Chapter 1

Algebraic geometry codes: general theory

Iwan M. Duursma

Department of Mathematics,
University of Illinois at Urbana-Champaign,
duursma@math.uiuc.edu

This chapter describes some of the basic properties of geometric Goppa codes, including relations to other families of codes, bounds for the parameters, and sufficient conditions for efficient error correction. Special attention is given to recent results on two-point codes from Hermitian curves and to applications for secret sharing.

Contents

Introduction

Geometric Goppa codes became famous when Tsfasman, Vladuts and Zink showed that infinite families of such codes can be constructed that exceed the Gilbert-Varshamov bound. An important step towards actual application of the codes came when Justesen, Larsen, Jensen, Havemose and Høholdt gave an efficient decoding algorithm for a special class of curves. Many curves have since then been proposed and studied for the construction of geometric Goppa codes. Decoding algorithms can now correct any geometric Goppa code up to half its designed minimum distance and improvements in their implementation continue to be made. Several new applications have been proposed that use special features of geometric Goppa codes. This chapter presents basic properties of geometric Goppa codes. The material is divided over four sections, with results on linear codes, cyclic codes, Reed-Muller codes, and geometric Goppa codes.

1.1. Linear codes and the affine line

Let $\mathbb{F}$ be a finite field. A $\mathbb{F}$-*linear code* C of *length* n is a linear subspace of $\mathbb{F}^n$. For $x, y \in \mathbb{F}^n$, the *Hamming distance* of x and y is

$$d(x,y) = |\{i : x_i \neq y_i, i = 1, 2, \ldots, n\}|.$$

The *minimum distance* of a nontrivial code C is

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

The dimension k of a code and the minimum distance d satisfy the Singleton bound,

$$k + d \leq n + 1.$$

Codes that attain the upper bound are called *maximum distance separable (MDS)*. An example is the code

$$C(< k, \mathbb{F}) = \{\ (f(a_1), f(a_2), \ldots, f(a_q))\ :\ f \in \mathbb{F}[x]_{<k}\ \},$$

for a fixed ordering $(a_1, a_2, \ldots, a_q)$ of the elements in $\mathbb{F}$. The code $C(< k, \mathbb{F})$ is a special case of an extended cyclic code, a Reed-Muller code, and a geometric Goppa code. Those three families of codes are the subject of the next three sections. In this section we describe a number of properties that are important for all three families but that actually hold for much larger classes of codes if not for all linear codes.

The *dual code* $C^\perp$ of a code C is the maximal subspace of $\mathbb{F}^n$ that is orthogonal to C with respect to the standard inner product. A code is nondegenerate if neither the code nor its dual has a coordinate where all words are zero. The dual of the code $C(< k, \mathbb{F})$ is the code $C(< q-k, \mathbb{F})$, since $\sum_{x\in\mathbb{F}} x^i = 0$, for $i = 0, 1, \ldots, q-2$.

The *Singleton defect* or the *genus* of a code is $g(C) = n + 1 - k - d$. The dual of a MDS code is again MDS, but in general a code and its dual may have different genera. Every subset of k coordinates in an MDS code carries full information about the codeword. For a general code the MDS *discrepancy* or the *information defect* is the minimal m such that every subset of k coordinates contains at least $k - m$ information symbols. The parameter m is the same for a code and its dual and is at most the genus of a code.

1.1.1. *Dimension and infinite families*

A code C of type $[n, k, d]$ is *optimal* if it has maximal dimension for given length and minimum distance. For a family $\{[n_i, k_i, d_i]\}$ of optimal codes of increasing length with $\lim d_i/n_i = \delta$, define $\alpha(\delta) = \limsup k_i/n_i$. For an optimal code, each of its q^{n-k} cosets in $\mathbb{F}^n$ contains at least one vector y with $d(y, 0) < d$. The lower bound

$$q^{n-k} \leq |\{y \in \mathbb{F}^n : d(y, 0) < d\}|$$

for the dimension of an optimal code is called the *Gilbert-Varshamov bound.* For $0 \leq \delta \leq \theta = (q-1)/q$,

$$\frac{1}{n} \log |\{y \in \mathbb{F}^n : d(y, 0) < \delta n\}| = H_q(\delta) + o(1),$$

where $H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$, for $0 < x \leq \theta$.

Theorem 1.1. *(asymptotic Gilbert-Varshamov bound) For an infinite family of optimal codes with relative distance $d/n = \delta$,*

$$\alpha(\delta) \geq 1 - H_q(\delta), \quad \textit{for } 0 < \delta \leq \theta.$$

Lemma 1.1. *For a q-ary linear code with $k > m+1$ and $n-k > m(q^{m+1}-1)/(q-1) - (m+1)$ the information defect is at least m.*

Proof. Divide the coordinates in a subset of $k - (m+1)$ independent coordinates and its complement of $n - k + (m+1) > m(q^{m+1}-1)/(q-1)$ coordinates. In the subcode with zeros in the $k - (m+1)$ coordinates

there is a block of size at least $m+1$ in which the nonzero coordinates are essentially repeated. Together the $k-(m+1)+(m+1)$ coordinates contain only $k-m$ information symbols. □

For families of $q-$ary linear codes with k and $n-k$ going to infinity, the information defect (and therefore also the genus) goes to infinity. As a consequence we obtain the following upper bound for the dimension of an optimal code.

Theorem 1.2. *(asymptotic Plotkin bound) For an infinite family of codes with $k, n-k \to \infty$, we have $d \leq \theta(n-k)$ as $n \longrightarrow \infty$, or*

$$\alpha(\delta) \leq 1 - \delta/\theta, \quad \textit{for } 0 < \delta \leq \theta.$$

1.1.2. *Duality and differentials*

Let C be a linear code of length n. Omitting the i-th coordinate produces the *punctured code* $P_i(C)$ of length $n-1$. The *shortened code* $S_i(C)$ is the subcode of $P_i(C)$ of words with omitted i-th coordinate equal to zero. In general $P(C)^\perp = S(C^\perp)$. For a subset $\mathcal{P} = \{a_1, a_2, \ldots, a_n\}$ of the field $\mathbb{F}$, define a code

$$C(< k, \mathcal{P}) = \{\ (f(a_1), f(a_2), \ldots, f(a_n))\ :\ f \in \mathbb{F}[x]_{<k}\ \}.$$

The code $C(< k, \mathcal{P})$ is a punctured version of the code $C(< k, \mathbb{F})$. The dual code is a shortened version of the code $C(< q-k, \mathbb{F})$.

$$C(< k, \mathcal{P})^\perp = \{\ (f(a_1), f(a_2), \ldots, f(a_n))\ :\ f \in \mathbb{F}[x]_{<q-k}, f|_{\mathbb{F}-\mathcal{P}} = 0\ \}.$$

Let $p(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$ and let $x^q - x = p(x)r(x)$. Then $-1 = p'(a_i)r(a_i)$, for $i = 1, 2, \ldots, n$. With f of the form $f = rh$,

$$C(< k, \mathcal{P})^\perp = \{\ (\frac{h(a_1)}{p'(a_1)}, \frac{h(a_2)}{p'(a_2)}, \ldots, \frac{h(a_n)}{p'(a_n)})\ :\ h \in \mathbb{F}[x]_{<n-k}\ \}.$$

We give a description of the dual code using differentials. For a polynomial $h \in \mathbb{F}[x]$ of degree $\deg h < n$, let

$$\omega = \frac{h}{p}\,dx = (\frac{c_1}{x-a_1} + \frac{c_2}{x-a_2} + \cdots + \frac{c_n}{x-a_n})\,dx$$

be a differential with at most simple poles and with residues $c_1, c_2, \ldots, c_n$ at $x = a_1, a_2, \ldots, a_n$, respectively. Then $h(a_i) = c_i p'(a_i)$ and

$$C(< k, \mathcal{P})^\perp = \{(\mathrm{res}_{a_1}(\omega), \mathrm{res}_{a_2}(\omega), \ldots, \mathrm{res}_{a_n}(\omega))\ :\ \omega = \frac{h}{p}\,dx,\ \deg h < n-k\}.$$

1.1.3. *Minimum distance*

Several useful inequalities exist for the parameters of codes A, B, C with

$$\sum_i a_i b_i c_i = 0, \quad \text{for all } a \in A, b \in B, c \in C.$$

Let $a * b = (a_1 b_1, \cdots, a_n b_n)$ denote the Hadamard product or coordinate-wise product of two vectors a and b. The relation between A, B, C can be formulated as $A * B = \{a * b : a \in A, b \in B\} \subset C^\perp$. Such decompositions of the dual code under the Hadamard product form the basis for several bounds for the minimum distance.

Theorem 1.3. *(Roos bound for linear codes) For a linear code C, and for linear codes A and B with $A * B \subset C^\perp$,*

$$g(A) < d(B^\perp) - 1 \;\Rightarrow\; d(C) \geq k(A) + d(B^\perp) - 1.$$

Proof. It is enough to show that for every subset I of $(k(A) - 1) + (d(B^\perp) - 1)$ positions there exists a word $a * b \in A * B$ with precisely one nonzero coordinate in those positions. First choose $a \in A$ with zeros in $k(A) - 1$ positions of I. Then choose $b \in B$ with a single nonzero coordinate in the remaining $d(B^\perp) - 1$ positions such that the nonzero coordinate appears in a position where a is nonzero. This is possible since a has no more then $n - d(A) < k(A) - 1 + d(B^\perp) - 1$ zeros. □

Theorem 1.4. *(Symmetric Roos bound for linear codes) For a linear code C, and for linear codes A and B with $A * B \subset C^\perp$,*

$$g(A) < k(B) \text{ and } g(B) < k(A) \\ \Rightarrow\; d(C) \leq g(A) + g(B) \text{ or } d(C) \geq k(A) + k(B).$$

The two versions of the Roos bound can be used in combination, with different choices for A and B, to produce stronger results.

Theorem 1.5. *(Shift bound or Coset bound) Let C be a linear code and let $C_1 \subset C$ be a maximal subcode. If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that*

$$\begin{cases} a_i * b_j \in C^\perp & \text{for } i + j \leq w, \\ a_i * b_j \in C_1^\perp \backslash C^\perp & \text{for } i + j = w + 1, \end{cases}$$

then words in $C \backslash C_1$ have weight at least w.

Proof. For all $c \in C \backslash C_1$ and $a * b \in C_1^\perp \backslash C^\perp$, $\sum_i a_i b_i c_i \neq 0$. Thus it suffices to show the existence, for any choice of $w-1$ coordinates, of a vector $a * b \in C_1^\perp \backslash C^\perp$ that vanishes in those coordinates. The conditions show that the vectors $a_1, \ldots, a_w$ are linearly independent, and there exists a nonzero linear combination a of the vectors $a_1, \ldots, a_w$ vanishing at $w-1$ given coordinates coordinates. If i is maximal such that a_i has a nonzero coefficient in the linear combination a then $a * b_{w+1-i} \in C_1^\perp \backslash C^\perp$ and vanishes in the $w-1$ coordinates. □

Theorem 1.6. *(Iterated coset bound) Repeated application of the coset bound to a sequence $C_r \subset \cdots \subset C_1 \subset C_0 = C$ gives the lower bound $d(C) \geq \min\{d_1, d_2, \ldots, d_r, d(C_r)\}$, where $d(C_{i-1}/C_i) \geq d_i$ is obtained with the coset bound.*

1.1.4. *Error correction*

Let A, B, and C be nondegenerate linear codes such that

$$\sum_i a_i b_i c_i = 0, \quad \text{for all } a \in A, b \in B, c \in C.$$

If $k(A) > t$ and $d(B^\perp) > t$ then (A, B) is called a t-error-locating pair for C. For a given error-locating pair the error positions in a received word can be located by solving a suitable system of linear equations.

Theorem 1.7. *Let (A, B) be a t-error-locating pair for C. For $c \in C$ and for a vector e of weight at most t, let $y = c + e$. Every vector $a \in A$ with $a * y \perp b$ for all $b \in B$ has the property $a * e = 0$.*

An error-locating pair for C is called error-correcting if moreover $d(A) + d(C) > n$. For a given error-correcting pair a codeword can be recovered from the zeros in an error locating vector $a \in A$ by solving a second suitable system of linear equations.

Theorem 1.8. *Let (A, B) be a t-error-correcting pair for C. For $c \in C$ and for a vector e of weight at most t, let $y = c + e$. Let $a \in A$ have the property $a * e = 0$. Then $c \in C$ is the unique solution to the system of equations $c \in C$ and $a * c = a * y$.*

The key equation $a * y \perp b$ for all $b \in B$ amounts to a linear system of $\dim(B)$ equations in $\dim(A)$ unknowns. A different formulation gives a key equation with n linear equations in $\dim(A) + \dim(B^\perp)$ unknowns.

Theorem 1.9. *For $c \in C$ and for a vector e of weight at most t, let $y = c + e$. For every pair of vectors $a \in A, \hat{b} \in B^\perp$ with $a * y = \hat{b}$, the vector c is the unique solution to the system of equations $c \in C$ and $a * c = \hat{b}$.*

In general, the decoding is not completed with $c \in C$ since c is merely an encoding of the relevant information symbols. In such cases it may be better to bypass the computation of c and to solve directly for the information symbols. The t-error-correcting code $C(< q - 2t, \mathbb{F})$ has a t-error-correcting pair $(A = C(\leq t, \mathbb{F}), B = C(< t, \mathbb{F})$. The key equation for an error-locating vector is: determine $g(x) \in \mathbb{F}[x]_{\leq t}$ such that

$$\sum_i y_i g(x_i) h(x_i) = 0, \quad \text{for all } h \in \mathbb{F}[x]_{<t}.$$

When t errors occur, the solution for $g(x)$ is the unique polynomial that vanishes in those positions. The second key equations is: determine $g(x) \in \mathbb{F}[x]_{\leq t}$ and $\hat{h}(x) \in \mathbb{F}[x]_{<q-t}$ such that

$$y_i g(x_i) = \hat{h}_i(x_i), \quad \text{for } i = 1, 2, \ldots, n.$$

When t errors occur, the solution is the pair $(g(x), f(x)g(x))$ where $c_i = f(x_i)$ for $i = 1, 2 \ldots, n$. In general, the information symbols are the coefficients of f. The key equation with n equations generalizes to list decoding. List decoding produces a list of bounded size ℓ that contains all code words that are within distance t of the received word.

Theorem 1.10. *For a code $C(< k, \{x_1, \ldots, x_n\})$ and a received vector y, let*

$$Q(x, y) = \sum_{i=0}^{\ell} g_i(x) y^i, \quad \deg g_i < n - t - i(k-1),$$

be a nonzero polynomial such that $Q(x_i, y_i) = 0$ for $i = 1, 2, \ldots, n$. Then $y - f(x)$ divides $Q(x, y)$ for all f with $y_i = f(x_i)$ in at least $n - t$ positions.

Let E_I be the subspace of $\mathbb{F}^n$ generated by unit vectors e_i with $i \in I$, for $I \subset \{1, \ldots, n\}$. For an error vector $e \in E_I$, we reformulate the sufficient conditions for error correction in terms of I. Let $\bar{I} = \{1, \ldots, n\} \backslash I$.

Theorem 1.11. *For a linear code C, let A and B be linear codes with $A * B \subset C^\perp$, such that for all $a \in A$ and $c \in C$, $a * c = 0$ if and only if $a = 0$ or $c = 0$. Let $y = c + e$, with $c \in C$ and $e \in E_I$. If I is such that*

$$A \cap E_{\bar{I}} \neq 0 \quad \textit{and} \quad B^\perp \cap E_I = 0$$

then there exists a nonzero vector $a \in A$ with $a * y \perp b$ for all $b \in B$. And for any such a, $c \in C$ is the unique solution to the system of equations $c \in C$ and $a * c = a * y$.

1.1.5. *Linear secret sharing schemes*

An *ideal $\mathbb{F}-$linear secret sharing scheme* (LSSS) $\Sigma = \Sigma_0(\Pi)$ on the set of *players* $\mathcal{P} = \{1, 2, \ldots, n\}$ is a sequence $\Pi = (\pi_0, \pi_1, \ldots, \pi_n)$ of surjective linear mappings $\pi_i \colon E \to \mathbb{F}$, where E is a vector space of finite dimension over $\mathbb{F}$. For a given $s \in \mathbb{F}$ and for a randomly chosen $x \in E$ with $\pi_0(x) = s$, the values $\pi_1(x), \ldots, \pi_n(x)$ form a collection of *shares* for the *secret value* $\pi_0(x)$. A subset $A \subset \mathcal{P}$ is *qualified* or *accepted by* Σ if the players in A can determine the secret value uniquely from their shares. Otherwise A is *unqualified* or *rejected by* Σ.

