Chapter 2

Bounds and Modifications

2

2

2 Bounds and Modifications

The fundamental parameters of a linear code are the length n, the dimension k, the minimum distance d and the size q of the finite field over which it is defined. For applications, we are interested in the information rate k/n and the relative minimum distance d/n both being large. We may think of this as a typical *packing problem of combinatorics.* Is it possible to pack a large number of vectors (codewords) into the Hamming space $H(n,q)$ such that no two words are close? Of course, these are contradicting aims. To see this, we think of the balls of radius $\lfloor (d-1)/2 \rfloor$ which are centered around codewords, since, for unique decoding using the maximum likelihood principle, we require that these balls should never overlap. It is intuitively clear that a large number of codewords can only be achieved if the balls are small. Conversely, if the balls are large then this tends to limit the number of codewords (or balls) which can be packed. This is the fundamental dilemma of Coding Theory (cf. Fig. 2.1).

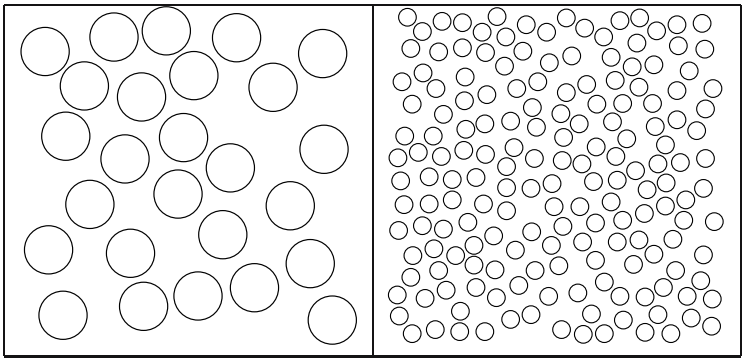

Fig. 2.1 The fundamental dilemma

In order to understand the situation better, we are going to study various bounds for the parameters of codes. We consider (n,k,d)-codes *optimal* if they optimize one parameter given the other two (the parameter q is kept fixed). Furthermore, we will discuss various constructions of new codes from old. These constructions in turn lead to bounds. Interesting classes of codes are obtained by analyzing whether bounds can be met with equality. Also, we will meet further series of codes which are connected to the above-mentioned constructions, or which are of interest because they meet one of the bounds which will be presented. Examples are the Hamming- and simplex-codes, perfect codes, Reed–Muller- and MDS-codes.

2.1

2.1 Combinatorial Bounds for the Parameters

For the purpose of applications we certainly prefer linear codes with *optimal* properties. The search for optimal codes can be described in three ways:

1. For given parameters k, d, q find a linear code of *least length*
$$n_{\min}(k,d,q) := \min\{\, n \mid \text{there exists an } (n,k,d,q)\text{-code} \,\}.$$
2. For given parameters n, k, q find a linear code of *maximal minimum distance*
$$d_{\max}(n,k,q) := \max\{\, d \mid \text{there exists an } (n,k,d,q)\text{-code} \,\}.$$
3. For given parameters n, d, q find a linear code of *maximal dimension*
$$k_{\max}(n,d,q) := \max\{\, k \mid \text{there exists an } (n,k,d,q)\text{-code} \,\}.$$

To begin with, we derive a few direct combinatorial bounds for the parameters of a code. Each such result in turn yields a bound for $n_{\min}(k,d,q)$, $d_{\max}(n,k,q)$ and $k_{\max}(n,d,q)$. After that, we will tabulate the best bounds we have obtained at that point. In the following section we will investigate the two functions $n_{\min}(k,d,q)$ and $d_{\max}(n,k,q)$ more thoroughly.

2.1.1 **The Singleton-bound** *For each linear (n,k,d)-code C over $\mathbb{F}_q$ we have the inequality*
$$d \le n - k + 1.$$

Proof: We know from 1.4 that isometric codes have the same coding theoretic properties. By 1.7 we may consider a code isometric to C which is generated systematically by the matrix $(I_k \mid A)$. Then, for each unit vector $e^{(i)} \in \mathbb{F}_q^k$, the vector $e^{(i)} \cdot (I_k \mid A)$ is of weight not greater than $n - k + 1$. This proves the statement, since by 1.2.8 the minimum distance is the minimum weight of a nonzero codeword. □

2.1.2 **Definition (MDS-codes)** Codes with minimum distance $d = n - k + 1$ are called *MDS-codes* (an abbreviation of *maximum distance separable*). ◇

Trivial MDS-codes are the $(n,1)$-repetition-codes, the $(n,n-1)$-parity check codes (cf. Exercise 1.3.11), and the (n,n)-codes. We will discuss MDS-codes in Section 2.5.

2.1.3 **The Hamming-bound** *The parameters of each (n,k,d,q)-code satisfy the inequality*
$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i \le q^{n-k}.$$
Equality holds if and only if the closed balls of radius $\lfloor (d-1)/2 \rfloor$ around codewords cover the whole Hamming space $H(n,q)$.

Proof: The number of vectors of Hamming distance i from a given vector is $\binom{n}{i}(q-1)^i$, since the first factor counts the number of ways of choosing i coordinates out of the n coordinate positions and the second term is the number of possibilities to change such an i-tuple in each place. We may think of these vectors as forming a ball of radius i around a given codeword. Summing over $i = 0, \ldots, r$ yields the number of vectors in a ball of radius r. Since the balls of radius $r = \lfloor (d-1)/2 \rfloor$ around codewords are all disjoint, the left hand side of the inequality multiplied by q^k is less than or equal to $|H(n,q)| = q^n$. Dividing by q^k yields the statement. □

Definition (perfect codes) Codes whose parameters attain the Hamming-bound are called *perfect.* ◇ **2.1.4**

Important examples of perfect codes are the Hamming-codes, which we will introduce next. Further perfect codes are the Golay-codes G_{23} and G_{11}; they will be presented in Section 4.4 (cf. Exercise 2.1.2). Trivial perfect codes are described in Exercise 2.1.1. A. Tietäväinen [191] and, independently, V.A. Zinovjev and V.K. Leontjev [207] have shown that there are no further perfect linear codes. However, there exist other perfect codes which are not linear.

The general form of the *Hamming-codes* was introduced first by M.J.E. Golay [70] and R.W. Hamming [80]. The binary $(7,4)$-Hamming-code is indeed older. It is mentioned in the seminal paper of C.E. Shannon [178]. The Hamming-codes form an infinite family of perfect, 1-error-correcting linear codes. The following definition specifies this class of codes up to isometry.

Definition (Hamming-codes, simplex-codes) Let Δ be any matrix whose columns form a system of nonzero representatives of the one-dimensional subspaces of $\mathbb{F}_q^m$. A linear code C which has Δ as its check matrix is called an *m-th order q-ary Hamming-code.* The dual code of a Hamming-code, i.e. the code which is *generated* by the matrix Δ (cf. 1.3.4) is called an *m-th order q-ary simplex-code.* Of course, both the Hamming- and the simplex-code are only defined up to isometry. ◇ **2.1.5**

In 1.3.6, we have already met the third order binary Hamming-code.

Theorem *For $m \geq 2$ the m-th order q-ary Hamming-code is a perfect code with parameters* **2.1.6**

$$(n,k,d,q) = \left(\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3, q \right).$$

Proof: The statement about the length is clear from the definition, since the number of one-dimensional subspaces of $\mathbb{F}_q^m$ is $(q^m-1)/(q-1)$. A check matrix Δ of a Hamming-code contains in particular the m unit vectors (or nonzero scalar multiples thereof). Hence Δ is of rank m and the dimension of the code is $\dim(C) = (q^m-1)/(q-1) - m$, by 1.3.1. It remains to determine the minimum distance. For this, we note that any two columns of Δ are by definition linearly independent. Furthermore, since $m \geq 2$ there exist three columns which are dependent. By 1.3.9 this implies that the minimum distance is $d = 3$. Finally, we see that this code is perfect, since

$$\begin{aligned}\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i}(q-1)^i &= \sum_{i=0}^{1} \binom{(q^m-1)/(q-1)}{i}(q-1)^i \\ &= 1 + \frac{q^m-1}{q-1}(q-1) = q^m. \qquad \square\end{aligned}$$

2.1.7 **Theorem** *The m-th order q-ary simplex-code C has parameters*

$$(n,k,d,q) = \Big(\frac{q^m-1}{q-1}, m, q^{m-1}, q\Big).$$

All nonzero codewords have weight q^{m-1}, i.e.

$$w_C(x) = 1 + (q^m-1)x^{q^{m-1}}, \text{ and } W_C(x,y) = y^{\frac{q^m-1}{q-1}} + (q^m-1)x^{q^{m-1}} y^{\frac{q^{m-1}-1}{q-1}}.$$

Proof: Consider the matrix Δ from the proof of 2.1.6. This time, regard Δ as a generator matrix. The statement about the length is clear, and the value for the dimension follows again from 1.3.1 together with 1.3.4. It remains to show that each nonzero codeword has weight q^{m-1}. For this, we consider the encoding map $v \mapsto v \cdot \Delta$. Write

$$\Delta = \Big({u^{(0)}}^\top \;\Big|\; \ldots \;\Big|\; {u^{(n-1)}}^\top \Big)$$

with $u^{(i)} \in \mathbb{F}_q^m$. Then, using the standard bilinear form, we have for $v \in \mathbb{F}_q^m$

$$v \cdot \Delta = \Big(\langle\, v, u^{(0)} \,\rangle, \ldots, \langle\, v, u^{(n-1)} \,\rangle \Big).$$

Fix an element $v \in \mathbb{F}_q^m \setminus \{0\}$. The mapping $u \mapsto \langle\, v,u \,\rangle$ for $u \in \mathbb{F}_q^m$ is a surjective linear form, as already pointed out in the proof of 1.6.8. It takes on each value of $\mathbb{F}_q$ exactly q^{m-1} times. Thus, for exactly $q^{m-1}(q-1)$ vectors $u \in \mathbb{F}_q^m$ the value of $\langle\, v,u \,\rangle$ is nonzero. By linearity, we have $\langle\, v, \lambda u \,\rangle = \lambda \langle\, v,u \,\rangle$ for all $\lambda \in \mathbb{F}_q$. In particular, the value of $\langle\, v,w \,\rangle$ is either always zero or always

nonzero for elements w of the form $w = \lambda u$, where $\lambda \in \mathbb{F}_q^*$. This means that the fact that $\langle v, u \rangle$ is zero or nonzero only depends on the one-dimensional subspace containing $u \neq 0$. Now recall that the $u^{(i)}$ form a transversal of the one-dimensional subspaces (disregarding the zero vector, which is in every subspace). This means that the products $\lambda \cdot u^{(i)}$ where $\lambda \in \mathbb{F}_q^*$ and $0 \leq i < (q^m - 1)/(q - 1)$ take on every nonzero vector $u \in \mathbb{F}_q^m$ exactly once. The previous remark implies that the $q^{m-1}(q-1)$ vectors $u \in \mathbb{F}_q^m$ with $\langle v, u \rangle \neq 0$ ($u = 0$ is not one of them!) are contained in exactly q^{m-1} one-dimensional subspaces. Thus

$$\mathrm{wt}(v \cdot \Delta) = \mathrm{wt}(\langle v, u^{(0)} \rangle, \ldots, \langle v, u^{(n-1)} \rangle) = q^{m-1}$$

for any $v \neq 0$. The statement about the weight enumerator $w_C(x)$ is clear. Using the identity $(q^m - 1)/(q - 1) = 1 + q + q^2 + \ldots q^{m-1}$ we obtain the homogeneous version $W_C(x, y)$. This finishes the proof. □

Example The third order ternary Hamming-code is a $(13, 10, 3, 3)$-code. It has a check matrix of the form **2.1.8**

$$\begin{pmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and its dual code is a ternary simplex-code of type $(13, 3, 9, 3)$. ◇

The next bound is an *explicit* bound for the minimum distance:

The Plotkin-bound *For each linear (n, k, d, q)-code C the following holds:* **2.1.9**

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

Proof: Consider the double sum of distances

$$D := \sum_{c \in C} \sum_{c' \in C} d(c, c').$$

It is bounded from below, since for each $c \neq c'$ we have $d(c, c') \geq d$, and this implies $D \geq q^k(q^k - 1)d$.

We may evaluate D in a different way. For this purpose we label the elements of $\mathbb{F}_q$ by $\{\kappa_1, \ldots, \kappa_q\}$. For $0 \leq j < n$ and $1 \leq i \leq q$ let D_{ij} denote the number of codewords which have as their j-th component the element κ_i. In terms of this notation we obtain

$$D = \sum_{j \in n} \sum_{i=1}^{q} D_{ij}(q^k - D_{ij}).$$

Since $\sum_{i=1}^{q} D_{ij} = q^k$, we get

$$D = nq^{2k} - \sum_{j\in n}\sum_{i=1}^{q} D_{ij}^2.$$

For $j \in n$ the following is true:

$$\begin{aligned} 0 \;&\leq\; \sum_{i=1}^{q}\sum_{t=i+1}^{q} (D_{ij} - D_{tj})^2 \\ &= \underbrace{\sum_{i=1}^{q}\sum_{t=i+1}^{q} D_{ij}^2}_{=\sum_i (q-i) D_{ij}^2} + \underbrace{\sum_{i=1}^{q}\sum_{t=i+1}^{q} D_{tj}^2}_{=\sum_i (i-1) D_{ij}^2} - \sum_{i=1}^{q}\sum_{t=i+1}^{q} 2D_{ij}D_{tj}. \end{aligned}$$

This yields the estimate

$$q\sum_{i=1}^{q} D_{ij}^2 \geq \sum_{i=1}^{q} D_{ij}^2 + \sum_{i=1}^{q}\sum_{t=i+1}^{q} 2D_{ij}D_{tj} = \left(\sum_{i=1}^{q} D_{ij}\right)^2 = q^{2k}.$$

Thus

$$\sum_{i=1}^{q} D_{ij}^2 \geq q^{2k-1}, \qquad j \in n,$$

from which we obtain

$$D = nq^{2k} - \sum_{j\in n}\sum_{i=1}^{q} D_{ij}^2 \leq nq^{2k-1}(q-1).$$

Combining these two bounds for D we conclude that

$$q^k(q^k - 1)d \leq D \leq nq^{2k-1}(q-1),$$

and the statement now follows by comparing the left hand side and the right hand side. □

A few remarks concerning this bound are in order.

2.1.10 Remarks

1. Since the term on the right hand side of the bound may evaluate to a fraction, the bound can actually be read as

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

However, since we want to investigate what happens if the bound is met with equality, let us consider the inequality as stated in 2.1.9.

2. Equality holds in 2.1.9 under the following two conditions:
   (a) The distance between any two distinct codewords is equal to a constant (such a code is called *equidistant*.)
   (b) At any coordinate position, each field element appears equally often.
   An example for such a code is the simplex-code (cf. Exercise 2.1.5).

3. We may reformulate the Plotkin-bound as a bound for the number of codewords or, equivalently, for the dimension of a linear code of length n and minimum distance d over $\mathbb{F}_q$ as

$$q^k \leq \frac{d}{d - n(q-1)/q}\,, \tag{2.1.11}$$

   provided that $d > n(q-1)/q$. ◇

Next we collect some facts about $n_{\min}(k, d, q)$.

Lemma *If there exists an (n, k, d, q)-code with $d > 1$, then for each $1 \leq d' < d$ there exist (n, k, d', q)-codes.* **2.1.12**

Proof: Since $d > 1$, we may assume without loss of generality that the (n, k, d)-code C whose existence we assume has a systematic generator matrix

$$\Gamma = (I_k \mid A) = \left(e^{(0)^\top} \,\middle|\, \ldots \,\middle|\, e^{(k-1)^\top} \,\middle|\, u^{(k)^\top} \,\middle|\, \ldots \,\middle|\, u^{(n-1)^\top}\right),$$

where A is a $k \times (n-k)$-matrix with $n - k \geq 1$. Replacing in Γ a column $u^{(j)^\top}$, $k \leq j < n$, by a column of zeros, we obtain a code C' with parameters (n, k, d) or $(n, k, d-1)$. The minimum distance of C' equals $d-1$ if and only if there exists a codeword $c \in C$ of weight d such that $c_j \neq 0$. Summarizing, the replacement of a column of A by a column of zeros either leaves the minimum distance of C unchanged or decreases it by 1.

We start with the code C of minimum distance $d > 1$. Replacing one by one all the columns of A by columns of zeros, we eventually obtain a matrix of the form $(I_k \mid 0)$ which is the generator matrix of an $(n, k, 1)$-code. In each step, the minimum distance either stays put or decreases by 1. Whence by this procedure we construct (n, k, d')-codes for all $1 \leq d' < d$. □

Lemma *Let q be a power of a prime and let k and d be positive integers. Then:* **2.1.13**

1. $n_{\min}(k, 1, q) = k$, *for* $k \geq 1$.
2. $n_{\min}(1, d, q) = d$, *for* $d \geq 1$.

3. *If* $d' \leq d$, *then* $n_{\min}(k, d', q) \leq n_{\min}(k, d, q)$ *for* $k \geq 1$.

4. *If* $k \geq 2$, *then* $n_{\min}(k, d, q) \geq d + n_{\min}(k-1, \lceil d/q \rceil, q)$ *for* $d \geq 1$, *where* $\lceil r \rceil$ *denotes as usual the least integer greater than or equal to* r.

