i/n_i \neq 0$ and $\liminf_{i\to\infty} k_i/n_i \neq 0$, we say that it is *asymptotically good*.

We define $U_q := \{(\delta, R) \,|\, \text{there exists an infinite sequence of } [n_i, k_i, d_i]_q \text{ codes } (C_i)_{i=1}^{\infty} \text{ with } n_i \to \infty \text{ such that } d_i/n_i \to \delta \text{ and } k_i/n_i \to R\}$. It is well-known that there exists a continuous function $\alpha_q(\delta)$ such that

$$U_q = \{(\delta, R) \,|\, 0 \leq R \leq \alpha_q(\delta)\}.$$

To this date, we only know some upper and lower bounds for this function, but not the exact values of it, except for the points $(0, 1)$ and $(\delta, 0)$ for $(q-1)/q \leq \delta \leq 1$. The subject of finding new bounds for $\alpha_q(\delta)$ has been the issue of some considerable research throughout the years.

In 1950, the Gilbert–Varshamov bound was found. It states that

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

where

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta) \log_q(1-\delta)$$

is the q-ary entropy function. For δ close to 0 and close to $(q-1)/q$, this is still the best bound known to this date. The bound was not improved until 1982.

The 1982 improvement—known as the Tsfasman–Vlăduţ–Zink bound—was due to the discovery of algebraic-geometric codes defined in 1981 by V.D. Goppa. Let X be a nonsingular, projective curve defined over $\mathbb{F}_q$, and let n be a positive integer less than or equal to the number of $\mathbb{F}_q$-rational points on X. Let $P_1, \ldots, P_n$ be $\mathbb{F}_q$-rational points on X, and let G be an $\mathbb{F}_q$-rational divisor with support disjoint from $\{P_1, \ldots, P_n\}$. Define the mapping

$$\begin{aligned} \psi : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

We call the image of this mapping a *Goppa code*. The 1982 improvement used an infinite sequence of curves with a large number of $\mathbb{F}_q$-rational points, and a Goppa code was defined on each curve. The length of the code was equal to the number of $\mathbb{F}_q$-rational points on the curve in question. This resulted in the bound

$$\alpha_q(\delta) \geq R_{\mathrm{TVZ}} := 1 - \delta - \frac{1}{\sqrt{q} - 1},$$

given that q is a square prime power. For $q \geq 49$, this became an improvement of the Gilbert–Varshamov bound for δ close to $q/(2(q-1))$. For larger values of q, the interval of improvement increases.

To my knowledge, the Tsfasman–Vlăduţ–Zink bound wasn't improved until 2001, when Chaoping Xing found good divisors G on X which increased the minimum distance of the Goppa codes around the areas where R_{TVZ} and R_{GV} intersect. In 2003, Xing found a further improvement using nonlinear codes defined over algebraic curves, which was a linear improvement of the Tsfasman–Vlăduţ–Zink bound. That same year, Elkies found another linear improvement, which to this date is still the best one. It is given by

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q} - 1} + \log_q \left(1 + \frac{1}{q^3}\right)$$

for square prime powers q.

In this thesis, I have given a presentation of how all these results have been found. I open with the classical bounds, such as the upper Plotkin bound and the Gilbert–Varshamov bound. All this is in Chapter 2. The following chapter presents theory about algebraic curves over finite fields which is used throughout the entire rest of this thesis. Chapter 3 concludes with the Riemann–Roch theorem for curves over finite fields.

Chapter 4 presents the construction of Goppa codes and closes with a code sequence found by Chaoping Xing in 2005 that shows that Goppa codes attain the asymptotic Gilbert–Varshamov bound. In Chapter 5 we get to see how these codes can be used to find the Tsfasman–Vlăduţ–Zink bound. In Chapter 6 I present the two improvements found in 2003.

Before presenting my own work and results, I also touch three other subjects concerning special kinds of codes. Stichtenoth discovered in 2005 that transitive codes meet Elkies's 2003 bound. A natural question to ask is then whether transitive codes are as asymptotically good as codes in general, which today is still unanswered. An outline of Stichtenoth's construction is presented in Chapter 7.

The second subject I touch is the asymptotic properties of frameproof codes, which Chaoping Xing found a new lower bound for in 2002. The reason why I have included a chapter of frameproof codes in this thesis, is that any linear code is also a frameproof code, and so it

follows that all asymptotic results we have obtained for linear codes so far in my thesis also apply for frameproof codes. All of this we find in Chapter 8.

Finally, I present some other possible constructions of codes from algebraic geometry, found by Xing, Niederreiter, and Lam. Such work has been important when it comes to improvements of the Tsfasman–Vlăduţ–Zink bound, since both 2003 improvements were made by codes different from Goppa codes. However, some constructions have proved to give the same codes as the Goppa construction gives us. In Chapter 9 I give two cases where the codes turn out to be Goppa codes and one case where they don't, which I take a closer look at in the last two chapters.

1.2 Generalised Algebraic-Geometric Codes

The code construction presented in the end of Chapter 9 defines a generalisation of the Goppa codes and was found in 1999 by Xing, Niederreiter, and Lam. In short, with notations as before, it involves evaluating the functions of $L(G)$ in closed points of higher degree on the curve X. If s is a positive integer and $P_1, \ldots, P_s$ are closed points of degree $k_1, \ldots, k_s$, respectively, let $C_1, \ldots, C_s$ be $[n_i, k_i, d_i]_q$-linear codes, respectively, where $n_1, \ldots, n_s$ are positive integers. Let G be an $\mathbb{F}_q$-rational divisor with support disjoint from $\{P_1, \ldots, P_s\}$. If $f \in L(G)$, then $f(P_i)$ is an element in $\mathbb{F}_{q^{k_i}}$, $0 \leq i \leq s$. Define isomorphisms $\phi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$. Let $n = n_1 + \cdots + n_s$. Define the mapping

$$\begin{aligned} \phi : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (\phi_1(f(P_1)), \ldots, \phi_s(f(P_s))). \end{aligned}$$

We call the image of ϕ a *generalised algebraic-geometric code*.

It is obvious that this is a generalisation of the Goppa codes. A natural question to ask is whether constructions involving Goppa codes can be generalised to involve generalised algebraic-geometric codes. I have made two attempts of this in Chapter 10. The first construction, presented in Section 10.1, involves using all points of degree 1 and 2 on the curves of an infinite curve sequence with many $\mathbb{F}_{q^2}$-rational points. The codes $C_1, \ldots, C_s$ are all $[1, 1, 1]_q$ and $[2, 2, 1]_q$ codes. This has given the rather pleasing result

$$R \geq R_1 := 1 - 2\delta - \frac{1}{q-1},$$

for any prime power q. This is not a good bound for large values of δ, but for small values, this comes very close to the Gilbert–Varshamov bound.

Another idea I have tried out, is letting $C_1, \ldots, C_s$ be asymptotically good codes, the lengths of which approach infinity as the length of C approaches infinity. Such a construction is given in Section 10.3. It appears that this also gives us an asymptotically good code sequence, but not as good as R_1 except for large values of δ.

For the sake of completeness, I have also included a construction made by Antonino Spera, presented as R_2 in Section 10.2, which is interesting because it doesn't demand a curve *sequence*, but only one single curve.

Improvements made on Goppa codes should also be possible to make on generalised algebraic-geometric codes. Xing's 2001 improvement using good divisors G was a natural start, since it improves the codes for small values of δ, and it was very tempting to try and

improve R_1 around the areas where it is closest to the Gilbert–Varshamov bound. The attempt produced a successful result, although the improvement is not enough to reach the Gilbert–Varshamov bound. It is all presented in Section 11.1.

It is an open question whether other improvements made on Goppa codes can also be made on generalised algebraic-geometric codes. One such question is presented in the end of Chapter 11.

Chapter 2

Bounds on Codes

In this chapter I present the classical upper and lower bounds on codes, concluding with the 1950 Gilbert–Varshamov bound. I begin by introducing some notation and important facts.

Throughout this chapter, when we are given a code C and nothing else is mentioned, the minimum distance of C will be assumed to be d, the dimension will be k, the code length n, the relative minimum distance δ, and the number of codewords M.

Most of this material is taken from [10], pp. 25–37.

Definition 2.1. *Let q be a prime power. We define $V_q := \{(\delta, R) \in [0,1]^2 \,|\, \text{there exists an } [n,k,d]_q\text{-code with } \frac{d}{n} = \delta \text{ and } \frac{k}{n} = R\}$. U_q is the set of points (δ, R) such that there exists an infinite sequence of codes $(C_i)_{i=1}^{\infty}$ with minimum distance d_i, dimension k_i, and length n_i such that $n_i \to \infty$ and*

$$\lim_{i\to\infty} (d_i/n_i, k_i/n_i) = (\delta, R).$$

If $\delta, R > 0$, then we say that the code sequence is asymptotically good.

Proposition 2.2. *Let q be a prime power. There exists a continuous function $\alpha_q(\delta), \delta \in [0,1]$, such that*

$$U_q = \{(\delta, R) \,|\, 0 \le R \le \alpha_q(\delta)\}.$$

Moreover, $\alpha_q(0) = 1$, and $\alpha_q(\delta) = 0$ for $\frac{q-1}{q} \le \delta \le 1$. We also have that $\alpha_q(\delta)$ decreases in the interval $[0, \frac{q-1}{q}]$.

Proof. See Theorem 1.3.1 in [13]. □

Note that this function is of the form $\alpha_q(\delta) = \sup\{R \,|\, (\delta, R) \in U_q\}$. This proposition is also valid if we restrict U_q to only apply for linear codes. We then denote the function by $\alpha_q^{\text{lin}}(\delta)$.

Theorem 2.3 (the Singleton Bound). *Let q be a prime power and n, k, d positive integers. If C is an $[n,k,d]_q$ code, then*

$$k \le n - d + 1.$$

Proof. Suppose C has minimum distance d. For each codeword $(x_1, \ldots, x_n)$, delete the last $d-1$ elements $x_{n-d+2}, \ldots, x_n$ such that we are left with $(x_1, \ldots, x_{n-d+1})$. Then all the words are still different from one another, or else the minimum distance would be strictly less than d. Now we have a code C' of length $n - d + 1$ and the same number of words as in C. We have $q^k = |C| = |C'| \le q^{n-d+1}$, so $k \le n - d + 1$. □

Corollary 2.4 (the Asymptotic Singleton Bound). *Let q be a prime power. We have that*

$$\alpha_q(\delta) \leq 1 - \delta.$$

Proof. Since $k \leq n - d + 1$, dividing by n on both sides yields $R \leq 1 - \delta + \frac{1}{n}$. Letting $n \to \infty$, we get $\alpha_q(\delta) \leq 1 - \delta$. □

Theorem 2.5 (the Plotkin Bound, 1960). *Let q be a prime power. For any $[n, k, d]_q$-code, we have*

$$d \leq \frac{nq^k(q-1)}{(q^k - 1)q}.$$

Proof. The average distance of all pairs of codewords can't be less than the minimum distance d. Let $M = q^k$, the number of codewords in C. The number of all ordered pairs of codewords is $M(M-1)$. Then

$$d \leq \frac{1}{M(M-1)} \sum_{x,y \in C} d(x, y).$$

If x is in C, denote it by $(x_1, \ldots, x_n)$. Set $m_{i,a} = |\{x \in C \,|\, x_i = a\}|$. It is clear that

$$\sum_{a \in \mathbb{F}_q} m_{i,a} = M$$

for any $i \in \{1, \ldots, n\}$. Let $\delta_{a,b} = 1$ if $a = b$ and $\delta_{a,b} = 0$ if $a \neq b$. We have

$$\begin{aligned}
M(M-1)d &\leq \sum_{x,y \in C} d(x, y) = \sum_{i=1}^{n} \sum_{x,y \in C} (1 - \delta_{x_i, y_i}) \\
&= \sum_{i=1}^{n} \sum_{a,b \in \mathbb{F}_q} (1 - \delta_{a,b}) m_{i,a} m_{i,b} = \sum_{i=1}^{n} \left(\left(\sum_{a \in \mathbb{F}_q} m_{i,a} \right)^2 - \sum_{a \in \mathbb{F}_q} m_{i,a}^2 \right) \\
&= \sum_{i=1}^{n} \left(M^2 - \sum_{a \in \mathbb{F}_q} m_{i,a}^2 \right) \leq \sum_{i=1}^{n} \left(M^2 - \frac{1}{q} \left(\sum_{a \in \mathbb{F}_q} m_{i,a} \right)^2 \right) \\
&= n \frac{q-1}{q} M^2.
\end{aligned}$$

The last inequality follows from the Cauchy–Schwartz inequality: In general,

$$\left(\sum_{a \in \mathbb{F}_q} x_a y_a \right)^2 \leq \left(\sum_{a \in \mathbb{F}_q} x_a^2 \right) \left(\sum_{a \in \mathbb{F}_q} y_a^2 \right).$$

The results in the calculations follow when we put each $y_a = 1$ and each $x_a = m_{i,a}$. This completes the proof. □

Corollary 2.6 (the Asymptotic Plotkin Bound). *Let q be a prime power. We have*

$$\alpha_q(\delta) = 0 \qquad \textit{for} \qquad \frac{q-1}{q} < \delta \leq 1$$

and

$$\alpha_q(\delta) \leq R_P(\delta) := 1 - \frac{q}{q-1}\delta \qquad \textit{for} \qquad 0 \leq \delta \leq \frac{q-1}{q}.$$

Proof. When $d > n\frac{q-1}{q}$, then Theorem 2.5 gives us

$$\begin{aligned} d &\leq \frac{nq^k(q-1)}{q(q^k-1)} \\ q^k n(q-1) &\geq dqq^k - dq \\ q^k(n(q-1)-dq) &\geq -dq \\ q^k(dq-n(q-1)) &\leq dq \\ M = q^k &\leq \frac{dq}{dq-n(q-1)} = \frac{d}{d-n\frac{q-1}{q}}. \end{aligned} \tag{2.1}$$

Now, if we fix $\delta = \frac{d}{n}$, the expression on the right remains constant for varying n. If we take logarithms on both sides, divide by n on both sides, and let $n \to \infty$, we get 0 on the right-hand side, and so $\frac{k}{n} = R$ goes to 0 as well, proving the first part of the corollary.

In order to prove the second part, we must construct a code C' of length n' small enough so that $d > n'\frac{q-1}{q}$. Assume $0 \leq \delta \leq \frac{q-1}{q}$ and define

$$n' = \left\lfloor \frac{(d-1)q}{q-1} \right\rfloor.$$

Then $n' < n$, since

$$\left\lfloor \frac{(d-1)q}{q-1} \right\rfloor \leq \frac{(d-1)q}{q-1} \leq \frac{d-1}{\delta} < n.$$

Also, it is clear that $d > n'\frac{q-1}{q}$, since

$$n' \cdot \frac{q-1}{q} = \left\lfloor \frac{(d-1)q}{q-1} \right\rfloor \cdot \frac{q-1}{q} \leq \frac{(d-1)q}{q-1} \cdot \frac{q-1}{q} = d-1 < d.$$

So given a code C' with word length n' and minimum distance d, we are allowed to apply (2.1).

We define C' the following way: Consider the $n-n'$ last symbols of the codewords of C and consider the different subsets of words ending in the same $n-n'$ symbols. Then one of these subsets has M' elements where

$$M' \geq \frac{M}{q^{n-n'}} = q^{n'-n+k},$$

or else we would have $M < q^{n'-n+k} \cdot q^{n-n'} = q^k$, a contradiction. We let C' consist of these M' words. We have from (2.1) that

$$\frac{M}{q^{n-n'}} \leq M' \leq \frac{d}{d-n'\frac{q-1}{q}} \leq d. \tag{2.2}$$

The last inequality follows because

$$d - n'\frac{q-1}{q} \geq d - \frac{(d-1)q}{q-1} \cdot \frac{q-1}{q} = d-(d-1) = 1.$$

Rewrite (2.2) as $q^{n'-n}M \leq M' \leq d$.

Let $d = \lfloor \delta n \rfloor$ and $n >> 0$. Then we have

$$\begin{aligned}
q^{n'-n+k} &\leq \lfloor \delta n \rfloor \\
\left\lfloor \frac{(d-1)q}{q-1} \right\rfloor - n + k &\leq \log_q \lfloor \delta n \rfloor \\
k &\leq n - \left\lfloor \frac{(d-1)q}{q-1} \right\rfloor + \log_q \lfloor \delta n \rfloor < n - \frac{(d-1)q}{q-1} + 1 + \log_q \lfloor \delta n \rfloor \\
k &< n - \frac{\lfloor \delta n \rfloor q}{q-1} + \frac{q}{q-1} + 1 + \log_q \lfloor \delta n \rfloor \\
k &< n - \frac{(\delta n - 1)q}{q-1} + \frac{q}{q-1} + 1 + \log_q \lfloor \delta n \rfloor \\
R &< 1 - \frac{\delta q}{q-1} + \frac{2q}{n(q-1)} + \frac{1}{n} + \frac{\log_q \lfloor \delta n \rfloor}{n} \\
\alpha_q(\delta) &\leq 1 - \frac{\delta q}{q-1}.
\end{aligned}$$

This finishes the proof. □

Lemma 2.7. *Let q be a prime power, n, d positive integers, and C a code of length n over $\mathbb{F}_q$, and suppose that any word with distance at least d to all words in C is also in C. Then*

$$|C| \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^n.$$

Proof. Suppose that

$$|C| \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i < q^n.$$

That means that when we take a $d-1$ ball around each codeword, there is some word x in $\mathbb{F}_q^n$ that is not covered. Then x has distance at least d to all codewords in C, a contradiction. □

Theorem 2.8 (the Gilbert–Varshamov Bound, 1950). *Let q be a prime power, n, k, d positive integers. If*

$$q^{n-k+1} > \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i,$$

then there exists an $[n, k, d]_q$-linear code over $\mathbb{F}_q$.

Proof. We induct on k. For $k = 1$, the theorem is trivial, since it is possible to make a 1-dimensional code with any minimum distance $d \in \{1, \ldots, n\}$. Suppose the inequality holds for $n, k-1, d$, that there exists an $[n, k-1, d]_q$-linear code C over $\mathbb{F}_q$, and that the inequality also holds for n, k, d. We shall try to construct an $[n, k, d]_q$-linear code from C. We rewrite the inequality as

$$q^n > q^{k-1} \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i.$$

Then, according to the previous lemma, there exists a word $x' \notin C$ with distance at least d to each word in C. We want to show that if we expand C with x', then all words in the code will

still have weight at least d. It will then follow that the minimum distance is still d. Suppose $x \in C$ and $\alpha \in \mathbb{F}_q \setminus \{0\}$. Then

$$\mathrm{wt}(x + \alpha x') = \mathrm{wt}(\alpha^{-1}x + x') = d(-\alpha^{-1}x, x') \geq d.$$

This completes the proof. □

Before finding the asymptotic Gilbert–Varshamov bound, we will need some results concerning the entropy function, which will also be used a lot throughout this thesis.

Definition 2.9 (the q-ary Entropy Function). *Let q be a positive integer and δ a real number satisfying $0 < \delta \leq \frac{q-1}{q}$. Then we have*

$$H_q(\delta) := \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta), \quad H_q(0) := 0.$$

Theorem 2.10 (Stirling's Formula). *Let q, n be positive integers. Then*

$$\log_q(n!) = n \log_q(n) - n + O(\log_q n).$$

Lemma 2.11. *If q, n are positive integers and t is a nonnegative integer such that $0 \leq t \leq \frac{(q-1)n}{q}$, then the last term in*

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

is the largest.

Proof. Let $\theta \leq \frac{(q-1)n}{q}$. We then have

$$\begin{aligned}
\frac{n!}{\theta!(n-\theta)!}(q-1)^\theta - \frac{n!}{(\theta-1)!(n-\theta+1)!}(q-1)^{\theta-1} &\geq 0 \\
\Updownarrow & \\
\frac{n!(q-1)^\theta(n-\theta+1) - n!(q-1)^{\theta-1}\theta}{\theta!(n-\theta+1)!} &\geq 0 \\
\Updownarrow & \\
n!(q-1)^{\theta-1}((q-1)(n-\theta+1) - \theta) &\geq 0 \\
\Updownarrow & \\
(q-1)(n-\theta+1) &\geq \theta \\
\Updownarrow & \\
q(n+1) - n - 1 &\geq \theta q \\
\Updownarrow & \\
\theta &\leq \frac{q(n+1) - n - 1}{q} \\
\Updownarrow & \\
\theta &\leq \frac{(q-1)n + q - 1}{q},
\end{aligned}$$

which is true. □

Lemma 2.12. *Let q, n be positive integers, t a nonnegative integer satisfying $0 \leq t \leq \frac{(q-1)n}{q}$. Then*

$$n^{-1} \log_q \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right) = H_q\left(\frac{t}{n}\right) + o(1).$$

Note that this is equivalent with stating that

$$\lim_{n\to\infty} n^{-1} \log_q \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right) = \lim_{n\to\infty} H_q\left(\frac{t}{n}\right).$$

Proof. From Lemma 2.11, we know that since $t \leq \frac{(q-1)n}{q}$, then the last term in

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

is the largest. That means that when we multiply that term with the number of terms in the sum, we get a larger number than the sum gives us:

$$\binom{n}{t}(q-1)^t \leq \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \leq (t+1)\binom{n}{t}(q-1)^t.$$

The left-hand side of this inequality gives us

$$\begin{aligned}
n^{-1} \log_q \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right) &\geq n^{-1} \log_q \binom{n}{t} + n^{-1} \log_q (q-1)^t \\
&= n^{-1} \log_q \left(\frac{n!}{t!(n-t)!} \right) + n^{-1} \log_q (q-1)^t \\
&= n^{-1} \left(\log_q(n!) - log_q(t!) - log_q(n-t)! \right) \\
&\quad + n^{-1} \log_q (q-1)^t \\
&= n^{-1} \Big(n \log_q(n) - n + O(\log_q(n)) \\
&\quad - t \log_q(t) + t - O(\log_q(t)) \\
&\quad - (n-t)\log_q(n-t) + (n-t) - O(\log_q(n-t)) \Big) \\
&\quad + n^{-1} \log_q (q-1)^t \\
&= \frac{t}{n} \log_q(q-1) + \log_q(n) - \frac{t}{n} \log_q(t) \\
&\quad - \left(1 - \frac{t}{n}\right) \log_q \left(n \left(1 - \frac{t}{n} \right) \right) + o(1) \\
&= \frac{t}{n} \log_q(q-1) - \frac{t}{n} \log_q(t) + \frac{t}{n} \log_q(n) \\
&\quad - \left(1 - \frac{t}{n}\right) \log_q \left(1 - \frac{t}{n} \right) + o(1)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{t}{n}\log_q(q-1) - \frac{t}{n}\log_q\left(\frac{t}{n}\right) \\
&\quad - \left(1-\frac{t}{n}\right)\log_q\left(1-\frac{t}{n}\right) + o(1) \\
&= H_q\left(\frac{t}{n}\right) + o(1).
\end{aligned}
$$

The right-hand side of the inequality gives us

$$
n^{-1}\log_q\left(\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\right) \leq n^{-1}\log_q(t+1) + n^{-1}\log_q\binom{n}{t} + n^{-1}\log_q(q-1)^t.
$$

The first term is $o(1)$, and the rest of the expression is the same as when we took logarithms of the left-hand side of the inequality and divided by n. Equality follows. □

Corollary 2.13 (the Asymptotic Gilbert–Varshamov Bound). *Let q be a prime power. We then have*

$$
\alpha_q^{\mathrm{lin}}(\delta) \geq R_{\mathrm{GV}}(\delta) := 1 - H_q(\delta).
$$

Proof. Suppose we have positive integers n, k, d satisfying

$$
|C| \cdot \sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i > q^n.
$$

Then, according to Theorem 2.8, there exists an $[n,k,d]_q$-linear code. Taking logarithms on both sides and dividing by n, we obtain

$$
R + n^{-1}\log_q\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i > 1.
$$

Letting $n \to \infty$, we get

$$
\alpha_q^{\mathrm{lin}}(\delta) \geq 1 - \lim_{n\to\infty}\left(n^{-1}\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i\right) = 1 - H_q(\delta).
$$

The last equality follows from Lemma 2.12. □

Chapter 3

Curves over Finite Fields

Before presenting the definition of Goppa codes and the Tsfasman–Vlăduţ–Zink bound, we will need some results from algebraic curves defined over finite fields, which I present in this chapter. We start by defining what is meant by a curve defined over $\mathbb{F}_q$ for q a prime power, and what is meant by $\mathbb{F}_q$-rational points and $\mathbb{F}_q$-rational divisors. I conclude this chapter by proving that the Riemann–Roch theorem is valid for curves over finite fields.

The entire material is taken from [10], pages 103–109, except for Proposition 3.8, which is taken from Proposition 2.3.4, page 173 in [13].

Throughout this chapter, $k = \mathbb{F}_q$ will denote a finite field, and k' will denote the closure of k. X will be assumed to be a non-singular, projective curve defined over k, i.e. its prime ideal $\mathfrak{p}(X)$ has a basis $\{F_1, \ldots, F_r\}$ where each F_i has coefficients in k. A point $x = (x_0, \ldots, x_n) \in \mathbb{P}^n_{k'}$ will be called k-rational if for all i, $x_i \neq 0 \Rightarrow x_j/x_i \in k$, $j = 0, \ldots, r$. The Galois group of k' over k will be denoted by $\mathrm{Gal}(k'/k)$. The element $\sigma \in \mathrm{Gal}(k'/k)$ we define as $\sigma(x_i) := x_i^q$, the Frobenius automorphism of X. If $x = (x_0, \ldots, x_n)$, then we define $\sigma(x) := (\sigma(x_0), \ldots, \sigma(x_n))$.

Let $\Gamma_k(X)$ be the coordinate ring of X over k. Then $f = F/G \in k'(X)$ will be defined to be k-rational if $F, G \in \Gamma_k(X)$ and $G \neq 0$ in $\Gamma_k(X)$. The field $k(X)$ will denote the set of all k-rational functions in $k'(X)$. $\mathrm{Div}'(X)$ denotes the set of all divisors on X. $\mathrm{Pic}'(X)$ denotes the set of all equivalence classes of divisors on X. If $D \in \mathrm{Div}'(X)$, then we let $\overline{D}$ denote the corresponding equivalence class. A closed point on X over k will be assumed to be a pair $(\mathcal{O}_v, \mathfrak{m}_v)$, where v is a discrete valuation of $k(X)$ and $\mathcal{O}_v$ is the associated DVR over k with maximal ideal $\mathfrak{m}_v$.

If $x = (x_0, \ldots, x_n)$ is a point on X such that $x_i = 1$ for some $i = 0, \ldots, n$, then $k(x)$ will denote the field extension of k generated by the coordinates of x.

Definition 3.1. *Let $D \in \mathrm{Div}'(X)$, $D = \sum n_x x$. Let $\sigma(D) := \sum n_x \sigma(x)$. Then D is defined to be k-rational if $\sigma(D) = D$. We denote the set of all such divisors by* $\mathrm{Div}(X)$. *An equivalence class $\overline{D} \in \mathrm{Pic}'(X)$ is defined to be k-rational if it contains at least one k-rational divisor. The set of such equivalence classes is denoted by* $\mathrm{Pic}(X)$.

Proposition 3.2. *Suppose x is a point on X over k'. Suppose $k(x) = \mathbb{F}_{q^\nu}$ for some positive integer ν. Then $x, \sigma(x), \ldots, \sigma^{\nu-1}(x)$ are all distinct and $\sigma^\nu(x) = x$.*

Proof. We can assume that $x = (1, x_1, \ldots, x_n)$ by first making a change of coordinates if necessary. If $\sigma^i(x) = \sigma^j(x)$ for $0 \leq i < j \leq \nu - 1$, then $\sigma^{j-i}(x_s) = x_s$ for $s = 1, \ldots, n$. Then $x_1, x_2, \ldots, x_n \in \mathbb{F}_{q^{j-i}}$. Since $x_1, \ldots, x_n$ were also assumed to generate $\mathbb{F}_{q^\nu}$ from $\mathbb{F}_q$, it follows that $\mathbb{F}_{q^\nu} \subseteq \mathbb{F}_{q^{j-i}}$, a contradiction.

$\sigma^\nu(x) = x$ follows directly from the fact that each element $x_1, \ldots, x_n$ is in $\mathbb{F}_{q^\nu}$ and the definition $\sigma(x_i) = x_i^q$. □

Definition 3.3. *Let x be a point on X over k'. A k-rational divisor P is defined to be prime if it is of the form*

$$P = P_x = \sum_{i=1}^{\nu} \sigma^{i-1}(x),$$

where ν is the degree of x over k. The points $\sigma^{i-1}(x)$ are called the components of P.

Proposition 3.4. *A divisor $D \in \mathrm{Div}'(X)$ is k-rational if and only if it can be written as $D = \sum_P a_P P$, where all the P are prime divisors, $a_P \in \mathbb{Z}$, and $a_P \neq 0$ for only a finite number of P.*

Proof. Suppose $D = \sum_P a_P P$, where all the P are prime divisors, $a_P \in \mathbb{Z}$, and $a_P \neq 0$ for only a finite number of P. Then clearly, $\sigma(D) = \sigma\left(\sum a_P P\right) = \sum a_P \sigma(P) = \sum a_P P$.

Conversely, if $D = \sum_x a_x x$ is k-rational, let ν be a common multiple for the degrees of all the components x. Then $\sigma^\nu(x) = x$ for all x and $D = \sigma(D) = \sigma^2(D) = \cdots = \sigma^{\nu-1}(D)$. Now, if we put in the expression for D in this equation, we get $\sum_x a_x x = \sigma\left(\sum_x a_x x\right) = \sigma^2\left(\sum_x a_x x\right) = \cdots = \sigma^{\nu-1}\left(\sum_x a_x x\right) \quad \Rightarrow \quad \sum_x a_x x = \sum_x a_x \sigma(x) = \sum_x a_x \sigma^2(x) = \cdots = \sum_x a_x \sigma^{\nu-1}(x)$. This shows that for any given x, the coefficient of $x, \sigma(x), \ldots, \sigma^{\nu-1}(x)$ are the same. Since $[k(x) : k]$ divides ν, we can put $x + \sigma(x) + \cdots + \sigma^{\nu-1}(x) = b_x P_x$, where b_x is an integer and P_x is the prime divisor associated with x, and so $D = \sum_{P_x} a_x b_x P_x = \sum_P c_P P$, as desired. □

Definition 3.5. *Define two points x and y to be equivalent if $y = \sigma^s(x)$ for some nonnegative integer s. We denote the equivalence class of x by $\overline{x}$.*

Proposition 3.6. *Let $f \in k'(X)$. Then $\mathrm{div}(f)$ is k-rational if and only if $f \in k(X)$, up to multiplication by constants.*

Proof. Suppose $f \in k(X)$ and let $\mathrm{div}(f) = \sum_x v_x(f) \cdot x$, where $v_x(f)$ is the valuation of f in x. Now, if x is a point and $\sigma^i(x) = y$, then since f is k-rational, we have that $v_x(f) = v_y(f)$. It follows that

$$\begin{aligned} \mathrm{div}(f) &= \sum_{\overline{x}} v_{\overline{x}}(f) \cdot (x + \sigma(x) + \cdots + \sigma^{\nu_x - 1}(x)) \\ &= \sum_{\overline{x}} v_{\overline{x}}(f) \cdot P_{\overline{x}}, \end{aligned}$$

where $\nu_x = [k(x) : k]$. It follows by Proposition 3.4 that $\mathrm{div}(f)$ is k-rational.

Conversely, suppose $\mathrm{div}(f) = \sum_x v_x(f) \cdot x$ is a k-rational divisor, $f = F/G \in k'(X)$, $G \neq 0$ in $\Gamma_{k'}(X)$. Since $\mathrm{div}(f)$ is k-rational, then if the point x is a zero in F, then $\sigma^i(x)$ is also a zero. Proposition 3.4 gives that the zeros have the same multiplicity. The same goes for G. It follows that $F, G \in \Gamma_k(X)$, and so $f \in k(X)$. □

Definition 3.7. *Let $L'(D) = \{f \in k'(X) \setminus \{0\} \mid \mathrm{div}(f) + D \succ 0\} \cup \{0\}$. Then we define $L(D) := L'(D) \cap k(X)$. The dimension of $L'(D)$ as a vector space over k' is $l'(D)$, and $l(D)$ is the dimension of $L(D)$ as a vector space over k.*

Proposition 3.8. *Let D be a k-rational divisor on X. Then $L(D)$ and $L'(D)$ have a common basis. In particular, $l(D) = l'(D)$.*

Proof. Let

$$L'(D) = \bigoplus_{i=1}^{m} f_i \cdot k'.$$

Let k'' be a finite extension of k so that $f_1, \ldots, f_m \in k''(X)$. Let $\{\alpha_1, \ldots, \alpha_\nu\}$ be a basis for k'' as a vector space over k. Then the Galois group $\mathrm{Gal}(k''/k)$ consists of ν elements with the Frobenius homomorphism as generator, and we have from Proposition 3.2 that $\mathrm{Gal}(k''/k) = \{\sigma, \ldots, \sigma^\nu\}$.