Lemma 1.2. *A subset $A \subset \mathcal{P}$ is unqualified if and only if there exists $x \in E$ with $\pi_0(x) = 1$ and $\pi_i(x) = 0$ for all $i \in A$.*

For a LSSS $\Sigma = \Sigma_0(\Pi)$, let $\hat{C} = \{(\pi_1(x), \ldots, \pi_n(x), \pi_0(x)) : x \in E\}$ be the linear code of length $n + 1$ with shares in the first n positions and secret value in the last position. Let C denote the punctured code $\{(\pi_1(x), \ldots, \pi_n(x)) : x \in E\}$ and let C^0 denote the shortened code $\{(\pi_1(x), \ldots, \pi_n(x)) : x \in E, \pi_0(x) = 0\}$.

Theorem 1.12. *(Rejection bound) Let $\Sigma = \Sigma(\hat{C})$. If there exist vectors $a_0, \ldots, a_t \in \mathbb{F}^n$ and $b_0, \ldots, b_t \in \mathbb{F}^n$ such that*

$$\begin{cases} a_i * b_j \in C^0 & \text{for } i + j < t. \\ a_i * b_j \in C \backslash C^0 & \text{for } i + j = t. \end{cases}$$

then any subset $A \subset \mathcal{P}$ of size at most t is rejected by Σ.

Proof. A subset of players can not recover the secret s if and only if there exists a vector in $C \backslash C^0$ that is zero in their positions. The conditions show that the vectors $a_0, \ldots, a_t$ are independent. For a given set of t players there exists a nonzero linear combination a of the vectors $a_0, \ldots, a_t$ that vanishes at their coordinates. If i is maximal such that a_i has a nonzero coefficient in the linear combination a then $a * b_{t-i} \in C \backslash C^0$ and vanishes in the t coordinates. □

A LSSS Σ is *nondegenerate* if the secret can be reconstructed as a linear combination of all the shares. That is, there exist $r_1, \ldots, r_n \in \mathbb{F}$ such that

$$\pi_0(x) = \sum_i r_i \pi_i(x), \quad \text{for all } x \in E.$$

The same values reconstruct the sum $\pi_0(x) + \pi_0(y)$ of two secrets from the pairwise sums $\pi_i(x) + \pi_i(y)$ of their shares. We call Σ *additive in $n-t$ positions* if for any subset $A \subset \mathcal{P}$ of size t there exists a choice for $r_1, \ldots, r_n \in \mathbb{F}$ with $r_i = 0$ for $i \in A$.

Proposition 1.1. *For a given LSSS $\Sigma(\hat{C})$, let $\Sigma(\hat{D})$ be the scheme defined with the dual code $\hat{D}$ of $\hat{C}$. Then $\Sigma(\hat{C})$ is additive in $n-t$ positions if and only if $\Sigma(\hat{D})$ rejects all subsets $A \subset \mathcal{P}$ of size t.*

To implement secure protocols for multiparty computations that involve addition and multiplication, a stronger property is needed. A LSSS Σ is *multiplicative* if the product $\pi_0(x) \cdot \pi_0(y)$ of two secrets can be reconstructed as a linear combination of the pairwise products $\pi_i(x) \cdot \pi_i(y)$ of the shares, i.e. if there exist $r_1, \ldots, r_n \in \mathbb{F}$ such that

$$\pi_0(x)\pi_0(y) = \sum_i r_i \pi_i(x) \pi_(y), \quad \text{for all } x, y \in E.$$

We call Σ *multiplicative in $n-t$ positions* if for any subset $A \subset \mathcal{P}$ of size t there exists a choice for $r_1, \ldots, r_n \in \mathbb{F}$ with $r_i = 0$ for $i \in A$. A LSSS Σ is called *strongly multiplicative* if for any unqualified subset $A \subset \mathcal{P}$ there exists a choice for $r_1, \ldots, r_n \in \mathbb{F}$ with $r_i = 0$ for $i \in A$.

Proposition 1.2. *For a given LSSS $\Sigma(\hat{C})$, let $\Sigma(\hat{B})$ be the scheme defined with the maximal code $\hat{B}$ that is orthogonal to $\hat{C} * \hat{C}$. Then $\Sigma(\hat{C})$ is multiplicative in $n-t$ positions if and only if $\Sigma(\hat{B})$ rejects all subsets $A \subset \mathcal{P}$ of size t. And $\Sigma(\hat{C})$ is strongly multiplicative if and only if $\Sigma(\hat{B})$ rejects all unqualified subsets $A \subset \mathcal{P}$.*

A LSSS $\Sigma(\hat{C})$ that is multiplicative in $n-t$ positions (or that is strongly multiplicative) has a decomposition $\hat{D} \supset \hat{C} * \hat{B}$ of the dual code $\hat{D}$. This decomposition can be used to apply error correction as in the previous section to recover the secret in the presence of corrupted shares. The following theorem outlines a dedicated secret reconstruction procedure that avoids correcting corrupted shares and instead computes the secret directly. For geometric Goppa codes the theorem is a way to recover the value $f(P_0)$ from possibly erroneous values $f(P_1), \ldots, f(P_n)$. Since the point P_0 can

be chosen arbitrarily, the function f can be recovered completely and the theorem provides a way to decode geometric Goppa codes up to half their designed minimum distance (Theorem 1.43 in Section 1.4.7).

Theorem 1.13. *(Secret reconstruction) Let* $\Sigma = \Sigma_0(\Pi), \Sigma' = \Sigma_0(\Pi'), \Sigma'' = \Sigma_0(\Pi'')$ *be LSSSs such that* $\sum_i \pi_i(x)\pi'(y)\pi''(z) = 0$, *for all* $x \in E, y \in E', z \in E''$. *For a possibly corrupted vector of shares* $(s_1, \ldots, s_n)$ *for* Σ, *let* $(y, z) \in E' \times E''$ *be such that* $\pi'_0(y) = \pi''_0(z) = 1$ *and*

$$0 = \sum_i s_i \pi'_i(y)\pi''_i(z_0) \quad \forall z_0 \in E'' \text{ with } \pi''_0(z_0) = 0,$$

$$0 = \sum_i s_i \pi'_i(y_0)\pi''_i(z) \quad \forall y_0 \in E' \text{ with } \pi'_0(y_0) = 0.$$

If the corrupted shares are contained in a subset A *that is rejected by both* Σ' *and* Σ'' *then such a pair* (y, z) *exists and the secret for the uncorrupted vector of shares is*

$$s = -\sum_i s_i \pi'(y)\pi''(z).$$

If either Σ' *or* Σ'' *rejects* A *but not both then a pair* (y, z) *may not exist. If it exists then the formula for the secret produces the correct value for* s.

Proof. Assume that A is rejected by Σ''. Then $z = z_1$ with $\pi''_0(z_1) = 1$ and $\pi''_i(z_1) = 0$ for $i \in A$ gives a solution for z. An arbitrary $z \in E''$ with $\pi''_0(z) = 1$ is of the form $z = z_0 + z_1$ with $\pi''_0(z_0) = 0$. For a solution y to the first equation and for an arbitrary $z \in E''$ with $\pi''_0(z) = 1$,

$$\sum_i s_i \pi'_i(y)\pi''_i(z) = \sum_i s_i \pi'(y)\pi''(z_1) = \sum_i \pi_i(x)\pi'(y)\pi''(z_1) = -s.$$

This clearly implies the claims in the theorem. □

The choices that are made for y and z in general need not vanish in the corrupted shares. In general, the secret is reconstructed without obtaining information about corrupted players. Clearly the two equations reduce to a single equation when $\Sigma' = \Sigma''$.

A LSSS $\Sigma = \Sigma_0(\Pi)$ with $\sum_i \pi_i(x)\pi_i(y)\pi_i(z) = 0$ for all $x, y, z \in E$ is called trilinear. Such a scheme is strongly multiplicative and can reconstruct the secret efficiently whenever the corrupted shares are contained in an unqualified subset. A trilinear scheme that rejects all subsets of size t is multiplicative in $n - t$ positions. The Shamir LSSS

$\Sigma_0(\leq t, \{a_1, \ldots, a_n, a_0\}\}$ is the scheme $\Sigma_0(\Pi)$, where $\Pi : \mathbb{F}[x]_{\leq t} \longrightarrow \mathbb{F}^{n+1}$, $f \to (f(a_1), \ldots, f(a_n), f(a_0))$.

Theorem 1.14. *The Shamir LSSS $\Sigma_0(\leq t, (a_1, \ldots, a_n, a_0)\})$ rejects all subsets of size t or less and accepts all subsets of size $t+1$ or more. For $3t < n$, the scheme is trilinear.*

Proof. For $p = (x - a_0)(x - a_1) \cdots (x - a_n)$, and for $r_i = p'(a_i)$,

$$\sum_{i=0}^{n} r_i f(a_i) g(a_i) h(a_i) = 0, \forall f, g, h \in \mathbb{F}_{\leq t}[x].$$

□

1.1.6. *Weight distributions and codes over extension fields*

The weight distribution of a linear code C of length n is the vector $(A_0, A_1, \ldots, A_n)$, where A_i is the number of words of weight i in C. For a q-ary code the weight enumerator $A(x, y)$ and the projective weight enumerator $\bar{A}(x, y)$ are defined by

$$A(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = x^n + (q-1)\bar{A}(x, y).$$

For the code $C(< k, \{a_1, \ldots, a_n\})$ we can describe the projective weight enumerator in terms of the zeta function of the affine line. The latter is a generating function for the number of monic polynomials of a given degree, with Euler product factorization

$$(1 - qT)^{-1} = \prod_{f \text{monic, irr}} (1 - T^{\deg f})^{-1}.$$

The number of monic polynomials of degree less than k that vanish in precisely $n - i$ elements of $\{a_1, \ldots, a_n\})$ becomes

$$\bar{A}_i = [T^{k-1}] \frac{\binom{n}{i} T^{n-i} (1 - T)^i}{(1 - T)(1 - qT)}$$

and

$$\bar{A}(x, y) = [T^{k-1}] \frac{(xT + y(1 - T))^n}{(1 - T)(1 - qT)}$$

For a given coordinate, the weight enumerator of a code can be described recursively in terms of the punctured code and the shortened code at the

given coordinate.

$$A(x,y) = \begin{cases} xS(x,y), & \text{if } j \text{ is a loop} \\ (x+(q-1)y)P(x,y), & \text{if } j \text{ is a bridge} \\ yP(x,y)+(x-y)S(x,y), & \text{otherwise} \end{cases}$$

A coordinate is called a loop if shortening preserves the dimension and a bridge if puncturing lowers the dimension. A code is nondegenerate if it has no loops or bridges. An invariant that satisfies a recursion of the above type is called a Tutte-Grothendieck invariant. By continuing the recursion it is clear that there exist polynomials $T(x,y)$, called the Tutte polynomial, and $W(x,y) = T(x+1,y+1)$, called the Whitney polynomial, such that

$$\frac{A(x,y)}{(x-y)^k y^{n-k}} \;=\; T(\frac{x+(q-1)y}{x-y}, \frac{x}{y}) \;=\; W(\frac{qy}{x-y}, \frac{x-y}{y}).$$

The recursive procedure, and thus the polynomials T and W, remains the same if the q-ary code is extended to a code with coefficients in an extension field of size q^m. The weight enumerator $A^{(m)}$ of the q^m-ary code is

$$\frac{A^{(m)}(x,y)}{(x-y)^k y^{n-k}} \;=\; W(\frac{q^m y}{x-y}, \frac{x-y}{y}).$$

For a weight enumerator $A(x,y)$, let

$$P(x,y) = \frac{1}{n}(\frac{\partial}{\partial_x} + \frac{\partial}{\partial_y})A(x,y), \qquad S(x,y) = \frac{1}{n}(\frac{\partial}{\partial_x})A(x,y)$$

be the average punctured and shortened weight enumerator, respectively. They clearly satisfy the recursion type $A(x,y) = yP(x,y) + (x-y)S(x,y)$ of a nondegenerate code. Let $a_w = A_w/\binom{n}{w}$, for $w = 0,1,\ldots,n$. Define the normalized weight enumerator as

$$a(t) = \frac{1}{q-1}(a_d + a_{d+1}t + \cdots + a_n t^{n-d})$$

Theorem 1.15. *The expression*

$$a(t)(1+t)^{d+1} \pmod{t^{n-d+1}}$$

is invariant under puncturing and averaging or shortening and averaging. For the q-ary code $C(<k, \{a_1,\ldots,a_n\}$ the expression agrees with the evaluation of $1/(1-T)(1-qT)$ at $T = t/(1+t)$.

1.2. Cyclic codes and classical Goppa codes

A $\mathbb{F}$-linear code C of length n with coordinates $\{0, 1, \ldots, n-1\}$ is cyclic if, after identifying words $c = (c_0, c_1, \ldots, c_n)$ with polynomials $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, the code is an ideal in the ring $R = \mathbb{F}[x]/(x^n - 1)$. The ring R is a principal ideal domain. Polynomials $g(x)$ and $\gcd(x^n - 1, g(x))$ generate the same ideal in R and cyclic codes of length n correspond one-to-one to factors $g(x)$ of $x^n - 1$. If $\gcd(\mathrm{char}\,\mathbb{F}, n) = 1$, then $x^n - 1$ factors over $\mathbb{F}$ as a product of distinct irreducible polynomials. For a factorization $x^n - 1 = f_1 \cdots f_t$ into t irreducible factors, there are 2^t cyclic codes of length n over $\mathbb{F}$.

The code C with generating polynomial $g(x)|x^n - 1$ is determined by the irreducible factors in $g(x)$ or by the zeros of $g(x)$ in an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. Let $\alpha \in \overline{\mathbb{F}}$ be a primitive n-th root of unity. For $i \in \mathbb{Z}/n\mathbb{Z}$, let $m_i(x)$ be the minimal polynomial of α^i over $\mathbb{F}$. If $g(x) = \mathrm{lcm}\{m_i(x) : i \in I\}$ then I is called a *defining set* for C. The maximal defining set for C is the set $\{i \in \mathbb{Z}/n\mathbb{Z} : g(\alpha^i) = 0\}$. The dual code of a cyclic code with maximal defining set I is cyclic with maximal defining set $I^* = \mathbb{Z}/n\mathbb{Z} \setminus -I$, where we use $\sum_{k=0}^{n-1}(\alpha^{i+j})^k = 0$, for all $i, j \in \mathbb{Z}/n\mathbb{Z}$ with $i + j \neq 0$, Thus, the dual code of the code generated by $g(x)$ is the code generated by $h(x) = (x^n - 1)/g^*(x)$, where $g^*(x)$ is the reciprocal polynomial of $g(x)$.

1.2.1. *Reed-Solomon and BCH codes*

Of particular interest among cyclic codes are *BCH codes*, that are defined with a defining set of the form $I = \{b + 1, b + 2, \ldots, b + \delta - 1\}$. A BCH code over a field of q elements is called *primitive* if the length $n = q^m - 1$, for $m \geq 1$. A Reed-Solomon code is a primitive BCH code of length $n = q^m - 1$ over the field of q^m elements. For the given defining set, a Reed-Solomon code has parameters $[q^m, q^m + 1 - \delta, \delta]$. Primitive BCH codes in general have a maximal defining set that is larger than I. They are subcodes of Reed-Solomon codes and have minimum distance $d \geq \delta$. A lower bound for the dimension is $k \geq n - m(\delta - 1)$, with an improvement $k \geq n - m(q-1)\lceil(\delta-1)/q\rceil$ when $b = 0$. BCH codes are an important way to construct long codes over a given finite field such that both the minimum distance and the dimension have lower bounds. However asymptotically BCH codes are not good. For an infinite family of BCH codes of increasing length, either the relative distance d/n or the information rate k/n goes to zero as n goes to infinity.

