8

More about Algebraic Geometry Codes

In Chapter 2 we studied algebraic geometry (AG) codes associated with divisors of an algebraic function field over $\mathbb{F}_q$. Here we continue their investigation. Let us fix some notation for the whole of Chapter 8.

$F/\mathbb{F}_q$ is an algebraic function field of genus g and $\mathbb{F}_q$ is the full constant field of F.

$P_1, \ldots, P_n \in \mathbb{P}_F$ are pairwise distinct places of degree one.

$D = P_1 + \ldots + P_n$.

G is a divisor of F with $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$.

$C_{\mathscr{L}}(D,G) = \{(x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n \,|\, x \in \mathscr{L}(G)\}$ is the algebraic geometry code associated with D and G.

$C_\Omega(D,G) = \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \,|\, \omega \in \Omega_F(G-D)\}$ is the dual code of $C_{\mathscr{L}}(D,G)$.

8.1 The Residue Representation of $C_\Omega(D,G)$

Let $P \in \mathbb{P}_F$ be a place of degree one and let $\omega \in \Omega_F$ be a Weil differential. In Chapter 4 we identified Ω_F with the differential module Δ_F (cf. Remark 4.3.7(a)). Via this identification the local component of ω at the place P can be evaluated by means of the residue of ω at P, namely $\omega_P(u) = \operatorname{res}_P(u\omega)$ for all $u \in F$ (Theorem 4.3.2(d)). In particular we have $\omega_P(1) = \operatorname{res}_P(\omega)$. Hence we have the following alternative description of the code $C_\Omega(D,G)$.

Proposition 8.1.1.

$$C_\Omega(D,G) = \{(\operatorname{res}_{P_1}(\omega), \ldots, \operatorname{res}_{P_n}(\omega)) \,|\, \omega \in \Omega_F(G-D)\}\,.$$

It is this representation that is most commonly used in the literature to define the code $C_\Omega(D,G)$.

H. Stichtenoth, *Algebraic Function Fields and Codes*,
Graduate Texts in Mathematics 254,

By Proposition 2.2.10 the code $C_\Omega(D,G)$ can also be written as $C_{\mathscr{L}}(D,H)$ where $H = D-G+(\eta)$ and η is a differential with $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $i = 1,\dots,n$. Using results from Chapter 4 one can easily construct such a differential η.

Proposition 8.1.2. *Let t be an element of F such that $v_{P_i}(t) = 1$ for $i = 1,\dots,n$. Then the following hold:*
(a) The differential $\eta := dt/t$ satisfies $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1,\dots,n$.
(b) $C_\Omega(D,G) = C_{\mathscr{L}}\big(D, D-G+(dt)-(t)\big)$.

Proof. (a) Since t is a prime element of $P := P_i$, the P-adic power series of $\eta = dt/t$ with respect to t is

$$\eta = \frac{1}{t}\, dt\,.$$

Hence $v_P(\eta) = -1$ and $\mathrm{res}_P(\eta) = 1$.
(b) Follows immediately from (a) and Proposition 2.2.10. □

Corollary 8.1.3. *Suppose that $t \in F$ is a prime element for all places $P_1,...,P_n$.*
(a) If $2G - D \le (dt/t)$ then the code $C_{\mathscr{L}}(D,G)$ is self-orthogonal; i.e.,

$$C_{\mathscr{L}}(D,G) \subseteq C_{\mathscr{L}}(D,G)^{\perp}\,.$$

(b) If $2G - D = (dt/t)$ then $C_{\mathscr{L}}(D,G)$ is self-dual.

Proof. This is an immediate consequence of Corollary 2.2.11. □

8.2 Automorphisms of AG Codes

The symmetric group $\mathcal{S}_n$ (whose elements are the permutations of the set $\{1,\dots,n\}$) acts on the vector space $\mathbb{F}_q^n$ via

$$\pi(c_1,\dots,c_n) := (c_{\pi(1)},\dots,c_{\pi(n)})$$

for $\pi \in \mathcal{S}_n$ and $c = (c_1,\dots,c_n) \in \mathbb{F}_q^n$.

Definition 8.2.1. *The automorphism group of a code $C \subseteq \mathbb{F}_q^n$ is defined by*

$$\mathrm{Aut}(C) := \{\pi \in \mathcal{S}_n \,|\, \pi(C) = C\}\,.$$

Obviously $\mathrm{Aut}(C)$ is a subgroup of $\mathcal{S}_n$. Many interesting codes have a non-trivial automorphism group. In this section we study automorphisms of algebraic geometry codes that are induced by automorphisms of the corresponding function field.

Let $F/\mathbb{F}_q$ be a function field and let $\mathrm{Aut}(F/\mathbb{F}_q)$ be the group of automorphisms of F over $\mathbb{F}_q$ (i.e., $\sigma(a) = a$ for $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ and $a \in \mathbb{F}_q$). The group $\mathrm{Aut}(F/\mathbb{F}_q)$ acts on $\mathbb{P}_F$ by setting $\sigma(P) := \{\sigma(x) \,|\, x \in P\}$, cf. Lemma 3.5.2. The corresponding valuations v_P and $v_{\sigma(P)}$ are related as follows:

$$v_{\sigma(P)}(y) = v_P(\sigma^{-1}(y)) \quad \textit{for all} \quad y \in F\,. \tag{8.1}$$

Moreover, $\deg \sigma(P) = \deg P$ since σ induces an isomorphism of the residue class fields of P and $\sigma(P)$ given by $\sigma(z(P)) := \sigma(z)(\sigma(P))$. The action of $\mathrm{Aut}(F/\mathbb{F}_q)$ on $\mathbb{P}_F$ extends to an action on the divisor group by setting

$$\sigma\left(\sum n_P P\right) := \sum n_P \sigma(P)\,.$$

As before we consider divisors $D = P_1 + \ldots + P_n$ and G of $F/\mathbb{F}_q$ where $P_1, \ldots, P_n$ are distinct places of degree one and $\mathrm{supp}\, G \cap \mathrm{supp}\, D = \emptyset$.