Proof: The first two assertions are clear. In order to prove the third, we consider an $(n_{\min}(k,d,q), k, d, q)$-code C. According to 2.1.12, there also exists an $(n_{\min}(k,d,q), k, d', q)$-code for any $d' \leq d$. Whence $n_{\min}(k,d',q) \leq n_{\min}(k,d,q)$. In other words, the function $n_{\min}(k,d,q)$ is monotone increasing in the second argument. Lastly, in order to prove the final assertion, we consider again a code C of type $(n_{\min}(k,d,q), k, d, q)$. Let w be a vector of weight d in C, and assume that this vector is an element of a basis of C. Permuting columns and multiplying them with suitable constants, if necessary, we can assume that $w = (\mathbf{1}_d, \mathbf{0})$ and we see that C is linearly isometric to a code with generator matrix

$$\Gamma := \left(\begin{array}{c} w \\ \hline * \end{array}\right) := \left(\begin{array}{c|c} \mathbf{1}_d & \mathbf{0} \\ \hline \Gamma_1 & \Gamma_2 \end{array}\right).$$

Here, the top row w of Γ is of Hamming weight d, and Γ_1 and Γ_2 are matrices of size $(k-1) \times d$ and $(k-1) \times (n_{\min}(k,d,q) - d)$, respectively.

We claim that Γ_2 is of rank $k-1$. Assume not. Then the rank of Γ is at most $k-2$, and we can assume that the first row of Γ_2 contains only zeros. By the condition on the minimum distance, all elements in the corresponding row of Γ_1 are nonzero. Using an elementary row transformation, we can transform at least one further element of the top row of Γ into zero, which of course contradicts the fact that w was a word of minimum weight d. This proves the claim.

At this point, we know that the code C_2 generated by Γ_2 has the parameters $(n_{\min}(k,d,q) - d, k-1, d_2)$, for some d_2 which is not yet known. Therefore

2.1.14
$$n_{\min}(k-1, d_2, q) \leq n_{\min}(k,d,q) - d.$$

Now we consider $c = (c^{(1)}, c^{(2)}) \in C$ where $c^{(2)} \in C_2$ and $\mathrm{wt}(c^{(2)}) = d_2$. By the pigeon-hole principle, there exists an element $\alpha \in \mathbb{F}_q$ which occurs at least $\lceil d/q \rceil$ many times in $c^{(1)}$. Without loss of generality, we can assume that $\alpha \in \mathbb{F}_q^*$. (If $\alpha = 0$, then choose any $\alpha_0 \in \mathbb{F}_q^*$ and replace c by the codeword $c + \alpha_0 w$ in which the element α_0 occurs at least $\lceil d/q \rceil$-many times among the first d components. Moreover, the last $n_{\min}(k,d,q) - d$ components of $c + \alpha_0 w$ are the same as in c.) Hence, subtracting the α-fold of the top row w of Γ from c yields the estimate

$$d \leq \mathrm{wt}(c - \alpha w) \leq (d - \lceil d/q \rceil) + d_2,$$

and so $d_2 \geq \lceil d/q \rceil$. Furthermore, since the function $n_{\min}(k,d,q)$ is monotone in the second argument (this was proved in 3), we get

$$n_{\min}(k-1,d_2,q) \geq n_{\min}(k-1,\lceil d/q \rceil,q).$$

This together with 2.1.14 implies the desired inequality. □

We remark that the fourth result of the previous Lemma is also known under the name "one-step Griesmer-bound". We will see that this result is essential for the Griesmer-bound, which we will present next. Recall that the Singleton-bound implies a bound for the length of (n,k,d)-codes,

$$n_{\min}(k,d,q) \geq k+d-1. \qquad \textbf{2.1.15}$$

A better estimate is obtained from the following bound, whose binary version was discovered by Griesmer [76]. We present the form for general q which is due to Solomon and Stiffler [186].

The Griesmer-bound *Each linear (n,k,d,q)-code satisfies* **2.1.16**

$$n \geq \sum_{i \in k} \lceil d/q^i \rceil.$$

Proof: The case $k=1$ is trivial, so we may assume that $k \geq 2$. Applying the inequality of the fourth item of 2.1.13 iteratively we obtain the statement (see also Exercise 2.1.7):

$$\begin{aligned}
n &\geq n_{\min}(k,d,q) \\
&\geq d + n_{\min}(k-1,\lceil d/q \rceil,q) \\
&\geq d + \lceil d/q \rceil + n_{\min}\Big(k-2, \underbrace{\left\lceil \frac{\lceil d/q \rceil}{q} \right\rceil}_{=\lceil d/q^2 \rceil}, q\Big) \\
&\geq \dots \\
&\geq \sum_{i \in k-1} \lceil d/q^i \rceil + \underbrace{n_{\min}(1,\lceil d/q^{k-1} \rceil,q)}_{=\lceil d/q^{k-1} \rceil} \\
&= \sum_{i \in k} \lceil d/q^i \rceil.
\end{aligned}$$

□

Example We claim that there is no binary $(31,10,13)$-code. To see this, we apply the Griesmer-bound, which gives us **2.1.17**

$$\begin{aligned}
n \;&\geq\; 13 + \left\lceil \frac{13}{2} \right\rceil + \left\lceil \frac{13}{4} \right\rceil + \left\lceil \frac{13}{8} \right\rceil + \left\lceil \frac{13}{16} \right\rceil + \dots + \left\lceil \frac{13}{512} \right\rceil \\
&=\; 13+7+4+2+1+1+1+1+1+1 = 32.
\end{aligned}$$

But our code has length 31, which is a contradiction. ◇

For each (n,k,d,q)-code C, the nonnegative integer $n-(k+d-1)$ has been called the *defect* of C (see 2.1.15). It can be estimated by an application of the Griesmer-bound:

2.1.18 Theorem *For each (n,k,d,q)-code with defect s we have:*

1. *If $k \geq 2$, then $d \leq q(s+1)$.*
2. *If $k \geq 3$ and $d = q(s+1)$, then $s+1 \leq q$.*

Proof: Both statements follow from the Griesmer-bound: As $\lceil d/q^i \rceil \geq 1$ we have

$$n \geq \sum_{i \in k} \lceil d/q^i \rceil \geq d + \lceil d/q \rceil + (k-2).$$

Assume indirectly that $d > q(s+1)$, and hence $\lceil d/q \rceil \geq s+2$. Then the right hand side is $\geq n+1$, which is clearly a contradiction.

Similarly, from $k \geq 3$ and $d = q(s+1)$ we obtain

$$d + k - 1 + s = n \geq \sum_{i \in k} \lceil d/q^i \rceil \geq d + (s+1) + \left\lceil \frac{s+1}{q} \right\rceil + (k-3),$$

thus $s+1 \geq s + \lceil (s+1)/q \rceil$, which implies that $s+1 \leq q$. □

After these upper bounds we now derive two important *lower bounds*. Such bounds are essentially existence results: they state the existence of good codes. There is a catch, however. It may not always be easy to explicitly *find* the code whose existence is predicted by the lower bound. The first bound, due to Gilbert [67] resembles the Hamming-bound quite astonishingly. The second bound, due to Varshamov [194], turns out to be stronger than the Gilbert-bound (cf. Exercise 2.1.8). Nevertheless, asymptotically the two bounds agree.

2.1.19 The Gilbert-bound *Let q be a power of a prime and $n,k,d \in \mathbb{N}^*$ with $n \geq k,d$. The inequality*

$$\sum_{i \in d} \binom{n}{i} (q-1)^i < q^{n-k+1}$$

implies the existence of a linear (n,k)-code over $\mathbb{F}_q$ with minimum distance at least d.

Proof: Let C be a linear (n,k',d,q)-code with k' maximal. This means that there is no (n,k'',d)-code with $k'' > k'$. Let $\rho(C) = \max_{x \in H(n,q)} \min_{c \in C} d(x,c)$ be the *covering radius* of C, which measures how far away a word in the Hamming space can be from the given code. We claim that $\rho(C) \leq d-1$. Assume otherwise. Let $x \in H(n,q)$ be a vector with

$$d(x,C) := \min_{c \in C} d(x,c) \geq d.$$

Then, for $\lambda, \mu \in \mathbb{F}_q^*$ and $c, c' \in C$, we have

$$d(c + \lambda x, c' + \mu x) = d((\lambda - \mu)x, c' - c) \geq d,$$

unless $\lambda = \mu$ and $c = c'$. This is clear when $\lambda - \mu = 0$, as C has distance d. Otherwise, it follows from the fact that x is at distance $\geq d$ from $c' - c \in C$. The inequality just proved implies that the span of C and x, i.e. $C \oplus \langle x \rangle$, has minimum distance at least d. But $C \oplus \langle x \rangle$ is a linear code of dimension $k' + 1$, which contradicts the fact the k' was the largest possible dimension of such a code. Thus we have proved that $\rho(C) \leq d - 1$.

Now consider an $(n, k, \geq d, q)$-code. If the inequality $q^k \sum_{i \in d} \binom{n}{i}(q-1)^i < q^n$ is satisfied, then the balls of radius $d - 1$ around codewords do not cover $H(n, q)$, i.e. there is a word $x \in H(n, q)$ with $d(x, C) \geq d$, i.e. $\rho(C) \geq d$. But this means that k is not maximal, i.e. there is a bigger code. The code whose existence is claimed can now be constructed directly. Start with the zero-code C, with $k = 0$. As long as the inequality $\sum_{i \in d} \binom{n}{i}(q-1)^i < q^{n-k}$ is satisfied, there is a vector $x \in H(n, q)$ with $d(x, C) > d$. Replace C by $C \oplus \langle x \rangle$, a code of dimension $k + 1$ and repeat the procedure. We stop the procedure if $\sum_{i \in d} \binom{n}{i}(q-1)^i \geq q^{n-k}$ and $q^{k-1} \sum_{i \in d} \binom{n}{i}(q-1)^i < q^{n-(k-1)}$. Thus we end up with a linear $(n, k, \geq d, q)$-code as claimed. □

The Varshamov-bound *Let q be a power of a prime and $n, k, d \in \mathbb{N}^*$ with $n \geq k, d$. The inequality* **2.1.20**

$$\sum_{i \in d-1} \binom{n-1}{i}(q-1)^i < q^{n-k}$$

implies the existence of a linear (n, k)-code over $\mathbb{F}_q$ with minimum distance at least d.

Proof: If $n = k$ the inequality is satisfied only for $d = 1$. In this case there exists the trivial $(n, n, 1)$-code. Now we assume that $n - k \geq 1$. First we prove that $d - 1 \leq n - k$. Assume on the contrary that $d - 1 > n - k$. We obtain, since $d - 2 \geq n - k$ and $n - 1 \geq n - k$,

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

which contradicts our assumption.

Inductively, we will now construct an $(n - k) \times n$-matrix Δ of rank $n - k$, any $d - 1$ columns of which are linearly independent. Then, according to 1.3.10, Δ is a check matrix of an (n, k, d')-code C with $d' \geq d$. We start with the matrix $\Delta_{n-k} = I_{n-k}$ which consists of the $n - k$ unit vectors of length $n - k$. It is of rank $n - k$ and any $d - 1$ columns are linearly independent. If Δ_i with $n - k \leq i < n$ is an $(n - k) \times i$-matrix with the desired properties, we try

to find a vector $u \in \mathbb{F}_q^{n-k}$ such that $\Delta_{i+1} = (\Delta_i \mid u^\top)$ also satisfies these properties. This vector u must be chosen from the set of elements of $\mathbb{F}_q^{n-k}$ which cannot be expressed as a linear combination of at most $d-2$ columns of Δ_i. Of course, any linear combination of at most $d-2$ columns of Δ_i is uniquely defined by its nonzero coefficients. Hence at most

$$\sum_{j \in d-1} \binom{i}{j} (q-1)^j$$

vectors can be written as linear combinations of at most $d-2$ columns of Δ_i. Since

$$\sum_{j \in d-1} \binom{i}{j} (q-1)^j \leq \sum_{j \in d-1} \binom{n-1}{j} (q-1)^j < q^{n-k},$$

there exists a vector u in $\mathbb{F}_q^{n-k}$ such that the system consisting of u and any $d-2$ columns of Δ_i is linearly independent. Therefore Δ_{i+1} is of rank $n-k$ and any $d-1$ columns of Δ_{i+1} are linearly independent. Finally, Δ can be chosen as the matrix Δ_n. □

2.1.21 **Example** In the following table, we display upper and lower bounds for the optimal minimum distance $d_{\max}(n,k,2)$ of binary codes with a given length n and dimension $k \leq n$. For a given pair (n,k), the table shows either the exact value of $d_{\max}(n,k,2)$, or an interval consisting of a lower bound and an upper bound. Subscripts are used to indicate which rule led to the bound. The subscripts V, S, H, G, or P stand for the Varshamov, Singleton, Hamming, Griesmer, or Plotkin-bound, respectively. For example, the table entry for $n = 8$ and $k = 2$ reads $4_V 5_P$ which stands for the two bounds $4 \leq d_{\max}(8,2,2)$ by Varshamov and $d_{\max}(8,2,2) \leq 5$ due to Plotkin.

$n \backslash k$	1	2	3	4	5	6	7	8
1	$1_{V,S}$							
2	$2_{V,S}$	$1_{V,S}$						
3	$3_{V,S}$	$2_{V,S}$	$1_{V,S}$					
4	$4_{V,S}$	$2_{V,H}$	$2_{V,S}$	$1_{V,S}$				
5	$5_{V,S}$	$3_{V,P}$	$2_{V,H}$	$2_{V,S}$	$1_{V,S}$			
6	$6_{V,S}$	$3_V 4_H$	$3_{V,P}$	$2_{V,H}$	$2_{V,S}$	$1_{V,S}$		
7	$7_{V,S}$	$4_{V,P}$	$3_V 4_H$	$3_{V,P}$	$2_{V,H}$	$2_{V,S}$	$1_{V,S}$	
8	$8_{V,S}$	$4_V 5_P$	$4_{V,H}$	$3_V 4_H$	$2_{V,H}$	$2_{V,H}$	$2_{V,S}$	$1_{V,S}$
9	$9_{V,S}$	$5_V 6_H$	$4_{V,G}$	$3_V 4_H$	$3_V 4_H$	$2_{V,H}$	$2_{V,H}$	$2_{V,S}$
10	$10_{V,S}$	$5_V 6_P$	$4_V 5_P$	$4_{V,G}$	$3_V 4_H$	$3_V 4_H$	$2_{V,H}$	$2_{V,H}$

This table will be improved in the next section, and the intervals will be replaced by exact values. ◇

Exercises

E.2.1.1 **Exercise** Show that the following codes are perfect:

1. the (n, n)-code over $\mathbb{F}_q$ for any $n \geq 1$,
2. the n-fold repetition code over $\mathbb{F}_2$ for n odd.

Exercise Verify that the following parameter sets attain the Hamming-bound: $(23, 12, 7, 2)$, $(11, 6, 5, 3)$, $(90, 78, 5, 2)$. (Note that there exist perfect codes only for the first two parameters.) **E.2.1.2**

Exercise Prove that a linear code C is perfect if and only if $\rho(C) = \text{dist}(C)$. **E.2.1.3**

Exercise Prove that 2.1.11 is equivalent to the Plotkin-bound. **E.2.1.4**

Exercise Check that the m-th order q-ary simplex-code meets the Griesmer-bound and the Plotkin-bound. **E.2.1.5**

Exercise Let C be the m-th order binary Hamming-code of length $n = 2^m - 1$. **E.2.1.6**

1. Show that the homogeneous weight enumerator is

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

2. Show that the coefficients A_i in $W_C(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$ satisfy the following recursion:

$$iA_i = \binom{n}{i-1} - A_{i-1} + (i - 2 - n)A_{i-2}$$

for $i \geq 3$ with initial conditions $A_0 = 1$, $A_1 = A_2 = 0$. Hint: Compute the formal derivative w'_C of $w_C(x) = W_C(x, 1)$ and verify that

$$(1 - x^2)w'_C(x) + (1 + nx)w_C(x) = (1 + x)^n.$$

After that, compare coefficients.

Exercise Prove the following formula for positive integers r, s, t: **E.2.1.7**

$$\left\lceil \frac{\lceil r/s \rceil}{t} \right\rceil = \left\lceil \frac{r}{st} \right\rceil.$$

E.2.1.8 Exercise

1. Verify that the Varshamov-bound 2.1.20 is sometimes stronger than the Gilbert-bound 2.1.19. For example, the Varshamov-bound guarantees the existence of a $(7,4,3,2)$-code, whereas the Gilbert-bound only predicts the existence of a $(7,3,3,2)$-code.
2. Prove that the Varshamov-bound is always at least as strong as the Gilbert-bound. Do this by showing that the validity of the inequality in 2.1.19 implies that the inequality in 2.1.20 holds as well. Hint: put $f(x) = \sum_{i\in d-1}\binom{n-1}{i}x^i$ and $g(x) = \sum_{i\in d}\binom{n}{i}x^i$ and verify that $g(x) = (1+x)f(x) + x^{d-1}\binom{n-1}{d-1}$. Then put $x = q-1$.

2.2 2.2 New Codes from Old and the Minimum Distance

Now we describe modifications of codes that permit the construction of new codes from given ones. An interesting application is, for example, that step by step we are able to improve our knowledge on the maximal minimum distance of (n,k)-codes over $\mathbb{F}_q$.

Recall the table obtained in 2.1.21. It contains bounds for maximal minimum distances $d_{\max}(n,k,2)$ of binary codes for $n \leq 10$ and $k \leq 8$. In several places it contains the *exact value* of $d_{\max}(n,k,2)$ while, in a few other places, it gives an *interval* containing the desired value $d_{\max}(n,k,2)$:

2.2.1

$n\backslash k$	1	2	3	4	5	6	7	8
1	1							
2	2	1						
3	3	2	1					
4	4	2	2	1				
5	5	3	2	2	1			
6	6	3 – 4	3	2	2	1		
7	7	4	3 – 4	3	2	2	1	
8	8	4 – 5	4	3 – 4	2	2	2	1
9	9	5 – 6	4	3 – 4	3 – 4	2	2	2
10	10	5 – 6	4 – 5	4	3 – 4	3 – 4	2	2

H.J. Helgert and R.D. Stinaff [85] gave such a table in 1973, containing lower and upper bounds for $d_{\max}(n,k,2)$, where $k \leq n \leq 127$. T. Verhoeff [195] improved it in 1987 by taking into account certain modifications. This work has been continued by Brouwer, who maintains an Internet database [32] with information on the best linear codes. A description of his methods and results

can be found in [33]. Further tables can be found at [13], [27] as well as on the attached compact disc. In this section we introduce elementary modifications, which produce new codes from given ones, and discuss their influence on the table of lower and upper bounds for $d_{\max}(n,k,q)$.