Theorem 1.16. *The Reed-Solomon code of length $n = q^m - 1$ over the field of q^m elements with defining set $I = \{b+1, b+2, \ldots, b+\delta-1\}$ has as codewords the vectors $(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}))$, for $f \in L = \langle x^{-b}, \ldots, x^{-1}, 1, x, \ldots, x^a \rangle$, where a is such that $a + b = n - \delta$. The BCH code over the field of q elements with the same length and defining set is a subcode of the Reed-Solomon code.*

The space L is the vector space of rational functions in x with pole order at most a at ∞, pole order at most b at 0, and no other poles. In the terminology of the next section the Reed-Solomon code over the field $\mathbb{F}$ with defining set $I = \{b+1, b+2, \ldots, b+\delta-1\}$ is a two-point code $C_L(aP_\infty + bP_0, \mathbb{F}^*)$. When $b = 0$ the code $C_L(aP_\infty, \mathbb{F})$ is called a one-point code. These are the codes $C(\leq a, \mathbb{F})$ that were used as a main example in the previous section. BCH codes with $b = 0$, i.e. subfield subcodes of one-point codes, are called *narrow sense*.

To apply the theorems in Section 1.1.3 to cyclic codes requires a decomposition of their defining set. We illustrate this for the dual of the two-error correcting BCH code of length $n = 15$ over $\mathbb{F}_4$. The BCH code has defining set $\{1, 2, 3, 4\}$ and complete defining set $I = \{1, 2, 3, 4, 8, 12\}$. The dual code has complete defining set $I^* = \{0, 1, 2, 4, 5, 6, 8, 9, 10\}$. The code and its dual are of type $[15, 9, 5]$ and $[15, 6, 8]$, respectively. For the decomposition $I^* \supset \{0, 1, 2, 4, 5, 6\} + \{0, 4\}$, Theorem 1.3 gives $d \geq 8$. For the decomposition $I^* \supset \{0, 2, 4\} + \{0, 2, 4, 6\}$, Theorem 1.3 only gives $d \geq 7$. On the other hand this decomposition can be used with Theorem 1.8 to correct any three errors. For the decomposition $I^* \supset \{0, 1, 4, 5\} + \{0, 1, 4, 5\}$, Theorem 1.4 gives $d \leq 4$ or $d \geq 8$. The pair meets the conditions of Theorem 1.8 for correcting three errors, so the possibility $d \leq 4$ is easily excluded. Of the two decompositions that correct any three errors, the second has the property that the codes A and B can be defined over $\mathbb{F}_4$, while in the first case decoding takes place over the field $\mathbb{F}_{16}$.

1.2.2. *Classical Goppa codes*

The family of classical Goppa codes includes as subfamily the BCH codes but is large enough to contain infinite families of codes of increasing length that attain the asymptotic Gilbert-Varshamov lower bound for the dimension of optimal codes.

Let $\alpha_1, \cdots, \alpha_n \subset \mathbb{F}$ be distinct field elements and let $g(x) \in \mathbb{F}[x]$ be a monic polynomial that is relatively prime to $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$.

The classical Goppa code defined with the polynomial $g(x)$ is the set of all words $c = (c_1, \cdots, c_n) \in \mathbb{F}^n$ with

$$\frac{c_1}{x-\alpha_1}\,dx + \cdots + \frac{c_n}{x-\alpha_n}\,dx \;=\; \frac{h(x)}{p(x)}\,dx, \text{ for } g(x)|h(x).$$

The polynomial h is of degree at most $n-1$. It vanishes at the zeros of a word $c = (c_1, \cdots, c_n)$. Since $g|h$, we have $n - d \leq \deg h - \deg g \leq n - 1 - t$ and $d \geq t + 1$.

Theorem 1.17. *Let C be the classical Goppa code over $\mathbb{F}_{q^m}$ defined with relatively prime polynomials $g(x)$ and $p(x)|x^{q^m} - x$. The dual code $C^\perp$ of C is obtained by evaluation of functions in $L = \langle h/g : \deg h < \deg g \rangle$.*

Proof. As in Section 1.1.2,

$$C = \langle\, (\frac{g(\alpha_1)\alpha_1^i}{p'(\alpha_1)}, \cdots, \frac{g(\alpha_n)\alpha_n^i}{p'(\alpha_n)}) \,:\, i = 0, 1, \ldots, n-t-1 \,\rangle,$$

$$C^\perp = \langle\, (\frac{\alpha_1^j}{g(\alpha_1)}, \cdots, \frac{\alpha_n^j}{g(\alpha_n)}) \,:\, j = 0, 1, \ldots, t-1 \,\rangle.$$

□

In the terminology of geometric Goppa codes, C is defined by evaluating residues of differentials $\omega \in \Omega(G - P_\infty)$ and $C^\perp$ by evaluating values of functions $f \in L(G - P_\infty)$, where G is the divisor of zeros of $g(x)$. A classical Goppa code over the subfield $\mathbb{F}$ of size q is a subfield subcode of the code C. The Reed-Solomon code of length $n = q^m - 1$ with $I = \{1, 2, \ldots, \delta - 1\}$ has a dual code that is defined by the evaluation of functions $f \in L((\delta-1)P_\infty - P_0) = \langle x, \ldots, x^{\delta-1} \rangle$. To realize a Reed-Solomon code as a classical Goppa code we evaluate instead the functions $f \in L((\delta-1)P_0 - P_\infty) = \langle x^{1-\delta}, \ldots, x^{-1} \rangle$. A value in position α for the Reed-Solomon code appears with the different evaluation in position α^{-1}. The rearranged Reed-Solomon code is a classical Goppa code with divisor $G = (\delta - 1)P_0$ and polynomial $g(x) = x^{\delta-1}$.

Let $V(d-1) = |\{y \in \mathbb{F}^n : d(y, 0) < d\}|$ be the number of words in a closed ball of Hamming radius $d - 1$. Recall that the Gilbert-Varshamov bound shows that for given n and d, there exist codes with $q^{n-k} \leq V(d-1)$.

Theorem 1.18. *For a given length $n = q^m$ and minimum distance d, there exist irreducible polynomials $g(x)$ over $\mathbb{F}_{q^m}$ such that the classical Goppa code defined with $g(x)$ has minimum distance at least d and dimension attaining the asymptotic Gilbert-Varshamov bound.*

Proof. Let t denote the degree of $g(x)$. The number of irreducible polynomials of degree t over q^m is at least $(q^{mt} - d(t)q^{mt/2})/t$, where $d(t)$ is the number of divisors of t. For a word $(c_1, \ldots, c_n)$ of weight at most $d-1$, $h(x)$ has at least $n-d+1$ zeros in common with $p(x)$, and the cofactor of degree at most $d-2$ contains no more than d/t irreducible factors of degree t. Thus, for $d/t \cdot V(d-1) < (q^{mt} - d(t)q^{mt/2})/t$, there exist classical Goppa codes with polynomial $g(x)$ of degree t and minimum distance d. Since $q^{n-k} \leq q^{mt}$, there exist classical Goppa codes with

$$q^{n-k} \cdot (1 - d(t)q^{-mt/2}) \leq dV(d-1).$$

After taking logarithms and dividing by n, the factors $(1 - d(t)q^{-mt/2})$ and d are absorbed in $o(1)$ as n goes to infinity. □

1.2.3. *Dual BCH codes*

The RS code of length $n = q^m - 1$ with defining set $I = \{1, 2, \ldots, \delta - 1\}$ has parameters $[q^m - 1, q^m - \delta, \delta]$ over the field $\mathbb{F}_{q^m}$. The BCH code over the subfield $\mathbb{F}_q$ with the same length and defining set is the subcode of the RS code with coefficients in $\mathbb{F}_q$. The dual of a BCH code is again cyclic but it is in general not a BCH code. With Delsarte's theorem it can be described as the trace of the dual RS code.

Theorem 1.19. *(Delsarte's Theorem) Let C be a linear code of length n over $\mathbb{F}_{q^m}$ with dual code $C^\perp$. For the subfield $\mathbb{F} = \mathbb{F}_q$ and for the trace map* $\mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{m-1}}$,

$$(C \cap \mathbb{F}^n)^\perp = \mathrm{Tr}(C^\perp).$$

The extended RS code of length $n = q^m$ is the code $C(\leq q^m - \delta, \mathbb{F}_{q^m})$, with dual code $C(\leq \delta - 1, \mathbb{F}_{q^m})$. The weights of nonconstant codewords in the dual of the extended BCH code can be estimated with the Hasse-Weil bound.

Theorem 1.20. *For a polynomial $f \in \mathbb{F}_{q^m}[x]$, let $N(f)$ denote the number of zeros in $(\mathrm{Tr}(f(\alpha)) : \alpha \in \mathbb{F}_{q^m})$. If f is of degree at most $\delta - 1$ and not of the form $a(y^q - y) + b$, for $a \in \mathbb{F}_q, b \in \mathbb{F}_{q^m}$, then*

$$|q \cdot N(f) - q^m| \leq (\delta - 2)(q-1)q^{m/2}.$$

The bound compares the number $q \cdot N(f)$ of solutions (x, y) for the equation $y^q - y = f(x)$ with the number q^m of points on the affine line.

The weight distribution of a dual BCH code describes the number of rational points on curves of the form $y^q - y = f(x)$, for f of bounded degree.

The RS code and the BCH code describe linear relations among the vectors $(\alpha, \alpha^2, \ldots, \alpha^{\delta-1}) \in \mathbb{F}_{q^m}^{\delta-1}$, for $\alpha \in \mathbb{F}_{q^m}^*$. With class field theory the vectors have a natural interpretation as reduced Frobenius automorphisms inside a ray class group of conductor δ. This interpretation will be used in two directions. Weil's theorem on $L-$series for ray class fields gives estimates for the weight distribution of BCH codes. And BCH codes describe the relations between elements in ray class groups that determine the properties of quotient fields of the ray class field with many rational points.

Let $\mathbb{F}$ be a finite field of size $q = p^m$, for a prime p. Let $Q_p(\alpha)$ be a cyclotomic extension of the p-adic numbers with α a primitive n-th roots of unity for $n = p^m - 1$ and let $Z_p[\alpha]$ be the ring of integers in $Q_p(\alpha)$. For a positive integer e, let R_e be the finite ring $Z_p[\alpha]/(p^e)$. So that $|R_e| = q^e$.

For a fixed positive integer δ, let $I = \{1, 2, \ldots, \delta - 1\}$ and let $I^* = \{i \in I : \gcd(p, i) = 1\}$. For $i \in I^*$, let e_i be the unique integer with $ip^{e_i - 1} < \delta \leq ip^{e_i}$. So that $\sum_{i \in I^*} e_i = \delta - 1$.

Theorem 1.21. *(Class field theory) Let $\mathbb{F}$ be a finite field. For every non-negative integer δ, there exists a unique maximal abelian extension $K/\mathbb{F}(x)$, called the* ray class field extension *of conductor δ, for which all characters have conductor at most $\delta(x)_\infty$ and in which $(x)_0$ splits completely. The extension is finite of degree $q^{\delta-1}$ with Galois group*

$$\mathrm{Gal}(K/\mathbb{F}(x)) \ \simeq \ (\mathbb{F}[T]/T^\delta)^*/\mathbb{F}^* \ \simeq \ \oplus_{i \in I^*} R_{e_i}.$$

For $\alpha \in \mathbb{F}$, let $(K/\mathbb{F}(x), \alpha) \in \mathrm{Gal}(K/\mathbb{F}(x)$ denote the Frobenius automorphism. Under the isomorphisms

$$(K/\mathbb{F}(x), \alpha) \ \leftrightarrow \ (1 + \alpha T) \ \leftrightarrow \ (\alpha^i : i \in I^*).$$

If H is the subgroup generated by the Frobenius elements for $\alpha \in \mathbb{F}$, then the fixed field $K^H/\mathbb{F}$ defines an extension with group G/H in which ∞ is completely ramified and in which $x = a$ splits completely, for all $a \in \mathbb{F}$.

The set of all relations $(c_\alpha \in \mathbb{Z}/p^e\mathbb{Z} : \alpha \in \mathbb{F}^*)$ with $\sum_\alpha c_\alpha F_\alpha = 0$ defines a cyclic code modulo p^e. The Frobenius element F_α, for $\alpha \in \mathbb{F}^a st$, can be represented by the column vector $h_\alpha = (p^{e-e_i}\alpha^i : i \in I^*) \in R_e^{|I^*|}$. The code

has a generator polynomial $g(x) = g_0(x) + pg_1(x) + \cdots + p^{e-1}g_{e-1}$ with $g_{e-1}|\cdots|g_1|g_0|x^n - 1$, such that, for $i \in I^*$, $g_j(\alpha^i) = 0$ if and only if $j < e_i$ if and only if $ip^j < \delta$. The extended cyclic code $C(p^m, \delta)$ modulo p^e is the set of all relations $(c_\alpha \in \mathbb{Z}/p^e\mathbb{Z} : \alpha \in F)$ with $\sum_\alpha c_\alpha F_\alpha = 0$ and moreover $\sum_\alpha c_\alpha = 0$. The code $C(2^m, 3)$ is defined modulo 4. It is known as the quaternary Preparata code and its dual as the quaternary Kerdock code. The reduction of the code $C(p^m, \delta)$ modulo p is the extended primitive BCH code with designed minimum distance δ.

Theorem 1.22. *(Weil bound) Let χ be a character for $K/\mathbb{F}(x)$ of conductor δ, and let F_α denote the Frobenius element in $G = \mathrm{Gal}(K/\mathbb{F}(x))$ that corresponds to $x = \alpha$. Then*

$$|\sum_{\alpha \in F} \chi(F_\alpha)| \leq (\delta - 2)\sqrt{q}.$$

The theorem applies to characters of characteristic p^e and is more general then Theorem .... The latter follows by writing $q \cdot N(f) - q^m = \sum_{\beta^{q-1}=1} \sum_{\alpha^{q^m-1}=1} \chi(\mathrm{Tr}(\beta f(\alpha))$. In general, for a polynomial $f = \sum_{i \in I^*} p^{e-e_i} \sum_{ip^j < \delta} f_{ip^j} x^{ip^j} \in R_e[x]$, for a trace map $\mathrm{Tr} : R_e \to \mathbb{Z}/p^e\mathbb{Z}$, and for a nontrivial character $\chi : \mathbb{Z}/p^e\mathbb{Z} \to \mathbb{C}$,

$$|\sum_{\alpha^{q^m} - \alpha = 0} \chi(\mathrm{Tr}(f(\alpha))| \leq (\delta - 2)\sqrt{q}.$$

Let $\Delta = \{\, i' \in I^* : \exists i \in I^* \,|\, i < i',$ and $i' \equiv i \cdot q^j \pmod{n} \,\}$. For $i' \in \Delta$ with witness i, a relation $\sum_j c_j \alpha^{ij} = 0 \in R_{e_i}$ implies that $\sum_j \alpha^{i'j} = 0 \in R_{e'_i}$. Therefore, the group G/H has size at least $\prod_{i' \in \Delta} |R_{e'_i}|$.

Theorem 1.23.

(1) For $q = r^2$, let $\delta = r + 2$ and $I = \{1, 2 \ldots, r + 1\}$. Then $|G/H| \geq r$.
(2) For $q_0 = 2^s, q = 2^{2s+1}$, let $\delta = 2q_0 + 2$ and $I = \{1, 2, \ldots, 2q_0 + 1\}$. Then $2q_0 + 1 \in I'$, and $|G/H| \geq |R_1| = q$.
(3) For $q_0 = 3^s, q = 3^{2s+1}$, let $\delta = 3q_0 + 3$ and $I = \{1, 2, \ldots, 3q_0 + 2\}$. Then $3q_0 + 1, 3q_0 + 2 \in I'$ and $|G/H| \geq |R_1 \times R_1| = q^2$.

Proof. (1) The elements α^{r+1} span the subfield $\mathbb{F}_r$ of $R_1 = \mathbb{F}_q$. And $|\mathbb{F}_q/\mathbb{F}_r| = r$. (2) $2q_0 + 1 \equiv 2q_0(q_0 + 1) \pmod{q-1}$. (3) $3q_0 + 1 \equiv 3q_0(q_0 + 1) \pmod{q-1}$ and $3q_0 + 2 \equiv 3q_0(2q_0 + 1) \pmod{q-1}$. □

1.3. Reed-Muller codes

For geometric Goppa codes defined by the evaluation of functions in points $X = \{P_1, \ldots, P_n\}$ that form an ideal-theoretic complete intersection, the main properties can be established without the usual tools for algebraic curves. The dimension is given by the Hilbert function of X (instead of the Riemann-Roch theorem for curves), the dual code is of the same explicit form as the code itself (instead of defined in terms of differentials), and the code and its dual are related by the a-invariant of X (instead of the residue theorem for curves). Codes defined on complete intersections generalize the affine Reed-Muller codes and are part of the larger class of evaluation codes.