Define

$$g_{i,j} = \sum_{s=1}^{\nu} \sigma^s(\alpha_j \cdot f_i) = \sum_{s=1}^{\nu} \sigma^s(\alpha_j) \cdot \sigma^s(f_i).$$

We show that $g_{1,1}, \ldots, g_{1,\nu}, \ldots, g_{m,\nu} \in k(X)$ and generate $L'(D)$. Then an m-subset of these will be a basis for $L'(D)$, and they will hence also be a basis for $L(D)$.

First of all, if $\beta \in k''$, it follows that $\sigma(\beta) + \cdots + \sigma^\nu(\beta) \in k$. (Proof: $\sigma, \ldots, \sigma^\nu$ take the element β_1 to all of its (not necessarily distinct) conjugates $\beta_2, \ldots, \beta_\nu$. So $\beta_1 + \cdots + \beta_\nu = \sigma(\beta_1) + \cdots + \sigma^\nu(\beta_1)$. Also, there exists a polynomial with coefficients in k that factors as $(x - \beta_1)(x - \beta_2) \cdots (x - \beta_\nu)$. The coefficient of $x^{\nu-1}$ in this polynomial is $\beta_1 + \beta_2 + \cdots + \beta_\nu$, but since the polynomial has coefficients in k, then $\beta_1 + \beta_2 + \cdots + \beta_\nu$ must be in k.) It follows that given an element $f \in k''(X)$, then $\sigma(f) + \cdots + \sigma^\nu(f) \in k(X)$.

To prove that $g_{1,1}, \ldots, g_{1,\nu}, \ldots, g_{m,\nu}$ generate $L'(D)$, note that the matrix

$$\mathscr{G} = \begin{pmatrix} \sigma(\alpha_1) & \sigma^2(\alpha_1) & \ldots & \sigma^\nu(\alpha_1) \\ \sigma(\alpha_2) & \sigma^2(\alpha_2) & \ldots & \sigma^\nu(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(\alpha_\nu) & \sigma^2(\alpha_\nu) & \ldots & \sigma^\nu(\alpha_\nu) \end{pmatrix}$$

by standard Galois theory has nonzero determinant, so the elements $\sum_s \sigma^s(\alpha_1 \cdot f_1), \sum_s \sigma^s(\alpha_2 \cdot f_1), \ldots, \sum_s \sigma^s(\alpha_\nu \cdot f_1)$ are linearly independent for each f_i. Also, for each α_j, we get linearly independent elements if we vary the f_i. So we only need to show that each $\mathrm{div}(g_{i,j}) + D \succ 0$.

To show this, it suffices to show that $f \in L'(D) \Rightarrow \sigma(f) \in L'(D)$, since then $g_{i,j}$ will be nothing more than a linear combination of elements from $L'(D)$. We will here use the property that D is a k-rational divisor. But first we show that $\sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f))$.

Note that for a point x, we have that σ is a ringhomomorphism from $\mathscr{O}_x$ to $\mathscr{O}_{\sigma(x)}$. If $\mathrm{ord}_x(f) = n \geq 0$ and $\mathfrak{m}_x$ is the maximal ideal in the associated DVR $\mathscr{O}_x$, then $f \in \mathfrak{m}_x^n / \mathfrak{m}_x^{n+1}$. If h is an element that generates $\mathfrak{m}_x$, then this means that h^n is the highest power of h that divides f in $\mathscr{O}_x$. We write $f = h^n \cdot f'$, where f' is a unit in $\mathscr{O}_x$. Then $\sigma(f) = \sigma(h)^n \cdot \sigma(f')$. We have $h(x) = 0$. Taking $\sigma(h)$ and evaluating it in $\sigma(x)$ gives $\sigma(h(x)) = \sigma(0) = 0$. It is clear that $\sigma(f')$ is a unit, since $\sigma(f'^{-1})$ is its inverse. Then $\sigma(h)$ generates the maximal ideal $\mathfrak{m}_{\sigma(x)}$ in the DVR $\mathscr{O}_{\sigma(x)}$, and it follows that $\mathrm{ord}_{\sigma(x)}(\sigma(f)) = n$. A similar argument applies for negative orders. It follows that $\sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f))$.

Suppose now that $\mathrm{div}(f_i) + D \succ 0$. Then $\sigma(\mathrm{div}(f_i)) + \sigma(D) \succ 0$. Since $\sigma(D) = D$, the above result gives us $\mathrm{div}(\sigma(f_i)) + D \succ 0$, as desired. □

Proposition 3.9. *Let K be a canonical divisor. Then $\overline{K}$ contains a k-rational element.*

Proof. Choose an $f \in k(X)$ such that $\mathrm{d}f \neq 0$. Then $\mathrm{d}f$ will also have coefficients in k. The rest of the proof is now identical of the proof in Proposition 3.6. □

Corollary 3.10. *Let K be a k-rational canonical divisor. Then $l(K) = l'(K)$.*

Corollary 3.11 (the Riemann–Roch Theorem). *Let D be a k-rational divisor, K a rational canonical divisor. Then*

$$l(D) = \deg(D) + 1 - g + l(K - D).$$

Chapter 4

Goppa Codes

In this chapter I present the construction of Goppa codes. This construction was discovered by V.D. Goppa in 1981 and is based on curves over finite fields. It is this construction that Tsfasman, Vlăduţ, and Zink used when they managed to improve the asymptotic Gilbert–Varshamov bound in 1982.

I begin this chapter by giving the basic definitions and results concerning Goppa codes. I will then give two examples of how to construct such codes. I conclude this chapter by presenting an infinite sequence of Goppa codes that attains the Gilbert–Varshamov bound, made by Chaoping Xing in 2005.

The material in Section 4.1 of this chapter is taken from [14]. The example of the Hermite curve in Section 4.2 can be found on page 62 of [14]. Section 4.3 is a presentation of [18].

Throughout this chapter, X will always be assumed to be a non-singular projective curve defined over $\mathbb{F}_q$. The divisors D, G, G^*; constants d, k, n, d^*, k^*; and maps $\alpha, \alpha^*, \beta^*$ will always be assumed to be as defined in Definition 4.1, Proposition 4.2, Definition 4.6, and Definition 4.13, unless specified otherwise. The genus of the curve X shall always be denoted by g. The field of rational functions on X with coefficients in $\mathbb{F}_q$ will be denoted by $\mathbb{F}_q(X)$. The set of $\mathbb{F}_q$-rational points on X will be denoted by $X(\mathbb{F}_q)$, and its cardinality by $|X(\mathbb{F}_q)|$. The discrete valuation ring over $\mathbb{F}_q$ at the closed point P will be denoted by $\mathcal{O}_P$.

All divisors and closed points will in this chapter be assumed to be $\mathbb{F}_q$-rational unless stated otherwise.

4.1 Definitions

Definition 4.1. *Let $P_1, \ldots, P_n$ be distinct points of X of degree 1 over $\mathbb{F}_q$ and let $D = P_1 + \cdots + P_n$ be a divisor. Let G be a divisor satisfying $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. Define the linear map $\alpha : L(G) \longrightarrow \mathbb{F}_q^n$ by*

$$f \longmapsto (f(P_1), \ldots, f(P_n)).$$

Then the image of the map defines a linear code $C(D, G)$ called a Goppa code.

Proposition 4.2. *For a Goppa code $C(D, G)$, we have dimension $k = l(G) - l(G - D)$ and minimum distance $d \geq n - \deg(G)$.*

Proof. We have $C(D, G) \cong L(G)/\ker(\alpha)$, so we must show that $\ker(\alpha) = L(G - D)$. Suppose $f \in \ker(\alpha)$. Then $f(P_i) = 0$, $i = 1, \ldots, n$, so $\mathrm{div}(f) \succ D$. Thus, $f \in L(G - D)$. Conversely,

suppose $f \in L(G-D)$. Then $\mathrm{div}(f) \succ D$ since $P_i \not\prec G$, $i = 1, \ldots, n$. It follows that $f(P_i) = 0$, $i = 1, \ldots, n$.

To show that $d \geq n - \deg(G)$, suppose the Hamming weight of $\alpha(f)$ is d. This means that $f(P_i) = 0$ for $n-d$ points among the P_i, say $P_{i_1}, \ldots, P_{i_{n-d}}$. Then $f \in L(G - P_{i_1} - \cdots - P_{i_{n-d}})$, and $\mathrm{div}(f) + G - P_{i_1} - \cdots - P_{i_{n-d}} \succ 0$. Taking degrees on both sides and noting that $\deg(\mathrm{div}(f)) = 0$, we get $\deg(G) - (n-d) \geq 0$, so $d \geq n - \deg(G)$. □

Remark 4.3. The last part of this proposition is only useful if $n - \deg(G) \geq 2$, since $d \geq 1$ always.

Corollary 4.4. *If $\deg(G) < n$, then α is an injection and $k = l(G)$.*

Definition 4.5. *Let E be a divisor. Then we define the vector space $\Omega(E)$ as follows.*

$$\Omega(E) = \{\omega \,|\, \omega \text{ is a rational differential form with } \mathrm{div}(\omega) \succ E\} \cup \{0\}.$$

Definition 4.6. *Define the linear map $\alpha^* : \Omega(G-D) \longrightarrow \mathbb{F}_q^n$ by*

$$\eta \longmapsto (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta)).$$

Then the image of the map defines a linear code $C^*(D,G)$ of length n.

Proposition 4.7. *Let ω be a rational differential form, $\mathrm{div}(\omega) = K$. Define a map $\beta^* : L(K+D-G) \longrightarrow \mathbb{F}_q^n$ by*

$$f \longmapsto (\mathrm{res}_{P_1}(f\omega), \ldots, \mathrm{res}_{P_n}(f\omega)).$$

Then the image of β^* is the same as the image of α^*.

Proof. Suppose $(\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta)) \in C^*(D,G)$. Since η is a rational differential form, we can write it as $f\omega$ for some $f \in \mathbb{F}_q(X)$. We then have $f\omega \in \Omega(G-D)$, so $\mathrm{div}(f) + \mathrm{div}(\omega) = \mathrm{div}(f) + K \succ G - D$. That is equivalent with $\mathrm{div}(f) \in L(K+D-G)$. □

Proposition 4.8. *For a code $C^*(D,G)$, we have dimension $k^* = l(K+D-G) - l(K-G)$ and minimum distance $d^* \geq \deg(G) + 2 - 2g$.*

Proof. Let f, ω be as in Proposition 4.7. We first show that $f\omega$ can't have order ≤ -2 in any P_i, $i = 1, \ldots, n$. This follows from Proposition 4.7, as $f\omega = \eta$ for some $\eta \in \Omega(G-D)$. Since $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$, we have that η can only have poles of order 1 in each P_i.

We now find the dimension k^* by proving that $\ker(\beta^*) = L(K-G)$. The formula for k^* then follows from the fact that $C^*(D,G) \cong L(K+D-G)/\ker(\beta^*)$.

Suppose $\eta \in \Omega(G-D)$ and $\mathrm{res}_{P_i}(\eta) = 0$, $i = 1, \ldots, n$. Then $\eta \in \Omega(G)$. Let $f\omega = \eta$. Then $\mathrm{div}(f\omega) \succ G$. So $\mathrm{div}(f) + K - G \succ 0$, which is the same as saying $f \in L(K-G)$.

Conversely, suppose $f \in L(K-G)$. Then $\mathrm{div}(f) + K \succ G$. Since $\mathrm{Supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$, then $f\omega$ has order at least 0 in each P_i.

To prove that $d^* \geq \deg(G) + 2 - 2g$, suppose we have $\mathrm{res}_{P_i}(f\omega) = 0$ for $n - d^*$ points P_i, say $P_{i_1}, \ldots, P_{i_{n-d^*}}$. We want to show that $f \in L(K + D - P_{i_1} - \cdots - P_{i_{n-d^*}} - G)$, because then $2g - 2 + n - (n - d^*) - \deg(G) \geq 0$.

Now, since $f\omega$ has nonnegative order in $P_{i_1}, \ldots, P_{i_{n-d^*}}$, then $f\omega \in \Omega(G - D + P_{i_1} + \cdots + P_{i_{n-d^*}})$. So $\mathrm{div}(f) + K \succ G - D + P_{i_1} + \cdots + P_{i_{n-d^*}}$. It follows that $f \in L(K - G + D - P_{i_1} - \cdots - P_{i_{n-d^*}})$, as desired. □

Proposition 4.9. *$C(D,G)$ and $C^*(D,G)$ are dual to each other.*

Proof. We must show that the scalar product of any element from $C(D,G)$ with any element from $C^*(D,G)$ is 0, and that $k^* = n - k$.

Let $f \in L(G)$ and $\eta \in \Omega(G-D)$. The dot product of the corresponding codewords is

$$\alpha(f) \cdot \alpha^*(\eta) = \big(f(P_1), \ldots, f(P_n)\big) \cdot \big(\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta)\big) = \sum_{i=1}^{n} f(P_i) \cdot \mathrm{res}_{P_i}(\eta).$$

Now consider one such P_i. Let t_i be a generator for the maximal ideal of $\mathscr{O}_{P_i}$. For $s >> 0$, let

$$f = a_0 + a_1 t_i + a_2 t_i^2 + \cdots + a_{s-1} t_i^{s-1} + g_s t_i^s,$$

where $v_{P_i}(a_j) = 0$ for all nonzero a_j and $g_s \in \mathscr{O}_{P_i}$, and

$$\eta = \left(\frac{b_{-1}}{t_i} + b_0 + b_1 t_i + b_2 t_i^2 + \cdots + b_{s-1} t_i^{s-1} + h_s t_i^s \right) \mathrm{d}t_i,$$

where $v_{P_i}(b_j) = 0$ for all nonzero b_j and $h_s \in \mathscr{O}_{P_i}$. It follows that

$$f\eta = \left(\frac{a_0 b_{-1}}{t_i} + (a_0 b_0 + a_1 b_{-1}) + (a_0 b_1 + a_1 b_0 + a_2 b_{-1}) t + \cdots + g_s h_s t_i^{2s} \right) \mathrm{d}t_i.$$

Therefore, $f(P_i) \cdot \mathrm{res}_{P_i}(\eta) = a_0 b_{-1} = \mathrm{res}_{P_i}(f\eta)$ for all i.

Also, since $f \in L(G)$ and $\eta \in \Omega(G-D)$, then $\mathrm{div}(f\eta) = \mathrm{div}(f) + \mathrm{div}(\eta) \succ -G + G - D = -D$. So $f\eta$ has no other possible residues other than in the points $P_1, \ldots, P_n$. We have

$$\sum_{i=1}^{n} \mathrm{res}_{P_i}(f\eta) = \sum_{P \in X} \mathrm{res}_P(f\eta) = 0,$$

according to the residue theorem. (See e.g. Theorem 4.24, page 89 in [10].)

To show that $k^* = n - k$, the Riemann–Roch theorem gives us $k + k^* = l(G) - l(G - D) + l(K + D - G) - l(K - G) = \big(l(G) - l(K - G)\big) - \big(l(G - D) - l(K - (G - D))\big) = \big(\deg(G) + 1 - g\big) - \big(\deg(G - D) + 1 - g\big) = \deg(D) = n$, as desired. □

Lemma 4.10. *Let $n \geq 2$ be an integer and $q \geq 2$ be a prime power. Given points $P_1, \ldots, P_n \in X$, there exists a rational differential form ω with simple poles in $P_1, \ldots, P_n$ and no poles elsewhere. In particular, $\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)$ are all nonzero.*

Proof. Let ω be a rational differential form, $\mathrm{div}(\omega) = K$. Since all rational differential forms can be written as $f\omega$ for some $f \in \mathbb{F}_q(X)$, we shall show that $f\omega$ fulfills the claim in the lemma for some $f \in \mathbb{F}_q(X)$.

Such an f must be an element of $L(K + P_1 + P_2 + \cdots + P_n)$, since this is equivalent with $\mathrm{div}(f\omega) = \mathrm{div}(f) + K \succ -P_1 - P_2 - \cdots - P_n$.

Let $U_i = L(K + P_1 + P_2 + \cdots + P_n - P_i)$. We must show that

$$L(K + P_1 + P_2 + \cdots + P_{n-1} + P_n) \neq \bigcup_{i=1}^{n} U_i. \tag{4.1}$$

We will prove this by calculating the dimension on the left- and right-hand side of the inequality, using Riemann–Roch.

First of all, we have

$$\begin{aligned} l(K) &= g, \\ l(K+P_1) &= g, \\ l(K+P_1+P_2) &= g+1, \\ l(K+P_1+P_2+P_3) &= g+2, \\ &\vdots \\ l(K+P_1+P_2+\cdots+P_{n-1}) &= g+n-2, \\ l(K+P_1+P_2+\cdots+P_n) &= g+n-1. \end{aligned}$$

From this we see that the left-hand side of (4.1) has dimension $g+n-1$, while each U_i has dimension $g+n-2$. If we were working over an infinite field, the proof would already be done, since a finite union of vector spaces of dimension $< g+n-1$ can't fill a vector space of dimension $g+n-1$. However, for finite fields, this isn't necessarily true.

If A is a set, let $|A|$ denote the number of elements in A. Since X is a curve over the field $\mathbb{F}_q$, we have

$$\begin{aligned} |L(K+P_1+P_2+\cdots+P_n)| &= q^{g+n-1}, \\ |U_1 \cup U_2 \cup \cdots \cup U_n| &= \sum_{i=1}^{n} |U_i| - \sum_{i<j} |U_i \cap U_j| + \sum_{i<j<k} |U_i \cap U_j \cap U_k| \\ &\quad + \cdots + (-1)^{n-2} \sum_{i_1<\cdots<i_{n-1}} |U_{i_1} \cap \cdots \cap U_{i_{n-1}}| \\ &\quad + (-1)^{n-1} |U_1 \cap \cdots \cap U_n| \\ &= \binom{n}{1} q^{g+n-2} - \binom{n}{2} q^{g+n-3} + \binom{n}{3} q^{g+n-4} \\ &\quad + \cdots + (-1)^{n-2} \binom{n}{n-1} q^g + (-1)^{n-1} \binom{n}{n} q^g \\ &= -\binom{n}{0} q^{g+n-1} + \binom{n}{1} q^{g+n-2} - \binom{n}{2} q^{g+n-3} \\ &\quad + \binom{n}{3} q^{g+n-4} + \cdots + (-1)^{n-2} \binom{n}{n-1} q^g \\ &\quad + (-1)^{n-1} \binom{n}{n} q^{g-1} + q^{g+n-1} \\ &\quad + (-1)^n q^{g-1} + (-1)^{n-1} q^g \\ &= -q^{g-1}(q-1)^n + q^{g+n-1} + (-1)^{n-1} q^{g-1}(q-1) \\ &= q^{g-1} \left(q^n - (q-1)^n + (-1)^{n-1}(q-1) \right). \end{aligned}$$

We want this last expression to be strictly smaller than q^{g+n-1}, i.e. that $q^n - (q-1)^n + (-1)^{n-1}(q-1) < q^n$. This is equivalent to $(q-1)^n - (-1)^{n-1}(q-1) > 0$, which we rewrite as $(q-1)^n > (-1)^{n-1}(q-1)$. Since $q \geq 2$, this last bit is clear for $n \geq 2$. □

Proposition 4.11. *Let ω be as in Lemma 4.10,* $\operatorname{div}(\omega) = K$. *Then the codes $C(D, K+D-G)$ and $C^*(D,G)$ are equivalent. In particular, $C(D, K+D-G)$ and $C^*(D,G)$ have the same dimension k and minimum distance d.*

Proof. We show that we obtain all codewords in $C^*(D,G)$ when we direct-multiply each element in $C(D, K+D-G)$ with the vector $(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$, thus showing by definition that the codes are equivalent since each $\mathrm{res}_{P_i}(\omega)$ is nonzero.

A codeword in $C(D, K+D-G)$ is of the form $(f(P_1), \ldots, f(P_n))$, $f \in L(K+D-G)$. Since $v_{P_i}(K) = -1$ for each P_i, then f has no poles in P_i, $i = 1, \ldots, n$. So f is of the form $f = a_0 + a_1 t_i + a_2 t_i^2 + \cdots + g_s t_i^s$, where t_i is a generator for the maximal ideal of $\mathscr{O}_{P_i}$, and where $v_{P_i}(a_j) = 0$ for all nonzero a_j and $g_s \in \mathscr{O}_{P_i}$.

We now direct-multiply the codeword with $(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$, use the same reasoning as in the proof of Proposition 4.9, and get $(\mathrm{res}_{P_1}(f\omega), \ldots, \mathrm{res}_{P_n}(f\omega))$. For all $f \in L(D, K+D-G)$, this yields the image of β^*, and by Proposition 4.7, this is the same as the image of α^*, and so we have the entire code $C^*(D,G)$. □

Remark 4.12. From this proposition it follows that whenever we speak of a code $C^*(D,G)$, it suffices to regard $C(D, K+D-G)$. Proposition 4.8 then follows easily from Proposition 4.11.

Definition 4.13. *Let ω be as in Lemma 4.10,* $\mathrm{div}(\omega) = K$. *We will denote $K+D-G$ by G^*.*

Definition 4.14. *A strongly algebraic-geometric code, SAG-code, is a code $C(D,G)$ satisfying* $n > \deg(G) > 2g-2$.

Recall from Corollary 4.4 that if $n > \deg(G)$, then α is an injection and $k = l(G)$. In particular, this is satisfied if the code is SAG.

Proposition 4.15. *$C(D,G)$ is a SAG-code if and only if $C^*(D,G)$ is a SAG-code.*

Proof. Because of Proposition 4.11, it suffices to show that $C(D,G)$ is a SAG-code if and only if $C(D,G^*)$ is a SAG-code.

Suppose $C(D,G)$ is a SAG-code. We have $\deg(G^*) = 2g-2+n-\deg(G)$, where $n > \deg(G) > 2g-2$. The first inequality yields $\deg(G^*) > 2g-2$, and the second inequality yields $\deg(G^*) < n$. From this, the converse follows trivially. □

4.2 Some Examples

Example 4.16. Let $X = \mathbb{P}^1$ over the field $\mathbb{F}_q$, $q \geq 2$. Choose a positive integer $n \leq q$, $n \geq 2$, and let $P_i = (a_i, 1)$ for $i = 1, \ldots, n$ so that all the a_i are distinct. Choose a positive integer $m < n$ and denote the point $(1,0) =: P_\infty$. Let $G = mP_\infty$ and $D = P_1 + \cdots + P_n$.

It is clear that $l(G) = m+1-g = m+1$ and

$$L(G) = \left\{ \frac{b_0 x^m + b_1 x^{m-1} y + \cdots + b_m y^m}{y^m} \;\middle|\; b_0, \ldots, b_m \in \mathbb{F}_q \right\},$$

where x, y are homogeneous coordinates for $\mathbb{P}^1$. We then get as basis for $L(G)$ the elements $(\frac{x}{y})^m, (\frac{x}{y})^{m-1}, \ldots, \frac{x}{y}, 1$. Note that this fits in with the fact that $l(G) = m+1$.

Let $(\frac{x}{y})^s =: f_s$, so that the basis for $L(G)$ is $f_0, \ldots, f_m$. The Goppa-code $C(D,G)$ is defined by

$$\begin{array}{rcl} L(G) & \longrightarrow & (\mathbb{F}_q)^n, \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

It follows that a generator matrix for $C(D,G)$ is

$$\mathscr{G} = \begin{pmatrix} f_0(P_1) & \dots & f_0(P_n) \\ f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_m(P_1) & \dots & f_m(P_n) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^m & a_2^m & \dots & a_n^m \end{pmatrix}.$$

Note that $C(D,G)$ satisfies $2g-2 < m < n$, since the genus is 0. By Definition 4.14, $C(D,G)$ is a SAG-code. It follows that $k = m+1-g = m+1$ and $d \geq n-m = n-(k-1) = n-k+1$, which we call the Goppa bound. According to the Singleton bound, $d \leq n-k+1$. Equality follows, and so the code is MDS.

From the above, we conclude that $C^*(D,G)$ is also MDS (see Corollary 15.7, page 195 in [5]). We then have from general coding theory that $k^* = n-k = n-m-1$, and so, using that C^* is MDS, $d^* = n-k^*+1 = n-(n-m-1)+1 = m+2$, which is the Goppa bound (see Proposition 4.8).

Let's find the rank of $\mathscr{G}$. We know that d^* equals the minimal number of linear dependent columns in $\mathscr{G}$ (see Theorem 8.4, page 85 in [5]). We found that number to be $d^* = m+2 = (k-1)+2 = k+1$. It follows that the rank of $\mathscr{G}$ is k, and so all submatrices of $\mathscr{G}$ have a nonzero determinant, and that fits in well with the fact that $\mathscr{G}$ is van der Monde, from which the same conclusion can be drawn and the argument reversed.

Example 4.17. A Hermite curve X is a curve over $\mathbb{F}_{q^2}$ given by

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

Its genus is

$$g = \frac{1}{2}\left(q^2 - q\right).$$

According to the Hasse–Weil bound (see Theorem 5.2), the number of $\mathbb{F}_{q^2}$-rational points on this curve is

$$|X(\mathbb{F}_{q^2})| \leq q^2 + 1 + 2g\sqrt{q^2} = q^3 + 1.$$

We shall show that we obtain equality with this curve.

If $z = 0$, we get $x = 0$, and so the only point at infinity is $H_\infty = (0,1,0)$.

If $z = 1$, we get the equation $y^q + y = x^{q+1}$. If $x = 0$, we get $y^q + y = 0$. This equation has q solutions, and with some calculations we find that they are all in $\mathbb{F}_{q^2}$. That gives us q points. If $x = x_0 \neq 0$, then we get the equation $y^q + y = x_0^{q+1}$. For each x_0, we find q values for y, and they are all found in $\mathbb{F}_{q^2}$. That gives us $(q^2-1)q$ new points.

It follows that X has $1+q+(q^2-1)q = q^3+1$ points. This shows that the Hermite curve, as desired, is maximal with respect to the Hasse–Weil bound.

The most usual way to make SAG-codes on X is to choose $2g-2 < m < n$, let $\{P_i\}_{i=1}^{q^3}$ be the set of all $\mathbb{F}_q$-rational points different from H_∞, and let

$$G_m = mP_\infty, \qquad D = \sum_{i=1}^{q^3} P_i.$$

We then get the parameters

$$2g-2 = q^2-q-2 < m < n = q^3, \quad k = m+1-g = m+1-\frac{q^2-q}{2}, \quad d \geq n-m = q^3-m.$$

4.3 A Lower Bound on Goppa Codes

In 2005, Xing showed in [18] that Goppa codes achieve the Gilbert–Varshamov bound (see Corollary 2.13). The main idea of Xing's proof is to choose good divisors G such that the minimum distance d increases compared to $\deg(G)$. He furthermore shows that such a divisor exists provided that $M_{t,l}(D) < h(X)$ (see definitions later in this section). It follows that the code attains the Gilbert–Varshamov bound. Xing's idea is based on an earlier paper that he published (see [15]), where he finds sufficient conditions for $M_{t,l}(D) < h(X)$ by finding an upper bound on $M_{t,l}(D)$. However, the upper bound that he finds here is much better. This is actually the whole difference between [15] and [18]. I here only give an outline of the main results of Xing's paper, but in the proof of Theorem 4.23 I have filled in calculations that Xing in his article left to the reader.

Recall that $X(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points on X.

Definition 4.18. *For any integer l and any effective divisor D with $\deg(D) \geq l$, let*

$$\mathscr{A}_l(D) := \{G \mid \deg(G) = l,\ 0 \prec G \prec D\}.$$

Furthermore, let t be a nonnegative integer and

$$\mathscr{M}_{t,l}(D) := \{H + G \mid \deg(H) = t,\ H \succ 0,\ G \in \mathscr{A}_l(D)\},$$

and let $M_{t,l}(D)$ denote the cardinality of $\mathscr{M}_{t,l}(D)$.

Before presenting the following lemma, note that for a curve X and any integer s, the number of divisor classes of degree s is always $h(X)$. I.e., the number of divisor classes of a certain degree s does not depend on s. (Proof: Let $\overline{A_1}, \ldots, \overline{A_h}$ be all the divisor classes of degree 0, and let $\overline{B}$ be a divisor class of degree s. Then I claim that $\overline{B} + \overline{A_1}, \ldots, \overline{B} + \overline{A_h}$ are all the divisor classes of degree s. To prove the claim, suppose $\overline{B'}$ is a divisor class of degree s not among the ones listed. Then $\overline{B'} - (\overline{B} + \overline{A_i}) \not\equiv \overline{0}$ for $i = 1, \ldots, h$. Including $\overline{0}$, we then have $h + 1$ distinct divisor classes of degree 0, a contradiction.)

Lemma 4.19. *Suppose there is at least one $\mathbb{F}_q$-rational point on the curve X, and let $h(X)$ be the number of divisor classes of a certain degree. Let $s \geq g$ be a positive integer and let S be a set of $\mathbb{F}_q$-rational divisors of degree s such that $|S| < h(X)$. Then there exists an effective divisor H of degree s such that H isn't equivalent to any divisor in S.*

Proof. It is clear that there exists a divisor H' (not necessarily effective) such that $\deg(H') = s$ and H' is not equivalent to any divisor in S. According to Riemann–Roch, $l(H') \geq \deg(H') + 1 - g \geq 1$. So we have at least q functions f such that $H' + \operatorname{div}(f) \succ 0$. Choose such an f and put $H := H' + \operatorname{div}(f)$. Since $H \equiv H'$, then H isn't equivalent to any element in S, as desired. □

In the following proposition we find sufficient conditions for the existence of good divisors G that increase the minimum distance of Goppa codes. Here we will use the Strong Approximation Theorem, which is Theorem I.6.4 on page 31 of [11].

Theorem 4.20 (Strong Approximation Theorem). *Let S be a proper subset of the set of all closed points on X of degree $1, 2, 3, \ldots$. Choose points $P_1, \ldots, P_r \in S$, functions $x_1, \ldots, x_r \in \mathbb{F}_q(X)$, and integers $n_1, \ldots, n_r$. Then there exists a function $x \in \mathbb{F}_q(X)$ such that $v_{P_i}(x - x_i) = n_i$ for all $i \in \{1, \ldots, r\}$ and $v_P(x) \geq 0$ for all $P \in S \setminus \{P_1, \ldots, P_r\}$.*

Proposition 4.21. *Let $P_1, \ldots, P_n$ be the set of $\mathbb{F}_q$-rational points on X and $D = P_1 + \cdots + P_n$. Let l, t be nonnegative integers satisfying $l \leq n$ and $t + l \geq g$. Suppose $M_{t,l}(D) < h(X)$. Then there exists a divisor G of degree $t + l$ such that $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$ and $C(D, G)$ is an $[n, k, d]_q$-linear code with*

$$k = l(G) \geq \deg(G) - g + 1 = t + l - g + 1 \quad \textit{and} \quad d \geq n - l + 1.$$

If $\deg(G) \geq 2g - 1$, then $k = \deg(G) - g + 1$.

Note that according to the theory of standard Goppa codes, $d \geq n - \deg(G) = n - l - t$.

Proof. According to Lemma 4.19, $M_{t,l}(D) < h(X)$ implies that there exists an effective divisor H of degree $t + l$ such that H isn't equivalent to any divisor in $\mathscr{M}_{t,l}(D)$. I now claim that $L(H - \sum_{P \in I} P) = \{0\}$ for any subset $I \subseteq \mathrm{Supp}(D)$ with $|I| = l$.

Suppose the claim is false. Then there exists an $I_0 \subseteq \mathrm{Supp}(D)$ with $|I_0| = l$ such that $L(H - \sum_{P \in I_0} P) \neq \{0\}$. Choose a nontrivial $f \in L(H - \sum_{P \in I_0} P)$. Then $\mathrm{div}(f) + H - \sum_{P \in I_0} P \succ 0$. Put $L = \mathrm{div}(f) + H - \sum_{P \in I_0} P$. Then $H \equiv L + \sum_{P \in I_0} P$. The effective divisor L is of degree t. We have $\sum_{P \in I_0} P \prec D$ and of degree l. So $L + \sum_{P \in I_0} P \in \mathscr{M}_{t,l}$ and H is equivalent to an element in $\mathscr{M}_{t,l}$, a contradiction.