Definition 8.2.2. *We define*

$$\mathrm{Aut}_{D,G}(F/\mathbb{F}_q) := \{\sigma \in \mathrm{Aut}(F/\mathbb{F}_q) \,|\, \sigma(D) = D \textit{ and } \sigma(G) = G\}\,.$$

Observe that an automorphism $\sigma \in \mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ need not fix the places $P_1, \ldots, P_n$, but it yields a permutation of $P_1, \ldots, P_n$. From (8.1) it follows easily that

$$\sigma(\mathscr{L}(G)) = \mathscr{L}(G) \tag{8.2}$$

for $\sigma \in \mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$, because $\sigma(G) = G$. Now we show that every automorphism $\sigma \in \mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ induces an automorphism of the corresponding code $C_{\mathscr{L}}(D, G)$.

Proposition 8.2.3. *(a)* $\mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ *acts on the code* $C_{\mathscr{L}}(D, G)$ *by*

$$\sigma((x(P_1), \ldots, x(P_n))) := (x(\sigma(P_1)), \ldots, x(\sigma(P_n)))$$

(for $x \in \mathscr{L}(G)$*). This yields a homomorphism from* $\mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ *into* $\mathrm{Aut}(C_{\mathscr{L}}(D, G))$.

(b) If $n > 2g+2$*, the above homomorphism is injective. Hence* $\mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ *can be regarded as a subgroup of* $\mathrm{Aut}(C_{\mathscr{L}}(D, G))$.

Proof. (a) We begin with the following assertion: given a place P of degree one and an element $y \in F$ with $v_P(y) \geq 0$, we have

$$\sigma(y)(\sigma(P)) = y(P)\,. \tag{8.3}$$

In fact, setting $a := y(P) \in \mathbb{F}_q$, we obtain $y - a \in P$. Hence $\sigma(y) - a = \sigma(y - a) \in \sigma(P)$, and (8.3) follows.

For the proof of (a) we have to show that for every $x \in \mathscr{L}(G)$ and $\sigma \in \mathrm{Aut}_{D,G}(F/\mathbb{F}_q)$ the vector $(x(\sigma(P_1)), \ldots, x(\sigma(P_n)))$ is in $C_{\mathscr{L}}(D, G)$. As $\mathscr{L}(G) = \sigma(\mathscr{L}(G))$ by (8.2), we can write $x = \sigma(y)$ with $y \in \mathscr{L}(G)$, so

$$(x(\sigma(P_1)), \ldots, x(\sigma(P_n))) = (y(P_1), \ldots, y(P_n)) \in C_{\mathscr{L}}(D, G)\,,$$

by (8.3).

(b) It is sufficient to prove that the only automorphism of $F/\mathbb{F}_q$ fixing more than $2g + 2$ places of degree one is the identity. So we assume that $\sigma(Q) = Q$ and $\sigma(Q_i) = Q_i$ for $i = 1, \ldots, 2g + 2$, where $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ and $Q, Q_1, \ldots, Q_{2g+2}$ are distinct places of degree one. Choose $x, z \in F$ such that $(x)_\infty = 2gQ$ and $(z)_\infty = (2g + 1)Q$ (this is possible by the Riemann-Roch Theorem). Then $\mathbb{F}_q(x, z) = F$ since the degrees $[F : \mathbb{F}_q(x)] = 2g$ and $[F : \mathbb{F}_q(z)] = 2g + 1$ are relatively prime. The elements $x - \sigma(x)$ and $z - \sigma(z)$ have at least $2g + 2$ zeros (namely $Q_1, \ldots, Q_{2g+2}$) but their pole divisor has degree $\leq 2g + 1$ because Q is their only pole. We conclude $\sigma(x) = x$ and $\sigma(z) = z$, hence σ is the identity. □

Example 8.2.4. As an example we consider a BCH code C of length n over $\mathbb{F}_q$. As shown in Section 2.3, C can be realized as a subfield subcode of a rational AG code as follows: let $n \mid (q^m - 1)$ and let $\beta \in \mathbb{F}_{q^m}$ be a primitive n-th root of unity. Consider the rational function field $F = \mathbb{F}_{q^m}(z)$. For $i = 1, \ldots, n$ let P_i be the zero of $z - \beta^{i-1}$, and set $D_\beta := P_1 + \ldots + P_n$. Denote by P_0 resp. P_∞ the zero resp. the pole of z in F. Then

$$C = C_{\mathscr{L}}(D_\beta, rP_0 + sP_\infty)\,|_{\mathbb{F}_q}$$

with $r, s \in \mathbb{Z}$ (see Proposition 2.3.9). The automorphism $\sigma \in \mathrm{Aut}(F/\mathbb{F}_{q^m})$ given by $\sigma(z) = \beta^{-1}z$ leaves the places P_0 and P_∞ invariant, and we have

$$\sigma(P_i) = P_{i+1} \quad (i = 1, \ldots, n - 1) \quad \textit{and}\ \sigma(P_n) = P_1\,.$$

Hence, by Proposition 8.2.3, σ induces the following automorphism of the code $C_{\mathscr{L}}(D_\beta, rP_0 + sP_\infty)$:

$$\sigma(c_1, \ldots, c_n) = (c_2, \ldots, c_n, c_1)\,. \tag{8.4}$$

This means (in the usual terminology of coding theory) that BCH codes are *cyclic* codes.