For a finite field $\mathbb{F}$, let $A = \mathbb{F}[x_0, x_1, ..., x_m] = \bigoplus_{\nu \geq 0} A(\nu)$ be the graded ring of polynomials in $m+1$ variables with homogeneous components $A(\nu)$, and let $X = \{P_1, ..., P_n\} \subseteq \mathbb{P}^m(\mathbb{F})$ be a set of n distinct points. For a positive integer ν, the $\mathbb{F}$-linear code $C(\nu, X)$ of length n is the image of the homogeneous component $A(\nu)$ after evaluation on X. That is, for a given choice of representatives for $P_1, \ldots, P_n$, the code $C(\nu, X) = \alpha(A(\nu))$, for the $\mathbb{F}$-linear evaluation map

$$\alpha : A \longrightarrow \mathbb{F}^n, \qquad \alpha(f) = (f(P_1), ..., f(P_n)).$$

For the field $\mathbb{F}$ of two elements, the *binary Reed-Muller code* $RM(\nu, m)$ is defined as the code $C(\nu, X)$ with $X = \{(1 : x_1 : \cdots : x_m) : x_i \in \mathbb{F}\}$. Replacing the binary field with an arbitrary finite field yields the class of *a*ffine or *g*eneralized Reed-Muller codes $GRM(\nu, m)$. Evaluation of $A(\nu)$ on a complete set X of representatives for the points of projective m-space over $\mathbb{F}$ yields the class of *projective Reed-Muller codes* $PRM(m, r)$.

Let $I_X = \bigoplus_{\nu \geq 0} I_X(\nu) \subseteq A$ be the vanishing ideal of X. Then the code $C(\nu, X)$ is isomorphic to $S(\nu)/I_X(\nu)$ and its dimension is $H_X(\nu)$, where H_X is the Hilbert function of I_X. If the ideal I_X is a complete intersection, that is if $I_X = (f_1, \ldots, f_m)$ such that f_i is not a zero divisor in $\mathbb{F}[x_0, x_1, \ldots, x_m]/(f_1, \ldots, f_{i-1})$, then the Hilbert function is completely determined by the multi-degree $(\nu_1, \ldots, \nu_m)$ of I_X. Moreover, duality of codes can be described in terms of the a-invariant $(\nu_1 + \cdots + \nu_m) - m - 1$ of X.

Theorem 1.24. *Let X be an ideal-theoretic complete intersection X of multi-degree $(\nu_1, ..., \nu_n)$ with ideal $I_X = (f_1, ..., f_m)$. Let $a_X = (\nu_1 + \cdots +$*

$\nu_m) - (m+1)$ *be the a-invariant of* I_X*. The Hilbert function* $H_X(\nu)$ *of* I_X *is*

$$\binom{m+\nu}{\nu} - \sum_i \binom{m+\nu-\nu_i}{\nu-\nu_i} + \sum_{i<j} \binom{m+\nu-(\nu_i+\nu_j)}{\nu-(\nu_i+\nu_j)} + \cdots + (-1)^m \binom{m+\nu-(\nu_1+\cdots+\nu_m)}{\nu-(\nu_1+\cdots+\nu_m)}$$

For $0 \le \nu \le a_X$, $H_X(\nu) + H_X(a_X - \nu) = n$.

The generalized Reed-Muller code $GRM(\nu, m)$ is defined with $X = \mathbb{P}^m(\mathbb{F})\backslash(x_0 = 0)$. It has vanishing ideal $I = (x_1^q - x_1 x_0^{q-1}, \ldots, x_m^q - x_m x_0^{q-1})$ with multi-degree $(\nu_1, \ldots, \nu_m) = (q, \ldots, q)$ and a-invariant $mq - (m+1)$. The code $GRM(\nu, m)$ has dual code $GRM(qm - m - 1 - \nu, m)$. The set $\mathbb{P}^m(\mathbb{F})$ of all points in projective $m-$space is in general not a complete intersection. Complete intersections in $\mathbb{P}^2(\mathbb{F})$ are described by the Bezout theorem.

Theorem 1.25. *(Bezout) The ideal generated by two polynomials* $f_1, f_2 \in \mathbb{F}[x_0, x_1, x_2]$ *with no common factors is a complete intersection. Over the algebraic closure of* $\mathbb{F}$ *the intersection of the curves* $f_1 = 0$ *and* $f_2 = 0$ *contains* $\deg f_1 \cdot \deg f_2$ *points counted with multiplicities.*

Examples of complete intersections in $\mathbb{P}^2$ are: (1) the projective line with multi-degree $(1, q+1)$ and $|X| = q+1, a_X = q-1$. (2a) the rational points on the Hermitian curve with multi-degree $(r+1, r^2-r+1)$ and $|X| = r^3+1, a_X = q-1$. (2b) the subset of rational points with multi-degree (r, r^2) and $|X| = r^3, a_X = r^2 + r - 3$. (3) the Klein curve with multi-degree $(4, 6)$ and $|X| = 24, a_X = 7$.

Theorem 1.26. *Let* $C(\nu, X)$ *be defined on the intersection* $X = \{P_1, ..., P_n\} \subseteq \mathbb{P}^2(\mathbb{F})$ *of two curves* $f_1 = 0$ *and* $f_2 = 0$ *with no common component. Let* $\nu_1 = \deg f_1$ *and* $\nu_2 = \deg f_2$*. The Hilbert polynomial* $H_X(\nu)$ *of* I_X *is*

$$\binom{2+\nu}{\nu} - \binom{2+\nu-\nu_1}{\nu-\nu_1} - \binom{2+\nu-\nu_2}{\nu-\nu_2} + \binom{2+\nu-(\nu_1+\nu_2)}{\nu-(\nu_1+\nu_2)}.$$

For $0 \le \nu \le a_X$, $H_X(\nu) + H_X(a_X - \nu) = n$.

Thus, when X is the set of r^3+1 rational points of the Hermitian curve of degree $r+1$ then, for any $0 \le \nu \le r^2 - 1$, the codes $C(\nu, X)$ and

$C(q-1-\nu, X)$ are dual to each other. This can also be seen as follows.

For codes $C(< k, \mathbb{F})$ on the affine line, duality of $C(< k, \mathbb{F})$ and $C(< q-k, \mathbb{F})$ amounts to the property $\sum_{x\in\mathbb{F}} x^i = 0$, for $i = 0, 1, \ldots, q-2$. If we extend the summation to points on the projective line, we have $\sum_{(x:y)} x^i y^{q-1-i} = 0$, for $i = 0, 1, \ldots, q-1$. The cases $i > 0$ reduce to the affine line $x = 1$ and the cases $i < q-1$ to the affine line $y = 1$. Note that the total degree $q-1$ of $x^i y^{q-1-i}$ makes the summation independent of a choice of representative for the projective points. That the a-invariant for the projective line and the Hermitian curve is $q-1$ in both cases corresponds to the fact that the rational points of the Hermitian curve form a codeword in the code spanned by lines [6], [50].

1.4. Geometric Goppa codes

Geometric Goppa codes use algebraic curves for their construction. Similar to codes on the affine line (Section 1.1), they can be defined in two different ways, by evaluating functions or by computing residues of differentials. In combination with well known theorems for algebraic curves, the definitions immediately reveal the following important properties of geometric Goppa codes:

- An explicit geometric description of both a code and its dual.
- Good lower bounds for the dimension, the minimum distance, and the dual minimum distance of a code.
- Expressions for code parameters in terms of invariants of algebraic curves.
- A multiplicative structure on codes.

Following are some important results for geometric Goppa codes that crucially depend on these properties:

- Constructions of polynomial complexity for asymptotically good codes.
- Efficient algebraic decoding.
- Applications to secret sharing and efficient multi-party computation.

In this section, we first give the definitions and the main properties of geometric Goppa codes (Sections 1.4.1, 1.4.2), followed by a summary of curves that have been used for their construction (Section 1.4.3). One-point codes and two-point codes are discussed in Sections 1.4.4 and 1.4.5. Finally, we present results on error correction (Section 1.4.6), secret sharing (Section 1.4.7), and weight distributions (Section 1.4.8).

1.4.1. *Curves and linear codes*

An *algebraic curve* $\mathcal{X}/\mathbb{F}$ is defined as an algebraic variety (i.e. an irreducible algebraic set) of dimension one over the field $\mathbb{F}$. The field of rational functions is denoted by $\mathbb{F}(\mathcal{X})$, the module of rational differentials by $\Omega(\mathcal{X})$. Among all curves with function field $\mathbb{F}(\mathcal{X})$ there is up to isomorphism a unique nonsingular projective curve. We define the codes in terms of the function field $\mathbb{F}(\mathcal{X})$ of $\mathcal{X}$. The geometric properties that we establish for codes hold for codes that are defined with the unique nonsingular projective model of $\mathcal{X}$. Function fields of algebraic curves over a finite field can be characterized as finite separable extensions $K/\mathbb{F}(x)$.

Points on a curve $\mathcal{X}$ are identified with places of the function field, rational points with places of degree one. Let t denote a generator of the maximal ideal of a place. For a rational function f, define the divisor $(f) = \sum \nu_t(f)P$, where P runs over all places and ν_t denotes the discrete valuation at P. For a divisor E, define

$$L(E) \;=\; \{\, f \in \mathbb{F}(\mathcal{X})^* \,:\, (f) + E \geq 0 \,\} \cup \{\, 0 \,\}$$

as the linear space of rational functions with pole divisor bounded by E.

Definition 1.1. Let $D = P_1 + P_2 + \cdots + P_n$, for distinct rational points $P_1, P_2, \ldots, P_n$, and let G be a divisor with support disjoint from D. The code $C_L(D, G)$ is the image of the linear map

$$\alpha_L \;:\; L(G) \;\longrightarrow\; \mathbb{F}^n, \qquad f \mapsto (\, f(P_1), \ldots, f(P_n)\,).$$

The map establishes an isomorphism $L(G)/L(G-D) \simeq C_L(D,G)$.

In general, $\dim L(G) \leq \deg G + 1$. To estimate the dimension of a code we need a lower bound for $L(G)$.

Theorem 1.27. *(Riemann) There exists a minimal constant $g \geq 0$ depending only on $\mathcal{X}$, such that $\dim L(G) \geq \deg G + 1 - g$. Moreover, for every divisor G of degree $\deg G > 2g - 2$, $\dim L(G) = \deg G + 1 - g$. The parameter g is called the genus of the curve $\mathcal{X}$.*

Theorem 1.28. *(code parameters) For $2g - 2 < \deg G < n$, the code $C_L(G, D)$ has dimension $k = \deg G + 1 - g$ and minimum distance $d \geq n - \deg G$. The dual code $C_L(G, D)$ has dimension $k^\perp = n - (\deg G + 1 - g)$ and minimum distance $d^\perp \geq \deg G - (2g - 2)$. In particular,*

$$n + 1 - g \leq k + d, k^\perp + d^\perp \leq n + 1.$$

Proof. The only part remaining is to show that $d^\perp \geq \deg G-(2g-2)$. For any $\tau < d^\perp$ positions $Q_1, \ldots, Q_\tau$, $\dim L(G) - \dim L(G - Q_1 \cdots - Q_\tau) = \tau$ and the encoding map α_L is surjective on the τ positions. □

A divisor is called principal if it is the divisor of a function. The relation $E_1 \sim E_2$ if and only if $E_1 - E_2$ is principal defines an equivalence relation on divisors.

Theorem 1.29. *(Approximation theorem) For a divisor E and a finite set of places S, there exists a divisor E' that is linearly equivalent to E and that has support outside S.*

In many cases it is attractive to define codes where D and G have one or more rational points in common. For the construction of such codes one may replace G with an equivalent divisor using the approximation theorem. However, the following theorem gives an important geometric property of algebraic curves that makes the construction of such codes straightforward without replacing the divisor G.

Theorem 1.30. *For a nonsingular curve $\mathcal{X}$ and for rational functions $(f_0, f_1, \ldots, f_m)$, the rational map $(f_0 : f_1 : \cdots : f_m) : \mathcal{X} \longrightarrow \mathbb{P}^m$ is a morphism (is defined everywhere).*

In case the divisors D and G have a rational point P in common, the evaluation map α_L in the definition of $C_L(G, D)$ is modified at the coordinate $\alpha_{L,P}$. For a given local parameter t at P, and for $i = \mathrm{ord}_P(G)$,

$$\alpha_{L,P} \ : \ L(G) \ \longrightarrow \ \mathbb{F}, \quad f \mapsto (t^i f)(P),$$

The bounds in Theorem 1.28 are based on properties of the geometric embedding of points in projective space and remain valid for the modified construction.

The Klein curve is defined by the equation $X^3Y + Y^3Z + Z^3X = 0$. Define a divisor $\Delta = (0 : 0 : 1) + (0 : 1 : 0) + (1 : 0 : 0)$. A monomial $X^aY^bZ^c$ intersects the curve with multiplicities

$$(X^3Y + Y^3Z + Z^3X = 0) \cap (X^aY^bZ^c = 0) = \\ (3a + b)(0 : 0 : 1) + (3b + c)(1 : 0 : 0) + (3c + a)(0 : 1 : 0).$$

We find a basis $\langle X^2Y/XYZ, Y^2Z/XYZ, Z^2X/XYZ, XYZ/XYZ\rangle$ for $L(2\Delta)$. Over the field of eight elements, the curve has 24 rational points. The given basis does not evaluate in the three points of Δ. An option

is to define the code on the remaining 21 points or to replace 2Δ with an equivalent divisor that has support in an extension field of $\mathbb{F}_8$. The straightforward solution suggested by the theorem is to embed the points as images of the morphism $(X^2Y : Y^2Z : Z^2X : XYZ)$. The morphism sends $(0:0:1) \mapsto (0:1:0:0)$, $(1:0:0) \mapsto (0:0:1:0)$, and $(0:1:0) \mapsto (1:0:0:0)$. There exist no 6 distinct rational points with $Q_1 + \cdots + Q_6 \sim 2\Delta$ and the code $C_L(2\Delta, D)$ is of type $[24, 4, 19]$. The distance is an arithmetic peculiarity of the configuration of flexpoints on the Klein curve that can be explained in terms of the large automorphism group of the curve but not with any of the theorems in this chapter.

Not all properties of codes are preserved by the modified construction: For divisors $G_1 \leq G_2$ that have supports disjoint from D, the code $C_L(D, G_1)$ is a subcode of the code $C_L(D, G_2)$. When $G_2 - G_1$ is not disjoint from D this is in general no longer true.

1.4.2. *Duality and differentials*

For a differential ω, define the divisor $(\omega) = \sum \nu_t(\omega)P$, where P runs over all places and $\nu_t(fdt) = \nu_t(f)$. The rational differentials $\Omega(\mathcal{X})$ form a free $\mathbb{F}(\mathcal{X})$ module of rank one. The divisor class of a differential is called the canonical divisor class, K denotes a divisor representing the class. For a divisor E, define the linear space of rational differentials

$$\Omega(E) \;=\; \{\, \omega \in \Omega(\mathcal{X})^* \;:\; (\omega) \geq E \,\} \cup \{\, 0 \,\}.$$

Definition 1.2. Let $D = P_1 + P_2 + \cdots + P_n$, for distinct rational points $P_1, P_2, \ldots, P_n$, and let G be a divisor with support disjoint from D. The code $C_\Omega(D, G)$ is the image of the linear map

$$\alpha_\Omega \;:\; \Omega(G - D) \;\longrightarrow\; \mathbb{F}^n, \qquad \omega \mapsto (\,\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)\,).$$

The map establishes an isomorphism $\Omega(G-D)/\Omega(G) \simeq C_\Omega(D, G)$.