Since n is less than the number of closed points of X, we can apply the Strong Approximation Theorem—Theorem 4.20—to choose functions $z_i \in \mathbb{F}_q(X)$, $i \in \{1, \ldots, n\}$ such that

$$\begin{aligned} v_{P_j}(z_i) = v_{P_j}(z_i - 0) = 0, \quad j \neq i, \\ v_{P_i}(z_i) = v_{P_i}(z_i - 0) = 1. \end{aligned}$$

Let

$$G := H + \mathrm{div}\left(\prod_{i=1}^{n} z_i^{-v_{P_i}(H)} \right).$$

Then $G \equiv H$, and we have that $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$, since whenever a point P_i has nonzero coefficient in H, then the order of the pole of $z_i^{-v_{P_i}(H)}$ at P_i is the same. Since $L(H - \sum_{P \in I} P) = \{0\}$ for any $I \subseteq \mathrm{Supp}(D)$ such that $|I| = l$, the same applies for G. I.e., $L(G - \sum_{P \in I} P) = \{0\}$ for any $I \subseteq \mathrm{Supp}(D)$ such that $|I| = l$.

Choose a nontrivial $f \in L(G)$ and let $r = \mathrm{wt}(f(P_1), \ldots, f(P_n))$. Then $f \in L(G - \sum_{P \in J} P)$ for some $J \subseteq \mathrm{Supp}(D)$ with $|J| = n - r$, since $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. It is clear that $n - r = |J| < l$, and so $r \geq n - l + 1$. Since we put in the conditions that $l \leq n$, we have $r \geq 1$, and so $\ker(\phi) = \{0\}$. It follows that ϕ is injective, the number of codewords is $L(G)$, and the dimension is $k = l(G)$. □

To find out when $M_{t,l}(D) < h(X)$, Xing finds a good upper bound for $M_{t,l}$. I here only give an outline of how this is done. He first shows that

$$M_{t,l}(D) = \sum_{i=0}^{t} \binom{n}{l+i} A_{t-i}^{(n-l-i)},$$

where, if S is a set of $\mathbb{F}_q$-rational points of cardinality $0 \leq s \leq |X(\mathbb{F}_q)|$, then $A_i^{(s)}$ is the number of effective divisors with support disjoint from S. So if he can find a good upper bound for each $A_{t-i}^{(n-l-i)}$, he is done. He uses the s-zeta-function to do that. We have

$$Z^{(s)}(X, T) := \sum_{i=0}^{\infty} A_i^{(s)} T^i = \exp\left(\sum_{i=1}^{\infty} \frac{|X(\mathbb{F}_{q^i})| - s}{i} T^i \right) = Z(X, T)(1 - T)^s, \quad 0 \leq s \leq |X(\mathbb{F}_q)|,$$

where

$$Z(X,T) := \sum_{i=0}^{\infty} A_i T^i = \exp\left(\sum_{i=1}^{\infty} \frac{|X(\mathbb{F}_{q^i})|}{i} T^i\right).$$

He uses this to show that $A_i^{(s)} = h(X) \cdot (q-1)^{s-1} q^{i-g-s+1}$ for $i \geq 2g+s-1$.

Using the fact that

$$\sum_{i=0}^{2g+s-2} A_i^{(s)} T^i = Z(X,T)(1-T)^s - \sum_{i=2g+s-1}^{\infty} A_i^{(s)} T^i$$

and putting $T = 1/q$, he finds that

$$A_i^{(s)} \leq \frac{(2g(\sqrt{q}+1)+2n)h}{q^{q-i}} \left(1 - \frac{1}{q}\right)^{s-1}.$$

And so we have

$$\frac{M_{t,l}(D)}{h} \leq \frac{2g(\sqrt{q}+1)+2n}{q^{g+n-t-l-1}} \sum_{i=0}^{t} \binom{n}{l+i} (q-1)^{n-l-i-1}. \tag{4.2}$$

We can now rephrase the above proposition with the following:

Proposition 4.22. *Let $l \leq n$ and $t + l \geq 1$. Suppose*

$$\frac{2g(\sqrt{q}+1)+2n}{q^{g+n-t-l-1}} \sum_{i=0}^{t} \binom{n}{l+i} (q-1)^{n-l-i-1} < 1.$$

Then there exists an $[n,k,d]_q$-linear code with $k = l(G)$ and $d \geq n - l + 1$.

We now show that these conditions are sufficient to achieve the Gilbert–Varshamov bound.

Theorem 4.23. *Goppa codes achieve the asymptotic Gilbert–Varshamov bound for any $\delta \in (0, 1 - \frac{1}{q})$.*

Proof. The idea of the proof is to start off with the Gilbert–Varshamov bound, find the necessary parameters, and use Proposition 4.22 to show that there exists a code satisfying these conditions.

Choose a sequence of curves $(X_i)_{i=1}^{\infty}$ with genus $g(X_i)$ defined over $\mathbb{F}_q$ such that

$$\lim_{i \to \infty} \frac{|X_i(\mathbb{F}_q)|}{g(X_i)} = a > 0.$$

Choose a small $\varepsilon > 0$ and a pair (δ, R) with $0 < \delta < 1 - \frac{1}{q}$ and $0 < R < 1$ such that

$$1 - H_q(\delta) - \varepsilon < R < 1 - H_q(\delta).$$

Choose positive integers $\{n_i := |X_i(\mathbb{F}_q)|\}_{i=1}^{\infty}$, $\{k_i\}_{i=1}^{\infty}$, and $\{d_i\}_{i=1}^{\infty}$ such that

$$\lim_{i \to \infty} \frac{k_i}{n_i} = R \qquad \text{and} \qquad \lim_{i \to \infty} \frac{d_i}{n_i} = \delta.$$

We will show that there exist Goppa codes C_i with these parameters. For simplicity, I will drop the i-indices.

The following inequality deserves a little argumentation:

$$H_q(\delta) = \lim_{n\to\infty} \frac{\log_q \left(4gn(k+d+g-n+1)\binom{n}{d}(q-1)^{d-1}\right)}{n} < 1 - R = \lim_{n\to\infty} \frac{n-k-1}{n}. \quad (4.3)$$

To prove the left-hand side equality of (4.3), we have

$$\begin{aligned}
&\frac{1}{n}\log_q\left(4gn(k+d+g-n+1)\binom{n}{d}(q-1)^{d-1}\right) \\
&\quad = \frac{1}{n}\left(\log_q\left(4gn(k+d+g-n+1)\right) + \log_q\binom{n}{d} + \log_q(q-1)^d - \log_q(q-1)\right) \\
&\quad \to \lim_{n\to\infty}\frac{1}{n}\log_q\left(\binom{n}{d}(q-1)^d\right) \\
&\quad = \lim_{n\to\infty}\frac{1}{n}\log_q\left((d+1)\binom{n}{d}(q-1)^d\right).
\end{aligned}$$

And in between these two last expressions we have according to Lemma 2.11

$$\lim_{n\to\infty}\frac{1}{n}\log_q\left(\sum_{i=0}^{d}\binom{n}{i}(q-1)^i\right),$$

which according to Lemma 2.12 equals $H_q(\delta)$.

To return to (4.3), the inequality $H_q(\delta) < 1-R$ follows from the choice of R. The equality $1 - R = \lim_{n\to\infty}(n-k-1)/n$ follows from the definition of R and the fact that $\frac{1}{n} \to 0$.

The choice of $0 < \delta < 1 - \frac{1}{q}$ implies that $d < (q-1)n/q$ for sufficiently large n. We also have the inequality

$$4gn(k+d+g-n+1)\binom{n}{d}(q-1)^{d-1} < q^{n-k-1}, \quad n >> 0.$$

Using a similar argument as in the proof of Lemma 2.11, it can be shown that

$$\binom{n}{n-d+i}(q-1)^{d-i-1} \quad (4.4)$$

decreases for $0 \le i < (q-1)n/q$. Recall that $d < (q-1)n/q$ and note that if we define $\binom{c}{d} = 0$ for $d > c$, then (4.4) is 0 for $i > d$. It follows that

$$\frac{4gn}{q^{n-k-1}}\sum_{i=0}^{k+d+g-n}\binom{n}{n-d+i}(q-1)^{d-i-1} \le \frac{4gn}{q^{n-k-1}}(k+d+g-n+1)\binom{n}{d}(q-1)^{d-1} < 1.$$

Putting $t = k+d+g-n$ and $l = n-d$, we get

$$\frac{4gn}{q^{g+n-t-l-1}}\sum_{i=0}^{t}\binom{n}{l+i}(q-1)^{n-l-i-1} < 1.$$

Our aim was to get

$$\frac{2g(\sqrt{q}+1)+2n}{q^{g+n-t-l-1}}\sum_{i=0}^{t}\binom{n}{l+i}(q-1)^{n-l-i-1}<1,$$

which has now been satisfied since we have for sufficiently large n (demanding that $g \neq 0$, which is OK), $2g(\sqrt{q}+1)+2n \leq 2gn+2n \leq 2gn+2gn = 4gn$. □

Remark 4.24. In order to construct a code that has a code rate close to the Gilbert–Varshamov bound, we need a large length n of the codewords. To get an idea of this, we can choose $\mathbb{F}_{q^3}$ with $q=5$, and $\delta = \frac{3}{4}$. We then get $R_{\mathrm{GV}}(\delta) = 1 - H_q(\delta) = 0.1347815102\ldots$. Put $R = 0.1347$. In [1] a tower of function fields has been constructed over $\mathbb{F}_{q^3}$ with $|X_i(\mathbb{F}_{q^3})| \geq q^i(q+1)$ and $g(X_i) = \frac{1}{2(q-1)}(q^{i+1}+2q^i-2q^{(i+2)/2}-2q^{i/2}+q) - \frac{i}{4}\cdot q^{(i-2)/2}\cdot(q+1)$ if $i \equiv 0 \pmod 4$. It is given by $F_1 = \mathbb{F}_{q^3}(x_1)$ and for $i \geq 1$, $F_{i+1} = F_i(x_{i+1})$ with

$$\frac{1-x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}$$

and satisfies $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^3})|/g_i = \frac{2\cdot(q^2-1)}{q+2} > 0$. Put $n_i = 5^i \cdot 6$ and define $k_i = \lfloor Rn_i \rfloor$ and $d_i = \lfloor \delta n_i \rfloor$. We want to have

$$\frac{2g_i(\sqrt{q}+1)+2n_i}{q^{g_i+n_i-t_i-l_i-1}}\sum_{j=0}^{t_i}\binom{n_i}{l_i+j}(q-1)^{n_i-l_i-j-1}<1, \tag{4.5}$$

where $t_i = k_i + d_i + g_i - n_i$ and $l_i = n_i - d_i$, which we know will be satisfied for large enough i. For $i=4$, (4.5) is not satisfied. For $i=8$, we have $n_8 = 2343750$, $g_8 = 339360$, $k_8 = 315894$, $d_8 = 1757812$, $l_8 = 585938$, $t_8 = 69316$, and $\deg(G_8) = t_8 + l_8 = 655254$. Computational problems arise when we try to find the binomial coefficients, so we don't know if these parameters satisfy (4.5).

However, we know that for $i >> 0$ we have (4.5). When we find such an i, we know that $M_{t_i,l_i}(D_i) < h(X_i)$. We then choose n_i distinct points that define the divisor D_i, and we know according to the proof of Proposition 4.21 that there exists an effective divisor H_i such that $L(H_i - \sum_{P\in I} P) = \{0\}$ for any l_i-subset I of $\mathrm{Supp}(D_i)$. We find that divisor and calculate G_i as was done in the proposition. Then $C(D_i, G_i)$ will have dimension $k_i = \lfloor 0.1347 n_i \rfloor$ and minimum distance at least $\lfloor \frac{3}{4} n_i \rfloor$.

In Chapter 8, we will see that linear codes are frameproof codes and that this δ will correspond to $s=4$ in s-frameproof codes. See Remark 8.6.

Chapter 5

The Tsfasman–Vlăduţ–Zink Bound

In 1982, about one year after the Goppa codes were discovered, Tsfasman, Vlăduţ, and Zink published an asymptotic improvement of the Gilbert–Varshamov bound. This improvement used standard Goppa codes together with an infinite sequence of curves with an optimal number of $\mathbb{F}_q$-rational points. In this chapter I start by presenting some results concerning how many $\mathbb{F}_q$-rational points a nonsingular projective curve defined over $\mathbb{F}_q$ can have. I conclude this chapter by presenting the proof of the Tsfasman–Vlăduţ–Zink bound.

The zeta-function of a curve can be found on pages 111–120 in [10]. The Drinfeld–Vlăduţ theorem is taken from page 162 of [10].

5.1 The Drinfeld–Vlăduţ Bound

Theorem 5.1 (Drinfeld–Vlăduţ). *Given an infinite sequence of non-singular projective curves $(X_i)_{i=1}^{\infty}$ with genus $g(X_i)$ and $|X_i(\mathbb{F}_q)|$ $\mathbb{F}_q$-rational points such that $\lim_{i\to\infty} |X_i(\mathbb{F}_q)| \to \infty$, we have*

$$\lim_{i\to\infty} \frac{|X_i(\mathbb{F}_q)|}{g(X_i)} \leq \sqrt{q} - 1.$$

To prove this, we need some facts about the number $|X(\mathbb{F}_q)|$ for a non-singular projective curve X, but to do that, we must first study the zeta-function of X.

The zeta-function is defined as

$$\zeta(X, s) = \sum_D (N(D))^{-s}, \qquad \mathrm{Re}(s) > 1,$$

where the sum is taken over all effective $\mathbb{F}_q$-rational divisors on X and $N(D) = q^{\deg(D)}$. The function converges for all $\mathrm{Re}(s) > 1$.

The zeta-function can be written as

$$\zeta(X, s) = \prod_P \frac{1}{1 - (N(P))^{-s}}, \qquad \mathrm{Re}(s) > 1,$$

where the product is taken over all prime $\mathbb{F}_q$-rational divisors P on X. The product is absolutely convergent. The function converges to

$$\zeta(X, s) = \frac{P(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}, \quad \text{where} \quad P(q^{-s}) = \sum_{j=0}^{2g} \sigma_j q^{-js},$$

where σ_j are real constants. By putting $q^{-s} =: t$, we define the function $Z(X,t) := \zeta(X,s)$. Hence, $Z(X,t) = \frac{P(t)}{(1-t)(1-qt)}$. If $|X(\mathbb{F}_{q^\nu})|$ is the number of $\mathbb{F}_{q^\nu}$-rational points on X, then

$$Z(X,t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{|X(\mathbb{F}_{q^\nu})|}{\nu} t^\nu\right).$$

This is used to show that if $P(q^{-s}) = P(t)$ factors as

$$P(t) = \prod_{j=1}^{2g}(1-\omega_j t),$$

then

$$|X(\mathbb{F}_{q^\nu})| = q^\nu + 1 - \sum_{j=1}^{2g} \omega_j^\nu. \tag{5.1}$$

Furthermore, each ω_j satisfies $|\omega_j| = \sqrt{q}$.

A consequence of this is that a curve of genus 0 has $q+1$ $\mathbb{F}_q$-rational points, as expected.

Before proving the theorem of Drinfeld and Vlăduţ, we include an important bound that is immediate from (5.1).

Theorem 5.2 (the Hasse–Weil Bound). *The number $|X(\mathbb{F}_{q^\nu})|$ of $\mathbb{F}_{q^\nu}$-rational points on a non-singular projective curve X satisfies*

$$|X(\mathbb{F}_{q^\nu})| \leq q^\nu + 1 + 2g\sqrt{q}^\nu.$$

Remark 5.3. A curve X of genus g satisfying $|X(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q}$ is called a *maximal curve*. As we see from Theorem 5.1, we are not able to find maximal curves of arbitrarily large genus g.

Another simple proof of that fact follows from the resently published article [21]. In the article, it is shown that for any maximal curve X over q^2 with genus $g(X)$, we can improve the Goppa code parameter $k+d$ by approximately $g(X)$ when q is large. If we now assume that $q >> 0$ and that there exists a maximal curve X over q^2 for arbitrarily large genus $g(X)$, we can construct a sequence of Goppa codes $(C_i(D_i, G_i))_{i=1}^{\infty}$ with parameters $k_i + d_i \geq \deg(G_i) - g(X_i) + 1 + n_i - \deg(G_i) + g(X_i) - \varepsilon(q) = 1 + n_i - \varepsilon(q)$, where $\varepsilon(q) \geq 0$ and $\varepsilon(q) \to 0$ as $q \to \infty$. By dividing with n_i on both sides and letting $n_i \to \infty$, we obtain the bound $R \geq 1 - \delta$, which exceeds the asymptotic Plotkin bound, an upper bound for $\alpha_q(\delta)$ which we proved in Corollary 2.6, a contradiction to the original assumption that there exists a maximal curve of arbitrarily large genus.

We now prove the theorem of Drinfeld and Vlăduţ.

Proof of Theorem 5.1. Let X have genus g and let

$$Z(t) = \frac{\prod_{j=1}^{2g}(1-\omega_j t)}{(1-t)(1-qt)}.$$

Let $\alpha_j = \omega_j/\sqrt{q}$. Then $|\alpha_j| = 1$. If $\nu \geq 1$, we have

$$|X(\mathbb{F}_q)| \cdot q^{-\nu/2} \leq |X(\mathbb{F}_{q^\nu})| \cdot q^{-\nu/2} = \left(q^\nu + 1 - \sum_{j=1}^{2g} \omega_j^\nu\right) q^{-\nu/2} = q^{\nu/2} + q^{-\nu/2} - \sum_{j=1}^{2g} \alpha_j^\nu.$$

Rearranging, we get

$$\sum_{j=1}^{2g} \alpha_j^\nu \leq q^{\nu/2} + q^{-\nu/2} - |X(\mathbb{F}_q)| \cdot q^{-\nu/2}. \tag{5.2}$$

Now, we have for any positive integer n,

$$0 \leq \left| \sum_{\nu=1}^{n} \alpha_j^\nu \right|^2 = \sum_{\nu=1}^{n} \alpha_j^\nu \cdot \overline{\sum_{\nu=1}^{n} \alpha_j^\nu} = \sum_{\nu=1}^{n} \alpha_j^\nu \cdot \sum_{\nu=1}^{n} \overline{\alpha_j}^\nu,$$

where $\overline{\xi}$ denotes the complex conjugate of the complex number ξ. If we pick an α_j^ν from the first sum and an $\overline{\alpha_j}^\tau$ from the second sum, then $\alpha_j^\nu \cdot \overline{\alpha_j}^\tau = |\alpha_j^\tau|^2 \cdot \alpha_j^{\nu-\tau}$. And since $|\alpha_j| = 1$, then this simply becomes $\alpha_j^{\nu-\tau}$. Hence,

$$\sum_{\nu=1}^{n} \alpha_j^\nu \cdot \sum_{\nu=1}^{n} \overline{\alpha_j}^\nu = \sum_{\nu,\tau=1}^{n} \alpha_j^{\nu-\tau}.$$

We divide the sum into two parts: When $\nu = \tau$, we have $\alpha_j^0 = 1$ n times, so the total contribution is n. When $\nu \neq \tau$, note that $\nu - \tau$ takes all nonzero values between $-(n-1)$ and $n-1$. We pick a positive integer $\kappa \leq n-1$ and count the possibilities for when $\nu - \tau = \kappa$. (The same will apply for negative κ.) If $\tau = 1$, then $\nu = \kappa + 1$. If $\nu = n$, then $\tau = n - \kappa$. So we have $n - \kappa$ possibilities. We get

$$\sum_{\nu,\tau=1}^{n} \alpha_j^{\nu-\tau} = n + \sum_{\kappa=1}^{n-1} (n-\kappa)(\alpha_j^\kappa + \alpha_j^{-\kappa}).$$

We sum this expression over $j = 1, \ldots, 2g$ and get

$$0 \leq 2gn + \sum_{j=1}^{2g} \sum_{\kappa=1}^{n} (n-\kappa)(\alpha_j^\kappa + \alpha_j^{-\kappa}) = 2gn + \sum_{\kappa=1}^{n} (n-\kappa) \sum_{j=1}^{2g} (\alpha_j^\kappa + \alpha_j^{-\kappa}).$$

Now note that since $|\alpha_j^\kappa| = 1$, we have $\alpha_j^\kappa \cdot \overline{\alpha_j^\kappa} = 1$, and so the complex conjugate of α_j^κ is $\alpha_j^{-\kappa}$. It follows that for each j, $\alpha_j^\kappa + \alpha_j^{-\kappa} = 2\mathrm{Re}(\alpha_j^\kappa)$. The sum $\sum_{j=1}^{2g} \alpha_j^\kappa$ is a real number, since $\sum_{j=1}^{2g} \omega_j^\nu$ is the only complex part of the formula for $|X(\mathbb{F}_{q^\nu})|$, so $\mathrm{Re} \sum_{j=1}^{2g} \alpha_j^\kappa = \sum_{j=1}^{2g} \alpha_j^\kappa$. We therefore get

$$0 \leq 2gn + \sum_{\kappa=1}^{n} (n-\kappa) \sum_{j=1}^{2g} (\alpha_j^\kappa + \alpha_j^{-\kappa}) = 2gn + 2 \sum_{\kappa=1}^{n} (n-\kappa) \sum_{j=1}^{2g} \alpha_j^\kappa.$$

Using (5.2), we get

$$0 \leq 2gn + 2 \sum_{\kappa=1}^{n} (n-\kappa) \sum_{j=1}^{2g} \alpha_j^\kappa \leq 2gn + 2 \sum_{\kappa=1}^{n} (n-\kappa)(q^{\kappa/2} + q^{-\kappa/2} - |X(\mathbb{F}_q)| \cdot q^{-\kappa/2}).$$

Rearranging and dividing by $2gn$, this becomes

$$\frac{|X(\mathbb{F}_q)|}{g} \sum_{\kappa=1}^{n} \frac{n-\kappa}{n} \cdot q^{-\kappa/2} \leq 1 + \frac{1}{g} \sum_{\kappa=1}^{n} \frac{n-\kappa}{n} (q^{\kappa/2} + q^{-\kappa/2}).$$

We let $g, n \to \infty$ such that $n/\log_q(g) \to 0$. Then, for any $\varepsilon > 0$,

$$\lim_{g\to\infty} \frac{|X(\mathbb{F}_q)|}{g} \cdot \sum_{\kappa=1}^{\infty} q^{-\kappa/2} \leq 1 + \varepsilon.$$

Since the infinite sum starts at $\kappa = 1$ instead of 0, it becomes

$$\frac{1}{1 - q^{-1/2}} - 1 = \frac{1}{\sqrt{q} - 1}.$$

This proves the theorem. □

5.2 Attaining the Drinfeld–Vlăduţ Bound

Using towers of function fields, it is possible to find a sequence of nonsingular projective curves that attains the Drinfeld–Vlăduţ bound. I here briefly present a construction found in [3].

Let $(X_i)_{i=1}^{\infty}$ be a sequence of nonsingular projective curves defined over $\mathbb{F}_{q^2}$ with genus $g(X_i)$ such that $|X_i(\mathbb{F}_{q^2})| \to \infty$. We know from the Drinfeld–Vlăduţ bound that

$$\lim_{i\to\infty} \frac{|X_i(\mathbb{F}_{q^2})|}{g(X_i)} \leq q - 1.$$

This means that is suffices to find a tower of function fields such that

$$\lim_{i\to\infty} \frac{|X_i(\mathbb{F}_{q^2})|}{g(X_i)} \geq q - 1.$$

To obtain that inequality, we need a large number of $\mathbb{F}_{q^2}$-rational points, and we must have control over the genuses of the curves. I here present a tower of function fields that meet this demand.

For the definition of ramified points and different exponents, see pages 130–138 in [10].

Definition 5.4. *Let $F_1 := \mathbb{F}_{q^2}(x_1)$. For $n \geq 1$, let $F_{n+1} := F_n(z_{n+1})$, where $z_{n+1}^q + z_{n+1} = x_n^{q+1}$, and where for $n \geq 2$ we have $x_n := z_n/x_{n-1}$.*

We must find the number of $\mathbb{F}_{q^2}$-rational points of F_n and the genus g_n. The genus is found by recursive usage of Hurwitz's genus formula,

$$2g_n - 2 = [F_n : F_{n-1}](2g_{n-1} - 2) + \deg \mathrm{Diff}(F_n/F_{n-1}).$$

The degree of $\mathrm{Diff}(F_n/F_{n-1})$ is the sum of all the different exponents $d(P'/P)$ taken over all prime divisors P of F_{n-1} and prime divisors P' of F_n lying over those P. The following proposition is part of proposition 1.1 in [3] and is also presented as Proposition 5.33 on page 138 of [10]:

Proposition 5.5. *Let P be a prime divisor of F_{n-1} in the tower as defined above, and suppose P is totally ramified. Then*

$$d(P'/P) = (q-1)\left(-v_P\left(x_{n-1}^{q+1}\right) + 1\right).$$

So here it will be a good idea to study the ramification index of the prime divisors of F_{n-1}.

I will call prime divisors for points from now on, but will consider them as DVRs of the function fields we consider. In the article, it is shown that there is a unique common zero Q_n for $x_1, z_2, \ldots, z_n$ in F_n, and that Q_n splits into q distinct points of F_{n+1}, one of them being Q_{n+1}. The following definition involves points lying over Q_n.

Definition 5.6. *Let Q_n be the unique point of F_n that is a common zero of $x_1, z_2, \ldots, z_n$.*

- *For $n \geq 2$, let $S_0^{(n)} := \{$points P of F_n such that $P \cap F_{n-1} = Q_{n-1}$ and $P \neq Q_n\}$.*
- *For $1 \leq i \leq \lfloor (n-3)/2 \rfloor$, let $S_i^{(n)} := \{$points P of F_n such that $P \cap F_{n-1} \in S_{i-1}^{(n-1)}\}$.*
- *Let P_∞ denote the pole of x_1 in F_1. Let $S^{(1)} := \{P_\infty\}$ and $S^{(2)} := \{$points P of F_2 such that $P \in S_0^{(2)}$ or $P \cap F_1 \in S^{(1)}\}$.*
- *For n odd, $n \geq 3$, let $S^{(n)} := \{$points P of F_n such that $P \cap F_{n-1} \in S^{(n-1)}\}$. For n even, $n \geq 4$, let $S^{(n)} := \{$points P of F_n such that $P \cap F_{n-1} \in S^{(n-1)} \cup S_{(n-4)/2}^{(n-1)}\}$.*

$S_0^{(n)}$ consists of $q-1$ points, since Q_{n-1} splits into q distinct points of F_n. $S_i^{(n)}$ consists of all points of F_n lying over Q_{n-i-1}. The set $S^{(2)}$ consists of points of F_2 that are either a pole of x_1 or a point $\neq Q_2$ lying over Q_1. If $n \geq 5$, then $S^{(n)}$ consists of points lying over the pole of x_1 and points $\neq Q_{(n-1)-(n-4)/2}$ lying over $Q_{(n-1)-(n-4)/2-1}$ if n is even and points $\neq Q_{(n-2)-(n-5)/2}$ lying over $Q_{(n-2)-(n-5)/2-1}$ if n is odd. The union of these sets consists of all points lying over $P_\infty, Q_1, \ldots, Q_n$.

Garcia and Stichtenoth show that the ramified points of F_n for the extension F_{n+1}/F_n are exactly the points in $S^{(n)}$, and that they are totally ramified. Thus, we can use Proposition 5.5, and for each of the ramified points P of F_n, we have

$$d(P'/P) = (q-1)(-v_P(x_n^{q+1}) + 1).$$

It is also shown that P is a simple pole of x_n, and that the number of elements in $S^{(n)}$ is $q^{\lfloor n/2 \rfloor}$. The degree of each field extension is q, and so Hurwitz's genus formula gives us

$$2g_{n+1} - 2 = q(2g_n - 2) + q^{\lfloor n/2 \rfloor}(q+2)(q-1),$$

with the initial condition $g_1 = 0$. We then get the following proposition:

Proposition 5.7. *The genus g_n of F_n is*

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

Proof. We induct on n. For $n = 1$, we have $q + 1 - q - 2 + 1 = 0$. For $n = 2$, Hurwitz's genus formula gives us $2g_2 - 2 = -2q + (q+2)(q-1) = q^2 - q - 2$. The proposition gives us $g_2 = q^2 + q - \frac{1}{2}q^2 - \frac{3}{2}q - 1 + 1 = \frac{1}{2}q^2 - \frac{1}{2}q$.

Now suppose n is even and the proposition is valid for n. Then Hurwitz's genus formula gives us

$$\begin{aligned} 2g_{n+1} - 2 &= q\left(2\left(q^n + q^{n-1} - \frac{1}{2}q^{n/2+1} - \frac{3}{2}q^{n/2} - q^{n/2-1} + 1\right) - 2\right) \\ &\quad + q^{n/2}(q+2)(q-1) \\ &= 2q^{n+1} + 2q^n - 2q^{n/2+1} - 4q^{n/2}, \end{aligned}$$

which agrees with the proposition. Now suppose n is odd and the proposition is valid for n. Then the recursion formula gives us

$$\begin{aligned} 2g_{n+1} - 2 &= q(2(q^n + q^{n-1} - q^{(n+1)/2} - 2q^{(n-1)/2} + 1) - 2) \\ &\quad + q^{(n-1)/2}(q+2)(q-1) \\ &= 2q^{n+1} + 2q^n - q^{(n+3)/2} - 3q^{(n+1)/2} - 2q^{(n-1)/2}, \end{aligned}$$

as desired. □

Now that the genus of each F_n has been calculated, it remains to find the number of points of degree 1. Some of those points are:

- all points of F_n lying over a point in {points P of F_1 such that P is a zero of $x_1 - \alpha$, $0 \neq \alpha \in \mathbb{F}_{q^2}$}
- all points of F_n lying over a point in $S^{(2)}$
- all points $S_0^{(n)} \cup \{Q_n\}$

It is shown that a zero of $x_1 - \alpha$, $\alpha \neq 0$ in F_1 splits completely in F_n. Then we have a total of $(q^2-1) \cdot q^{n-1}$ points of the first type. To determine the number of points of the second type, remember that points in $S^{(n)}$ are totally ramified. This means that the number of points lying over a point in $S^{(2)}$ equals the number of elements in $S^{(2)}$, and there are q of those. The number of points of the third type is the number of points of F_n lying over Q_{n-1}, which is q.

It follows that the number of points of degree 1 of F_n is

$$N_n \geq (q^2-1) \cdot q^{n-1} + 2q.$$

We then get

$$\begin{aligned} \lim_{n\to\infty} \frac{g_n}{N_n} &\leq \lim_{n\to\infty} \frac{q^n + q^{n-1}}{(q^2-1) \cdot q^{n-1} + 2q} \\ &= \frac{1+q^{-1}}{q-q^{-1}} = \frac{1+q^{-1}}{q(1-q^{-2})} = \frac{1+q^{-1}}{q(1+q^{-1})(1-q^{-1})} = \frac{1}{q-1}. \end{aligned}$$

We have now reached the desired conclusion.

Theorem 5.8. *There exists a sequence of nonsingular projective curves $(X_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$, $q = p^{2s}$, p prime, with genus $g(X_i)$, $|X_i(\mathbb{F}_q)|$ the number of $\mathbb{F}_q$-rational points, such that $|X_i(\mathbb{F}_q)| \to \infty$ and*

$$\lim_{i\to\infty} \frac{|X_i(\mathbb{F}_q)|}{g(X_i)} = \sqrt{q} - 1.$$

Corollary 5.9 (the Tsfasman–Vlăduţ–Zink Theorem). *Suppose*

$$0 \leq R_0 \leq 1 - \frac{1}{\sqrt{q}-1}.$$

Then there exists a sequence of linear codes over $\mathbb{F}_q$, $q = p^{2s}$, p prime, such that $n_i \to \infty$ and

$$R_0 \geq 1 - \lim_{i\to\infty} \delta_i - \frac{1}{\sqrt{q}-1} \quad \text{and} \quad \lim_{i\to\infty} R_i = R_0.$$

Equivalently,

$$\lim_{i\to\infty} \delta_i \geq 1 - R_0 - \frac{1}{\sqrt{q}-1} \quad \text{and} \quad \lim_{i\to\infty} R_i = R_0.$$

Proof. Let R_0 be as in the theorem and define

$$\mu_0 := R_0 + \frac{1}{\sqrt{q}-1}.$$

Let $(X_i)_{i=1}^{\infty}$ be an infinite sequence of nonsingular projective curves with genus $g(X_i)$ defined over $\mathbb{F}_q$ such that $|X_i(\mathbb{F}_q)| \to \infty$ and $\lim_{i\to\infty} |X_i(\mathbb{F}_q)|/g(X_i) = \sqrt{q}-1$. For each i, choose an $\mathbb{F}_q$-rational point P_i on X_i and let

$$D_i = \sum_{P \neq P_i} P,$$

where the sum is taken over all $\mathbb{F}_q$-rational points on X_i. Let $n_i = \deg(D_i)$. Choose a nonnegative integer m_i such that

$$\lim_{i\to\infty} \frac{m_i}{n_i} = \mu_0.$$

This can be done by e.g. letting $m_i = \lfloor \mu_0 n_i \rfloor + \mu'$ where μ' is a constant. We can then ensure—possibly by putting $\mu' = -1$—that $m_i < n_i$. Let $G_i = m_i P_i$. We have that the dimension $k_i = l(G_i) \geq m_i + 1 - g(X_i)$.