Clearly, the entries in the leftmost column and the elements of the main diagonal are

$$d_{\max}(n,1,q) = n \text{ and } d_{\max}(n,n,q) = 1, \qquad n \geq 1.$$

Also, from 2.1.12 it follows that each value $0 < d \leq d_{\max}(n,k,q)$ occurs as a minimum distance of a suitable (n,k)-code over $\mathbb{F}_q$.

Parity extension Let C be an (n,k,d,q)-code with generator matrix **2.2.2**

$$\Gamma = (\gamma_0 \mid \ldots \mid \gamma_{n-1}),$$

where γ_i denotes the i-th column vector of the matrix. Then the *parity extension* of C is the code $P(C)$ with generator matrix

$$\Gamma' := (\gamma_0 \mid \gamma_1 \mid \ldots \mid \gamma_{n-1} \mid -\sum_{i \in n} \gamma_i),$$

the additional last column of which contains the negative sum of the columns of Γ. The code $P(C)$ is an $(n+1,k)$-code with minimum distance at least d. ◇

Example In the binary case, we obtain $P(C)$ by simply adding an entry 0 to all even codewords, and an entry 1 to all codewords of odd weight. In any case, the resulting codewords of $P(C)$ will have even Hamming weight. ◇ **2.2.3**

Corollary *If C denotes an $(n,k,d,2)$-code with* odd *minimum distance d, then $P(C)$ is an $(n+1,k,d+1,2)$-code.* □ **2.2.4**

Example For the binary $(7,4)$-Hamming-code, the parity extension yields **2.2.5**

$$\Gamma = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \Gamma' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

More generally, by 2.1.6 and 2.2.4 the *extended m-th order binary Hamming-code* is a $(2^m, 2^m - m - 1, 4)$-code. Furthermore, the parity extension of $H(n,q)$ is an $(n+1,n,2)$-code. ◇

Let us see what the parity extension gives for the bounds for $d_{\max}(n,k,2)$ of 2.2.1. In three places, we have codes of length n and dimension k whose

minimum distance is odd. These are the $(5,2,3)$, $(6,3,3)$ and $(7,4,3)$-codes. We deduce that there exist $(6,2,4)$, $(7,3,4)$ and $(8,4,4)$-codes. In the table, we replace the intervals $3-4$ by an exact bound, which is 4, indicated by the boxed entries in 2.2.6. A further consequence is the existence of a $(9,4,4)$-code which results from the $(8,4,4)$-code by attaching a zero coordinate to every codeword. This improves the bound for $d_{\max}(9,4,2)$ to 4, which is shown underlined in the table.

2.2.6

$n\backslash k$	1	2	3	4	5	6	7	8
1	1							
2	2	1						
3	3	2	1					
4	4	2	2	1				
5	5	3	2	2	1			
6	6	$\boxed{4}$	3	2	2	1		
7	7	4	$\boxed{4}$	3	2	2	1	
8	8	4 – 5	4	$\boxed{4}$	2	2	2	1
9	9	5 – 6	4	$\underline{4}$	3 – 4	2	2	2
10	10	5 – 6	4 – 5	4	3 – 4	3 – 4	2	2

The last operation can be formulated as follows:

2.2.7 **Corollary** *For given q and k, the entries of the table $(d_{\max}(n,k,q))_{n,k}$, are weakly increasing downwards in each column, i.e.,*

$$d_{\max}(n+1,k,q) \geq d_{\max}(n,k,q), \qquad n \geq 1. \qquad \square$$

The next modification shows that the entries in these columns increase by at most 1:

2.2.8 **Puncturing a code** Assume that C is an (n,k)-code with $k < n$ and generator matrix

$$\Gamma = (\gamma_0 \mid \ldots \mid \gamma_{n-1}).$$

Then, without loss of generality (recall the definition of linear isometry of codes), we assume that there exists an information set *to which the last coordinate does not belong.* When canceling this component in all codewords, the resulting code $Pu(C)$, which is called *punctured code of* C, has the generator matrix

$$\Gamma' = (\gamma_0 \mid \gamma_1 \mid \ldots \mid \gamma_{n-2}).$$

According to our choice of the information set of C and of the canceled coordinate, the dimension k of the code is not changed and, therefore, $Pu(C)$ is an $(n-1,k)$-code. Its minimum distance is at least $d-1$. $\diamond$

Using 2.1.12, we obtain

Corollary 2.2.9 *For $k < n$, the existence of an (n,k,d,q)-code implies that there is also an $(n-1,k,d-1,q)$-code. In particular, the entries in a column of the matrix $(d_{\max}(n,k,q))_{n,k}$ increase by at most 1 at a time, i.e.,*

$$d_{\max}(n+1,k,q) - d_{\max}(n,k,q) \leq 1, \qquad n \geq 1. \qquad \square$$

Puncturing improves the preceding table in the following two boxed entries, whereas the underlined value follows from 2.2.4:

$n\backslash k$	1	2	3	4	5	6	7	8
1	1							
2	2	1						
3	3	2	1					
4	4	2	2	1				
5	5	3	2	2	1			
6	6	4	3	2	2	1		
7	7	4	4	3	2	2	1	
8	8	4 – 5	4	4	2	2	2	1
9	9	5 – 6	4	4	$\boxed{3}$	2	2	2
10	10	5 – 6	4 – 5	4	$\underline{4}$	$\boxed{3}$	2	2

2.2.10

Another way of combining codes is the concatenation, and there are essentially *two* different ways of doing this:

The concatenation (outer direct sum) 2.2.11 Let C_i be an (n_i,k_i,d_i,q)-code with generator matrix Γ_i for $i = 0,1$. The *outer direct sum* of C_0 and C_1 is defined as

$$C_0 \dot{+} C_1 := \left\{ (c \mid c') \;\middle|\; c \in C_0, c' \in C_1 \right\}.$$

It is clear that $C_0 \dot{+} C_1$ is an $(n_0+n_1, k_0+k_1, \min\{d_0,d_1\}, q)$-code with generator matrix

$$\left(\begin{array}{c|c} \Gamma_0 & 0 \\ \hline 0 & \Gamma_1 \end{array}\right).$$

The outer direct sum can be expressed as

$$C_0 \dot{+} C_1 = \left\{ (u \cdot \Gamma_0 \mid v \cdot \Gamma_1) \;\middle|\; u \in \mathbb{F}_q^{k_0},\ v \in \mathbb{F}_q^{k_1} \right\}.$$

in terms of the generator matrices. $\diamond$

Since the minimum distance of the outer direct sum is the minimum of the minimum distances of the summands, this construction is not very exciting as far as $d_{\max}$ is concerned. But it leads to another concatenation. In the particular case $k_0 = k_1$ we can consider a subset of the outer sum which is, in a certain sense, a diagonal:

2.2.12 **The diagonal concatenation ((u,v)-construction)** Let C_i be an (n_i,k,d_i,q)-code with generator matrix Γ_i for $i=0,1$. Then there exists an (n_0+n_1,k,d,q)-code $C:=(C_0,C_1)$, with $d\geq d_0+d_1$, called the *diagonally concatenated code* or the (u,v)-*construction* applied to C_0 and C_1. It is generated by $\Gamma:=(\Gamma_0\mid\Gamma_1)$,

$$C:=\left\{(w\cdot\Gamma_0\mid w\cdot\Gamma_1)\;\middle|\;w\in\mathbb{F}_q^k\right\}. \qquad \diamond$$

For example, we know from 2.2.10 that there exist both a $(5,2,3,2)$-code and a $(3,2,2,2)$-code, and so we obtain via diagonal concatenation of these codes an $(8,2,5,2)$-code: Since $d_{\max}(8,2,2)\in\{4,5\}$, we get $d_{\max}(8,2,2)=5$. In the same way we deduce from $d_{\max}(6,3,2)=3$ and $d_{\max}(4,3,2)=2$ that $d_{\max}(10,3,2)=5$. Moreover, using 2.2.4 we obtain that $d_{\max}(9,2,2)=6$, whereas $d_{\max}(10,2,2)=6$ follows from the fact that the values in each column are increasing, as shown in 2.2.7. This way we improve the preceding table, obtaining

2.2.13

$n\backslash k$	1	2	3	4	5	6	7	8
1	1							
2	2	1						
3	3	2	1					
4	4	2	2	1				
5	5	3	2	2	1			
6	6	4	3	2	2	1		
7	7	4	4	3	2	2	1	
8	8	$\boxed{5}$	4	4	2	2	2	1
9	9	$\boxed{6}$	4	4	3	2	2	2
10	10	$\boxed{6}$	$\boxed{5}$	4	4	3	2	2

as the upper left hand corner of the table $(d_{\max}(n,k,2))_{n,k}$.

Hence, the upper left hand part of the desired table of maximal minimum distances of binary codes looks as follows:

$$(d_{\max}(n,k,2))_{n,k}=\begin{pmatrix}
1 & & & & & & & & & \\
2 & 1 & & & & & & & & \\
3 & 2 & 1 & & & & & & & \\
4 & 2 & 2 & 1 & & & & & & \\
5 & 3 & 2 & 2 & 1 & & & & & \\
6 & 4 & 3 & 2 & 2 & 1 & & & & \\
7 & 4 & 4 & 3 & 2 & 2 & 1 & & & \\
8 & 5 & 4 & 4 & 2 & 2 & 2 & 1 & & \\
9 & 6 & 4 & 4 & 3 & 2 & 2 & 2 & 1 & \\
10 & 6 & 5 & 4 & 4 & 3 & 2 & 2 & 2 & 1 \\
\vdots & & & & & & & & & \ddots
\end{pmatrix}.$$

From this table we can directly deduce that the upper left hand corner of the matrix of $n_{\min}(k,d,2)$ is given by

$$(n_{\min}(k,d,2))_{k,d} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ 2 & 3 & 5 & 6 & 8 & 9 & \dots & \\ 3 & 4 & 6 & 7 & 10 & \dots & & \\ 4 & 5 & 7 & 8 & \dots & & & \\ 5 & 6 & 9 & 10 & \dots & & & \\ 6 & 7 & 10 & \dots & & & & \\ 7 & 8 & \dots & & & & & \\ 8 & 9 & \dots & & & & & \\ 9 & 10 & \dots & & & & & \\ \vdots & & & & & & & \end{pmatrix}.$$

Moreover, for $k_{\max}(n,d,q)$ we obtain

$$(k_{\max}(n,d,2))_{n,d} = \begin{pmatrix} 1 & & & & & & & & \\ 2 & 1 & & & & & & & \\ 3 & 2 & 1 & & & & & & \\ 4 & 3 & 1 & 1 & & & & & \\ 5 & 4 & 2 & 1 & 1 & & & & \\ 6 & 5 & 3 & 2 & 1 & 1 & & & \\ 7 & 6 & 4 & 3 & 1 & 1 & 1 & & \\ 8 & 7 & 4 & 4 & 2 & 1 & 1 & 1 & \\ \vdots & & & & & & & & \ddots \end{pmatrix}.$$

We have seen that the entries in each column of the matrix $(d_{\max}(n,k,q))_{n,k}$ weakly increase and that the difference between two neighbors in the same column is at most 1. Now we note that the diagonal concatenation

$$\Gamma' := (\Gamma \mid I_k)$$

of a generator matrix Γ of an (n,k,d,q)-code and the identity matrix I_k generates an $(n+k,k,d',q)$-code with $d' \geq d+1$.

Corollary **2.2.14** *For $k < n$ the existence of an (n,k,d,q)-code implies the existence of an $(n+k,k,d',q)$-code with $d' > d$. In particular, this shows that the entries in a column of the matrix $(d_{\max}(n,k,q))_{n,k}$ increase by at least 1 within an interval of k values for the length, and so each column of this matrix contains every positive integer at least once.* □

A slight modification of the outer direct sum construction is

2.2.15 **The $(u \mid u+v)$-construction** For $i = 0, 1$ let C_i be an (n, k_i, d_i, q)-code with generator matrix Γ_i. We define a linear code $C_0 \mid C_1$ by putting

$$C_0 \mid C_1 := \{(c, c+c') \mid c \in C_0, c' \in C_1\}.$$

This code is called the $(u \mid u+v)$-*construction* of C_0 and C_1. It is also known as the *semidirect sum* or *Plotkin construction* of C_0 and C_1. A generator matrix of it is

$$\left(\begin{array}{c|c} \Gamma_0 & \Gamma_0 \\ \hline 0 & \Gamma_1 \end{array}\right).$$

The $(u \mid u+v)$-construction $C_0 \mid C_1$ has the parameters

$$\big(2n, k_0 + k_1, \min\{2d_0, d_1\}, q\big).$$

Proof: The statements on the generator matrix, the length, and the dimension of $C_0 \mid C_1$ are clearly true. For the Hamming distance of two different codewords $(c, c+c')$ and $(w, w+w')$ of $C_0 \mid C_1$ the following holds:

$$d(c, w) + d(c+c', w+w') = \mathrm{wt}(c-w) + \mathrm{wt}(c-w+c'-w').$$

In the case when $c' = w'$ this sum is $2d(c, w) \geq 2d_0$, while otherwise we obtain a lower bound:

$$\mathrm{wt}(c-w) + \mathrm{wt}(c-w+c'-w') \geq$$
$$\mathrm{wt}(c-w) + \mathrm{wt}(c'-w') - \mathrm{wt}(c-w) = \mathrm{wt}(c'-w') \geq d_1. \qquad \square$$

2.2.16 **Example** The binary code C_0 with check matrix $\Delta = \mathbf{1}_4$ is a $(4, 3)$-code. Each $c \in C_0$ has even parity because of $c \cdot \Delta^\top = c_0 + c_1 + c_2 + c_3 = 0$. Hence, C_0 consists of all vectors of even weight in $\mathbb{F}_2^4$. We deduce that C_0 is a $(4, 3, 2)$-parity check code. If C_1 denotes the $(4, 1, 4)$-repetition code, then $C_0 \mid C_1$ is an $(8, 4, 4)$-code. $\diamond$

The next construction allows us to deduce properties of the entries in the *subdiagonals* of $(d_{\max}(n, k, q))_{n,k}$, the entries $d_{\max}(n, n-i, q)$, for $i \in \mathbb{N}$ fixed.

2.2.17 **Shortening a code** Assume that the generator matrix $\Gamma = (\gamma_{ij})$ of C with $k > 1$ does not contain a column of zeros and that it is (after a permutation of rows) of the form

$$\left(\begin{array}{c|c} * & \gamma_{0,n-1} \\ \hline \Gamma' & \mathbf{0}^\top \end{array}\right), \text{ where } \gamma_{0,n-1} \neq 0.$$

We indicate the code generated by the submatrix Γ' by $S(C)$,

$$S(C) := \{(c_0, \ldots, c_{n-2}) \mid (c_0, \ldots, c_{n-2}, 0) \in C\}.$$

It is an $(n-1, k-1, d')$-code with $d' \geq d$ and it is called a *shortening* of C (in its last coordinate). $\diamond$

Let $k > 1$. If there is a codeword of C of weight d the last coordinate of which is zero, then the shortening $S(C)$ has minimum distance $d' = d$. This implies

Corollary 2.2.18 *If $n \geq k > 1$, then we obtain from the existence of (n, k, d, q)-codes the existence of $(n-1, k-1, d, q)$-codes. This means for the table $(d_{\max}(n, k, q))_{n,k}$, for fixed q, that its entries are weakly decreasing down each subdiagonal:*

$$d_{\max}(n-1, k-1, q) \geq d_{\max}(n, k, q). \qquad \square$$

This corollary, together with 2.2.4, 2.2.7, 2.2.9, and 2.2.14, yields

Theorem 2.2.19 *The matrix $(d_{\max}(n, k, q))_{n,k}$ of maximal minimum distances of has the following properties:*

1. *It is a lower triangular matrix.*
2. *Its main diagonal consists of 1's.*
3. *The entries in each column are weakly increasing from top to bottom.*
4. *Each column contains every positive integer at least once.*
5. *The entries in each subdiagonal are weakly decreasing from top left to bottom right.*
6. *In the binary case each odd positive integer occurs in each column* exactly *once.*

$\square$

Moreover, we obtain via shortening several inequalities for $n_{\min}(k, d, q)$:

Lemma 2.2.20 *The least length $n_{\min}(k, d, q)$ satisfies:*

1. *If $k \geq 2$, then $n_{\min}(k, d, q) \geq n_{\min}(k-1, d, q) + 1$.*
2. *If $d \geq 2$, then $n_{\min}(k, d, q) > k$.*
3. *If $d \geq 2$, then $n_{\min}(k, d, q) \geq n_{\min}(k, d-1, q) + 1$.*

Proof: 1. Assume that C is an $(n_{\min}(k, d, q), k, d)$-code, $k \geq 2$. Shortening C yields the $(n_{\min}(k, d, q) - 1, k-1, d')$-code $S(C)$ with $d' \geq d$. Consequently

$$n_{\min}(k-1, d, q) \leq n_{\min}(k-1, d', q) \leq n_{\min}(k, d, q) - 1.$$

2. The second statement can be proved by induction on k, using the second assertion of 2.1.13.

3. We again assume that C is an $(n_{\min}(k,d,q),k,d)$-code. Since $d \geq 2$, we obtain from the second assertion that $k < n_{\min}(k,d,q)$. The punctured code $Pu(C)$ is an $(n_{\min}(k,d,q)-1,k,d')$-code with $d' \geq d-1$. Consequently

$$n_{\min}(k,d-1,q) \leq n_{\min}(k,d',q) \leq n_{\min}(k,d,q)-1,$$

which completes the proof. □

Exercises

E.2.2.1 **Exercise** Prove that the weight enumerator of the outer direct sum $C_0 \dot{+} C_1$ is $W_{C_0 \dot{+} C_1}(x,y) = W_{C_0}(x,y) \cdot W_{C_1}(x,y)$.