In case the divisors D and G have a rational point P in common, the evaluation map α_Ω is modified at the coordinate $\alpha_{\Omega,P}$. For a given local parameter t at P, and for $i = \mathrm{ord}_P(G)$,

$$\alpha_{\Omega,P} \;:\; \Omega(G - D) \;\longrightarrow\; \mathbb{F}, \quad \omega \mapsto \mathrm{res}_P(t^{-i}\omega).$$

Theorem 1.31. *(Residue theorem) The summation over all places of the residues of a differential is well-defined and equal to zero.*

Each differential ω induces a natural isomorphism

$$L((\omega) - E) \quad \xrightarrow{\sim} \quad \Omega(E), \qquad f \mapsto f\omega.$$

If η is a differential with a simple pole at P and residue $\mathrm{res}_P(\eta) = 1$, and if f is a function with no pole at P, then $\mathrm{res}_P(f\eta) = f(P)$.

Lemma 1.3. *If η is a differential with simple poles at $P_1, P_2, \ldots, P_n$ and residues equal to 1 at those points then*

$$C_\Omega(G, D) = C_L((\eta) + D - G, D)$$

Proof. For $f \in L((\eta) + D - G)$, $f(P) = \mathrm{res}_P(f\eta)$, where the differential $\omega = f\eta$ has divisor $(\omega) = (f) + (\eta) \geq G - D$. □

Lemma 1.4. *Let f be a nonzero rational function. The differential df/f has at most simple poles and the residue at P is $\mathrm{res}_P(df/f) = \mathrm{ord}_P(f)$.*

Theorem 1.32. *(Riemann-Roch) The dimensions of $L(E)$ and $L(K-E) \simeq \Omega(E)$ are related by*

$$\dim L(E) - \dim L(K - E) = \deg(E) + 1 - g.$$

Together, the Residue theorem and the Riemann-Roch theorem imply that $C_\Omega(G, D)$ is the dual code of $C_L(D, G)$.

Theorem 1.33. *The codes $C_L(D, G)$ and $C_\Omega(G, D)$ are dual codes.*

As the dual of $C_L(D, G)$, the code $C_\Omega(D, G)$ has minimum distance at least $\deg G - (2g - 2)$ (Theorem 1.28).

Theorem 1.34. *(Symmetric floor bound) Let $G = A + B + Z$, for $Z \geq 0$ such that $L(A + Z) = L(A)$ and $L(B + Z) = L(B)$. For D with $D \cap Z = 0$, a nonzero word in $C_\Omega(D, G)$ has weight at least $\deg G - (2g - 2) + \deg Z$.*

Proof. Suppose that $c \in C_\Omega(D, G)$ is nonzero in the positions $Q = Q_1 + \cdots + Q_d$, so that there exists $E \geq 0$ with $K + Q \sim A + B + Z + E$. With the Riemann-Roch theorem,

$$\dim L(A + E) - \dim L(B + Z - Q) = \deg(A + E) + 1 - g,$$
$$\dim L(A + Z) - \dim L(B + E - Q) = \deg(A + Z) + 1 - g.$$

It follows that

$$\deg E - \deg Z = l(A + E) - l(A) + l(B + E - Q) - l(B - Q) \geq 0.$$

Finally, $\deg E \geq \deg Z$ gives $d \geq \deg G - (2g - 2) + \deg Z$. □

The divisor K satisfies: $\deg K = 2g-2$ and $l(K) = g$. The genus g of a nonsingular plane curve of degree m satisfies $g = (m-1)(m-2)/2$. For a plane curve, let the divisor L denote the intersection divisor of a line with the curve, then $K = (m-2)L$ represents the canonical class.

For divisors $G + G' \sim D$, the codes $C_L(G, D)$ and $C_L(G', D)$ are in general not dual codes, unless $g = 1$. The two codes have the same number of words of designed distance. Namely G is equivalent to a sum of rational points Q if and only if G' is equivalent to the sum of rational points Q', where $Q + Q' = D$. If one code has distance greater than the designed distance then the other code as well. With the Klein curve over $\mathbb{F}_8$, and for $G = 2\Delta$, we found a code of type $[24, 4, 19]$. In this case, $D \sim 8\Delta$ and the code with $G' = 6\Delta$ is of type $[24, 16, 7]$. This is the best known three-error-correcting code of length 24 over $\mathbb{F}_8$. Its weight distribution is given in Table 1.3.

Theorem 1.35. *(Clifford's theorem) For a divisor E such that both $L(E)$ and $\Omega(E)$ are nontrivial,*

$$\dim L(E) \leq \frac{\deg(E)}{2} + 1.$$

1.4.3. *Families of curves*

The first step towards good geometric Goppa codes over a field $\mathbb{F}_q$ is the search for curves $\mathcal{X}/\mathbb{F}_q$ that have many rational points for a given genus. For a given curve $\mathcal{X}/\mathbb{F}_q$ of genus g with N rational points, we can construct $\mathbb{F}_q$-linear codes of length N of any dimension $0 \leq k \leq N$ such that $k + d \geq N + 1 - g$.

The class of Deligne-Lusztig varieties was defined for the purpose of studying representations of algebraic groups. The class contains three families of irreducible curves (Table 1.1). Curves in each family have the maximal number of rational points for their genus and they have large automorphism groups. In each case, the automorphism group is of order $N(N-1)(q-1)$ and acts $2-$transitively on the set of rational points. The curve of unitary type was already known as the Hermitian curve. Another much studied curve is the Klein curve, or the modular curve $X(7)$. From its definition as a modular curve it follows that it is a nonsingular quartic with automorphism group the simple group $PSL(2, 7)$ of order 168. Klein found the model $X^3Y + Y^3Z + Z^3X = 0$ for the unique curve with these properties. Over the field of eight elements it has the maximal number of 24 rational

points for a curve of genus 3.

Table 1.1. Deligne-Lusztig curves $X/\mathbb{F}_q$.

Type	Unitary	Suzuki	Ree
X	$y^r + y = x^{r+1}$.	$y^q + y = x^{q_0}(x^q + x)$.	$y^q - y = x^{q_0}(x^q - x)$, $z^q - z = x^{q_0}(y^q - y)$.
q	$q = r^2$	$q = 2q_0^2 \geq 8$.	$q = 3q_0^2 \geq 27$.
g	$r(r-1)/2$	$q_0(q-1)$	$\frac{3}{2}q_0(q-1)(q+q_0+1)$
N	r^3+1	q^2+1	q^3+1
conductor	$r+2$	$2q_0+2$	$3q_0+3$

Serre initiated the construction of curves with many points using class field theory. This has been a very successful method to show that certain pairs (N, g) occur as the number of rational points and the genus of a curve. The actual construction of the curves is in general not straightforward. Lauter uses class field theory to show the existence of curves with the parameters of the Deligne-Lusztig curves. In those cases there is a connection between class field theory and BCH codes (Theorem 1.23).

For asymptotic results we need families of curves of increasing genus such that $\liminf N_i/g_i > 0$ as $g_i \to \infty$. For any given family $\limsup N_i/g_i \leq \sqrt{q} - 1$ (Drinfeld-Vladuts bound). Asymptotic results were first obtained by Tsfasman, Vladuts and Zink. They use families of modular curves over $\mathbb{F}_q$ to attain the best possible $\liminf N_i/g_i = \ell - 1$, for $q = \ell^2$. In subsequent papers polynomial constructions were given for the codes from these curves. Garcia and Stichtenoth presented several constructions for optimal towers that have a short and explicit recursive definition (Table 1.2).

Table 1.2. Recursively defined towers of function fields ($F_1 = \mathbb{F}_q(x_1)$).

(A)	$F_{n+1} = F_n(z_{n+1})$	$z_{n+1}^\ell + z_{n+1} = x_n^{\ell+1}$, $x_n = z_n/x_{n-1}$	$q = \ell^2$
(B)	$F_{n+1} = F_n(x_{n+1})$	$x_{i+1}^\ell + x_{i+1} = x_i^\ell/(x_i^{\ell-1}+1)$	$q = \ell^2$
(C)	$F_{n+1} = F_n(x_{n+1})$	$x_{i+1}^m + (x_i+1)^m = 1$	$m \mid (q-1)/(p-1)$
(D)	$F_{n+1} = F_n(x_{n+1})$	$x_{i+1}^{\ell-1} + (x_i+1)^{\ell-1} = 1$	$q = \ell^2$

The towers (A) and (B) are wildly ramified while the towers (C) and (D) are tamely ramified. An efficient construction of codes in the tower

(A) is given in [70]. In [78], codes are constructed with the field F_3 in the tower (B). The towers (A) and (B) correspond to Drinfeld modular curves [27] and the towers (C) and (D) to classical modular curves [25]. Examples are the modular towers $X_0(3^n)$ in char $= 2$ and $X_0(2^n)$ in char $= 3$. Klein gives solutions for the modular equations $J_2(j(\tau), j(2\tau)) = 0$ and $J_3(j(\tau), j(3\tau)) = 0$ in terms of resolvents,

$$J_2(\psi_2(\eta), \psi_2(\eta_0)) = 0, \quad \text{for } \psi_2(\eta) = 64\frac{(\eta+3)^3}{(\eta-1)^2}, \ (\eta-1)(\eta_0-1) = 1,$$
$$J_3(\psi_3(\eta), \psi_3(\eta_0)) = 0, \quad \text{for } \psi_3(\eta) = 27\frac{\eta(\eta+8)^3}{(eta-1)^3}, \ (\eta-1)(\eta_0-1) = 1,$$

such that $\psi_2(z'^2) = \psi_2(z^2)$ for all symmetries of the triangle $\{1, -1, \infty\}$, and $\psi_3(z'^3) = \psi_3(z^3)$ for all symmetries of the tetrahedron $\{1, \omega, \omega^2, \infty\}$. In particular,

$$\psi_2(z'^2) = \psi_2(z^2), \quad \text{for } z' = \frac{z+3}{z-1} \ (1 \leftrightarrow \infty, -1 \leftrightarrow -1).$$
$$\psi_3(z'^3) = \psi_3(z^3), \quad \text{for } z' = \frac{z+2}{z-1} \ (1 \leftrightarrow \infty, \omega \leftrightarrow \omega^2).$$

The modular equation is symmetric in its two arguments and so is the equation $(\eta - 1)(\eta_0 - 1) = 1$ in the variables η, η_0. In the $z-$plane, a recursive formula for the modular tower can be achieved by rotating z before adjoining z_0 (as described in Cohn, Iteration and the icosahedron).

$$z' = \frac{z+3}{z-1}, \quad (z'^2 - 1)(z_0^2 - 1) = 1.$$
$$z' = \frac{z+2}{z-1}, \quad (z'^3 - 1)(z_0^3 - 1) = 1.$$

In the variables $x = -1/z, y = -1/z_0$, the recursive formulas are

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

In char $= 3$ the first tower $X_0(2^n)$ is of type (D), and in char $= 2$ the second tower $X_0(3^n)$ is of type (C).
The equation $F_{n+1} = F_n(x_{n+1}), x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i$ defines an asymptotically good tower over $\mathbb{F}_8$. It has a generalization to arbitrary cubic fields.

1.4.4. *One-point codes*

For a curve with many rational points for a given genus, any choice of divisor G will give a good code. In many cases, once the degree of G has been fixed, a convenient choice is a divisor $G = mP_\infty$ with support at a single point P_∞. The codes $C_L(mP_\infty, D)$ are called one-point codes. It follows from Lemma 1.3 that the dual code of a one-point code is again a one-point code if there exists a differential η with divisor $(2g-2+n)P_\infty - D$ that has residues equal to 1 at the points $P_1, P_2, \ldots, P_n$. In that case

$$C_\Omega(mP_\infty, D) = C_L((2g-2+n-m)P_\infty, D).$$

For the projective line, for the Hermitian curves, and for the Suzuki curves, the dual of a one-point code is again a one-point code. For each of these curves, the divisor D can be chosen to be the set of all rational points minus the point P_∞. For this choice of D, there exists an algebraic function $x \in K$ such that $n = [K : \mathbb{F}(x)] \cdot q$ and $\eta = df/f$ for $f = x^q - x$.. The one-point codes can be extended by including the point P_∞ in D. The modified construction for one-point codes is straightforward and in some cases the longer codes that are obtained in this way have larger automorphism groups.

For the Klein curve $X^3Y + Y^3Z + Z^3X = 0$, the dual of a one-point code is in general not a one-point code. The curve has three points O_0, O_1, O_2 with $XYZ = 0$. Let $K = L$ be the canonical divisor class and let $\Delta = O_0 + O_1 + O_2$. The divisor classes K and 2Δ are invariant under the full automorphism group $PSL(2,7)$. The spaces $L(m(L-\Delta))$ are spanned by monomials. For the Klein curve over $\mathbb{F}_8$, the codes $C_L(m(L-\Delta), D)$ are better than the one-point codes on the same curve, are closed under duality, and have interesting geometric properties.

The space $L(mP_\infty)$ is a subset of the affine ring $R = \cup_{m \geq 0} L(mP_\infty)$ of rational functions with poles only at P_∞. The ring is a finitely generated $\mathbb{F}$-algebra. If $\phi_1, \ldots, \phi_r$ are generators and $m_1, \ldots, m_r$ are their pole orders then the set of all possible pole orders is the semigroup $\Lambda = \mathbb{Z}m_1 + \cdots + \mathbb{Z}m_r \subset \mathbb{Z}$ The complement $\mathbb{Z} \backslash \Lambda$ is finite of size g. Especially when r is small, the ring R can be used for efficient encoding (if the code is a one-point code) or efficient decoding (using a key equation in standard form if the dual code is a one-point code, or a key equation in Welch-Berlekamp form if the code is a one-point code).

The Hermitian curve over a field $\mathbb{F}$ of size q^2 is the curve $X/\mathbb{F} : y^q + y = x^{q+1}$. For every $x \in \mathbb{F}$, there are q solutions for $y \in \mathbb{F}$. Together with the point at infinity $P_\infty = (0:1:0)$ the curve has q^3+1 rational points. Codes from Hermitian curves are among the most studied geometric Goppa codes. The semigroup Λ of nongaps is generated by $\{q, q+1\}$.

Lemma 1.5. *For an integer a, write $a = a_0(q+1) - a_1$ with $0 \le a_1 \le q$. Then a is a nongap if and only if $a_1 \le a_0$.*

For the Suzuki curve, the semigroup of nongaps is generated by $\{q, q + q_0, q + 2q_0, q + 2q_0 + 1\}$, and for the Klein curve by $\{3, 5, 7\}$. For Hermitian one-point codes, the actual minimum distance is completely determined by properties of the nongaps. We give a first proof based on the following lemma.

Lemma 1.6. *For every point $R = (x_0, y_0) \neq P_\infty$, there exists an effective divisor E_R of degree q such that $(y - y_0) = R + E_R - (q+1)P_\infty$ and $E_R \cap P_\infty = 0$.*

Theorem 1.36. *Let $G = K + (a_0(q+1) - a_1)P_\infty$, with $K = (q-2)(q+1)P_\infty$ a canonical divisor. Then*

$$d(C_\Omega(G, D)) = \begin{cases} a_0(q+1) - a_1 & \text{if } a_1 \le a_0 \\ a_0(q+1) - a_0 & \text{if } a_1 > a_0 \end{cases}$$

Proof. Let $Q = Q_1 + \cdots + Q_d$ and assume that there exists a nonzero differential $\omega \in \Omega(G - Q)$ with $(\omega) = G - Q + E, E \ge 0$. Then $Q \sim (a_0(q+1) - a_1)P_\infty + E$. For each point $R \in E$ apply the lemma to find $Q + \sum E_R \sim ((a_0 + \deg E)(q+1) - a_1)P_\infty$. With the first lemma $a_1 \le a_0 + \deg E$. □

In this case, it appears natural to formulate the bound for the code $C_\Omega(G, D)$. The result and the proof depends on G but not on D. Below we repeat the proof for a code $C_L(G^*, D)$ which essentially leads us back to the case of a code $C_\Omega(G, D)$ after making the assumption $D \sim nP_\infty$.

Proof. (second proof) We prove the minimum distance bound for the code $C_L(m^*P_\infty, D)$, where $m^* = n + 2g - 2 - m = n - a_0(q+1) + a_1$. Assume that there exists a nonzero $f \in L(m^*P_\infty - Q')$, with $(f) = Q' + E - m^*P_\infty$, $E \ge 0$. Then the complement $Q = D - Q' \sim (n - m^*)P_\infty + E$. As in the first proof, $Q + \sum E_R \sim ((a_0 + \deg E)(q+1) - a_1)P_\infty$ and $a_1 \le a_0 + \deg E$. □

A special case of the theorem can be obtained with Theorem 1.34. Let $A = B = (a_0(q+1)-q)P_\infty, Z = (q-a_0-1)P_\infty, 1 \le a_0 \le q-1$. Then the code $C_\Omega(G,D)$ with $G = (2a_0-1)(q+1)-a_0$ has $d = d^* + (q-a_0-1)$. This corresponds to the case $G = ((q-2)(q+1) + (2a_0+1-q)(q+1) - a_0)P_\infty$ in the theorem above, with $a_0 \ge 2a_0 + 1 - q$ if and only if $a_0 \le q-1$.