We have now defined a Goppa code $C(D_i, G_i)$. If $k_i > m_i + 1 - g(X_i)$, then choose a linear subset of $C(D_i, G_i)$ of dimension k_i' such that $k_i' = m_i + 1 - g(X_i)$. Otherwise, define $k_i' := k_i$.

We get

$$R_i = \frac{k_i'}{n_i} = \frac{m_i}{n_i} + \frac{1}{n_i} - \frac{g(X_i)}{n_i} \to \mu_0 + 0 - \frac{1}{\sqrt{q}-1} = R_0.$$

Since $k_i' = m_i + 1 - g(X_i)$ and $d_i \geq n_i - m_i$, we have $k_i' \geq n_i - d_i + 1 - g(X_i)$. Dividing on both sides by n_i, we get

$$R_i \geq 1 - \delta_i + \frac{1}{n_i} - \frac{g(X_i)}{n_i}.$$

If we let $i \to \infty$, then also $n_i \to \infty$, and so we have

$$R_0 = \lim_{i\to\infty} R_i \geq 1 - \lim_{i\to\infty} \delta_i - \lim_{i\to\infty} \frac{g(X_i)}{n_i} = 1 - \lim_{i\to\infty} \delta_i - \frac{1}{\sqrt{q}-1},$$

as desired. □

Corollary 5.10. *Let $q = p^{2s}$, p prime. If*

$$0 \leq \delta \leq 1 - \frac{1}{\sqrt{q}-1},$$

then

$$\alpha_q^{\mathrm{lin}}(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q}-1}.$$

Proof. Choose any δ_0 such that

$$0 \leq \delta_0 \leq 1 - \frac{1}{\sqrt{q}-1},$$

and put

$$R_0 := 1 - \delta_0 - \frac{1}{\sqrt{q}-1}.$$

According to the above theorem, there exists a point (δ_1, R_0) in U_q (see Definition 2.1) such that $\delta_0 \leq \delta_1$. For that given δ_1, it is clear that $\alpha_q^{\text{lin}}(\delta_1) \geq R_0$, since $(\delta_1, R_0) \in U_q$. According to Proposition 2.2—which also applies for the class of linear codes—α_q^{lin} is decreasing wherever α_q^{lin} is positive, so $\alpha_q^{\text{lin}}(\delta_0) \geq \alpha_q^{\text{lin}}(\delta_1) \geq R_0$, which we defined to be

$$1 - \delta_0 - \frac{1}{\sqrt{q} - 1}.$$

□

Remark 5.11. For any prime power q and any nonnegative integer g, put

$$N_q(g) := \max\{|X(\mathbb{F}_q)|\},$$

where the maximum is taken over all nonsingular projective curves of genus g defined over $\mathbb{F}_q$. Define

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

It then follows that

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

The Tsfasman–Vlăduţ–Zink theorem is a consequence of this when q is a square.

Chapter 6

Improvements of the Tsfasman–Vlăduţ–Zink Bound

To my knowledge, the Tsfasman–Vlăduţ–Zink bound wasn't improved until after the turn of the century. In this chapter I present two of the improvements that have been made, both first published in 2003. However, when it comes to the improvement of Elkies, I use a proof by Xing and Stichtenoth that was published in 2005. To this date, I have not found any bounds that have improved the one of Elkies.

There is one earlier improvement of the Tsfasman–Vlăduţ–Zink bound that I know of, which Xing published in 2001 and is found in [15]. Although I don't present it here, I have used his method on a generalised version of the Goppa codes in Chapter 11.

6.1 Xing's 2003 Improvement

The following construction is found in [17] by Chaoping Xing. I have put in calculations that Xing in his article left for the reader.

The improvement is given by

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \sum_{i=2}^{\infty} \log_q \left(1 + \frac{q-1}{q^{2i}}\right),$$

where $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$ and $N_q(g)$ is the maximal number of $\mathbb{F}_q$-rational points on a nonsingular projective curve of genus g defined over $\mathbb{F}_q$. If q is a square, then $A(q) = \sqrt{q} - 1$.

Let X be a nonsingular projective curve defined over $\mathbb{F}_q$ and let t_P be a generator for the maximal ideal of the DVR associated with the point P on X. Let $P_1, \ldots, P_n$ be $\mathbb{F}_q$-rational points on X and let G be a divisor on X such that $\mathrm{Supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Let $P \in \{P_1, \ldots, P_n\}$ and $t := t_P$. Suppose $f \in L(G)$. The following can easily be shown by induction on s: For an integer $s > 0$, we have $f = a_0 + a_1 t + a_2 t^2 + \cdots + g_s t^s$, where $g_s \in \mathcal{O}_P$ and $v_{P_i}(a_i) = 0$ for all nonzero a_i. Now let $s >> 0$ and define recursively $f^{(0)}(P) := f(P)$ and

$$f^{(m)}(P) = \frac{f - f^{(0)}(P) - f^{(1)}(P)t - f^{(2)}(P)t^2 - \cdots - f^{(m-1)}(P)t^{m-1}}{t^m}(P)$$

for all integers $m \geq 1$. In other words, let $f^{(m)}(P)$ be the function $a_m + a_{m+1}t + a_{m+2}t^2 + \cdots + g_s t^s$ evaluated in P. It then follows that if $v_P(f) \geq m$, then $a_0 = \cdots = a_{m-1} = 0$, and

so $f^{(0)}(P) = \cdots = f^{(m-1)}(P) = 0$. On the other hand, if $f^{(0)}(P) = \cdots = f^{(m-1)}(P) = 0$, then $a_0 = \cdots = a_{m-1} = 0$, and so $f = a_m t^m + a_{m+1}t^{m+1} + \cdots + g_s t^s$, and it follows that $v_P(f) \geq m$.

For each $i = 0, 1, 2, \ldots$, define the map

$$\begin{aligned} \phi_i : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f^{(i)}(P_1), \ldots, f^{(i)}(P_n)), \end{aligned}$$

and for each ϕ_i define a radius r_i, $0 < r_i < n$ such that r_i is an integer.

Lemma 6.1. *Fix a nonnegative integer i. Let ϕ_i, the divisor G, and r_i be defined as above. For each element $\mathbf{c} \in \mathbb{F}_q^n$, define $\mathscr{M}_{r_i}(\mathbf{c}; G) := \{f \in L(G) \,|\, \phi_i(f) \in S_{r_i}(\mathbf{c})\}$, where $S_{r_i}(\mathbf{c})$ is the sphere of radius r_i with centre $\mathbf{c}$. Then there exists an element $\mathbf{c}_i \in \mathbb{F}_q^n$ such that $\mathscr{M}_{r_i}(\mathbf{c}_i; G)$ has cardinality at least*

$$\frac{|L(G)| \cdot \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right)}{q^n}.$$

Proof. $S_{r_i}(\mathbf{c})$ has

$$\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j}$$

elements. Therefore, for any f, the point $\phi_i(f)$ lies in exactly $\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j}$ such spheres.

Now, assume the cardinality of every $\mathscr{M}_{r_i}(\mathbf{c}; G)$ is strictly less than

$$\frac{|L(G)| \cdot \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right)}{q^n}$$

and let $\mathbf{c}_i$ be chosen such that $\mathscr{M}_{r_i}(\mathbf{c}_i; G)$ is maximal. Then

$$\sum_{\mathbf{c} \in \mathbb{F}_q^n} |\mathscr{M}_{r_i}(\mathbf{c}; G)| \leq q^n \cdot |\mathscr{M}_{r_i}(\mathbf{c}_i; G)| < |L(G)| \cdot \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right).$$

Since each $\phi_i(f)$ is in exactly $\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j}$ spheres, the above inequality gives us

$$\left| \bigcup_{\mathbf{c} \in \mathbb{F}_q^n} \mathscr{M}_{r_i}(\mathbf{c}; G) \right| < |L(G)|,$$

but $\bigcup_{\mathbf{c} \in \mathbb{F}_q^n} \mathscr{M}_{r_i}(\mathbf{c}; G) = L(G)$, a contradiction. □

For some $\mathbf{c}_0, \ldots, \mathbf{c}_{m-1}$, define

$$\mathscr{M}_m := \bigcap_{i=0}^{m-1} \mathscr{M}_{r_i}(\mathbf{c}_i; G) = \{f \in L(G) \,|\, \phi_i(f) \in S_{r_i}(\mathbf{c}_i),\ i = 0, 1, \ldots, m-1\}.$$

Lemma 6.2. *There exist* $\mathbf{c}_0, \ldots, \mathbf{c}_{m-1}$ *such that*

$$|\mathscr{M}_m| \geq |L(G)| \cdot \prod_{i=0}^{m-1} \left(\frac{1}{q^n} \sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right).$$

Proof. We induct on m. If $m = 1$, this is simply Lemma 6.1. Suppose now that $m \geq 2$ and that

$$|\mathscr{M}_{m-1}| \geq |L(G)| \cdot \prod_{i=0}^{m-2} \left(\frac{1}{q^n} \sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right).$$

Then it follows from the proof of Lemma 6.1 (using $\mathscr{M}_{m-1}$ instead of $L(G)$) that there exists some $\mathbf{c}_{m-1}$ such that the number of elements $f \in \mathscr{M}_{m-1}$ satisfying $\phi_{m-1}(f) \in S_{r_{m-1}}(\mathbf{c}_{m-1})$ is at least

$$\frac{|\mathscr{M}_{m-1}| \cdot \left(\sum_{j=0}^{r_{m-1}} (q-1)^j \binom{n}{j} \right)}{q^n}.$$

□

We are now ready to define the desired code. Let

$$\begin{aligned} \pi_m : \mathscr{M}_m &\longrightarrow \mathbb{F}_q^n, \\ f &\longmapsto (f^{(m)}(P_1), \ldots, f^{(m)}(P_n)) \end{aligned}$$

and let the code $C_m := \mathrm{im}(\pi_m)$.

Proposition 6.3. *Let*

$$\deg(G) < (m+1)n - \sum_{i=0}^{m-1} 2(m+1-i)r_i.$$

Then C_m *is a* q*-ary* (n, M_m, d_m) *code with*

$$M_m = |\mathscr{M}_m| \qquad \text{and} \qquad d_m \geq (m+1)n - \deg(G) - \sum_{i=0}^{m-1} 2(m+1-i)r_i.$$

Proof. Let $f, h \in \mathscr{M}_m$, $f \neq h$. We prove that

$$\mathrm{wt}(\pi_m(f) - \pi_m(h)) \geq (m+1)n - \deg(G) - \sum_{i=0}^{m-1} 2(m+1-i)r_i,$$

which is strictly positive since we assumed that $\deg(G) < (m+1)n - \sum_{i=0}^{m-1} 2(m+1-i)r_i$. It then follows that π_m is injective so that $M_m = |\mathscr{M}_m|$.

Since $f, h \in \mathscr{M}_m$, then $\phi_i(f), \phi_i(h) \in S_{r_i}(\mathbf{c}_i)$, $i = 0, 1, \ldots, m-1$, and so $\mathrm{wt}(\phi_i(f) - \phi_i(h)) \leq 2r_i$. Let $I_i \subseteq \{1, 2, \ldots, n\}$ such that $(f-h)^{(i)}(P_j) = 0 \Leftrightarrow j \in I_i$. Then

$$|I_i| = n - \mathrm{wt}(\phi_i(f-h)) \geq n - 2r_i, \quad i = 0, 1, \ldots, m-1. \tag{6.1}$$

Let $w := \mathrm{wt}(\pi_m(f) - \pi_m(h)) = \mathrm{wt}(\pi_m(f-h))$. Then

$$|I_m| = n - \mathrm{wt}(\phi_m(f-h)) = n - \mathrm{wt}(\pi_m(f-h)) = n - w, \tag{6.2}$$

since π_m is simply ϕ_m restricted to $\mathscr{M}_m$.

For k, $0 \le k \le m$, we have

$$j \in \bigcap_{i=0}^{k} I_i \;\Rightarrow\; (f-h)^{(0)}(P_j) = \cdots = (f-h)^{(k)}(P_j) = 0.$$

This is equivalent with $v_{P_j}(f-h) \ge k+1$, and so

$$f - h \in L\left(G - \sum_{k=0}^{m} \sum_{j \in \bigcap_{i=0}^{k} I_i} P_j\right).$$

(We see that a point P_j with $j \in I_0 \cap \cdots \cap I_l$ is counted once for $k=0, k=1, \ldots, k=l$, i.e. $l+1$ times.) Since f and h are distinct, then $f - h \neq 0$, so

$$l\left(G - \sum_{k=0}^{m} \sum_{j \in \bigcap_{i=0}^{k} I_i} P_j\right) \ge 0.$$

It follows that

$$\deg(G) \ge \deg \sum_{k=0}^{m} \sum_{j \in \bigcap_{i=0}^{k} I_i} P_j = \sum_{k=0}^{m} \left|\bigcap_{i=0}^{k} I_i\right|.$$

Now,

$$\left|\bigcap_{i=0}^{k} I_i\right| \ge n - \sum_{i=0}^{k} 2r_i, \qquad 0 \le k \le m-1$$

because of (6.1), and

$$\left|\bigcap_{i=0}^{m} I_i\right| \ge n - w - \sum_{i=0}^{m-1} 2r_i$$

because of (6.2). Then

$$\deg(G) \ge \sum_{k=0}^{m} \left|\bigcap_{i=0}^{m} I_i\right| \ge \sum_{k=0}^{m-1} \left(n - \sum_{i=0}^{k} 2r_i\right) + n - w - \sum_{i=0}^{m-1} 2r_i.$$

So

$$w \ge (m+1)n - \deg(G) - \sum_{i=0}^{m-1} 2r_i(m+1-i),$$

as desired. □

Lemma 6.4. *Let*

$$\sigma_i := \frac{q-1}{q^{2(m+1-i)} + q - 1}.$$

Then

$$H_q(\sigma_{m+1-i}) - 2i\sigma_{m+1-i} = \log_q\left(1 + \frac{q-1}{q^{2i}}\right).$$

Proof.

$$\begin{aligned}
H_q(\sigma_{m+1-i}) &= \frac{q-1}{q^{2(m+1-m-1+i)}+q-1}\cdot\log_q(q-1) - \frac{q-1}{q^{2i}+q-1}\cdot\log_q\left(\frac{q-1}{q^{2i}+q-1}\right) \\
&\quad - \left(1-\frac{q-1}{q^{2i}+q-1}\right)\cdot\log_q\left(1-\frac{q-1}{q^{2i}+q-1}\right) \\
&= \frac{(q-1)\log_q(q-1)}{q^{2i}+q-1} - \frac{(q-1)\log_q(q-1)}{q^{2i}+q-1} + \frac{(q-1)\log_q(q^{2i}+q-1)}{q^{2i}+q-1} \\
&\quad - \left(1-\frac{q-1}{q^{2i}+q-1}\right)\log_q\left(\frac{q^{2i}+q-1-q+1}{q^{2i}+q-1}\right) \\
&= \frac{(q-1)\log_q(q^{2i}+q-1)}{q^{2i}+q-1} - \frac{(q-1)\log_q(q^{2i}+q-1)}{q^{2i}+q-1} \\
&\quad - \log_q\left(\frac{q^{2i}}{q^{2i}+q-1}\right) + \frac{(q-1)\log_q(q^{2i})}{q^{2i}+q-1} \\
&= \log_q\left(\frac{q^{2i}+q-1}{q^{2i}}\right) + \frac{2i(q-1)}{q^{2i}+q-1} \\
&= \log_q\left(1+\frac{q-1}{q^{2i}}\right) + 2i\sigma_{m+1-i}.
\end{aligned}$$

□

Theorem 6.5. *Let q be a prime power. Then there exists a sequence of codes $(C_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ with length n_i, code rate R_i, and relative minimum distance δ_i such that $n_i \to \infty$ and*

$$R_0 \geq 1 - \delta_0 - \frac{1}{A(q)} + \sum_{i=2}^{\infty}\log_q\left(1+\frac{q-1}{q^{2i}}\right),$$

where $R_i \to R_0$ and $\delta_i \to \delta_0$ as $i \to \infty$.

Proof. Let $(X_i)_{i=1}^{\infty}$ be a sequence of nonsingular projective curves defined over $\mathbb{F}_q$ with growing genus $g(X_i)$ and number of rational points $|X_i(\mathbb{F}_q)|$ such that $|X_i(\mathbb{F}_q)| \to \infty$ and

$$\lim_{i\to\infty}\frac{|X_i(\mathbb{F}_q)|}{g(X_i)} = A(q).$$

From now on I will skip the indices i and consider X to be some $X \in \{X_i\}_{i=1}^{\infty}$.
Let m be a positive integer, $n := |X(\mathbb{F}_q)| - 1$, and $r_j := \lfloor \sigma_j n \rfloor$ with

$$\sigma_j := \frac{q-1}{q^{2(m+1-j)}+q-1},$$

and pick an $\mathbb{F}_q$-rational divisor G such that Proposition 6.3 is satisfied. Call the code we have just made for C_m, and let the number of codewords be M_m. Proposition 6.3 and Riemann–Roch then give us

$$\begin{aligned}
\frac{\log_q M_m}{n} + \frac{d}{n} \geq \frac{\deg(G)-g+1}{n} + \sum_{k=0}^{m-1}\frac{1}{n}\log_q\left(\sum_{i=0}^{r_k}(q-1)^i\binom{n}{i}\right) - \frac{m\cdot\log_q q^n}{n} \\
+ (m+1) - \frac{\deg(G)}{n} - \frac{1}{n}\sum_{i=0}^{m-1}2(m+1-i)r_i.
\end{aligned}$$

We now let $n \to \infty$ and get

$$R + \delta \geq -A(q) + \lim_{n\to\infty} \sum_{k=0}^{m-1} \frac{1}{n} \log_q \left(\sum_{i=0}^{r_k} (q-1)^i \binom{n}{i} \right) + 1 - \sum_{i=0}^{m-1} 2(m+1-i)\sigma_i.$$

Using Lemma 2.12 on $\lim_{n\to\infty} \frac{1}{n} \log_q \left(\sum_{i=0}^{r_k} (q-1)^i \binom{n}{i} \right)$, we find that the right-hand side of the above inequality is

$$\begin{aligned}
&= 1 - \frac{1}{A(q)} - \sum_{i=0}^{m-1} 2(m+1-i)\sigma_i + \lim_{n\to\infty} \sum_{k=0}^{m-1} H_q\left(\frac{r_k}{n}\right) \\
&= 1 - \frac{1}{A(q)} - \sum_{i=0}^{m-1} 2(m+1-i)\sigma_i + \sum_{k=0}^{m-1} H_q(\sigma_k) \\
&= 1 - \frac{1}{A(q)} + \sum_{i=0}^{m-1} (H_q(\sigma_i) - 2(m+1-i)\sigma_i) \\
&= 1 - \frac{1}{A(q)} + \sum_{i=2}^{m+1} (H_q(\sigma_{m+1-i}) + 2i\sigma_{m+1-i}) \\
&= 1 - \frac{1}{A(q)} + \sum_{i=2}^{m+1} \log_q \left(1 + \frac{q-1}{q^{2i}}\right),
\end{aligned}$$

according to Lemma 6.4. Letting $m \to \infty$, we get the desired result. □

The following was in [17] presented with proof as in our proof of Theorem 6.5. I here present it as a corollary instead.

Corollary 6.6. *For any prime power q and $\delta \in [0, 1 - (A(q))^{-1} + \sum_{i=2}^{\infty} \log_q(q + q^{-2i}(q-1))]$, we have*

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \sum_{i=2}^{\infty} \log_q \left(1 + \frac{q-1}{q^{2i}}\right).$$

Proof. Since $\alpha_q(\delta)$ is continuous and decreasing in the interval $[0, \frac{q-1}{q}]$, it suffices to show that given any $R_0 \in [0, 1 - (A(q))^{-1} + \sum_{i=2}^{\infty} \log_q(q + q^{-2i}(q-1))]$, we can find a sequence of codes $(C_i)_{i=1}^{\infty}$ such that $R_i \to R_0$, where the sequence of codes is defined as in Theorem 6.5 and R_i denotes the code rate of C_i.

It is clear that we can make $R_i \to 0$ simply by choosing divisors G_i so that $\deg(G_i) = 0$. Then, since the number of words in each code C_i is $M_i \leq |L(G)|$, we will never have more than q words in each code. Then

$$0 \leq R_i \leq \frac{\log_q(q)}{n_i} \to 0.$$

On the other hand, it is clear that given a curve X, the greater $\deg(G)$ is, the greater the code rate of C_m is. Because of the condition that $\deg(G) < (m+1)n - \sum_{i=0}^{m-1} 2(m+1-i)r_i$, we can find out how big we can make R by putting $\deg(G) = (m+1)n - \sum_{i=0}^{m-1} 2(m+1-i)r_i - 1$.

We then get the following calculation:

$$\begin{aligned}
\frac{1}{n}\log_q M_m &\geq \frac{1}{n}\log_q\left(|L(G)|\cdot\prod_{i=0}^{m-1}\left(\frac{1}{q^n}\left(\sum_{j=0}^{r_i}(q-1)^j\binom{n}{j}\right)\right)\right)\\
&= \frac{1}{n}l(G)+\frac{1}{n}\sum_{i=0}^{m-1}\left(\log_q\sum_{j=0}^{r_i}(q-1)^j\binom{n}{j}-n\right)\\
&\quad \text{Letting } n\to\infty\text{, Riemann–Roch and Lemma 2.12 give us}\\
R &\geq \lim_{n\to\infty}\frac{1}{n}(\deg(G)+1-g)+\lim_{n\to\infty}\sum_{i=0}^{m-1}H_q\left(\frac{r_i}{n}\right)-m\\
&\quad \text{Substituting } (m+1)n-\sum_{i=0}^{m-1}2(m+1-i)r_i-1 \text{ for } \deg(G)\text{, we get}\\
&= \lim_{n\to\infty}\frac{1}{n}\left((m+1)n-\sum_{i=0}^{m-1}2(m+1-i)r_i-1+1-g\right)\\
&\quad +\sum_{i=0}^{m-1}H_q(\sigma_i)-m\\
&= m+1-\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{m-1}2(m+1-i)r_i-\frac{1}{A(q)}+\sum_{i=0}^{m-1}H_q(\sigma_i)-m\\
&= 1-\sum_{i=0}^{m-1}2(m+1-i)\sigma_i-\frac{1}{A(q)}+\sum_{i=0}^{m-1}H_q(\sigma_i)\\
&\quad \text{We now have the same expression as in the middle of the proof of}\\
&\quad \text{Theorem 6.5, which gave us}\\
&= 1-\frac{1}{A(q)}+\sum_{i=2}^{m+1}\log_q\left(1+\frac{q-1}{q^{2i}}\right),
\end{aligned}$$

and, again as in the proof of Theorem 6.5, we obtain the desired result by letting $m\to\infty$.

Now we know that we can make $R(C_i)$ approach 0 as well as $1-(A(q))^{-1}+\sum_{i=2}^{\infty}\log_q(q+q^{-2i}(q-1))$. Now let $R_0\in[0,1-(A(q))^{-1}+\sum_{i=2}^{\infty}\log_q(q+q^{-2i}(q-1))]$. We want to find a sequence of codes $(C_i)_{i=1}^{\infty}$ such that $R_i\to R_0$.

In the previous calculations we found that

$$\lim_{n\to\infty}\frac{\log_q M_m}{n}\geq\lim_{n\to\infty}\frac{l(G)}{n}+\sum_{i=0}^{m-1}H_q(\sigma_i)-m.$$

That followed from the fact that

$$M_m\geq|L(G)|\cdot\prod_{i=0}^{m-1}\left(\frac{1}{q^n}\left(\sum_{j=0}^{r_i}(q-1)^j\binom{n}{j}\right)\right).$$

Now, since the codes C_m are not necessarily linear, we can remove codewords from C_m (if

necessary) and obtain equality for M_m. It then follows that

$$\lim_{n\to\infty} \frac{\log_q M_m}{n} = \lim_{n\to\infty} \frac{l(G)}{n} + \sum_{i=0}^{m-1} H_q(\sigma_i) - m.$$

Recall that for each positive integer n, we are considering a code C_m on one of the curves $X \in \{X_i\}_{i=1}^{\infty}$ for a positive integer m. Let

$$S := \sum_{i=0}^{m-1} H_q(\sigma_i) - m.$$

I now claim that we can choose G such that

$$l(G) = \lfloor (R_0 - S) \cdot n \rfloor .$$

It will then follow that

$$\lim_{n\to\infty} \frac{\log_q M_m}{n} \to R_0.$$

To prove the claim that we can choose such a G, it suffices to use Proposition 8.3 page 192–193 in [2] (the proposition is meant for characteristic 0, but the proof is valid for all characteristics) and induction. If $\deg(G) = 0$, then $l(G) = 1$ or 0. Suppose $l(G) \geq 0$ and choose G' such that $G' \succ G$ and $\deg(G') = \deg(G) + 1$. Then it follows from the proposition that $l(G') = l(G) + 1$ or $l(G') = l(G)$. As soon as $\deg(G) \geq 2g - 1$, then $l(G') = l(G) + 1$ always.

It follows that given any nonnegative integer, we can choose G such that $l(G)$ equals that integer. From the argument in the beginning of this proof, it also follows that $\deg(G)$ won't exceed the bound in Proposition 6.3. □

The proof of this bound is nonconstructive, since the code C_m that was defined uses vectors $\mathbf{c} \in \mathbb{F}_q^n$ such that $\mathscr{M}_r$ has big cardinality. But Xing never shows how to pick these vectors.

6.2 An Explicit Construction

In [8] it is shown that the codes defined in the previous chapter can be constructed explicitly. The main idea is to prove that given certain conditions, Lemma 6.2 is fulfilled for any $\mathbf{c}_0, \ldots, \mathbf{c}_{m-1}$. This makes it possible to choose such vectors explicitly. The drawback is that the choices of δ (or R) will be limited compared to the codes of the previous chapter.

For a nonsingular projective curve X defined over $\mathbb{F}_q$ with at least one $\mathbb{F}_q$-rational point, a nonnegative integer i, and a function $f \in \mathbb{F}_q(X)$, let $f^{(i)}(P)$ be defined as in Section 6.1. Let m be a positive integer, G an $\mathbb{F}_q$-rational divisor, and let $P_1, \ldots, P_n$ be $\mathbb{F}_q$-rational points such that $P_1, \ldots, P_n \notin \mathrm{Supp}(G)$. Furthermore, let $\mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ be the $\mathbb{F}_q$-vector space of all $m \times n$ matrices over $\mathbb{F}_q$. Define

$$\begin{array}{rcl} \nu_m : L(G) & \longrightarrow & \mathrm{Mat}_{l\times n}(\mathbb{F}_q) \\ f & \longmapsto & \begin{pmatrix} f^{(0)}(P_1) & f^{(0)}(P_2) & \ldots & f^{(0)}(P_n) \\ f^{(1)}(P_1) & f^{(1)}(P_2) & \ldots & f^{(1)}(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f^{(m-1)}(P_1) & f^{(m-1)}(P_2) & \ldots & f^{(m-1)}(P_n) \end{pmatrix}. \end{array}$$

For given nonnegative integers $r_0, \ldots, r_{m-1}$, we want to consider all functions in $L(G)$ such that each row i of the above matrix is a vector in $B_{r_i}(\mathbf{0})$. (In the previous section, we considered functions such that each row i was a vector in $B_{r_i}(\mathbf{c}_i)$ for some vector $\mathbf{c}_i$, $i = 0, \ldots, m-1$.) We denote that set by $\tilde{Y}(r_0, \ldots, r_{m-1})$, i.e.

$$\tilde{Y}(r_0, \ldots, r_{m-1}) := \{f \in L(G) \,|\, \mathrm{wt}((f^{(i)}(P_1), \ldots, f^{(i)}(P_n))) \leq r_i,\ i = 0, \ldots, m-1\}.$$

Now, the crucial bit of the proof of the bound in the previous chapter was that we had enough functions in the subset of $L(G)$ that we considered. Our goal is to show that given certain conditions,

$$|\tilde{Y}(r_0, \ldots, r_{m-1})| \geq |L(G)| \cdot \prod_{i=0}^{m-1} \left(\frac{1}{q^n} \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right) \right).$$

It will appear that a sufficient condition is $\deg(G) \geq mn + 2g - 1$, as the following proposition shows.

Proposition 6.7. *If* $\deg(G) \geq mn + 2g - 1$, *then*

$$|\tilde{Y}(r_0, \ldots, r_{m-1})| = |L(G)| \cdot \prod_{i=0}^{m-1} \left(\frac{1}{q^n} \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right) \right).$$

Proof. Note that if J is the set of all matrices satisfying that row i is an element in $B_{r_i}(\mathbf{0})$, $i = 0, \ldots, m-1$, then $\tilde{Y}(r_0, \ldots, r_{m-1}) = \nu_m^{-1}(J)$. Since the number of elements in J is

$$|J| = \prod_{i=0}^{m-1} \left(\sum_{j=0}^{r_i} (q-1)^j \binom{n}{j} \right),$$

we only need to show that given any matrix $T \in \mathrm{Mat}_{m \times n}(\mathbb{F}_q)$, we have $|\nu_m^{-1}(T)| = |L(G)|/q^{mn}$.

Now, before proceeding, note that the condition $\deg(G) \geq mn + 2g - 1$ and the fact that $mn \geq 0$ imply that $l(G) = \deg(G) - g + 1$, and so $|L(G)| = q^{\deg(G)-g+1}$.

We start the proof by showing that ν_m is surjective. Then, since ν_m is linear, we have that $|\nu_m^{-1}(0)| = |\nu_m^{-1}(T)|$, and so it suffices to find the kernel of ν_m.

We show that ν_m is surjective by finding $|L(G)|/|\ker(\nu_m)|$. The kernel is

$$\ker(\nu_m) = L(G - mD),$$

where $D = P_1 + \cdots + P_n$. This follows from the discussion of $f^{(i)}(P)$ in the previous section, where we concluded that $f^{(0)}(P) = \cdots = f^{(m-1)}(P) = 0$ if and only if P is a zero of order $\geq m$ of f. Since $\deg(G) \geq mn + 2g - 1$, then $|L(G - mD)| = q^{\deg(G)-mn-g+1}$, and it follows that

$$|\nu_m(L(G))| = |L(G)|/|\ker(\nu_m)| = q^{\deg(G)-g+1-\deg(G)+mn+g-1} = q^{mn},$$

which is exactly the number of possible $m \times n$ matrices. So this proves that ν_m is surjective.

It follows that $\nu_m^{-1}(T) = |\ker(\nu_m)| = q^{\deg(G)-mn-g+1} = |L(G)|/q^{mn}$, as desired. □

The rest of the construction is the same as in the previous section. A calculation similar to the calculation in Corollary 6.6 reveals that these codes can be constructed for any

$$\delta \in \left[0, 1 - \frac{2}{A(q)} - \frac{2(q^3+q^2-1)}{(q+1)^2(q-1)(q^2+q-1)} \right].$$

6.3 Another Way to Reach Xing's Bound

In Section IV of [8] another construction has been made which reaches the same bound. I will here only show a special case involving the bound we get when we put $m = 1$ in the previous two sections.

The following construction involves a standard Goppa code and some of its cosets. This will make the minimum distance smaller, but the code rate will be much larger. Note that the code will no longer be linear, since a coset C' of C doesn't contain $\mathbf{0}$ and hence itself won't be linear. I first present the construction and next show that this code will be the same as the code presented in the previous section with $m = 1$.