8.3 Hermitian Codes

In Chapter 6 we discussed several examples of algebraic function fields. One can use all these examples for the explicit construction of algebraic geometry

codes. In this section we investigate some codes which are constructed by means of the Hermitian function field. This class of codes provides interesting and non-trivial examples of AG codes. These codes are codes over $\mathbb{F}_{q^2}$, they are not too short compared with the size of the alphabet, and their parameters k and d are fairly good.

First we recall some properties of the Hermitian function field H (cf. Lemma 6.4.4). H is a function field over $\mathbb{F}_{q^2}$; it can be represented as

$$H = \mathbb{F}_{q^2}(x, y) \quad \textit{with} \quad y^q + y = x^{q+1} \,. \tag{8.5}$$

The genus of H is $g = q(q-1)/2$, and H has $N = 1 + q^3$ places of degree one, namely

- the unique common pole Q_∞ of x and y, and
- for each pair $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ with $\beta^q + \beta = \alpha^{q+1}$ there is a unique place $P_{\alpha,\beta} \in \mathbb{P}_H$ of degree one such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$.

Observe that for all $\alpha \in \mathbb{F}_{q^2}$ there exist q distinct elements $\beta \in \mathbb{F}_{q^2}$ with $\beta^q + \beta = \alpha^{q+1}$, hence the number of places $P_{\alpha,\beta}$ is q^3.

Definition 8.3.1. *For $r \in \mathbb{Z}$ we define the code*

$$C_r := C_{\mathscr{L}}(D, rQ_\infty) \,, \tag{8.6}$$

where

$$D := \sum_{\beta^q + \beta = \alpha^{q+1}} P_{\alpha,\beta} \tag{8.7}$$

is the sum of all places of degree one (except Q_∞) of the Hermitian function field $H/\mathbb{F}_{q^2}$. The codes C_r are called Hermitian codes.

Hermitian codes are codes of length $n = q^3$ over the field $\mathbb{F}_{q^2}$. For $r \le s$ we obviously have $C_r \subseteq C_s$. Let us first discuss some trivial cases. For $r < 0$, $\mathscr{L}(rQ_\infty) = 0$ and therefore $C_r = 0$. For $r > q^3 + q^2 - q - 2 = q^3 + (2g-2)$, Theorem 2.2.2 and the Riemann-Roch Theorem yield

$$\begin{aligned} \dim C_r &= \ell(rQ_\infty) - \ell(rQ_\infty - D) \\ &= (r + 1 - g) - (r - q^3 + 1 - g) = q^3 = n \,. \end{aligned}$$

Hence $C_r = \mathbb{F}_{q^2}^n$ in this case, and it remains to study Hermitian codes with $0 \le r \le q^3 + q^2 - q - 2$.

Proposition 8.3.2. *The dual code of C_r is*

$$C_r^\perp = C_{q^3 + q^2 - q - 2 - r} \,.$$

Hence C_r is self-orthogonal if $2r \le q^3 + q^2 - q - 2$, and C_r is self-dual for $r = (q^3 + q^2 - q - 2)/2$.

Proof. Consider the element

$$t := \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha) = x^{q^2} - x \,.$$

t is a prime element for all places $P_{\alpha,\beta} \le D$, and its principal divisor is $(t) = D - q^3 Q_\infty$. Since $dt = d(x^{q^2} - x) = -dx$, the differential dt has the divisor $(dt) = (dx) = (q^2 - q - 2)Q_\infty$ (Lemma 6.4.4). Now Theorem 2.2.8 and Proposition 8.1.2 imply

$$\begin{aligned} C_r^\perp &= C_\Omega(D, rQ_\infty) = C_{\mathscr{L}}\big(D, D - rQ_\infty + (dt) - (t)\big) \\ &= C_{\mathscr{L}}\big(D, (q^3 + q^2 - q - 2 - r)Q_\infty\big) = C_{q^3+q^2-q-2-r} \,. \end{aligned}$$

□

Our next aim is to determine the parameters of C_r. We consider the set I of pole numbers of Q_∞ (cf. Definition 1.6.7); i.e.,

$$I = \{\, n \ge 0 \,|\, \textit{there is an element } z \in H \textit{ with } (z)_\infty = nQ_\infty \,\} \,.$$

For $s \ge 0$ let

$$I(s) := \{n \in I \,|\, n \le s\} \,. \tag{8.8}$$

Then $|I(s)| = \ell(sQ_\infty)$, and the Riemann-Roch Theorem gives

$$|I(s)| = s + 1 - q(q-1)/2 \textit{ for } s \ge 2g - 1 = q(q-1) - 1 \,.$$

From Lemma 6.4.4 we obtain the following description of $I(s)$:

$$I(s) = \{n \le s \,|\, n = iq + j(q+1) \textit{ with } i \ge 0 \textit{ and } 0 \le j \le q-1\} \,,$$

hence

$$|I(s)| = \big|\{\, (i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 \,;\, j \le q-1 \textit{ and } iq + j(q+1) \le s \,\}\big| \,.$$