For Hermitian one-point codes of length q^3, the q^3 finite rational points form a complete intersection with coordinate ring

$$\begin{aligned} & \mathbb{F}[x,y]/(y^q + y - x^{q+1}, x^{q^2} - x) \\ = \ & \langle x^i y^j : 0 \le i \le q^2 - 1, 0 \le j \le q-1 \rangle. \end{aligned}$$

For the q^3 monomials $x^i y^j$ in the vector space basis,

$$\sum_{P \in D} x^i y^j = \begin{cases} 1 & \text{if } x^i y^j = x^{q^2-1} y^{q-1} \\ 0 & \text{otherwise} \end{cases}$$

Duality can be stated as

$$\sum_{P \in D} x^i y^j = 0, \quad \text{for } i + j \le q-1, \ (i,j) \ne (0, q-1).$$

The monomials with $i + j \le q-1$, $(i,j) \ne (0,q-1)$ generate but do not form a basis for the coordinate ring. The set of all q^3+1 rational points is also a complete intersection, with coordinate ring

$$\begin{aligned} & \mathbb{F}[x,y]/(y^q + y - x^{q+1}, x(y^{q^2} - y)/(y^q + y)) \\ = \ & \langle x^i y^j : 0 \le i \le q, 0 \le j \le q^2 - q \rangle. \end{aligned}$$

For the q^3+1 monomials $x^i y^j$ in the vector space basis,

$$\sum_{P \in D \cup P_\infty} x^i y^j = \begin{cases} 1 & \text{if } x^i y^j = x^q y^{q^2-q} \\ 0 & \text{otherwise} \end{cases}$$

Duality can be stated as

$$\sum_{P \in D} x^i y^j = 0, \quad \text{for } i + j \le q-1.$$

This is the same duality as that for a summation over all points of the projective line, and indeed follows from that duality since the points on the Hermitian curve form a codeword in the code of the point-line graph of the projective plane [6], [50]. The monomials with $i + j \le q-1$ generate but

do not form a basis for the coordinate ring. The tables give the monomial basis for each of the two coordinate rings when $q = 3$.

$-$	1	y	y^2
1	0	4	8
x	3	7	11
x^2	6	10	14
x^3	9	13	17
x^4	12	16	20
x^5	15	19	23
x^6	18	22	26
x^7	21	25	29
x^8	24	28	32

$-$	1	y	y^2	y^3	y^4	y^5	y^6
1	0	4	8	12	16	20	24
x	3	7	11	15	19	23	27
x^2	6	10	14	18	22	26	30
x^3	9	13	17	21	25	29	33

The coordinate ring $\mathbb{F}[x, y]$ of the Hermitian curve itself is often considered as an $\mathbb{F}[x]$ algebra with free basis $\{1, y, \ldots, y^{q-1}\}$. For one-point codes of full length q^3+1, the ring $\mathbb{F}[x, y]$ may be considered as an $\mathbb{F}[y]$ algebra with free basis $\{1, x, \ldots, x^q\}$.

1.4.5. *Two-point codes*

Let $\mathcal{X}$ be a curve and let P_∞, P_0 be distinct rational points. A two-point code is defined with a divisor $G = aP_\infty + bP_0$. For the rational function field $\mathbb{F}(x)$ let P_∞ be the simple pole of x and P_0 the simple zero of x. Then, for $a + b \geq 0$, $L(aP_\infty + bP_0) = \langle x^{-b}, \ldots, x^a \rangle$. Thus, two-point codes are to one-point codes what BCH codes are to narrow sense BCH codes. The larger class of codes contains some codes that are better without giving up the advantages of efficient encoding and decoding. The subsemigroup $H(P_\infty, P_0)$ of $\mathbb{N} \times \mathbb{N}$ was introduced in 1985 by Joe Harris. It consists of all ordered pairs (a, b) such that there exists a rational function on $\mathcal{X}$ with polar divisor $aP_\infty + bP_0$. It generalizes the subsemigroup $H(P_\infty)$ of $\mathbb{N}$. The complement $G(P_\infty) = \mathbb{N} \backslash H(P_\infty)$ of gaps at P_∞ is of size g. The size of the complement $G(P_\infty, P_0) = \mathbb{N} \times \mathbb{N} \backslash H(P_\infty, P_0)$ does not depend on the genus alone. For the questions that we are interested in we extend $H(P_\infty, P_0)$ to the subsemigroup of $\mathbb{Z} \times \mathbb{Z}$ of nongaps at P_∞ and P_0. Thus

$$H(P_\infty, P_0) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \\ \exists f \in L(aP_\infty + bP_0) | \operatorname{ord}_{P_\infty} = -a, \operatorname{ord}_{P_0} = -b\}$$

The semigroup is contained in the halfplane $a + b \geq 0$, but not in the first quadrant. The complement $G(P_\infty, P_0) = \mathbb{Z} \times \mathbb{Z} \backslash H(P_\infty, P_0)$ is contained

in the halfplane $a + b \leq 2g - 1$. We extend the definition of the set Γ by Kim [51] to the subsemigroup of the full integer plane.

$$\Gamma(P_\infty, P_0) = \{(a,b) \in H(P_\infty, P_0) : \\ \text{for given } a,\ b \text{ is minimal with } (a,b) \in H(P_\infty, P_0)\}.$$

Proposition 1.3. *The set Γ is defined as the graph of a function $\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}$. The function σ is a permutation of the integers. If f is a nonzero rational function with $(f) = m(P_0 - P_\infty)$ then σ is determined by its images on a set of representatives for the integers modulo m.*

Proof. The pair (a,b) is in $\Gamma(P_\infty, P_0)$ if and only if $L(aP_\infty + bP_0) \neq L((a-1)P_\infty + bP_0)$ and $L(aP_\infty + (b-1)P_0) = L((a-1)P_\infty + (b-1)P_0)$ if and only if $L(aP_\infty + bP_0) \neq L(aP_\infty + (b-1)P_0)$ and $L((a-1)P_\infty + bP_0) = L((a-1)P_\infty + (b-1)P_0)$. That is, for given b, a is minimal with $(a,b) \in H(P_\infty, P_0)$. Clearly, if $(a,b) \in \Gamma$ then $(a+m, b-m) \in \Gamma$. □

We call the ordered pair $(a,b) \in \Gamma$ a discrepancy pair. A pair of integers (a,b) is a nongap if and only if the discrepancies (a,b') and (a',b) satisfy $b' \leq b$ and $a' \leq a$.

Lemma 1.7. *For two rational points P_∞, P_0 on the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$, there exists f with $(f) = (q+1)(P_0 - P_\infty)$. The set of discrepancies*

$$\Gamma(P_\infty, P_0) = \{(a_0(q+1) - a_1, -a_0(q+1) + a_1 q) : a_0 \in \mathbb{Z}, 0 \leq a_1 \leq q\}.$$

Proof. It suffice to consider $a_0 = 0, a_1 = 0, 1, \ldots, q$. The minimal choices correspond to functions $(y/x)^{a_1}$ with order $-a_1$ at P_∞ and qa_1 at $P_0 = (0,0)$. □

Lemma 1.8. *Write $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ as $(a_0(q+1) - a_1, b_0(q+1) - b_1)$ with $a_0, b_0 \in \mathbb{Z}$ and $0 \leq a_1, b_1, \leq q$. Then (a,b) is a nongap if and only if $a_1, b_1 \leq a_0 + b_0$.*

The following result was first obtained, in a different formulation and with a different proof, by Homma and Kim. We state the result as formulated by Beelen [3] and Park [65].

Theorem 1.37. *Let $G = K + aP_\infty + bP_0 \geq K + P_\infty + P_0$, where K is the canonical divisor, and write*

$$a = a_0(q+1) - a_1, \quad 0 \leq a_1 \leq q,$$
$$b = b_0(q+1) - b_1, \quad 0 \leq b_1 \leq q.$$

Let $d = d(C_\Omega(G,D))$ *and let* $d^* = \deg(G) - (2g-2) = a+b$.

(1)	$a_1, b_1 \le a_0 + b_0$,	$d = d^*$.
(2a)	$b_1 \le a_0 + b_0 \le a_1$,	$d = d^* + a_1 - (a_0 + b_0)$.
(2b)	$a_1 \le a_0 + b_0 \le b_1$,	$d = d^* + b_1 - (a_0 + b_0)$.
(3a)	$a_0 + b_0 \le a_1 \le b_1$ *and* $a_1 < q$,	$d = d^* + a_1 + b_1 - 2(a_0 + b_0)$.
(3b)	$a_0 + b_0 \le b_1 \le a_1$ *and* $b_1 < q$	$d = d^* + a_1 + b_1 - 2(a_0 + b_0)$.
(4)	$a_0 + b_0 \le a_1 = b_1 = q$	$d = d^* + q - (a_0 + b_0)$.

Proof. Let $H = (q+1)P_\infty$. For $a_0 + b_0 \le a_0 + b_0 + r < a_1$,

$$G + P_\infty = ((a_0 + b_0 + r)H - a_1 P_\infty) + ((q - 1 - r)H - qP_\infty - b_1 P_0)$$

is the sum of two gaps. For $a_0 + b_0 \le a_0 + b_0 + s < b_1$,

$$G + P_\infty = ((q - 1 - s)H - qP_\infty) + ((a_0 + b_0 + s)H - a_1 P_\infty - b_1 P_0)$$

is the sum of two gaps. Applying the coset bound Theorem 1.5 repeatedly, as in Theorem 1.6, gives a lower bound for the minimum distance that adds the number of pairs of gaps to the designed distance. The first group of pairs adds $a_1 - (a_0 + b_0)$ to cases (2a,3a,4). The second group adds $b_1 - (a_0 + b_0)$ to the case (3a). The cases (2b) and (3b) follow by symmetry. □

1.4.6. *Error correction*

For algebraic decoding it is important to have triples of codes A, B, C with $\sum a_i b_i c_i = 0$ for all $a \in A, b \in B, c \in C$. For a choice of error-locating code $A = C_L(F,D)$, the general formats we use are

(1) $A = C_L(F,D)$ $B = C_L(G-F,D)$ $C = C_\Omega(G,D)$.
(2) $A = C_L(F,D)$ $B = C_\Omega(G+F,D)$ $C = C_L(G,D)$.

The direct application of Theorems 1.7 and 1.8 to geometric Goppa codes is as follows. For $c \in C$, let $y = c + e$ be a received word such that e is nonzero in the error positions $Q = Q_1 + \ldots + Q_t$. For $\dim A > t$, there exists a nonzero $f \in L(F - Q)$, i.e. a nonzero function that vanishes in the error positions. The function f is obtained as a solution to the key equation.

(1) Find $f \in L(F)$: $\sum_i f(P_i)g(P_i)y_i = 0$, $\forall g \in L(G-F)$.
(2) Find $f \in L(F), h \in L(G+F)$: $f(P_i)y_i = h(P_i)$, for $i = 1, 2, \ldots, n$.

The key equations produce a nonzero $f \in L(F-Q)$ from which the codeword c can be uniquely decoded if

$$\begin{array}{ll} (1) & L(F-Q) \neq 0 \text{ and } \Omega(G-F-Q) = 0. \\ (2) & L(F-Q) \neq 0 \text{ and } L(G+F+Q-D) = 0. \end{array}$$

Two codes $C_\Omega(G,D)$ and $C_L(G^*,D)$ are equal if $G+G^* = (\eta)+D$, for a suitable differential η that depends on D but not on G and G^*. The two key equations are equivalent and lead to algorithms with the same performance. In particular, using the first with G and the second with $G^* = (\eta)+D-G$ leads to similar conditions for decoding the same codes.

Theorem 1.38. *(Basic algorithm) In both key equations, a choice of F with $\deg F = g+t$ will correctly decode a received word with $t \leq (d^*-1)/2 - g/2$ errors.*

Proof.

$$\begin{array}{ll} (1) & \deg(G-F-Q) \;=\; 2g-2+d^*-g-2t > 2g-2. \\ (2) & \deg(G+F+Q-D) \;=\; g+2t-d^* < 0. \end{array}$$

□

If decoding fails with the divisor F because $L(F-Q)=0$ then with little extra computational cost decoding can be attempted with the updated divisor $F+P_\infty$. For this process it is important that

$$\begin{array}{ll} (1) & L(F-Q) = 0 \;\Rightarrow\; \Omega(G-F-P_\infty-Q) = 0. \\ (2) & L(F-Q) = 0 \;\Rightarrow\; L(G+F+P_\infty+Q-D) = 0. \end{array}$$

Lemma 1.9. *For a pair of divisors A and B with $\deg B < \dim L(A+B)$*

$$L(B) \neq 0 \;\Rightarrow\; L(A) \neq 0$$

Proof. Assume $L(B) \neq 0$. Replacing B with an equivalent effective divisor if necessary, $\dim L(A+B) \leq \dim L(A) + \deg B$, and thus $L(A) \neq 0$.

□

Theorem 1.39. *(Modified algorithm) In both key equations, the implications necessary for updating the key equation from a choice F to a choice $F+P_\infty$ hold when*

$$t \leq (d^*-1)/2 + (\dim L(E) - 1) - \deg E/2,$$

where (1) $E = K-G+2F+P_\infty$, or (2) $E = G+2F+P_\infty-D$.

With the Riemann-Roch theorem, the defect is the same for E and for $K - E$,

$$\deg(E)/2 - (l(E) - 1) \;=\; \deg(K - E)/2 - (l(K - E) - 1).$$

A divisor is called special if both $L(E) \neq 0$ and $L(K - E) \neq 0$. Clifford's theorem gives that the defect is nonnegative when E is a special divisor.

For the Hermitian curve $K \sim (2g - 2)P_\infty$ and $D \sim nP_\infty$. For one-point codes with odd designed distance $d^* = 2t + 1$, if F goes through $tP_\infty, \ldots, (t+g)P_\infty$ then up to equivalence E goes through (1) $K, \ldots, 2P_\infty, 0$ or (2) $0, 2P_\infty, \ldots, K$.

Theorem 1.40. *The modified algorithm for one-point Hermitian codes from the curve $y^q + y = x^{q+1}$ corrects any number of errors $t \leq (d^* - 1)/2 - q(q-2)/8$.*

For the case $q = 4$, the defect is one and we present an example where an error of size $t = (d^* - 1)/2$ is decoded as an error of size $t + 1$ in the same coset.

Consider $X/\mathbb{F}_{16} : y^4 + y = x^5$. The evaluation of

$$f = x^9y + x^8y + x^8 + x^7y^2 + x^6 + x^5y^3 + x^5 + x^4y^3 + x^4y^2 + x^4 + x^3y^3 + x^3 + x^2y^3 + xy^3 + x + y^3$$

gives a word $c = (c_1, \ldots, c_{23}, 0, \ldots, 0) \in C_L(41P_\infty, D)$ of weight 23. The nonzero positions lie on the lines

$$\ell_1 : x = \alpha^5,\ \ell_2 : x = \alpha^{10},\ \ell_3 : y = (x + 1),\ \ell_4 : y = \alpha^5(x + 1),\ \ell_5 : y = \alpha^{10}(x + 1).$$

Let

$$Q_1 = (\ell_1 - P_\infty) + (\ell_2 - P_\infty) + (\ell_3 - (0, 1)) \sim 13P_\infty - (0, 1).$$
$$Q_2 = \ell_4 + \ell_5 + (0, 1) \sim 10P_\infty + (0, 1).$$

The vanishing ideals for Q_1 and Q_2 are generated by

$$Q_1 : (x^5 + y^4 + y, f_1 = x^2y + \cdots, g_1 = x^6 + \cdots),$$
$$Q_2 : (x^5 + y^4 + y, f_2 = x^2y^2 + \cdots, g_2 = y^3 + \cdots).$$

$-$	1	y	y^2	y^3	y^4	y^5	y^6	$\cdots$
1	$-$	$-$	$-$	$-$	$-$	$+$	$+$	$\cdots$
x	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$\cdots$
x^2	$-$	$+$	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^3	$-$	$+$	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^4	$-$	$+$	$+$	$+$	$+$	$+$	$+$	$\cdots$

$-$	1	y	y^2	y^3	y^4	y^5	y^6	$\cdots$
1	$-$	$-$	$-$	$+$	$+$	$+$	$+$	$\cdots$
x	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^2	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^3	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^4	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$\cdots$

If the word $c = (c_1, \ldots, c_{23}, 0, \ldots, 0)$ is received as $(c_1, \ldots, c_{12}, 0, \ldots, 0)$, with errors in the eleven positions corresponding to Q_2, then the modified algorithm finds the smallest error-locating function f_1 for Q_1 before it finds the smallest error-locating function f_2 for Q_2, and the word is decoded as the allzero word. Among the functions that solve the key equation, there are functions with leading monomial x^2y, x^3y, x^4y that locate Q_1 and functions with leading monomials xy^2, y^3, xy^3, y^4 that locate Q_2. Assuming that the codeword is of the form $s \cdot x^9y + \cdots$, for a given $s \in \mathbb{F}$, we can add one more constraint to the key equation. The functions with leading monomial x^2y, x^3y, x^4y remain valid only when $s = 0$. The functions with leading monomials xy^2, y^3, xy^3, y^4 remain valid only when $s = 1$. None of the seven functions remains valid when $s \neq 0, 1$. The number of errors t is therefore at least 11 if $s = 1$, at least 12 if $s = 0$ and at least 15 if $s \neq 0, 1$. The decoder should therefore first explore the case $s = 1$ which in this case leads to the closest codeword.