Let $(X_i)_{i=1}^{\infty}$ be the curve sequence from the last two sections, let $X \in \{X_i\}_{i=1}^{\infty}$, let $n = |X(\mathbb{F}_q)| - 1$, and let r be a nonnegative integer such that $n - 4r \geq 1$. This r will serve the same role as r_0 did in the two previous sections. Let the Goppa code be $C(D, G)$ with $D = P_1 + \cdots + P_n$ and $\deg(G) < n - 4r$. Let $e_1, \ldots, e_n$ be functions in $\mathbb{F}_q(X)$ such that e_i has a simple pole in P_i and $v_{P_i}(e_j) \geq 0$ if $i \neq j$, $i, j = 1, \ldots, n$. Let $\varphi : \mathbb{F}_q(X) \longrightarrow \mathbb{F}_q(X)/L(G)$ be the canonical homomorphism and put

$$S(r) := \varphi^{-1}\left(\left\{\sum_{i\in I} a_i e_i + L(G) \,|\, I \subset \{1, \ldots, n\}, 0 \leq |I| \leq r \text{ and } a_i \in \mathbb{F}_q^{\times},\, i \in I\right\}\right),$$

where for $I = \emptyset$ we put $\sum_{i\in I} a_i e_i := 0$. Note that $S(r)$ contains $L(G)$ as a subset. Now define $\mu : S(r) \longrightarrow \mathbb{F}_q^n$ where μ maps f to $(\mu_1(f), \ldots, \mu_n(f))$, where μ_i maps f to its free coefficient in the P_i-adic power series expansion as described in Section 6.1, but where we choose a single t such that $v_{P_i}(t) = 1$ for $i = 1, \ldots, n$. (Such a t exists according to the Strong Approximation Theorem, Theorem 4.20.) Note that the free coefficient in a P-adic power series expansion can be 0 even though f has a pole in P.

We define the code $C'_r(D, G)$ to be

$$C'_r(D, G) := \mu(S(r)).$$

The Goppa code $C(D, G)$ is a subset of $C'_r(D, G)$. Furthermore, whenever there exists a function f with poles in some of the P_i, then $f + L(G)$ maps to a coset of $C(D, G)$ (not necessarily unequal to $C(D, G)$ itself) because of the linearity of μ. The coset representative of least weight always has weight of at most r. It is explicitly proved in [8] that this code reaches the Xing bound. (It is in that proof that we use the condition that $\deg(G) < n - 4r$.) Here I will show how C_r from the previous section is equal to such a code.

Suppose G' is a divisor such that $P_i \notin \mathrm{Supp}(G')$, $i = 1, \ldots, n$. Define the map

$$\begin{aligned} \pi : L(G') &\longrightarrow \mathbb{F}_q^n, \\ f &\longmapsto \left(f^{(1)}(P_1), \ldots, f^{(1)}(P_n)\right). \end{aligned}$$

Note that this is the special case of Xing's codes where $m = 1$, and in the previous section we showed that if $\deg(G') \geq 1 \cdot n + 2g - 1$, then we could reach Xing's bound for $m = 1$ by defining the code $C_r(D, G') := \pi\left(\phi_{G'}^{-1}(B_r(\mathbf{0}))\right)$, where $\phi_{G'} : L(G') \longrightarrow \mathbb{F}_q^n$ is defined by $f \longmapsto (f(P_1), \ldots, f(P_n))$.

Now, with t defined as above, redefine G to be $G := G' - D + \mathrm{div}(t)$. It then clearly follows that $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. Since $G' = G + D - \mathrm{div}(t)$, we have

$$\ker(\phi_{G'}) = L(G' - D) = L(G - \mathrm{div}(t)).$$

Define an isomorphism $L(G) \xrightarrow{\simeq} L(G - \mathrm{div}(t))$ by $f \longmapsto tf$ and note that $\pi(tf) = \phi(f)$. From this, we obtain that

$$\pi(\ker(\phi_{G'})) = \pi(L(G - \mathrm{div}(t))) = \mathrm{im}(\phi_G) = C(D, G).$$

Because of linearity, it follows that C_r is a union of cosets of $C(D, G)$.

The author also presents a way to find the elements $e_1, \ldots, e_n$ in polynomial time.

6.4 Elkies's 2003 Improvement

I here present a construction that improves Xing's 2003 bound. The bound we obtain here is given by

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right).$$

The bound was originally found by Elkies in 2003 for square prime powers q and by H. Niederreiter and F. Özbudak in 2004 for any prime power q. However, the following construction is due to Stichtenoth and Xing in 2005. In this section I give a proof of the main results of Stichtenoth and Xing. In the end of this section I have made a proof that this bound is indeed better than Xing's 2003 bound.

$\mathbb{N}$ will here denote the set of positive integers $\{1, 2, 3, \ldots\}$. I define $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$.

We shall here construct a map from a certain subset J of $L(mP_0 + G)$ such that we always have at least t zeros in any codeword. This gives us very good control over the minimum distance d. With a proper choice of m and G, the map becomes an injection, and so we get a high amount of codewords. If we take the union of all $L(mP_0 + G)$ where we vary G, then the minimum distance is not very much affected, but the code rate increases so that we obtain the desired bound.

I will here skip the proofs of the lemmas and the first proposition and rather focus on the construction of the code sequence.

Lemma 6.8. *Let n, s, t be integers such that $n \geq t > 0$ and $s \geq 0$. Let*

$$B(n, t, s) = \left| \{(m_1, \ldots, m_n) \in \mathbb{N}_0^n \mid \mathrm{wt}(m_1, \ldots, m_n) = t \text{ and } \sum_{i=1}^{n} m_i = s\} \right|.$$

Then

$$B(n, t, s) = \binom{n}{t}\binom{s-1}{t-1}.$$

Lemma 6.9. *Let q be a positive integer and $(n_i)_{i=1}^{\infty}$ and $(t_i)_{i=1}^{\infty}$ be sequences of positive integers such that $n_i \to \infty$ and $t_i/n_i \to \sigma$ as $i \to \infty$, where σ is a real number satisfying $0 < \sigma < 1$. Then*

$$\frac{\log_q \binom{n_i}{t_i}}{n_i} \to -\sigma \log_q(\sigma) - (1 - \sigma)\log_q(1 - \sigma).$$

Proposition 6.10. *Let X be a nonsingular projective curve defined over $\mathbb{F}_q$ with function field F and at least two $\mathbb{F}_q$-rational points, let D be a divisor with support consisting of $\mathbb{F}_q$-rational points and such that $\deg(D) \geq 2g - 1$, and let $P_1, \ldots, P_t$ be $\mathbb{F}_q$-rational points on X such that $P_i \notin \mathrm{Supp}(D)$, $i = 1, \ldots, t$. Let $G = \sum_{i=1}^{t} m_i P_i$ where $m_1, \ldots, m_t$ are positive integers. Let*

$$F_D(G) := \{f \in L(D + G) \mid v_{P_i}(f) = -m_i,\ i = 1, \ldots, t\}.$$

Then

$$|F_D(G)| = q^{m+s-g+1}\left(1-\frac{1}{q}\right)^t, \quad \textit{where} \quad m=\deg(D), \quad s=\sum_{i=1}^{t} m_i = \deg(G).$$

We now start defining the desired code. Let the curve X have function field F and genus g. Let $P_0, P_1, \ldots, P_n$ be distinct $\mathbb{F}_q$-rational points on X. Define

$$S = S(mP_0; P_1, \ldots, P_n; s, t) := \bigcup_G F_{mP_0}(G), \quad m, t, s \in \mathbb{N}, \quad t \leq n, \quad t \leq s,$$

where G runs over all divisors of the form

$$G = \sum_{j=1}^{t} m_{i_j} P_{i_j}, \quad 1 \leq i_j \leq n, \quad m_{i_j} \in \mathbb{N}, \quad \deg(G) = s.$$

In other words, S consists of all elements f in all vector spaces $L(mP_0 + G)$ such that f has poles in the entire support of G and of the same order for each point, and where $\mathrm{Supp}(G)$ consists of exactly t points among $P_1, \ldots, P_n$ and G is of degree s.

It is clear that $G_1 \neq G_2 \Rightarrow F_{mP_0}(G_1) \cap F_{mP_0}(G_2) = \emptyset$, since the elements in $F_{mP_0}(G_1)$ must have poles in all points $P \in \mathrm{Supp}(G_1)$ and of exactly the same order as those points. The following map is therefore well-defined. Let

$$\phi : S \longrightarrow \mathbb{F}_q^n$$

such that $f \in F_{mP_0}(G) \Rightarrow \phi(f) = (x_1, \ldots, x_n)$ with

$$x_i = \begin{cases} f(P_i) & \text{if } P_i \notin \mathrm{Supp}(G), \\ 0 & \text{if } P_i \in \mathrm{Supp}(G). \end{cases}$$

An immediate consequence of this definition is that any element in $\mathrm{im}(\phi)$ will have Hamming weight at most $n - t$, since any divisor G has t points in its support.

Definition 6.11. *We define the non-linear code*

$$C = C(mP_0; P_1, \ldots, P_n; s, t) := \phi(S) \subseteq \mathbb{F}_q^n.$$

Proposition 6.12. *Let $m, s, t \in \mathbb{N}$ such that*

$$m \geq 2g-1, \quad s \geq t, \quad n - m - 2s - 2t \geq 1.$$

Then C is a q-ary (n, M, d) code with

$$M = q^{m+s+1-g}\left(1-\frac{1}{q}\right)^t \binom{n}{t}\binom{s-1}{t-1}$$

and

$$d \geq n - m - 2s - 2t.$$

Proof. Each G gives us $|F_{mP_0}(G)| = q^{m+s+1-g}(1-q^{-1})^t$ elements in S. The number of ways to change the divisor G is the same as the number of ways to give $P_1, \ldots, P_n$ nonnegative coefficients such that the sum of the coefficients is s and the weight is t. According to Lemma 6.8, there are $\binom{n}{t} \cdot \binom{s-1}{t-1}$ ways to do that.

We now show that given $f, h \in S$, then $\mathrm{wt}(\phi(f) - \phi(h)) \geq n - m - 2s - 2t$, which we assumed was at least 1.

Suppose

$$f \in F_{mP_0}(G_1), \quad h \in F_{mP_0}(G_2), \quad f \neq h.$$

Since $f - h$ can't have poles of higher order than either f or h has, we have that $f - h \in L(mP_0 + G_1 + G_2)$. Now define

$$Z := \{P_i \,|\, P_i \notin \mathrm{Supp}(G_1) \cup \mathrm{Supp}(G_2),\, f(P_i) = h(P_i),\, i = 1, \ldots, n\}.$$

Then $(f-h)(P_i) = 0$ whenever $P_i \in Z$, and so

$$f - h \in L\left(mP_0 + G_1 + G_2 - \sum_{P \in Z} P\right).$$

Since $f - h \neq 0$, the above vector space is nontrivial, and so

$$\deg\left(mP_0 + G_1 + G_2 - \sum_{P \in Z} P\right) = m + 2s - |Z| \geq 0.$$

To determine the weight of $\phi(f) - \phi(h)$, remember that $\mathrm{wt}(\phi(f)) \leq n - t$, and the same with $\mathrm{wt}(\phi(h))$. It follows that

$$\mathrm{wt}(\phi(f) - \phi(h)) \geq n - |Z| - 2t.$$

We have from above that $-|Z| \geq -m - 2s$, and so

$$\mathrm{wt}(\phi(f) - \phi(h)) \geq n - m - 2s - 2t,$$

as desired. □

Theorem 6.13. *Let q be a prime power and let*

$$0 \leq \delta \leq 1 - \frac{2}{A(q)} - \frac{4q-2}{(q-1)(q^3+1)}.$$

Then

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right).$$

Proof. Since $\alpha_q(\delta)$ is continuous, we assume that

$$0 < \delta < 1 - \frac{2}{A(q)} - \frac{4q-2}{(q-1)(q^3+1)}.$$

Let $(X_i)_{i=1}^{\infty}$ be a sequence of nonsingular projective curves defined over $\mathbb{F}_q$ with genus $g(X_i)$ such that $g(X_i) \to \infty$ and $\frac{|X_i(\mathbb{F}_q)|}{g(X_i)} \to A(q)$. Put

$$n_i = |X_i(\mathbb{F}_q)| - 1, \quad s_i = \left\lfloor \frac{qn_i}{(q-1)(q^3+1)} \right\rfloor, \quad t_i = \left\lfloor \frac{n_i}{q^3+1} \right\rfloor, \quad m_i = n_i - \lfloor \delta_i n_i \rfloor - 2s_i - 2t_i.$$

For simplicity, I drop the i-indices, but always assume that the curves in question are elements in $\{X_i\}_{i=1}^{\infty}$.

Because of the upper bound we put on δ, we have that

$$\lim_{n\to\infty}\frac{m}{n} = 1-\delta-\frac{4q-2}{(q-1)(q^3+1)} > \frac{2}{A(q)} = \lim_{n\to\infty}\frac{2g}{n}.$$

Multiplying with n on both sides, we have $m > 2g$, or rather $m \geq 2g+1$. Also, note that s without the floor-function is t without the floor-function multiplied with $\frac{q}{q-1}$. So $s \geq t$. It follows that for big enough n, we have from the previous proposition that there exists a q-ary (n, M, d') code where $d' \geq d$ and

$$M = q^{m+s+1-g}\left(1-\frac{1}{q}\right)^t\binom{n}{t}\binom{s-1}{t-1}, \qquad d = n-m-2s-2t.$$

Since we defined $m = n - \lfloor \delta n \rfloor - 2s - 2t$, it follows that for $n >> 0$,

$$d = \lfloor \delta n \rfloor \qquad \text{and} \qquad \lim_{n\to\infty}\frac{d}{n} = \delta.$$

This brings us to

$$\begin{aligned}
\frac{\log_q(M)}{n}+\frac{d}{n} &= \frac{1}{n}\left(m+s+1-g+\log_q\left(1-\frac{1}{q}\right)^t+\log_q\left(\binom{n}{t}\binom{s-1}{t-1}\right)+d\right)\\
&\quad \text{We replace } m \text{ with } n-d-2s-2t, \text{ we note that}\\
&\quad \left(1-\frac{1}{q}\right)^t = \frac{(q-1)^t}{q^t}, \text{ and get:}\\
&= \frac{1}{n}\Bigg(n-d-2s-2t+s+1-g+t\log_q(q-1)-t\\
&\qquad +\log_q\left(\binom{n}{t}\binom{s-1}{t-1}\right)+d\Bigg)\\
&= \frac{1}{n}\left(n-g-s-3t+1+t\log_q(q-1)+\log_q\binom{n}{t}+\log_q\binom{s-1}{t-1}\right).
\end{aligned}$$

We now let $n\to\infty$ and apply Lemma 6.9 on the two last logarithms. On the last logarithm we note that $(s-1)/s \to 1$ as $n\to\infty$, and similarly with t. We then let s act as n does in the lemma and note that

$$\lim_{n\to\infty}\frac{1}{n}\log_q\binom{s}{t} = \lim_{n\to\infty}\frac{s}{n}\cdot\frac{1}{s}\log_q\binom{s}{t} = \lim_{n\to\infty}\frac{q}{(q-1)(q^3+1)}\cdot\frac{1}{s}\log_q\binom{s}{t}.$$

We get:

$$\begin{aligned}
\frac{\log_q(M)}{n}+\frac{d}{n} \;\to\; & 1-\frac{1}{A(q)}-\frac{q}{(q-1)(q^3+1)}-\frac{3}{q^3+1}+\frac{\log_q(q-1)}{q^3+1}\\
&-\left(\frac{1}{q^3+1}\log_q\left(\frac{1}{q^3+1}\right)+\left(1-\frac{1}{q^3+1}\right)\log_q\left(1-\frac{1}{q^3+1}\right)\right)\\
&-\frac{q}{(q-1)(q^3+1)}\cdot\left(\frac{q-1}{q}\log_q\left(\frac{q-1}{q}\right)+\frac{1}{q}\log_q\left(\frac{1}{q}\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&= 1 - \frac{1}{A(q)} - \frac{q}{(q-1)(q^3+1)} - \frac{3}{q^3+1} + \frac{\log_q(q-1)}{q^3+1} \\
&\quad + \frac{\log_q(q^3+1)}{q^3+1} - \log_q(q^3) + \log_q(q^3+1) + \frac{\log_q(q^3)}{q^3+1} - \frac{\log_q(q^3+1)}{q^3+1} \\
&\quad - \frac{q(q-1)\log_q(q-1)}{q(q-1)(q^3+1)} + \frac{q(q-1)}{q(q-1)(q^3+1)} + \frac{q}{q(q-1)(q^3+1)} \\
&= 1 - \frac{1}{A(q)} - \frac{q}{(q-1)(q^3+1)} - \frac{3}{q^3+1} + \frac{\log_q(q-1)}{q^3+1} \\
&\quad + \frac{\log_q(q^3+1)}{q^3+1} - 3 + \log_q(q^3+1) + \frac{3}{q^3+1} - \frac{\log_q(q^3+1)}{q^3+1} \\
&\quad - \frac{\log_q(q-1)}{q^3+1} + \frac{1}{q^3+1} + \frac{1}{(q-1)(q^3+1)} \\
&= 1 - \frac{1}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right).
\end{aligned}
$$

Since $d' \geq d$, the theorem follows. □

Remark 6.14. The following calculations show that Elkies's bound is better than Xing's bound for $q \geq 2$. Let q be a prime power.

$$
\begin{aligned}
\log_q\left(1 + \frac{1}{q^3}\right) &\geq \sum_{i=2}^{\infty} \log_q\left(1 + \frac{1}{q^{2i}}\right) \\
&\Updownarrow \\
1 + \frac{1}{q^3} &\geq \prod_{i=2}^{\infty}\left(1 + \frac{1}{q^{2i}}\right) = 1 + \frac{1}{q^4} + \frac{1}{q^6} + \frac{1}{q^8} + 2\cdot\frac{1}{q^{10}} + 2\cdot\frac{1}{q^{12}} + \cdots \\
&\Updownarrow \\
\frac{1}{q^3} &\geq \frac{1}{q^4} + \sum_{i=3}^{\infty}\left\lfloor\frac{i-1}{2}\right\rfloor\cdot\frac{1}{q^{2i}}
\end{aligned}
$$

The last expression follows because of the number of ways we can multiply together distinct pairs of $1, q^4, q^6, \ldots, q^{2\lfloor i/2\rfloor}, \ldots, q^{2i}$ to get q^{2i}. Before continuing, remember that if $|x| < 1$, we have

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

If we differentiate on both sides and multiply with x, we get

$$x + 2x^2 + 3x^3 + \cdots = \frac{x}{(1-x)^2}.$$

Note that the sum in our expression begins with $i = 3$ instead of $i = 0$. We now have

$$
\begin{aligned}
\frac{1}{q^4} + \sum_{i=3}^{\infty}\left\lfloor\frac{i-1}{2}\right\rfloor\cdot\frac{1}{q^{2i}} &< \frac{1}{q^4} + \frac{1}{2}\sum_{i=3}^{\infty}\frac{i-1}{q^{2i}} \\
&= \frac{1}{q^4} + \frac{1}{2}\left(\sum_{i=3}^{\infty} i\cdot(q^{-2})^i - \sum_{i=3}^{\infty}(q^{-2})^i\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{q^4} + \frac{1}{2}\left(\frac{q^{-2}}{(1-q^{-2})^2} - q^{-2} - 2q^{-4}\right. \\
&\qquad \left. - \left(\frac{1}{1-q^{-2}} - 1 - q^{-2} - q^{-4}\right)\right) \\
&= \frac{1}{q^4} + \frac{1}{2}\left(\frac{1}{(q-q^{-1})^2} - q^{-2} - 2q^{-4}\right. \\
&\qquad \left. - \frac{q^2(1-q^{-2})}{(q-q^{-1})^2} + \frac{(q-q^{-1})^2}{(q-q^{-1})^2} + q^{-2} + q^{-4}\right) \\
&= \frac{1}{2} \cdot \frac{1 - q^2 + 1 + (q-q^{-1})^2}{(q-q^{-1})^2} + \frac{1}{2q^4} \\
&= \frac{1}{2} \cdot \frac{(2 - q^2 + q^2 - 2 + q^{-2}) \cdot q^2}{(q-q^{-1})^2 \cdot q^2} + \frac{1}{2q^4} \\
&= \frac{1}{2} \cdot \frac{(q^2 \cdot q^{-2})}{(q^2-1)^2} + \frac{1}{2q^4} \\
&= \frac{1}{2} \cdot \frac{1}{q^4 - 2q^2 + 1} + \frac{1}{2q^4} \\
&\leq \frac{1}{2 \cdot (1/2)q^4} + \frac{1}{2q^4} \\
&= \frac{3}{2q^4} \\
&\leq \frac{1}{q^3}
\end{aligned}
$$

when $q \geq 2$, as desired.

Chapter 7

Transitive Codes

An important question that has arisen in connection with finding new bounds for $\alpha_q(\delta)$ and $\alpha_q^{\text{lin}}(\delta)$, is whether special kinds of codes have as good asymptotic properties as codes in general. An unsolved question is whether or not cyclic codes are asymptotically good at all. In February this year, a new article (see [6]) proved that several classes of cyclic codes are asymptotically bad. However, if we losen up on our restrictions a bit and consider the more general class of transitive codes, they actually reach the bound that we found in Section 6.4. This was proved by Stichtenoth in [12]. The idea of Stichtenoth was to let the Galois group of the function field over the rational function field define the permutations of each codeword. I will here go through the main parts of the proof.

Stichtenoth first proves that the class of transitive codes meets the Tsfasman–Vlăduţ–Zink bound. With $q = l^2$, l a prime power, he defines a tower of function fields $F_0 \subset F_1 \subset F_2 \subset \cdots$ by $F_0 := \mathbb{F}_q(x_0)$, the rational function field, and for all $i \geq 0$, $F_{i+1} := F_i(x_{i+1})$ where $x_{i+1}^l + x_{i+1} = x_i^l/(x_i^{l-1} + 1)$. Furthermore, he lets $w := x_0^l + x_0$ and $z := w^{l-1}$ and defines a new tower $E_0 \subset E_1 \subset E_2 \subset \cdots$ where $E_0 := \mathbb{F}_q(z)$ is the rational function field and for all $i \geq 1$, E_i is the Galois closure of the field extension F_{i-1}/E_0. This tower meets the Drinfeld–Vlăduţ bound.

Given an n, we define the divisors G_0 and D on E_n in the following way: We let G_0 be the sum of all points of E_n lying over the pole of z in $\mathbb{F}_q(z)$, and we let D be the sum of all points of E_n lying over the zero of $z-1$ in $\mathbb{F}_q(z)$. It is shown that $z-1$ splits completely in the extension $E_n/\mathbb{F}_q(z)$. Define $N := [E_n : \mathbb{F}_q(z)]$. It follows that $\deg(D) = N$. Given a number δ between 0 and 1, we next choose a nonnegative integer r such that the relative minimum distance of $C(D, rG_0)$ is at least δ. Stichtenoth then shows that N grows quickly enough to ensure that the code rate can be placed arbitrarily near $1 - \delta - 1/(l-1)$.

We now show that each $C(D, rG_0)$ is transitive. Since $P_1, \ldots, P_N$ are all the points lying over the zero of $z-1$, we have that $\text{Gal}(E_n/E_0)$ acts transitively on $P_1, \ldots, P_N$. Since $\text{Supp}(G_0)$ are all the points lying over the pole of z, we have that rG_0 will remain invariant under the action of any $\sigma \in \text{Gal}(E_n/E_0)$. So if $f \in L(G_0)$, then also $\sigma(f) \in L(G_0)$. This means that if $(f(P_1), \ldots, f(P_N)) \in C(D, rG_0)$, then also $(\sigma(f(P_1)), \ldots, \sigma(f(P_N))) \in C(D, rG_0)$. But $(\sigma(f(P_1)), \ldots, \sigma(f(P_N))) = (f(\sigma P_1), \ldots, f(\sigma P_N))$, which is a permutation of the codeword $(f(P_1), \ldots, f(P_N))$. This proves that $C(D, G_0)$ is transitive.

The choice of the divisors G_0 and D also works in Section 6.4. We let rG_0 , $r \geq 0$ from this chapter substitute mP_0 from Section 6.4 and let the support of D from this chapter substitute the points $P_1, \ldots, P_n$ from Section 6.4.

Stichtenoth's proof is not valid for cyclic codes, since this would demand a tower of function fields $E_0 \subset E_1 \subset E_2 \subset \cdots$ where each $\mathrm{Gal}(E_n/E_0)$ is cyclic, and it has been proved that any such tower of function fields satisfies

$$\lim_{i \to \infty} N(E_i)/g(E_i) = 0,$$

where $N(E_i)$ is the number of $\mathbb{F}_q$-rational points of E_i and $g(E_i)$ is the genus of E_i. With this limit, we would get the trivial bound on R.

Chapter 8

Separating and Frameproof Codes

Another kind of codes that are asymptotically good are separating and frameproof codes. In this chapter I present a new bound on frameproof codes presented by Chaoping Xing in 2002. Details can be found in [16].

An (s,t)-separating code is a code $C \subseteq \mathbb{F}_q^n$ (or more generally, vectors over a set S with $|S| = q$ elements) such that whenever disjoint subsets $A \subset C$ and $B \subset C$ satisfy $|A| = s$ and $|B| = t$, then there exists a positive integer $i \in \{1, \ldots, n\}$ such that any $(a_1, \ldots, a_n) \in A$ and $(b_1, \ldots, b_n) \in B$ satisfy $a_i \neq b_i$. Separating codes are useful in constructions of hash functions and authenticating ownership claims. If we put $t = 1$, the code is said to be s-frameproof. We say that the code is an $\mathrm{FPC}_s(n, q^k)$-code, where n is the length of the code and q^k is the number of codewords. As the name suggests, frameproof codes are used to prevent framing, such as when the set of codewords is a set of different fingerprints and we want to prevent people from forging other people's fingerprints.

From the above definitions, it follows that an $\mathrm{FPC}_s(n, M)$-code has the property that for any $A \subset C$ satisfying $|A| \leq s$, and for any element $(x_1, \ldots, x_n) \in C \setminus A$, there exists an $i \in \{1, \ldots, n\}$ such that for all $(y_1, \ldots, y_n) \in A$, we have $y_i \neq x_i$.

From this, it is clear that any code C is 1-frameproof. It also immediately follows that for a q-ary code C to be q-frameproof, it is necessary that any q-subset of C has two codewords that have a coordinate in common. We see here that the parameter s in an s-frameproof code has put an upper bound on the minimum distance d. It can in fact be shown that an $[n, k, d]_q$-linear code C is an s-frameproof code where $s = \lfloor (n-1)/(n-d) \rfloor$. It follows that all bounds that apply for linear codes also apply for frameproof codes.

Now suppose we have a projective nonsingular curve X defined over $\mathbb{F}_q$, two positive integers $n \geq 1$ and $s \geq 2$, and $\mathbb{F}_q$-rational points $P_1, \ldots, P_n$. Let $P_1 + \cdots + P_n = D$. Suppose an $\mathbb{F}_q$-rational, effective divisor G can be chosen so that $L(sG - D) = \{0\}$. For each $i = 1, \ldots, n$, let t_i be a local parameter at P_i and let $v_i = v_{P_i}(G)$. (These are all nonnegative since G is effective.) Define

$$\begin{aligned} \phi : L(G) &\longrightarrow \mathbb{F}_q^n, \\ f &\longmapsto ((t_1^{v_1} f)(P_1), \ldots, (t_n^{v_n} f)(P_n)). \end{aligned}$$

Define the code $C(D, G) := \mathrm{im}(\phi)$.

Proposition 8.1. *Let D, G, n, and s be as above. Then $C(D, G)$ is an $\mathrm{FPC}_s(n, q^{l(G)})$-code.*

Proof. If $((t_1^{v_1}f)(P_1),\ldots,(t_n^{v_n}f)(P_n)) = \mathbf{0}$, then $v_{P_i}(f) \geq -v_i + 1$, $i = 1,\ldots,n$. It follows that $f \in L(sG - D)$, and so $f = 0$. Hence, ϕ is injective, and the number of codewords is $q^{l(G)}$.

We want to make sure that for any r-subset A of $C(D,G)$ with $1 \leq r \leq s$, any codeword $(b_1,\ldots,b_n) \notin A$ has a coordinate b_i satisfying $b_i \neq a_i$ for any codeword $(a_1,\ldots,a_n) \in A$. For any $f \in L(G)$, let c_f denote $((t_1^{v_1}f)(P_1),\ldots,(t_n^{v_n}f)(P_n))$. Let $A = \{c_{f_1},\ldots,c_{f_r}\}$. Suppose $c_g \in C(D,G)$, and suppose that for any $i = 1,\ldots,n$, the ith coordinate $(t_i^{v_i}g)(P_i)$ of c_g is equal to the ith coordinate $(t_i^{v_i}f_j)(P_i)$ of the word c_{f_j} for some $j \in \{1,\ldots,r\}$. We want to prove that $c_g \in A$, i.e. that $g = f_l$ for some $l \in \{1,\ldots,r\}$.

For $i \in \{1,\ldots,n\}$, let $\pi_i : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, $(a_1,\ldots,a_n) \longmapsto a_i$, be the ith projection map. Now, with c_g defined as above, we have

$$0 = \prod_{j=1}^{r} \pi_i(c_{f_j} - c_g) = \prod_{j=1}^{r} (t_i^{v_i}f_j - t_i^{v_i}g)(P_i).$$

It follows that

$$v_{P_i}\left(\prod_{j=1}^{r}(t_i^{v_i}f_j - t_i^{v_i}g)\right) \geq 1.$$

Since $t_i^{rv_i}$ is a factor in the above product, we find that

$$v_{P_i}\left(\prod_{j=1}^{r}(f_j - g)\right) \geq -rv_i + 1.$$

Now recall that $v_i = v_{P_i}(G)$. Since i was randomly chosen, it then follows that

$$\prod_{j=1}^{r}(f_j - g) \in L\left(rG - D\right) \subseteq L\left(sG - D\right) = \{0\}.$$

So $f_l = g$ for some $l \in \{1,\ldots,r\}$, as desired. □

We prove here that sequences of such codes have good asymptotic bounds. In his article, Xing has found the existence of divisors G of large degree that meet the conditions of the proposition. The proof of the following lemma can be found in [16].

Lemma 8.2. *Let g be the genus of X, and let m, n, and s be nonnegative integers such that $s \geq 2$ and $g \leq m \leq n < sm$. Let D be any effective divisor of degree n. If we have*

$$sm - n \leq g(1 - 2\log_q s) - 1 - \log_q \frac{(3\sqrt{q} - 1)g}{(q-1)(\sqrt{q} - 1)},$$

then there exists an effective divisor G of degree m such that $L(sG - D) = \{0\}$.

In the following theorem we fix m and show that these conditions hold. We then have the code from the previous proposition and use that to find the asymptotic bound.

Let $R_q(s) := \limsup_{n\to\infty} \frac{1}{n}\log_q M_q(n,s)$, where $M_q(n,s) := \max\{M \mid \text{there exists a } q\text{-ary frameproof code } \mathrm{FPC}_s(n,M)\}$. In the following theorem, we let $A(q) = \limsup_{g\to\infty} N_q(g)/g$, where $N_q(g) = \max\{|X(\mathbb{F}_q)|\}$ where the maximum is taken over all nonsingular projective curves of genus g. For q a square prime power, we have $A(q) = \sqrt{q} - 1$. For all other prime powers q, we have $A(q) \leq \sqrt{q} - 1$ from the Drinfeld–Vlăduţ bound.

Theorem 8.3. *Let q be a prime power and suppose s is an integer such that $2 \leq s \leq A(q)$. Then*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - 2\log_q s}{sA(q)}.$$

Proof. Let $(X_i)_{i=1}^{\infty}$ be a sequence of nonsingular projective curves defined over $\mathbb{F}_q$ with genus $g(X_i)$ such that $|X_i(\mathbb{F}_q)| \to \infty$ and $|X_i(\mathbb{F}_q)|/g(X_i) \to A(q)$, and put $|X_i(\mathbb{F}_q)| = n_i$. Let $P_1, \ldots, P_{n_i}$ be all points on X_i and put $P_1 + \cdots + P_{n_i} = D_i$. We shall here define an m_i and show that s and m_i meet the conditions of Lemma 8.2. We then know that there exists a divisor G_i of degree m_i that satisfies $L(sG_i - D_i) = \{0\}$. It follows from Proposition 8.1 that there exists a frameproof code $C(D_i, G_i)$, and, letting $i \to \infty$, we shall see that this code sequence gives us the desired result.