Proposition 8.3.3. *Suppose that $0 \le r \le q^3 + q^2 - q - 2$. Then the following hold:*
(a) The dimension of C_r is given by

$$\dim C_r = \begin{cases} |I(r)| & \textit{for } 0 \le r < q^3 \,, \\ q^3 - |I(s)| & \textit{for } q^3 \le r \le q^3 + q^2 - q - 2 \,, \end{cases}$$

where $s := q^3 + q^2 - q - 2 - r$ and $I(r)$ is defined by (8.8).
(b) For $q^2 - q - 2 < r < q^3$ we have

$$\dim C_r = r + 1 - q(q-1)/2 \,.$$

(c) The minimum distance d of C_r satisfies

$$d \geq q^3 - r\,.$$

If $0 \leq r < q^3$ and both numbers r and $q^3 - r$ are pole numbers of Q_∞, then

$$d = q^3 - r\,.$$

Proof. (a) For $0 \leq r < q^3$ Corollary 2.2.3 gives

$$\dim C_r = \dim \mathscr{L}(rQ_\infty) = |I(r)|\,.$$

For $q^3 \leq r \leq q^3 + q^2 - q - 2$ we set $s := q^3 + q^2 - q - 2 - r$. Then $0 \leq s \leq q^2 - q - 2 < q^3$. By Proposition 8.3.2 we obtain

$$\dim C_r = q^3 - \dim C_s = q^3 - |I(s)|\,.$$

(b) For $q^2 - q - 2 = 2g - 2 < r < q^3$, Corollary 2.2.3 gives

$$\dim C_r = r + 1 - g = r + 1 - q(q-1)/2\ .$$

(c) The inequality $d \geq q^3 - r$ follows from Theorem 2.2.2. Now let $0 \leq r < q^3$ and assume that both numbers r and $q^3 - r$ are pole numbers of Q_∞. In order to prove the equality $d = q^3 - r$ we distinguish three cases.

Case 1: $r = q^3 - q^2$. Choose $i := q^2 - q$ distinct elements $\alpha_1, \ldots, \alpha_i \in \mathbb{F}_{q^2}$. Then the element

$$z := \prod_{\nu=1}^{i} (x - \alpha_\nu)\ \in\ \mathscr{L}(rQ_\infty)$$

has exactly $qi = r$ distinct zeros $P_{\alpha,\beta}$ of degree one, and the weight of the corresponding codeword $\mathrm{ev}_D(z) \in C_r$ is $q^3 - r$. Hence $d = q^3 - r$.

Case 2: $r < q^3 - q^2$. We write $r = iq + j(q+1)$ with $i \geq 0$ and $0 \leq j \leq q - 1$, so $i \leq q^2 - q - 1$. Fix an element $0 \neq \gamma \in \mathbb{F}_q$ and consider the set $A := \{\alpha \in \mathbb{F}_{q^2} \,|\, \alpha^{q+1} \neq \gamma\}$. Then $|A| = q^2 - (q+1) \geq i$, and we can choose distinct elements $\alpha_1, \ldots, \alpha_i \in A$. The element

$$z_1 := \prod_{\nu=1}^{i} (x - \alpha_\nu)$$

has iq distinct zeros $P_{\alpha,\beta} \leq D$. Next we choose j distinct elements $\beta_1, \ldots, \beta_j \in \mathbb{F}_{q^2}$ with $\beta_\mu^q + \beta_\mu = \gamma$ and set

$$z_2 := \prod_{\mu=1}^{j} (y - \beta_\mu)\,.$$

z_2 has $j(q+1)$ zeros $P_{\alpha,\beta} \le D$, and all of them are distinct from the zeros of z_1 because $\beta_\mu^q + \beta_\mu = \gamma \neq \alpha_\nu^{q+1}$ for $\mu = 1, \ldots, j$ and $\nu = 1, \ldots, i$. Hence

$$z := z_1 z_2 \in \mathscr{L}\big((iq + j(q+1))Q_\infty\big) = \mathscr{L}(rQ_\infty)$$

has r distinct zeros $P_{\alpha,\beta} \le D$. The corresponding codeword $\mathrm{ev}_D(z) \in C_r$ has weight $q^3 - r$.

Case 3: $q^3 - q^2 < r < q^3$. By assumption, $s := q^3 - r$ is a pole number and $0 < s < q^2 \le q^3 - q^2$. By case 2 there exists an element $z \in H$ with principal divisor $(z) = D' - sQ_\infty$ where $0 \le D' \le D$ and $\deg D' = s$. The element $u := x^{q^2} - x \in H$ has the divisor $(u) = D - q^3 Q_\infty$, hence

$$(z^{-1}u) = (D - D') - (q^3 - s)Q_\infty = (D - D') - rQ_\infty\,.$$

The codeword $\mathrm{ev}_D(z^{-1}u) \in C_r$ has weight $q^3 - r$. □

We mention that the minimum distance of C_r is known also in the remaining cases (where $r \ge q^3$, or one of the numbers r or $q^3 - r$ is a gap of Q_∞).