	1	y	y^2	y^3	y^4	y^5	y^6	$\cdots$
1	0	1	1	1	0	1	1	$\cdots$
x	1	1	0	1	0	0	$s?$	$\cdots$
x^2	0	0	0	1	1	0	.	$\cdots$
x^3	0	0	0	0	1	.	.	$\cdots$
x^4	0	1	0	1	1	.	.	$\cdots$

	1	y	y^2	y^3	y^4	y^5	y^6	$\cdots$
1	$-$	$-$	$-$	?	?	$+$	$+$	$\cdots$
x	$-$	$-$	?	?	$+$	$+$	$+$	$\cdots$
x^2	$-$	?	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^3	$-$	?	$+$	$+$	$+$	$+$	$+$	$\cdots$
x^4	$-$	?	$+$	$+$	$+$	$+$	$+$	$\cdots$

1.4.7. *Secret reconstruction for algebraic-geometric LSSSs*

An ideal $\mathbb{F}$-linear secret sharing scheme $\Sigma = \Sigma_0(\Pi)$ on the set of players $\{1, 2, \ldots, n\}$ is defined as an $\mathbb{F}$-linear map $\Pi : E \longrightarrow \mathbb{F}^{n+1}$. For $x \in E$, the values $\pi_1(x), \ldots, \pi_n(x) \in \mathbb{F}$ are the shares of the secret value $\pi_0(x) \in \mathbb{F}$. We recast the main properties of a linear secret sharing scheme in the language of geometric Goppa codes. We also show that every geometric Goppa code can be decoded up to half the designed distance.

Let $\mathcal{X}/\mathbb{F}$ be a curve. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n rational points and let P_0 be a fixed rational point not in $\mathcal{P}$. For a choice of divisor G, define an algebraic geometric LSSS $\Sigma = \Sigma_0(G, \mathcal{P})$ with the $\mathbb{F}-$linear map $\alpha_L : L(G) \longrightarrow \mathbb{F}^{n+1}$. For $f \in L(G)$, the values $f(P_1), \ldots, f(P_n) \in \mathbb{F}$ are the shares of the secret value $f(P_0) \in \mathbb{F}$.

Lemma 1.10. *For G of degree $\deg G = 2g + t$, the AG-LSSS $\Sigma_0(G, \mathcal{P})$ rejects any subset of size at most t and accepts any subset of size at least $t + 2g + 1$.*

Proof. A subset $A = \{Q_1, \ldots, Q_a\} \subset \mathcal{P}$ is unqualified if and only if $L(G - A) \neq L(G - A - P_0)$. The latter holds for all $a \leq t$ and fails for all $a \geq t + 2g + 1$. □

For a different proof, that uses Riemann's Theorem, let $f_0, \ldots, f_g \in L(G - Q_1 \cdots - Q_t)$ be functions with increasing orders of vanishing at P_0 in the range $\{0, \ldots, 2g\}$. And let $h_0, \ldots, h_g \in L(2gP_0)$ be functions with increasing pole order at P_0 in the range $\{0, \ldots, 2g\}$. By the pigeonhole principle there exist f_i and g_j such that $f_i g_j$ is a unit at P_0.

For a proof that uses Riemann's theorem in combination with Theorem 1.12, let $f_0, f_1, \ldots, f_{g+t} \in L(G)$ be functions with increasing orders of vanishing at P_0 in the range $\{0, \ldots, 2g+t\}$. And let $g_0, \ldots, g_{g+t} \in L((2g+t)P_0)$ be functions with increasing pole order at P_0 in the range $\{0, \ldots, 2g+t\}$. By the pigeonhole principle there exist subsequences $f'_0, \ldots, f'_t$ and $g'_0, \ldots, g'_t$ such that

$$\begin{cases} f'_i * g'_j \in L(G - P_0) & \text{for } i + j < t. \\ f'_i * g'_j \in L(G) \backslash L(G - P_0) & \text{for } i + j = t. \end{cases}$$

Now apply Theorem 1.12. The last proof shows that in special cases the rejection threshold can be higher depending on the vanishing orders at P_0 of the divisor G. The following theorem appears in [9].

Theorem 1.41. *For a divisor G of degree $\deg G = 2g + t$, and for a set of rational points $\mathcal{P}$ of size n, the AG-LSSS $\Sigma_0(G, \mathcal{P})$ is multiplicative in $n - t$ positions (resp. strongly multiplicative) if $3t < n - 4g$ (resp. $3t < n - 6g$).*

Proof. A subset of $n - t$ players can interpolate the product fg of two functions $f, g \in L(G)$ if $2\deg G < n - t$, that is if $3t < n - 4g$. Unqualified subsets for Σ are of size at most $t + 2g$. Strong multiplication is guaranteed if the dual code $C_L(G', D + P_0)$ of $C_L(2G, D + P_0)$ rejects all subsets of size

$t + 2g$. This is the case if $\deg G' = n + 1 + 2g - 2 - 2\deg G \geq 4g + t$, that is if $3t < n - 6g$. □

The theorem shows that for a curve $\mathcal{X}/\mathbb{F}$ of genus g with N rational points, and for $3t+4g < n \leq N-1$, there exist linear secret sharing schemes $\Sigma = \Sigma_0(G, \mathcal{P})$ on n participants such that

- Σ reject all subsets of size t, and
- Σ reconstructs products of secrets from any $n - t$ products of shares.

One of the main results in [9] is that efficient linear secret sharing schemes for an increasing number of participants can be constructed over a small base field using asymptotically good families of curves.

Strong multiplication can be realized with the weaker bound $3t+4g < n$ by choosing the divisor G of degree $2g + t$ such that $\Sigma_0(G, \mathcal{P})$ is trilinear, i.e. such that $C_L(G, D + P_0)$ is essentially orthogonal to $C_L(2G, D + P_0)$. This gives the following generalization of a Shamir secret sharing scheme (Theorem 1.14).

Theorem 1.42. *For a divisor G such that there exists a differential η with $(\eta) = 3G - D - P_0$, the AG-LSSS $\Sigma_0(G, \mathcal{P})$ is trilinear.*

We give such a choice for the Hermitian curve $\mathcal{X}/\mathbb{F}_{16} : Y^4Z+YZ = X^5$. It has 65 rational points that form a complete intersection $X = \mathcal{P}$ with a-invariant $a = q - 1 = 15$. The LSSS $\Sigma(\hat{C})$ defined with the Reed-Muller code $\hat{C} = RM(\nu = 5, X = \mathcal{P})$ is trilinear. The Reed-Muller code is equivalent to a geometric Goppa code defined with a divisor $G \sim 5L$. The curve has parameters $N = 65$ and $g = 6$, the code $\hat{C}$ is of type $[65, 20, 40]$, and the scheme $\Sigma(\hat{C})$ has parameters $n = 64$ and $t = 13$.

For a LSSS $\Sigma_0(G, \mathcal{P})$ with $\deg G \leq n - (2t + 1)$, any two vectors of shares differ in at least $2t + 1$ positions. If at most t shares are corrupted then it is a priori possible to detect the corrupted shares and to determine their correct value. The assumption $4g + 2t = 2\deg G < n - t$ that is used for schemes that are multiplicative in $n - t$ positions corresponds to the much weaker $\deg G \leq n - (2t + 1) - 2g$.

For a LSSS $\Sigma_0(G, \mathcal{P})$ with $\deg G \leq n - (2t + 1) - 2g$, correcting t corrupted shares is straightforward with the key equation in Theorem 1.9. Let $(s_1, \ldots, s_n)$ be a vector of possibly corrupted shares that differs in at

most t positions from the vector $(f(P_1), \ldots, f(P_n))$, for $f \in L(G)$.. After choosing a suitable divisor F, we solve for $g \in L(F)$ and $h \in L(G+F)$ such that $g(P_i)s_i = h(P_i)$ for $i = 1, \ldots, n$. The function f is recovered as $f = h/g$. The procedure succeeds if the corrupted positions $Q = Q_1 + \ldots + Q_t$ satisfy

$$L(F - Q) \neq 0 \quad \text{and} \quad L(G + F + Q - D) = 0.$$

The conditions hold for $t + g \leq \deg F \leq t + 2g$. The choice $\deg F = t + g$ gives a key equation with smallest number of variables and this is the most efficient choice. For F of degree $\deg F = t+3g/2$, both conditions hold with $\deg Q = t+g/2$. This choice corrects the largest number of corrupted shares. For $\deg F = t + 2g$, and in particular for $F = G$, only up to t corrupted shares can be corrected but there exists a solution for g with $g(P_0) \neq 0$ and in that case the secret can be recovered as $f(P_0) = h(P_0)/g(P_0)$. The last choice corresponds to the reconstruction procedure in [12] for a general LSSS. The constraint $g(P_0) \neq 0$ is not needed for an AG-LSSS if we evaluate the secret as $f(P_0) = (h/g)(P_0)$.

To correct t corrupted shares in a LSSS $\Sigma = \Sigma_0(G, \mathcal{P})$ with $\deg G \leq n - (2t + 1)$, we use the procedure in Theorem 1.13. The procedure makes use of two schemes $\Sigma' = \Sigma_0(F, \mathcal{P})$ and $\Sigma'' = \Sigma_0(F^*, \mathcal{P})$ such that $C_L(F + F^*, \mathcal{P} + P_0)$ is orthogonal to $C_L(G, \mathcal{P} + P_0)$. Let $f \in L(G)$. If $(s_1, \ldots, s_n)$ is a vector that differs from the vector $(f(P_1), \ldots, f(P_n))$ in the positions $Q = Q_1 + \ldots + Q_t$, then the procedure returns the correct value for $f(P_0)$ if

$$L(F - Q) \neq L(F - Q - P_0) \quad \text{and} \quad L(F^* - Q) \neq L(F^* - Q - P_0).$$

If one of the conditions fails the procedure may not return a value. An incorrect value is returned only if

$$L(F - Q) = L(F - Q - P_0) \quad \text{and} \quad L(F^* - Q) = L(F^* - Q - P_0).$$

Theorem 1.43. *Let $C = C_L(G, \mathcal{P})$ be a geometric Goppa code of length n with divisor G of degree $\deg G = n - (2t + 1)$. Let P_0 be a point not in $\mathcal{P}$. For $f \in L(G)$, let $(s_1, \ldots, s_n)$ be a vector that differs in no more than t positions from the vector $(f(P_1), \ldots, f(P_n))$. Among the values for $f(P_0)$ that are returned by the reconstruction procedure when it is applied with $F = tP_0, \ldots, (t + 2g)P_0$, the correct value for $f(P_0)$ outnumbers any other value.*

Proof. $\dim L((t+2g)P_0 - Q) - \dim L(tP_0 - Q - P_0) = g + 1$. For $F = tP_0, \ldots, (t+2g)P_0$, the condition $L(F-Q) \neq L(F-Q-P_0)$ holds $g+1$ times and fails g times. The matching divisor F^* similarly meets the condition $L(F^* - Q) \neq L(F^* - Q - P_0)$ exactly $g+1$ times and fails it g times. With the pigeonhole principle, both conditions hold, and the correct value is returned, at least once. Moreover, the number of times that an incorrect value is returned is at most the number of times that both conditions fail which is one less than the number of times that both conditions hold. □

1.4.8. *Weight distributions*

Weight distributions of linear codes are in general hard to determine. The extra structure of geometric Goppa codes makes it possible to approach their weight distribution as a distribution problem of effective divisors over divisor classes and to benefit from the group structure on the divisor classes. For a code $C_L(G, D)$ with injective encoding map $L(G) \longrightarrow C_L(G, D)$, words of weight w correspond to functions in $L(G)$ with $n - w$ zeros in D. The correspondence between nonzero words of weight w and effective divisors in the class of G that intersect D in $n - w$ points is $(q-1)$-to-one. Thus, in order to determine weight distributions, we may consider all effective divisors of a given degree that intersect D in a given number of points and their distribution over the finitely many divisor classes of that degree.

The main tools for pursuing the above approach are zeta functions, to study divisor distributions, and Fourier analysis over the finite group of divisor classes of degree zero. In this section we show that the weight distributions of the codes $C_L(G, D)$, where G runs over a full set of inequivalent divisors $G_1, G_2, \cdots, G_h$ of the same degree, have an average weight distribution that depends only on the zeta function of the curve and the degrees of the divisors G and D. The error terms for each individual weight distribution are controlled by the $L-series$ $L(T, \chi)$, where $\chi = \chi_1, \ldots, \chi_h$ is an unramified character of the function field.

Let $K = \mathbb{F}(\mathcal{X})$ be the function field of $\mathcal{X}$ and let $\mathcal{P}_K$ be the set of all the places of K. The *group of divisors* $D(K)$ is the free abelian group generated by the set of places $\mathcal{P}_K$. The principal divisors (f), for a nonzero $f \in K$, form a subgroup $P(K)$ of $D(K)$. The quotient $D(K)/P(K)$ is the *divisor class group* $C(K)$. The group $C(K)$ is finitely generated of the form $\Gamma \times \mathbb{Z}$. The finite torsion subgroup Γ is the group of divisor classes of degree zero.

The set of places $\mathcal{P}_K$ generates the *semigroup of effective divisors* $E(K)$. For a fixed divisor class E of degree one, let

$$L(T) = \sum_{a \geq 0} \sum_{g \in \Gamma} |(g + aE) \cap E(K)| \, X^g T^a$$

be a generating function for the number of effective divisors in the divisor class $g + aE$. Let $\{e_\chi : \chi \in \hat{\Gamma}\}$ be a basis of primitive idempotents for $\mathbb{C}\Gamma$,

$$e_\chi = \frac{1}{|\Gamma|} \sum_{g \in \Gamma} \chi(-g) X^g,$$

so that $X^g \, e_\chi = \chi(g) \, e_\chi$. Define coordinate functions $L(T, g), L(T, \chi) \in \mathbb{C}[[T]]$ via

$$L(T) = \sum_g L(T, g) X^g = \sum_\chi L(T, \chi) e_\chi.$$

The function $L(T, g)$ is a generating function for the number of effective divisors in the divisor class $g + aE$, for $a \geq 0$. The function $L(T, \chi)$ is a Dirichlet L-series for a Dirichlet character of trivial conductor. For a non-trivial character χ, $L(T, \chi)$ is a polynomial of degree $2g - 2$ with cyclotomic integer coefficients. For the trivial character χ_0, $L(T, \chi_0) = Z(T)$ is the zeta function of the curve. For a rational place P, let $g_P + E$ be the divisor class of P, for $g_P \in \Gamma$. For a subset $\mathcal{P}$ of rational places, define

$$\Lambda(T) = \prod_{P \in \mathcal{P}} (1 + X^{g_P} T) \in \mathbb{C}\Gamma[T],$$

with coordinate functions

$$\Lambda(T) = \sum_g \Lambda(T, g) X^g = \sum_\chi \Lambda(T, \chi) e_\chi.$$

Theorem 1.44. *The distribution over divisor classes of effective divisors that contain precisely a given number of elements from $\mathcal{P}$ is given by*

$$A(U, T) = L(T)\Lambda(U - T) \in \mathbf{C}\Gamma[U](T).$$

The coordinate function $A(U, T, g) \in \mathbf{C}[U][[T]]$ is the generating function for the number of effective divisors in the divisor class $g + (i + j)E$ with precisely i elements of $\mathcal{P}$ in the support.