E.2.2.2 **Exercise** Let C be a linear code over $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q$ let $\sigma(\alpha)$ be the number of codewords $c \in C$ whose parity sum $\sum_{i=0}^{n} c_i$ equals α. Prove that either $\sigma(0) = q^k$ and $\sigma(\alpha) = 0$ for $\alpha \in \mathbb{F}_q^*$, or $\sigma(\alpha) = q^{k-1}$ for all $\alpha \in \mathbb{F}_q$. Hint: The parity sum is a vector space homomorphism $C \to \mathbb{F}_q : c \mapsto \sum_{i \in n} c_i$.

2.3 Further Modifications and Constructions

We continue the description of modifications and constructions.

2.3.1 **Prolongation** A *prolongation* of an (n,k)-code C is an $(n+1,k+1)$-code obtained by adding an information place to C. ◇

2.3.2 **Binary Augmentation** If Γ is the generator matrix of a binary (n,k,d)-code C which does not contain the all-one vector, then the code generated by

$$\left(\frac{\mathbf{1}_n}{\Gamma}\right)$$

is called the *(binary) augmentation* of C. It contains all codewords of C and also the complement of each codeword. (The complement of a binary vector is obtained by replacing each 0 by 1 and vice versa.) The augmentation of C is an $(n,k+1)$-code with minimum distance equal to $\min\{d, n-d'\}$, where $d' := \max\{\mathrm{wt}(c) \mid c \in C\}$ is the *maximum weight* of C. ◇

In the proof of the Griesmer-bound we encountered another modification called

The A-construction Any binary (n,k,d)-code C is linearly isometric to a code with generator matrix **2.3.3**

$$\left(\begin{array}{c|c} \mathbf{1}_d & \mathbf{0}_{n-d} \\ \hline * & \Gamma' \end{array}\right),$$

whose first row contains a codeword of minimum weight whose entries 1 are left-aligned. As shown in 2.1.13, the matrix Γ' generates an $(n-d,k-1)$-code, $A(C)$, called the *A-construction*. The minimum distance of $A(C)$ is at least $\lceil d/q \rceil$. ◇

Example The A-construction enables us to prove that there cannot be a binary $(16,6,7)$-code. Assume on the contrary that there is a $(16,6,7)$-code C. Using the A-construction we obtain a binary $(9,5,4)$-code $A(C)$ so that $9 \geq n_{\min}(5,4,2)$, which contradicts our previous result that $n_{\min}(5,4,2) = 10$. **2.3.4**
◇

Corollary *The existence of an (n,k,d,q)-code implies the existence of a linear code of type* **2.3.5**

$$(n-d, k-1, \geq \lceil d/q \rceil, q).$$ □

The next modification uses the check matrix of a code.

The Y1-construction Without loss of generality, we assume that the check matrix Δ of an (n,k,d)-code with $n-1 > k$ is of the form **2.3.6**

$$\Delta = \left(\begin{array}{c|c} \mathbf{1}_{d^\perp} & \mathbf{0}_{n-d^\perp} \\ \hline * & \Delta' \end{array}\right),$$

where the first row is an element of minimum weight $d^\perp$ belonging to $C^\perp$. If $d^\perp \leq k$, then the submatrix Δ' is the check matrix of an $(n-d^\perp, k-d^\perp+1)$-code, whose minimum distance is at least d by 1.3.10. This construction is called the *Y1-construction*. ◇

A generalization of the Y1-construction is

The B-construction Assume the existence of an (n,k,d,q)-code C with $n-1 > k$ and $d_{\max}(n,n-k,q) \leq k$, which guarantees that $d^\perp \leq k$. From the (n,k,d,q)-code C we obtain by Y1-construction an $(n-d^\perp, k-d^\perp+1, d', q)$-code C' with $d' \geq d$. Hence, for all s with $d^\perp \leq s \leq k$, the *B-construction* yields, by successive shortening, $(n-s, k-s+1)$-codes $B_s(C)$ with minimum distance at least d. ◇ **2.3.7**

2.3.8 **Example** Using the B-construction, one can give another proof that there is no binary $(16,6,7)$-code. Assume on the contrary that there is such a code. In order to apply the B-construction, we need an upper bound on the minimum distance of the dual code, which is a $(16,10)$-code. The Hamming-bound shows that there is no $(16,10,5)$-code, since

$$\binom{16}{0}+\binom{16}{1}+\binom{16}{2}=1+16+8\cdot 15=137\not\leq 2^{16-10}=64.$$

Thus $d_{\max}(16,10,2)\leq 4=s\leq 6=k$. The assumptions for the B-construction are satisfied, and we can produce from the $(16,6,7)$-code a $(16-4,6-4+1,7)=(12,3,7)$-code. But such a code does not exist because the parameters do not satisfy the Plotkin-bound:

$$d=7\not\leq\left\lfloor\frac{12\cdot 2^2\cdot 1}{2^3-1}\right\rfloor=\left\lfloor\frac{48}{7}\right\rfloor=\lfloor 6+6/7\rfloor=6.$$

This shows that the assumption was invalid, i.e. there does not exist a $(16,6,7)$-code, i.e. $d_{\max}(16,6,2)\leq 6$. ◇

Another interesting combination of codes is

2.3.9 **The X-construction** It applies to chains of codes

$$C_1\subset C_0\subseteq\mathbb{F}_q^n,$$

which means that C_1 is a proper *subcode* of the code C_0. We can assume that C_1 is generated by the k_1-rowed submatrix Γ_1 of the generator matrix

$$\Gamma_0=\left(\frac{\Gamma'}{\Gamma_1}\right)$$

of C_0 with $1\leq k_1<k_0$. If C_2 denotes an (n_2,k_0-k_1,d_2)-code with generator matrix Γ_2, then

$$\Gamma=\left(\begin{array}{c|c}\Gamma' & \Gamma_2\\ \hline \Gamma_1 & 0\end{array}\right)$$

generates a code C called the *X-construction*, which is of type (n_0+n_2,k_0,d,q) with $d\geq\min\{d_1,d_0+d_2\}$.

Proof: The statements on the length and on the dimension are obviously true. The surjective linear mapping

$$\phi\colon C_0\to C_2\ :\ v\cdot\Gamma_0\mapsto v\cdot\left(\frac{\Gamma_2}{0}\right),\qquad v\in\mathbb{F}_q^{k_1},$$

is well-defined and has kernel C_1. Therefore, the code C has the form

$$C=\left\{(c,\phi(c))\ \middle|\ c\in C_0\right\}.$$

For each nonzero $c \in C_0$ the following holds:

$$\mathrm{wt}(c, \phi(c)) = \mathrm{wt}(c) + \mathrm{wt}(\phi(c)) \geq \begin{cases} d_1 & \text{if } c \in C_1, \\ d_0 + d_2 & \text{else.} \end{cases}$$

□

Example The binary $(5,3,1)$-code C_0 generated by **2.3.10**

$$\Gamma_0 = \left(\begin{array}{ccccc} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 \end{array}\right)$$

contains a $(5,1,4)$-subcode C_1 with generator matrix $\Gamma_1 = (1 \quad 1 \quad 1 \quad 0 \quad 1)$. Together with the binary $(3,2,2)$-code C_2, generated by

$$\Gamma_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

we obtain via X-construction an $(8,3,3)$-code with generator matrix

$$\Gamma = \left(\begin{array}{ccccc|ccc} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right).$$

◇

Now we introduce a construction that gives, for example, one of the most famous codes, the binary Golay-code G_{24}.

The $(u+w \mid v+w \mid u+v+w)$-construction For $i = 0,1$ let C_i be an (n, k_i, d_i, q)-code, generated by Γ_i. The *$(u+w \mid v+w \mid u+v+w)$-construction*, applied to C_0 and C_1, is the linear code with generator matrix **2.3.11**

$$\left(\begin{array}{c|c|c} \Gamma_0 & 0 & \Gamma_0 \\ \hline \Gamma_1 & \Gamma_1 & \Gamma_1 \\ \hline 0 & \Gamma_0 & \Gamma_0 \end{array}\right).$$

It is, therefore, the following set:

$$\{(u+w \mid v+w \mid u+v+w) \mid u, v \in C_0, w \in C_1\}.$$

It is a $(3n, 2k_0 + k_1)$-code. ◇

Here is the announced prominent example:

2.3.12 **Example** Let C_0 be the extended third-order binary Hamming-code with generator matrix Γ_0 as in 2.2.5. Now reverse the columns of the (unextended) Hamming-code, and let C_1 be the parity extension of this code, i.e. C_1 is generated by

$$\Gamma_1 := \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

We know that C_0 and C_1 are both $(8,4,4,2)$-codes. From the $(u+w \mid v+w \mid u+v+w)$ construction, we obtain the following generator matrix $\Gamma = \Gamma_{24}$ of a binary $(24,12)$-code.

2.3.13

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc} 1&1&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \\ 1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&1 \\ 0&1&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1 \\ 1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&0 \\ \hline 0&0&0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0&1&1&1 \\ 0&0&1&0&1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1&0&1&1 \\ 0&1&0&0&1&1&0&1&0&1&0&0&1&1&0&1&0&1&0&0&1&1&0&1 \\ 1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0 \\ \hline 0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&1&1&0&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0 \end{array}\right).$$

One can show (see below) that its minimum distance is 8. This code is the binary *Golay-code* G_{24}, one of the most prominent linear codes. In fact, it can be shown that this code is the unique (up to linear isometry) code with parameters $(24,12,8,2)$. It played an important role during the Voyager 1 and 2 missions to Jupiter and Saturn in the late 1970s. A reason for its importance is that it carries many interesting combinatorial structures (like Steiner systems, etc.), and it was used even in the classification of finite simple groups (cf. [40]). ◇

2.3.14 **Theorem** *The binary code C generated by the matrix Γ_{24} of 2.3.13 is a self-dual $(24,12,8)$-code.*

Proof: The codes C_0 and C_1 consist of 16 words of length 8 each, as shown in Table 2.1.

Table 2.1 The words of C_0 and C_1

message v	$v \cdot \Gamma_0$	$v \cdot \Gamma_1$
$(0,0,0,0)$	$(0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0)$
$(1,0,0,0)$	$(1,1,0,1,0,0,0,1)$	$(0,0,0,1,0,1,1,1)$
$(0,1,0,0)$	$(1,0,1,0,1,0,0,1)$	$(0,0,1,0,1,0,1,1)$
$(1,1,0,0)$	$(0,1,1,1,1,0,0,0)$	$(0,0,1,1,1,1,0,0)$
$(0,0,1,0)$	$(0,1,1,0,0,1,0,1)$	$(0,1,0,0,1,1,0,1)$
$(1,0,1,0)$	$(1,0,1,1,0,1,0,0)$	$(0,1,0,1,1,0,1,0)$
$(0,1,1,0)$	$(1,1,0,0,1,1,0,0)$	$(0,1,1,0,0,1,1,0)$
$(1,1,1,0)$	$(0,0,0,1,1,1,0,1)$	$(0,1,1,1,0,0,0,1)$
$(0,0,0,1)$	$(1,1,1,0,0,0,1,0)$	$(1,0,0,0,1,1,1,0)$
$(1,0,0,1)$	$(0,0,1,1,0,0,1,1)$	$(1,0,0,1,1,0,0,1)$
$(0,1,0,1)$	$(0,1,0,0,1,0,1,1)$	$(1,0,1,0,0,1,0,1)$
$(1,1,0,1)$	$(1,0,0,1,1,0,1,0)$	$(1,0,1,1,0,0,1,0)$
$(0,0,1,1)$	$(1,0,0,0,0,1,1,1)$	$(1,1,0,0,0,0,1,1)$
$(1,0,1,1)$	$(0,1,0,1,0,1,1,0)$	$(1,1,0,1,0,1,0,0)$
$(0,1,1,1)$	$(0,0,1,0,1,1,1,0)$	$(1,1,1,0,1,0,0,0)$
$(1,1,1,1)$	$(1,1,1,1,1,1,1,1)$	$(1,1,1,1,1,1,1,1)$

By inspection, we see that $C_0 \cap C_1 = \{\mathbf{0}_8, \mathbf{1}_8\}$. Also, we know that C_0 and C_1 are both self-dual with weight enumerator $1 + 14x^4 + x^8$. The statement about the dimension of C is clear, since the 12 vectors of the form $(u, \mathbf{0}, u)$, $(\mathbf{0}, v, v)$ and (w, w, w) are linearly independent, provided that u and v run through a basis of C_0 and w is taken from a basis for C_1. It is easy to check that C is self-orthogonal, and hence self-dual (Exercise 2.3.2). By Exercise 1.3.19, in a self-orthogonal code, the sum of 4-divisible codewords is 4-divisible. In C, any word can be written as a sum of vectors of the form $(u, \mathbf{0}, u)$, $(\mathbf{0}, v, v)$ and (w, w, w), with $u, v \in C_0$ and $w \in C_1$. Since u, v and w are all 4-divisible, so are the three vectors and hence any vector in C. To show that the minimum distance of C is 8, we need to exclude the existence of words of weight 4. For this, let us assume that $c \in C$ is a word of weight less than 8. By Exercise 1.2.14, the sum of even vectors is even. Hence each of the three components of $c = (u + w, v + w, u + v + w)$ is even. In order to have weight either 4 or 0, at least one of the components must be zero. But $u, v \in C_0$ and $w \in C_1$, and we have seen that $C_0 \cap C_1$ consists of $\mathbf{0}_8$ and $\mathbf{1}_8$. Consider the case $w = \mathbf{0}_8$. Then $c = (u, v, u + v)$. Since C_0 only has words of weight $0, 4$ and 8, we have $c = 0$. Otherwise, if $w = \mathbf{1}_8$, then $c = (u + \mathbf{1}, v + \mathbf{1}, u + v + \mathbf{1})$. Again it follows that $c = 0$. This proves the assertion. □

A further important way of combining two codes is the following product:

2.3.15 **The tensor product** We recall from multilinear algebra that the *tensor product* $C_0 \otimes C_1$ of two linear codes C_0, C_1 can be defined as follows: It consists of the elements $c \otimes c'$, where $c \in C_0$ and $c' \in C_1$, and

$$c \otimes c' := \big(c_0 c'_0, \dots, c_0 c'_{n_1-1}, \dots, c_{n_0-1} c'_0, \dots, c_{n_0-1} c'_{n_1-1}\big).$$

In other words, the generator matrix is the Kronecker product

$$\Gamma := \Gamma_0 \otimes \Gamma_1 := \left(\begin{array}{c|c|c} \gamma_{00}\Gamma_1 & \dots & \gamma_{0,n_0-1}\Gamma_1 \\ \hline \dots & \dots & \dots \\ \hline \gamma_{k_0-1,0}\Gamma_1 & \dots & \gamma_{k_0-1,n_0-1}\Gamma_1 \end{array}\right).$$

If C_i is a (n_i, k_i, d_i)-code, then by Exercise 2.3.5 the parameters of $C := C_1 \oplus C_2$ are

$$(n, k, d, q) = (n_0 n_1, k_0 k_1, d_0 d_1, q). \qquad \diamond$$

2.3.16 **Examples** The product $C_0 \otimes C_0$ of the binary $(7, 4)$-Hamming-code C_0 with itself is a binary $(49, 16, 9)$-code. If we denote by C_1 the binary $(7, 1)$-repetition code, then each word of the product code $C_0 \otimes C_1$ can be obtained as a 7-fold repetition of a codeword in C_0. $\diamond$

The next two constructions modify the field over which the codes are considered. For the reader not familiar with the theory of finite fields, the missing details will be presented in Chapter 3.

2.3.17 **Restriction** The *restriction* of a code C over $\mathbb{F}_q$ of length n to a subfield $\mathbb{F}$ of $\mathbb{F}_q$ is the code

$$C \downarrow \mathbb{F} := C \cap \mathbb{F}^n,$$

when considered as a linear code over $\mathbb{F}$. $\diamond$

A different way of constructing from a code over $\mathbb{F}_q$ a code over a subfield $\mathbb{F}$ uses the fact that $\mathbb{F}_q$ is a vector space over $\mathbb{F}$.