Let $0 < \varepsilon < 1 - 2\log_q s$. This is possible since $A(q) \leq \sqrt{q} - 1$ gives us $s \leq \sqrt{q} - 1$, and so $\log_q s < \frac{1}{2}$. Now put

$$m_i := \left\lfloor \frac{n_i + (1 - 2\log_q s - \varepsilon)g(X_i)}{s} \right\rfloor.$$

We show that the conditions in Lemma 8.2 are satisfied for $i >> 0$. We have

$$\lim_{i\to\infty} \frac{m_i}{g(X_i)} = \frac{A(q) + 1 - 2\log_q s - \varepsilon}{s} > \frac{A(q)}{s} \geq 1$$

from the assumption that $s \leq A(q)$, and since we have assumed that $A(q) \geq 2$ and $s \geq 2$, we have

$$\lim_{i\to\infty} \frac{m_i}{n_i} = \frac{A(q) + 1 - 2\log_q s - \varepsilon}{sA(q)} < \frac{A(q) + 1}{sA(q)} < \frac{2A(q)}{sA(q)} \leq 1.$$

It is clear that

$$\lim_{i\to\infty} \frac{sm_i}{n_i} = 1 + \frac{1 - 2\log_q s - \varepsilon}{A(q)} > 1$$

and that

$$\lim_{i\to\infty} \frac{sm_i - n_i - (1 - 2\log_q s)g(X_i)}{g(X_i)} = -\varepsilon < 0. \tag{8.1}$$

We conclude that for $i >> 0$, we have $g(X_i) < m_i < n_i < sm_i$, and so almost all the conditions from Lemma 8.2 are satisfied. For the final bit, we have from (8.1) the following inequality (8.2). We see that this must be true for $i >> 0$ by dividing by $g(X_i)$ on both sides of (8.2) and letting $i \to \infty$. (Recall that $g(X_i) \to \infty$, so $\log_q(g(X_i))/g(X_i) \to 0$.) Thus, for $i >> 0$, we have

$$sm_i - n_i \leq g(X_i)(1 - 2\log_q s) - 1 - \log_q \frac{(3\sqrt{q} - 1)g(X_i)}{(q-1)(\sqrt{q} - 1)}. \tag{8.2}$$

So for $i >> 0$, there is a divisor G_i of degree m_i such that $L(sG_i - D_i) = \{0\}$, and so the proposition gives us that there exists a code $C(D_i, G_i)$ for $i >> 0$. From the definition of m_i together with Riemann–Roch, we have

$$R_q(s) \geq \lim_{i\to\infty} \frac{\log_q q^{l(G_i)}}{n_i} \geq \lim_{i\to\infty} \frac{m_i - g(X_i) + 1}{n_i} = \frac{1}{s} + \frac{1 - 2\log_q s}{sA(q)} - \frac{\varepsilon}{sA(q)} - \frac{1}{A(q)}.$$

Letting $\varepsilon \to 0$, we get the desired result. □

Remark 8.4. It could be tempting to substitute $s = 1/(1-\delta)$ and get

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \frac{(1-\delta)(1+2\log_q(1-\delta))}{A(q)}, \quad \frac{1}{2} \leq \delta \leq 1 - \frac{1}{A(q)},$$

which for square q would be a much better bound than the one found in Section 6.4. The problem with such an approach is that even though an $[n,k,d]_q$-linear code is an s-frameproof code with $s = \lfloor (n-1)/(n-d) \rfloor$, we don't know if an s-frameproof code in general will give us a good minimum distance d. For the code sequence of the last theorem, we only found a value for s independent of what the minimum distance was.

Remark 8.5. It is possible to get a bound for (s,t)-separating codes using the construction from this section. Generalising the proof of Proposition 8.1, we can show that if $L(stG-D) = \{0\}$, then the code $C(D,G)$ is an (s,t)-separating code. Let A and B be as in the beginning of this chapter. We simply suppose that for any index i, there exist a pair of codewords $a \in A$ and $b \in B$ such that a and b are equal in the ith coordinate. We then get a product as in the proof of Proposition 8.1, and we see that the condition $L(stG-D) = \{0\}$ gives us $a = b$.

However, there are constructions for separating codes that give us much better bounds than the one we get with this approach.

Remark 8.6. In Section 4.3, we saw that Goppa codes attain the Gilbert–Varshamov bound. Since any $[n,k,d]_q$-linear code is an s-frameproof code with $s = \lfloor (n-1)/(n-d) \rfloor$, it immediately follows that $R_q(s) \geq 1 - H_q(1-1/s)$, where $H_q(\delta)$ is the q-ary entropy function. Some numbers were given as an example in Remark 4.24, where δ was set to be $3/4$. This corresponds to $s = 4$.

Chapter 9

Other Codes from Algebraic Curves

The improvements of the Tsfasman–Vlăduţ–Zink bound that were presented in Chapter 6 were mostly based on constructions of codes different from Goppa codes. It seems that an important part of the work to find new bounds for $\alpha_q(\delta)$ is to find new ways to define codes from algebraic curves.

A few articles have been published since the turn of the century where new constructions of codes from algebraic curves have been attempted. I will here mention three constructions made by Xing, Niederreiter, and Lam in 1999. In chapters 10 and 11 I will study the asymptotic properties of the third of these classes of codes.

9.1 Two Constructions

One challenge that presents itself when it comes to defining new ways to construct codes is to find constructions that don't give codes that are equivalent to already existing ones. I here present two constructions that are equivalent to Goppa codes. The constructions were made by Xing, Niederreiter, and Lam in [19], and the proof that they are equivalent to Goppa codes were made by Özbudak and Stichtenoth in [7]. I have filled in the calculations that Özbudak and Stichtenoth left to the reader in [7].

9.1.1 The Construction of C^{I}

I here present the first construction, which I call C^{I}.

Let q be a prime power and let X be a nonsingular projective curve defined over $\mathbb{F}_q$ with at least two $\mathbb{F}_q$-rational points. Let g be the genus of X. Choose $n+1$ distinct points $P_\infty, P_1, \ldots, P_n$ of degree 1 and an effective divisor E of degree $2g$ with $P_\infty \notin \mathrm{Supp}(E)$. Then $l(E) = g+1$. Note that $l(E - P_\infty) = g$. This means that there exists a basis element w_0 for $L(E)$ such that $v_{P_\infty}(w_0) = 0$. (There are actually q such elements to choose from.) Similarly, there exists an integer n_1 such that $l(E - n_1 P_\infty) = g$ while $l(E - (n_1+1)P_\infty) = g-1$, so that there exists a second basis element w_1 for $L(E)$ such that $v_{P_\infty}(w_1) = n_1$. Continue in that manner until we have $g+1$ basis elements

$$w_0, \ldots, w_g \qquad \text{with} \qquad v_{P_\infty}(w_i) = n_i,\ n_0 = 0.$$

It is clear that $0 = n_0 < n_1 < \cdots < n_g \leq 2g$. The last inequality follows because $l(E - 2gP_\infty) \leq 1$.

Since E is nonspecial, we can for each $i \in \{1, \ldots, n\}$ choose an

$$f_i \in L(E + P_i) \setminus L(E).$$

We then have that $w_0, \ldots, w_g, f_1, \ldots, f_n$ are linearly independent and a basis for $L(E + P_1 + \cdots + P_n)$.

Let t be a local parameter at P_∞. Let

$$t_r := \begin{cases} t^r & \text{for } r \notin \{n_0, \ldots, n_g\}, \\ w_l & \text{for } r = n_l \in \{n_0, \ldots, n_g\}. \end{cases}$$

In other words, if $r = n_i = v_{P_\infty}(w_i)$ for some $i \in \{0, \ldots, g\}$, then we set $t_r = t_{n_i} = w_i$. Let s be a positive integer. Since no f_i has a pole in P_∞, then any f_i can be written as

$$f_i = \sum_{r=0}^{s} a_{r,i} t_r + h_{s+1,i} t_{s+1}, \quad i = 1, \ldots, n,$$

where $a_{r,i} \in \mathbb{F}_q$ and $h_{s+1,i} \in \mathcal{O}_{P_\infty}$. We will assume that s is large enough for the rest of the construction to make sense.

Let m be an integer with $g \leq m < n$, and (supposing for a moment that $n_g \neq m + g$) let

$$\mathbf{c}_i = (\widehat{a_{n_0,i}}, a_{1,i}, \ldots, \widehat{a_{n_1,i}}, \ldots, \widehat{a_{n_l,i}}, \ldots, a_{m+g,j}), \quad i = 1, \ldots, n.$$

Here, $\hat{x}$ means that the element x has been deleted. This means that we have $m+g+1-(g+1) = m$ entries in $\mathbf{c}_i$. Simplify this vector as $\mathbf{c}_i = (c_{1,i}, \ldots, c_{m,i})$. Let H be the $m \times n$ matrix

$$H = (\mathbf{c}_1^{\mathrm{T}}, \ldots, \mathbf{c}_n^{\mathrm{T}}).$$

We define

$$C^{\mathrm{I}} := C(P_\infty, P_1, \ldots, P_n; E; m)$$

as the code with parity-check matrix H.

9.1.2 The Construction of C^{II}

The second construction of Xing, Niederreiter, and Lam I call C^{II}. Let q, g, and X be as before and let $D \succ 0$ be a nonspecial divisor with $\deg(D) = g$. (See [19] for details on how to prove that such a divisor exists.) Then $l(D) = 1$. Let $P_\infty, P_1, \ldots, P_n$ be distinct points of degree 1. For $1 \leq i \leq n$, choose

$$g_i \in L(D + P_i) \setminus L(D).$$

Since $l(D) = 1$, we have that $L(D)$ consists of all constant functions. From this it follows that $1, g_1, \ldots, g_n$ is a basis for $L(D + \sum_{i=1}^{n} P_i)$.

Let t be a local parameter at P_∞ and put $v = v_{P_\infty}(D)$. We have $v \geq 0$ since D is effective and $v \leq g$ since $\deg(D) = g$. Let s be a positive integer. For each $i \in \{1, \ldots, n\}$, we can write

$$g_i = t^{-v} \cdot \left(\sum_{r=0}^{s} b_{r,i} t^r + k_{s+1,i} t^{s+1} \right),$$

where each $b_{r,i} \in \mathbb{F}_q$ and $k_{s+1,i} \in \mathcal{O}_{P_\infty}$. Assume s is large enough for the rest of the construction to make sense. For $i = 1, \ldots, n$, define

$$c_{r,i} := \begin{cases} b_{r-1,i} & \text{for } 1 \leq r \leq v, \\ b_{r,i} & \text{for } r \geq v+1. \end{cases}$$

So $c_{r,i}$ runs through all non-free coefficients in the power-series expansion of g_i. Let m be a positive integer such that $g \leq m < n$. For $i = 1, \ldots, n$, put

$$\mathbf{c}_i = (c_{1,i}, \ldots, c_{m,i}) \in \mathbb{F}_q^m.$$

Define the $m \times n$ matrix

$$H = (\mathbf{c}_1^{\mathrm{T}}, \ldots, \mathbf{c}_n^{\mathrm{T}}).$$

The code

$$C^{\mathrm{II}} = C(P_\infty, P_1, \ldots, P_n; D; m)$$

is defined to be the code with parity-check matrix H.

9.1.3 Proof that the Codes Are Goppa Codes

To prove that the codes in [19] are Goppa codes, Özbudak and Stichtenoth make another construction, which I call C^{III}. Next, they prove that C^{I} and C^{II} are special cases of C^{III}. Finally, they prove that C^{III} is a special case of the Goppa codes.

To construct C^{III}, let q, g, and X be as before, let B be a non-special divisor, and let $P_1, \ldots, P_n$ be points of degree 1. Then $l(B + P_i) = l(B) + 1$ for $i = 1, \ldots, n$. Let

$$f_i \in L(B + P_i) \setminus L(B)$$

for $i = 1, \ldots, n$. Then any $f \in L(B + \sum_{i=1}^n P_i)$ can be uniquely written as

$$f = \sum_{i=1}^n c_i f_i + w \tag{9.1}$$

where each c_i is in $\mathbb{F}_q$ and $w \in L(B)$. We see easily that the map

$$\alpha : L(B + \sum_{i=1}^n P_i) \longrightarrow \mathbb{F}_q^n$$

defined by $f \longmapsto (c_1, \ldots, c_n)$, with $c_1, \ldots, c_n$ defined by (9.1), is surjective with $\ker(\alpha) = L(B)$.

Choose $A \succ 0$ with $\mathrm{Supp}(A) \cap \{P_1, \ldots, P_n\} = \emptyset$. We then define

$$C^{\mathrm{III}} := C(B; P_1, \ldots, P_n; A) = \alpha\left(L\left(B + \sum_{i=1}^n P_i - A\right)\right).$$

Proposition 9.1. *C^{I} is a special case of C^{III}.*

Proof. We show that $C^{\mathrm{I}} = C(E; P_1, \ldots, P_n; (m+g+1)P_\infty)$. We use notations from the construction of C^{I}.

The proof is in two parts. We first prove that $(\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_q^n$ is in C^{I} if and only if $\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$ for some $w \in L(E)$ and u satisfying $v_{P_\infty}(u) \geq m+g+1$. Next we show that such vectors are exactly the codewords in $C(E; P_1, \ldots, P_n; (m+g+1)P_\infty)$.

Suppose $(\lambda_1, \ldots, \lambda_n) \in C^{\mathrm{I}}$. Then $\lambda_1 c_{i,1} + \lambda_2 c_{i,2} + \cdots + \lambda_n c_{i,n} = 0$ for $i = 1, \ldots, m$. Let $k_1, \ldots, k_m$ be such that $\mathbf{c}_i = (a_{k_1,i}, \ldots, a_{k_m,i})$ (i.e. k_i are all of the indices among $a_0, \ldots, a_{m+g}$ that are not equal to any n_j). Recall that

$$f_i = \sum_{r=0}^{s} a_{r,i} t_r + h_{s+1,i} t_{s+1}.$$

We have for all $1 \leq i \leq m$ that

$$\lambda_1 a_{k_i,1} + \lambda_2 a_{k_i,2} + \cdots + \lambda_n a_{k_i,n} = 0 \Rightarrow (\lambda_1 a_{k_i,1} + \cdots + \lambda_n a_{k_i,n}) t_{k_i} = 0.$$

If we do that for $i = 1, \ldots, n$ and add the expressions together, we get

$$(\lambda_1 a_{k_1,1} + \cdots + \lambda_n a_{k_1,n}) t_{k_1} + \cdots + (\lambda_1 a_{k_m,1} + \cdots + \lambda_n a_{k_m,n}) t_{k_m} = 0.$$

Now add similar expressions for all the other t_i that we haven't included here, and note that $t_i = w_i$ if $i = n_l$ for some $l \in \{0, \ldots, g\}$. We get

$$\begin{aligned}(\lambda_1 a_{0,1} + \cdots + \lambda_n a_{0,n}) t_0 + \cdots + (\lambda_1 a_{m+g,1} + \cdots + \lambda_n a_{m+g,n}) t_{m+g} \\ = (\lambda_1 a_{n_0,1} + \cdots + \lambda_n a_{n_0,n}) w_0 + \cdots + (\lambda_1 a_{n_g,1} + \cdots + \lambda_n a_{n_g,n}) w_g.\end{aligned}$$

Remember that $w_0, \ldots, w_g$ is a basis for $L(E)$, so the element on the right-hand side of the equation sign is in $L(E)$. Denote it by w. We reorganise the expression on the left-hand side and get

$$\lambda_1(a_{0,1}t_0 + a_{1,1}t_1 + \cdots + a_{m+g,1}t_{m+g}) + \cdots + \lambda_n(a_{0,n}t_0 + a_{1,n}t_1 + \cdots + a_{m+g,n}t_{m+g}) = w.$$

Now, since

$$f_i = \sum_{r=0}^{s} a_{r,i} t_r + h_{s+1,i} t_{s+1},$$

where we let $s \geq m+g+1$, we have

$$\lambda_1(f_1 - f_1') + \cdots + \lambda_n(f_n - f_n') = w,$$

where each $f_i' = \sum_{r=m+g+1}^{s} a_{r,i} t_r + h_{s+1,i} t_{s+1}$. Note that $f_1', \ldots, f_n'$ have order at least $m+g+1$ in P_∞. It follows that

$$\lambda_1 f_1 + \cdots + \lambda_n f_n = w + \lambda_1 f_1' + \cdots + \lambda_n f_n' = w + u,$$

where u has order at least $m+g+1$ in P_∞, as desired. This shows that if $(\lambda_1, \ldots, \lambda_n) \in C^{\mathrm{I}}$, then $\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$ where $w \in L(E)$ and u satisfies $v_{P_\infty}(u) \geq m+g+1$.

Now suppose

$$\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$$

where $w \in L(E)$ and u satisfies $v_{P_\infty}(u) \geq m+g+1$. We want to show that $\lambda_1 a_{k_i,1} + \cdots + \lambda_n a_{k_i,n} = 0$ for $i = 1, \ldots, m$. We have that

$$\lambda_1 \left(\sum_{r=0}^{s} a_{r,1} t_r + h_{s+1} t_{s+1} \right) + \cdots + \lambda_n \left(\sum_{r=0}^{s} a_{r,n} t_r + a_{s+1,n} t_{s+1} \right) = w + u.$$

We want the right-hand side to have the t_{k_i}-coefficients equal to 0 (because then the same applies for the left-hand side).

Since each $k_i \leq m+g$ and $v_{P_\infty}(u) \geq m+g+1$, the coefficient of t_{k_i} in u is 0. Furthermore, w can be written as a unique linear combination of $w_0, \ldots, w_g$, and those are exactly $t_{n_0}, \ldots, t_{n_g}$, which are the elements not among $t_{k_1}, \ldots, t_{k_m}$. This shows that if $\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$, then $\lambda_1 a_{k_i,1} + \cdots + \lambda_n a_{k_i,n} = 0$ for $i = 1, \ldots, m$.

We now prove that $\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$ with $w \in L(E)$ and $v_{P_\infty}(u) \geq m+g+1$ if and only if $(\lambda_1, \ldots, \lambda_n) \in C(E; P_1, \ldots, P_n; (m+g+1)P_\infty)$. We know from the construction of C^{III} that

$$\begin{aligned} &(c_1, \ldots, c_n) \in C(E; P_1, \ldots, P_n; (m+g+1)P_\infty) \\ &\qquad \Leftrightarrow \qquad c_1 f_1 + \cdots + c_n f_n + w' \in L\left(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty \right), \end{aligned}$$

where $w' \in L(E)$. Recall from the construction of C^{I} that $P_\infty \notin \mathrm{Supp}(E)$.

Suppose $\lambda_1 f_1 + \cdots + \lambda_n f_n = w + u$ with $w \in L(E)$ and $v_{P_\infty}(u) \geq m+g+1$. Then u is a linear combination of $f_1, \ldots, f_n$ modulo $L(E)$, so $v_{P_i}(u) \geq -1$ for each $i = 1, \ldots, n$ because of how we chose $f_1, \ldots, f_n$. It follows that $\lambda_1 f_1 + \cdots + \lambda_n f_n - w = u \in L(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty)$. Since $-w \in L(E)$, this shows that $(\lambda_1, \ldots, \lambda_n) \in C(E; P_1, \ldots, P_n; (m+g+1)P_\infty)$.

Suppose $(\lambda_1, \ldots, \lambda_n) \in C(E; P_1, \ldots, P_n; (m+g+1)P_\infty)$. Then $\lambda_1 f_1 + \cdots + \lambda_n f_n + w' \in L(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty)$, where $w' \in L(E)$. We then have that $\lambda_1 f_1 + \cdots + \lambda_n f_n + w' = u$ with $v_{P_\infty}(u) \geq m+g+1$, as desired. □

Proposition 9.2. *C^{II} is a special case of C^{III}.*

Proof. We use notations from the construction of C^{II}. We first prove that $(\lambda_1, \ldots, \lambda_n) \in C^{\mathrm{II}} \Leftrightarrow \lambda_1 g_1 + \cdots + \lambda_n g_n = b + w$ with $b \in L(D)$ and $v_{P_\infty}(w) \geq m - v + 1$. Recall from the construction of C^{II} that $l(D) = 1$, and so $L(D) = \mathbb{F}_q$. Recall also that $v \leq g \leq m$.

Let $\gamma_1, \ldots, \gamma_m$ be the m first nonzero exponents of t in the power series expansion of the g_i. (E.g. if $v = 2$, then $\gamma_1 = -2$, $\gamma_2 = -1$, $\gamma_3 = 1$.) We have

$$\begin{aligned} & (\lambda_1, \ldots, \lambda_n) \in C^{\mathrm{II}} \\ \Rightarrow \quad & \begin{cases} \lambda_1 c_{1,1} + \lambda_2 c_{1,2} + \cdots + \lambda_n c_{1,n} = 0 \\ \vdots \\ \lambda_1 c_{m,1} + \lambda_2 c_{m,2} + \cdots + \lambda_n c_{m,n} = 0 \end{cases} \\ \Rightarrow \quad & (\lambda_1 c_{1,1} + \lambda_2 c_{1,2} + \cdots + \lambda_n c_{1,n}) t^{\gamma_1} + \cdots + (\lambda_1 c_{m,1} + \cdots + \lambda_n c_{m,n}) t^{\gamma_m} = 0 \\ \Rightarrow \quad & \lambda_1 (g_1 - b_{0,1} - g_1') + \cdots + \lambda_n (g_n - b_{0,n} - g_n') = 0 \\ \Rightarrow \quad & \lambda_1 g_1 + \cdots + \lambda_n g_n = b + w, \end{aligned}$$

where $v_{P_\infty}(g_i') \geq m - v + 1$ for $i = 1, \ldots, n$, the element w is a combination of the g_i' (which means that also $v_{P_\infty}(w) \geq m - v + 1$), and $b \in \mathbb{F}_q = L(D)$.

Suppose now that $\lambda_1 g_1 + \cdots + \lambda_n g_n = b + w$ where $b \in \mathbb{F}_q = L(D)$ and $v_{P_\infty}(w) \geq m - v + 1$. We then have

$$\lambda_1 t^{-v} \left(\sum_{r=0}^{s} b_{r,1} t^r + b_{s+1,1} t^{s+1} \right) + \cdots + \lambda_n t^{-v} \left(\sum_{r=0}^{s} b_{r,n} t^r + b_{s+1,n} t^{s+1} \right) = b + w.$$

Since the right-hand side of this expression doesn't have negative order at P_∞, the sum of the coefficients on the left-hand side for negative powers of t will be 0. If $m = v$, we are done. If $m > v$, then since b is a constant function and $v_{P_\infty}(w) \geq m - v + 1$, we will also get 0 when we sum the coefficients of t^r for $1 \leq r \leq m - v$.

We now show that $\lambda_1 f_1 + \cdots + \lambda_n f_n = b + w$ for some $b \in \mathbb{F}_q$ and $v_{P_\infty}(w) \geq m - v + 1$ if and only if $(\lambda_1, \ldots, \lambda_n) \in C(D; P_1, \ldots, P_n; (m+1)P_\infty)$. If $\lambda_1 f_1 + \cdots + \lambda_n f_n = b + w$, then $\lambda_1 f_1 + \cdots + \lambda_n f_n - b = w \in L(D + \sum_{i=1}^{n} P_i - (m+1)P_\infty)$, as desired. (Remember that $v = v_{P_\infty}(D)$.) If $\lambda_1 f_1 + \cdots + \lambda_n f_n - b \in L(D + \sum_{i=1}^{n} P_i - (m+1)P_\infty)$ for some $b \in L(D)$, then $\lambda_1 f_1 + \cdots + \lambda_n f_n - b = w$ with $v_{P_\infty}(w) \geq m - v + 1$.

This gives us $C(D; P_1, \ldots, P_n; (m - v + 1)P_\infty)$ where $l(D) = 1$ and D is non-special. $(m - v + 1)P_\infty$ is effective because $m \geq g \geq v$. This finishes the proof. □

The last step of Özbudak and Stichtenoth in [7] is to prove that C^{III} is a special case of standard Goppa codes. The notations are the same as in the construction of C^{III}. The existence of z in the following theorem follows from the Strong Approximation Theorem, Theorem 4.20. The code $C(D, G)$ denotes the code from the Goppa construction presented in Section 4.1.

Theorem 9.3. *Let $z \in \mathbb{F}_q(X)$ so that $v_{P_i}(zf_i) = 0$ and $(zf_i)(P_i) = 1$, $i = 1, \ldots, n$. Then $C^{\mathrm{III}} = C(D, G)$ with $D = P_1 + \cdots + P_n$ and $G = B + \sum_{i=1}^{n} P_i - A - \mathrm{div}(z)$.*

Proof. Since $f_i \in L(B + P_i) \setminus L(B)$, $i = 1, \ldots, n$, we have $v_{P_i}(G) = v_{P_i}(B) + 1 - v_{P_i}(z) = -v_{P_i}(f_i) - v_{P_i}(z) = 0$, and so $\mathrm{Supp}(G) \cap \{P_1, \ldots, P_n\} = \emptyset$. Define the map

$$\beta : L(G) \longrightarrow \mathbb{F}_q^n$$

by $h \longmapsto (h(P_1), \ldots, h(P_n))$ and the map

$$\phi : L(B + \sum_{i=1}^{n} P_i - A) \longrightarrow L(G)$$

by $f \longmapsto zf$. The map ϕ is an isomorphism. Let α be as defined in the construction of C^{III}. We have the following diagram:

$$\begin{array}{ccc} L(B + \sum_{i=1}^{n} P_i - A) & \xrightarrow{\ \phi\ } & L(G) \\ & \searrow^{\alpha} & \downarrow \beta \\ & & \mathbb{F}_q^n \end{array}$$

We want the image of β to be the same as the image of α. Let $f \in L(B + \sum_{i=1}^{n} P_i - A)$. Then $f = \sum_{i=1}^{n} c_i f_i + w$ for some $c_1, \ldots, c_n \in \mathbb{F}_q$ and $w \in L(B)$, and so $\alpha(f) = (c_1, \ldots, c_n)$.

Recall that $(zf_i)(P_i) = 1$, $i = 1, \ldots, n$. We have $\phi(f) = zf = \sum_{i=1}^{n} c_i z f_i + zw$, and

$$\begin{aligned}
\beta(\phi(f)) &= ((zf)(P_1), \ldots, (zf)(P_n)) \\
&= \left(\left(\sum_{i=1}^{n} c_i z f_i + zw \right)(P_1), \ldots, \left(\sum_{i=1}^{n} c_i z f_i + zw \right)(P_n) \right) \\
&= \left(c_1 + \left(\sum_{i=2}^{n} c_i z f_i + zw \right)(P_1), \ldots, c_n + \left(\sum_{i=1}^{n-1} c_i z f_i + zw \right)(P_n) \right).
\end{aligned}$$

Now note that since $v_{P_i}(zf_i) = 0$, we have $v_{P_i}(z) = v_{P_i}(B) + 1$. Also recall that $v_{P_i}(f_j) \geq -v_{P_i}(B)$, $i \neq j$, $i, j = 1, \ldots, n$. This means that the above expression becomes $(c_1, \ldots, c_n)$, as desired. □

9.2 A Generalisation of Goppa Codes

The fourth construction that Özbudak and Stichtenoth comment on is found in [20] and is a generalised version of the third construction in their article, which Xing, Niederreiter, and Lam made a bit earlier the same year. I here only present the fourth construction.

Let X be a nonsingular projective curve defined over $\mathbb{F}_q$ with at least one $\mathbb{F}_q$-rational point. Denote its genus by g. Let $P_1, \ldots, P_s$ be distinct points with $\deg(P_i) = k_i$, and let $C_1, \ldots, C_s$ be $[n_i, k_i, d_i]_q$-linear codes with isomorphisms $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$. Note that given a function $f \in \mathscr{O}_{P_i}$, then $f(P_i)$ is regarded as f modulo $\mathfrak{m}_{P_i}\mathscr{O}_{P_i}$. This is regarded as an element in $\mathbb{F}_{q^{k_i}}$.

Let

$$\pi : L(G) \longrightarrow \mathbb{F}_q^n$$

be defined by $f \longmapsto (\pi_1(f(P_1)), \ldots, \pi_n(f(P_n)))$.

Definition 9.4. *Let the map π be defined as above. We then define the linear algebraic-geometric code $C := C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ to be the image of π. We will call C a* generalised AG code.

The length of the code is obviously $n := n_1 + \cdots + n_s$.

Let

$$Z = \left\{ S \subseteq \{1, \ldots, s\} \;\middle|\; \sum_{i \in S} k_i \leq \deg(G) \right\}.$$

Define the integer

$$\nu := \min \left\{ \sum_{i \notin S} d_i \;\middle|\; S \in Z \right\}.$$

Proposition 9.5. *Suppose $g \leq \deg(G) < \sum_{i=1}^{s} k_i$. Then $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ is an $[n, k, d]_q$-code with parameters*

$$k = l(G) \geq \deg(G) + 1 - g \qquad \text{and} \qquad d \geq \nu.$$

Proof. Note that the code is linear. To show that $k = l(G)$, we must show that π is injective. Suppose $h \in L(G)$ and $\pi(h) = 0$. We show that $h = 0$. We have $\pi_i(h(P_i)) = 0$ for $i = 1, \ldots, s$. Since the π_i are isomorphisms, we have $h(P_i) = 0$ for $i = 1, \ldots, s$, and so $h \in L(G - \sum_{i=0}^{s} P_i)$.

Since $\deg(P_i) = k_i$ for $i = 1, \ldots, s$, we have $\deg(G) < \sum_{i=1}^{s} k_i = \deg(\sum_{i=1}^{s} P_i)$, which means that $h = 0$.

To find the minimum distance, we only need to find the non-zero codeword of minimum weight. Suppose $0 \neq f \in L(G)$. Let

$$S = \{i \in \{1, \ldots, s\} \mid f(P_i) = 0\}.$$

We want to show that $S \in Z$, which we defined above. Next we will show that the weight $\mathrm{wt}((f(P_1, \ldots, f(P_s)) \geq \sum_{i \notin S} d_i$.

We have

$$0 \neq f \in L\left(G - \sum_{i \in S} P_i\right) \quad \Rightarrow \quad \deg(G) \geq \deg\left(\sum_{i \in S} P_i\right) = \sum_{i \in S} k_i.$$

So $S \in Z$.

Since $f(P_i) = 0 \Leftrightarrow \pi_i(f(P_i)) = 0$, we have $i \in S \Leftrightarrow \pi_i(f(P_i)) = 0$. It follows that

$$\mathrm{wt}(\pi(f)) = \sum_{i=1}^{s} \mathrm{wt}(\pi_i(f(P_i))) = \sum_{i \notin S} \mathrm{wt}(\pi_i(f(P_i))) \geq \sum_{i \notin S} d_i \geq \nu.$$

The second last inequality follows because the codes $C_1, \ldots, C_s$ are linear. This finishes the proof. □

Proposition 9.6. *Goppa codes are a special case of generalised AG codes.*

Proof. Let the cardinality of a set A be denoted by $\mathrm{card}(A)$. For $i = 1, \ldots, s$, put $k_i = 1$, $n_i = 1$, and $s = n$. Then the map π is exactly the same as the Goppa-code map. Note that the previous proposition with these parameters gives us $Z = \{S \subseteq \{1, \ldots, n\} \mid \mathrm{card}(S) \leq \deg(G)\}$ and $\nu = \min\{\mathrm{card}(\{1, \ldots, n\} - S) \mid S \in Z\} = n - \deg(G)$, as expected. □

In the rest of this thesis I will study different ways of how we can construct infinite sequences of such codes.

Chapter 10

Asymptotic Properties of Generalised AG Codes

In this chapter I present three ways to construct an infinite sequence of generalised AG codes. The first involves an infinite sequence of curves where I use closed points of degree 1 and 2. The second involves letting the degree of the points in question approach infinity and was found by Antonino Spera in [9]. The third is a combination of the first two constructions. I close with a graph showing the three bounds compared to the Gilbert–Varshamov and Tsfasman–Vlăduţ–Zink bounds.

10.1 The First Construction

This construction involves using the proof of the Tsfasman–Vlăduţ–Zink (TVZ) bound on generalised AG codes where $C_1, \ldots, C_s$ are fixed. I have made several attempts on getting relatively good asymptotic results for different versions of the C_i. I here present the attempt that gave the best result. The bound we find here comes close to the Gilbert–Varshamov bound for small values of δ.

Before presenting the construction, we need the following theorem.

Theorem 10.1. *For prime powers q, there exists an infinite sequence of projective nonsingular curves $(X_i)_{i=1}^{\infty}$ defined over $\mathbb{F}_q$ such that $|X_i(\mathbb{F}_{q^2})| \to \infty$ and $|X_i(\mathbb{F}_{q^2})|/g(X_i) \to q-1$, where $g(X)$ is the genus of X.*

Proof. A desired sequence of curves is presented by Garcia and Stichtenoth in [4] and is given by $\mathbb{F}_{q^2}(X_i) := \mathbb{F}_{q^2}(x_1, \ldots, x_i)$, where

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1}+1}, \qquad i = 1, \ldots, n-1.$$

It is shown there that $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i) = q-1$. It is clear that we for each X_i have a prime ideal with generator polynomials with coefficients in $\mathbb{F}_q$. □

The following proposition will also be important to us.