Proof. The generating function $L(T)$ has an Euler product decomposition. The contribution of $P \in \mathcal{P}$ to $A(U, T)$ is, with $g = g_P$,

$$\frac{1 + X^g(U - T)}{1 - X^g T} = 1 + X^g U + X^{2g} UT + X^{3g} UT^2 + \cdots .$$

Hence the variable U keeps track of the precise number of places $P \in \mathcal{P}$ that contribute to a term of $A(U,T)$. □

To compute weight distributions with the theorem we compute the coordinate functions $A(U,T,\chi) = L(T,\chi)\Lambda(U-T,\chi)$ on the basis of idempotents and apply an inverse Fourier transform to recover coordinate functions $A(U,T,g)$ for $A(U,T)$. The top row in the table below gives the weight distribution for a code of type $[24,16,7]$ over $\mathbb{F}_8$ constructed with the Klein curve. The method outlined here produces the weight distributions for all $2744 = 14^3$ codes of type $[24,16]$ on the Klein curve. For the code and its dual, only the weights below the Singleton bound are listed. Using only the contribution of the trivial character $\chi = \chi_0$ gives the average weight distribution for codes defined with inequivalent divisors of the same degree.

$$\frac{1}{|\Gamma|}\sum_g A(U,T,g) = \frac{1}{|\Gamma|}Z(T)(1+U-T)^n.$$

Table 1.3. Weight distributions for the 2744 distinct $[24,16,\geq 6]$ codes on the Klein quartic over $\mathbb{F}_8$.

	Small weights			Small dual weights		
#	$\bar{A}_6$	$\bar{A}_7$	$\bar{A}_8$	$\bar{A}^\perp_{14}$	$\bar{A}^\perp_{15}$	$\bar{A}^\perp_{16}$
1	0	2520	37620	696	4200	11340
7	52	2184	38643	852	3720	11907
24	35	2170	38709	672	4329	11753
24	56	2138	37968	707	4469	10846
168	38	2167	38642	683	4312	11752
168	60	2131	37896	745	4278	11276
168	47	2190	38106	735	4212	11544
168	53	2136	38340	747	4167	11643
126	52	2104	38430	692	4404	11378
126	40	2176	38280	660	4484	11336
252	60	2060	38537	729	4246	11718
504	48	2140	38288	692	4374	11506
504	49	2154	38336	731	4222	11558
504	46	2165	38348	717	4272	11478
avg	49.1	2144.2	38328.1	714.7	4288.5	11525.2

Computed as an inverse Fourier transform of the unramified $L-$series of the curve.

1.5. Bibliographic notes

There are many textbooks for coding theory, including [4], [48], [55], [57]. The books [5], [36], [44], [49], [54], [62], [68], [71], [72], [75], [77], [79], as well as the survey chapters [10], [42], [45], [47], discuss algebraic geometry codes, each with a distinct approach and emphasis. We give a few more references for the topics discussed in this chapter. Roos bound for the minimum distance [22], Linear secret sharing schemes [12], Weight distributions and codes over extension fields [21], [76], Dual BCH codes [20], [32], [69], Codes from the Klein and Suzuki curves [8], [17], [33], [39], [61], Floor bound [7], [58], [56], Explicit towers [1], [11], [25], [30], [31], [59], [70], [78], One-point codes [29], [52], [80], Two-point codes [2], [3], [46], [51], [60], [65], Error correction [13], [23], [37], [38], [66], Secret reconstruction for algebraic-geometric LSSSs [9], [10], [14], Weight distributions [18].

References

[1] P. Beelen and I. I. Bouw, Asymptotically good towers and differential equations, *Compos. Math.* **141**(6), 1405–1424, (2005).
[2] P. Beelen and N. Tutaş, A generalization of the Weierstrass semigroup, *J. Pure Appl. Algebra.* **207**(2), 243–260, (2006).
[3] P. Beelen, The order bound for general algebraic geometric codes, *Finite Fields Appl.* **13**(3), 665–680, (2007).
[4] J. Bierbrauer, *Introduction to coding theory.* Discrete Mathematics and its Applications (Boca Raton), (Chapman & Hall/CRC, Boca Raton, FL, 2005).
[5] R. E. Blahut, *Algebraic codes on lines, planes, and curves: an engineering approach.* (Cambridge University Press, Cambridge, 2008)
[6] A. Blokhuis, A. Brouwer, and H. Wilbrink, Hermitian unitals are code words, *Discrete Math.* **97**(1-3), 63–68, (1991).
[7] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, *Des. Codes Cryptogr.* **35**(2), 211–225, (2005).
[8] C.-Y. Chen and I. M. Duursma, Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$, *IEEE Trans. Inform. Theory.* **49**(5), 1351–1353, (2003).
[9] H. Chen and R. Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *CRYPTO*, pp. 521–536, (2006).
[10] H. Chen, Algebraic geometric codes with applications, *Front. Math. China.* **2**(1), 1–11, (2007).
[11] H. Cohn, *Introduction to the construction of class fields.* Cambridge Studies in Advanced Mathematics volume 6 (Cambridge University Press, Cambridge, 1985). Reprint by (Dover Publications Inc., New York, 1994).
[12] R. Cramer, V. Daza, I. Gracia, J. J. Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids and secure multi-party computation from

linear secret sharing schemes. In *Advances in cryptology—CRYPTO 2005*, vol. 3621, *Lecture Notes in Comput. Sci.*, pp. 327–343. Springer, Berlin, (2005).

[13] I. M. Duursma, Algebraic decoding using special divisors, *IEEE Trans. Inform. Theory.* **39**(2), 694–698, (1993).

[14] I. M. Duursma, Majority coset decoding, *IEEE Trans. Inform. Theory.* **39** (3), 1067–1070, (1993).

[15] I. M. Duursma, *Decoding codes from curves and cyclic codes.* (Technische Universiteit Eindhoven, Eindhoven, 1993). Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1993.

[16] I. M. Duursma and R. Kötter, Error-locating pairs for cyclic codes, *IEEE Trans. Inform. Theory.* **40**(4), 1108–1121, (1994).

[17] I. M. Duursma, Monomial embeddings of the Klein curve, *Discrete Math.* **208/209**, 235–246, (1999). Combinatorics (Assisi, 1996).

[18] I. M. Duursma, Weight distributions of geometric Goppa codes, *Trans. Amer. Math. Soc.* **351**(9), 3609–3639, (1999).

[19] I. M. Duursma, C. Rentería, and H. Tapia-Recillas, Reed-Muller codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.* **11**(6), 455–462, (2001).

[20] I. M. Duursma, Preparata codes through lattices, *IEEE Trans. Inform. Theory.* **47**(1), 36–44, (2001).

[21] I. M. Duursma. Combinatorics of the two-variable zeta function. In *Finite fields and applications*, vol. 2948, *Lecture Notes in Comput. Sci.*, pp. 109–136. Springer, Berlin, (2004).

[22] I. M. Duursma and R. Pellikaan, A symmetric Roos bound for linear codes, *J. Combin. Theory Ser. A.* **113**(8), 1677–1688, (2006).

[23] D. Ehrhard. Decoding algebraic-geometric codes by solving a key equation. In *Coding theory and algebraic geometry (Luminy, 1991)*, vol. 1518, *Lecture Notes in Math.*, pp. 18–25. Springer, Berlin, (1992).

[24] D. Ehrhard, Achieving the designed error capacity in decoding algebraic-geometric codes, *IEEE Trans. Inform. Theory.* **39**(3), 743–751, (1993).

[25] N. D. Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (Univ. of Illinois at Urbana-Champaign.*

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

[27] N. D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, vol. 202, *Progr. Math.*, pp. 189–198. Birkhäuser, Basel, (2001).

[28] G. L. Feng and T. R. N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. Inform. Theory.* **39**(1), 37–45, (1993).

[29] A. García, S. J. Kim, and R. F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, *J. Pure Appl. Algebra.* **84**(2), 199–207, (1993).

[30] A. García and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladuts bound, *Invent. Math.* **121**(1), 211–222, (1995).
[31] A. Garcia and H. Stichtenoth. Explicit towers of function fields over finite fields. In *Topics in geometry, coding theory and cryptography*, vol. 6, *Algebr. Appl.*, pp. 1–58. Springer, Dordrecht, (2007).
[32] G. van der Geer, R. Schoof, and M. van der Vlugt, Weight formulas for ternary Melas codes, *Math. Comp.* **58**(198), 781–792, (1992).
[33] M. Giulietti, G. Korchmáros, and F. Torres, Quotient curves of the Suzuki curve, *Acta Arith.* **122**(3), 245–274, (2006).
[34] V. D. Goppa, Decoding and Diophantine approximations, *Problems of Control and Information Theory/Problemy Upravlenija i Teorii Informacii.* **5** (3), 195–206, (1976).
[35] V. D. Goppa, Codes on algebraic curves, *Dokl. Akad. Nauk SSSR.* **259**(6), 1289–1290, (1981).
[36] V. D. Goppa, *Geometry and codes.* vol. 24, *Mathematics and its Applications (Soviet Series)*, (Kluwer Academic Publishers Group, Dordrecht, 1988). Translated from the Russian by N. G. Shartse.
[37] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE Trans. Inform. Theory.* **45**(6), 1757–1767, (1999).
[38] V. Guruswami and A. C. Patthak, Correlated algebraic-geometric codes: improved list decoding over bounded alphabets, *Math. Comp.* **77**(261), 447–473 (electronic), (2008).
[39] J. P. Hansen and H. Stichtenoth, Group codes on certain algebraic curves with many rational points, *Appl. Algebra Engrg. Comm. Comput.* **1**(1), 67–77, (1990).
[40] J. P. Hansen and J. P. Pedersen, Automorphism groups of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.* **440**, 99–109, (1993).
[41] J. P. Hansen, Linkage and codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.* **14**(3), 175–185, (2003).
[42] J. W. P. Hirschfeld. Linear codes and algebraic curves. In *Geometrical combinatorics (Milton Keynes, 1984)*, vol. 114, *Res. Notes in Math.*, pp. 35–53. Pitman, Boston, MA, (1984).
[43] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. The number of points on an algebraic curve over a finite field. In *Surveys in combinatorics 2007*, vol. 346, *London Math. Soc. Lecture Note Ser.*, pp. 175–200. Cambridge Univ. Press, Cambridge, (2007).
[44] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field.* (Princeton University Press, Princeton, 2008)
[45] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry of codes. In *Handbook of coding theory, Vol. I, II*, pp. 871–961. North-Holland, Amsterdam, (1998).
[46] M. Homma and S. J. Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, *Des. Codes Cryptogr.* **40**

(1), 5–24, (2006).
[47] W.-b. Hu and C.-p. Xing, A survey on algebraic-geometry codes, *Adv. Math. (China)*. **35**(6), 641–656, (2006).
[48] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. (Cambridge University Press, Cambridge, 2003).
[49] N. E. Hurt, *Many rational points. Coding theory and algebraic geometry* Mathematics and its Applications, 564. (Kluwer Academic Publishers, Dordrecht, 2003)
[50] J. D. Key, Hermitian varieties as codewords, *Des. Codes Cryptogr.* **1**(3), 255–259, (1991).
[51] S. J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve, *Arch. Math.* **62**(1), 73–82, (1994).
[52] C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inform. Theory*. **41**(6, part 1), 1720–1732, (1995). Special issue on algebraic geometry codes.
[53] K. Lauter, Deligne-Lusztig curves as ray class fields, *Manuscripta Math.* **98** (1), 87–96, (1999).
[54] J. H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*. vol. 12, *DMV Seminar*, (Birkhäuser Verlag, Basel, 1988).
[55] J. H. van Lint, *Introduction to coding theory*. vol. 86, *Graduate Texts in Mathematics*, (Springer-Verlag, Berlin, 1999), third edition.
[56] B. Lundell and J. McCullough, A generalized floor bound for the minimum distance of geometric Goppa codes, *J. Pure Appl. Algebra* **207**(1), 155–164, (2006).
[57] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. (North-Holland Publishing Co., Amsterdam, 1977). North-Holland Mathematical Library, Vol. 16.
[58] H. Maharaj and G. L. Matthews, On the floor and the ceiling of a divisor, *Finite Fields Appl.* **12**(1), 38–55, (2006).
[59] H. Maharaj. Explicit towers and codes. In *Recent trends in coding theory and its applications*, vol. 41, *AMS/IP Stud. Adv. Math.*, pp. 35–71. Amer. Math. Soc., Providence, RI, (2007).
[60] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, *Des. Codes Cryptogr.* **22**(2), 107–121, (2001).
[61] G. L. Matthews, Codes from the Suzuki function field, *IEEE Trans. Inform. Theory*. **50**(12), 3298–3302, (2004).
[62] C. Moreno, *Algebraic curves over finite fields*. vol. 97, *Cambridge Tracts in Mathematics*, (Cambridge University Press, Cambridge, 1991).
[63] H. Niederreiter and C. P. Xing, Low-discrepancy sequences obtained from algebraic function fields over finite fields, *Acta Arith.* **72**(3), 281–298, (1995).
[64] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*. vol. 285, *London Mathematical Society Lecture Note Series*, (Cambridge University Press, Cambridge, 2001).
[65] S. Park, *Applications of algebraic curves to cryptography*, Thesis (University of Illinois, Urbana, 2007).
[66] F. Parvaresh and A. Vardy. Correcting errors beyond the guruswami-sudan

radius in polynomial time. In *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science (FOCS), 2005*.

[67] J. P. Pedersen. A function field related to the Ree group. In *Coding theory and algebraic geometry (Luminy, 1991)*, vol. 1518, *Lecture Notes in Math.*, pp. 122–131. Springer, Berlin, (1992).

[68] O. Pretzel, *Codes and algebraic curves*. vol. 8, *Oxford Lecture Series in Mathematics and its Applications*, (The Clarendon Press Oxford University Press, New York, 1998).

[69] R. Schoof, Families of curves and weight distributions of codes, *Bull. Amer. Math. Soc. (N.S.)*. **32**(2), 171–183, (1995).

[70] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolaikar, A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound, *IEEE Trans. Inform. Theory*. **47** (6), 2225–2241, (2001).

[71] S. A. Stepanov, *Codes on algebraic curves*. (Kluwer Academic/Plenum Publishers, New York, 1999).

[72] H. Stichtenoth, *Algebraic function fields and codes*. Universitext, (Springer-Verlag, Berlin, 1993).

[73] H. Stichtenoth and C. Xing, Excellent nonlinear codes from algebraic function fields, *IEEE Trans. Inform. Theory*. **51**(11), 4044–4046, (2005).

[74] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109**, 21–28, (1982).

[75] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*. vol. 58, *Mathematics and its Applications (Soviet Series)*, (Kluwer Academic Publishers Group, Dordrecht, 1991). Translated from the Russian by the authors.

[76] M. A. Tsfasman and S. G. Vlăduţ, Geometric approach to higher weights, *IEEE Trans. Inform. Theory*. **41**(6, part 1), 1564–1588, (1995). Special issue on algebraic geometry codes.

[77] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic geometric codes: basic notions*. vol. 139, *Mathematical Surveys and Monographs*, (American Mathematical Society, Providence, RI, 2007).

[78] C. Voss and T. Høholdt, An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound: the first steps, *IEEE Trans. Inform. Theory*. **43**(1), 128–135, (1997).

[79] J. L. Walker, *Codes and curves*. vol. 7, *Student Mathematical Library*, (American Mathematical Society, Providence, RI, 2000). IAS/Park City Mathematical Subseries.

[80] K. Yang and P. V. Kumar. On the true minimum distance of Hermitian codes. In *Coding theory and algebraic geometry (Luminy, 1991)*, vol. 1518, *Lecture Notes in Math.*, pp. 99–107. Springer, Berlin, (1992).

[81] C. Xing, Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound, *IEEE Trans. Inform. Theory*. **49**(7), 1653–1657, (2003).