One can easily specify a generator matrix for the Hermitian codes C_r. We fix an ordering of the set $T := \{(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid \beta^q + \beta = \alpha^{q+1}\}$. For $s = iq + j(q+1)$ (where $i \ge 0$ and $0 \le j \le q-1$) we define the vector

$$u_s := \big(\alpha^i \beta^j\big)_{(\alpha,\beta)\in T} \in (\mathbb{F}_{q^2})^{q^3}\,.$$

Then we have:

Corollary 8.3.4. *Suppose that* $0 \le r < q^3$. *Let* $0 = s_1 < s_2 < \ldots < s_k \le r$ *be all pole numbers* $\le r$ *of* Q_∞. *Then the* $k \times q^3$ *matrix* M_r *whose rows are* $u_{s_1}, \ldots, u_{s_k}$, *is a generator matrix of* C_r.

Proof. Corollary 2.2.3. □

In the same manner we obtain a parity check matrix for C_r (for $r > q^2 - q - 2$), since the dual of C_r is the code C_s with $s = q^3 + q^2 - q - 2 - r$.

Finally we study automorphisms of Hermitian codes. Let $H = \mathbb{F}_{q^2}(x, y)$ as before, cf. (8.5). Let

$$\varepsilon \in \mathbb{F}_{q^2} \setminus \{0\}\,,\ \ \delta \in \mathbb{F}_{q^2} \ \ \textit{and}\ \ \mu^q + \mu = \delta^{q+1}\,. \tag{8.9}$$

Then $\mu \in \mathbb{F}_{q^2}$, and there exists an automorphism $\sigma \in \mathrm{Aut}(H/\mathbb{F}_{q^2})$ with

$$\sigma(x) = \varepsilon x + \delta \ \ \textit{and}\ \ \sigma(y) = \varepsilon^{q+1} y + \varepsilon \delta^q x + \mu\,. \tag{8.10}$$

(The existence of an automorphism σ satisfying (8.10) follows from the fact that $\sigma(y)$ and $\sigma(x)$ satisfy the equation $\sigma(y)^q + \sigma(y) = \sigma(x)^{q+1}$, which is a consequence of (8.9).) The set of all automorphisms (8.10) of $H/\mathbb{F}_{q^2}$ constitutes

a group $\Gamma \subseteq \mathrm{Aut}(H/\mathbb{F}_{q^2})$ of order $q^3(q^2-1)$ (as $\varepsilon \neq 0$ and δ are arbitrary, and for each δ there are q possible values of μ). Clearly $\sigma(Q_\infty) = Q_\infty$ for all $\sigma \in \Gamma$, and σ permutes the places $P_{\alpha,\beta}$ of H since they are the only places of H of degree one other than Q_∞. By Proposition 6.3.3, Γ acts as a group of automorphisms on the Hermitian codes C_r. We have proved:

Proposition 8.3.5. *The automorphism group* $\mathrm{Aut}(C_r)$ *of the Hermitian code* C_r *contains a subgroup of order* $q^3(q^2-1)$.

Remark 8.3.6. It is easily seen that Γ acts *transitively* on the places $P_{\alpha,\beta}$; i.e., given $P_{\alpha,\beta}$ and $P_{\alpha',\beta'}$ then there exists some $\sigma \in \Gamma$ with $\sigma(P_{\alpha,\beta}) = P_{\alpha',\beta'}$.

8.4 The Tsfasman-Vladut-Zink Theorem

It is well-known in coding theory that large block lengths (hence large dimension and large minimum distance) are required to achieve reliable transmission of information. We introduce some notation that will simplify discussion of asymptotic performance of codes.

Definition 8.4.1. *(a) Given an* $[n,k,d]$ *code* C *over* $\mathbb{F}_q$*, we define its information rate*

$$R = R(C) := k/n$$

and its relative minimum distance

$$\delta = \delta(C) := d/n\,.$$

(b) Let $V_q := \{(\delta(C), R(C)) \in [0,1]^2 \mid C$ *is a code over* $\mathbb{F}_q\}$ *and* $U_q \subseteq [0,1]^2$ *be the set of limit points of* V_q.

This means: a point $(\delta, R) \in \mathbb{R}^2$ is in U_q if and only if there are codes C over $\mathbb{F}_q$ of arbitrary large length such that the point $(\delta(C), R(C))$ is arbitrarily close to (δ, R).

Proposition 8.4.2. *There is a continuous function* $\alpha_q : [0,1] \to [0,1]$ *such that*

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

Moreover the following hold: $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ *for* $1 - q^{-1} \leq \delta \leq 1$, *and* α_q *is decreasing in the interval* $0 \leq \delta \leq 1 - q^{-1}$.

The proof of this proposition requires only elementary techniques of coding theory; we refer to [29].

For $0 < \delta < 1 - q^{-1}$ the exact value of $\alpha_q(\delta)$ is unknown. However, several upper and lower bounds are available. In the following propositions we state

some of these bounds. Proofs can be found in most books on coding theory, e.g. in [28]. The *q-ary entropy function* $H_q : [0, 1 - q^{-1}] \to \mathbb{R}$ is defined by $H_q(0) := 0$ and

$$H_q(x) := x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

for $0 < x \leq 1 - q^{-1}$.

Proposition 8.4.3. *The following upper bounds for $\alpha_q(\delta)$ hold:*
(a) (Plotkin Bound) *For $0 \leq \delta \leq 1 - q^{-1}$,*

$$\alpha_q(\delta) \leq 1 - \frac{q}{q-1} \cdot \delta \,.$$

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

$$\alpha_q(\delta) \leq 1 - H_q(\delta/2) \,.$$

(c) (Bassalygo-Elias Bound) *For $0 \leq \delta \leq \theta := 1 - q^{-1}$,*

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

Out of the upper bounds in Proposition 8.4.3, the Bassalygo-Elias Bound is always the best, see Figure 8.1 below; an even better upper bound (which is more complicated to state and more difficult to prove) is the *McEliece-Rodemich-Rumsey-Welch Bound*, see [28],[32].