2.3.18 **Blowing up** If m is the $\mathbb{F}$-dimension of $\mathbb{F}_q$ and

$$B = \{\beta_0, \dots, \beta_{m-1}\}$$

is an $\mathbb{F}$-basis of $\mathbb{F}_q$, then we obtain from the (n, k)-code C over $\mathbb{F}_q$ a linear code of length mn over $\mathbb{F}$ by replacing the components of the codewords in C by the m-tuples with respect to the basis B. This new code is called the *blow up* of C with respect to B. We denote it by $\mathrm{Bl}_B(C)$. Formally speaking, we obtain $\mathrm{Bl}_B(C)$ as the image $\psi_B(C)$ of C under the linear map

$$\psi_B : \mathbb{F}_q^n \to \mathbb{F}^{mn} \ : \ (c_0, \dots, c_{n-1}) \mapsto \big(\phi_B(c_0) \mid \dots \mid \phi_B(c_{n-1})\big),$$

which is the n-fold extension of the coordinate map

$$\phi_B : \mathbb{F}_q \to \mathbb{F}^m : \sum_{i \in m} \kappa_i \beta_i \mapsto (\kappa_0, \ldots, \kappa_{m-1}),$$

with respect to the basis B. This shows that each $\mathbb{F}_q$-basis $\{b^{(0)}, \ldots, b^{(k-1)}\}$ of C yields an $\mathbb{F}$-basis $\{\psi_B(\beta_i b^{(j)}) \mid i \in m,\ j \in k\}$ of $\mathrm{Bl}_B(C)$. The code $\mathrm{Bl}_B(C)$ is therefore an (mn, mk)-code over $\mathbb{F}$. Its minimum distance d' satisfies $d' \geq d$, since from $c_i \neq 0$ we obtain $\phi_B(c_i) \neq 0$, and so $\mathrm{wt}(\phi_B(c_0), \ldots, \phi_B(c_{n-1})) \geq \mathrm{wt}(c)$ holds true for each $c = (c_0, \ldots, c_{n-1}) \in C$. ◇

Example The field $\mathbb{F}_4$ consists of the elements **2.3.19**

$$0,\ 1,\ \alpha,\ \alpha^2,$$

where α is a root of the polynomial $x^2 + x + 1$ and, therefore, $\alpha^2 = \alpha + 1$. We consider the $(3,2)$-code C over $\mathbb{F}_4$ with generator matrix

$$\Gamma = \begin{pmatrix} 1 & \alpha^2 & 0 \\ 0 & 1 & \alpha^2 \end{pmatrix}.$$

It consists of the following codewords:

000	$01\alpha^2$	$1\alpha^2 0$	$\alpha^2 01$
$0\alpha 1$	$\alpha 10$	10α	$0\alpha^2\alpha$
$\alpha^2\alpha 0$	$\alpha 0\alpha^2$	111	$\alpha\alpha\alpha$
$\alpha^2\alpha^2\alpha^2$	$1\alpha\alpha^2$	$\alpha\alpha^2 1$	$\alpha^2 1\alpha.$

This shows that C has minimum distance 2. Its blow up $\mathrm{Bl}_B(C)$ with respect to the $\mathbb{F}_2$-basis $B = \{\alpha, \alpha^2\}$ of $\mathbb{F}_4$ is a binary code, consisting of the words

000000	001101	110100	010011
001011	101100	110010	000110
011000	100001	111111	101010
010101	111001	100111	$011110.$

Hence, $\mathrm{Bl}_B(C)$ is a $(6,4,2)$-code. The restriction of C to $\mathbb{F}_2$ is the repetition code $\{000, 111\}$. ◇

Let us summarize the results on lower and upper bounds for $d_{\max}(n,k,q)$. Following the ideas of T. Verhoeff [195], we may express the bounds in terms of two predicates,

$$(Lb, n, k, d, q) :\Longleftrightarrow \text{there exists an } (n,k,d,q)\text{-code}$$

and

$$(Ub, n, k, d, q) :\Longleftrightarrow \text{there does not exist an } (n,k,d,q)\text{-code},$$

so that

$$(Lb, n, k, d_1, q) \wedge (Ub, n, k, d_2, q) \Longrightarrow d_1 \leq d_{\max}(n, k, q) < d_2.$$

For example, the predicates

$$(Lb, n, n, 1, q),\ (Ub, n, n, 2, q),\ (Lb, n, 1, n, q),\ \text{and}\ (Ub, n, 1, n+1, q)$$

hold true, since over any field $\mathbb{F}_q$ and for any length n there is the $(n, n, 1)$-code $H(n, q)$ and the $(n, 1, n)$-repetition code.

If M denotes one of the modifications of codes described above, then we may deduce further predicates, which we shall denote as $M(b, n, k, d, q)$. Here, b stands for either Lb or Ub and (b, n, k, d, q) denotes a previously known predicate. Thus, we can consider the modifications as operators on the set of predicates. The goal is to tabulate the best known lower and upper bounds for the minimum distance of a linear code with a given length n and dimension k. This can be done in a systematic way by applying all modifications to an initial set of predicates. If this process is repeated sufficiently often, the resulting table will eventually be invariant under these modifications. Let

$$LB(n, k, q) := \max\{d \mid Lb(n, k, d, q)\},\ UB(n, k, q) := \min\{d \mid Ub(n, k, d, q)\}.$$

In the following, we will restrict our attention to binary codes and therefore we will omit the parameter $q = 2$ from the list of arguments. For the nonbinary case, see Exercise 2.3.11.

2.3.20 Theorem *For binary codes the following is true:*

1. *Parity extension:*

$$P(Lb, n, k, d) = \begin{cases} (Lb, n+1, k, d+1) & \text{if } d \text{ is odd,} \\ (Lb, n+1, k, d) & \text{otherwise,} \end{cases} \quad n \geq 1,$$

$$P(Ub, n, k, d) = \begin{cases} (Ub, n-1, k, d-1) & \text{if } d \geq 2 \text{ is even,} \\ (Ub, n-1, k, d) & \text{otherwise,} \end{cases} \quad n > k \geq 1.$$

2. *Puncturing:*

$$Pu(Lb, n, k, d) = (Lb, n-1, k, d-1) \text{ for } n > k \text{ and } d > 1,$$
$$Pu(Ub, n, k, d) = (Ub, n+1, k, d+1).$$

3. *Shortening:*

$$S(Lb, n, k, d) = (Lb, n-1, k-1, d) \text{ for } k > 1,$$
$$S(Ub, n, k, d) = (Ub, n+1, k+1, d).$$

4. A-construction:

$$\begin{aligned} A(Lb,n,k,d) &= (Lb,n-d,k-1,\lceil d/2\rceil) \text{ for } k>1,\\ A(Ub,n,k,d) &= (Ub,n+2d,k+1,2d). \end{aligned}$$

5. B-construction:

$$\begin{aligned} B_1(Lb,n,k,d) &= (Lb,n-s,k-s+1,d)\\ &\quad \text{for } UB(n,n-k)-1\le s\le k.\\ B_2(Ub,n,\ell,s+1) &= (Lb,n-s,n-\ell-s+1,LB(n,n-\ell))\\ &\quad \text{for } UB(n,\ell)-1\le s\le n-\ell.\\ B_3(Ub,n,k,d) &= (Ub,n+s,k+s-1,d),\\ &\quad \text{for } UB(n+s,n-k+1)-1\le s.\\ B_4(Ub,n,\ell,s+1) &= (Ub,n,n-\ell,UB(n-s,n-\ell-s+1))\\ &\quad \text{for } UB(n,\ell)-1\le s\le n-\ell. \end{aligned}$$

Proof: The statements concerning parity extension, puncturing, shortening, and the A-construction are obvious. The B-construction gives, for $k\ge s\ge UB(n,n-k)-1$,

$$(Lb,n,k,d)\wedge(Ub,n,n-k,s+1)\Longrightarrow(Lb,n-s,k-s+1,d) \qquad \textbf{2.3.21}$$

and

$$(Ub,n,k,d)\wedge(Ub,n+s,n-k+1,s+1)\Longrightarrow(Ub,n+s,k+s-1,d). \qquad \textbf{2.3.22}$$

B_1 and B_2 come from 2.3.21, by keeping the first, respectively the second member of the conjunction fixed. Analogously we obtain B_3 and B_4 from 2.3.22. The details are left to the reader (Exercise 2.3.9). □

An invariant table of bounds can be improved by externally obtained bounds or by applications of non-primitive operations. Good lower bounds can be obtained from cyclic codes, from generalized Reed–Solomon-codes, from Alternant-, or Goppa-codes. We introduce these codes later in the Sections 4.5 and 4.6. Typical nonprimitive operations that can be used for such improvements of parameter tables are code combinations like the outer direct sum, (u,v)-construction, $(u\mid u+v)$construction, or the tensor product. In the case when we use prolongation methods, then we obtain infinitely many entries, in which case we must restrict attention to a maximal block length $n_{\max}$.

In case a new predicate $Q=(b,n,k,d,q)$ has been found, the invariance of the parameter table can be restored by the following recursive algorithm:

2.3.23 **Algorithm** To enter a bound in a table of parameter bounds:
Input: A predicate Q, a table of parameters.
Output: The invariant table of parameters that takes Q into account.

Update(Q)
(1) **if** Q improves the table **then**
(2) insert Q into the table;
(3) **for each** primitive modification M **do**
(4) **Update**$(M(Q))$
(5) **end do**
(6) **end if** □

An application of this algorithm to a table of code parameters usually produces many primitive operations that do not improve the table. If we are given two lower bounds for the minimum distance of (n,k)-codes over $\mathbb{F}_q$, then the larger one is considered better. Similarly, the smaller upper bound is preferred. In terms of predicates, with $Q_1 = (b,n,k,d_1,q)$ and $Q_2 = (b,n,k,d_2,q)$ we put

$$(b,n,k,d_1,q) \leq (b,n,k,d_2,q) :\Longleftrightarrow \begin{cases} d_1 \leq d_2 & \text{if } b = Lb, \\ d_1 \geq d_2 & \text{if } b = Ub. \end{cases}$$

Therefore, $Q_1 \leq Q_2$ means that the predicate Q_2 is an estimate which is at least as sharp for $d_{\max}(n,k,q)$ as Q_1. This notion can also be used to compare primitive modifications M_1 and M_2. We write $M_1 \leq M_2$ in order to indicate that for each predicate Q contained in the range of both M_1 and M_2, the inequality $M_1(Q) \leq M_2(Q)$ holds true. We can use that in order to define

$$M_1 = M_2 :\Longleftrightarrow M_1 \leq M_2 \wedge M_2 \leq M_1.$$

For example, the operations A and S commute in the binary case, since

$$\begin{aligned} (S \circ A)(Lb,n,k,d,2) &= S(Lb,n-d,k-1,\lceil d/2 \rceil,2) \\ &= (Lb,n-d-1,k-2,\lceil d/2 \rceil,2) \\ &= A(Lb,n-1,k-1,d,2) \\ &= (A \circ S)(Lb,n,k,d,2) \end{aligned}$$

and

$$\begin{aligned} (S \circ A)(Ub,n,k,d,2) &= S(Ub,n+2d,k+1,2d,2) \\ &= (Ub,n+2d+1,k+2,2d,2) \\ &= A(Ub,n+1,k+1,d,2) \\ &= (A \circ S)(Ub,n,k,d,2). \end{aligned}$$

A detailed analysis of the primitive modifications allows the reduction of the number of recursive calls of functions in **Update** (see Exercise 2.3.11).

Besides the primitive operations we have also discussed some methods for the combination of linear codes. Now we describe how they can be used to improve a table of bounds for $d_{\max}(n,k,d,q)$. Among others we have obtained the following rules:

Corollary **2.3.24**

1. *Outer direct sum:*

$$(Lb, n_1, k_1, d_1, q) \wedge (Lb, n_2, k_2, d_2, q) \Rightarrow (Lb, n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}, q).$$

2. $(u \mid u + v)$*-construction:*

$$(Lb, n, k_1, d_1, q) \wedge (Lb, n, k_2, d_2, q) \Rightarrow (Lb, 2n, k_1 + k_2, \min\{2d_1, d_2\}, q).$$

3. *Tensor product:*

$$(Lb, n_1, k_1, d_1, q) \wedge (Lb, n_2, k_2, d_2, q) \Rightarrow (Lb, n_1 n_2, k_1 k_2, d_1 d_2, q). \qquad \square$$

We refrain from giving the corresponding upper bounds since their influence on the quality of a parameter table has shown to be rather small [203]. Further details on the construction of an invariant table of parameters and its improvement by using code combinations can be found in Exercise 2.3.11.

Exercises

Exercise For binary codes, prove the following expression for the weight of the elements in a $(u + w \mid v + w \mid u + v + w)$-construction: **E.2.3.1**

$$\mathrm{wt}(u + w \mid v + w \mid u + v + w) = 2 \cdot \mathrm{wt}(u \vee v) - \mathrm{wt}(w) + 4 \cdot s,$$

where $s := |\{i \mid u_i = v_i = 0, w_i = 1\}|$ and $u \vee v$ is as defined in Exercise 1.2.14. Derive from this equation that the minimum distance of G_{24} is 8.

Exercise Verify that the code generated by Γ_{24} in 2.3.12 is self-orthogonal. **E.2.3.2**

Exercise Confirm the parameters of the augmentation of a linear code given in 2.3.2. **E.2.3.3**

E.2.3.4 **Exercise** In Multilinear Algebra the *tensor product* $U \otimes V$ of the $\mathbb{F}_q$-vector spaces U and V *of finite dimension* is defined to be the factor group

$$U \otimes V := \mathbb{Z}^{U \times V} / T.$$

Here $\mathbb{Z}^{U \times V}$ means the free abelian group over the cartesian product $U \times V$, the set of mappings f from $U \times V$ to $\mathbb{Z}$ with pointwise addition. The set T indicates the subgroup of $\mathbb{Z}^{U \times V}$ generated by the elements of the following forms

$$\begin{aligned} &(u + u', v) - (u, v) - (u', v), \\ &(u, v + v') - (u, v) - (u, v'), \\ &(u, \alpha v) - (\alpha u, v), \end{aligned}$$

with $u, u' \in U$, $v, v' \in V$, and $\alpha \in \mathbb{F}_q$. The pair $(u, v) \in U \times V$ stands for the element $f_{(u,v)} \in \mathbb{Z}^{U \times V}$, defined by

$$f_{(u,v)}(x, y) = \begin{cases} 1 & \text{if } (u, v) = (x, y), \\ 0 & \text{else.} \end{cases}$$

The elements in $U \otimes V$ are called *tensors*.

1. Prove that the canonical mapping from $\mathbb{Z}^{U \times V}$ onto the factor group, i.e.

$$\otimes \colon \mathbb{Z}^{U \times V} \to \mathbb{Z}^{U \times V} / T \ : \ (u, v) \mapsto u \otimes v := (u, v) + T,$$

satisfies the rules

$$\begin{aligned} (u + u') \otimes v &= u \otimes v + u' \otimes v, \\ u \otimes (v + v') &= u \otimes v + u \otimes v', \\ u \otimes (\alpha v) &= (\alpha u) \otimes v. \end{aligned}$$

2. Verify that $U \otimes V$ turns into an $\mathbb{F}_q$-vector space via

$$\alpha \sum_i \left(u^{(i)} \otimes v^{(i)} \right) := \sum_i \left((\alpha u^{(i)}) \otimes v^{(i)} \right), \qquad \alpha \in \mathbb{F}_q.$$

The elements of $U \otimes V$ are finite sums $\sum_i \left(u^{(i)} \otimes v^{(i)} \right)$ with $u^{(i)} \in U$ and $v^{(i)} \in V$.

3. Show that, if B is a basis of U and B' a basis of V, then

$$\left\{ b \otimes b' \;\middle|\; b \in B,\ b' \in B' \right\}$$

is a basis of $U \otimes V$.

4. Check that each element of $U \otimes V$ can uniquely be expressed in the form

$$\sum_{b \in B,\ b' \in B'} \alpha_{bb'} \left(b \otimes b' \right), \qquad \alpha_{bb'} \in \mathbb{F}_q,$$

and we have

$$\dim(U \otimes V) = \dim(U) \cdot \dim(V).$$

5. Show that the mapping

$$\Phi_{m,n} : \mathbb{F}_q^m \otimes \mathbb{F}_q^n \to \mathbb{F}_q^{m \times n} \; : \; \sum_{i \in m} \sum_{j \in n} \left(\alpha_{ij} e^{(i)} \otimes f^{(j)} \right) \mapsto (\alpha_{ij})_{i,j},$$

(where $e^{(i)}$ and $f^{(j)}$ denote the respective unit vectors in $\mathbb{F}_q^m$ and $\mathbb{F}_q^n$) is an $\mathbb{F}_q$-isomorphism. So the elements of $\mathbb{F}_q^m \otimes \mathbb{F}_q^n$ can be written as $m \times n$-matrices, and we can speak of rows and columns of a tensor.

Exercise Assume that C_i is a linear (n_i, k_i, d_i, q)-code for $i = 0, 1$. Show that $C_0 \otimes C_1$ is an $(n_0 n_1, k_0 k_1, d_0 d_1, q)$-code. **E.2.3.5**

Exercise Let C be a binary $(3, 2)$-parity check code. Evaluate the elements of the product code $C \otimes C$. **E.2.3.6**

Exercise Evaluate a generator matrix of the binary code obtained in 2.3.18 by blowing up. **E.2.3.7**

Exercise Suppose that C is an (n, k, d)-code with $n > k > 1$ and $c' \in C^\perp$ has $\mathrm{wt}(c') = d'$. Show that an $(n-1, k-1, d)$-code exists, the dual code of which contains a codeword of weight $d' - 1$. **E.2.3.8**

Exercise Prove 2.3.20 and rephrase it for nonbinary codes. **E.2.3.9**

Exercise Assume that M is a primitive modification on codes. Iterating the operation M until it does not change the parameters any more is denoted by M^*. Prove that the following assertions (cf. [203]) are true: **E.2.3.10**

$$\begin{aligned}
P \circ Pu &= id \quad \text{for even } d \\
P \circ Pu &\leq id \quad \text{for each } d \\
Pu \circ P &= id \quad \text{for odd } d \\
Pu \circ P &\leq id \quad \text{for each } d \\
P \circ S &= S \circ P \\
Pu \circ S &= S \circ Pu,
\end{aligned}$$

where id denotes the identity mapping on the predicates.

Show that for lower bounds we have:

$$\begin{aligned} A \circ P &\leq P^* \circ A \\ A \circ Pu &\leq A \\ A \circ S &= S \circ A, \end{aligned}$$

while for upper bounds

$$\begin{aligned} A \circ P &= P \circ A \text{ for even } d \\ (Pu)^3 \circ A &= A \circ Pu \\ A \circ S &= S \circ A. \end{aligned}$$

E.2.3.11 **Exercise** Implement a database for the lower and upper bounds of linear binary codes, i.e. of 5-tuples of the form (b, n, k, d, q) where $b = Lb$ or $b = Ub$ and $q = 2$.