Proposition 10.2. *Let X be a nonsingular projective curve defined over $\mathbb{F}_q$. If s_i is the number of closed points of degree i on X over $\mathbb{F}_q$, then $|X(\mathbb{F}_{q^2})| = s_1 + 2s_2$.*

Proof. See page 179 in [13]. □

Let q be a prime power and let $(X_i)_{i=1}^{\infty}$ be an infinite sequence of nonsingular projective curves defined over $\mathbb{F}_q$ such that $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})| = \infty$ and $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i) = q-1$, where $g(X)$ is the genus of the curve X. For some curve X in $\{X_i\}_{i=1}^{\infty}$, let $s_1 = |X(\mathbb{F}_q)| - 1$ and $s_2 = \frac{1}{2}(|X(\mathbb{F}_{q^2})| - |X(\mathbb{F}_q)|)$. Then s_2 is the number of closed points of degree 2 on X. Let $P_1, \ldots, P_{s_1}$ be all points of degree 1 except for one—say P'—and let $P_{s_1+1}, \ldots, P_{s_1+s_2}$ be the closed points of degree 2. Let $C_1, \ldots, C_{s_1}$ be $[1,1,1]_q$-linear codes and $C_{s_1+1}, \ldots, C_{s_1+s_2}$ be $[2,2,1]_q$-linear codes.

Let $m \geq s_1$ be an integer with $m < s_1 + 2s_2$ and $G = mP'$. Say that

$$\deg(G) = s_1 + t$$

for some nonnegative integer $t < 2s_2$. We see that $\deg(G) < \sum_{i=1}^{s_1+s_2} k_i$ is fulfilled. Note also that we can assume that $g(X) \leq \deg(G)$ since we are naturally interested in positive values of $\deg(G) + 1 - g(X)$. Substituting $\deg(G) - s_1$ for t, we have from Proposition 9.5 that

$$d \geq s_1 + s_2 - s_1 - \left\lfloor \frac{t}{2} \right\rfloor \geq \frac{1}{2}s_1 + s_2 - \frac{1}{2}\deg(G). \tag{10.1}$$

This gives us $\deg(G) \geq s_1 + 2s_2 - 2d$. The dimension k satisfies $k \geq \deg(G) + 1 - g$. By choosing, if necessary, a linear subspace of the code we are constructing, we can say that $k = \deg(G)+1-g \geq s_1+2s_2-2d+1-g$. Since the length of the code is $s_1+2s_2 = |X(\mathbb{F}_{q^2})|-1$, we divide by $|X(\mathbb{F}_{q^2})| - 1$, let $|X(\mathbb{F}_{q^2})| \to \infty$, and get

$$R \geq 1 - 2\delta - \frac{1}{q-1}.$$

Theorem 10.3. *Let q be a prime power. Then for any $\delta \in [0, \sqrt{q}/(2(1+\sqrt{q}))]$, we can find an infinite sequence of generalised AG codes $(C_i)_{i=1}^{\infty}$ with minimum distances d_i, dimensions k_i, and lengths n_i such that $d_i/n_i \to \delta$ and $k_i/n_i \to R$ satisfying*

$$R \geq R_1 := 1 - 2\delta - \frac{1}{q-1}.$$

Proof. The only thing left to show is that it is sufficient to put $\deg(G) \geq s_1$ in order to obtain $\delta \leq \sqrt{q}/(2(1+\sqrt{q}))$ in the above construction, as it is clear that larger $\deg(G)$ gives us smaller δ.

A sufficient way of achieving $\delta = \sqrt{q}/(2(1+\sqrt{q}))$, is putting

$$d = \left\lfloor \frac{\sqrt{q}}{2(1+\sqrt{q})}(s_1 + 2s_2) \right\rfloor.$$

We want to find what $\deg(G)$ must be. Using (10.1), we get

$$\left\lfloor \frac{\sqrt{q}}{2(1+\sqrt{q})}(s_1 + 2s_2) \right\rfloor \geq \frac{1}{2}s_1 + s_2 - \frac{1}{2}\deg(G).$$

This gives us

$$\frac{\deg(G)}{s_1 + 2s_2} \geq \frac{1}{1+\sqrt{q}}.$$

I now show that $\deg(G)$ must be at least s_1 in order to satisfy this. We have

$$\frac{s_1}{s_1+2s_2} = \frac{s_1/g(X)}{(s_1+2s_2)/g(X)}.$$

Letting $|X(\mathbb{F}_{q^2})| \to \infty$, we get $q-1$ in the denominator and at most $\sqrt{q}-1$ in the numerator. This gives us

$$\frac{s_1/g(X)}{(s_1+2s_2)/g(X)} \to a \leq \frac{1}{1+\sqrt{q}}.$$

as $|X(\mathbb{F}_{q^2})| \to \infty$. So it follows that $\deg(G)$ must be at least s_1 in order to obtain $\delta \geq \sqrt{q}/(2(1+\sqrt{q}))$. □

Remark 10.4. In Section 11.1 I show that the curve sequence from Theorem 10.1 satisfies $s_1/s_2 \to 0$, so the construction from this section could have been simplified by only using the points of degree 2. In that case, the bound would be valid for all $\delta \in [0,(q-2)/(2(q-1))]$. However, I have here chosen to hold on to the points of degree 1 so as to show how it can be done. This is practical for other curve sequences where s_1/s_2 doesn't approach 0. (In constructions with other curve sequences we may of course need to change $q-1$ for some other value of $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i)$.) In the next chapter I stick to points of degree 2.

It is easy to verify that this bound is better than the TVZ bound for $\delta < \sqrt{q}/(q-1)$ when q is a square. We also know that the Gilbert–Varshamov bound is better than the TVZ bound for small δ. One could hope that there were some interval on the δ axis where this new bound was better than both the TVZ bound and the Gilbert–Varshamov bound. Sadly, as far as I know, this is not the case.

Lemma 10.5. *For prime powers $q \geq 4$ and $\delta = \sqrt{q}/(q-1)$, we have $1-2\delta-1/(q-1) < 1-H_q(\delta)$.*

Note that for $q \leq 3$, this value for δ lies outside of the interval where R_1 is defined.

Proof. We have $R_{\mathrm{GV}}(\sqrt{q}/(q-1)) > R_1(\sqrt{q}/(q-1))$ if and only if

$$1-\frac{\sqrt{q}}{q-1}\log_q(q-1)+\frac{\sqrt{q}}{q-1}\log_q\left(\frac{\sqrt{q}}{q-1}\right)+\frac{q-1-\sqrt{q}}{q-1}\log_q\left(\frac{q-1-\sqrt{q}}{q-1}\right) > 1-\frac{2\sqrt{q}+1}{q-1}$$

$$\Updownarrow$$

$$\sqrt{q}\log_q(q-1)-\sqrt{q}\log_q(\sqrt{q})+\sqrt{q}\log_q(q-1)-(q-1-\sqrt{q})\log_q(q-1-\sqrt{q}) + (q-1-\sqrt{q})\log_q(q-1) < 2\sqrt{q}+1$$

$$\Updownarrow$$

$$(q-1+\sqrt{q})\log_q(q-1)-(q-1-\sqrt{q})\log_q(q-1-\sqrt{q})-\frac{1}{2}\sqrt{q} < 2\sqrt{q}+1.$$

This is correct for $q = 4,5,7,8,9$. To show the last statement for larger q, it suffices to show that

$$(q-1+\sqrt{q})-(q-1-\sqrt{q})\log_q(q-1-\sqrt{q})-\frac{1}{2}\sqrt{q} < 2\sqrt{q}+1.$$

If $q \geq 11$, this last bit becomes

$$\log_q(q-1-\sqrt{q}) > \frac{q-2-\frac{3}{2}\sqrt{q}}{q-1-\sqrt{q}}.$$

Suppose $1+\sqrt{q} = \varepsilon q$ for some ε. It is then clear that $\varepsilon \to 0$ as $q \to \infty$. The above expression becomes

$$\log_q(1-\varepsilon)+1 > \frac{(1-\frac{3}{2}\varepsilon)q - \frac{1}{2}}{(1-\varepsilon)q}.$$

To ensure this, is it sufficient that

$$\log_q(1-\varepsilon)+1 > \frac{1-\frac{3}{2}\varepsilon}{1-\varepsilon},$$

which becomes

$$\log_q(1-\varepsilon) > \frac{\frac{1}{2}\varepsilon}{\varepsilon-1}. \tag{10.2}$$

Note that $\varepsilon < 1$ for all the q we are interested in. Also note that when $\varepsilon = 0$, we have equality in (10.2). This means that if $\frac{1}{2}\varepsilon/(\varepsilon-1)$ decreases more quickly as a function in ε (with q constant) between $\varepsilon = 0$ and $\varepsilon = 1$ than $\log_q(1-\varepsilon)$ does, then (10.2) is satisfied for all $q \geq 11$ and all ε between 0 and 1, and then especially for all $\varepsilon = (\sqrt{q}+1)/q$.

For $\varepsilon = 0$, it is easy to check that the slope is steepest on the right-hand side. Since the derivatives are continuous functions, I put the two derivatives equal to one another and check that we then can't have $0 \leq \varepsilon < 1$, thus proving the lemma. Using the assumption that $q \geq 11$, we have

$$\begin{aligned}
\frac{1}{(\varepsilon-1)\ln(q)} &= \frac{-\frac{1}{2}}{(\varepsilon-1)^2} \\
&\Updownarrow \\
\frac{1}{\ln(q)} &= \frac{-1}{2(\varepsilon-1)} \\
&\Updownarrow \\
2(\varepsilon-1) &= -\ln(q) \\
&\Updownarrow \\
\varepsilon &= \frac{-\ln(q)}{2}+1 < \frac{-\ln(e^2)}{2}+1 = 0.
\end{aligned}$$

This finishes the proof. □

What remains is to show that this is also the case to the left of $\delta = \sqrt{q}/(q-1)$, which is much more difficult. R_1 is worse than R_{GV} for all $0 \leq \delta \leq \sqrt{q}/(q-1)$ for all values of q I have tested, but I have yet to prove the inequalities for general q, as this involves solving second-degree logarithmic equations. I will here therefore only present what needs to be shown.

Let $\delta' := \sqrt{q}/(q-1)$. Consider the line

$$f(\delta) := 1 - \frac{1}{q-1} - \frac{1-\frac{1}{q-1} - R_{\mathrm{GV}}(\delta')}{\delta'}\delta.$$

We see that $f(\delta') = R_{\mathrm{GV}}(\delta')$ and that $f(0) = R_1(0)$. It follows that if R_{GV} has a steeper slope than f for every $\delta \in [0, \delta']$, then R_{GV} will never cross R_1 to the left of δ'. However, R_{GV} doesn't have a steeper slope in δ'. But we know that $R_1(\delta') < R_{\mathrm{GV}}(\delta')$, and since R_{GV} has positive second derivative, it is sufficient to show that when $R_1(\delta'') = R_{\mathrm{GV}}(\delta')$ for some $\delta'' < \delta'$, then $f(\delta'') < R_{\mathrm{GV}}(\delta'')$. This means that R_{GV} has grown more than f has between δ' and δ'', and R_{GV} becomes even steeper when we approach 0.

The value for δ'' is given by the equation

$$1 - 2\delta'' - \frac{1}{q-1} = 1 - H_q(\delta'),$$

which becomes

$$\delta'' = \frac{1}{2}H_q(\delta') - \frac{1}{2(q-1)}.$$

$f(\delta'') < R_{\mathrm{GV}}(\delta'')$ is the second-degree logarithmic expression which I have yet to prove.

Another possible approach is to find a δ''' that doesn't involve logarithms and that lies between δ'' and δ' and show that $f(\delta''') < R_{\mathrm{GV}}(\delta''')$. However, it has proved difficult to find such a δ'''.

10.2 The Second Construction

The second way to make infinite sequences of generalised AG codes is to use only one curve and let the degree of the points in question approach infinity. This is done by Antonino Spera in [9]. I here only briefly present what is done.

Let X be a curve and a be a positive integer such that $a^2 < q$. Then it is shown that for $n >> 0$, there exist $s_n := \lceil a^n\sqrt{q}^n \rceil$ points of degree n over $\mathbb{F}_q$. It follows that $q^n \geq s_n$. Let $C_1, \ldots, C_{s_n}$ be $[n, n, 1]_q$-linear codes and $\phi_i : \mathbb{F}_{q^n} \longrightarrow C_i$ be isomorphisms. For a given n, let the desired points of degree n be $P_1, \ldots, P_{s_n}$ and let G be a divisor with support disjoint from $\{P_1, \ldots, P_{s_n}\}$. Let η be an element of order $q^n - 1$ in the group $\mathbb{F}_{q^n}^{\times}$. Let $\psi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q^n$ de defined by $\psi : a_1 + a_2\eta + \cdots + a_n\eta^{n-1} \longmapsto (a_1, a_2, \ldots, a_n)$, and put $\xi := \psi(\eta)$. Then we have defined a field structure on $\mathbb{F}_q^n$, and it makes sence multiplying elements with each other in $\mathbb{F}_q^n$.

We now define $\phi : L(G) \longrightarrow \mathbb{F}_q^{2ns_n}$ by

$$f \longmapsto \left(\phi_1(f(P_1)), \phi_1(f(P_1)); \phi_2(f(P_2)), \xi\phi_2(f(P_2)); \ldots; \phi_{s_n}(f(P_{s_n})), \xi^{s_n-1}\phi_{s_n}(f(P_{s_n}))\right).$$

Note that since $q^n \geq s_n$, each ξ^i is different in the codewords. This ensures us that if $f(P_i) = f(P_j)$ for some f and some P_i and P_j, $i \neq j$, then we are guaranteed that $(\phi_i(f(P_i)), \xi^{i-1}\phi_i(f(P_i))) \neq (\phi_j(f(P_j)), \xi^{j-1}\phi_j(f(P_j)))$. Spera uses this fact to find a good bound for the minimum distance. When $n \to \infty$, he finds that for $q > 16$ and $0 < R < \frac{1}{2}$, we have

$$R \geq \frac{1}{2} - \delta.$$

10.3 The Third Construction

This construction is based on an obvious question: Suppose we have an infinite sequence of codes $(C_i(P_{1,i}, \ldots, P_{s_i,i}; G_i; C_{1,i}, \ldots, C_{s_i,i}))_{i=1}^{\infty}$ such that the lengths of $C_{1,i}, \ldots, C_{s_i,i}$ approach

infinity. If $C_{1,i}, \ldots, C_{s_i,i}$ have good asymptotic properties, will we obtain good asymptotic properties for $(C_i(P_{1,i}, \ldots, P_{s_i,i}; G_i; C_{1,i}, \ldots, C_{s_i,i}))_{i=1}^{\infty}$ as well? To give this a test, I have considered an infinite sequence of nonsingular projective curves $(X_i)_{i=1}^{\infty}$ defined over $\mathbb{F}_q$ which obtain the Drinfeld–Vlăduţ bound over $\mathbb{F}_q$, and for each such curve X_i, I have let $C_{1,i}, \ldots, C_{s_i,i}$ be codes defined in the proof of the TVZ bound, Corollary 5.9. Now, note that for each X_i, we are given the length n_i^{TVZ} of the codes $C_{1,i}, \ldots, C_{s_i,i}$, and that the length approaches infinity as $i \to \infty$. When that happens, the dimension k_i^{TVZ} approaches infinity as well (unless it is 0). The consequence is that we must also let the degree of the points $P_{1,i}, \ldots, P_{s_i,i}$ approach infinity as $i \to \infty$.

So suppose q is a square prime power and that we are given a sequence of nonsingular projective curves $(X_i)_{i=1}^{\infty}$ defined over $\mathbb{F}_q$ with $|X_i(\mathbb{F}_q)| \to \infty$ such that $|X_i(\mathbb{F}_q)|/g(X_i) \to \sqrt{q}-1$, where $g(X_i)$ is the genus of X_i. For each curve X_i, we first construct the codes $C_{1,i}, \ldots, C_{s_i,i}$. It is already decided from the construction of these codes in Corollary 5.9 that the length is to be $n_i^{\mathrm{TVZ}} = |X_i(\mathbb{F}_q)| - 1$. There is also defined a divisor $G_i^{\mathrm{TVZ}} = \lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor Q_i^{\mathrm{TVZ}}$, where Q_i^{TVZ} is a point of degree 1 on X_i and μ^{TVZ} is a constant satisfying $1/(\sqrt{q}-1) < \mu^{\mathrm{TVZ}} < 1$. Let the divisor

$$D_i^{\mathrm{TVZ}} = \sum_{P \in X_i(\mathbb{F}_q) \setminus \{Q_i^{\mathrm{TVZ}}\}} P.$$

We have then ensured that $\mathrm{Supp}(D_i^{\mathrm{TVZ}}) \cap \mathrm{Supp}(G_i^{\mathrm{TVZ}}) = \emptyset$, and so we can define $C_{j,i} = C(D_i^{\mathrm{TVZ}}, G_i^{\mathrm{TVZ}})$ for each j. As we did in the proof of the TVZ bound, we let each code $C_{j,i}$ have dimension $k_i^{\mathrm{TVZ}} := \deg(G_i^{\mathrm{TVZ}}) + 1 - g(X_i)$, if necessary by only considering a linear subspace of the code.

For all $i \geq 1$, define s_i to be the number of points on X_i of degree k_i^{TVZ}, but if $k_i^{\mathrm{TVZ}} = 1$, let $s_i = |X_i(\mathbb{F}_q)| - 1$ (to ensure that we have a spare point Q_i of degree 1 for our "main" divisor G_i), and let $P_{1,i}, \ldots, P_{s_i,i}$ be those points. For some μ such that $0 < \mu < 1$, let $G_i = \lfloor \mu n_i \rfloor Q_i$, where n_i is the length of the code $C_i(P_{1,i}, \ldots, P_{s_i,i}; G_i; C_{1,i}, \ldots, C_{s_i,i})$ and Q_i is a point of degree 1 on X_i not among $P_{1,i}, \ldots, P_{s_i,i}$, even though they might be of degree 1. It is clear that $n_i = s_i n_i^{\mathrm{TVZ}}$.

For the time being, assume that we always have $g(X_i) \leq \deg(G_i) < s_i k_i^{\mathrm{TVZ}}$. Then the conditions in Proposition 9.5 are satisfied. In the end of this section, I will prove that these are met.

A code $C_i(P_{1,i}, \ldots, P_{s_i,i}; G_i; C_{1,i}, \ldots, C_{s_i,i})$ has the dimension $k_i = l(G_i)$. On the other hand, we are allowed to choose a linear subspace of the code such that the dimension is

$$k_i := \deg(G_i) + 1 - g(X_i).$$

Before continuing, we need a small lemma.

Lemma 10.6. *If $\mu^{\mathrm{TVZ}} > 1/(\sqrt{q}-1)$, then*

$$\lim_{i \to \infty} \frac{g(X_i)}{s_i n_i^{\mathrm{TVZ}}} = 0.$$

Proof. Since $\lim_{i\to\infty} g(X_i)/n_i^{\mathrm{TVZ}} = 1/(\sqrt{q}-1)$, we only need to show that $\lim_{i\to\infty} s_i = \infty$.

From the proof of Lemma 3.1 of [9], we have that if

$$\frac{\sqrt{q}^{k_i^{\mathrm{TVZ}}}}{k_i^{\mathrm{TVZ}}} \geq 1 + \frac{2 + 7g(X_i)}{k_i^{\mathrm{TVZ}}}, \tag{10.3}$$

then $s_i \geq \sqrt{q}^{k_i^{\mathrm{TVZ}}}$, which will imply that $s_i \to \infty$ since $k_i^{\mathrm{TVZ}} \to \infty$.

The left-hand side of (10.3) obviously approaches infinity, so it suffices to show that the right-hand side remains constant. We first calculate $\lim_{i\to\infty} g(X_i)/k_i^{\mathrm{TVZ}}$:

$$\lim_{i\to\infty} \frac{g(X_i)}{k_i^{\mathrm{TVZ}}} = \lim_{i\to\infty} \left(\frac{\deg(G_i^{\mathrm{TVZ}})}{g(X_i)} - 1 \right)^{-1} = \left(\mu^{\mathrm{TVZ}}(\sqrt{q}-1) - 1 \right)^{-1}.$$

The right-hand side thus approaches

$$1 + \frac{7}{\mu^{\mathrm{TVZ}}(\sqrt{q}-1) - 1}$$

as $i \to \infty$. Since μ^{TVZ} was assumed to be strictly greater than $1/(\sqrt{q}-1)$, this proves the lemma. □

From Proposition 9.5, we have

$$\begin{aligned} d_i &\geq d_i^{\mathrm{TVZ}} \left(s_i - \left\lfloor \frac{\deg(G_i)}{k_i^{\mathrm{TVZ}}} \right\rfloor \right) \\ &= d_i^{\mathrm{TVZ}} \left(s_i - \left\lfloor \frac{\deg(G_i)}{\deg(G_i^{\mathrm{TVZ}}) + 1 - g(X_i)} \right\rfloor \right) \\ &\geq d_i^{\mathrm{TVZ}} \left(s_i - \frac{\deg(G_i)}{\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)} \right). \end{aligned}$$

Putting $\deg(G_i)$ on the left-hand side of the expression, we get

$$\deg(G_i) \geq \left(d_i^{\mathrm{TVZ}} s_i - d_i \right) \left(\frac{\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)}{d_i^{\mathrm{TVZ}}} \right). \tag{10.4}$$

We substitute in the expression for k_i and get

$$\begin{aligned} k_i &= \deg(G_i) + 1 - g(X_i) \\ &\geq s_i \left(\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i) \right) - d_i \left(\frac{\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)}{d_i^{\mathrm{TVZ}}} \right) + 1 - g(X_i) \\ &\geq s_i \left(\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i) \right) - d_i \left(\frac{\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)}{n_i^{\mathrm{TVZ}} - \deg(G_i^{\mathrm{TVZ}})} \right) + 1 - g(X_i) \\ &= s_i \left(\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i) \right) - d_i \left(\frac{\lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)}{n_i^{\mathrm{TVZ}} - \lfloor \mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}} \rfloor} \right) + 1 - g(X_i). \end{aligned}$$

The length of $C_i(P_{1,i}, \ldots, P_{s_i,i}; G_i; C_{1,i}, \ldots, C_{s_i,i})$ is $s_i n_i^{\mathrm{TVZ}}$, so we divide by $s_i n_i^{\mathrm{TVZ}}$ and let $i \to \infty$. We have that $g(X_i)/(s_i n_i^{\mathrm{TVZ}}) \to 0$ from Lemma 10.6. The rest of the expression becomes

$$R \geq \mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1} - \delta \left(\frac{\mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1}}{1 - \mu^{\mathrm{TVZ}}} \right). \tag{10.5}$$

Now two obvious questions arise: What values of μ^{TVZ} are we allowed to use, and for what value is R greatest with respect to δ? In the following, I will do things a bit backwards (making calculations a bit simpler). I will first find the value for μ^{TVZ} that makes R greatest and afterwards show that this is a "valid" value for μ^{TVZ}.

Lemma 10.7. *The value for μ^{TVZ} that makes (10.5) the greatest is*

$$\mu^{\mathrm{TVZ}} = 1 - \sqrt{\frac{\delta(\sqrt{q}-2)}{\sqrt{q}-1}}.$$

This function of δ I will denote by ξ.

Proof. I differentiate (10.5) with respect to μ^{TVZ} and find what value of μ^{TVZ} makes the derivative of (10.5) equal to 0.

$$\frac{\mathrm{d}}{\mathrm{d}\mu^{\mathrm{TVZ}}}\left(\mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1} - \delta\left(\frac{\mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1}}{1-\mu^{\mathrm{TVZ}}}\right)\right)$$
$$= 1 - \delta\left(\frac{1\cdot\left(1-\mu^{\mathrm{TVZ}}\right) - \left(\mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1}\right)\cdot(-1)}{\left(1-\mu^{\mathrm{TVZ}}\right)^2}\right).$$

We put the expression on the right-hand side equal to 0 and get:

$$\begin{aligned}
\delta\cdot\frac{(1-\mu^{\mathrm{TVZ}}) + \mu^{\mathrm{TVZ}} - \frac{1}{\sqrt{q}-1}}{\left(1-\mu^{\mathrm{TVZ}}\right)^2} &= 1\\
\delta\cdot\frac{\sqrt{q}-1-1}{\left(\sqrt{q}-1\right)\left(1-\mu^{\mathrm{TVZ}}\right)^2} &= 1\\
\left(\sqrt{q}-1\right)\left(1-\mu^{\mathrm{TVZ}}\right)^2 &= \delta\left(\sqrt{q}-2\right)\\
1-\mu^{\mathrm{TVZ}} &= \sqrt{\frac{\delta\left(\sqrt{q}-2\right)}{\left(\sqrt{q}-1\right)}}.
\end{aligned}$$

□

There are two things we now have to check. First of all, we need to find out for what values of δ we have $\xi \in \left(1/\left(\sqrt{q}-1\right), 1\right)$. Secondly, we must show that the conditions in Proposition 9.5 are kept.

Lemma 10.8. *For $q \geq 3^2$ and $0 < \delta < \left(\sqrt{q}-2\right)/\left(\sqrt{q}-1\right)$, we have*

$$\frac{1}{\sqrt{q}-1} < \xi < 1.$$

Proof. It is clear that $\xi < 1$ for any $\delta > 0$. To find out when $1/(\sqrt{q}-1) < \xi$, we have

$$\begin{aligned}
1 - \left(\frac{\sqrt{(\sqrt{q}-2)}}{\sqrt{(\sqrt{q}-1)}}\right)\sqrt{\delta} - \frac{1}{\sqrt{q}-1} &> 0\\
&\Updownarrow\\
\frac{\left(1-\frac{1}{\sqrt{q}-1}\right)^2\left(\sqrt{q}-1\right)}{\sqrt{q}-2} &> \delta\\
&\Updownarrow\\
\frac{\left(1-\frac{2}{\sqrt{q}-1}+\frac{1}{\left(\sqrt{q}-1\right)^2}\right)\left(\sqrt{q}-1\right)}{\left(\sqrt{q}-2\right)} &> \delta
\end{aligned}$$

$$\begin{array}{rcl} & \Updownarrow & \\ \dfrac{\left(\sqrt{q}-1\right)^2-2\left(\sqrt{q}-1\right)+1}{\left(\sqrt{q}-2\right)\left(\sqrt{q}-1\right)} & > & \delta \\ & \Updownarrow & \\ \dfrac{\left(q-4\sqrt{q}+4\right)}{\left(\sqrt{q}-2\right)\left(\sqrt{q}-1\right)} & > & \delta \\ & \Updownarrow & \\ \dfrac{\sqrt{q}-2}{\sqrt{q}-1} & > & \delta, \end{array}$$

as desired. □

Lemma 10.9. *Let $q \geq 3^2$ be a prime power. The expression*

$$(1-\xi(\delta)-\delta)\left(\frac{\xi(\delta)-\frac{1}{\sqrt{q}-1}}{1-\xi(\delta)}\right)$$

is strictly decreasing as a function in δ in the interval $(0,(\sqrt{q}-2)/(\sqrt{q}-1))$.

Proof. This can very quickly be done in Maple. Differentiate the function with respect to δ (with q just a symbol) and note that the derivative is a continuous function in the interval $(0,(\sqrt{q}-2)/(\sqrt{q}-1))$. Let $\delta = 0.1$ and find out for which q the derivative is negative. Maple gives the answer $q \in [0,1) \cup (4.46,\infty)$, and in particular all $q \geq 3^2$. Now find out for which δ the derivative is 0. Put that value of δ equal to δ' and find out for which q we have $\delta' \geq (\sqrt{q}-2)/(\sqrt{q}-1)$. The answer is $q \in [0,1) \cup (1,4) \cup (4,\infty)$, and in particular all $q \geq 3^2$. □

Lemma 10.10. *When $\mu^{\mathrm{TVZ}} = \xi$ in (10.5), the conditions in Proposition 9.5 are met for all $\delta \in (0,(\sqrt{q}-2)/(\sqrt{q}-1))$ for large enough i.*

Proof. The condition that $g(X_i) \leq \deg(G_i)$ is simply the condition that the dimension of the code is nonzero, since k_i is given by $\deg(G_i)+1-g(X_i)$.

Next we must show that $\deg(G_i) < s_i k_i^{\mathrm{TVZ}}$ when $\mu^{\mathrm{TVZ}} = \xi$. This is the same as showing

$$\begin{array}{rcl} \lfloor \mu s_i n_i^{\mathrm{TVZ}} \rfloor & < & s_i \left(\deg(G_i^{\mathrm{TVZ}}) + 1 - g(X_i)\right), \\ \lfloor \mu s_i n_i^{\mathrm{TVZ}} \rfloor & < & s_i \left(\lfloor \xi n_i^{\mathrm{TVZ}} \rfloor + 1 - g(X_i)\right). \end{array}$$

Dividing both sides by $s_i n_i^{\mathrm{TVZ}}$ and letting $i \to \infty$, we get

$$\mu < \xi - \frac{1}{\sqrt{q}-1},$$

which is what we want to show.

Now consider (10.4). Substitute $\mu s_i n_i^{\mathrm{TVZ}}$ for $\deg(G_i)$, substitute $n_i^{\mathrm{TVZ}} - \deg(G_i^{\mathrm{TVZ}})$ for d_i^{TVZ}, substitute $\mu^{\mathrm{TVZ}} n_i^{\mathrm{TVZ}}$ for $\deg(G_i^{\mathrm{TVZ}})$, substitute $\xi(\delta)$ for μ^{TVZ}, divide by $s_i n_i^{\mathrm{TVZ}}$ on both sides, and let $i \to \infty$. We then obtain the following:

$$\mu \geq (1-\xi(\delta)-\delta)\left(\frac{\xi(\delta)-\frac{1}{\sqrt{q}-1}}{1-\xi(\delta)}\right).$$

In the previous lemma we showed that the expression on the right-hand side above is strictly decreasing with respect to δ in the interval $(0, (\sqrt{q}-2)/(\sqrt{q}-1))$. It is therefore possible to choose (formally) $\delta' \leq \delta$ such that we get

$$\mu = \left(1 - \xi(\delta') - \delta'\right)\left(\frac{\xi(\delta') - \frac{1}{\sqrt{q}-1}}{1-\xi(\delta')}\right).$$

We want to show that

$$\left(1 - \xi\left(\delta'\right) - \delta'\right)\left(\frac{\xi\left(\delta'\right) - \frac{1}{\sqrt{q}-1}}{1-\xi\left(\delta'\right)}\right) < \xi\left(\delta'\right) - \frac{1}{\sqrt{q}-1}.$$

We get

$$\left(1 - \xi\left(\delta'\right) - \delta'\right)\left(\xi\left(\delta'\right) - \frac{1}{\sqrt{q}-1}\right) < \left(\xi\left(\delta'\right) - \frac{1}{\sqrt{q}-1}\right)\left(1 - \xi\left(\delta'\right)\right)$$

$$\Updownarrow$$

$$-\left(\xi\left(\delta'\right)\right)^2 + \left(1 - \delta' + \frac{1}{\sqrt{q}-1}\right)\xi\left(\delta'\right) + \left(-\frac{1}{\sqrt{q}-1} + \frac{\delta'}{\sqrt{q}-1}\right) < -\left(\xi\left(\delta'\right)\right)^2 + \left(1 + \frac{1}{\sqrt{q}-1}\right)\xi\left(\delta'\right) - \frac{1}{\sqrt{q}-1}$$

$$\Updownarrow$$

$$-\delta'\xi\left(\delta'\right) + \frac{\delta'}{\sqrt{q}-1} < 0,$$

which means that $\xi\left(\delta'\right) > 1/(\sqrt{q}-1)$ if and only if $\deg(G_i) < s_i k_i^{\mathrm{TVZ}}$ for large enough i and where $\delta \geq \delta'$, and so the result follows from Lemma 10.8. □

This finishes the proof that all requirements are held in the construction of (10.5) for $\mu^{\mathrm{TVZ}} = \xi$, and so we have the following theorem:

Theorem 10.11. *For any square prime power $q \geq 3^2$ and $0 < \delta < (\sqrt{q}-2)/(\sqrt{q}-1)$, there exists an infinite sequence of generalised AG codes $(C_i)_{i=1}^{\infty}$ with minimum distances d_i, dimensions k_i, and lengths n_i such that $d_i/n_i \to \delta$ and $k_i/n_i \to R$ satisfying*

$$R \geq R_3 := \xi - \frac{1}{\sqrt{q}-1} - \delta\left(\frac{\xi - \frac{1}{\sqrt{q}-1}}{1-\xi}\right),$$

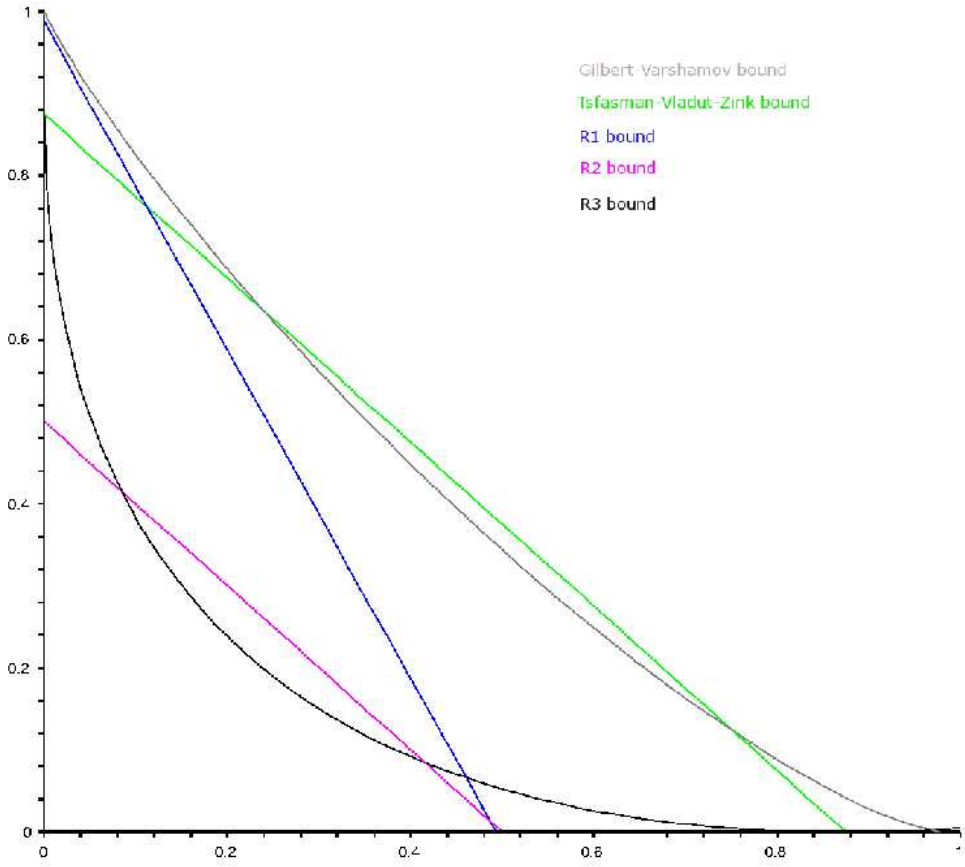
where

$$\xi = 1 - \sqrt{\frac{\delta\left(\sqrt{q}-2\right)}{\sqrt{q}-1}}.$$

However, this does not exceed the TVZ bound.