Perhaps more important than *upper* bounds are *lower* bounds for $\alpha_q(\delta)$, because every non-trivial lower bound for $\alpha_q(\delta)$ guarantees the existence of arbitrary long codes with good parameters $(\delta(C), R(C))$.

Proposition 8.4.4 (Gilbert-Varshamov Bound). *For $0 \leq \delta \leq 1 - q^{-1}$,*

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

The Gilbert-Varshamov bound is the best lower bound for $\alpha_q(\delta)$ which is known from elementary coding theory. However, its proof is not constructive (i.e., it does not provide a simple algebraic algorithm for the construction of good long codes).

Our aim is to construct algebraic geometry codes of large length in order to improve the Gilbert-Varshamov Bound. Given an algebraic function field $F/\mathbb{F}_q$ with $N = N(F)$ places of degree one, the length of any AG code $C_{\mathscr{L}}(D, G)$ (resp. $C_{\Omega}(D, G)$) associated with divisors D and G of F is bounded by N, since D is a sum of places of degree one. In fact, this is the only restriction on the length of an AG code which can be constructed by means of the function field F.

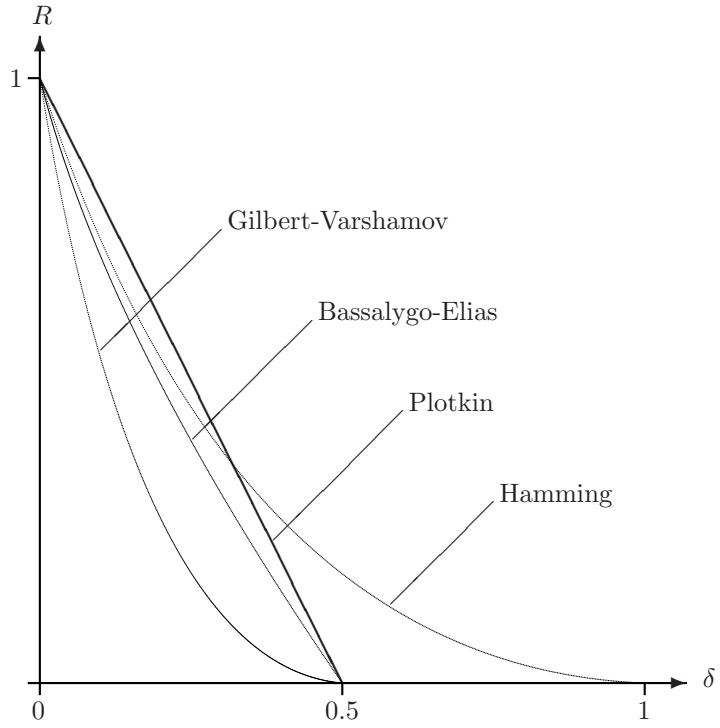

Fig. 8.1. Bounds for $q = 2$.

Lemma 8.4.5. *Suppose that $P_1, \ldots, P_n$ are distinct places of $F/\mathbb{F}_q$ of degree one. Then there exists, for each $r \geq 0$, a divisor G such that $\deg G = r$ and $P_i \notin \operatorname{supp} G$ (for $i = 1, \ldots, n$).*

Proof. The lemma is trivial if there is another place Q of degree one, different from $P_1, \ldots, P_n$. In this case we set $G := rQ$. If $P_1, \ldots, P_n$ are all the places of $F/\mathbb{F}_q$ of degree one, we choose a divisor $G \sim rP_1$ (i.e., G is equivalent to rP_1) such that $v_{P_i}(G) = 0$ for $i = 1, \ldots, n$. This is possible by the Approximation Theorem. □

According to Lemma 8.4.5 one needs function fields over $\mathbb{F}_q$ having many rational places in order to construct long AG codes. We recall the definition of Ihara's constant $A(q)$ given in Chapter 7. For $g \geq 0$ let

$$N_q(g) := \max\{N(F) \,|\, F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g \,\},$$

where $N(F)$ denotes the number of places of $F/\mathbb{F}_q$ of degree one. Then $A(q)$ is defined as

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

Proposition 8.4.6. *Suppose that* $A(q) > 1$. *Then*

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

in the interval $0 \leq \delta \leq 1 - A(q)^{-1}$.

Proof. Let $\delta \in [0, 1 - A(q)^{-1}]$. Choose a sequence of function fields $F_i/\mathbb{F}_q$ of genus g_i such that

$$g_i \to \infty \quad \textit{and} \quad n_i/g_i \to A(q)\,, \tag{8.11}$$

where $n_i := N(F_i)$. Choose $r_i > 0$ such that

$$r_i/n_i \to 1 - \delta\,. \tag{8.12}$$

This is possible as $n_i \to \infty$ for $i \to \infty$. Let D_i be the sum of all places of $F_i/\mathbb{F}_q$ of degree one, thus $\deg D_i = n_i$. By Lemma 8.4.5 there exists a divisor G_i of $F_i/\mathbb{F}_q$ such that $\deg G_i = r_i$ and $\operatorname{supp} G_i \cap \operatorname{supp} D_i = \emptyset$. Consider the code $C_i := C_{\mathscr{L}}(D_i, G_i)$; this is an $[n_i, k_i, d_i]$ code whose parameters k_i and d_i satisfy the inequalities

$$k_i \geq \deg G_i + 1 - g_i = r_i + 1 - g_i \quad \textit{and} \quad d_i \geq n_i - \deg G_i = n_i - r_i$$