1. Implement each of the primitive modifications of 2.3.20.
2. Write a procedure that initializes the database with the "trivial" bounds
$$(Lb, n, n, 1, q), \quad (Lb, n, 1, n, q), \quad (Ub, n, n, 2, q), \quad (Ub, n, 1, n+1, q)$$
for all nonnegative n up to a user defined maximal length $n_{\max}$.
3. Allow for input of external lower and upper bounds to the parameter table. Note that this addition should be combined with an application of the procedure **Update**.
4. Develop a procedure which applies, for fixed block length $n \leq n_{\max}$, the following rules (see 2.3.24) to the entries (lower bounds) of the tables and which inserts newly found lower bounds for codes of length n:
   - Outer direct sum:
   $$(Lb, n_0, k_0, d_0, q) \wedge (Lb, n - n_0, k_1, d_1, q) \Rightarrow (Lb, n, k_0 + k_1, \min\{d_0, d_1\}, q).$$
   - $(u \mid u + v)$-construction:
   $$(Lb, \frac{n}{2}, k_0, d_0, q) \wedge (Lb, \frac{n}{2}, k_1, d_1, q) \Rightarrow (Lb, n, k_0 + k_1, \min\{2d_0, d_1\}, q).$$
   - Tensor product:
   $$(Lb, n_0, k_0, d_0, q) \wedge (Lb, \frac{n}{n_0}, k_1, d_1, q) \Rightarrow (Lb, n, k_0 k_1, d_0 d_1, q).$$
5. Use the program in order to search for good codes. After the initialization of the table, add lower bounds from the existence results of Chapter 9. Also, use parameters of Reed–Muller-codes (cf. Section 2.4), BCH-codes (Section 4.3) as lower bounds. Then apply the combination methods described above. Compare the results with the list of best known binary linear codes [32].

Exercise Assume that C_i is a linear code with check matrix Δ_i for $i = 0, 1$. Show that **E.2.3.12**

$$\left(\begin{array}{c|c} \Delta_0 & 0 \\ \hline 0 & \Delta_1 \end{array}\right)$$

is a check matrix of $C_0 \dotplus C_1$.

Exercise Let C_0, C_1 and C_2 be linear codes. Prove the following properties of the outer direct sum: **E.2.3.13**

- If C_0 is linearly isometric to C_0' and C_1 linearly isometric to C_1', then $C_0 \dotplus C_1$ is linearly isometric to $C_0' \dotplus C_1'$.
- $C_0 \dotplus C_1$ is linearly isometric to $C_1 \dotplus C_0$.
- $C_0 \dotplus (C_1 \dotplus C_2) = (C_0 \dotplus C_1) \dotplus C_2$.
- $(C_0 \dotplus C_1)^\perp = C_0^\perp \dotplus C_1^\perp$.

Exercise Let A, B, C and D be matrices over a field $\mathbb{F}$. Prove the following properties of the Kronecker product: **E.2.3.14**

- $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.
- $(A \otimes B)^\top = B^\top \otimes A^\top$.
- If the number of columns of A respectively B coincides with the number of rows of C respectively D, then $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$.
- If A is an $r \times s$-matrix and B a $t \times u$-matrix, then there exist permutations $\pi \in S_{rt}$ and $\sigma \in S_{su}$, so that $A \otimes B = M_\pi \cdot (B \otimes A) \cdot M_\sigma$, where M_π and M_σ are the permutation matrices corresponding to π and σ. Determine the two permutations π and σ which depend only on the numbers r, s, t, and u but not on the particular values of the matrices A and B.

Exercise Let C_0, C_1 and C_2 be linear codes. Prove the following properties of the tensor product: **E.2.3.15**

- If C_0 is linearly isometric to C_0' and C_1 linearly isometric to C_1', then $C_0 \otimes C_1$ is linearly isometric to $C_0' \otimes C_1'$.
- $C_0 \otimes C_1$ is linearly isometric to $C_1 \otimes C_0$.
- $C_0 \otimes (C_1 \otimes C_2)$ is linearly isometric to $(C_0 \otimes C_1) \otimes C_2$.
- $C_0 \otimes (C_1 \dotplus C_2)$ is linearly isometric to $(C_0 \otimes C_1) \dotplus (C_0 \otimes C_2)$.
- In general, $(C_0 \otimes C_1)^\perp$ is not linearly isometric to $C_0^\perp \otimes C_1^\perp$.

E.2.3.16 **Exercise** Assume that C_i is a linear (n_i, k_i)-code with a systematic generator matrix $(I_{k_i} \mid A_i)$ for $i = 0, 1$. Show that $C_0 \otimes C_1$ is linearly isometric to the code generated by

$$(I_{k_0} \otimes I_{k_1} \mid I_{k_0} \otimes A_1 \mid A_0 \otimes I_{k_1} \mid A_0 \otimes A_1).$$

If we denote the last $n_0 n_1 - k_0 k_1$ columns of this matrix by B, prove that $(I_{n_0 n_1 - k_0 k_1} \mid -B^\top)$ is a check matrix of a code linearly isometric to $C_0 \otimes C_1$.

E.2.3.17 **Exercise** Let C_0, C_1 and C_2 be linear codes and denote the linear isometry of a linear code C by $\hat{C}$. Deduce from Exercise 2.3.13 and Exercise 2.3.15 that the following sum and product of linear isometry classes

$$\hat{C}_0 \dotplus \hat{C}_1 := \widehat{C_0 \dotplus C_1}, \qquad \hat{C}_0 \otimes \hat{C}_1 := \widehat{C_0 \otimes C_1}$$

are well-defined. Moreover, prove the following assertions:

- $\hat{C}_0 \dotplus \hat{C}_1 = \hat{C}_1 \dotplus \hat{C}_0$.
- $\hat{C}_0 \dotplus (\hat{C}_1 \dotplus \hat{C}_2) = (\hat{C}_0 \dotplus \hat{C}_1) \dotplus \hat{C}_2$.
- $\hat{C}_0 \otimes \hat{C}_1 = \hat{C}_1 \otimes \hat{C}_0$.
- $\hat{C}_0 \otimes (\hat{C}_1 \otimes \hat{C}_2) = (\hat{C}_0 \otimes \hat{C}_1) \otimes \hat{C}_2$.
- $\hat{C}_0 \otimes (\hat{C}_1 \dotplus \hat{C}_2) = (\hat{C}_0 \otimes \hat{C}_1) \dotplus (\hat{C}_0 \otimes \hat{C}_2)$.
- The linear $(1,1)$-code D with generator matrix $\Gamma = (1)$ satisfies $\hat{C} \otimes \hat{D} = \hat{D} \otimes \hat{C} = \hat{C}$ for all linear isometry classes $\hat{C}$.

2.4 Reed–Muller-Codes

From 1969 until 1977, spacecrafts of NASA were equipped with a 7-error-correcting binary $(32, 6)$-code, a Reed–Muller-code. This is a low rate code with good error correction capabilities. A very prominent mission was Mariner 9, which was devoted to the photographic observation of the surface of Mars. Mariner 9 actually entered a Martian orbit in 1971 and became a satellite. The mission was complicated by a heavy dust storm which engulfed the whole Martian surface. It was not until 1972 that the storm subsided and the first clear photos arrived and changed our view of that planet so profoundly. We introduce the Reed–Muller-codes following the original ideas of D.E. Muller [154], who discovered their binary version. However, we will present the more general version of these codes which works for all finite fields $\mathbb{F}_q$. Later on, we will specialize to the binary case.

Reed–Muller-codes are subspaces of the vector space of all mappings

$$f : \mathbb{F}_q^m \to \mathbb{F}_q \ : \ (u_0, \ldots, u_{m-1}) \mapsto f(u_0, \ldots, u_{m-1})$$

with pointwise addition $(f+g)(u) := f(u) + g(u)$ and scalar multiplication $(\alpha f)(u) := \alpha \cdot f(u)$ for $u \in \mathbb{F}_q^m$ and $\alpha \in \mathbb{F}_q$. Together with pointwise multiplication $(fg)(u) := f(u)g(u)$, this set of mappings forms the $\mathbb{F}_q$-algebra (Exercise 2.4.1)

$$\mathcal{B}_m^q.$$

In the case $q = 2$ these are the well-known Boolean functions or switching functions of degree m. It is helpful to note that these functions f are polynomial, i.e. for each $f \in \mathcal{B}_m^q$ there exists a polynomial $\tilde{f} \in \mathbb{F}_q[x_0, \ldots, x_{m-1}]$ such that $f(u) = \tilde{f}(u_0, \ldots, u_{m-1})$ for all $u \in \mathbb{F}_q^m$. For this purpose, we consider both $\mathcal{B}_m^q$ and the space of polynomial functions as vector spaces. Our first goal is to exhibit a basis for this space.

The "unit vectors" of $\mathcal{B}_m^q$ are the functions f_u for $u = (u_0, \ldots, u_{m-1}) \in \mathbb{F}_q^m$ with

$$f_u(v) = \begin{cases} 1 & \text{if } v = u, \\ 0 & \text{else.} \end{cases}$$

A function from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ that takes exactly the same values as f_u is obtained from the polynomial

$$\tilde{f}_u(x_0, \ldots, x_{m-1}) := \prod_{i \in m} \left(1 - (x_i - u_i)^{q-1}\right) \in \mathbb{F}_q[x_0, \ldots, x_{m-1}]. \qquad \textbf{2.4.1}$$

Since $u^{q-1} = 1$, for each element $u \in \mathbb{F}_q^*$ (see 3.2.2), $(x_i - u_i)^{q-1} = 1$ if $x_i \neq u_i$, and so it is clear that this polynomial takes the value 1 exactly at

$$(x_0, \ldots, x_{m-1}) = (u_0, \ldots, u_{m-1}) \in \mathbb{F}_q^m$$

and 0 elsewhere. Any f in $\mathcal{B}_m^q$ is a linear combination

$$f = \sum_{u \in \mathbb{F}_q^m} f(u) f_u \qquad \textbf{2.4.2}$$

of unit vectors f_u, i.e. every element of $\mathcal{B}_m^q$ is a polynomial function. Hence the f_u generate $\mathcal{B}_m^q$ as a vector space. However, the representation is not unique. The non-uniqueness lies in the fact that $x^q - x$ is identically zero on $\mathbb{F}_q$. Thus two polynomials f and g in $\mathbb{F}_q[x_0, \ldots, x_{m-1}]$ induce the same function if and only if f and g are congruent modulo $x_0^q - x_0, \ldots, x_{m-1}^q - x_{m-1}$. This means that f and g cannot be distinguished from their functions if and only if their difference $f - g$ is a polynomial in the terms $x_i^q - x_i$ for $i = 0, \ldots, m-1$. Let us see what this condition means in terms of monomials. We use multi-index notation and let x^b denote the monomial $x_0^{b_0} \cdots x_{m-1}^{b_{m-1}}$ for $b = (b_0, \ldots, b_{m-1})$.

Applying the relation $x_i^q - x_i$ means reducing the exponent b_i modulo $q-1$ in the following sense: If b_i is either zero or not divisible by $q-1$ then $x_i^{b_i}$ may be replaced by $x_i^{a_i}$ where a_i is the remainder after dividing b_i by $q-1$, i.e. a_i is the unique integer in $b_i = c(q-1) + a_i$ with $0 \le a_i < q-1$ (where c is another suitable integer). If $q-1$ divides $b_i \neq 0$ then $x_i^{b_i}$ may be replaced by x_i^{q-1}. It is clear that any polynomial $f \in \mathbb{F}_q[x_0, \ldots, x_{m-1}]$ may be *reduced* to one whose monomials x^a satisfy $0 \le a_i \le q-1$ for $i = 0, \ldots, m-1$. The main point is that if we restrict to polynomials in $\mathbb{F}_q[x_0, \ldots, x_{m-1}]$ which are reduced in this sense then any function in $\mathcal{B}_m^q$ can be expressed uniquely as a reduced polynomial. We summarize this as

2.4.3 Theorem *The $\mathbb{F}_q$-algebra $\mathcal{B}_m^q$ is isomorphic to the ring of polynomials*

$$\mathbb{F}_q[x_0, \ldots, x_{m-1}]$$

modulo $x_0^q - x_0, \ldots, x_{m-1}^q - x_{m-1}$. An $\mathbb{F}_q$-basis is given by the reduced polynomials

$$\left\{ x_0^{b_0} \ldots x_{m-1}^{b_{m-1}} \;\middle|\; b_i \in q \right\}. \qquad \square$$

Because of this result, we will identify the elements f of $\mathcal{B}_m^q$ with polynomial functions in the following.

In the theory of switching functions, the multinomials $x^b = x_0^{b_0} \ldots x_{m-1}^{b_{m-1}}$ are called *minterms*. The *degree* of x^b is the sum of its exponents $\sum_i b_i$, and the degree of $f \in \mathcal{B}_m^q$ is defined to be the largest degree of a multinomial x^b which occurs in a reduced expression of f with a nonzero coefficient (which is at most $m(q-1)$ by the preceding discussion).

Bounding the degree of the polynomials to any number $t \le m(q-1)$ results in a vector subspace of $\mathcal{B}_m^q$ (but not a sub-algebra). This enables us to define the Reed–Muller-codes in the following way:

2.4.4 Definition (Reed–Muller-code) Assume that $0 \le t \le m(q-1)$. The *t-th order Reed–Muller-code* of degree m over $\mathbb{F}_q$ is defined to be

$$\mathrm{RM}_{m,t}^q := \left\{ f \in \mathcal{B}_m^q \;\middle|\; \deg f \le t \text{ or } f = 0 \right\}. \qquad \diamond$$

The considerations above show that the elements of this code can be described in two ways, either as mappings or as polynomials. If we think of them as mappings, we may display the images of all vectors. We may do so by defining another vector of length q^m whose i-th entry is the value of the i-th vector of $\mathbb{F}_q^m$. Of course, one needs to fix an ordering on the elements of $\mathbb{F}_q^m$ for this. Here are a few examples:

Examples 2.4.5

- The 0-th order binary Reed–Muller-code of length $n = 2^m$ consists of the two constant functions 0 and 1. Hence $\mathrm{RM}^2_{m,0}$ is the n-th order binary repetition code.
- The m-th order binary Reed–Muller-code of length 2^m consists of all vectors in $\mathbb{F}_2^{2^m}$.
- The first order binary Reed–Muller-code $\mathrm{RM}^2_{2,1}$ of degree 2 is of length 4 and consists of the vectors in the following table. (In the left column we list the polynomial f and in the right column the values of the corresponding polynomial function.)

f	$f(00)$	$f(10)$	$f(01)$	$f(11)$
0	0	0	0	0
1	1	1	1	1
x_0	0	1	0	1
x_1	0	0	1	1
$x_0 + x_1$	0	1	1	0
$1 + x_0$	1	0	1	0
$1 + x_1$	1	1	0	0
$1 + x_0 + x_1$	1	0	0	1

- The second order binary Reed–Muller-code $\mathrm{RM}^2_{2,2}$ of degree 2 is of length 4 and contains the elements of $\mathrm{RM}^2_{2,1}$ *together* with the codewords shown in the following table:

f	$f(00)$	$f(10)$	$f(01)$	$f(11)$
x_0x_1	0	0	0	1
$1 + x_0x_1$	1	1	1	0
$x_0 + x_0x_1$	0	1	0	0
$x_1 + x_0x_1$	0	0	1	0
$x_0 + x_1 + x_0x_1$	0	1	1	1
$1 + x_0 + x_0x_1$	1	0	1	1
$1 + x_1 + x_0x_1$	1	1	0	1
$1 + x_0 + x_1 + x_0x_1$	1	0	0	0

- A closer examination of $\mathrm{RM}^2_{2,2}$ shows its recursive structure: Each of the 16 polynomials f in

$$\{0, 1, x_0, x_1, \ldots, 1 + x_1 + x_0x_1, 1 + x_0 + x_1 + x_0x_1\}$$

can be written as $f = h + x_1g$, where both h and g are polynomials in the single indeterminate x_0, and therefore uniquely determined. For example,

$$1 + x_1 + x_0x_1 = 1 + x_1(1 + x_0) = h + x_1g.$$

The mappings h (= 1) and g (= $1 + x_0$) take $\mathbb{F}_2^1 = \{(0), (1)\}$ to $\mathbb{F}_2$, and so

$$f : \{(00), (10), (01), (11)\} \to \mathbb{F}_2 : (x_0, x_1) \mapsto h(x_0) + x_1 g(x_0),$$

is of the form

$$f = (h(0), h(1), h(0) + 1 \cdot g(0), h(1) + 1 \cdot g(1)).$$

In terms of code constructions (recall 2.2.15),

$$f = (h \mid h + g),$$

i.e. we obtain

$$\mathrm{RM}_{2,2}^2 = \underbrace{\mathrm{RM}_{1,2}^2}_{=\mathrm{RM}_{1,1}^2} \mid \mathrm{RM}_{1,1}^2,$$

an $(u \mid u + v)$-construction! ◇

More generally, any polynomial f in $\mathrm{RM}_{m,t}^2$ can be expressed (uniquely) in the form

$$f(x_0, \ldots, x_{m-1}) = h(x_0, \ldots, x_{m-2}) + x_{m-1} g(x_0, \ldots, x_{m-2}),$$

where $\deg h \leq t$ and $\deg g \leq t - 1$ (Exercise 2.4.2), and we obtain

2.4.6 Corollary *The Reed–Muller-code* $\mathrm{RM}_{m,t}^2$ *is the* $(u \mid u + v)$*-construction of two Reed–Muller-codes, namely*

$$\mathrm{RM}_{m,t}^2 = \mathrm{RM}_{m-1,t}^2 \mid \mathrm{RM}_{m-1,t-1}^2, \qquad 1 \leq t \leq m.$$

(Note that $\mathrm{RM}_{m,t}^2 = \mathrm{RM}_{m,m}^2$*, if* $t > m$*.) Hence, if* $\Gamma_{m,t}$ *generates* $\mathrm{RM}_{m,t}^2$*, then*

$$\Gamma_{m,t} = \left(\begin{array}{c|c} \Gamma_{m-1,t} & \Gamma_{m-1,t} \\ \hline 0 & \Gamma_{m-1,t-1} \end{array}\right). \qquad \square$$

Its parameters are as follows:

2.4.7 Theorem *The binary Reed–Muller-code* $\mathrm{RM}_{m,t}^2$ *is of type*

$$\left(2^m, \sum_{i=0}^{t} \binom{m}{i}, 2^{m-t}, 2\right).$$

Proof: $\mathrm{RM}^2_{m,t}$ is a linear $(2^m, k)$-code with

$$k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{t},$$

since it has a basis consisting of the multinomials x^b, $0 \leq b_i \leq 1$, $\sum_i b_i \leq t$.