Remark 10.12. There is another formula for the minimum distance d_i, where we must consider separate cases when $d_i^{\mathrm{TVZ}} \leq k_i^{\mathrm{TVZ}}$ and $d_i^{\mathrm{TVZ}} > k_i^{\mathrm{TVZ}}$. When $d_i^{\mathrm{TVZ}} \leq k_i^{\mathrm{TVZ}}$, Corollary 3.3 in [20] tells us that $d_i \geq s_i d_i^{\mathrm{TVZ}} - \deg(G_i)$. When $d_i^{\mathrm{TVZ}} > k_i^{\mathrm{TVZ}}$, we get from Theorem 3.2 in [20] that $d_i \geq s_i k_i^{\mathrm{TVZ}} - \deg(G_i)$.

On the next page we have a figure showing some of the different bounds we have encountered so far for $q = 81$.


Gilbert-Varshamov bound
Tsfasman-Vladut-Zink bound
R1 bound
R2 bound
R3 bound
1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8

Chapter 11

Improvements of R_1

In this chapter I attempt to improve R_1 around the area where it is closest to the Gilbert–Varshamov bound. Since the construction of generalised AG codes is done in a similar way to that of Goppa codes, I will use methods taken from improvements that have been made on Goppa codes.

In this chapter, all curves will be assumed to be nonsingular projective curves, and all divisors will be assumed to be $\mathbb{F}_q$-rational divisors. The divisor-class number of a curve X will be denoted by $h(X)$, and its genus will be denoted by $g(X)$.

11.1 The First Improvement

In [15] Chaoping Xing finds good divisors G for Goppa codes $C(D, G)$ such that the minimum distance is improved. The method he uses is the same as in Section 4.3, only that the evaluation of $M_{t,l}$ is a bit simpler in [15]. Here he finds an upper bound of $M_{t,l}$ (or $N_{s,m}$, which it is called here) and finds out when it is strictly less than the divisor-class number $h(X)$. He then finds an asymptotic improvement of the Tsfasman–Vlăduţ–Zink and Gilbert–Varshamov bounds.

I here show that the same method can be used to improve R_1. In the following construction I will use the curve sequence $(X_i)_{i=1}^{\infty}$ mentioned in Theorem 10.1, which satisfies $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i) = q - 1$ and is also defined over $\mathbb{F}_q$. Before continuing, we need the following proposition.

Proposition 11.1. *For the curve sequence presented in Theorem 10.1, we have*

$$\lim_{i\to\infty} \frac{|X_i(\mathbb{F}_q)|}{g(X_i)} = 0.$$

Proof. Let the function field $\mathbb{F}_{q^2}(X_i)$ be denoted by $\mathbb{F}_{q^2}(x_1, \ldots, x_i)$, with each x_j satisfying

$$x_j^q + x_j = \frac{x_{j-1}^q}{x_{j-1}^{q-1} + 1}, \quad j \geq 2.$$

Let Ω^{∞} be the set consisting of $\mathbb{F}_{q^2}$-rational points on X_1 satisfying $x_1^q + x_1 = 0$ and $x_1 = \infty$. In [4] it is shown that for $i \geq 2$, the set of points on X_i *not* lying over the points of Ω^{∞} has cardinality N_i satisfying $\lim_{i\to\infty} N_i/g(X_i) = q - 1$. Hence, if some of the points on X_i lying over Ω^{∞} should have cardinality M_i satisfying $\lim_{i\to\infty} M_i/g(X_i) = A > 0$, the number

$\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i)$ would exceed the Drinfeld–Vlăduţ bound, a contradiction. It follows that $\lim_{i\to\infty} M_i/g(X_i) = 0$.

I now show that for each $\mathbb{F}_q$-rational point $(x_1, \ldots, x_i)$ with $x_i = a$ on X_i, there is only one $\mathbb{F}_q$-rational point $(x_1, \ldots, x_{i+1})$ with $x_{i+1} = b$ on X_{i+1} lying over $x_i = a$.

First suppose $\mathbb{F}_q$ is of characteristic $p \neq 2$. Suppose $x_{i+1} = b \in \mathbb{F}_q$ and let $x_i = a \in \mathbb{F}_q$. We then have

$$b^q + b = \frac{a^q}{a^{q-1} + 1},$$

which becomes

$$b + b = \frac{a}{1 + 1},$$

which becomes $b = a/4$. Since a point $(x'_1, \ldots, x'_i)$ on X_i is $\mathbb{F}_q$-rational only if each x'_j is $\mathbb{F}_q$-rational, it follows that—disregarding points lying over the elements of Ω^∞—there are fewer $\mathbb{F}_q$-rational points on X_i than the total number of $\mathbb{F}_q$-rational points on X_1.

Now suppose $\mathbb{F}_q$ is of characteristic 2. Then if $x_1 = a \in \mathbb{F}_q$, then $x_1^q + x_1 = x_1 + x_1 = 0$, and so $x_1 = a$ belongs to the set Ω^∞, and we have previously argued that the points lying over Ω^∞ give no contribution to $\lim_{i\to\infty} |X_i(\mathbb{F}_q)|/g(X_i)$.

It follows that there is a maximum of $q - 1$ $\mathbb{F}_q$-rational points on each X_i that could possibly give any contribution to $\lim_{i\to\infty} |X_i(\mathbb{F}_q)|/g(X_i)$, and since $\lim_{i\to\infty} g(X_i) = \infty$, we can conclude that $\lim_{i\to\infty} |X_i(\mathbb{F}_q)|/g(X_i) = 0$, as desired. □

Corollary 11.2. *Let the curve sequence $(X_i)_{i=1}^\infty$ be as in Theorem 10.1. If $r_i^{(j)}$ is the number of closed points of degree j on X_i over $\mathbb{F}_q$, then*

$$\lim_{i\to\infty} \frac{r_i^{(1)}}{r_i^{(2)}} = 0.$$

Proof. This follows from the previous proposition and Proposition 10.2. □

A consequence of this is that we only need to consider points of degree 2 for the rest of this section.

Lemma 11.3. *Let X be a curve over $\mathbb{F}_q$ with genus $g(X)$ and at least one $\mathbb{F}_q$-rational point. Let S be a set of divisors of degree s with $s \geq g(X)$. If $|S| < h(X)$, then there exists an effective divisor H of degree s such that H is not equivalent to any divisors in S.*

Proof. This was proved in Lemma 4.19. □

Suppose we have r closed points of degree 2 on X denoted by $P_1, \ldots, P_r$. Let s and m be integers such that $s \geq m$ and m is even. Denote

$$S_{s,m}(P_1, \ldots, P_r) := \left\{ \sum_{P\in I} P + D \,|\, I \subseteq \{P_1, \ldots, P_r\}, \sum_{P\in I} \deg(P) = m, \right.$$
$$\left. D \text{ is an effective divisor of degree } s - m \right\}$$

and $N_{s,m} := |S_{s,m}|$.

Proposition 11.4. *Let X be a projective nonsingular curve with genus $g(X)$, $P_1, \ldots, P_r$ defined as above, s, m positive integers with m even such that $m \leq \min\{s, 2r\}$ and $s \geq g(X)$. Let $C_1, \ldots, C_r$ be $[2, 2, 1]_q$-linear codes. If $N_{s,m} < h(X)$, then there exists a divisor G of degree s such that $\mathrm{Supp}(G) \cap \{P_1, \ldots, P_r\} = \emptyset$ and $C(P_1, \ldots, P_r; G; C_1, \ldots, C_r)$ is an $[n, k, d]_q$-linear code with*

$$k \geq s - g(X) + 1, \qquad d \geq r - \frac{1}{2}m + 1.$$

Proof. Since $N_{s,m} < h(X)$, there exists an effective divisor H of degree s such that H is not equivalent to any divisors in $S_{s,m}$. I claim that

$$L\left(H - \sum_{P \in I} P\right) = \{0\}$$

for any subset $I \subseteq \{P_1, \ldots, P_r\}$ satisfying $\sum_{P \in I} \deg(P) = m$.

If $0 \neq f \in L(H - \sum_{P \in I_0} P)$ for some I_0 satisfying the above, then $\mathrm{div}(f) + H - \sum_{P \in I_0} P \succ 0$. Put $D = \mathrm{div}(f) + H - \sum_{P \in I_0} P$. Then D is effective of degree $s - m$, and so H is equivalent to $D + \sum_{P \in I_0}$, a contradiction.

Since $\{P_1, \ldots, P_r\}$ is a proper subset of all closed points on X of degree $1, 2, 3, \ldots$, then according to the Strong Approximation Theorem, Theorem 4.20, there exists an $\mathbb{F}_q$-rational function t_i for each $i = 1, \ldots, r$ such that

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

Define

$$G := H + \mathrm{div}\left(\prod_{i=1}^{r} t_i^{-v_{P_i}(H)}\right).$$

We have $\mathrm{Supp}(G) \cap \{P_1, \ldots, P_r\} = \emptyset$ and $G \equiv H$, so

$$L\left(G - \sum_{P \in I} P\right) = \{0\}$$

for any $I \subseteq \{P_1, \ldots, P_r\}$ satisfying $\sum_{P \in I} \deg(P) = m$. Suppose $0 \neq f \in L(G)$ has zeros in all the points of a subset $\{P_{i_1}, \ldots, P_{i_l}\} \subseteq \{P_1, \ldots, P_r\}$. Then $f \in L(G - P_{i_1} - \cdots - P_{i_l})$, and so $\sum_{j=1}^{l} \deg(P_{i_j}) \leq m - 2$. (The sum of the degrees can't be $m - 1$ since they all are even.) From the conditions we put in this proposition, it follows that $l < r$, and so the mapping is injective, in which follows $k = l(G) \geq s - g(X) + 1$.

To find the minimum distance, define

$$Z = \left\{ T \subseteq \{1, \ldots, r\} \;\middle|\; \sum_{i \in T} \deg(P_i) \leq m - 2 \right\}$$

and $\nu = \min\{r - \mathrm{card}(T) \,|\, T \in Z\}$. For a nonzero $f \in L(G)$, let

$$T = \{i \in \{1, \ldots, r\} \,|\, f(P_i) = 0\}.$$

Since $0 \neq f \in L(G - \sum_{i \in S} P_i)$, we have $\sum_{i \in S} \deg(P_i) \leq m - 2$, so $T \in Z$.

From the end of the proof of Proposition 9.5, we now have that the minimum distance is at least ν. This is easily reformulated as

$$d \geq r - \frac{1}{2}m + 1,$$

as desired. □

Let A_l be the number of effective divisors of degree l. An upper bound for $N_{s,m}$ is then

$$N_{s,m} \leq \binom{r}{m/2} A_{s-m}. \tag{11.1}$$

So if we can show that the right-hand side of (11.1) is strictly less than $h(X)$ for some parameters s, m satisfying m even, $m \leq \min\{s, 2r\}$, and $s \geq g(X)$, then all the conditions of Proposition 11.4 are satisfied.

Before presenting the asymptotic results for generalised AG codes satisfying these conditions, we need some lemmas. In the following, I will consider the sequence of curves $(X_i)_{i=1}^{\infty}$ presented in Theorem 10.1. The number of closed points of degree 2 of X_i is denoted by r_i. Recall that $\lim_{i\to\infty} |X_i(\mathbb{F}_{q^2})|/g(X_i) = q - 1$.

In the following, we will let the binary entropy function be defined as

$$H_2(\delta) := -\delta \log_2(\delta) - (1-\delta)\log_2(1-\delta), \qquad 0 < \delta < 1,$$

$$H_2(0) := H_2(1) := 0.$$

The following lemma follows from Stirling's formula.

Lemma 11.5. *Let n be a positive integer and $0 \leq \delta \leq 1$ a real number such that δn is an integer. Then*

$$\binom{n}{\delta n} \leq 2^{nH_2(\delta)}.$$

The following result gives an upper bound on (11.1).

Lemma 11.6. *For each i, let $m_i = 2r_i - 2d_i$, where d_i are nonnegative integers such that $d_i/(2r_i) \to \delta$ as $i \to \infty$, $0 \leq \delta \leq 1$. Then*

$$\lim_{i\to\infty} \frac{\log_q \binom{r_i}{m_i/2}}{g(X_i)} \leq \frac{q-1}{2} H_2(2\delta)\log_q(2).$$

Proof. Since $m_i/2 = r_i - d_i$, the previous lemma gives us

$$\binom{r_i}{m_i/2} = \binom{r_i}{d_i} \leq 2^{r_i H_2(2\delta)}.$$

Hence,

$$\lim_{i\to\infty} \frac{\log_q \binom{r_i}{m_i/2}}{g(X_i)} \leq \lim_{i\to\infty} \frac{\log_q \left(2^{r_i H_2(2\delta)}\right)}{g(X_i)} = \lim_{i\to\infty} \frac{r_i H_2(2\delta)\log_q(2)}{g(X_i)} = \frac{q-1}{2} H_2(2\delta)\log_q(2).$$

□

Proposition 11.7. *Let σ satisfy $0 < \sigma < 2/(\sqrt{q}+1)$. Then*

$$\limsup_{i\to\infty} \frac{\log_q\left(A_{\lfloor \sigma g(X_i)\rfloor}(X_i)\right)}{g(X_i)} \leq \frac{\sigma}{2} + 2H_2\left(\frac{\sigma}{2}\right)\log_q(2).$$

Proof. See Poposition 3.4 in [15]. □

Proposition 11.8. *We have*

$$\liminf_{i\to\infty} \frac{\log_q(h(X_i))}{g(X_i)} \geq 2\log_q\left(\sqrt{q}-1\right).$$

Proof. This follows easily from Theorem 2.3.15, page 177 in [13]. □

Define the function

$$f_q(x) = \frac{x}{2} + 2H_2\left(\frac{x}{2}\right)\log_q(2).$$

f_q is continuous and strictly increasing on $[0,1]$, so its inverse exists. Since $f_q(1) = 1/2 + 2\log_q(2)$, then for any real number $u \in [0, 1/2 + 2\log_q(2)]$, there exists a unique solution to $f_q(x) = u$.

Note that the positive number $2/(\sqrt{q}+1) < 1/2 + 2\log_q(2)$ for all prime powers q. This can easily enough be checked for all $2 \leq q \leq 8$. For $q \geq 9$, we see that $2/(\sqrt{q}+1) \leq 1/2$ while $1/2 + 2\log_q(2) > 1/2$.

Define the function

$$h_q(y) = \begin{cases} f_q^{-1}(y) & \text{if } 0 < y < 2/(\sqrt{q}-1), \\ 0 & \text{otherwise.} \end{cases}$$

Note that $h_q(y)$ is continuous in the interval $(0, 2/(\sqrt{q}-1))$. It can easily be shown that when $0 < y < 2/(\sqrt{q}-1)$, then also $0 < h_q(y) < 2/(\sqrt{q}-1)$.

Theorem 11.9. *Suppose q is a prime power and $0 \leq \delta \leq (q-2)/(2(q-1))$. With notations as above, there exists an infinite sequence of generalised AG codes $(C_i)_{i=1}^{\infty}$ with minimum distances d_i, dimensions k_i, and lengths n_i such that $d_i/n_i \to \delta$ and $k_i/n_i \to R$ satisfying*

$$R \geq R_4 := 1 - 2\delta - \frac{1}{q-1} + \frac{1}{q-1} h_q\left(2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2}H_2(2\delta)\log_q(2)\right).$$

Proof. Fix $\delta \in [0, (q-2)/(2(q-1))]$. If $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2) \notin (0, 2/(\sqrt{q}+1))$, this is the same bound as R_1 from Section 10.1. (See Remark 10.4 about for which δ the bound is valid.)

Now suppose $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2) \in (0, 2/(\sqrt{q}+1))$. Choose $\varepsilon > 0$ small enough such that $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2) - \varepsilon \in (0, 2/(\sqrt{q}+1))$ and choose σ such that

$$f_q(\sigma) = 2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2}H_2(2\delta)\log_q(2) - \varepsilon.$$

Then

$$\sigma = h_q\left(2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2}H_2(2\delta)\log_q(2) - \varepsilon\right).$$

Since $0 < y < 2/(\sqrt{q}-1)$ implies that $0 < h_q(y) < 2/(\sqrt{q}-1)$, we now have that $0 < \sigma < 2/(\sqrt{q}-1)$. Let the sequence of curves $(X_i)_{i=1}^{\infty}$ be as in Theorem 10.1, and let all notations be

as previously in this section. For each i, put $m_i = 2r_i - 2d_i'$ where the d_i' are chosen such that $\lim_{i\to\infty} d_i'/(2r_i) = \delta$. Then m_i is even and $\lim_{i\to\infty} m_i/(2r_i) = 1-2\delta$. Let $s_i = m_i + \lfloor \sigma g(X_i) \rfloor$. Then $(s_i - m_i)/g(X_i) \to \sigma$.

We want to show that

$$\lim_{i\to\infty} \frac{\log_q(N_{s_i,m_i})}{g(X_i)} < \lim_{i\to\infty} \frac{\log_q(h(X_i))}{g(X_i)}. \tag{11.2}$$

On the right-hand side, we have according to Proposition 11.8 that a lower bound is

$$2\log_q(\sqrt{q}-1) \le \lim_{i\to\infty} \frac{\log_q(h(X_i))}{g(X_i)}.$$

On the left-hand side of (11.2), we combine (11.1) with Lemma 11.6 and Proposition 11.7, using the facts that $(s_i - m_i)/g(X_i) \to \sigma$ and $0 < \sigma < 2/(\sqrt{q}-1)$, and get

$$\lim_{i\to\infty} \frac{\log_q(N_{s_i,m_i})}{g(X_i)} \le \frac{q-1}{2} H_2(2\delta)\log_q(2) + \frac{\sigma}{2} + 2H_2\left(\frac{\sigma}{2}\right)\log_q(2).$$

From the definition of f_q, we have $\sigma/2 + 2H_2(\sigma/2)\log_q(2) = f_q(\sigma) = 2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2) - \varepsilon$, and so the above becomes

$$\lim_{i\to\infty} \frac{\log_q(N_{s_i,m_i})}{g(X_i)} \le 2\log_q(\sqrt{q}-1) - \varepsilon.$$

So $N_{s,m} < h(X)$ for $i >> 0$. In addition, we obviously have $m_i \le 2r_i$ and $m_i \le s_i$. It follows that there exists for each $i >> 0$ a generalised AG code C_i with parameters

$$k_i \ge s_i - g(X_i) + 1, \qquad d_i \ge r_i - \frac{1}{2}m_i + 1.$$

The asymptotic parameters are

$$\liminf_{i\to\infty} \frac{d_i}{2r_i} \ge \lim_{i\to\infty}\left(\frac{1}{2} - \frac{1}{2}\cdot\frac{m_i}{2r_i}\right) = \lim_{i\to\infty}\left(\frac{1}{2} - \frac{1}{2}\cdot\frac{2r_i - 2d_i'}{2r_i}\right) = \delta$$

and

$$\begin{aligned}
\liminf_{i\to\infty} \frac{k_i}{2r_i} &\ge \lim_{i\to\infty} \frac{m_i - g(X_i) + (s_i - m_i) + 1}{2r_i} \\
&= \lim_{i\to\infty} \frac{2r_i - 2d_i'}{2r_i} - \frac{1}{q-1} + \frac{\sigma}{q-1} \\
&= 1 - 2\delta - \frac{1}{q-1} + \frac{1}{q-1} h_q\left(2log_q(\sqrt{q}-1) - \frac{q-1}{2}H_2(2\delta)\log_q(2) - \varepsilon\right).
\end{aligned}$$

Letting $\varepsilon \to 0$, we get the desired result. □

The following proposition shows that R_4 is an improvement of R_1 for some nonempty subinterval of $[0, 1/4]$ for each prime power $q \ge 5$. We use the fact that $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2)$ is continuous and show that when δ varies between 0 and 1/4, then $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2)$ will vary from something negative to something positive if $q \ge 5$. If $q \ge 8$, then we actually get $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2) > 2/(\sqrt{q}-1)$ for $\delta = 1/4$. It then follows that $h_q(2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta)\log_q(2))$ is nonzero and positive for some subinterval of $[0, 1/4]$.

Proposition 11.10. *Let $q \geq 5$ be a prime power. Then*

$$2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2} H_2\left(2 \cdot \frac{1}{4}\right) \log_q(2) < 0 \quad \textit{and} \quad 2log_q\left(\sqrt{q}-1\right) > 0.$$

If $q \geq 8$, we have

$$2log_q\left(\sqrt{q}-1\right) > \frac{2}{\sqrt{q}-1}.$$

Proof. The only bit we need to show is that $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2 \cdot \frac{1}{4}) \log_q(2) < 0$. Since $H_2(\frac{1}{2}) = 1$, we must show that $2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1) \log_q(2) < 0$. For $q = 5$, this is true.

Suppose $q \geq 7$. It is then sufficient to show that $2 \log_q(\sqrt{q}) - \frac{1}{2}(q-1) \log_q(2) = 1 - \frac{1}{2}(q-1) \log_q(2) < 0$, i.e. show that

$$\frac{q-1}{2} > \log_2(q).$$

For $q = 7$, this is true. So if we can show that the derivative with respect to q on the left-hand side is greater than the one on the right-hand side for all $q \geq 7$, the proposition is proved.

On the left-hand side we have

$$\frac{\mathrm{d}}{\mathrm{d}q} \frac{q-1}{2} = \frac{1}{2}.$$

On the right-hand side we have

$$\frac{\mathrm{d}}{\mathrm{d}q} \log_2(q) = \frac{1}{q \ln(2)},$$

which is less than $\frac{1}{2}$ for all $q \geq 3$. This finishes the proof. □

I here show two examples where R_4 is better than R_1.

Example 11.11. If $q = 81$, we have for $0 \leq \delta = 0.008 \leq (q-2)/(2(q-1))$ that

$$R_1 = 1 - 2\delta - \frac{1}{q-1} = 0.9715.$$

Since $0 < 2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta) \log_q(2) < 2/(\sqrt{q}+1)$, we have $h_q(2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta) \log_q(2)) = 0.1532$, which gives us

$$R_4 = 1 - 2\delta - \frac{1}{q-1} + \frac{1}{q-1} h_q\left(2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2} H_2(2\delta) \log_q(2)\right) = 0.9734.$$

In comparison, we have $R_{\mathrm{GV}} = 0.9814$.

Example 11.12. If $q = 1024$, we have for $0 \leq \delta = 0.00086 \leq (q-2)/(2(q-1))$ that

$$R_1 = 1 - 2\delta - \frac{1}{q-1} = 0.99730.$$

Since $0 < 2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta) \log_q(2) < 2/(\sqrt{q}+1)$, we have $h_q(2log_q(\sqrt{q}-1) - \frac{1}{2}(q-1)H_2(2\delta) \log_q(2)) = 0.047439$, which gives us

$$R_4 = 1 - 2\delta - \frac{1}{q-1} + \frac{1}{q-1} h_q\left(2log_q\left(\sqrt{q}-1\right) - \frac{q-1}{2} H_2(2\delta) \log_q(2)\right) = 0.99735.$$

In comparison, we have $R_{\mathrm{GV}} = 0.99814$.

11.2 A Possible Second Improvement

The idea of the previous section was to use Chaoping Xing's ideas of improving the bounds of Goppa codes by using good divisors and an upper bound for $N_{s,m}$. The tools of Xing's article [15] from 2001 were also used in [18] from 2005. As mentioned in Section 4.3, the difference between the two articles is that the 2005-article finds a better bound for the number $N_{s,m}$. This bound is so good that it is valid for all values of δ, whereas the 2001-bound is only valid for two small intervals of δ.

It should be expected that a similar improvement could be made for the bound we found in the previous section. I will here give a sketch of how the improvement can—possibly—be made.

The main proposition of the construction is still Proposition 11.4. Let X be a nonsingular projective curve and let notations be the same as in the previous section. We need to find a good upper bound for $N_{s,m}$. Let $M_{l,m} := N_{l+m,m}$ and let S be a set of s closed points of degree 2. Define $\mathscr{A}_l$ to be the set of all effective divisors of degree l, and let $\mathscr{A}_l^{(s)}$ be the set of effective divisors of degree l with support disjoint from S. Furthermore, for l even, let $\mathscr{P}$ be the set of all closed points of degree 2, and define $\mathscr{A}_l(\mathscr{P})$ to be all effective divisors D such that $D \prec \sum_{P\in\mathscr{P}} P$ and $\deg(D) = l$. For l a nonnegative integer, m a nonnegative even integer, and $0 \leq i \leq l/2$, let $\mathscr{M}_{l,m,i} = \{H + D \,|\, D \in \mathscr{A}_{m+2i}(\mathscr{P}),\ H \in \mathscr{A}_{l-2i},\ \mathrm{Supp}(H) \cap (\mathscr{P} - \mathrm{Supp}(D)) = \emptyset\}$. It then follows that $\mathscr{M}_{l,m,i} \cap \mathscr{M}_{l,m,j} = \emptyset$ for $0 \leq i < j \leq l/2$. It follows that

$$M_{l,m} = \sum_{i=0}^{\lfloor l/2 \rfloor} M_{l,m,i}.$$

Furthermore, if we let $A_l^{(s)} = |\mathscr{A}_l^{(s)}|$ and r be the number of closed points of degree 2 over $\mathbb{F}_q$ on X, then we have

$$|\mathscr{M}_{l,m,i}(\mathscr{P})| = \binom{r}{m/2+i} A_{l-2i}^{(r-m/2-i)}.$$

The first thing we need to do is to find an estimate for $A_l^{(s)}$ for general l and s. This can be done by defining the s-zeta-function for points of degree 2. Define

$$Z^{(s)}(X,T) = \sum_{i=0}^{\infty} A_i^{(s)} T^i.$$

From Section 5.1, we have that

$$Z(X,T) = \exp\left(\sum_{i=1}^{\infty} \frac{|X(\mathbb{F}_{q^i})|}{i} T^i\right).$$

It then follows that

$$Z^{(s)}(X,T) = \exp\left(|X(\mathbb{F}_q)|T + \sum_{i=2}^{\infty} \frac{|X(\mathbb{F}_{q^i})| - 2s}{i} T^i\right).$$

Taking natural logarithms on both sides, rearranging, and then removing the logarithms again, it can easily be shown that

$$Z^{(s,t)}(X,T) = Z(X,T)(1-T)^{2s} e^{2sT}.$$

The rest of the calculations are pretty much the same as in Xing's 2005-article, except that we sometimes must choose upper or lower bounds where the sums are otherwise difficult to find. It should however be possible to find an improvement of R_4 with this method.

Bibliography

[1] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *Journal für die reine und angewandte Mathematik*, pages 159–199, 2005.

[2] W. Fulton. *Plane Algebraic Curves*, pages 192–193. W.A. Benjamin, New York, 1969.

[3] A. Garcia and H. Stichtenoth. A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound. *Inventiones Mathematicae, Springer-Verlag*, pages 211–222, 1995.

[4] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61:248–273, 1996.

[5] R. Hill. *A First Course in Coding Theory*, pages 85, 195. Clarendon Press, Oxford, 1986.

[6] C. Martínez-Pérez and W. Willems. Is the class of cyclic codes asymptotically good? *IEEE Transactions on Information Theory*, 525(2):696–700, February 2006.

[7] F. Özbudak and H. Stichtenoth. Constructing codes from algebraic curves. *IEEE Transactions on Information Theory*, 45(7):2502–2505, November 1999.

[8] Y. Shany. Toward and explicit construction of nonlinear codes exceeding the Tsfasman–Vlăduţ–Zink bound. *IEEE Transactions on Information Theory*, 50:2844–2850, November 2004.

[9] A. Spera. Asymptotically good codes from generalized algebraic-geomtery codes. *Designs, Codes and Cryptography*, 37:305–312, 2005.

[10] S.A. Stepanov. *Codes on Algebraic Curves*, pages 25–37, 89, 103–120, 130–138, 162. Kluwer Academic/Plenum Publishers, New York, 1999.

[11] H. Stichtenoth. *Algebraic Function Fields and Codes*, page 31. Springer Verlag, Berlin, 1993.

[12] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman–Vlăduţ–Zink bound. *arXiv:math.AG/0506264*, 1, June 2005.

[13] M.A. Tsfasman and S.G. Vlăduţ. *Algebraic-Geometric Codes*, pages 68, 173, 177, 179. Kluwer Academic Publishers, 1991.

[14] J. van Lint and G. van der Geer. *Introduction to Coding Theory and Algebraic Geometry*, pages 55–58, 62. Birkhäuser Verlag, Basel, 1988.

[15] C. Xing. Algebraic-geometry codes with asymptotic parameters better than the Gilbert–Varshamov and the Tsfasman–Vlăduţ–Zink Bounds. *IEEE Transactions on Information Theory*, 47(1):347–352, January 2001.

[16] C. Xing. Asymptotic bounds on frameproof codes. *IEEE Transactions on Information Theory*, 48(11):2991–2995, November 2002.

[17] C. Xing. Nonlinear codes from algebraic curves improving the Tsfasman–Vlăduţ–Zink bound. *IEEE Transactions on Information Theory*, 49(7):1653–1657, July 2003.

[18] C. Xing. Goppa geometric codes achieving the Gilbert–Varshamov bound. *IEEE Transactions on Information Theory*, 51(1):259–264, January 2005.

[19] C. Xing, H. Niederreiter, and K.Y. Lam. Constructions of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(4):1186–1193, May 1999.

[20] C. Xing, H. Niederreiter, and K.Y. Lam. A generalization of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(7):2498–2501, November 1999.

[21] L. Xu. Improvement on parameters of goppa geometry codes from maximal curves using the Vlăduţ–Xing method. *IEEE Transactions on Information Theory*, 51(6):2207–2210, June 2005.