(cf. Corollary 2.2.3). Hence

$$R_i := R(C_i) \geq \frac{r_i + 1}{n_i} - \frac{g_i}{n_i} \quad \textit{and} \quad \delta_i := \delta(C_i) \geq 1 - \frac{r_i}{n_i}\,. \tag{8.13}$$

W.l.o.g. we can assume that the sequences $(R_i)_{i\geq 1}$ and $(\delta_i)_{i\geq 1}$ are convergent (otherwise we choose an appropriate subsequence), say $R_i \to R$ and $\delta_i \to \tilde{\delta}$. From (8.11), (8.12) and (8.13) it follows that $R \geq 1 - \delta - A(q)^{-1}$ and $\tilde{\delta} \geq \delta$. So $\alpha_q(\tilde{\delta}) \geq R \geq 1 - \delta - A(q)^{-1}$. Since α_q is non-increasing, this implies

$$\alpha_q(\delta) \geq \alpha_q(\tilde{\delta}) \geq 1 - \delta - A(q)^{-1}\,.$$

□

Now we can easily prove the main result of this section.

Theorem 8.4.7 (Tsfasman-Vladut-Zink Bound). *Let* $q = \ell^2$ *be a square. Then we have for all* δ *with* $0 \leq \delta \leq 1 - (q^{1/2} - 1)^{-1}$,

$$\alpha_q(\delta) \geq \left(1 - \frac{1}{q^{1/2} - 1}\right) - \delta\,.$$

Proof. By Corollary 7.4.8 we have $A(q) = q^{1/2} - 1$ if q is a square. Now the assertion follows immediately from Proposition 8.4.6. □

For all $q \geq 49$ the Tsfasman-Vladut-Zink Bound improves the Gilbert-Varshamov Bound in a certain interval, see Figure 8.2 .

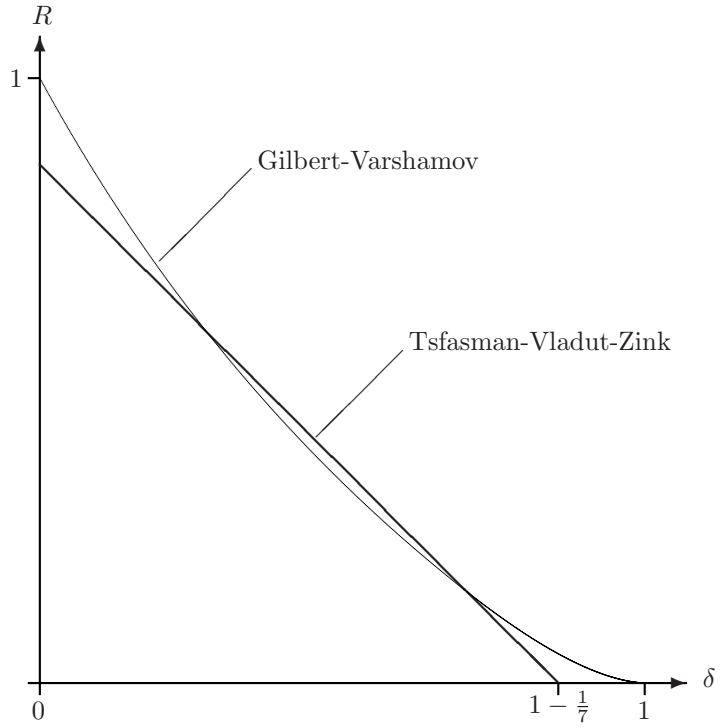

Fig. 8.2. Bounds for $q = 64$.

Remark 8.4.8. Also if q is not a square one can obtain an improvement of the Gilbert-Varshamov Bound if a good lower bound for Ihara's constant $A(q)$ is available. For instance, let $q = \ell^3$ be a cube. Then we have for all δ with $0 \le \delta \le 1 - (\ell + 2)/(2(\ell^2 - 1))$ the following lower bound for $\alpha_q(\delta)$:

$$\alpha_q(\delta) \ge \left(1 - \frac{\ell + 2}{2(\ell^2 - 1)}\right) - \delta \ . \tag{8.14}$$

The proof of this bound is exactly the same as in Theorem 8.4.7; one just uses the bound for $A(\ell^3)$ given in Corollary 7.4.18. We note that (8.14) improves the Gilbert-Varshamov Bound for all cubes $q \ge 7^3$.

In the proof of the Tsfasman-Vladut-Zink Theorem we have only used that there *exists* a sequence of function fields $F_i/\mathbb{F}_q$ (for $q = \ell^2$) with $\lim_{n\to\infty} N(F_i)/g(F_i) = \ell - 1$. If the function fields F_i have additional nice properties, one can hope that the corresponding AG codes also have nice properties. As an example for this idea we shall prove the existence of long self-dual codes whose parameters attain the Tsfasman-Vladut-Zink Bound.