In order to evaluate its minimum distance, we use induction both on m and t. For $m = 1$ and $t = 0, 1$ the statement is clearly true. Now assume that $m > 1$. As we have seen already, the code $\mathrm{RM}^2_{m,0}$ consists of only the two vectors $\mathbf{0}_{2^m}$ and $\mathbf{1}_{2^m}$. Thus $\mathrm{RM}^2_{m,0}$ is the repetition code of length 2^m with minimum distance 2^m, and so the statement is true in this case. Therefore, we can assume that $t \geq 1$. By the induction hypothesis, the Reed–Muller-code $\mathrm{RM}^2_{m-1,s}$ has minimum distance 2^{m-1-s}. From 2.4.6 and 2.2.15 we deduce that $\mathrm{RM}^2_{m,t}$ has minimum distance

$$\min\left\{2 \cdot 2^{m-1-t}, 2^{m-1-(t-1)}\right\} = 2^{m-t}. \qquad \square$$

For example, the above-mentioned code $\mathrm{RM}^2_{5,1}$ used during Mariner missions is of type $(32, 6, 16)$. Therefore, this code can indeed correct 7 errors.

Finally, we also consider the codes which are dual to Reed–Muller-codes:

Theorem *For $0 \leq t < m$, the code dual to $\mathrm{RM}^2_{m,t}$ is $\mathrm{RM}^2_{m,m-t-1}$.* **2.4.8**

Proof: Consider $f \in \mathrm{RM}^2_{m,t}$ and $g \in \mathrm{RM}^2_{m,m-t-1}$. Their product $h = fg$ is of degree not greater than $m - 1$. Hence, h is in $\mathrm{RM}^2_{m,m-1}$ and one can show (Exercise 2.4.3) that h has even weight. Now identify $\mathbb{F}_2^m$ with the set $\{0, \ldots, 2^m - 1\} = 2^m$ via the bijection $(a_0, \ldots, a_{m-1}) \mapsto \sum_{i \in m} a_i 2^i$. Represent f, g, and h as $\mathbb{F}_2^{2^m}$-vectors $(f(i))_{i \in 2^m}$, $(g(i))_{i \in 2^m}$ and $(h(i))_{i \in 2^m}$, respectively. The inner product of f and g is

$$\langle f, g \rangle = \sum_{i \in 2^m} f(i)g(i) = \sum_{i \in 2^m} (fg)(i) = \sum_{i \in 2^m} h(i) = 0,$$

since h has even weight. For this reason, $\mathrm{RM}^2_{m,m-t-1}$ is contained in the dual of $\mathrm{RM}^2_{m,t}$. Moreover, the dimension of $\mathrm{RM}^2_{m,m-t-1}$ is

$$\sum_{i \in m-t} \binom{m}{i} = \sum_{i=t+1}^{m} \binom{m}{i} = 2^m - \dim(\mathrm{RM}^2_{m,t}) = n - k,$$

whence $\mathrm{RM}^2_{m,m-t-1}$ is the dual of $\mathrm{RM}^2_{m,t}$, as stated. $\square$

Another more algebraic description of Reed–Muller-codes will be presented in Section 4.10.

The binary Reed–Muller-code $\mathrm{RM}^2_{m,m}$, which is $\mathbb{F}_2^{2^m}$, has a generator matrix with a highly recursive structure. (See also [84, first edition, Section 8.11.2].) Clearly, for $m = 0$

$$\Gamma_0 := (\,1\,)$$

is a generator matrix of $\mathrm{RM}^2_{0,0}$. According to 2.4.6, for $m > 0$ the Reed–Muller-code $\mathrm{RM}^2_{m,m}$ is the $(u \mid u+v)$-construction

$$\mathrm{RM}^2_{m,m} = \mathrm{RM}^2_{m-1,m-1} \mid \mathrm{RM}^2_{m-1,m-1},$$

since obviously $\mathrm{RM}^2_{m-1,m} = \mathrm{RM}^2_{m-1,m-1}$. Therefore, it has a generator matrix of the form

$$\Gamma_m := \left(\begin{array}{c|c} \Gamma_{m-1} & \Gamma_{m-1} \\ \hline 0 & \Gamma_{m-1} \end{array}\right)$$

where Γ_{m-1} is a generator matrix of $\mathrm{RM}^2_{m-1,m-1}$. The matrix Γ_m is an upper triangular matrix. In order to describe it in more detail and to show further properties of Reed–Muller-codes, in particular relations to Hamming- and simplex-codes, we label its rows (respectively columns) from top to bottom (respectively from left to right) with values from 0 to $2^m - 1$. We express the row number i in binary form, $i = \sum_{j\in m} b_j 2^j$ and identify i with the characteristic set $B_i := \{j \in m \mid b_j \neq 0\}$. Finally, we associate B_i with the monomial $\prod_{j\in B_i} x_j$.

We also express the column index i in binary form as $i = \sum_{j\in m} t_j 2^j$. This means that t_j takes the value 0 in all columns with index

$$i \in \bigcup_{r\in 2^{m-j-1}} \left\{ s \in \mathbb{N} \mid 2r2^j \leq s < (2r+1)2^j \right\}.$$

In all other columns t_j takes the value 1. The (i,j)-th entry of Γ_m is the monomial associated with the characteristic set B_i evaluated at $(x_0, \ldots, x_{m-1}) = (t_0, \ldots, t_{m-1}) \in \mathbb{F}_2^m$ where $(t_0, \ldots, t_{m-1})$ is determined by j.

From this description it is easy to compute directly (i.e. without recursion) the entries of the i-th row $(y_0, \ldots, y_{2^m-1})$ of Γ_m. Let B_i be the characteristic set of i, then for

$$t \in \bigcup_{j\in B_i} \Big(\bigcup_{r\in 2^{m-j-1}} \left\{ s \in \mathbb{N} \mid 2r2^j \leq s < (2r+1)2^j \right\} \Big)$$

we have $y_t = 0$. Otherwise $y_t = 1$.

If we have two characteristic sets B_i and B_j, then $B_i \cup B_j$ is also a characteristic set, of row ℓ say. There occurs the entry 1 in the t-th position of the ℓ-th row if and only if both in the i-th row and in the j-th row there is the

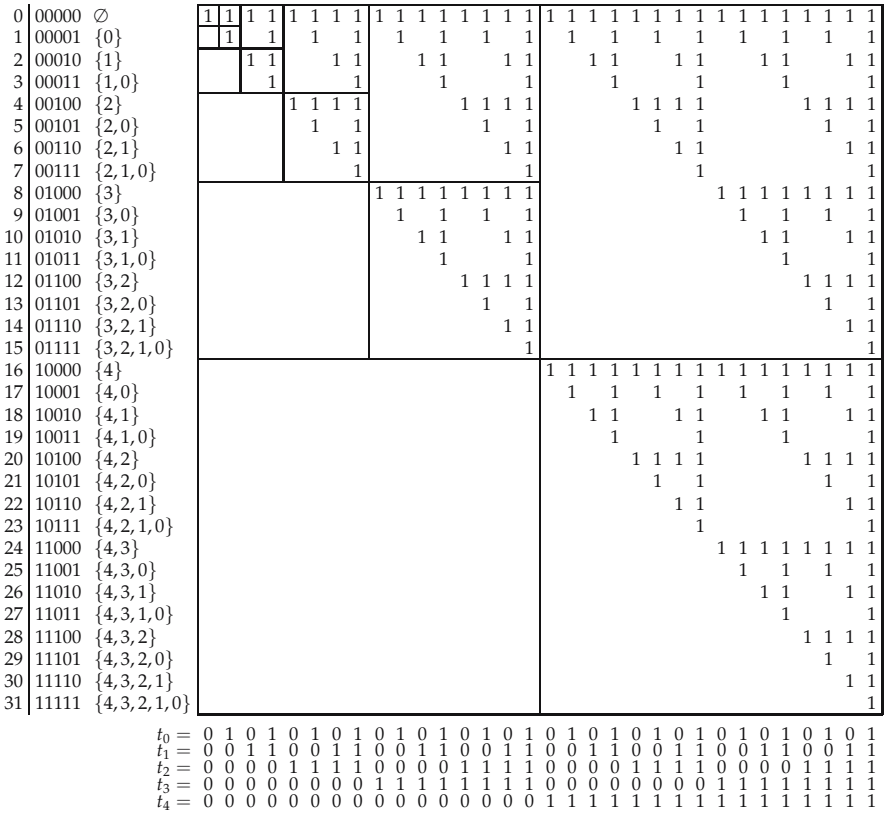

Fig. 2.2 Recursive structure of a generator matrix of $\mathrm{RM}^2_{5,5}$

entry 1 in the t-th coordinate. Hence, knowing the rows corresponding to all characteristic sets of cardinality 1, it is easy to write down any other row of Γ_m.

We recall the recursive structure of the generator matrix in the general case of a binary Reed–Muller-code. For $0 \le t \le m$,

$$\Gamma_{m,t} = \left(\begin{array}{c|c} \Gamma_{m-1,t} & \Gamma_{m-1,t} \\ \hline 0 & \Gamma_{m-1,t-1} \end{array}\right)$$

Of course $\Gamma_{m,m} = \Gamma_m$ is a generator matrix of $\mathrm{RM}^2_{m,m}$. The matrix $\Gamma_{m,0}$ contains just one vector, the all-one vector, which is the top row of Γ_m (cf. Exercise 2.4.4). It is a generator matrix of the repetition code $\mathrm{RM}^2_{m,0}$. The identification of characteristic sets and monomials shows that $\Gamma_{m,t}$ is a generator matrix of $\mathrm{RM}^2_{m,t}$. We call it the *canonical generator matrix* of $\mathrm{RM}^2_{m,t}$.

2.4.9 **Example** Figure 2.2 shows a generator matrix of $\mathrm{RM}^2_{5,5}$. The rows are labeled by integers, the corresponding binary numbers and characteristic sets. The columns are labeled by the $(t_0, \ldots, t_4) \in \mathbb{F}_2^5$. ◇

2.4.10 **Theorem** *For $0 \leq t < m$, the Reed–Muller-code $\mathrm{RM}^2_{m,t}$ is even.*

Proof: For $t = 0$, the Reed–Muller-code is the binary repetition code of length 2^m. From the recursive construction of Γ_m it is clear that each row with exception of the last one has even weight. If $t > 0$, by puncturing $\mathrm{RM}^2_{m,t}$ in the last component, we obtain the code $Pu(\mathrm{RM}^2_{m,t})$. All rows in its generator matrix have odd weight. Hence by 1.6.3, exactly half of its codewords have odd weight. Thus, the Reed–Muller-code $\mathrm{RM}^2_{m,t}$ is the parity extension of $Pu(\mathrm{RM}^2_{m,t})$ which contains codewords of even weight only. □

Adding the first row to all remaining rows of $\Gamma_{m,s}$ we obtain another generator matrix $\tilde{\Gamma}_{m,s}$ of $\mathrm{RM}^2_{m,s}$. Apart from the first row, any row of $\tilde{\Gamma}_{m,s}$ is the complement of the corresponding row of $\Gamma_{m,s}$. The last column of $\tilde{\Gamma}_{m,s}$ is $(1, 0, \ldots, 0)^\top$. Due to 2.4.8, for $0 \leq s \leq m-1$ the matrix $\tilde{\Gamma}_{m,m-s-1}$ is a check matrix of $\mathrm{RM}^2_{m,s}$. Hence, from Exercise 1.3.10 we derive that $\Gamma_{m,s} \cdot \tilde{\Gamma}^\top_{m,m-s-1} = 0$. Moreover, if $s < m-1$ then we may write

$$\Gamma_{m,s} = (\Gamma \mid \mathbf{1}^\top) \text{ and } \tilde{\Gamma}_{m,m-s-1} = \left(\begin{array}{c|c} \mathbf{1} & 1 \\ \hline \tilde{\Gamma} & \mathbf{0}^\top \end{array}\right)$$

where Γ is a generator matrix of $Pu(\mathrm{RM}^2_{m,s})$ and $\tilde{\Gamma}$ is a matrix with $\sum_{i=1}^{m-s-1} \binom{m}{i}$ rows and $2^m - 1$ columns. The rows of $\tilde{\Gamma}$ are orthogonal to the rows of Γ. Therefore, $\tilde{\Gamma}$ is the generator matrix of the dual code $Pu(\mathrm{RM}^2_{m,s})^\perp$.

If $s = m-2$, the columns of the $m \times (2^m - 1)$-matrix $\tilde{\Gamma}$ are exactly all nonzero vectors in $\mathbb{F}_2^m$. Thus $\tilde{\Gamma}$ is a generator matrix both of the m-th order binary simplex-code and of $Pu(\mathrm{RM}^2_{m,m-2})^\perp$. In other words, $\tilde{\Gamma}$ is a check matrix of the m-th order binary Hamming-code and a check matrix of $Pu(\mathrm{RM}^2_{m,m-2})$. Conversely, the matrix

$$\left(\begin{array}{c} \mathbf{1} \\ \hline \tilde{\Gamma} \end{array}\right)$$

is a generator matrix of $Pu(\mathrm{RM}^2_{m,1})$, whence $Pu(\mathrm{RM}^2_{m,1})$ is the augmentation of the m-th order binary simplex-code (cf. 2.3.2). We collect these results in the following

2.4.11 **Theorem**

1. *$\mathrm{RM}^2_{m,m-2}$ is the parity extension of the m-th order binary Hamming-code.*

2. *$Pu(\mathrm{RM}^2_{m,1})$ is the augmentation of the m-th order binary simplex-code.*
3. *The weight distributions of $Pu(\mathrm{RM}^2_{m,1})$ and $\mathrm{RM}^2_{m,1}$ are given by*

$$w_{Pu(\mathrm{RM}^2_{m,1})}(x) = 1 + (2^m - 1)x^{2^{m-1}-1} + (2^m - 1)x^{2^{m-1}} + x^{2^m-1}$$

and

$$w_{\mathrm{RM}^2_{m,1}}(x) = 1 + 2(2^m - 1)x^{2^{m-1}} + x^{2^m},$$

respectively.

Proof: The first two assertions follow directly from the considerations above. The weight distribution of the simplex-code was determined in 2.1.7. The final statement follows from the definitions of augmentation and puncturing. □

Example From the matrix **2.4.12**

$$\Gamma_{5,1} = \begin{pmatrix}
1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\\
0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\\
0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\\
0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\\
0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1
\end{pmatrix}$$

we obtain the matrix

$$\tilde{\Gamma}_{5,1} = \begin{pmatrix}
1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\\
1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\\
1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\\
1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\\
1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0
\end{pmatrix}$$

and

$$\tilde{\Gamma} = \begin{pmatrix}
1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\\
1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\\
1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\\
1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\\
1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0
\end{pmatrix},$$

a generator matrix of the 5-th order binary simplex-code. ◇

Exercises

Exercise Prove that $\mathcal{B}^q_m$ is in fact an $\mathbb{F}_q$-algebra, which means that it is both a vector space over $\mathbb{F}_q$ and a ring so that **E.2.4.1**

$$\alpha(f \cdot g) = (\alpha f) \cdot g = f \cdot (\alpha g)$$

holds true, for all $\alpha \in \mathbb{F}_q$ and $f, g \in \mathcal{B}^q_m$.

E.2.4.2 **Exercise** Show that each polynomial f in $\mathrm{RM}^2_{m,t}$ can be uniquely expressed in the form

$$f(x_0,\ldots,x_{m-1}) = h(x_0,\ldots,x_{m-2}) + x_{m-1}g(x_0,\ldots,x_{m-2}),$$

where $\deg h \leq t$ and $\deg g \leq t-1$.

E.2.4.3 **Exercise** Verify that the $(m-1)$-th order binary Reed–Muller-code of length 2^m consists of all vectors of even weight in $\mathbb{F}_2^{2^m}$.

E.2.4.4 **Exercise** Check that the top row and the rightmost column in the canonical form of $\Gamma_{m,t}$ consist of all-one vectors.

E.2.4.5 **Exercise** Write down Pascal's triangle, reduce the entries modulo 2 and compare with the generator matrix of the Reed–Muller-code in Fig. 2.2. Do you see a connection?

2.5 MDS-Codes

As MacWilliams and Sloane [139] put it, *we come now to one of the most fascinating chapters in all of coding theory: MDS-codes*. As we have seen in 2.1.1, for any (n,k,d)-code over any field we have $d \leq n-k+1$. Codes with $d = n-k+1$ have been called *maximum distance separable*, or MDS for short. These codes have a wide range of applications, and they tie in well with structures in projective geometry. The compact disc stores music using linear $(32,28,5)$ and $(28,24,5)$-MDS-codes over $\mathbb{F}_{2^8}$ (for details see Chapter 5). *Trivial* MDS-codes are the codes of types $(n,1,n)$, $(n,n-1,2)$, and $(n,n,1)$, which exist over any field $\mathbb{F}_q$ (cf. Exercise 2.5.1). Here we collect some properties characterizing MDS-codes:

2.5.1 **Theorem** *For linear (n,k)-codes C the following properties are equivalent:*

1. *C is an MDS-code.*
2. *In each check matrix of C any $n-k$ columns are linearly independent.*
3. *In each generator matrix of C any k columns are linearly independent.*
4. *$C^\perp$ is an MDS-code.*

Proof: The equivalence of the first two statements follows from 1.3.9 and the Singleton-bound 2.1.1. Together with 1.3.4 we obtain the equivalence of the third and the fourth property.

Now assume that C is an MDS-code, i.e. that $d = n-k+1$. To show that $C^\perp$ is also MDS, we prove that its minimum distance $d^\perp$ equals $n-(n-k)+1 = k+1$. Assume, indirectly, that $C^\perp$ contains an element $c \neq 0$ of Hamming weight at most k. Each nonzero element of the dual code can occur as a row in a check matrix of C. Let Δ be a check matrix of C containing c as its top row. Now consider the columns of Δ which are zero in their top component. By assumption, there are at least $n-k$ of them. Since Δ has $n-k$ rows, these columns are dependent. According to 1.3.9, these columns give rise to a word in C of weight at most $n-k$, which contradicts the assumption. This shows that $d^\perp \geq k+1$. From the Singleton-bound we obtain $d^\perp \leq n-(n-k)+1 = k+1$ so finally $d^\perp = k+1$, which means that $C^\perp$ is MDS.

A symmetric argument shows that C is MDS provided that $C^\perp$ has this property. □

The third item of 2.5.1 yields

Corollary 2.5.2 *An (n,k)-code is MDS if and only if any k coordinates form an information set.* □

Recall that $\mathbb{F}_q^{(J)}$ has been defined in 1.7.4 as the set of vectors which are zero on all of $\overline{J}$. It is a subspace of dimension $|J|$.

Theorem 2.5.3 *For each (n,k,d,q)-code C the following statements are equivalent:*

1. *C is an MDS-code.*
2. *For each $J \subseteq n$ with $|J| = d-1$ we have $C \oplus \mathbb{F}_q^{(J)} = \mathbb{F}_q^n$.*
3. *For each $J \subseteq n$ with $|J| = k$ we have $C \oplus \mathbb{F}_q^{(\overline{J})} = \mathbb{F}_q^n$.*

Proof: Let C denote an MDS-code and consider a set $J \subseteq n$ with $|J| = d-1$. By 1.7.7

$$C \oplus \mathbb{F}_q^{(J)} \subseteq \mathbb{F}_q^n.$$

Counting dimensions we see that the space on the left hand side is of dimension $k+(d-1) = n$, since C is MDS. Thus $C \oplus \mathbb{F}_q^{(J)} = \mathbb{F}_q^n$.

Conversely, assume that $C \oplus \mathbb{F}_q^{(J)} = \mathbb{F}_q^n$ for some $J \subseteq n$ with $|J| = d-1$. Then $k = \dim(C) = n-d+1$, i.e. C is MDS. The equivalence between the first and the third statement can be derived from 2.5.2 together with 1.7.6. □

2.5.4 **Theorem** *Suppose that C is an (n,k)-code with systematic generator matrix $\Gamma = (I_k \mid A)$. Then C is MDS if and only if, for each $i = 1,\dots,\min\{k, n-k\}$, all $i \times i$-submatrices of A are regular.*

Proof: We assume that C is an MDS-code. We introduce some notation. For a matrix M, and for X and Y subsets of the sets of row and column indices, let $M_{X,Y}$ be the submatrix containing the elements of A which are at the intersection of rows indexed by elements of X and columns indexed by elements of Y. Moreover, $\overline{X}$ denotes the complement of X in the set of row indices. Now consider $\Gamma = (I_k \mid A)$ and let $k = \{0,\dots,k-1\}$ and $\{k,\dots,n-1\} = n \setminus k$ be index sets for the matrix $A = (a_{ij})_{i\in k,\, j\in n\setminus k}$. Assume that $A' = A_{X,Y}$ is a submatrix of A consisting of $i \le \min\{k, n-k\}$ rows and columns, i.e. with $X \subseteq k$, and $Y \subseteq \{k,\dots,n-1\}$ and $|X| = |Y| = i$. Consider the matrix of k columns of Γ

$$A'' = \left(\begin{array}{c|c} I_{X,\overline{X}} & A_{X,Y} \\ \hline I_{\overline{X},\overline{X}} & A_{\overline{X},Y} \end{array}\right) = \left(\begin{array}{c|c} 0 & A' \\ \hline I_{k-i} & * \end{array}\right),$$

where 0 denotes the $i \times (k-i)$ zero matrix and where $*$ denotes a $(k-i) \times i$-matrix. According to 2.5.1, A'' is regular and hence $\det A'' = \pm \det A' \neq 0$.

The converse of this statement follows directly from 2.5.1. □

2.5.5 **Example** We consider the $(4,2)$-code C over the field with four elements $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ subject to the relation $\alpha^2 = 1 + \alpha$ with $\Gamma = (I \mid A)$, where

$$A = \begin{pmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha \end{pmatrix}.$$

Since each $i \times i$-submatrix of A is regular ($i = 1, 2$), C is MDS. ◇

2.5.6 **Theorem** *Up to linear isometry, each MDS-code is generated systematically by a matrix $\Gamma = (I \mid B)$, where B is of the form*

$$B = \left(\begin{array}{c|c} 1 & \mathbf{1} \\ \hline \mathbf{1}^\top & * \end{array}\right).$$

Proof: Up to isometry we may assume that the code is generated systematically by the matrix $\Gamma = (I \mid A)$ where $A = \left(a_{ij}\right)_{i\in k, j\in n\setminus k}$. By 2.5.4, all entries of A are nonzero, so that

$$D = \operatorname{diag}\left(1, \frac{a_{1,k}}{a_{0,k}}, \dots, \frac{a_{k-1,k}}{a_{0,k}}, a_{0,k}^{-1}, \dots, a_{0,n-1}^{-1}\right)$$

is a regular diagonal matrix. From 1.7.3 we know that $(I \mid A)$ and $(I \mid D * A) = (I \mid B)$ generate linearly isometric codes. Moreover, we know from 1.7.2 that

$$b_{ij} = d_{ii}^{-1} a_{ij} d_{jj}.$$

Hence, an easy check shows that the leftmost column and the top row consist of all-one vectors, as stated. □

Let us now discuss the question of when MDS-codes exist.

Theorem 2.5.7 *For each (n,k)-MDS-code over $\mathbb{F}_q$ with $2 \leq k \leq n-2$ the inequality*

$$q \geq \max\{k, n-k\} + 1$$

holds true.

Proof: By 2.5.6, each MDS-code is linearly isometric to an MDS-code with a systematic generator matrix $\Gamma = (I \mid B)$, where

$$B = \left(\begin{array}{c|c} 1 & \mathbf{1} \\ \hline \mathbf{1}^\top & B' \end{array}\right).$$

By 2.5.4, each $i \times i$-submatrix of B is regular. In particular, the 2×2-submatrices containing two elements of the highest row or of the left column have determinants

$$\det\begin{pmatrix} 1 & 1 \\ \alpha & \alpha' \end{pmatrix} = \alpha' - \alpha \quad \text{and} \quad \det\begin{pmatrix} 1 & \alpha \\ 1 & \alpha' \end{pmatrix} = \alpha' - \alpha$$

distinct from zero. Consequently, the elements in the rows and in the columns of B' are pairwise distinct and also distinct from 0 and 1. For this reason, the alphabet $\mathbb{F}_q$ contains at least $\max\{k-1, n-k-1\} + 2$ elements. □

Example 2.5.8 By the previous theorem, there are no nontrivial binary MDS-codes. For $n \geq 4$, $(n,2)$-MDS-codes over $\mathbb{F}_q$ with $q \geq n-1$ exist, they are generated by $(I \mid B)$ where B is any matrix of the form

$$B = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & b_{1,3} & \dots & b_{1,n-1} \end{pmatrix},$$

where $b_{1,3}, \dots, b_{1,n-1}$ are pairwise different field elements, which are all distinct from both 0 and 1. ◇

Theorem 2.5.9 *For any $n \geq 6$ there exists an $(n,3)$-MDS-code over $\mathbb{F}_q$ with $q = 2^m$ and $q \geq n-2$.*

Proof: Assume that $0, b_3 := 1, b_4, \dots, b_{n-1}$ are pairwise distinct elements in $\mathbb{F}_q$ with $q = 2^m$. From $q \geq n-2$ it follows that $m \geq 2$. We form the matrix

$$B = \begin{pmatrix} 1 & 1 & \dots & 1 \\ b_3 & b_4 & \dots & b_{n-1} \\ b_3^2 & b_4^2 & \dots & b_{n-1}^2 \end{pmatrix},$$

and consider the $(n,3)$-code C over $\mathbb{F}_q$ generated by $(I \mid B)$. From 2.5.4 it follows that C is MDS: To begin with, each 3×3-submatrix of B is a Vandermonde matrix and hence regular (cf. Exercise 2.5.2). Furthermore, each 2×2-submatrix

$$\begin{pmatrix} b_i & b_j \\ b_i^2 & b_j^2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ b_i & b_j \end{pmatrix}, \qquad 3 \le i < j \le n-1,$$

is non-singular. Finally, the elements 0, 1, b_4^2, $\ldots$, b_{n-1}^2 are pairwise distinct, since by 3.2.13 the Frobenius mapping $\mathbb{F}_{2^m} \ni \alpha \mapsto \alpha^2 \in \mathbb{F}_{2^m}$ is an automorphism. Hence, the submatrices

$$\begin{pmatrix} 1 & 1 \\ b_i^2 & b_j^2 \end{pmatrix}, \qquad 3 \le i < j \le n-1,$$

are also regular. □

The condition $q = 2^m$ turns out to be necessary (see Exercise 2.5.5).

2.5.10 **Example** By 2.5.9, the $(6,3)$-code over $\mathbb{F}_4 = \{0,1,\alpha,\alpha+1\}$ $(\alpha^2 = \alpha + 1)$ with generator matrix

$$\Gamma = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha \end{pmatrix}$$

is MDS. This code is known as the *hexacode.* ◇

Let $N_q(k)$ be the maximal length of an MDS-code of dimension k over $\mathbb{F}_q$. From 2.5.7 and 2.5.9 we obtain the important

---

2.5.11 **Corollary** *For $q = 2^m$ we have $N_q(3) = q + 2$.* □

For all other cases we have the following conjecture ([139], p. 328):

$$N_q(k) = \begin{cases} q+1 & \text{if } 2 \le k \le q, \\ k+1 & \text{if } q < k. \end{cases}$$

Finally, let us consider the weight distribution of MDS-codes.

2.5.12 **Theorem** *Suppose that C is an (n,k)-MDS-code over $\mathbb{F}_q$. We denote by A_i the number of codewords in C of weight i. Then the following holds:*

- $A_0 = 1$, $A_1 = A_2 = \ldots = A_{n-k} = 0$.
- *For each $i \in \{0,1,\ldots,k-1\}$:*

$$A_{n-i} = \sum_{m=i}^{k-1} (-1)^{m-i} \binom{m}{i} \binom{n}{m} (q^{k-m} - 1).$$

Proof: For each subset J of $n = \{0, \ldots, n-1\}$, let $C(\overline{J})$ denote the set of codewords in C whose components c_j for $j \in J$ are all zero. i.e.

$$C(\overline{J}) := \left\{ c \in C \;\middle|\; \forall\, j \in J \;:\; c_j = 0 \right\}.$$

Since each nonzero codeword in C has at most $k-1$ zero entries, $C(\overline{J}) = \emptyset$ for each J with $|J| \geq k$.

For each m with $0 \leq m \leq k-1$ we determine the cardinality of the set

$$\mathcal{S} = \left\{ (J, c) \;\middle|\; J \in \binom{n}{m},\ 0 \neq c \in C(\overline{J}) \right\} \qquad \textbf{2.5.13}$$

in two different ways. (Here $\binom{n}{m}$ indicates the set of all m-subsets of the set n.) On the one hand, each k-subset of n is an information set of C, and hence by 1.7.6 for each $J \subseteq n$ with $|J| \leq k-1$ we have

$$|C(\overline{J})| = q^{k-|J|}.$$

Thus the set $\mathcal{S}$ is of cardinality

$$\binom{n}{m} \cdot (q^{k-m} - 1).$$

On the other hand, we may decompose the set of codewords of C into sets

$$C_i := \{ c \in C \mid \mathrm{wt}(c) = n - i \} \;\text{ for }\; 0 \leq i \leq n.$$

Thus, the coefficients of the weight distribution are $A_{n-i} = |C_i|$. If $i \geq m$, for each $c \in C_i$ there are exactly $\binom{i}{m}$ subsets J of n of cardinality m such that $c \in C(\overline{J})$. Hence, there exist exactly $\binom{i}{m} \cdot A_{n-i}$ pairs of the form (J, c) with $c \in C_i \cap C(\overline{J})$. Thus, the set $\mathcal{S}$ of 2.5.13 is of cardinality

$$\sum_{i=m}^{k-1} \binom{i}{m} \cdot A_{n-i}.$$

This way we obtain the following system of k equations in the k indeterminates $A_{n-k+1}, \ldots, A_n$:

$$\sum_{i=m}^{k-1} \binom{i}{m} \cdot A_{n-i} = \binom{n}{m} \cdot (q^{k-m} - 1), \qquad 0 \leq m \leq k-1.$$

Rearranging the indeterminates as $A_n, \ldots, A_{n-k+1}$, the coefficient matrix of this system of equations turns out to be upper triangular with ones along its main diagonal, i.e. with determinant 1. Therefore this system has a unique solution, which is given by (Exercise 2.5.6)

$$A_{n-i} = \sum_{m=i}^{k-1} (-1)^{m-i} \binom{m}{i} \binom{n}{m} (q^{k-m} - 1), \qquad 0 \leq i \leq k-1. \qquad \square$$

The weight distribution gives an upper bound for $N_q(k)$.

2.5.14 **Lemma** *For each $k \geq 2$ we have $N_q(k) \leq q + k - 1$.*

Proof: Every (n,k)-MDS-code over $\mathbb{F}_q$ satisfies

$$\begin{aligned} A_{n-k+2} &= \binom{n}{k-2}(q^2-1) - (k-1)\binom{n}{k-1}(q-1) \\ &= \binom{n}{k-2}(q-1)(q-1-(n-k)). \end{aligned}$$

As A_{n-k+2} cannot be negative, the factor $q-1-n+k$ is ≥ 0. □

Exercises

E.2.5.1 **Exercise** Prove that trivial MDS-codes of length n exist over every finite field.

E.2.5.2 **Exercise** Consider field elements $\alpha_0, \ldots, \alpha_{n-1}$. Show that the *Vandermonde matrix*

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1}^2 & \ldots & \alpha_{n-1}^{n-1} \end{pmatrix}$$

has as determinant the expression

$$\prod_{i<j}(\alpha_j - \alpha_i) = \prod_{i=0}^{n-2}\prod_{j=i+1}^{n-1}(\alpha_j - \alpha_i).$$

In particular, this determinant is nonzero provided that $\alpha_i \neq \alpha_j$ for $i \neq j$.

E.2.5.3 **Exercise** Show that every shortened MDS-code is again MDS.

E.2.5.4 **Exercise** Construct a $(5,2)$-MDS-code over the field $\mathbb{F}_5$.

E.2.5.5 **Exercise** Prove that there is no $(7,4)$-MDS-code over $\mathbb{F}_5$. Hint: use 2.5.4.

E.2.5.6 **Exercise** Prove

$$\binom{n}{m}\binom{m}{p} = \binom{n}{p}\binom{n-p}{m-p}, \qquad p \leq m \leq n.$$

Verify that for $0 \leq m \leq n$ the identity

$$\sum_{k=m}^{n} (-1)^{n-k} \binom{n}{k} \binom{k}{m} = \begin{cases} 0 & \text{if } n \neq m, \\ (-1)^{n-m} & \text{if } n = m \end{cases}$$

holds true. Fill in the missing details of the proof of 2.5.12.

Exercise Show that the nonzero coefficients in the weight enumerator of the hexacode of Example 2.5.10 are $A_0 = 1$, $A_4 = 45$ and $A_6 = 18$. **E.2.5.7**

Exercise Determine the weight enumerator of the $(6,3)$-MDS-code over $\mathbb{F}_5$ which is generated by **E.2.5.8**

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

Exercise Prove that for $n - k + 1 \leq r \leq n$ the coefficients A_r in the weight distribution of an (n,k)-MDS-code over $\mathbb{F}_q$ are given by **E.2.5.9**

$$A_r = \binom{n}{r} \sum_{i \in r-d+1} (-1)^i \binom{r}{i} (q^{r-i-d+1} - 1).$$

Exercise Show that the two $(10,5)$-codes over $\mathbb{F}_9$ generated by **E.2.5.10**

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 2+\eta & 1+\eta & \eta & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 1+\eta & 1+2\eta & 2\eta & \eta & 1 & 0 & 0 & 2 & 0 & 0 \\ 2\eta & 2+2\eta & 1+\eta & 2+\eta & 1 & 0 & 0 & 0 & 2 & 0 \\ 1+2\eta & 2 & 2+2\eta & 2\eta & 1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 2+\eta & 1+\eta & \eta & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 2+2\eta & 2+\eta & 2\eta & 1+\eta & 1 & 0 & 0 & 2 & 0 & 0 \\ 2\eta & 2+2\eta & 2 & 1+2\eta & 1 & 0 & 0 & 0 & 2 & 0 \\ 1+2\eta & \eta & 2+\eta & 2+2\eta & 1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

are semilinearly inequivalent and MDS. Here, we have $\mathbb{F}_9 = \{a + b\eta \mid a, b \in \mathbb{F}_3\}$ subject to the relation $\eta^2 = 2\eta + 1$. (The first code is obtained from a rational normal curve, with automorphism group $\mathrm{P\Gamma L}_2(9)$ of order 1440. The second code is obtained from the Glynn-arc [69] in $\mathrm{PG}_4(9)$, with automorphism group $\mathrm{PGL}_2(9)$ of order 720. Both automorphism groups act transitively on the 10 coordinates. It is known that there is no $(11,6)$-MDS-code over $\mathbb{F}_9$.)