Theorem 8.4.9. *Let $q = \ell^2$ be a square. Then there exists a sequence of self-dual codes $(C_i)_{i\geq 0}$ over $\mathbb{F}_q$ with parameters $[n_i, k_i, d_i]$ such that $n_i \to \infty$ and*

$$\liminf_{i\to\infty} \frac{d_i}{n_i} \geq \frac{1}{2} - \frac{1}{\ell - 1} \ . \tag{8.15}$$

Note that Inequality (8.6) just says that the sequence $(C_i)_{i\geq 0}$ attains the Tsfasman-Vladut-Zink Bound, because the information rate of a self-dual code C is $R(C) = 1/2$. As a consequence we obtain that there are self-dual codes over $\mathbb{F}_q$ (with $q = \ell^2 \geq 49$) of arbitrary large length whose performance is better than the Gilbert-Varshamov bound.

Proof of Theorem 8.4.9. For simplicity we will assume that q is even; i.e., $\operatorname{char} \mathbb{F}_q = 2$ (the assertion is also true in the case of odd characteristic, but the proof is then a bit more complicated). We will use the Galois tower $\mathcal{G}^* = (G_0^*, G_1^*, G_2^*, ...)$ of function fields over $\mathbb{F}_q$ that was studied in Section 7.4, see Theorem 7.4.15 and Corollary 7.4.16. We recall briefly the properties of this tower that will be needed below.

The field $G_0^* = \mathbb{F}_q(u_0)$ is a rational function field. For $i \geq 1$ we have

$$n_i = [G_i^* : G_0^*] = (\ell - 1)m_i \ ,$$

where $m_i \geq \ell$ is a power of $p = \operatorname{char} \mathbb{F}_q$. The zero divisor of u_0 in G_i^* has the form

$$(u_0)_0^{G_i^*} = D_i = \sum_{j=1}^{n_i} P_j^{(i)} \tag{8.16}$$

with pairwise distinct places $P_j^{(i)}$ of degree one, and the divisor of the differential $\eta^{(i)} = du_0/u_0$ in the function field G_i^* is given by

$$(\eta^{(i)}) = (\ell e_i^{(0)} - 2)A_i + (e_i^{(\infty)} - 2)B_i - D_i \tag{8.17}$$

with positive divisors A_i, B_i and

$$\big(\operatorname{supp} A_i \cup \operatorname{supp} B_i\big) \cap \operatorname{supp} D_i = \emptyset \ .$$

Moreover the degrees of the divisors A_i, B_i satisfy

$$e_i^{(0)} \cdot \deg A_i = e_i^{(\infty)} \cdot \deg B_i = n_i/(\ell - 1) \ . \tag{8.18}$$

with certain integers $e_i^{(0)}, e_i^{(\infty)}$. Now we define the divisor $H_i \in \operatorname{Div}(G_i^*)$ as

$$H_i := \big(\frac{\ell e_i^{(0)} - 2}{2}\big)A_i + \big(\frac{e_i^{(\infty)} - 2}{2}\big)B_i \ .$$

At this point we have used the assumption that q (and hence ℓ) is even. Since $2H_i - D_i = (\eta^{(i)})$ by (8.17), it follows from Corollary 8.1.3 that the code

$$C_i := C_{\mathscr{L}}(D_i, H_i) \subseteq \mathbb{F}_q^{n_i}$$

is self-dual. By Theorem 2.2.2 its minimum distance $d_i := d(C_i)$ can be estimated by

$$\begin{aligned} d_i &\geq \deg(D_i - H_i) = \deg D_i - \deg H_i \\ &= n_i - \Big(\frac{\ell e_i^{(0)} - 2}{2}\Big) \deg A_i - \Big(\frac{e_i^{(\infty)} - 2}{2}\Big) \deg B_i \\ &\geq n_i - \frac{1}{2}\Big(\ell e_i^{(0)} \deg A_i + e_i^{(\infty)} \deg B_i\Big) \\ &= n_i - \frac{1}{2}\Big(\ell \frac{n_i}{\ell - 1} + \frac{n_i}{\ell - 1}\Big) \\ &= n_i\Big(\frac{1}{2} - \frac{1}{\ell - 1}\Big) \end{aligned}$$

(here we have used Equations (8.16) and (8.18)). Therefore we obtain

$$\delta_i := \delta(C_i) = \frac{d_i}{n_i} \geq \frac{1}{2} - \frac{1}{\ell - 1}\ .$$

□

8.5 Decoding AG Codes

For a code to have practical use, it is essential that one has an effective decoding algorithm. Let us briefly explain what this means. We consider an $[n, k, d]$ code $C \subseteq \mathbb{F}_q^n$. Then C is t-error correcting for all $t \leq (d-1)/2$, cf. Section 2.1. Suppose $a \in \mathbb{F}_q^n$ is an n-tuple such that

$$a = c + e\,, \tag{8.19}$$

where $c \in C$ is a codeword and $e \in \mathbb{F}_q^n$ has weight

$$\mathrm{wt}(e) \leq (d-1)/2\,. \tag{8.20}$$

Then c is uniquely determined by a and the conditions (8.19) and (8.20); it is the unique codeword whose distance to a is minimal. The vector e in (8.19) is called the *error vector* of a with respect to C. A *decoding algorithm* is an algorithm which calculates for every element $a \in \mathbb{F}_q^n$ satisfying (8.19) and (8.20) the corresponding codeword c (or, equivalently, the corresponding error vector e).

For algebraic geometry codes a very general decoding algorithm is available. We consider the code

$$C_\Omega := C_\Omega(D, G) \tag{8.21}$$

http://www.springer.com/978-3-540-76877-7

Algebraic Function Fields and Codes
Stichtenoth, H.
2009, XIV, 360 p., Hardcover
ISBN: 978-3-540-76877-7